Kreuzer · Robbiano
Computational Commutative Algebra 2

Martin Kreuzer · Lorenzo Robbiano

Computational Commutative Algebra 2

Springer

Martin Kreuzer
Universität Dortmund
Fachbereich Mathematik
44221 Dortmund, Germany
e-mail: Martin.Kreuzer@mathematik.uni-dortmund.de

Lorenzo Robbiano
Università di Genova
Dipartimento di Matematica
Via Dodecaneso 35
16146 Genova, Italy
e-mail: robbiano@dima.unige.it

Library of Congress Control Number: 00046340

Mathematics Subject Classification (2000): Primary: 13P10; Secondary: 68W30, 13A02, 13D40, 14Qxx

ISBN-10 3-540-25527-3 Springer-Verlag Berlin Heidelberg

ISBN-13 978-3-540-25527-7 Springer-Verlag Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media
springeronline.com

Printed in The Netherlands

Typesetting: by the authors and TechBooks using a Springer LaTeX macro package
Cover design: *design & production GmbH*, Heidelberg

SPIN: 11000211 46/TechBooks - 5 4 3 2 1 0 – Printed on acid-free paper

Foreword

Hofstadter's Law: It always takes longer than you think it will take, even if you take into account Hofstadter's Law.
(Douglas R. Hofstadter)

Dear Reader,

why did we begin the foreword of this second volume with the same quote as the first? There we wrote that it took three years of intense work just to fill three centimeters of your bookshelf. The completion of this volume took four years and it is about four centimeters thick. Thus we have a confirmed invariant which governs our writing: our velocity is one centimeter per year, after all effects due to Hofstadter's Law have been taken into account. When we started this project in the last millennium, we planned a book for learning, teaching, reading and, most of all, enjoying the topic at hand. Surely there is no law which says that a mathematical book has to be dull, boring, dry, or tedious. But how do you make it enjoyable?

Our approach has been to fill it with amusing quotes, varied jokes, funny word games, flowery metaphors and occasional literary efforts. There are two possible drawbacks of this method. Firstly, not everyone has the same sense of humour and not every metaphor works as intended. For instance, it is easy to joke about certain politicians, but what happens if they read this book? And when we wrote of a small boat sailing slowly into the Brazilian sunset, it was pointed out to us that this entails a geographical problem. Secondly, it is very difficult to write humorously in a foreign language. In the foreword of our first book, we acknowledged a modest lack of linguistic sophistication. This time around, our scribbling has utterly changed for the worse. When confronted with a concoction such as

> ... and if the whole section was a piece of cake for you, bring your bite to bear on Tutorials 47 and 48 [...].

even our hardest, steadfastest advisors John Abbott and Tony Geramita had to concede soft spots. The most enthusiastic remark we could wring from them was that one can find almost every word we use in an English dictionary. But if a word in the dictionary were *mispelled*, how would we know? Should we have taken more heed of the suggestions of our readers, one of whom

recommended correcting "I is an ideal" to "I am an ideal"? And what about definitions like "A flower is an educated weed"?

Another source for trouble were commas. Their distribution in this volume is rather random, because we were puzzled by rules such as the following one: "If you use then after an if, then don't put a comma before then."

I must thank my parents,
but mostly my mother and my father.
("Spillo" Altobelli)

As with the first volume, the second is really a joint effort of many people. We won't bore you with platitudes about how many people contributed to this book; we'll just bore you with a complete list of those people. A special mention goes to John Abbott who spent a lot of time, and almost all his patience, to help us improve our text. Moreover, he continually stimulated our writing with profound and enlightening remarks. Further substantial proofreading was done by Valentina Bertella, Anna Bigatti, Achim Kehrein, and Tony Geramita. We are also grateful to Laura Bazzotti, Henrik Bresinsky, Aldo Conca, Giorgio Dalzotto, Giulio Genovese, Daniel Heldt, Eva Ludwig, Matthias Machnik, and Maria Evelina Rossi for helpful remarks. In spite of this extensive proofreading, the book still contains infinitely many errors. (Proof by induction: You can always find another one.) We shoulder the full responsibility for everything that is still wrong, in particular if we have any words out.

Let us also not forget the many other people who have contributed to this book in more indirect ways: all famous and infamous people (including ourselves) whose quotes we abused, the soccer players of our favourite teams Bayern München and Juventus Turin who showed us that we were not the only ones who had their ups and downs, and the central bankers of this world who furnished us with never-ending amazement about their uncanny ability to create money out of nothing. Very instrumental in the writing of this book was the support we received from our families. Our wives Bettina and Gabriella and our children Chiara, Francesco, Katharina, Veronika, as well as the latest addition, Martin junior, devoted a significant part of their lives to aid us as much as possible.

A very special "thank you" goes to the Springer team, in particular to Dr. Martin Peters and his assistant Ruth Allewelt, for their efficient and professional help in the editorial and production part of this endeavour. Last, but not least, we acknowledge the book itself: after we have spent the better part of eight years putting much of what we know about computer algebra into it, the book knows more than we do since it also remembers what we have already forgotten. May it be as enjoyable and instructive to you as it is to us!

Martin Kreuzer and Lorenzo Robbiano,
Dortmund and Genova, March 2005

Contents

Introduction

Writing, for him who knows it
is better than all other professions;
it pleases more than bread and beer,
more than clothing and ornament.
(20^{th} Dynasty, Egypt)

0.1 What Is This Book About?

The title of this book is "Computational Commutative Algebra 2". It is the natural continuation of "Computational Commutative Algebra 1" written by us in the last millennium. In the introduction to the first volume we wrote that the fundamental ideas of Computational Commutative Algebra were deeply rooted in the development of mathematics in the 20^{th} century, and that we planned to be back with more in the not so distant future. So, here we are!

But why did it take so long? We love deadlines, in particular the whooshing sound they make as they fly by. Therefore we successfully missed every deadline we had set for ourselves. Clearly, one reason is that writing this book pleased us more than pasta and wine. Another reason is that laying the foundations for Computational Commutative Algebra in the third millennium turned out to be more of a job than we had bargained for. Many sections of this book are like small research papers because we tried to present the material in the style that pleases us so much and differs markedly from existing literature.

The result is a volume having almost twice the size of the first: some of its 23 sections are as big as a whole chapter, some of its 55 tutorials are as big as a whole section, and some exercises are as big as a tutorial. Together the two books form a compilation of about 900 pages which includes a vast collection of 99 tutorials to keep you busy for a long, long time. To sustain your interest, we have tried to continue the presentation in the lively style of the first volume. Alas, we have to inform you that this is absolutely and definitively the second and last volume of the trilogy.

0.2 Now, What Is This Book *Really* About?

As I said before,
I never repeat myself.
(Anonymous)

Let us examine some concrete problems whose solutions we shall try to explain in this book. For a similar description of the contents of Volume 1 we refer the reader to its introduction. Let us start with the problem of using Gröbner bases in the homogeneous case. Suppose we are given a polynomial ring $P = K[x_1, \ldots, x_n]$ over some field K.

Question 1 *How can we equip P with gradings which are useful for Computational Commutative Algebra?*

More precisely, we are asking whether it is possible to find a monoid Γ and a Γ-grading on P such that homogeneous ideals and graded modules have additional invariants and are simpler to handle computationally. The answer will turn out to be "positive $\mathbb{Z}^m$-gradings", whatever they are.

Question 2 *How can we relate an arbitrary ideal or module to a homogeneous ideal or a graded module?*

In other words, how can we pass from the inhomogeneous to the homogeneous case? At least three possibilities will be discussed: degree form ideals and Macaulay bases, homogenization, and the homogeneous part of an ideal.

Question 3 *How can we exploit homogeneity to compute Gröbner bases and perform elementary operations on ideals and modules more efficiently?*

Related questions are: Are there special term orderings which can be used to advantage in the graded setting? Are Gröbner bases of homogeneous ideals again homogeneous? If we stop the computation of a homogeneous Gröbner basis after some degree is finished, is the resulting *truncated Gröbner basis* any good?

The fact that the gradings we use are positive implies that all irredundant homogeneous systems of generators of a finitely generated graded module are minimal. Hence the minimal number of generators of such a module is a well-behaved invariant. This leads us to examine the following problems.

Question 4 *How can we compute minimal homogeneous systems of generators, minimal homogeneous presentations, and minimal graded free resolutions of finitely generated graded modules?*

Another aspect of positive gradings is that they force the homogeneous components of a finitely generated graded P-module M to be finite dimensional K-vector spaces. This allows us to define the *Hilbert function* $\mathrm{HF}_M : \mathbb{Z}^m \longrightarrow \mathbb{Z}$ of M by $\mathrm{HF}_M(i) = \dim_K(M_i)$ and to study its generating power series, the *Hilbert series* of M.

Question 5 *How can we compute the Hilbert function and the Hilbert series of a finitely generated graded module? What are their basic properties? How fast do Hilbert functions grow?*

In the standard graded case, i.e. when $\deg(x_1) = \cdots = \deg(x_n) = 1$, one of these basic properties of Hilbert functions is that $\mathrm{HF}_M(i)$ is given by the value of the *Hilbert polynomial* of M for large enough i.

Question 6 *How can we compute the Hilbert polynomial of a graded module M? Can we derive other invariants of M from it?*

It turns out that one of these invariants is the dimension of a graded ring or a graded module. Thus we ask ourselves:

Question 7 *What are the algebraic and geometric interpretations of the dimension of a graded ring?*

These are our questions. And if they are not enough for you ... well, we have others. For instance, we shall address the following existential question:

Question 8 *Can mathematicians be replaced by computers?*

In other words, can computers take over the job of proving theorems? Is there true artificial intelligence?

Question 9 *What is there beyond Gröbner bases?*

Which other kinds of problems can be addressed using Computational Commutative Algebra? Are there situations in which the theory of Gröbner bases can be imitated or generalized?

Let us end this discussion by pointing out one unimportant choice we have made. We have decided to change the title of Chapter 6 slightly and call it simply *"Further Applications"* rather than mentioning Gröbner bases explicitly. The justification is that the chapter has in fact a much wider scope. Although Gröbner bases are always sneaking in one way or another, we *cover all the bases:* binomial bases of toric ideals, Hilbert bases of monoids, liftings and distractions of monomial bases, SuperG bases, bases of vanishing ideals of finite sets of points, border bases of zero-dimensional ideals, standard bases of filtered modules, SAGBI bases of subalgebras, and a basis for automatic theorem proving. You name it, we've got it! *(Well, almost.)*

Last, but not least, let us henceforth limit the use of "let us", lest we run the risk of repeating ourselves.

Repetita iuvant.
(Ancient Latin Adage)

0.3 What Is This Book *Not* About?

All is the same
A year has gone by
Some day you came
Some day you'll die.
(Cesare Pavese)

Had we written this sentence in Volume 1, this very moment would have occurred about four years ago. In those days we mentioned that the list of topics which we did *not* talk about contained soccer, chess, gardening, and our other favourite pastimes. Since life is too short and precious to miss out on the good stuff, we decided to remedy these shortcomings. The current volume includes two tutorials related to chess, and in the introductions of the last two chapters we meet a gardener and a chess player engaged in an animated *trilogue* with an amateur mathematician. Unfortunately, they are so immersed in the discussion that the gardener forgets to advise us about the right time to sow tomato seeds and the correct composition of the soil for growing azaleas.

What else is *not* in this book? There is still nothing about computability or complexity. We use the expression *effectively computable* loosely to mean that there is some algorithm to perform the computation. And when we write that some algorithm is *efficient*, we are usually indicating a personal opinion. In fact, analyzing the worst-case or average-case complexity of algorithms is not only beyond the scope of this book, but in our experience it would tell little about their *practical complexity*, i.e. their running time for those examples we happen to be interested in.

Even the terms *algorithm* and *procedure* are applied in a purely intuitive and informal manner. In fact, the way we present algorithms in this book differs from computer science texts. For us, an algorithm is really a more general form of theorem where the instructions do not necessarily follow linearly one after another, but conditionals and recursive constructions are allowed. Consequently, it is usually not sufficient to prove correctness alone (as for a theorem) but also finiteness. Later in this book we shall encounter *enumerating procedures*. Roughly speaking, we think of them as algorithms with only partial finiteness proofs. You will not find Turing machines or recursive sets mentioned anywhere because for all algorithms and procedures we explain there exist practical implementations (for instance in CoCoA), so that a theoretical consideration of their workability is superfluous.

Finally, in Volume 1 we wrote that we did not cite anything anywhere. This is still true. However, if you have devoured this book and crave for more, you can find some suggestions for further reading in Appendix D.

0.4 Are There any Applications of This Theory?

There is no branch of mathematics, however abstract,
which may not some day be applied
to phenomena of the real world.
(Nikolai Lobachevsky)

Allow us to be bold and brazen: Computational Commutative Algebra is going to be one of the pillars of the applications of mathematics to the real world in the third millennium. With the advance of computing technology it has become feasible to grapple with industrial sized problems using symbolic computations. One of the main purposes of this volume is to continue laying the theoretical foundations for this development. Scattered throughout it you can discover clues and suggestions relating the topics we discuss to actual applications.

One aspect of this trend is nevertheless conspicuously absent here: symbolic methods should really be viewed as complementary to the numerical methods which have predominated up to now. Although a few computer algebra systems, including CoCoA, offer you some possibilities of performing *hybrid* computations, i.e. computations mixing symbolic and numerical methods, the area of numerical polynomial algebra is still in its infancy. Therefore we leave to future treatises the questions of how to represent measured data using numerical polynomials and of how to compute Gröbner bases, border bases, SAGBI bases etc. with numerical polynomials. Let us just say that actual industrial applications of Computational Commutative Algebra exist, are being continually developed, and will become more important in the coming years.

0.5 How Was This Book Written?

Those are my principles,
and if you don't like them ...
well, I have others.
(Groucho Marx)

A short answer to this question is that this book was written using LaTeX and the Springer macro package. Another quick reply is that this book is written in the same style as Volume 1. Colloquially speaking, it contains more of the same, much more. Furthermore, we tried to adhere to the rules formulated in Section 0.7 of the first volume. Browsing this second volume, you will also notice that we spruced it up with a rather generous sprinkling of quotes and occasional literary efforts. Although this may be rare in a mathematical book, we believe that a good mathematical joke is better than a dozen mediocre papers. Moreover, some things are so serious that you can

only joke about them. And if you don't like our quotes ..., well, we have others.

One of the problems we faced when we wrote Volume 1 is still as unsolved as ever, namely the problem of differing notations. The following case in point arose when we drafted Section 6.4. In accordance with books in commutative algebra, we called a non-empty set of terms an *order ideal* if it is closed under forming divisors. When we were criticized for this choice of name, we did some research and found out that the same concept had been "discovered" in several branches of mathematics. Of course, everybody had "introduced" a different name, and few authors seemed to be aware of the alternative terminologies. The following table summarizes our findings.

	order ideal	Computational Commutative Algebra
1)	canonical term basis	computer algebra
2)	Δ-set	coding theory
3)	Ferrer diagram	differential algebra
4)	footprint	coding theory
5)	normal set	numerical mathematics
6)	poset ideal	combinatorics
7)	set of terms connected to 1	computer algebra
8)	staircase	algebraic geometry
9)	standard set	commutative algebra
10)	term filter	set theory

After the publication of the first volume, some questions arose concerning the prerequisites for reading these books. Not surprisingly, for Volume 2 we assume that you have mastered the essential parts of Volume 1. But what do you need to know to be able to read Volume 1? In principle, a good working knowledge of basic algebraic structures and techniques should suffice: groups, rings, modules and fields, as well as homomorphisms, residue classes, exact sequences and a few basic proof methods. Although we tried to keep everything as self-contained as possible, it surely won't hurt if you peek into a standard algebra textbook (e.g. [La70]) in case of need. At times we also assume that you apply your common sense and produce a reasonable guess at what we mean, rather than expecting a formal definition of every single word. Isn't it clear what a *subtuple* should be?

Finally, let us point out one "rule" which has not yet been mentioned. Normally, every section or subsection in this book has some global hypotheses. Unless we specifically mention something else, they apply to everything in that section or subsection. We tried not to change these global hypotheses frequently during the course of the presentation. For propositions and theorems we deem important, we repeat the global hypotheses to aid the reader in looking up references. Of course we were not able to impose this rule unwaveringly. There are no exceptions to the rule that every theorem likes to be an exception to the rule.

0.6 What Is a Tutorial?

The hardest thing to understand is the income tax.
(Albert Einstein)

The second hardest thing to understand could be some of the tutorials in this book. Fortunately, there exists another rule: it is not necessary to do and understand the tutorials in order to continue reading the main text. Besides containing links to a wide variety of applications, tutorials provide fodder for student projects, lab classes, term papers, and so on. But teachers beware! The complexity of solving a tutorial may vary dramatically from one to the next. Some tutorials require a lot of programming, while others expect the reader to find rather tricky proofs. For some tutorials you can find the solution in research papers or other literature; maybe there even exists a pointer in Appendix D.

So, what are the tutorials good for? As we wrote in Volume 1, they are mainly intended to help bridge the gap between the theory and actual computations. What is computer algebra without a computer? Just another dry part of algebra. Gröbner bases, gradings, Hilbert functions, all these notions only come to life when you actually compute them. The tutorials should entice you into experimenting, playing with CoCoA, computing special cases, and thinking about what is going on inside the machine. If you use this book for teaching, we believe it is important that you try your hand at the tutorials before you assign them. Do not skip the computational parts of this book. Do not teach according to the motto:

He who can, does. He who cannot, teaches.

0.7 What Is CoCoA?

With computers you can
waste time a lot faster.
(Darryl Mc Cullough)

If you want to heed our advice and do some actual computations, you need access to a computer and a computer algebra system. As for the computer, we are not offering advice. But as for the computer algebra system, we suggest that you visit the web page

`http://cocoa.dima.unige.it/`

and download the free computer algebra system CoCoA. In fact, we hope that you have already done so.

Naturally there are many other computer algebra systems that you can use to implement the algorithms in this book or to solve the programming parts of the tutorials. If you are expert enough, using several computer algebra

systems in parallel certainly has advantages. However, if you are struggling to come to grips with just one computer algebra system, then CoCoA is a very good choice.

To help you master CoCoA usage and programming, we have given some basic information in Volume 1. In this volume we have added appendices describing its graphical interface and further programming techniques. If this is still not enough for you, have a look at the on-line CoCoA tutorial and the above web site.

Before plunging into action, however, you should carefully plan your time table. Although the speed of time is one-second per second, when you sit in front of your computer time passes a lot faster. And when you are playing with CoCoA, you `Can't Stop!`

0.8 And What Is This Book Good for?

You can fool all the people some of the time,
and some of the people all the time,
but you cannot fool all the people all of the time.
(Abraham Lincoln)

This book is good for learning, teaching, reading, and most of all, enjoying the topic at hand. The theories it describes can be applied to anything from children's toys to oil production. Even browsing it superficially will show you that it is different from other books on mathematics, except for Volume 1 of course. We fool around much more! It is so different that it didn't fit into any of the regular book series of Springer Verlag and had the chance to get its own colourful cover.

In earnest, this book is primarily intended as a textbook for advanced courses in Computational Commutative Algebra. We don't think that we can fool you into believing that the material we cover is easy. But we hope the presentation is comprehensible and pleasant enough to tempt you to read on. Books and research papers in computer algebra differ even from other works in mathematics. Since computers are very difficult to fool, the standard of correctness of a computer algebra text has to be raised until the implementation of the theorems and algorithms works. This is a high mark. We hope we have achieved it.

The advice to go through this book with an open and critical mind applies to Volume 2 as much as it did to Volume 1. Suppose you are playing with CoCoA and you discover the following series of calculations:

$$\begin{array}{lll} 7 \times 15 = 105 & \text{and} & 10 + 5 = 15 \\ 7 \times 18 = 126 & \text{and} & 12 + 6 = 18 \\ 7 \times 21 = 147 & \text{and} & 14 + 7 = 21 \\ 7 \times 24 = 168 & \text{and} & 16 + 8 = 24 \\ 7 \times 27 = 189 & \text{and} & 18 + 9 = 27 \end{array}$$

Have you unearthed a wonderful new method of checking multiplication tables? Not until you provide an actual formulation and a proof of the theorem you claim to have found. This is what this book is really good at: it contains formulations and (hopefully) correct proofs of many results which are "folklore" or otherwise hard to nail down.

You cannot fool all the people all of the time. At some point somebody has to sit down and implement an algorithm for computing graded free resolutions, or a procedure for computing SAGBI bases. And no amount of friendly but imprecise advice is going to deceive that person into believing this is easy: his computer would quickly disabuse him of any such misconception. In this sense, we hope you will find the combination of Volumes 1 and 2 not only valuable for learning or teaching, but also as an ultra-explicit compendium of the state of the art in Computational Commutative Algebra.

0.9 Some Final Words of Wisdom

Drillers shape holes,
bow makers shape arrows,
carpenters shape wood,
and the wise man shapes himself.
(Siddhartha Gotama)

After having typed about 900 pages of densely written mathematics, we still cannot answer profound philosophical questions such as: What is the deeper meaning of Computational Commutative Algebra? How is it going to develop in the future? Instead of philosophizing endlessly, let us end this introduction and send you off to Chapter 4 with a few words of wisdom by Peter Taylor.

> *My premise is that we mathematicians are sitting on a gold mine. In terms of structural beauty, stunning insights, unexpected power, all from simple, accessible ingredients, very little can compare with our wonderful subject. But we do a terrible job at communicating that to most of our students. In the classroom we blow it, and we thereby alienate just about the entire population. And we've no one to blame but ourselves.*

Thus the mathematician shapes everybody. May this book shape you into a fan of Computational Commutative Algebra. May it be a gold mine of material for studying and teaching. May it help you appreciate the beauty and the usefulness of our wonderful subject.

This is not the end
or the beginning of the end,
but it is the end of the beginning.
(Sir Winston Churchill)

4. The Homogeneous Case

Das Spiel dauert 90 Minuten.
[The game lasts 90 minutes.]
(Sepp Herberger)

Well, not quite: sometimes a soccer game lasts 93 minutes and 36 seconds. Also the writing of this chapter took some unexpected turns. Initially, our intention was to compose a small collection of the necessary background material for our true goal, namely to write a linchpin chapter about Hilbert functions. Hilbert functions arise in graded situations, and thus we were naturally led to ask the following basic questions.

1) Which gradings on the polynomial ring are useful for Computational Commutative Algebra?

2) How are the graded and the non-graded settings related to each other? Can one pass from one to the other?

3) What, if any, are the computational advantages of being in a graded setting?

4) How can one compute some typical invariants of homogeneous ideals and graded modules, such as the minimal number of generators and the graded Betti numbers?

As we struggled to answer these questions, the chapter grew and grew. Time and again we discovered that the intricacies of some topic put up more resistance than we had expected, and now that everything is finished, Chapter 4 has more than 150 pages. So, what is all the fuss about?

Instead of delving into a detailed, proposition by proposition account of the chapter, let us walk though a typical example originating in algebraic geometry. As we explain in Tutorial 27, the Zariski closure of the set $\{(t, t^3, t^4) \in \mathbb{A}^3_{\mathbb{Q}} \mid t \in \mathbb{Q}\}$ is an affine variety. In Tutorial 39.h we saw that the vanishing ideal of this curve is $I = (x_1 - t,\, x_2 - t^3,\, x_3 - t^4) \cap \mathbb{Q}[x_1, x_2, x_3]$, and using Theorem 3.4.5 we find that $I = (x_1x_2 - x_3,\, x_1^3 - x_2)$. Moreover, a glance at $\mathrm{LT}_{\texttt{DegRevLex}}(I) = (x_1x_2,\, x_1^3,\, x_1^2x_3,\, x_2^3)$ convinces us that I is not principal, i.e. that the given system of generators is minimal.

However, this is not the end of the story. Usually, algebraic geometers are even more interested in the projective closure of this curve, i.e. the curve $C = \{(u^4 : tu^3 : t^3u : t^4) \in \mathbb{P}^3_{\mathbb{Q}} \mid (t : u) \in \mathbb{P}^1_{\mathbb{Q}}\}$. The homogeneous vanishing ideal of C is the homogenization $I^{\mathrm{hom}} = (f^{\mathrm{hom}} \mid f \in I)$ of I in

$P = \mathbb{Q}[x_0, \ldots, x_3]$ where $f^{\text{hom}} = x_0^{\deg(f)} f(\frac{x_1}{x_0}, \ldots, \frac{x_3}{x_0})$ denotes the homogenization of a polynomial $f \in \mathbb{Q}[x_1, x_2, x_3]$. How can we compute I^{hom}? As we shall see, it is not sufficient to homogenize the generators of I. Instead, Section 4.3 contains three methods for computing I^{hom}. Firstly, Corollary 4.3.8 shows $I^{\text{hom}} = (x_0x_3 - x_1x_2,\ x_0^2x_2 - x_1^3) :_P (x_0)^\infty$. Secondly, Proposition 4.3.21 yields $I^{\text{hom}} = (x_1x_2 - x_0x_3,\ x_1^3 - x_0^2x_2,\ x_1^2x_3 - x_0x_2^2,\ x_2^3 - x_1x_2^2)$, since $G = \{x_1x_2 - x_3,\ x_1^3 - x_2,\ x_1^2x_3 - x_2^2,\ x_2^3 - x_1x_3^2\}$ is a `DegRevLex`-Gröbner basis of I. The third method is based on Tutorial 51 and requires us to compute the elimination ideal $(x_0 - y_0^4,\ x_1 - y_0^3y_1,\ x_2 - y_0y_1^3,\ x_3 - y_1^4) \cap P$.

After determining the homogeneous vanishing ideal I^{hom} of C in the ring P, we would like to calculate some invariants associated to it. For instance, what is the minimal number of generators of I^{hom}? By the Graded Version of Nakayama's Lemma 1.7.15, the irredundant system of generators consisting of the four polynomials given above is minimal. In fact, using the variant of Buchberger's algorithm we present in Theorem 4.6.3, we can discover this property while performing a suitable Gröbner basis computation. Another way of expressing the insight we have just gained is to say that there is a homogeneous surjective P-linear map $\varphi : F \longrightarrow I^{\text{hom}}$, where $F = P(-2) \oplus P(-3)^3$ and $\text{Ker}(\varphi)$ is contained in $(x_0, \ldots, x_3)\,F$.

A finer set of invariants can be attached to I^{hom} if we notice that it is actually a bigraded ideal. This means that if we use a $\mathbb{Z}^2$-grading on P for which $\deg(x_0) = \binom{1}{0}$, $\deg(x_1) = \binom{1}{1}$, $\deg(x_2) = \binom{1}{3}$, and $\deg(x_3) = \binom{1}{4}$, then I^{hom} is a homogeneous ideal with respect to this grading. Hence we can use the results in Sections 4.7 and 4.8 to compute the minimal bigraded free resolution

$$0 \longrightarrow P\left(-\binom{5}{10}\right) \xrightarrow{\lambda} P\left(-\binom{4}{6}\right) \oplus P\left(-\binom{4}{7}\right) \oplus P\left(-\binom{4}{9}\right) \oplus P\left(-\binom{4}{10}\right) \xrightarrow{\psi}$$
$$\xrightarrow{\psi} P\left(-\binom{2}{4}\right) \oplus P\left(-\binom{3}{3}\right) \oplus P\left(-\binom{3}{6}\right) \oplus P\left(-\binom{3}{9}\right) \xrightarrow{\varphi} I^{\text{hom}} \longrightarrow 0$$

of I^{hom}. The multiplicities of the shifts appearing in this resolution are called the graded Betti numbers of I^{hom}. They encode subtle properties of the geometry of C.

In the light of this example, let us come back to the basic questions we asked above and discuss them. Let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K.

1) The gradings on P have to be over an explicitly given, easily computable monoid. For our purposes, the monoid $\Gamma = \mathbb{Z}^m$ is well-suited. Moreover, each indeterminate should be homogeneous, and non-zero constants should be homogeneous of degree zero. Fixing the degree of each indeterminate gives a uniquely defined grading on P with these properties. Let $W \in \text{Mat}_{m,n}(\mathbb{Z})$ be the matrix whose columns are the degrees of the indeterminates. We shall say that the grading on P is given by W. Such gradings are studied in Sections 4.1 and 4.2.A. Later we introduce and study gradings of positive type and positive gradings, because they offer additional nice

properties such as finite dimensional homogeneous components of finitely generated graded modules, the applicability of the graded version of Nakayama's lemma, a natural and easily computable well-ordering on the set of degrees of non-zero homogeneous polynomials, or the existence of a degree compatible term ordering.

2) There are several ways of passing from a non-homogeneous polynomial f (or ideal I) to a homogeneous one. The first method is to consider only those terms in the polynomial having maximal degree. They yield the degree form of f. In analogy with the theory developed in Chapter 2, we can now define the degree form ideal of I and study Macaulay bases, i.e. sets of polynomials whose degree forms generate the degree form ideal of I. This is done in Section 4.2.B. Another approach is followed in Section 4.3, where we introduce new indeterminates and use them to homogenize a polynomial by multiplying terms of non-maximal degree with suitable power products of the homogenizing indeterminates. The ideal generated by the homogenizations of the polynomials in I is then called the homogenization of I and denoted by I^{hom}. After a detailed discussion of the algebraic and computational aspects of the passage from I to I^{hom} (and back), we also explain its relationship to Macaulay bases, Gröbner bases, and flat families. Finally, in Tutorial 50, we show how to compute the homogeneous ideal obtained from a non-homogeneous one by simply taking the ideal generated by the homogeneous elements contained in it.

3) In Chapters 2 and 3 we have already encountered situations where the difficulty of computing a particular Gröbner basis depended strongly on the chosen term ordering. In many cases, the degree reverse lexicographic term ordering turned out to be a good choice. So, what is so special about it? This is the topic of Section 4.4, where we use term orderings which are similar to `DegRevLex` for computing saturations, colon modules, addition of an indeterminate, and reduction modulo an indeterminate in an efficient way if the ideals and modules in question are suitably graded. Further advantages of using gradings surface in Section 4.5, where we examine the computation of Gröbner bases in a graded setting. The homogeneous version of Buchberger's algorithm permits substantial optimizations. This is because we can use the fact that it proceeds degree by degree and also that the S-vectors it has to process are homogeneous. Moreover, if we stop the computation after a fixed degree is finished, we have computed a truncated Gröbner basis and, as we shall see in Section 4.5.B, this may be all we need for a particular problem.

4) The first and most obvious invariant of a homogeneous ideal or graded module is its minimal number of generators. Due to the Graded Version of Nakayama's Lemma 1.7.15, every irredundant homogeneous system of generators is minimal, and all of them have the same number of elements. In Section 4.6, we prove that a slight variation of the Homogeneous Buchberger Algorithm 4.5.5 yields a minimal homogeneous system of generators $\mathcal{V}_{\min}$ contained in the original system of generators. The next step is to compute

a minimal homogeneous system of generators of $\mathrm{Syz}_P(\mathcal{V}_{\min})$, i.e. a minimal homogeneous presentation of the ideal or module we started with. This step is taken in Section 4.7, where we not only introduce several strategies for computing such minimal homogeneous presentations, but also prove that the ranks and shifts of the graded free modules involved in such a presentation are invariants of M, i.e. they do not depend on the chosen presentation. Continuing this process of computing minimal homogeneous systems of generators of syzygy modules, we obtain a minimal graded free resolution

$$\cdots \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

of a finitely generated graded P-module M, where $F_0, F_1, \ldots$ are finitely generated graded free P-modules. After proving in Section 4.8.A that a finite minimal graded free resolution of M exists and is essentially unique (up to isomorphisms of graded free modules), we present three methods for computing it in Section 4.8.B.

After all is said and done, it seems that the advantages of working in a graded setting more than compensate for the additional conceptual and notational toil and trouble it requires. Do you think that this is an obvious conclusion, something French people would call a "lapalissade"? At times *lapalissades* contain profound truths.

Monsieur de La Palisse est mort
il est mort devant Pavie
un quart d'heure avant sa mort
il était encore en vie.
(Bernard de la Monnoye)

4.1 Polynomial Rings Graded by Matrices

Begin at the beginning
and go on till you come to the end;
then stop.
(Lewis Carroll)

Before beginning our journey into the realm of gradings on polynomial rings, let us have a look at where we are. In Volume 1 we devoted all of Section 1.7 to the hidden secrets of general gradings. This generality was motivated by the goal of providing correct proofs in the theory of Gröbner bases of modules. Now, where do we want to go from there? For actual computations, gradings on polynomial rings given by arbitrary commutative monoids are too general. Therefore we need to restrict our attention to a more limited class of gradings. How can we manufacture a suitable notion?

To get some inspiration, let us have another look back at the path we took in Volume 1. In Example 1.7.2 we introduced the most common grading on the polynomial ring, namely the standard grading, and in Section 1.4 we saw that the most useful term orderings on a polynomial ring are those defined by matrices. What is the connection here? In both cases there is a matrix of integers which plays a key role. Comparison of terms is based on taking scalar products of the rows of this matrix with logarithms of terms. For instance, the standard degree of a term $t \in \mathbb{T}^n$ is given by the product $\deg(t) = W \cdot \log(t)^{\mathrm{tr}}$, where W is the matrix $W = (1\ 1 \cdots 1)$.

Thus we are led in a natural way to *connect the dots*. On the polynomial ring $P = K[x_1, \ldots, x_n]$ we define a $\mathbb{Z}^m$-grading by means of a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. The degrees of the indeterminates are the columns of W, and constant polynomials are homogeneous of degree $(0, \ldots, 0)^{\mathrm{tr}}$. So, what are the applications of such gradings? A first answer comes from Proposition 4.1.8 which yields a characterization of monomial ideals as the *most homogeneous* ones, since they are the only ideals which are homogeneous with respect to every grading. But in order to be able to answer the question more satisfactorily, we need to examine the basic properties of gradings by matrices and to generalize this notion to include graded modules.

Do we really have to take the long and twisty road of modules again? Absolutely yes! As we frequently saw in Volume 1, and as is becoming increasingly clear, Computational Commutative Algebra is really about computations in and with modules. This aspect is taken care of in Subsection B, where we show that the most important operations on graded modules respect the grading. For actual computations, arbitrary gradings by matrices are too general. Therefore in the last subsection we restrict our attention further and turn to the subject of *gradings of positive type*. These are the gradings defined by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ such that some linear combination of its rows with integer coefficients has all entries positive (see Definition 4.1.17).

Why are they called of positive type, and why are they important? Concerning these questions, we offer you two pieces of good news and one

piece of bad news. The good news is that, under a grading of positive type, the vector space of all elements of any given degree has finite dimension over K (see Proposition 4.1.19). Moreover, the Graded Version of Nakayama's Lemma 1.7.15 holds for such gradings, so that irredundant systems of generators are minimal (see Proposition 4.1.22). Hence gradings of positive type enjoy two of the most useful properties we can hope for. So, what is the bad news? Do you really want the bad news right now? Let's postpone it to a subsequent section and be happy for a while!

4.1.A Gradings by Matrices

Having introduced the general notions of graded rings and modules in Section 1.7, we are now going to concentrate on certain special kinds of graded object. We are interested in gradings on polynomial rings which have two properties: the indeterminates are homogeneous, and the constants are homogeneous of degree zero.

In what follows, we let K be a field, $n \geq 1$, and $P = K[x_1, \ldots, x_n]$ a polynomial ring over K. Furthermore, we let $(\Gamma, +)$ be a monoid whose identity element is denoted by 0. As in Volume 1, we assume that Γ is a commutative monoid.

Recall that in Section 1.7 we defined a Γ-grading on P to be a decomposition $P = \bigoplus_{\gamma\in\Gamma} P_\gamma$ into additive subgroups such that $P_\gamma \cdot P_{\gamma'} \subseteq P_{\gamma+\gamma'}$ for all $\gamma, \gamma' \in \Gamma$. A P-module M will be called a **graded P-module** if it is a Γ-graded P-module in the sense of Definition 1.7.4, i.e. if we have a decomposition $M = \bigoplus_{\gamma\in\Gamma} M_\gamma$ into additive subgroups such that $P_\gamma \cdot M_{\gamma'} \subseteq M_{\gamma+\gamma'}$ for all $\gamma, \gamma' \in \Gamma$. In other words, a graded P-module is understood to be graded over the same monoid. By Proposition 1.7.10, a finitely generated module is graded if and only if it has a finite system of generators consisting of homogeneous elements. In this case, as in Volume 1, we shall say that M has a finite homogeneous system (or set) of generators.

Proposition 4.1.1. *Let Γ be a monoid, and let $\gamma_1, \ldots, \gamma_n \in \Gamma$.*

a) There exists exactly one Γ-grading on P such that the non-zero constant polynomials are homogeneous of degree 0 and, for $i = 1, \ldots, n$, the indeterminate x_i is homogeneous of degree γ_i.

b) Under this grading, the set $\{\gamma \in \Gamma \mid P_\gamma \neq 0\}$ is the submonoid of Γ generated by $\{\gamma_1, \ldots, \gamma_n\}$.

Proof. To prove a), let us show existence first. For $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$ and $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, we let t be homogeneous of degree $\deg(t) = \alpha_1\gamma_1 + \cdots + \alpha_n\gamma_n$. More generally, given $\gamma \in \Gamma$, we say that a polynomial $f \in P$ is homogeneous of degree γ if all terms in its support are homogeneous of degree γ. This means that $P_\gamma = \bigoplus_{\alpha_1\gamma_1+\cdots+\alpha_n\gamma_n=\gamma} K\, x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for all $\gamma \in \Gamma$. Then we have

$$P = \bigoplus_{(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}^n} K\, x_1^{\alpha_1}\cdots x_n^{\alpha_n} = \bigoplus_{\gamma\in\Gamma}\left(\bigoplus_{\alpha_1\gamma_1+\cdots+\alpha_n\gamma_n=\gamma} K\, x_1^{\alpha_1}\cdots x_n^{\alpha_n}\right) = \bigoplus_{\gamma\in\Gamma} P_\gamma$$

and it is clear that $P_\gamma \cdot P_{\gamma'} \subseteq P_{\gamma+\gamma'}$ for all $\gamma, \gamma' \in \Gamma$. Thus we have defined a Γ-grading on P which has the desired properties.

Now we show uniqueness. Given any Γ-grading on P with the stated properties, the conditions $\deg(x_1) = \gamma_1, \ldots, \deg(x_n) = \gamma_n$ imply that $\deg(x_1^{\alpha_1}\cdots x_n^{\alpha_n}) = \alpha_1\gamma_1 + \cdots + \alpha_n\gamma_n$ for $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$. So, in fact, the above definition is forced upon us by the rules satisfied by a Γ-grading, i.e. we have proved uniqueness.

The proof of b) follows from the observation that, for any $\gamma \in \Gamma$, the vector space P_γ is generated by the terms of degree γ. The degrees of those terms are contained in the submonoid of Γ generated by the set $\{\gamma_1, \ldots, \gamma_n\}$. Conversely, every degree in this submonoid is the degree of a term because P is an integral domain. □

Even in the case $\Gamma = \mathbb{Z}$, the gradings on P provided by this proposition are still very general, as the following example shows.

Example 4.1.2. Let the polynomial ring $P = K[x_1, x_2]$ be equipped with the $\mathbb{Z}$-grading defined by $K \subseteq P_0$, $x_1 \in P_{-1}$, and $x_2 \in P_1$. Then we have $x_1x_2 \in P_0$, and hence $K \subset P_0$. In fact, it is easy to see that $\dim_K(P_0) = \infty$.

Our main interest will be in gradings for which all homogeneous components are finite dimensional K-vector spaces. The following definition generalizes Example 1.7.2 and is a case in point.

Definition 4.1.3. A K-algebra R is called a **standard graded K-algebra** if it is $\mathbb{N}$-graded, satisfies $R_0 = K$ and $\dim_K(R_1) < \infty$, and if R is generated by the elements of R_1 as a K-algebra.

Standard graded algebras are characterized by the existence of special presentations as follows.

Remark 4.1.4. Using Corollary 1.1.14 and Remark 1.7.9, we see that a standard graded K-algebra R is an algebra of the form $R \cong P/I$, where $P = K[x_1, \ldots, x_n]$ is $\mathbb{N}$-graded such that $K = P_0$, each x_i is homogeneous of degree one, and I is a homogeneous ideal in P. Conversely, every algebra of this form P/I is a standard graded K-algebra.

In this and the following chapters, standard graded K-algebras will play an important role. But not every $\mathbb{N}$-graded, finitely generated K-algebra is standard graded.

Example 4.1.5. Let $P = K[x_1, x_2]$ be equipped with the standard grading. Then the K-subalgebra $S = K[x_1^2, x_1x_2, x_2^2]$ of P is a finitely generated $\mathbb{N}$-graded algebra, but it is not standard graded, since $S_1 = \{0\}$.

To bring all the graded algebras which we want to examine in this chapter under one umbrella requires a concept of gradings whose level of generality is somewhere between the very wide class of gradings considered in Proposition 4.1.1 and the rather limited class of standard graded K-algebras. For our purposes, the following concept will prove most useful.

Definition 4.1.6. Let $m \geq 1$, and let the polynomial ring $P = K[x_1, \ldots, x_n]$ be equipped with a $\mathbb{Z}^m$-grading such that $K \subseteq P_0$ and $x_1, \ldots, x_n$ are homogeneous elements.

a) For $j = 1, \ldots, n$, let $(w_{1j}, \ldots, w_{mj}) \in \mathbb{Z}^m$ be the degree of x_j. The matrix $W = (w_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ is called the **degree matrix** of the grading. In other words, the columns of the degree matrix are the degrees of the indeterminates. The rows of the degree matrix are called the **weight vectors** of the indeterminates $x_1, \ldots, x_n$.
b) Conversely, given a matrix $W = (w_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, we can consider the $\mathbb{Z}^m$-grading on P for which $K \subseteq P_0$ and the indeterminates are homogeneous elements whose degrees are given by the columns of W. In this case, we say that P is **graded by** W.
c) Let $d \in \mathbb{Z}^m$. The set of homogeneous polynomials of degree d is denoted by $P_{W,d}$, or simply by P_d if it is clear which grading we are considering. A polynomial $f \in P_{W,d}$ is also called **homogeneous of degree** d, and we write $\deg_W(f) = d$.

To aid the reader in understanding our notation, we point out that a degree is a vector in $\mathbb{Z}^m$. If we use it in matrix equations, its representation is a column. Sometimes we also denote it by a row if no confusion arises. If a grading on P is defined by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, the degree of a term $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is given by $\deg_W(t) = W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}}$. So, we have $\{d \in \mathbb{Z}^m \mid P_{W,d} \neq 0\} = \{W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}} \mid (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n\}$.

Example 4.1.7. Let $P = K[x_1, x_2, x_3, x_4]$ be graded by the matrix

$$W = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

and let $f = x_1x_4 - x_2x_3$. Then f is homogeneous of degree $(2, 1, 1)$, because $W \cdot \log(x_1x_4)^{\mathrm{tr}} = W \cdot \log(x_2x_3)^{\mathrm{tr}} = (2, 1, 1)^{\mathrm{tr}}$. The principal ideal generated by f is a homogeneous ideal by Proposition 1.7.10.

A first non-trivial example of a graded object is given by the following characterization of monomial ideals as the "most homogeneous" ideals. Recall that a square matrix is called non-singular if its determinant is non-zero.

Proposition 4.1.8. *Let I be an ideal of P. Then the following conditions are equivalent.*

a) The ideal I is monomial.
b) There is a non-singular matrix $W \in \mathrm{Mat}_n(\mathbb{Z})$ such that I is homogeneous with respect to the grading on P given by W.
c) For every $m \geq 1$ and every matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, the ideal I is homogeneous with respect to the grading on P given by W.

Proof. Since I is generated by terms, and terms are homogeneous with respect to the gradings we are considering, Proposition 1.7.10 shows that a) implies c). Obviously, b) is a special case of c). Therefore it suffices to show that b) implies a).

We take a homogeneous polynomial $f \in I_{W,d}$ and show that there is only one term in its support. Let $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $t' = x_1^{\beta_1} \cdots x_n^{\beta_n}$ be terms in the support of f. Then $d = \deg_W(t) = \deg_W(t')$ implies $W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}} = W \cdot (\beta_1, \ldots, \beta_n)^{\mathrm{tr}}$. Since we have $\det(W) \neq 0$, the $\mathbb{Z}$-linear map defined by W is injective. Therefore we obtain $(\alpha_1, \ldots, \alpha_n) = (\beta_1, \ldots, \beta_n)$, and hence $t = t'$. □

In general, this proposition does not hold for monomial submodules of graded free P-modules (see Exercises 5 and 6). If two matrices in $\mathrm{Mat}_{m,n}(\mathbb{Z})$ can be transformed into each other by elementary row operations, the relation between the corresponding gradings on P is fairly simple to understand.

Proposition 4.1.9. *Let $m \geq 1$, let $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let $V \in \mathrm{Mat}_{\ell,m}(\mathbb{Z})$ for some $\ell \geq 1$.*

a) The gradings on P given by W and $V \cdot W$ are related by $P_{W,d} \subseteq P_{V \cdot W, V \cdot d}$ for all $d \in \mathbb{Z}^m$. In particular, the map $(\mathrm{id}_P, \psi) : (P, \mathbb{Z}^m) \longrightarrow (P, \mathbb{Z}^\ell)$, where $\psi : \mathbb{Z}^m \longrightarrow \mathbb{Z}^\ell$ is the left multiplication by V, is a homomorphism of graded rings in the sense of Definition 1.7.7.
b) If ψ is injective, then we have $P_{W,d} = P_{V \cdot W, V \cdot d}$ for all $d \in \mathbb{Z}^m$.

Proof. First we prove a). Since P is generated by $\mathbb{T}^n$ as a K-vector space, and since terms are homogeneous, it suffices to prove the claim for a term $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in P_{W,d}$. In this case we have $\deg_W(t) = d$, and therefore $\deg_{V \cdot W}(t) = V \cdot W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}} = V \cdot d$.

Now we prove b). Let $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in P_{V \cdot W, V \cdot d}$ for some $d \in \mathbb{Z}^m$. Then $\deg_{V \cdot W}(t) = V \cdot d$ implies $V \cdot W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}} = V \cdot d$. By hypothesis, ψ is injective, so we get $W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}} = d$, i.e. we have $\deg_W(t) = d$. Thus the inclusion $P_{W,d} \subseteq P_{V \cdot W, V \cdot d}$ is in fact an equality. □

Let us apply this proposition in the setting of Example 4.1.7.

Example 4.1.10. Let $P = K[x_1, x_2, x_3, x_4]$ be graded by $W = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$. First we want to determine the homogeneous component $P_{W,d}$ of degree $d = (2, 1, 1)$.

By definition, this vector space is generated by the terms $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ such that $W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}} = d$. The set of solutions in $\mathbb{N}^n$ of this system of equations is $\{(1, 0, 0, 1), (0, 1, 1, 0)\}$. Thus we have $P_{W,d} = K \cdot x_1 x_4 \oplus K \cdot x_2 x_3$.

Now let w_1, w_2, w_3 be the rows of W. We replace w_2 by $w_1 + w_2$ and w_3 by $w_1 + w_3$, i.e. we form the matrix $V \cdot W$, where $V = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{smallmatrix}\right)$. Then we get $V \cdot d = (2,3,3)^{\mathrm{tr}}$, and therefore the homogeneous component of P of degree $e = (2,3,3)$ with respect to the grading defined by $V \cdot W$ is given by $P_{V \cdot W, e} = K \cdot x_1 x_4 \oplus K \cdot x_2 x_3$.

4.1.B Graded Modules

Here we take a look at graded modules over graded polynomial rings. Let a $\mathbb{Z}^m$-grading on the polynomial ring $P = K[x_1, \ldots, x_n]$ be defined by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$. In Section 1.7 we defined a very general notion of graded P-modules. In the following we consider modules graded over the $\mathbb{Z}^m$-monomodule $\mathbb{Z}^m$, i.e. we use the same monoid that we used for the grading of P. Thus a graded P-module has a decomposition $M = \bigoplus_{d \in \mathbb{Z}^m} M_d$ and we have $P_d \cdot M_{d'} \subseteq M_{d+d'}$ for all $d, d' \in \mathbb{Z}^m$. We shall now see that the usual ideal-theoretic and module-theoretic operations again produce homogeneous ideals and graded modules when they are applied to such objects.

Proposition 4.1.11. *Let P be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $I \subseteq P$ be a homogeneous ideal, let U be a graded P-module, and let M and N be graded submodules of U.*

a) The sum $M + N$ and the intersection $M \cap N$ are graded submodules of U.
b) The colon ideal $N :_P M$ is a homogeneous ideal in P.
c) The ideal $\mathrm{Ann}_P(M)$ is a homogeneous ideal in P.
d) The colon module $N :_M I$ and the saturation $N :_M I^\infty$ are graded submodules of U.
e) The radical ideal $\sqrt{I}$ is a homogeneous ideal in P.

Proof. The proof of a) is straightforward, so let us proceed to b). Clearly, the claim is true if $N :_P M = (0)$. Let $f \in P$ be a non-zero polynomial such that $f \cdot M \subseteq N$, and let $f = \sum_{d \in \mathbb{Z}^m} f_d$ be its decomposition into homogeneous components. For every homogeneous vector $v \in M$, we have $fv = \bigoplus_{d \in \mathbb{Z}^m} f_d v \in N$. This sum is the decomposition of fv into homogeneous components. Since N is a graded module, we get $f_d v \in N$ for all $d \in \mathbb{Z}^m$. Hence we see that $f_d \in N :_P M$ for all $d \in \mathbb{Z}^m$, as we wanted to show. Claim c) is a special case of b), and d) follows in a similar way.

To prove e), we write $f \in \sqrt{I}$ as the sum of its homogeneous components $f = f_{d_1} + \cdots + f_{d_\ell}$, where $d_1 >_{\mathtt{Lex}} d_2 >_{\mathtt{Lex}} \cdots >_{\mathtt{Lex}} d_\ell$. We shall show that $f - f_{d_1} \in \sqrt{I}$. Then the claim follows by induction on ℓ. Let $i > 0$ be a number such that $f^i \in I$. When we expand this power, we obtain a sum of homogeneous polynomials among which $f_{d_1}^i$ has the largest degree with respect to `Lex`. Hence $f_{d_1}^i$ is the homogeneous component of degree $i \cdot d_1$

of f^i, and the fact that I is a homogeneous ideal implies $f_{d_1}^i \in I$. Thus we get $f_{d_1} \in \sqrt{I}$, as desired. □

Corollary 4.1.12. *Let I be a monomial ideal in P. Then the radical $\sqrt{I}$ is the monomial ideal generated by the squarefree parts of the terms in the minimal monomial system of generators of I.*

Proof. Let $W \in \mathrm{Mat}_n(\mathbb{Z})$ be a non-singular matrix. By Proposition 4.1.8, the ideal I is homogeneous with respect to the grading given by W. Then part e) of the proposition says that $\sqrt{I}$ is homogeneous, too. Now another application of Proposition 4.1.8 shows that $\sqrt{I}$ is a monomial ideal. Clearly, if a term $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is one of the minimal monomial generators of I, then its squarefree part $\prod_{\{i|\alpha_i>0\}} x_i$ is contained in $\sqrt{I}$. On the other hand, every term in $\sqrt{I}$ has a power which is a multiple of one of the minimal monomial generators of I, and therefore the term is a multiple of one of those squarefree parts. □

As usual, we want to relate different graded modules to each other using suitable homomorphisms. Recall that in Definition 1.7.7 we introduced homomorphisms of rings graded by monoids, and of modules graded by monomodules. In the present situation, that definition specializes in the following way.

Let P be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let M, N be two $\mathbb{Z}^m$-graded P-modules. A P-linear map $\varphi : M \longrightarrow N$ is called a **homomorphism of graded modules** or a **homogeneous P-linear map** if $\varphi(M_d) \subseteq N_d$ for all $d \in \mathbb{Z}^m$. Important examples of such maps are constructed as follows.

Remark 4.1.13. Let P be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let M be a graded P-module. Given homogeneous elements $v_1, \ldots, v_r \in M$ with $\deg_W(v_i) = \delta_i \in \mathbb{Z}^m$ for $i = 1, \ldots, r$, the P-linear map $\varphi : F \longrightarrow M$ defined by $e_i \mapsto v_i$ for $i = 1, \ldots, r$ is a homomorphism of graded modules. We shall say that φ is the map **induced by** $(v_1, \ldots, v_r)$.

An easy way to construct graded modules comes from the observation that, given a homogeneous P-linear map $\lambda : M \longrightarrow N$ between $\mathbb{Z}^m$-graded P-modules, the kernel $\mathrm{Ker}(\lambda)$ is a graded submodule of M and the image $\mathrm{Im}(\lambda)$ is a graded submodule of N. Another kind of graded modules are graded submodules of graded free modules. Let us briefly recall the pertinent definitions.

According to Definition 1.7.6, the grading on P induces a $\mathbb{Z}^m$-grading on the graded free P-module $F = \bigoplus_{i=1}^r P(-\delta_i)$: this grading is given by

$$F_d = \bigoplus_{i=1}^{r} P_{W,\, d-\delta_i}$$

for all $d \in \mathbb{Z}^m$. Thus a term $te_i \in \mathbb{T}^n\langle e_1, \ldots, e_r\rangle$, where $i \in \{1, \ldots, r\}$ and $t \in \mathbb{T}^n$, is a homogeneous element of F of degree $\deg_W(te_i) =$

$\deg_W(t) + \delta_i$. In particular, the module F is the graded free P-module such that $\deg_W(e_i) = \delta_i$ for $i = 1, \ldots, r$.

Given a graded P-submodule M of F, we shall briefly say that M is **graded by** W. The homogeneous components of M will be denoted by $M_{W,d}$ for $d \in \mathbb{Z}^m$. Recall, from Definition 1.7.8, that a graded submodule of P is also called a **homogeneous ideal** of P.

Under the change of grading homomorphism considered in Proposition 4.1.9, a graded submodule of a graded free module is transformed into a graded submodule with respect to the new grading, as the following proposition shows.

Proposition 4.1.14. *Let P be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $r \geq 1$, let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, and let M be a graded submodule of F. Moreover, let $V \in \mathrm{Mat}_{\ell,m}(\mathbb{Z})$ for some $\ell \geq 1$. Then M is also a graded submodule of $\bigoplus_{i=1}^r P(-V \cdot \delta_i)$ with respect to the grading defined by $V \cdot W$.*

Proof. Using Proposition 4.1.9 and the definition of the grading on F, we see that

$$F_{W,d} = \bigoplus_{i=1}^r P_{W,\, d-\delta_i} \subseteq \bigoplus_{i=1}^r P_{V\cdot W,\, V\cdot d - V\cdot\delta_i} = (\bigoplus_{i=1}^r P(-V\cdot\delta_i))_{V\cdot W,\, V\cdot d}$$

for all $d \in \mathbb{Z}^m$. Since a system of generators of M consisting of homogeneous elements with respect to the grading defined by W is also homogeneous with respect to the grading defined by $V \cdot W$, the claim follows. □

This proposition has a number of useful consequences.

Remark 4.1.15. Suppose we are in the setting of the proposition.

a) Let $V = (a_1\ a_2\ \cdots\ a_m) \in \mathrm{Mat}_{1,m}(\mathbb{Z})$, and let us form the linear combination $V \cdot W$ of the rows $w_1, \ldots, w_m$ of W. Then M is a graded module with respect to the grading defined by the $1 \times n$-matrix $V \cdot W$.
b) Let $a \in \mathbb{Z} \setminus \{0\}$. Then M is a graded submodule of F with respect to the grading given by W if and only if it is a graded submodule with respect to the grading given by $a\,W$. This follows from the observation that the inclusion $F_{W,d} \subseteq F_{aW,ad}$ given by the corollary is, in fact, an equality.

Corollary 4.1.16. *Let $W \neq 0$ have $\mathbb{Z}$-linearly dependent rows, and let W' be a submatrix of W which consists of a maximal linearly independent set of rows. Denote the number of rows of W' by m', and let $V \in \mathrm{Mat}_{m,m'}(\mathbb{Z})$ be the matrix such that $V \cdot W' = W$. Then we have $P_{W',d'} = P_{W,V\cdot d'}$ for all $d' \in \mathbb{Z}^{m'}$.*

Proof. It suffices to show that the inclusion $P_{W',d'} \subseteq P_{V\cdot W',V\cdot d'}$ given by the proposition is an equality. Let $t \in \mathbb{T}^n$ be a term of degree $V \cdot d' = W \cdot \log(t)^{\mathrm{tr}}$. Now, the linear map defined by V is injective, so $d' = W' \cdot \log(t)^{\mathrm{tr}}$. Hence t is homogeneous of degree d' with respect to the grading given by W', and the above inclusion is indeed an equality. □

In view of this corollary, we shall, from now on, assume tacitly that the matrix W has $\mathbb{Z}$-linearly independent rows, unless we explicitly say something else.

4.1.C Gradings of Positive Type

Our first goal in this subsection is to find hypotheses which force the homogeneous components of P to be finite dimensional K-vector spaces. For instance, this is the case for the grading defined by $W = (1\ 1\ \cdots\ 1)$. Moreover, Proposition 4.1.9.a shows that it is then also the case for every grading defined by a matrix whose first row is $(1\ 1\ \cdots\ 1)$. Inspired by this observation, we introduce the following notions.

Definition 4.1.17. Let $m \geq 1$, let P be graded by a matrix W of rank m in $\mathrm{Mat}_{m,n}(\mathbb{Z})$, and let $w_1, \ldots, w_m$ be the rows of W.

a) The grading on P given by W is called **of non-negative type** if there exist $a_1, \ldots, a_m \in \mathbb{Z}$ such that the entries of $v = a_1w_1 + \cdots + a_mw_m$ corresponding to the non-zero columns of W are positive. In this case, we shall also say that W is a matrix of non-negative type.

b) We say that the grading on P given by W is **of positive type** if there exist $a_1, \ldots, a_m \in \mathbb{Z}$ such that all entries of $a_1w_1 + \cdots + a_mw_m$ are positive. In this case, we shall also say that W is a matrix of positive type.

For instance, the matrix $W = (-1\ -1\ 0)$ is of non-negative type, the matrix $W' = (-1\ -1)$ is of positive type, but $W'' = (1\ -1)$ is neither. Gradings of non-negative type are intimately connected to $\mathbb{N}$-gradings, as the following proposition shows.

Proposition 4.1.18. *Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of non-negative type, let $\Gamma = \{d \in \mathbb{Z}^m \mid P_{W,d} \neq 0\}$, and suppose that $V = (a_1\ a_2\ \cdots\ a_m) \in \mathrm{Mat}_{1,m}(\mathbb{Z})$ is such that $V \cdot W = a_1w_1 + \cdots + a_mw_m$ has all entries non-negative.*

a) The map $(\mathrm{id}_P, \psi) : (P, \mathbb{Z}^m) \longrightarrow (P, \mathbb{Z})$, where $\psi : \mathbb{Z}^m \longrightarrow \mathbb{Z}$ is left multiplication by V, is a homomorphism of graded rings. It satisfies $\psi(\Gamma) \subseteq \mathbb{N}$.

b) There exists a matrix $U \in \mathrm{Mat}_m(\mathbb{Z})$ such that $\det(U) \neq 0$ and the non-zero columns of $U \cdot W$ have all entries positive.

c) If W is of positive type, there exists a matrix $U \in \mathrm{Mat}_m(\mathbb{Z})$ such that $\det(U) \neq 0$ and $U \cdot W$ has positive entries only.

Proof. The first part of claim a) follows from Proposition 4.1.9.a, while the second part is a consequence of the fact that $V \cdot W$ has non-negative entries only.

To prove b), we note that if $a_i \neq 0$ for some $i \in \{1, \ldots, m\}$, then we can replace the i^{th} row of W by $a_1 w_1 + \cdots + a_m w_m$ using a suitable transformation given by a matrix $U_1 \in \mathrm{Mat}_m(\mathbb{Z})$. Next we multiply by a permutation matrix $U_2 \in \mathrm{Mat}_m(\mathbb{Z})$ such that this row becomes the first row. Finally, by adding sufficiently high multiples of this new first row to the other rows, we can make all entries in the non-zero columns of W positive. Let $U_3 \in \mathrm{Mat}_m(\mathbb{Z})$ correspond to those row operations. Then $U = U_3 \cdot U_2 \cdot U_1$ is the desired matrix.

Finally we note that c) follows from b), because a matrix of positive type has all columns non-zero. □

Now we are ready to show that polynomial rings with gradings of positive type and finitely generated graded modules over them have finite dimensional homogeneous components.

Proposition 4.1.19. *Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type, and let M be a finitely generated graded P-module.*

a) We have $P_0 = K$.
b) For all $d \in \mathbb{Z}^m$, we have $\dim_K(M_d) < \infty$.

Proof. First we show a). Let $V = (a_1 \ a_2 \ \cdots \ a_m) \in \mathrm{Mat}_{1,m}(\mathbb{Z})$ be such that $V \cdot W$ has positive entries only. Using Proposition 4.1.9, we see that $P_{W,0} \subseteq P_{V \cdot W,0}$. Now it suffices to note that every term $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \neq 1$ has positive degree $\deg_{V \cdot W}(t) = V \cdot W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}} > 0$.

In order to prove b), we choose a finite homogeneous system of generators of M and consider the corresponding representation $M \cong F/N$ where N is a graded submodule of F.

Clearly, it suffices to prove the claim for F. We do this by showing it is true for each $P(-\delta_i)$. Since $P(-\delta_i)_d = P_{d-\delta_i}$, it suffices to prove that $\dim_K(P_d) < \infty$ for all $d \in \mathbb{Z}^m$. Since W is of positive type, there exists a matrix $V \in \mathrm{Mat}_{1,m}(\mathbb{Z})$ such that $V \cdot W$ has all entries positive. We use Proposition 4.1.9.a to see that $P_{W,d} \subseteq P_{V \cdot W, V \cdot d}$. Hence we only have to show that the K-vector spaces $P_{V \cdot W, i}$ are finite dimensional for all $i \in \mathbb{Z}$. Their vector space bases $\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid V \cdot W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}} = i\}$ are finite, because $V \cdot W$ has positive entries only. □

A further advantage of considering finitely generated graded P-modules in the case of gradings of positive type is that Nakayama's Lemma applies to them. In Corollary 1.7.16 we used the notion of a minimal system of generators of M, and in Corollary 3.1.12 we mentioned irredundant systems of generators. Let us give the precise definitions.

Definition 4.1.20. Let R be a ring and M a finitely generated R-module.

a) A finite system of generators of M is called a **minimal system of generators** if its number of elements is minimal among all systems of generators of M.

b) A system of generators of M is called an **irredundant system of generators** if no proper subset generates M.

Minimal systems of generators are irredundant. Over arbitrary rings, the two notions do not coincide. For instance, when $R = \mathbb{Z}$ and M is the ideal generated by $\{2\}$, the system of generators $\{4, 6\}$ is irredundant, but not minimal. One of the most important consequences of Nakayama's Lemma is that, in the case of gradings of positive type, irredundant systems of homogeneous generators of finitely generated graded modules are minimal. This will be shown in Proposition 4.1.22.

To formulate our next result, we need two additional objects. Let P be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let $M \neq 0$ be a graded P-module. Then the set $\Gamma = \{d \in \mathbb{Z}^m \mid P_d \neq 0\}$ is clearly a submonoid of $\mathbb{Z}^m$, and we can define the Γ-submonomodule Σ of $\mathbb{Z}^m$ generated by $\{d \in \mathbb{Z}^m \mid M_d \neq 0\}$. It is easy to see that $\Sigma = \{d \in \mathbb{Z}^m \mid M_d \neq 0\}$ if M is a submodule of a graded free P-module. If the grading on P is of non-negative type, these monomodules are well-ordered, as the following proposition shows.

Proposition 4.1.21. *Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of non-negative type.*

a) There exists a monoid ordering τ on $\mathbb{Z}^m$ such that the restriction of τ to Γ is a well-ordering.
b) For every finitely generated, graded P-module M, the restriction of τ to the monomodule Σ is a well-ordering.
c) If W is of positive type, there exists a monoid ordering τ on Γ which is a well-ordering and for which the set $P_+ = \bigoplus_{d>_\tau 0} P_d$ is the ideal generated by $\{x_1, \ldots, x_n\}$.

Proof. First we show a). Using Proposition 4.1.18.b, we find $U \in \mathrm{Mat}_m(\mathbb{Z})$ such that $\det(U) \neq 0$ and all non-zero columns of $U \cdot W$ have positive entries only. For vectors $d, d' \in \mathbb{Z}^m$, we define $d \geq_\tau d'$ if and only if $U \cdot d \geq_{\mathtt{Lex}} U \cdot d'$. Clearly, this rule specifies a monoid ordering τ on $\mathbb{Z}^m$. Its restriction to the submonoid Γ is still a monoid ordering. It remains to show that $\tau|_\Gamma$ is a well-ordering on Γ.

Suppose that $d_1 >_\tau d_2 >_\tau \cdots$ is an infinite descending chain of elements of Γ. Then, by definition, we have $U \cdot d_1 >_{\mathtt{Lex}} U \cdot d_2 >_{\mathtt{Lex}} \cdots$. For every $d_i \in \Gamma$, there exists a term $t_i = x_1^{\alpha_{i1}} \cdots x_n^{\alpha_{in}}$ such that $d_i = W \cdot (\alpha_{i1}, \ldots, \alpha_{in})^{\mathrm{tr}}$. Therefore we have $U \cdot d_i = U \cdot W \cdot (\alpha_{i1}, \ldots, \alpha_{in})^{\mathrm{tr}}$, and this vector has all entries non-negative. Since $\mathtt{Lex}$ is a term ordering on $\mathbb{N}^n$, Proposition 1.4.18 and Theorem 1.4.19 imply that an infinite chain $U \cdot d_1 >_{\mathtt{Lex}} U \cdot d_2 >_{\mathtt{Lex}} \cdots$ does not exist.

To prove b), we let $\{m_1, \ldots, m_s\} \subseteq M \setminus \{0\}$ be a homogeneous system of generators of M and define $\gamma_i = \deg(m_i)$ for $i = 1, \ldots, s$. By Corollary 1.7.11, we have $\Sigma \subseteq \cup_{i=1}^s (\Gamma + \gamma_i)$. Let σ be the restriction of τ to the Γ-submonomodule Σ of $\mathbb{Z}^m$. Clearly, σ is a module ordering which is compatible with τ.

Now we show that the restriction of τ to $\cup_{i=1}^{s}(\Gamma+\gamma_i)$ is a well-ordering. Suppose there is an infinite descending chain $d_1 >_\tau d_2 >_\tau \cdots$ in $\cup_{i=1}^{s}(\Gamma+\gamma_i)$. Then one of the sets $\Gamma+\gamma_i$ has to contain infinitely many degrees d_j, i.e. there exist indices $j_1 < j_2 < \cdots$ such that $d_{j_1} >_\tau d_{j_2} >_\tau \cdots$ is a chain in $\Gamma+\gamma_i$. Now the chain $d_{j_1}-\gamma_i >_\tau d_{j_2}-\gamma_i >_\tau \cdots$ contradicts the fact that τ is a well-ordering on Γ.

Finally, we note that c) follows from the observation that the well-ordering τ constructed in the proof of a) satisfies $\deg_W(x_i) >_\tau 0$, since $\deg_{U\cdot W}(x_i) >_{\mathtt{Lex}} 0$ for $i = 1, \ldots, n$. □

Using this proposition, we see that the hypotheses of the Graded Version of Nakayama's Lemma 1.7.15 are satisfied for gradings of non-negative type. If the grading is actually of positive type, we obtain the result we strived for.

Proposition 4.1.22. *Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type, and let $M \neq 0$ be a finitely generated graded P-module.*

a) A set of homogeneous elements $m_1, \ldots, m_s$ generates the P-module M if and only if their residue classes $\overline{m}_1, \ldots, \overline{m}_s$ generate the K-vector space $M/(x_1, \ldots, x_n)M$.

b) Every homogeneous system of generators of M contains a minimal one. All irredundant systems of homogeneous generators of M are minimal and have the same number of elements.

Proof. By Proposition 4.1.21.c, there exists a well-ordering τ on Γ such that $P_+ = \bigoplus_{d>_\tau 0} P_d = (x_1, \ldots, x_n)$, and therefore $P/P_+ \cong K$. Hence a) follows from Corollary 1.7.16.a. Now we prove b). Since $P_0 = K$ is a field, Corollary 1.7.16.b shows that every homogeneous system of generators of M contains a subset which is minimal among the homogeneous systems of generators of M and whose residue classes form a K-basis of $M/(x_1, \ldots, x_n)M$. This subset is also minimal among all systems of generators of M because, for any set of generators of M, their set of residue classes generates $M/(x_1, \ldots, x_n)M$. □

This proposition is not true in general if W is of non-negative type.

Example 4.1.23. Let $P = \mathbb{Q}[x, y]$ be graded by the matrix $W = (0\ 1)$, and let $I = (xy,\ y - xy)$. Then W is of non-negative type, I is a homogeneous ideal, and $\{xy,\ y - xy\}$ is an irredundant homogeneous system of generators of I. However, since $I = (y)$, this system of generators is not minimal. Notice that we have $P_+ = (y)$ and $P/P_+ \cong K[x]$ here.

Exercise 1. Let K be a field, let Γ be a monoid, let R be a Γ-graded K-algebra for which $K \subseteq R_0$, and let $S \subset R$ be a K-subalgebra which is generated, as a K-algebra, by homogeneous elements. Show that if we define $S_\gamma = S \cap R_\gamma$ for all $\gamma \in \Gamma$, then S is a Γ-graded K-subalgebra of R.

Exercise 2. Let K be a field, and let $P = K[x_1, x_2]$ be equipped with the standard grading. In Example 4.1.5 we have seen that the ring $S = K[x_1^2, x_1x_2, x_2^2]$ is a graded K-subalgebra of P but is not a standard graded K-algebra. On the other hand, it is easy to see (by hand or by using the CoCoA procedure `Elim`) that $S \cong K[y_1, y_2, y_3]/(y_1y_3 - y_2^2)$. If we endow $K[y_1, y_2, y_3]$ with the standard grading, the ideal $(y_1y_3 - y_2^2)$ is homogeneous and S is a standard graded K-algebra. Explain the apparent contradiction.

Exercise 3. Let $P = K[x_1, \ldots, x_n]$ be standard graded. For a polynomial $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in P$ and for $i \in \{1, \ldots, n\}$, we define

$$\tfrac{\partial f}{\partial x_i} = \sum_{\alpha \in \mathbb{N}^n} \alpha_i \, c_\alpha \, x_1^{\alpha_1} \cdots x_{i-1}^{\alpha_{i-1}} \, x_i^{\alpha_i - 1} \, x_{i+1}^{\alpha_{i+1}} \cdots x_n^{\alpha_n}$$

and call it the **partial derivative** of f by x_i.

a) For $f, g \in P$ and $i \in \{1, \ldots, n\}$, show that $\frac{\partial (f+g)}{\partial x_i} = \frac{\partial f}{\partial x_i} + \frac{\partial g}{\partial x_i}$.
b) Let $d \geq 0$, and let $f \in P_d$ be a homogeneous polynomial of degree d. Prove **Euler's formula** $d\,f = \sum_{i=1}^n x_i \cdot \frac{\partial f}{\partial x_i}$.

Exercise 4. Let $P = K[x_1, \ldots, x_n]$ be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $w_1, \ldots, w_m$ be the rows of W, and let $a_1, \ldots, a_m \in \mathbb{Z}$. Show that the pair (id_P, ψ), where $\psi : \mathbb{Z}^m \longrightarrow \mathbb{Z}$ is defined by $\psi(e_i) = a_i$ for $i = 1, \ldots, m$, is a homomorphism of graded rings.

Exercise 5. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be graded by a non-singular matrix $W \in \mathrm{Mat}_n(\mathbb{Z})$, and let M be a graded submodule of a graded free P-module $F = \oplus_{i=1}^r P(-\delta_i)$, where $\delta_1, \ldots, \delta_r \in \mathbb{Z}^n$. Prove that M is generated by vectors of the form $v = (c_1t_1, \ldots, c_rt_r)$, where $c_1, \ldots, c_r \in K$ and $t_1, \ldots, t_r \in \mathbb{T}^n$ are terms with the property that $\deg_W(t_1) + \delta_1 = \cdots = \deg_W(t_r) + \delta_r$.

Exercise 6. Let $P = K[x_1, \ldots, x_n]$, let $r > 0$, and let M be a P-submodule of P^r. Show that the following conditions are equivalent.

a) The module M is a monomial module.
b) For every $m \geq 1$ and every matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and for all vectors $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, the module M is a graded submodule of $\bigoplus_{i=1}^r P(-\delta_i)$ with respect to the grading on P given by W.
c) For some non-singular matrix $W \in \mathrm{Mat}_n(\mathbb{Z})$ and for all vectors $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, the module M is a graded submodule of $\bigoplus_{i=1}^r P(-\delta_i)$ with respect to the grading on P given by W.

Furthermore, give an example which shows that a) is not equivalent to the following condition.

d) For every $m \geq 1$ and every matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and for some vectors $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, the module M is a graded submodule of $\bigoplus_{i=1}^r P(-\delta_i)$ with respect to the grading on P given by W.

Exercise 7. Let K be a field, and let $P = K[x_1, \ldots, x_n]$ be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$.

a) Given an invertible matrix $V \in \mathrm{Mat}_m(\mathbb{Z})$, consider the homomorphism of graded rings $(\mathrm{id}_P, \varphi) : (P, \mathbb{Z}^m) \longrightarrow (P, \mathbb{Z}^m)$, where the ring on the right-hand side is graded by $V \cdot W$ and $\varphi : \mathbb{Z}^m \longrightarrow \mathbb{Z}^m$ is left multiplication by V. Show that (id_P, φ) is an isomorphism of graded rings, i.e. that there exists a homomorphism of graded rings $(\mathrm{id}_P, \psi) : (P, \mathbb{Z}^m) \longrightarrow (P, \mathbb{Z}^m)$ such that $\varphi \circ \psi = \psi \circ \varphi = \mathrm{id}_{\mathbb{Z}^m}$.

b) Find an example which shows that it is not sufficient in a) to assume that V is non-singular.

c) Can you find necessary and sufficient conditions for two matrices $W, W' \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ to give isomorphic gradings in the sense that there is an isomorphism of graded rings $(\mathrm{id}_P, \psi) : (P, \mathbb{Z}^m) \longrightarrow (P, \mathbb{Z}^m)$?

Exercise 8. Show that $W = \left(\begin{smallmatrix} 1 & -1 & 1 \\ -1 & 2 & 0 \end{smallmatrix}\right)$ is of positive type and that $W = \left(\begin{smallmatrix} 1 & -1 & 1 \\ 1 & 1 & -1 \end{smallmatrix}\right)$ is not of non-negative type.

Exercise 9. Let $K[x_1, \ldots, x_n]$ be graded by $W = (w_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $f \in P$ be a homogeneous polynomial, and let $(a_1, \ldots, a_n) \in K^n$ such that $f(a_1, \ldots, a_n) = 0$.

a) For $m = 1$, show that $f(a_1 b^{w_{11}}, \ldots, a_n b^{w_{1n}}) = 0$ for all $b \in K$.

b) For $m = 2$, show that $f(a_1 b_1^{w_{11}} b_2^{w_{21}}, \ldots, a_n b_1^{w_{1n}} b_2^{w_{2n}}) = 0$ for all $b_1, b_2 \in K$.

c) Find and prove a generalization of a) and b) to arbitrary $m \geq 1$.

Exercise 10. Let $P = K[x]$ be graded by $W \in \mathrm{Mat}_{m,1}(\mathbb{Z}) \setminus \{0\}$. Show that $\dim_K(P_d) \leq 1$ for all $d \in \mathbb{Z}^m$.

Exercise 11. Let $P = K[x_1, \ldots, x_n]$ be graded by $W \in \mathrm{GL}_n(\mathbb{Z})$.

a) Show that $\dim_K(P_d) \leq 1$ for all $d \in \mathbb{Z}^m$.

b) Give an example where $P_d = 0$ for some $d \in \mathbb{Z}^m$.

Exercise 12. Let K be a field, and let $P = K[x_1, \ldots, x_n]$ be graded by a matrix $W \in \mathrm{Mat}_{n-1,n}(\mathbb{Z})$ of rank $n-1$. For each degree $d \in \mathbb{N}^{n-1}$, prove that there exists a line ℓ_d in $\mathbb{Q}^n$ for which $\ell_d \cap \mathbb{N}^n$ coincides with the set $\{\log(t) \mid t \in \mathbb{T}^n, \deg_W(t) = d\}$.

Exercise 13. Let $K[x_1, \ldots, x_n]$ be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and assume that $\dim_K(P_0) < \infty$. Prove that $P_0 = K$.

Exercise 14. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type, let I be a homogeneous ideal in P, and let $A = P/I$. Moreover, let $\Sigma = \{d \in \mathbb{Z}^m \mid A_d \neq 0\}$, and let τ be a monoid ordering on $\mathbb{Z}^m$ whose restriction to Σ is a well-ordering (see Proposition 4.1.21). Finally, let $a_1, \ldots, a_s \in A$ be homogeneous elements such that $\deg_W(a_i) >_\tau 0$ for $i = 1, \ldots, s$, and let $A_+ = \bigoplus_{d >_\tau 0} A_d$. Prove that the following conditions are equivalent.

a) $A = K[a_1, \ldots, a_s]$

b) $A_+ = (a_1, \ldots, a_s)$

Exercise 15. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type, let M be a finitely generated graded P-module, and let $\varphi : M \longrightarrow M$ be a homogeneous P-linear map. Prove that the following conditions are equivalent.

a) The map φ is an isomorphism.
b) The map φ is injective.
c) The map φ is surjective.

Moreover, show that φ is an isomorphism if $v - \varphi(v) \in (x_1, \ldots, x_n)M$ for all $v \in M$.

Tutorial 45: Homogeneous Maps and Toric Ideals

One of the most important tools for computing kernels and images of K-algebra homomorphisms is the **diagonal ideal**. Given two polynomial rings $P = K[x_1, \ldots, x_n]$ and $P' = K[y_1, \ldots, y_m]$ over a field K and two ideals $I \subset P$ and $I' \subset P'$, a K-algebra homomorphism $\varphi : P/I \longrightarrow P'/I'$ is determined by polynomials $f_1, \ldots, f_n \in P'$ such that $\varphi(x_i + I) = f_i + I'$ for $i = 1, \ldots, n$. Then the **diagonal ideal** corresponding to φ is defined to be the ideal

$$J = I'Q + (x_1 - f_1, \ldots, x_n - f_n)$$

in the polynomial ring $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$. Its usefulness for studying φ was amply exhibited in Section 3.6. What is the correct analog of these constructions in the graded case? In this tutorial, we shall try to answer this question, and to apply our results to toric ideals.

Let $\ell \geq 1$, let P be graded by $W \in \mathrm{Mat}_{\ell,n}(\mathbb{Z})$, and let P' be graded by $W' \in \mathrm{Mat}_{\ell,m}(\mathbb{Z})$. Suppose that I and I' are homogeneous ideals with respect to these gradings.

a) Show that φ is a homomorphism of graded rings if and only if each polynomial f_i is homogeneous and $\deg_{W'}(f_i) = \deg_W(x_i)$.
b) Now suppose that $I = (0)$ and that $f_1, \ldots, f_n \in P'$ are homogeneous polynomials. Prove that there is a unique grading on P by a matrix $W \in \mathrm{Mat}_{\ell,n}(\mathbb{Z})$ such that φ is a homomorphism of graded algebras.
c) Assume that φ is a homomorphism of graded rings. Prove that if W' is of positive type, then W is of positive type, too. (*Hint:* Observe that $W = W'S$ for a suitable matrix $S \in \mathrm{Mat}_{m,n}(\mathbb{N})$.)
d) Next we equip the polynomial ring $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ with the grading given by the matrix $W'' = (W|W') \in \mathrm{Mat}_{\ell,m+n}(\mathbb{Z})$. Show that the diagonal ideal J is homogeneous if and only if φ is a homomorphism of graded rings.

For the remainder of this tutorial, we assume that φ is a homomorphism of graded rings and that W, W', W'' are chosen as above.

e) Prove that if W' is of positive type, then W'' is of positive type.
f) Given any homogeneous ideal $\widetilde{J} \subseteq Q$, show that $\widetilde{J} \cap P$ is a homogeneous ideal in P. Use this result and Proposition 3.6.3 to give two proofs for the fact that $J \cap P$ is a homogeneous ideal in P.

Now we specialize the above to the situation where $I' = (0)$ and $f_1, \ldots, f_n$ are terms. Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{N})$ be such that $f_i = y_1^{a_{1i}} \cdots y_m^{a_{mi}}$ for $i = 1, \ldots, n$, and let $I = J \cap P$ be the **toric ideal** associated to $\mathcal{A}$ (see Tutorial 38).

g) Prove that I is homogeneous with respect to the grading given by $\mathcal{A}$. (*Hint:* Use the grading on P' given by the identity matrix $W' = \mathcal{I}_n$.)

h) Let $I_{\mathcal{L}}$ be the **lattice ideal** associated to the lattice of integer solutions of the homogeneous system of Diophantine equations defined by $\mathcal{A}$ (see Tutorial 38.h). Use the identity $I = I_{\mathcal{L}} :_P (x_1 \cdots x_n)^\infty$ to give an alternative proof of g).

Tutorial 46: Projective Varieties

In algebraic geometry, graded rings occur in a variety of ways. The most important way they appear is undoubtedly as the homogeneous coordinate rings of projective varieties. In order to define and study projective varieties, we need to assume that you have mastered Section 2.6, and that you have a good working knowledge both of Tutorial 27 on affine varieties and of the first part of Tutorial 35 on projective spaces.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ and $\overline{P} = K[x_0, \ldots, x_n]$ be standard graded, and let $\mathbb{A}_K^n$ (resp. $\mathbb{P}_K^n$) be the n-dimensional affine (resp. projective) space over K. Moreover, let L be an extension field of K, and let $\overline{K}$ be the algebraic closure of K. For every homogeneous ideal $J \subseteq \overline{P}$, we let

$$\mathcal{Z}_L^+(J) = \{(p_0 : \ldots : p_n) \in \mathbb{P}_L^n \mid f(p_0, \ldots, p_n) = 0 \text{ for all homogeneous } f \in J\}$$

A subset $V \subseteq \mathbb{P}_L^n$ is called a **projective zero-set** defined over K if it is of the form $V = \mathcal{Z}_L^+(J)$ for some homogeneous ideal $J \subseteq \overline{P}$. Projective zero-sets in $\mathbb{P}_{\overline{K}}^n$ are also called **projective varieties**.

a) Show that projective zero-sets have the following properties.

   1) The empty set $\emptyset$ and $\mathbb{P}_L^n$ are projective zero-sets.
   2) If $V_1, \ldots, V_s \subseteq \mathbb{P}_L^n$ are projective zero-sets, then $\cup_{i=1}^s V_i$ is a projective zero-set.
   3) If I is a set of indices and $\{V_i\}_{i \in I}$ a set of projective zero-sets indexed by I, then $\cap_{i \in I} V_i$ is a projective zero-set.

   Conclude that projective zero-sets can be taken as the closed sets of a topology on $\mathbb{P}_L^n$. When $K = L$, this topology is called the **Zariski topology** on $\mathbb{P}_K^n$.

b) Recall that, in Tutorial 36, we defined $\mathbb{P}_K^n$ as a set of equivalence classes $(K^{n+1} \setminus \{0\})/\sim$. Every point $p = (p_0 : \ldots : p_n)$ in $\mathbb{P}_K^n$ is the equivalence class of a punctured line $L(p) = \{(\lambda p_0, \ldots, \lambda p_n) \mid \lambda \in K \setminus \{0\}\}$ in $\mathbb{A}_K^{n+1}$. Show that, for every homogeneous ideal $J \subseteq \overline{P}$, the projective zero-set

$\mathcal{Z}_L^+(J) \subseteq \mathbb{P}_L^n$ is the set of equivalence classes of punctured lines contained in $\mathcal{Z}_L(J) \subseteq \mathbb{A}_L^{n+1}$. In other words, we have $p \in \mathcal{Z}_L^+(J)$ if and only if $L(p) \subseteq \mathcal{Z}_L(J)$.

The affine zero-set $\mathcal{Z}_L(J) \subseteq \mathbb{A}_L^{n+1}$ is called the **affine cone over** $\mathcal{Z}_L^+(J)$.

c) Prove the following projective version of the Weak Nullstellensatz:
For a homogeneous ideal $J \subseteq \overline{P}$, we have $\mathcal{Z}_{\overline{K}}^+(J) = \emptyset$ if and only if $\sqrt{J} = (x_0, \ldots, x_n)$.
Hint: If there exists a point $q \in \mathcal{Z}_{\overline{K}}(J) \backslash \{0\}$, then the punctured line $L(q)$ is contained in $\mathcal{Z}_{\overline{K}}(J)$. Now use b) and Proposition 3.7.1.

d) Using c), show that, for a homogeneous ideal $J \subseteq \overline{P}$, the following conditions are equivalent.
   1) $\mathcal{Z}_{\overline{K}}^+(J) = \emptyset$
   2) There exists a number $s \geq 1$ such that $(x_0, \ldots, x_n)^s \subseteq J$.
   3) For each $i \in \{0, \ldots, n\}$, there exists a number $\alpha_i \geq 1$ such that $x_i^{\alpha_i} \in J$.

Next we introduce the projective analog of Definition 2.6.15. For a set $S \subseteq \mathbb{P}_L^n$, we let $\mathcal{I}^+(S)$ be the ideal in $\overline{P}$ generated by all homogeneous polynomials $F \in \overline{P}$ such that $F(p_0, \ldots, p_n) = 0$ for all $(p_0 : \ldots : p_n) \in S$ (see Tutorial 16.e). The ideal $\mathcal{I}^+(S)$ is called the **homogeneous vanishing ideal** of S. If we have $L = \overline{K}$ and if $S \subseteq \mathbb{P}_{\overline{K}}^n$ is a projective variety defined over K, then the standard graded K-algebra $\overline{P}/\mathcal{I}^+(S)$ is called the **homogeneous coordinate ring** of S.

e) Show that $\mathcal{I}^+(S)$ is a well-defined homogeneous ideal in $\overline{P}$ which satisfies $\mathcal{Z}_L^+(\mathcal{I}^+(S)) \supseteq S$.

f) Prove the following projective version of the Strong Nullstellensatz:
For every homogeneous ideal $J \subseteq \overline{P}$ such that $\sqrt{J} \subset (x_0, \ldots, x_n)$, we have $\mathcal{I}^+(\mathcal{Z}_{\overline{K}}^+(J)) = \sqrt{J}$.
Hint: Show that $\mathcal{I}(\mathcal{Z}_{\overline{K}}(J)) = \mathcal{I}^+(\mathcal{Z}_{\overline{K}}^+(J))$ and apply Hilbert's Nullstellensatz 2.6.16.

g) Construct a 1-1 correspondence between non-empty projective varieties $V \subseteq \mathbb{P}_{\overline{K}}^n$ defined over K and reduced standard graded K-algebras $\overline{P}/J$, where the ideal J is a homogeneous radical ideal which is strictly contained in $(x_0, \ldots, x_n)$.

4.2 Degree Forms and Macaulay Bases

First things first,
but not necessarily in that order.
(Dr. Who)

The introduction to the preceding section ended with the preannouncement of some problems related to gradings of positive type. Is it time to face up to reality? Well, maybe not yet. The aim of the introduction to this section is to highlight the most important points, but we do not necessarily have to do it in the order in which they appear in the section. Let us instead start by confronting the following fundamental question.

What is the degree of a polynomial?

To explain the problem, assume that the polynomial ring $K[x_1, \ldots, x_n]$ over a field K is graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. For the standard grading defined by $W = (1\ 1\ \cdots\ 1)$, we gave the standard answer right away in Section 1.1: the standard degrees of terms are natural numbers, and for a polynomial f, we defined $\deg(f)$ to be the maximum of the degrees of the terms in its support. In the case of the grading defined by an arbitrary matrix W, we have also seen that terms are homogeneous and that their degrees can be computed easily. Furthermore, given two terms, we can decide whether their degrees are equal or not. But which degree is larger?

Let us have a look at a concrete example. Let $K[x_1, x_2]$ be graded by $W = \left(\begin{smallmatrix} 2 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. The polynomial $f = x_1 + x_2$ is the sum of two terms of degrees $\deg_W(x_1) = (2, -1)$ and $\deg_W(x_2) = (1, 0)$. So, what is $\deg_W(f)$? There is no canonical answer. Since degrees are elements of $\mathbb{Z}^m$, we have to choose an ordering on $\mathbb{Z}^m$ to decide which homogeneous component of a given polynomial has the largest degree. In the example at hand, we may observe that W also represents a term ordering $\sigma = \mathtt{Ord}(W)$ on $\mathbb{T}^2$. Using σ, we get $x_1 >_\sigma x_2$, since $W \cdot \log(x_1)^{\mathrm{tr}} >_{\mathtt{Lex}} W \cdot \log(x_2)^{\mathrm{tr}}$. As we saw in Section 1.4, the comparison of two terms with respect to the monoid ordering given by a matrix V is effected by lexicographically comparing the vectors obtained from multiplying V by their logarithms. Thus we get a first clue for solving our problem.

Now consider the following example. Let $K[x_1, x_2, x_3]$ be graded by $W = \left(\begin{smallmatrix} 2 & 1 & 3 \\ -1 & 0 & 1 \end{smallmatrix}\right)$. The polynomial $f = x_1x_3 + x_2^5 + x_1^2x_3$ is the sum of two homogeneous polynomials, namely $f_1 = x_1x_3 + x_2^5$ of degree $\deg_W(f_1) = (5, 0)$ and $f_2 = x_1^2x_3$ of degree $\deg_W(f_2) = (7, -1)$. Again we ask ourselves: what is the degree of f? Suppose we complete the matrix W to a non-singular matrix V by appending the row $(1\ 0\ 0)$. The vectors obtained by taking the scalar products of the logarithms of the three terms in the support of f with the rows of V are $(5, 0, 1)$, $(5, 0, 0)$, and $(7, -1, 2)$. Their lexicographical comparison yields $(7, -1, 2) >_{\mathtt{Lex}} (5, 0, 1) >_{\mathtt{Lex}} (5, 0, 0)$. By construction, the degrees of the three terms are the first two components of those vectors.

Therefore, if we want to let the grading interact with the ordering in a natural way, we should compare degrees lexicographically. In other words, there is a natural *law* for ordering degrees, namely `Lex`.

Having decided to apply the principle of `Lex` *and order*, we can venture further. A grading induces a *partial* ordering on the set of terms. Using this partial ordering, we mimic the developments in Volume 1. The homogeneous component of lexicographically largest degree of a vector of polynomials v will be called the *degree form* of v, and plays a role analogous to its leading term. Then we define degree form ideals and, more generally, degree form modules of submodules of graded free modules. A set of vectors is called a *Macaulay basis* of such a module M if their degree forms generate the degree form module of M. In Subsection B we explore this idea and develop part of the theory of Macaulay bases in analogy with, and as a generalization of, the theory of Gröbner bases.

But something is still missing, both theoretically and practically. Theoretically, we would like Macaulay bases to be systems of generators, and practically we would like to compute them. To fulfil these desires, gradings of positive type are not good enough. Finally the bad news has hit! We need the stronger notion of positive gradings. This corresponds to needing term orderings in Gröbner basis theory instead of arbitrary monoid orderings. Positive gradings are characterized by a degree matrix which has the look and feel of the upper part of a matrix defining a term ordering. The subtleties of positive gradings are investigated in Subsection A. If you want to get a good grasp of this topic, we suggest that you compare Propositions 4.1.21 and 4.2.3 carefully.

Finally, *dulcis in fundo*, we use a mix of positive gradings, term orderings and Gröbner basis theory to compute Macaulay bases (see Proposition 4.2.15 and Corollary 4.2.16). At this point you should be quite satisfied, unless you interpret *dulcis in fundo* as the technical latin term for the melted ice cream at the bottom of a tall thin glass which the spoon is unable to reach. However, if you are developing a taste for Macaulay bases, and have an appetite for further sweet delights, skip ahead to Section 4.3.B where two more treats await you. And if it is all a piece of cake for you, try getting your teeth into Tutorials 47 and 48 where several additional generalizations and characterizations of Macaulay bases are on the menu.

4.2.A Positive Gradings

Let K be a field, let $m \geq 1$, and let $P = K[x_1, \ldots, x_n]$ be $\mathbb{Z}^m$-graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. Recall that we always assume that the rows of W are $\mathbb{Z}$-linearly independent. Moreover, let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, and let F be the graded free P-module $F = \bigoplus_{i=1}^{r} P(-\delta_i)$. The following definition provides us with a first link between gradings and term orderings.

Definition 4.2.1. Let τ be a monoid ordering on $\mathbb{T}^n$ and σ a module ordering on $\mathbb{T}^n\langle e_1,\dots,e_r\rangle$.

a) The ordering τ is called **compatible with** $\deg_W$, or simply **degree compatible**, if $\deg_W(t) >_{\mathtt{Lex}} \deg_W(t')$ implies $t >_\tau t'$ for all $t,t' \in \mathbb{T}^n$.
b) The ordering σ is called **compatible with** $\deg_W$, or simply **degree compatible**, if $\deg_W(te_i) >_{\mathtt{Lex}} \deg_W(t'e_j)$ implies $te_i >_\sigma t'e_j$ for all $t,t' \in \mathbb{T}^n$ and all $i,j \in \{1,\dots,r\}$.

In the case of the standard grading, i.e. for $W = (1\ 1\ \cdots\ 1)$, this definition agrees with Definition 1.4.9. The typical situation in which we have a degree compatible monoid ordering is described in the following example.

Example 4.2.2. Suppose that $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ has rank m. If we choose a matrix $W' \in \mathrm{Mat}_{n-m,n}(\mathbb{Z})$ such that $V = \binom{W}{W'}$ is non-singular, then the monoid ordering $\sigma = \mathtt{Ord}(V)$ is compatible with $\deg_W$.

Proposition 4.2.3. *Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of rank m, and let $\mathbb{T}^n\langle e_1,\dots,e_r\rangle$ be the set of terms in F. The following conditions are equivalent.*

a) The first non-zero element in each non-zero column of W is positive.
b) For $i = 1,\dots,n$, we have $\deg_W(x_i) \geq_{\mathtt{Lex}} 0$.
c) The restriction of $\mathtt{Lex}$ to the monoid $\Gamma = \{d \in \mathbb{Z}^m \mid P_{W,d} \neq 0\}$ is a well-ordering.
d) The restriction of $\mathtt{Lex}$ to the monoid $\Gamma = \{d \in \mathbb{Z}^m \mid P_{W,d} \neq 0\}$ is a term ordering.
e) There exists a term ordering τ on $\mathbb{T}^n$ which is compatible with $\deg_W$.
f) There exists a module term ordering σ on $\mathbb{T}^n\langle e_1,\dots,e_r\rangle$ which is compatible with $\deg_W$.

Proof. Conditions a) and b) are clearly equivalent. Next we prove "a)⇒c)". Since the rank of W is m, there are standard basis vectors $e_{i_1},\dots,e_{i_{n-m}}$ which we can add as new rows to W such that the resulting matrix V is non-singular. Hence every column of V has a non-zero entry, and the first non-zero entry is positive. By Proposition 1.4.12, the monoid ordering $\sigma = \mathtt{Ord}(V)$ is a term ordering, and by construction it is compatible with $\deg_W$. It follows that there is no infinite decreasing sequence of terms $t_1 >_\sigma t_2 >_\sigma \cdots$. Since every element of Γ is the degree of a term and since σ is degree compatible, every decreasing chain in Γ is eventually stationary. Now the claim follows from Proposition 1.4.18.

The implication "c)⇒d)" follows from the last part of that proposition, and the implication "d)⇒b)" follows from the definition of a term ordering. Now we prove "a)⇒e)". As above, we choose standard basis vectors $e_{i_1},\dots,e_{i_{n-m}} \in \mathbb{Z}^n$ and append them as new rows to W such that the resulting matrix $V \in \mathrm{Mat}_n(\mathbb{Z})$ is non-singular. Then the term ordering $\sigma = \mathtt{Ord}(V)$ is compatible with $\deg_W$.

In order to show "e)⇒f)", we define an ordering σ on $\mathbb{T}^n\langle e_1,\dots,e_r\rangle$ in the following way. Given $te_i, t'e_j \in \mathbb{T}^n\langle e_1,\dots,e_r\rangle$, we let $te_i \geq_\sigma t'e_j$ if $\deg_W(te_i) >_{\mathtt{Lex}} \deg_W(t'e_j)$, or if $\deg_W(te_i) = \deg_W(t'e_j)$ and $i < j$, or if $\deg_W(te_i) = \deg_W(t'e_j)$ and $i = j$ and $t \geq_\tau t'$. It is easy to check that σ is a module ordering. We note that $te_i \geq_\sigma t'e_i$ if and only if $t \geq_\tau t'$, i.e. inside every component of F the ordering σ is induced by τ. Thus we see that $te_i \geq_\sigma e_i$ for all $t \in \mathbb{T}^n$ and all $i \in \{1,\dots,r\}$. Hence σ is a module term ordering. By construction, σ is degree compatible.

Finally we prove "f)⇒b)". For $i = 1,\dots,n$, we have $x_ie_1 >_\sigma e_1$, and therefore $\deg_W(x_ie_1) = \deg_W(x_i) + \deg_W(e_1) \geq_{\mathtt{Lex}} \deg_W(e_1)$. Consequently, we have $\deg_W(x_i) \geq_{\mathtt{Lex}} 0$ for $i = 1,\dots,n$. □

As we shall see, gradings by matrices which satisfy the conditions of this proposition are very useful in a number of ways. For this reason we introduce the following notions.

Definition 4.2.4. Let $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ be a matrix of rank m.

a) The grading on P defined by W is called **non-negative** if the first non-zero element in each non-zero column of W is positive. In this case, we shall also say that W is a non-negative matrix.
b) The grading on P defined by W is called **positive** if no column of W is zero and the first non-zero element in each column is positive. In this case, we shall also say that W is a positive matrix.

Thus the above proposition implies that, if W defines a non-negative grading defined by W, there exists a term ordering on $\mathbb{T}^n$ which is compatible with $\deg_W$. Notice also that if W is positive, then we have $\deg_W(x_i) >_{\mathtt{Lex}} 0$ for $i = 1,\dots,n$, and hence $P_+ = \bigoplus_{d>_{\mathtt{Lex}}0} P_{W,d} = (x_1,\dots,x_n)$. The following corollary shows that in a finitely generated graded P-module there exists no infinite decreasing chain $\deg_W(v_1) >_{\mathtt{Lex}} \deg_W(v_2) >_{\mathtt{Lex}} \cdots$ if the grading defined by W is non-negative.

Corollary 4.2.5. *Assume that $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ defines a non-negative grading on P. Let M be a finitely generated, graded P-module, and let Σ be the set $\{d \in \mathbb{Z}^m \mid M_{W,d} \neq 0\}$. Then the relation $\mathtt{Lex}|_\Sigma$ is a well-ordering.*

Proof. By applying Remark 4.1.13 to a finite homogeneous system of generators of M, we construct a surjective homomorphism of graded P-modules of the form $\bigoplus_{i=1}^r P(-\delta_i) \longrightarrow M$. Now the claim follows from Proposition 4.2.3.c, because we have $\Sigma \subseteq \cup_{i=1}^r(\Gamma + \delta_i)$. □

Our next corollary shows that non-negative gradings are of non-negative type and positive gradings are of positive type, as their names suggests.

Corollary 4.2.6. *Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$.*

a) If the grading defined by W is non-negative, it is of non-negative type.

b) If the grading defined by W is positive, it is of positive type.

Proof. To prove claim a), we let C_i denote for $i = 1, \ldots, m$ the set of all indices $j \in \{1, \ldots, n\}$ such that the j^{th} column of W has its first non-zero entry in the i^{th} row. If we add high enough multiples of the first row to the rows below, the resulting matrix has strictly positive entries in the columns indexed by C_1. In particular, the second row of this matrix has strictly positive entries in the columns indexed by $C_1 \cup C_2$, and if we add high enough multiples of that row to the rows below, rows $2, 3, \ldots, m$ of the resulting matrix have strictly positive entries in the columns indexed by $C_1 \cup C_2$. Continuing this way, we finally arrive at a matrix whose last row has strictly positive entries in columns $C_1 \cup \cdots \cup C_m$, i.e. in all non-zero columns. Claim b) follows in the same way, except that there are no zero columns in W, so that the last row of the final matrix has positive entries everywhere. □

The converse implications are not true, since for instance the grading on $K[x]$ given by $W = (-1)$ is of positive type, but not positive. However, the following remark says that there exists a change of grading which transforms a grading of non-negative (resp. positive) type into a non-negative (resp. positive) one.

Remark 4.2.7. Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$.

a) If the grading defined by W is of non-negative type, then there exists a non-singular matrix $V \in \mathrm{Mat}_m(\mathbb{Z})$ such that the grading defined by the matrix $W' = V \cdot W$ is non-negative and $P_{W',V\cdot d} = P_{W,d}$ for all $d \in \mathbb{Z}^m$.

b) Similarly, if the grading defined by W is of positive type, then there exists a non-singular matrix $V \in \mathrm{Mat}_m(\mathbb{Z})$ such that the grading defined by the matrix $W' = V \cdot W$ is positive and $P_{W',V\cdot d} = P_{W,d}$ for all $d \in \mathbb{Z}^m$.

These observations follow from Propositions 4.1.18 and 4.1.9.b. Let us order the degrees of homogeneous polynomials with respect to the grading given by W' using the ordering $d \geq_\tau d' \iff W' \cdot d \geq_{\mathtt{Lex}} W' \cdot d'$ introduced in the proof of Proposition 4.1.21.a. Then the isomorphism of graded rings $(\mathrm{id}_P, \psi) : (P, \mathbb{Z}^m) \longrightarrow (P, \mathbb{Z}^m)$, where ψ is the map defined by W', is compatible with the ordering of the degrees.

4.2.B Macaulay Bases

As in the first subsection, we let $P = K[x_1, \ldots, x_n]$ be graded by the matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and we let M be a non-zero P-submodule of the graded free P-module $F = \bigoplus_{i=1}^{r} P(-\delta_i)$. But, unless stated otherwise, we do not assume anymore that M is a *graded* submodule of F. In Definition 4.1.6, we introduced the concept of degree of a homogeneous element of P. Now we extend this notion as follows.

Definition 4.2.8. Let v be a non-zero vector in M and $v = v_{d_1} + \cdots + v_{d_s}$ its decomposition into homogeneous components, where v_{d_i} has degree $d_i \in \mathbb{Z}^m$ for $i = 1, \ldots, s$. Without loss of generality, we may assume that we have $d_1 >_{\mathtt{Lex}} \cdots >_{\mathtt{Lex}} d_s$.

a) The vector $\deg_W(v) = d_1 \in \mathbb{Z}^m$ is called the **degree** of v with respect to the grading given by W. If it is clear which grading we are considering, we shall also write $\deg(v)$.
b) The vector $\mathrm{DF}_W(v) = v_{d_1}$ is called the **degree form** of v with respect to the grading given by W. For the zero vector, we define $\mathrm{DF}_W(0) = 0$.

In the case $r = 1$, $\delta_1 = 0$, and $W = (1\ 1\ \ldots\ 1)$, i.e. if we equip P with the standard grading, this definition of the degree of a polynomial and of its degree form agrees with the usual one. Moreover, degree forms generalize leading terms in the following sense.

Remark 4.2.9. Let $W \in \mathrm{Mat}_n(\mathbb{Z})$ be a non-singular matrix which defines a positive grading. Then $\sigma = \mathtt{Ord}(W)$ is a term ordering on $\mathbb{T}^n$ by Proposition 1.4.12. Given a non-zero polynomial $f \in P$, we have $\mathrm{DF}_W(f) = \mathrm{LT}_\sigma(f)$.

It is also instructive to compare the current situation with the definition of σ-degrees and σ-leading forms in Section 2.3.

Remark 4.2.10. In the situation of Section 2.3, consider the case of an ideal $M \subseteq P$. In this case we defined a $\mathbb{T}^n$-grading on the module P^s which was induced by a system of generators $\{g_1, \ldots, g_s\}$ of M (see Proposition 2.3.3). By using the injective map $\log : \mathbb{T}^n \longrightarrow \mathbb{Z}^n$ and by letting $\gamma_i = \log(\mathrm{LT}_\sigma(g_i))$ for $i = 1, \ldots, s$, we can see that this $\mathbb{T}^n$-grading corresponds exactly to the $\mathbb{Z}^n$-grading on $\bigoplus_{i=1}^s P(-\gamma_i)$ defined by the identity matrix.

Let us illustrate the concepts of degrees and degree forms with some examples.

Example 4.2.11. Let $P = K[x_1, x_2, x_3]$.

a) If we equip P with the grading defined by $W = (1\ 2\ 1)$, then the polynomial $f = x_1^3 - x_1x_2 + x_1$ has degree $\deg_W(f) = 3$. More precisely, it has two homogeneous components $f = f_3 + f_1$, where $\mathrm{DF}_W(f) = f_3 = x_1^3 - x_1x_2$ is the degree form of f and $f_1 = x_1$ has degree one.
b) Now we equip P with the grading defined by $W = (-1\ -1\ -1)$. In this case the same polynomial $f = x_1^3 - x_1x_2 + x_1$ has degree -1 and three homogeneous components f_{-1}, f_{-2}, f_{-3}, where $\mathrm{DF}_W(f) = f_{-1} = x_1$, where $f_{-2} = -x_1x_2 \in P_{-2}$, and where $f_{-3} = x_1^3 \in P_{-3}$.
c) Finally, we equip P with the grading defined by $W = \left(\begin{smallmatrix} 1 & 2 & 4 \\ 2 & 1 & 3 \end{smallmatrix}\right)$ and consider the polynomial $g = x_1^2x_2^5 - x_3^3 + x_1^3x_3^2$. It has two homogeneous components $g = g_{(12,9)} + g_{(11,12)}$, where $g_{(12,9)} = x_1^2x_2^5 - x_3^3 \in P_{(12,9)}$ and $g_{(11,12)} = x_1^3x_3^2 \in P_{(11,12)}$. Notice that $(12, 9) >_{\mathtt{Lex}} (11, 12)$. Thus we have $\mathrm{DF}_W(g) = x_1^2x_2^5 - x_3^3$ and $\deg_W(g) = (12, 9)$.

Our next remark collects some useful rules for computing with degree forms. Their proofs are straightforward and proceed exactly as the proofs of the corresponding rules for leading terms (see Proposition 1.5.3).

Remark 4.2.12. Let $v_1, v_2 \in M \setminus \{0\}$, and let $f \in P$.

a) If $\deg_W(v_1) = \deg_W(v_2)$ and $\mathrm{DF}_W(v_1) \neq -\mathrm{DF}_W(v_2)$, then we have $\mathrm{DF}_W(v_1 + v_2) = \mathrm{DF}_W(v_1) + \mathrm{DF}_W(v_2)$.
b) If $\deg_W(v_1) >_{\mathtt{Lex}} \deg_W(v_2)$, then we have $\mathrm{DF}_W(v_1 + v_2) = \mathrm{DF}_W(v_1)$.
c) We have $\mathrm{DF}_W(fv_1) = \mathrm{DF}_W(f) \cdot \mathrm{DF}_W(v_1)$.

To develop the theory of degree forms further, we now introduce the analogs of leading term ideals and Gröbner bases.

Definition 4.2.13. Let M be a submodule of the graded free P-module F.

a) The graded P-submodule $\mathrm{DF}_W(M) = \langle \mathrm{DF}_W(v) \mid v \in M \rangle$ of F is called the **degree form module** of M with respect to the grading given by W.

b) A set $\{v_1, \ldots, v_s\} \subseteq M$ is called a **Macaulay basis** of M with respect to the grading given by W if we have $\mathrm{DF}_W(M) = \langle \mathrm{DF}_W(v_1), \ldots, \mathrm{DF}_W(v_s) \rangle$.

In the literature, Macaulay bases are also called **H-bases**. Under the hypotheses of Remark 4.2.9, a Macaulay basis with respect to the grading given by W is nothing but a Gröbner basis with respect to $\mathtt{Ord}(W)$. More generally, given a suitable partial ordering on the set of degrees of the elements of M, one can define Macaulay bases with respect to this partial ordering. We invite you to explore this notion further in Tutorial 47. Continuing the analogy between Macaulay bases and Gröbner bases, we now imitate Proposition 2.4.3.a and show that a Macaulay basis is additionally a system of generators of M under suitable hypotheses.

Proposition 4.2.14. *Let P be non-negatively graded by the matrix W, and let $\{v_1, \ldots, v_s\}$ be a Macaulay basis of M. Then the set $\{v_1, \ldots, v_s\}$ is a system of generators of M.*

Proof. Without loss of generality, we may assume $v_i \neq 0$ for $i = 1, \ldots, s$. Suppose that the claim is false, i.e. that $\langle v_1, \ldots, v_s \rangle \subset M$. Since the grading is non-negative, the restriction of $\mathtt{Lex}$ to $\Sigma = \{d \in \mathbb{Z}^m \mid F_{W,d} \neq 0\}$ is a well-ordering by Corollary 4.2.5. So, there is an element $v \in M \setminus \langle v_1, \ldots, v_s \rangle$ such that $d = \deg_W(v)$ is minimal. Using Corollary 1.7.11, we can write $\mathrm{DF}_W(v) = f_1 \mathrm{DF}_W(v_1) + \cdots + f_s \mathrm{DF}_W(v_s)$, where f_i is a homogeneous polynomial of degree $\deg_W(f_i) = d - \deg_W(v_i)$ for $i = 1, \ldots, s$. Now the rules given in Remark 4.2.12 show that $\deg_W(v - f_1 v_1 - \cdots - f_s v_s) <_{\mathtt{Lex}} d$. Because of the minimality of d, this implies that there are polynomials $g_1, \ldots, g_s$ such that $v - f_1 v_1 - \cdots - f_s v_s = g_1 v_1 + \cdots + g_s v_s$. This representation contradicts the supposition that $v \notin M$ and finishes the proof. □

The conclusion of this proposition obviously holds if W is positive, but it need not hold if W is of positive type (see Exercise 5). Degree compatible term orderings allow us to connect the two notions of Gröbner basis and Macaulay basis. Recall that, by Proposition 4.2.3, a degree compatible term ordering exists if and only if P is non-negatively graded by W.

Proposition 4.2.15. *Let the polynomial ring P be non-negatively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let σ be a term ordering which is compatible with $\deg_W$, and let $G = \{g_1, \ldots, g_s\}$ be a σ-Gröbner basis of M.*

a) The set $\{\mathrm{DF}_W(g_1), \ldots, \mathrm{DF}_W(g_s)\}$ is a σ-Gröbner basis of $\mathrm{DF}_W(M)$.
b) The set G is a Macaulay basis of M with respect to W.

Proof. First we prove a). Let $v \in M \setminus \{0\}$. Since σ is degree compatible, the term $\mathrm{LT}_\sigma(v)$ has to be one of the terms in $\mathrm{Supp}(\mathrm{DF}_W(v))$. Therefore we have $\mathrm{LT}_\sigma(v) = \mathrm{LT}_\sigma(\mathrm{DF}_W(v))$. By assumption, $\mathrm{LT}_\sigma(v)$ is a multiple of $\mathrm{LT}_\sigma(g_j)$ for some $j \in \{1, \ldots, s\}$. This shows a), and b) is an immediate consequence of a) and Proposition 2.4.3.a. □

The converse of part b) of this proposition is not true in general (see Exercise 6). A common situation in which we can apply b) is given by Example 4.2.2. In fact, we can use this idea to compute Macaulay bases effectively as follows.

Corollary 4.2.16. (Computation of Macaulay Bases)
Let P be non-negatively graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let M be a P-submodule of F. Consider the following sequence of instructions.

1) Choose a matrix $W' \in \mathrm{Mat}_{n-m,n}(\mathbb{N})$ such that $V = \binom{W}{W'}$ is non-singular and positive.
2) Using Buchberger's Algorithm 2.5.5, compute a Gröbner basis G of M with respect to the term ordering $\mathtt{Ord}(V)$.
3) Return the result G.

This is an algorithm which computes a Macaulay basis G of M with respect to the grading given by W.

Proof. Clearly, we may assume that $M \neq 0$. By Proposition 4.2.3, a matrix W' as required in step 1) exists. By Proposition 1.4.12, the monoid ordering $\sigma = \mathtt{Ord}(V)$ is then a term ordering. Hence Buchberger's Algorithm can be used to compute a σ-Gröbner basis of M. By the proposition, this Gröbner basis is a Macaulay basis of M with respect to the grading given by W. □

There are several ways to perform step 1) of this algorithm. One possibility is to choose suitable standard basis vectors (see Exercise 9).

Exercise 1. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, and let $F = \bigoplus_{i=1}^{r} P(-\delta_i)$. Show that the grading given by W is non-negative if and only if the restriction of `Lex` to the set $\Sigma = \{d \in \mathbb{Z}^m \mid F_{W,d} \neq 0\}$ is a well-ordering.

Exercise 2. Let K be a field, and let $P = K[x_1, \ldots, x_n]$ be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. Give an alternative proof of Corollary 4.2.6.a using induction on m.

Exercise 3. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let I be a non-zero principal ideal in P. Show that $\mathrm{DF}_W(I)$ is generated by the degree form of a generator of I.

Exercise 4. In the following cases, try to find a non-zero matrix $W \in \mathrm{Mat}_{1,3}(\mathbb{Z})$ such that the support of the degree form of the following polynomials contains as many terms as possible.

a) $f_1 = x_1^3 - x_2x_3 + x_1$
b) $f_2 = x_1^2x_2^5 - x_3^3 + x_1^3x_3^2$
c) $f_3 = x_1^3 + x_2^3 + x_3^3 - x_1^2x_2^2x_3^2$

Exercise 5. Let us equip the polynomial ring $P = K[x]$ over a field K with the $\mathbb{Z}^2$-grading defined by $W = \binom{-1}{1}$. Prove that $x - x^2$ is a Macaulay basis of the ideal (x) which does not generate that ideal.

Exercise 6. Let us equip the polynomial ring $P = K[x, y]$ over a field K with the standard grading. Show that $\{x^2 - y^2, xy\}$ is a Macaulay basis of the ideal $(x^2 - y^2, xy)$, but not a Gröbner basis with respect to any term ordering.

Exercise 7. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let $f \in P \setminus \{0\}$.

a) Show that if $\mathrm{DF}_W(f)$ is irreducible then f is irreducible.
b) Show that the converse is not true in general.
c) Let $f = x_1^2 + g(x_2, \ldots, x_n)$. Show that, up to units, f has at most two irreducible factors.

Exercise 8. Let K be a field, and let $P = K[x_1, \ldots, x_n]$ be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type.

a) Show that there exists a non-singular matrix $U \in \mathrm{Mat}_m(\mathbb{Z})$ such that $U \cdot W$ defines a positive grading on P and such that (id_P, φ), where $\varphi : \mathbb{Z}^m \longrightarrow \mathbb{Z}^m$ is defined by U, is an isomorphism of graded rings.
b) Find an example where such an isomorphism does not preserve Macaulay bases.

Exercise 9. Let $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ be a matrix of rank m. Show that one can choose $n - m$ standard basis vectors $e_{i_1}, \ldots, e_{i_{n-m}}$ such that the matrix

$$V = \begin{pmatrix} W \\ e_{i_1} \\ \vdots \\ e_{i_{n-m}} \end{pmatrix}$$

is non-singular. Moreover, show that the matrix V is positive if W is non-negative.

Tutorial 47: Computation of Macaulay Bases

Computers are useless.
They can only give you answers.
(Pablo Picasso)

In this tutorial we invite you to explore the notion of a Macaulay basis further. Be prepared to work by doing both some thinking and some programming. Let us start with a little programming.

a) Let $P = \mathbb{Q}[x_1, \ldots, x_n]$ be non-negatively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. Write a CoCoA function `CompatibleTO(...)` which takes W and computes a matrix $V \in \mathrm{Mat}_n(\mathbb{Z})$ of the kind required by step 1) of the algorithm in Corollary 4.2.16. (*Hint:* You may want to solve Exercise 9 first.)
b) In the setting of a), let I be an ideal of P which is homogeneous with respect to the grading given by W. Implement a CoCoA function `MacaulayBasis(...)` which computes a Macaulay basis of I with respect to this grading.

Switching to the thinking part, we shall now generalize Macaulay bases by using partial monoid orderings on $\mathbb{T}^n$. They are defined as follows. A relation π on a monoid $(\Gamma, \circ)$ is called a **partial monoid ordering** if the following conditions are satisfied for all $\gamma_1, \gamma_2, \gamma_3 \in \Gamma$.

1) $\gamma_1 \geq_\pi \gamma_1$ (reflexivity)
2) $\gamma_1 \geq_\pi \gamma_2$ and $\gamma_2 \geq_\pi \gamma_3$ imply $\gamma_1 \geq_\pi \gamma_3$ (transitivity)
3) $\gamma_1 \geq_\pi \gamma_2$ implies $\gamma_1 \circ \gamma_3 \geq_\pi \gamma_2 \circ \gamma_3$

Now it is time for you to start working again.

c) Compare this definition to the definition of a monoid ordering in 1.4.1. For each of the additional properties in Definition 1.4.1, find a partial monoid ordering which has this property but not the others.
Hint: Use $\Gamma = \mathbb{T}^1$ and $\Gamma = \mathbb{T}^1 \cup \{\infty\}$.

Next we choose $m \in \{1, \ldots, n\}$, let $v_1, \ldots, v_m \in \mathbb{R}^n$ be $\mathbb{R}$-linearly independent vectors, and define $V \in \mathrm{Mat}_{m,n}(\mathbb{R})$ to be the matrix with rows $v_1, \ldots, v_m$. For two terms $t_1, t_2 \in \mathbb{T}^n$, we set $t_1 \geq_{\mathtt{Ord}(V)} t_2$ if and only if $V \cdot (\log(t_1) - \log(t_2)) \geq_{\mathtt{Lex}} 0$. Now back to work!

d) Prove that $\mathtt{Ord}(V)$ is a partial monoid ordering on $\mathbb{T}^n$. It is called the **partial ordering represented by** V.
e) Consider the matrix $U = (1\ \sqrt{2}\ \sqrt{2}) \in \mathrm{Mat}_{1,3}(\mathbb{R})$. Write a CoCoA function `CompareOrdU(...)` which takes two terms $t_1, t_2 \in \mathbb{T}^3$ and returns the Boolean value corresponding to $t_1 \geq_{\mathtt{Ord}(U)} t_2$.
f) Show that there do not exist $m \geq 1$ and $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ such that $\mathtt{Ord}(U)$ is the lexicographic ordering on the degrees of the terms in $\mathbb{T}^3$ with respect to the grading given by W.
g) Find a number $m \geq 1$ and a matrix $W \in \mathrm{Mat}_{m,3}(\mathbb{R})$ such that $\mathtt{Ord}(W)$ is a term ordering which refines the partial ordering represented by U.

h) Implement a CoCoA program `CompareOrdW(...)` which takes two terms $t_1, t_2 \in \mathbb{T}^3$ and returns the Boolean value corresponding to $t_1 \geq_{\mathtt{Ord}(W)} t_2$.

At this point we can continue to generalize the definitions given in the text. Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let $V \in \mathrm{Mat}_{m,n}(\mathbb{R})$ be a matrix as above. Given a non-zero polynomial $f \in P$, we write $f = c_1 t_1 + \cdots + c_s t_s$ with $c_1, \ldots, c_s \in K \setminus \{0\}$ and $t_1, \ldots, t_s \in \mathbb{T}^n$. Without loss of generality we may assume that $t_1 \geq_{\mathtt{Ord}(V)} t_2 \geq_{\mathtt{Ord}(V)} \cdots \geq_{\mathtt{Ord}(V)} t_s$. Then the polynomial

$$\mathrm{DF}_V(f) = c_1 t_1 + \cdots + c_j t_j \qquad \text{where} \qquad j = \max\{i \mid t_i \geq_{\mathtt{Ord}(V)} t_1\}$$

is called the **degree form** of f with respect to the partial ordering $\mathtt{Ord}(V)$. Furthermore, we define the degree form ideal $\mathrm{DF}_V(I)$ and a Macaulay basis with respect to $\mathtt{Ord}(V)$ of an ideal $I \subseteq P$ as in the text.

i) Prove that we have $t \geq_{\mathtt{Ord}(V)} 1$ for every term $t \in \mathbb{T}^n$ if and only if the first non-zero entry in each non-zero column of V is positive. In this case, we shall say that $\mathtt{Ord}(V)$ is a **non-negative partial ordering**.

j) Generalize Proposition 4.2.14 in the following way. Suppose that $\mathtt{Ord}(V)$ is a non-negative partial ordering and $\{f_1, \ldots, f_s\}$ is a Macaulay basis of an ideal $I \subseteq P$ with respect to $\mathtt{Ord}(V)$. Then $\{f_1, \ldots, f_s\}$ generates I.

k) Let $\mathtt{Ord}(V)$ be a non-negative partial ordering on $\mathbb{T}^n$. Generalize the algorithm of Corollary 4.2.16 to an algorithm which computes a Macaulay basis of a given ideal I in P with respect to $\mathtt{Ord}(V)$.
Hint: Complete V to a non-singular matrix in $\mathrm{Mat}_n(\mathbb{R})$ in order to find a term ordering which is compatible with $\mathtt{Ord}(V)$.

l) Write a CoCoA program `GenMacBasis(...)` which implements this generalized algorithm in the case of the non-negative partial ordering given by $U = (1\ \sqrt{2}\ \sqrt{2})$.
Hint: Use the function written in part h) above. You will need to reimplement Buchberger's Algorithm 2.5.5 for the term ordering represented by this function.

Tutorial 48: Characterizations of Macaulay Bases

As we shall see in this tutorial, it is possible to define Macaulay bases in a very general setting, namely for submodules of Γ-graded free R-modules, at the level of generality we introduced in Section 1.7. We shall show that such general Macaulay bases enjoy properties analogous to the ones we used to characterize Gröbner bases (see Theorem 2.4.1). In fact, these Macaulay bases can be considered as generalizations of Gröbner bases.

Let Γ be a commutative monoid obeying the cancellation law and for which there exists a term ordering σ on Γ. Let R be a Γ-graded ring, let $\gamma_1, \ldots, \gamma_r \in \Gamma$, let $F = \bigoplus_{i=1}^{r} R(\gamma_i)$ be a Γ-graded free R-module, and

let M be an R-submodule of F. Every element $v \in M \setminus \{0\}$ has a unique decomposition $v = v_1 + \cdots + v_s$, where $v_1, \ldots, v_s$ are homogeneous and $\deg(v_1) >_\sigma \deg(v_2) >_\sigma \cdots >_\sigma \deg(v_s)$.

In this situation, we call $\mathrm{DF}_\Gamma(v) = v_1$ the **degree form** of v with respect to the Γ-grading on F. For $v = 0$, we set $\mathrm{DF}_\Gamma(v) = 0$. Then the Γ-graded submodule $\mathrm{DF}_\Gamma(M) = \langle \mathrm{DF}_\Gamma(m) \mid m \in M \rangle$ of F is called the **degree form module** of M. A set of elements $\{m_1, \ldots, m_t\} \subseteq M$ is called a **Macaulay basis** of M with respect to the Γ-grading on F if $\mathrm{DF}_\Gamma(M) = \langle \mathrm{DF}_\Gamma(m_1), \ldots, \mathrm{DF}_\Gamma(m_t) \rangle$.

a) Explain how the situation described at the beginning of the section and Definitions 4.2.8 and 4.2.13 are special cases of the above assumptions and definitions.

b) Imitate the proof of Proposition 4.2.14 to show that every Macaulay basis of M is a system of generators of M.

c) Prove that $\{m_1, \ldots, m_t\} \subseteq M$ is a Macaulay basis of M if and only if every element $v \in M \setminus \{0\}$ has a representation $v = \sum_{i=1}^t f_i m_i$ such that $f_1, \ldots, f_t \in R$ and $\deg(v) = \max_\sigma\{\deg(f_i m_i) \mid i \in \{1, \ldots, t\},\ f_i m_i \neq 0\}$. *Hint:* Proceed as in the proof of Proposition 2.1.3.

d) Let $\mathcal{M}$ be the tuple $(m_1, \ldots, m_t)$, and let $v, w \in M$. We write $v \xrightarrow{\mathcal{M}} w$ if there exist $f_1, \ldots, f_t \in R$ such that $v = w + \sum_{i=1}^t f_i m_i$, and such that $\deg(w) <_\sigma \deg(v)$ or $w = 0$. The reflexive, transitive closure of $\xrightarrow{\mathcal{M}}$ is denoted again by $\xrightarrow{\mathcal{M}}$. Show that the following conditions are equivalent.

   1) The elements of $\mathcal{M}$ are a Macaulay basis of M.
   2) For an element $v \in F$, we have $v \xrightarrow{\mathcal{M}} 0$ if and only if $v \in M$.
   3) If $v \in M$ is irreducible with respect to $\xrightarrow{\mathcal{M}}$, then we have $v = 0$.
   4) For every $v \in F$, there exists a unique $w \in M$ such that $v \xrightarrow{\mathcal{M}} w$ and such that w is irreducible with respect to $\xrightarrow{\mathcal{M}}$.
   5) The relation $\xrightarrow{\mathcal{M}}$ on F is confluent.

   Hint: Imitate the proofs of Propositions 2.2.5 and 2.2.8.

e) Prove that the conditions of d) are also equivalent to $\sum_{i=1}^t f_i m_i \xrightarrow{\mathcal{M}} 0$ for all $(f_1, \ldots, f_t) \in \mathrm{Syz}_R(\mathrm{DF}_\Gamma(\mathcal{M}))$. (*Hint:* Use the method of the proof of Proposition 2.3.12.)

f) Show that it suffices to check the condition of e) for a system of generators of $\mathrm{Syz}_R(\mathrm{DF}_\Gamma(\mathcal{M}))$.

g) Explain how one can use the preceding results to characterize Macaulay bases by a suitable criterion for the lifting of syzygies.

h) Show that Gröbner bases are a special case of the general kind of Macaulay bases considered here. Then use the results you proved above to generalize Theorem 2.4.1 accordingly.

4.3 Homogenization

The real world is a special case.
(Anonymous)

Throughout this chapter, we examine gradings on polynomial rings and study some of their applications. For instance, we shall see that many algorithms can be improved if we know beforehand that the input polynomials are homogeneous. But unfortunately not every polynomial occurring in the real world is homogeneous. Therefore we would like somehow to approximate a non-homogeneous polynomial by a homogeneous one. How can we view an arbitrary polynomial as a special case of something homogeneous?

First, let us search for a solution in an easy case. Let $P = \mathbb{Q}[x_1, x_2, x_3]$ be standard graded and $f = x_1^2 + x_2^5 x_3$. The first term in the support of f has degree 2 and the second term has degree 6. In order to view f as a special case of a homogeneous polynomial, we introduce a new indeterminate y_1 and form $F = y_1^4 x_1^2 + x_2^5 x_3$. Then F is a homogeneous polynomial in the standard graded ring $\overline{P} = \mathbb{Q}[y_1, x_1, x_2, x_3]$ and we can recreate f by plugging $y_1 = 1$ into F. In this sense, we can say that this process of *homogenization* allows us to regard arbitrary real-world polynomials as special cases of homogeneous ones. Notice that we would not have had to do anything if f had been homogeneous to start with.

A natural question is whether we can extend everything to the $\mathbb{Z}^m$-graded situation. For the moment, let us study the general case by means of an example. Let $P = \mathbb{Q}[x_1, x_2, x_3]$ be graded by $W = \left(\begin{smallmatrix} 2 & 1 & 1 \\ 1 & 0 & 1 \end{smallmatrix}\right)$. Again the polynomial $f = x_1^2 + x_2^5 x_3$ is not homogeneous, since $\deg_W(x_1^2) = (4, 2)$, while $\deg_W(x_2^5 x_3) = (6, 1)$. The degree form of f is $\mathrm{DF}_W(f) = x_2^5 x_3$. First we consider the upper row of weights. By introducing a new indeterminate y_1 of degree one, we may homogenize f with respect to this row by forming $y_1^2 x_1^2 + x_2^5 x_3$. But then there is no way to endow y_1 with a second integer degree such that $y_1^2 x_1^2 + x_2^5 x_3$ becomes homogeneous with respect to the lower row of weights. What we have to do is introduce another indeterminate y_2 and then set $\deg_W(y_1) = (1, 0)$ and $\deg_W(y_2) = (0, 1)$. Then the polynomial $y_1^2 x_1^2 + y_2 x_2^5 x_3$ is the *homogenization* of f.

This approach works quite generally, and the usual homogenization for standard gradings (occurring most frequently in real life) is a special case. Thus the section starts by providing all the necessary rules for dealing with the processes of homogenizing and dehomogenizing polynomials. Then we really get going and play the same game with ideals. Again we provide the good rules for the interaction between homogenization and ideal-theoretic operations (see Propositions 4.3.5, 4.3.10 and 4.3.12) and point out a few bad ones (see Examples 4.3.9 and 4.3.11). As an application, we see that we can compute homogenizations using saturation with respect to the product of the homogenizing indeterminates, an operation we have mastered in Section 3.5. A further application is discussed in Tutorial 51, where we suggest an efficient method for computing the homogenization of implicitization ideals.

In the last part of the first subsection we examine the behaviour of Gröbner bases of ideals under dehomogenization. For this purpose we have to relate a term ordering on the monoid $\mathbb{T}(x_1, \ldots, x_n)$ to a term ordering on the monoid $\mathbb{T}(y_1, \ldots, y_m, x_1, \ldots, x_n)$. After doing this in the correct way in Definition 4.3.13, we can then show that Gröbner bases dehomogenize in a natural way (see Proposition 4.3.18).

What about homogenizing Macaulay bases and Gröbner bases? Since there are some problems in the general case, we assume in Subsection 4.3.B that $P = K[x_1, \ldots, x_n]$ is positively $\mathbb{Z}$-graded. Then we continue our investigation by studying the effect of homogenization on Macaulay bases. We characterize Macaulay bases as those systems of generators of an ideal I whose homogenizations generate the homogenization of I. This is not generally true for $m \geq 2$ (see Exercises 8 and 9), but for $m = 1$ it yields an alternative way of computing the homogenization of an ideal (see Corollary 4.3.20). Moreover, we show that Gröbner bases homogenize in the natural way (see Proposition 4.3.21).

The final topic in this section has a more geometric flavour. Given an ideal I in P, the rings P/I and $P/\operatorname{DF}_W(I)$ are shown to be members of a family of rings which is *flat*. Although we do not define this concept here, we show how this family is constructed using the homogenization of I, and that it has good properties. For instance, it turns out that Macaulay bases are characterized by the property that they generate the defining ideal of each fiber of the family (see Proposition 4.3.23). Again these results require a positive grading with $m = 1$ (see Exercise 11).

Should we shed more light on these intricacies? On a fortune cookie we read that "a good example is the best gift we can bestow on others". Therefore we conclude the section with some elementary examples which cast a few rays of illumination into the vast areas of flat families, deformations, and Hilbert functions. In due course, we shall revisit some of them.

What about homogenization of modules? Haven't we been stressing the need to concentrate on modules all along? Well, yes, but... in this section we prefer to leave the job to you, in Tutorial 49. Finally, we mention that there is another nice geometric interpretation of the operation of homogenizing a polynomial ideal. It is related to the process of forming the projective closure of an affine variety. In Tutorial 52 we invite you to explore this interpretation by following our guided tour.

4.3.A Homogenization of Polynomials and Ideals

Let K be a field and $P = K[x_1, \ldots, x_n]$ a polynomial ring over K which is graded by a matrix $W \in \operatorname{Mat}_{m,n}(\mathbb{Z})$ of rank $m \geq 1$. In this situation we choose new indeterminates $y_1, \ldots, y_m$ and call them **homogenizing indeterminates**. Then we equip the ring $\overline{P} = K[y_1, \ldots, y_m, x_1, \ldots, x_n]$ with

the grading defined by the matrix $\overline{W} = (\mathcal{I}_m \mid W)$, where $\mathcal{I}_m$ denotes the identity matrix of size m.

Clearly, the map $(\imath, \mathrm{id}_{\mathbb{Z}^m}) : (P, \mathbb{Z}^m) \hookrightarrow (\overline{P}, \mathbb{Z}^m)$, where $\imath$ is the inclusion and $\mathrm{id}_{\mathbb{Z}^m}$ is the identity, is a homomorphism of $\mathbb{Z}^m$-graded rings. The processes of homogenizing and dehomogenizing a polynomial are now defined as follows.

Definition 4.3.1. Let $f \in P \setminus \{0\}$ and $F \in \overline{P}$.

a) Write $f = c_1 t_1 + \cdots + c_s t_s$ with $c_1, \ldots, c_s \in K \setminus \{0\}$ and distinct terms $t_1, \ldots, t_s \in \mathbb{T}^n$. For $j = 1, \ldots, s$, let $\deg_W(t_j) = (\tau_{1j}, \ldots, \tau_{mj}) \in \mathbb{Z}^m$. Moreover, for $i = 1, \ldots, m$, let $\mu_i = \max\{\tau_{ij} \mid j = 1, \ldots, s\}$ be the maximum of the i^{th} components of the degrees of the terms $t_1, \ldots, t_s$. Then $(\mu_1, \ldots, \mu_m)$ is called the **top degree** of f with respect to the grading given by W and is denoted by $\mathrm{topdeg}_W(f)$.

b) In the context of a), the **homogenization** of f with respect to the grading given by W is the polynomial

$$f^{\mathrm{hom}} = \sum_{j=1}^{s} c_j \, t_j \, y_1^{\mu_1 - \tau_{1j}} \cdots y_m^{\mu_m - \tau_{mj}} \ \in \overline{P}$$

For the zero polynomial, we set $0^{\mathrm{hom}} = 0$.

c) The polynomial $F^{\mathrm{deh}} = F(1, \ldots, 1, x_1, \ldots, x_n) \in P$ is called the **dehomogenization** of F with respect to $y_1, \ldots, y_m$.

Our first observation is that the process of homogenizing a polynomial can be described informally as follows. Multiply each term in the support of f by the appropriate power product of $y_1, \ldots, y_m$ in order to make it homogeneous of degree $\mathrm{topdeg}_W(f)$. Hence the polynomial f^{hom} is indeed a homogeneous polynomial in $\overline{P}$ of degree $\deg_{\overline{W}}(f^{\mathrm{hom}}) = \mathrm{topdeg}_W(f)$.

Secondly, we note that the operation of dehomogenization has been defined for all polynomials in $\overline{P}$, but usually we shall apply it only to homogeneous polynomials $F \in \overline{P}$. Homogenization and dehomogenization of polynomials obey the following rules.

Proposition 4.3.2. (Rules for Homogenizing Polynomials)
Let polynomials $f, g \in P$ and $F, G \in \overline{P}$ be given.

a) Let $f \neq 0$, let $\mu = \mathrm{topdeg}_W(f)$, and let $f = f_1 + \cdots + f_r$ be the decomposition of f into its homogeneous components, where each $f_i \in P$ is homogeneous of degree $d_i \in \mathbb{Z}^m$. Then we have

$$f^{\mathrm{hom}} = y^{\mu - d_1} f_1 + \cdots + y^{\mu - d_r} f_r$$

where $y^{\mu - d_i} = y_1^{\alpha_{i1}} \cdots y_m^{\alpha_{im}}$ for $\mu - d_i = (\alpha_{i1}, \ldots, \alpha_{im}) \in \mathbb{Z}^m$.

b) Let $(\mu_1, \ldots, \mu_m) = \mathrm{topdeg}_W(f)$. Then we have

$$f^{\mathrm{hom}} = y_1^{\mu_1} \cdots y_m^{\mu_m} \cdot f\left(\frac{x_1}{y_1^{w_{11}} \cdots y_m^{w_{m1}}}, \ldots, \frac{x_n}{y_1^{w_{1n}} \cdots y_m^{w_{mn}}}\right)$$

c) We have $(f^{\mathrm{hom}})^{\mathrm{deh}} = f$.
d) If $fg \neq 0$, *we have* $\mathrm{topdeg}_W(fg) = \mathrm{topdeg}_W(f) + \mathrm{topdeg}_W(g)$.
e) We have $(fg)^{\mathrm{hom}} = (f^{\mathrm{hom}})(g^{\mathrm{hom}})$.
f) Let $f, g, f+g \in P \setminus \{0\}$, *and let* d *be the componentwise maximum of* $\mathrm{topdeg}_W(f)$ *and* $\mathrm{topdeg}_W(g)$. *Then we have*

$$y^{d-\mathrm{topdeg}_W(f+g)} \cdot (f+g)^{\mathrm{hom}} = y^{d-\mathrm{topdeg}_W(f)} \cdot f^{\mathrm{hom}} + y^{d-\mathrm{topdeg}_W(g)} \cdot g^{\mathrm{hom}}$$

g) We have $(FG)^{\mathrm{deh}} = F^{\mathrm{deh}}\, G^{\mathrm{deh}}$ *and* $(F+G)^{\mathrm{deh}} = F^{\mathrm{deh}} + G^{\mathrm{deh}}$.
h) Suppose that F *is non-zero and homogeneous. For* $j = 1, \ldots, m$, *let* $s_j = \max\{i \geq 0 \mid y_j^i \text{ divides } F\}$. *Then* $y_1^{s_1} \cdots y_m^{s_m} \cdot (F^{\mathrm{deh}})^{\mathrm{hom}} = F$. *In particular, we have* $F^{\mathrm{deh}} \neq 0$.
i) Given two terms $T, T' \in \mathbb{T}(y_1, \ldots, y_m, x_1, \ldots, x_n)$ *with* $\deg_{\overline{W}}(T) = \deg_{\overline{W}}(T')$ *and* $T^{\mathrm{deh}} = (T')^{\mathrm{deh}}$, *we have* $T = T'$.

Proof. Claim a) follows by combining the terms $t_1, \ldots, t_s$ in Definition 4.3.1.a into groups according to their degrees.

To prove b), we decompose $f = c_1 t_1 + \cdots + c_s t_s$ as in the definition, and we write $t_j = x_1^{\alpha_{1j}} \cdots x_n^{\alpha_{nj}}$ for $j = 1, \ldots, s$. Then we have the equality $\deg_W(t_j) = W \cdot (\alpha_{1j}, \ldots, \alpha_{nj})^{\mathrm{tr}} = (\tau_{1j}, \ldots, \tau_{mj})^{\mathrm{tr}}$, and therefore

$$\begin{aligned}
f^{\mathrm{hom}} &= \sum_{j=1}^{s} c_j\, t_j\, y_1^{\mu_1 - \tau_{1j}} \cdots y_m^{\mu_m - \tau_{mj}} \\
&= y_1^{\mu_1} \cdots y_m^{\mu_m} \cdot \sum_{j=1}^{s} c_j \, \frac{x_1^{\alpha_{1j}} \cdots x_n^{\alpha_{nj}}}{y_1^{\tau_{1j}} \cdots y_m^{\tau_{mj}}} \\
&= y_1^{\mu_1} \cdots y_m^{\mu_m} \cdot \sum_{j=1}^{s} c_j \, \left(\frac{x_1}{y_1^{w_{11}} \cdots y_m^{w_{m1}}}\right)^{\alpha_{1j}} \cdots \left(\frac{x_n}{y_1^{w_{1n}} \cdots y_m^{w_{mn}}}\right)^{\alpha_{nj}} \\
&= y_1^{\mu_1} \cdots y_m^{\mu_m} \cdot f\left(\frac{x_1}{y_1^{w_{11}} \cdots y_m^{w_{m1}}}, \ldots, \frac{x_n}{y_1^{w_{1n}} \cdots y_m^{w_{mn}}}\right)
\end{aligned}$$

Claim c) follows easily from the definition. To prove d), we proceed component by component. For $i \in \{1, \ldots, m\}$, consider the i^{th} component. Let $(\mu_1, \ldots, \mu_m) = \mathrm{topdeg}_W(f)$ and $(\nu_1, \ldots, \nu_m) = \mathrm{topdeg}_W(g)$. Then we write $f = f' + f''$ where f' contains the terms of f whose degree has i^{th} component equal to μ_i and f'' contains the remaining terms of f. Similarly, we decompose $g = g' + g''$. Then $fg = f'g' + (f'g'' + f''g' + f''g'')$ where $f'g'$ consists of terms whose degree has i^{th} component equal to $\mu_i + \nu_i$ and the second summand consists of terms whose degree has a smaller i^{th} component. Hence the i^{th} component of $\mathrm{topdeg}_W(fg)$ is $\mu_i + \nu_i$, as we wanted to show.

For the proof of e), it suffices to use b) and d). Claim f) follows easily from a), and claim g) from the fact that dehomogenization is nothing but the substitution homomorphism $y_i \mapsto 1$ for $i = 1, \ldots, m$.

Finally we prove h) and i). We write $F = y_1^{s_1} \cdots y_m^{s_m}\, \widetilde{F}$, where $\widetilde{F}$ is not divisible by any y_i. We need to show that $(\widetilde{F}^{\mathrm{deh}})^{\mathrm{hom}} = \widetilde{F}$. To

this end, we note that no two terms in the support of $\widetilde{F}$ dehomogenize to the same term, since the dehomogenization of $y_1^{\alpha_1}\cdots y_m^{\alpha_m}x_1^{\beta_1}\cdots x_n^{\beta_n}$ is $x_1^{\beta_1}\cdots x_n^{\beta_n}$ and the exponents $\alpha_1,\ldots,\alpha_m$ are determined by the equation $(\alpha_1,\ldots,\alpha_m)^{\mathrm{tr}} = \deg_{\overline{W}}(\widetilde{F}) - W\cdot(\beta_1,\ldots,\beta_n)^{\mathrm{tr}}$. Moreover, the degree of $(\widetilde{F}^{\mathrm{deh}})^{\mathrm{hom}}$ equals $\deg_{\overline{W}}(\widetilde{F})$, because for every index $j\in\{1,\ldots,m\}$ there exists one term in the support of $\widetilde{F}$ which is not divisible by y_j. Altogether, the homogenization of $\widetilde{F}^{\mathrm{deh}}$ is $\widetilde{F}$. Claim i) is a special case of h). □

Notice also that $\deg_W(f)\leq_{\mathtt{Lex}}\deg_{\overline{W}}(f^{\mathrm{hom}}) = \mathrm{topdeg}_W(f)$. For $m=1$, the first inequality is an equality. The following example shows that it may be a strict inequality when $m\geq 2$.

Example 4.3.3. Let $P=\mathbb{Q}[x_1,x_2]$ be graded by the matrix $W=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, and let $f=x_1+x_2$. Then we have $\mathrm{topdeg}_W(f)=(1,1)$ and $f^{\mathrm{hom}}=y_2x_1+y_1x_2$. Hence we see that $\deg_W(f)=(1,0)<_{\mathtt{Lex}}\mathrm{topdeg}_W(f)$.

Based on the notions of homogenization and dehomogenization of polynomials, we can now introduce the same processes for ideals.

Definition 4.3.4. Let I be an ideal in P and J an ideal in $\overline{P}$.

a) The ideal $I^{\mathrm{hom}}=(f^{\mathrm{hom}}\mid f\in I)$ in $\overline{P}$ is called the **homogenization** of I with respect to the grading given by W.
b) The set $J^{\mathrm{deh}}=\{F^{\mathrm{deh}}\mid F\in J\}$ in P is called the **dehomogenization** of J with respect to $y_1,\ldots,y_m$.

Obviously, the set J^{deh} is an ideal in P, since it is the image of J under the surjective ring homomorphism $\overline{P}\longrightarrow P$ defined by $y_j\mapsto 1$ for $j=1,\ldots,m$ and $x_i\mapsto x_i$ for $i=1,\ldots,n$. In particular, we see that $J^{\mathrm{deh}}=(J:(y_1\cdots y_m)^\infty)^{\mathrm{deh}}$. Although we have defined the dehomogenization of an arbitrary ideal in $\overline{P}$, we shall mainly be interested in the case of homogeneous ideals, thereby justifying the choice of the name. Homogenization and dehomogenization of ideals are governed by the following rules.

Proposition 4.3.5. (Rules for Homogenizing Ideals)
Let I be an ideal in P and J a homogeneous ideal in $\overline{P}$.

a) We have $(I^{\mathrm{hom}})^{\mathrm{deh}}=I$. In particular, the operation which associates to an ideal in P its homogenization is injective, and the operation which associates to a homogeneous ideal in $\overline{P}$ its dehomogenization is surjective.
b) For a homogeneous polynomial $F\in\overline{P}$, we have

$$\begin{aligned} F\in I^{\mathrm{hom}} &\iff F^{\mathrm{deh}}\in I\\ &\iff F=y_1^{s_1}\cdots y_m^{s_m}f^{\mathrm{hom}} \text{ for some } f\in I \text{ and } s_1,\ldots,s_m\in\mathbb{N}\end{aligned}$$

c) For a homogeneous polynomial $F\in\overline{P}$, we have $F^{\mathrm{deh}}\in J^{\mathrm{deh}}$ if and only if $(y_1\cdots y_m)^sF\in J$ for some $s\geq 0$.

d) We have $J \subseteq (J^{\mathrm{deh}})^{\mathrm{hom}} = J :_{\overline{P}} (y_1 \cdots y_m)^\infty$.
e) If $I \neq P$, *then* $y_1 \cdots y_m$ *is a non-zerodivisor for* $\overline{P}/I^{\mathrm{hom}}$.
f) If I *is a proper homogeneous ideal in* P, *then we have* $I^{\mathrm{hom}} = I \cdot \overline{P}$. *In particular, in this case* $y_1 \cdots y_m$ *is a non-zerodivisor for* $\overline{P}/I \cdot \overline{P}$.

Proof. First we prove a). By Proposition 4.3.2.c, we have $I \subseteq (I^{\mathrm{hom}})^{\mathrm{deh}}$. Now let $f \in (I^{\mathrm{hom}})^{\mathrm{deh}}$. By definition, the polynomial f is of the form $f = (\sum_{i=1}^r G_i g_i^{\mathrm{hom}})^{\mathrm{deh}}$, where $G_1, \ldots, G_r \in \overline{P}$ and $g_1, \ldots, g_r \in I$. Using Proposition 4.3.2.g, it follows that $f = \sum_{i=1}^r G_i^{\mathrm{deh}} g_i \in I$.

Next we show b). For a homogeneous polynomial $F \in I^{\mathrm{hom}}$, we have $F^{\mathrm{deh}} \in (I^{\mathrm{hom}})^{\mathrm{deh}} = I$ by a). Given $F \in \overline{P}$ such that $F^{\mathrm{deh}} \in I$, we have $F = y_1^{s_1} \cdots y_m^{s_m} f^{\mathrm{hom}}$ for $f = F^{\mathrm{deh}}$ and some $s_1, \ldots, s_m \in \mathbb{N}$ by Proposition 4.3.2.h. And if $F = y_1^{s_1} \cdots y_m^{s_m} f^{\mathrm{hom}}$, then we clearly have $F \in I^{\mathrm{hom}}$.

For the proof of c), we note that the implication "$\Leftarrow$" follows from the fact that $(y_1 \cdots y_m)^s F \in J$ implies $F^{\mathrm{deh}} = ((y_1 \cdots y_m)^s F)^{\mathrm{deh}} \in J^{\mathrm{deh}}$. Conversely, let a homogeneous polynomial $F \in \overline{P}$ be given such that $F^{\mathrm{deh}} \in J^{\mathrm{deh}}$. Since J^{deh} is a homomorphic image of J, there exists a polynomial $G \in J$ such that $G^{\mathrm{deh}} = F^{\mathrm{deh}}$. The homogeneous components of G are also in J, because J is a homogeneous ideal. By multiplying them with the appropriate terms in $\mathbb{T}(y_1, \ldots, y_m)$, we may assume that G is a homogeneous polynomial in J which satisfies $G^{\mathrm{deh}} = F^{\mathrm{deh}}$. Thus Proposition 4.3.2.h yields numbers $s_1, \ldots, s_m, s_1', \ldots, s_m' \in \mathbb{N}$ such that $F = y_1^{s_1} \cdots y_m^{s_m} (F^{\mathrm{deh}})^{\mathrm{hom}} = y_1^{s_1} \cdots y_m^{s_m} (G^{\mathrm{deh}})^{\mathrm{hom}}$ and $G = y_1^{s_1'} \cdots y_m^{s_m'} (G^{\mathrm{deh}})^{\mathrm{hom}}$. Altogether, this shows $(y_1 \cdots y_m)^s F \in (G) \subseteq J$ for $s = \max\{0, \max\{s_i' - s_i \mid i = 1, \ldots, m\}\}$.

The inclusion $J \subseteq (J^{\mathrm{deh}})^{\mathrm{hom}}$ in d) follows from Proposition 4.3.2.h, and $(J^{\mathrm{deh}})^{\mathrm{hom}} \subseteq J :_{\overline{P}} (y_1 \cdots y_m)^\infty$ is a consequence of c). To prove the remaining containment, we note that $J :_{\overline{P}} (y_1 \cdots y_m)^\infty$ is clearly a homogeneous ideal in $\overline{P}$. Let a homogeneous polynomial $F \in J :_{\overline{P}} (y_1 \cdots y_m)^\infty$ be given. Then there exists an $r \geq 0$ such that $(y_1 \cdots y_m)^r F \in J$. Therefore we have $F^{\mathrm{deh}} \in J^{\mathrm{deh}}$. Using Proposition 4.3.2.h, we get numbers $s_1, \ldots, s_m \in \mathbb{N}$ such that $F = y_1^{s_1} \cdots y_m^{s_m} (F^{\mathrm{deh}})^{\mathrm{hom}} \in (J^{\mathrm{deh}})^{\mathrm{hom}}$, and this was to be shown.

To prove e), we suppose that $y_1 \cdots y_m F \in I^{\mathrm{hom}}$ for some homogeneous polynomial $F \in \overline{P}$. Part a) implies $F^{\mathrm{deh}} = (y_1 \cdots y_m F)^{\mathrm{deh}} \in (I^{\mathrm{hom}})^{\mathrm{deh}} = I$, and then b) yields $F \in I^{\mathrm{hom}}$. Finally, we observe that a homogeneous polynomial in P is its own homogenization because of Proposition 4.3.2.a. This proves claim f). □

The following example shows that the inclusion in part d) of the preceding proposition can be strict.

Example 4.3.6. Let $P = K[x_1]$ be standard graded and $\overline{P} = K[y_1, x_1]$. Then we have $J \subset (J^{\mathrm{deh}})^{\mathrm{hom}}$ for the principal ideal $J = (y_1 x_1 - y_1^2)$ in $\overline{P}$, since Proposition 4.3.5.d shows $(J^{\mathrm{deh}})^{\mathrm{hom}} = J :_{\overline{P}} (y_1)^\infty = (x_1 - y_1)$ and $x_1 - y_1 \notin J$.

As a consequence of these rules, we can characterize the homogenization of an ideal as follows.

Corollary 4.3.7. (Characterization of the Homogenization)
Let I be an ideal in P. For an ideal J in $\overline{P}$, the following conditions are equivalent.

a) $J = I^{\text{hom}}$
b) The ideal J is homogeneous, has dehomogenization I, and satisfies the equality $J = J :_{\overline{P}} (y_1 \cdots y_m)^\infty$.

Proof. Since a) implies b) by parts a) and d) of the proposition, it remains to prove the converse. Using the hypothesis and part d) of the proposition, we calculate $J = J :_{\overline{P}} (y_1 \cdots y_m)^\infty = (J^{\text{deh}})^{\text{hom}} = I^{\text{hom}}$. □

Another application of the proposition is a way of actually computing homogenizations and dehomogenizations of ideals. Later we will see alternative ways to do this (see Corollary 4.3.20 and Corollary 4.4.15).

Corollary 4.3.8. (Computation of the Homogenization)
Let I be an ideal in P which is generated by polynomials $f_1, \ldots, f_r \in P$, and let J be a homogeneous ideal in $\overline{P}$ which is generated by polynomials $F_1, \ldots, F_s \in \overline{P}$.

a) The homogenization of I can be computed via the formula

$$I^{\text{hom}} = (f_1^{\text{hom}}, \ldots, f_r^{\text{hom}}) :_{\overline{P}} (y_1 \cdots y_m)^\infty$$

b) The dehomogenization of J can be computed via the formula

$$J^{\text{deh}} = (F_1^{\text{deh}}, \ldots, F_s^{\text{deh}})$$

Proof. Claim a) follows from part d) of the proposition, since I is the dehomogenization of $(f_1^{\text{hom}}, \ldots, f_r^{\text{hom}})$, and b) is a consequence of the fact that J^{deh} is an image of J under a surjective ring homomorphism. □

Is the saturation needed in the above corollary? The following example answers this affirmatively.

Example 4.3.9. Let $P = K[x_1, x_2, x_3]$ be equipped with the standard grading given by $W = (1\ 1\ 1)$, let $f_1 = x_1^2 + x_2$, $f_2 = x_1^2 + x_3$, let $I = (f_1, f_2)$, and let $\overline{P} = K[y_1, x_1, x_2, x_3]$. Then we have $(f_1^{\text{hom}}, f_2^{\text{hom}}) \subset I^{\text{hom}}$, since $(f_1 - f_2)^{\text{hom}} = (x_2 - x_3)^{\text{hom}} = x_2 - x_3$ is contained in I^{hom}, but not in the ideal $(f_1^{\text{hom}}, f_2^{\text{hom}}) = (x_1^2 + y_1 x_2,\ x_1^2 + y_1 x_3)$ which does not contain any non-zero homogeneous element of degree one.

Our next two propositions deal with the next level of generality, namely with the behaviour of homogenization and dehomogenization under important ideal-theoretic operations.

Proposition 4.3.10. *Let I, I_1, and I_2 be ideals in P.*

a) If $I_1 \subseteq I_2$, then we have $I_1^{\mathrm{hom}} \subseteq I_2^{\mathrm{hom}}$.
b) We have $(I_1 \cap I_2)^{\mathrm{hom}} = I_1^{\mathrm{hom}} \cap I_2^{\mathrm{hom}}$.
c) We have $(\sqrt{I})^{\mathrm{hom}} = \sqrt{I^{\mathrm{hom}}}$.
d) The ideal I is prime if and only if I^{hom} is prime.

Proof. Claim a) follows immediately from Definition 4.3.4.a. In b), the inclusion "$\subseteq$" follows from a). Now let $F \in I_1^{\mathrm{hom}} \cap I_2^{\mathrm{hom}}$ be a homogeneous polynomial. Then Proposition 4.3.5 shows $F^{\mathrm{deh}} \in I_1 \cap I_2$, and Proposition 4.3.2.h yields $F = (y_1 \cdots y_m)^s (F^{\mathrm{deh}})^{\mathrm{hom}} \in (I_1 \cap I_2)^{\mathrm{hom}}$ for some $s \geq 1$. Since $I_1^{\mathrm{hom}} \cap I_2^{\mathrm{hom}}$ is a homogeneous ideal, this proves the claim.

Next we prove claim c). By Proposition 4.3.5.b, a homogeneous polynomial $F \in \overline{P}$ satisfies $F \in (\sqrt{I})^{\mathrm{hom}}$ if and only if $F^{\mathrm{deh}} \in \sqrt{I}$, and this means that there exists $s \geq 0$ such that $(F^{\mathrm{deh}})^s \in I$. By Proposition 4.3.2.g, the latter condition is equivalent to $(F^s)^{\mathrm{deh}} \in I$ for some $s \geq 0$, and thus, by Proposition 4.3.5.b, equivalent to $F^s \in I^{\mathrm{hom}}$ for some $s \geq 0$, i.e. to $F \in \sqrt{I^{\mathrm{hom}}}$.

For the proof of d) we use Proposition 1.7.12 which says that I^{hom} is a prime ideal if and only if $FG \in I^{\mathrm{hom}}$ implies $F \in I^{\mathrm{hom}}$ or $G \in I^{\mathrm{hom}}$ for homogeneous polynomials $F, G \in \overline{P}$. Notice that this proposition is applicable, because `Lex` defines a monoid ordering on $\mathbb{Z}^m$. In order to prove "$\Rightarrow$", let $F, G \in \overline{P}$ be homogeneous polynomials such that $FG \in I^{\mathrm{hom}}$. Using Proposition 4.3.2.h, we find $r, s \geq 0$ such that $F = (y_1 \cdots y_m)^r (F^{\mathrm{deh}})^{\mathrm{hom}}$ and $G = (y_1 \cdots y_m)^s (G^{\mathrm{deh}})^{\mathrm{hom}}$. Then we use $F^{\mathrm{deh}} G^{\mathrm{deh}} \in I$ to conclude that $F^{\mathrm{deh}} \in I$ or $G^{\mathrm{deh}} \in I$. Hence we have $F = (y_1 \cdots y_m)^r (F^{\mathrm{deh}})^{\mathrm{hom}} \in I^{\mathrm{hom}}$ or $G = (y_1 \cdots y_m)^s (G^{\mathrm{deh}})^{\mathrm{hom}} \in I^{\mathrm{hom}}$. Finally, the implication "$\Leftarrow$" follows from the observation that every element $f \in I$ is the dehomogenization of $f^{\mathrm{hom}} \in I^{\mathrm{hom}}$. □

Although, as we have seen, homogenization is compatible with many ideal-theoretic operations, this is not true for sums and products of ideals. Our next example shows that the corresponding claims in [ZS60], Ch. VII, Thm. 17, do not hold (see also Exercise 4).

Example 4.3.11. Using the same assumptions as in Example 4.3.9, we let $I_1 = (f_1)$ and $I_2 = (f_2)$.

a) We have $I_1^{\mathrm{hom}} = (f_1^{\mathrm{hom}}) = (x_1^2 + y_1 x_2)$ and $I_2^{\mathrm{hom}} = (f_2^{\mathrm{hom}}) = (x_1^2 + y_1 x_3)$. Since the element $f_1 - f_2 = x_2 - x_3 \in I_1 + I_2$ satisfies $(f_1 - f_2)^{\mathrm{hom}} = x_2 - x_3 \in (I_1 + I_2)^{\mathrm{hom}}$ and $(f_1 - f_2)^{\mathrm{hom}} \notin I_1^{\mathrm{hom}} + I_2^{\mathrm{hom}} = (f_1^{\mathrm{hom}}, f_2^{\mathrm{hom}}) = (x_1^2 + y_1 x_2,\ x_1^2 + y_1 x_3)$, we see that the inclusion $I_1^{\mathrm{hom}} + I_2^{\mathrm{hom}} \subseteq (I_1 + I_2)^{\mathrm{hom}}$ can be strict.

b) Consider the ideals $I_3 = (f_1, x_2^2)$ and $I_4 = (f_2, x_2^2)$. Then $f_1 x_2^2 - x_2^2 f_2 = x_2^3 - x_2^2 x_3 \in I_3 \cdot I_4$ implies that we have $x_2^3 - x_2^2 x_3 \in (I_3 \cdot I_4)^{\mathrm{hom}}$. Using Corollary 4.3.8.a, we calculate $I_3^{\mathrm{hom}} = (f_1^{\mathrm{hom}},\ x_2^2) :_{\overline{P}} y_1^\infty = (x_1^2 + y_1 x_2,\ x_2^2)$ and, similarly, $I_4^{\mathrm{hom}} = (f_2^{\mathrm{hom}}, x_2^2) :_{\overline{P}} y_1^\infty = (x_1^2 + y_1 x_3, x_2^2)$. It follows that

the ideal $I_3^{\mathrm{hom}} \cdot I_4^{\mathrm{hom}}$ contains no non-zero elements of degree three. Hence the inclusion $I_3^{\mathrm{hom}} \cdot I_4^{\mathrm{hom}} \subseteq (I_3 \cdot I_4)^{\mathrm{hom}}$ can be strict.

Since dehomogenization is nothing but the application of a surjective ring homomorphism, it is well-behaved with respect to many ideal-theoretic operations. The following proposition summarizes this good behaviour.

Proposition 4.3.12. *Let J, J_1, and J_2 be homogeneous ideals in $\overline{P}$.*

a) If $J_1 \subseteq J_2$, then we have $J_1^{\mathrm{deh}} \subseteq J_2^{\mathrm{deh}}$.
b) We have $(J_1 \cap J_2)^{\mathrm{deh}} = J_1^{\mathrm{deh}} \cap J_2^{\mathrm{deh}}$ and $(J_1 + J_2)^{\mathrm{deh}} = J_1^{\mathrm{deh}} + J_2^{\mathrm{deh}}$.
c) We have $(\sqrt{J})^{\mathrm{deh}} = \sqrt{J^{\mathrm{deh}}}$.
d) If J is a prime ideal of $\overline{P}$ which does not contain $y_1 \cdots y_m$, then J^{deh} is a prime ideal of P. Conversely, if J^{deh} is a prime ideal of P and $y_1 \cdots y_m$ is not a zerodivisor for $\overline{P}/J$, then J is a prime ideal of $\overline{P}$.

Proof. It is clear that a) holds, and in b) the only non-trivial part is the containment "$\supseteq$" in the first formula. Let $f \in J_1^{\mathrm{deh}} \cap J_2^{\mathrm{deh}}$. By Proposition 4.3.5.b, there exists a number $s \geq 0$ such that $(y_1 \cdots y_m)^s f^{\mathrm{hom}} \in J_1$ and $(y_1 \cdots y_m)^s f^{\mathrm{hom}} \in J_2$. Hence we get $f = ((y_1 \cdots y_m)^s f^{\mathrm{hom}})^{\mathrm{deh}} \in (J_1 \cap J_2)^{\mathrm{deh}}$.

For the proof of c), we note that, by Proposition 4.3.5.b, a polynomial $f \in P$ satisfies $f = (f^{\mathrm{hom}})^{\mathrm{deh}} \in (\sqrt{J})^{\mathrm{deh}}$ if and only if $(y_1 \cdots y_m)^s f^{\mathrm{hom}} \in \sqrt{J}$ for some $s \geq 0$. This is equivalent to $((y_1 \cdots y_m)^s f^{\mathrm{hom}})^t \in J$ for some $t \geq 0$, and therefore to $f^t = ((y_1 \cdots y_m\, f^{\mathrm{hom}})^t)^{\mathrm{deh}} \in J^{\mathrm{deh}}$ for some $t \geq 0$, i.e. to $f \in \sqrt{J^{\mathrm{deh}}}$.

It remains to prove d). First we assume that J is a prime ideal which does not contain $y_1 \cdots y_m$. Then $J^{\mathrm{deh}} \subset P$ is a proper ideal of P, since $1 \in J^{\mathrm{deh}}$ would imply $(y_1 \cdots y_m)^s \cdot 1 \in J$ for some $s \geq 0$, contradicting our assumption. Now let $f, g \in P$ such that $fg \in J^{\mathrm{deh}}$. By Propositon 4.3.5.b, there exists a number $s \geq 0$ such that $(y_1 \cdots y_m)^s (fg)^{\mathrm{hom}} = (y_1 \cdots y_m)^s f^{\mathrm{hom}} g^{\mathrm{hom}} \in J$. Since $y_1 \cdots y_m \notin J$, this yields $f^{\mathrm{hom}} \in J$ or $g^{\mathrm{hom}} \in J$. Therefore we have $f = (f^{\mathrm{hom}})^{\mathrm{deh}} \in J^{\mathrm{deh}}$ or $g = (g^{\mathrm{hom}})^{\mathrm{deh}} \in J^{\mathrm{deh}}$.

Conversely, let $F, G \in \overline{P}$ be homogeneous polynomials such that $FG \in J$. Then $(FG)^{\mathrm{deh}} = F^{\mathrm{deh}} G^{\mathrm{deh}} \in J^{\mathrm{deh}}$ implies $F^{\mathrm{deh}} \in J^{\mathrm{deh}}$ or $G^{\mathrm{deh}} \in J^{\mathrm{deh}}$. Using Proposition 4.3.5.c, we get $(y_1 \cdots y_m)^s F \in J$ for some $s \geq 0$ or $(y_1 \cdots y_m)^t G \in J$ for some $t \geq 0$. Since $y_1 \cdots y_m$ is a non-zerodivisor for P/J, this implies $F \in J$ or $G \in J$. Now Propositon 1.7.12 shows that J is a prime ideal of $\overline{P}$. □

The last part of this subsection deals with the behaviour of Gröbner bases under dehomogenization. To this end, we first explain how to relate term orderings on P to term orderings on $\overline{P}$. Recall that $\overline{P}$ is graded by $\overline{W} = (\mathcal{I}_m \mid W)$, and observe that $\overline{W}$ is non-negative (resp. positive) if and only if W is non-negative (resp. positive).

Definition 4.3.13. Let σ be a monoid ordering on $\mathbb{T}^n = \mathbb{T}(x_1, \ldots, x_n)$ and let us consider the relation $\overline{\sigma}^W$ on $\mathbb{T}^{m+n} = \mathbb{T}(y_1, \ldots, y_m, x_1, \ldots, x_n)$

which is defined by the following rule. Given two terms $t_1, t_2 \in \mathbb{T}^{m+n}$, we say that $t_1 \geq_{\overline{\sigma}^W} t_2$ if either we have $\deg_{\overline{W}}(t_1) >_{\mathtt{Lex}} \deg_{\overline{W}}(t_2)$ or we have $\deg_{\overline{W}}(t_1) = \deg_{\overline{W}}(t_2)$ and $t_1^{\mathrm{deh}} \geq_\sigma t_2^{\mathrm{deh}}$. We call $\overline{\sigma}^W$ the **extension** of σ by W. If it is clear which grading we are considering, we shall simply denote it by $\overline{\sigma}$.

Notice that $\overline{\sigma}$ is not necessarily a true extension of σ in the sense that its restriction to $\mathbb{T}^n$ need not coincide with σ. However, this is the case if σ is compatible with $\deg_W$. The extension of a monoid ordering satisfies the following properties.

Proposition 4.3.14. *Let σ be a monoid ordering on $\mathbb{T}^n$, and let $\overline{\sigma}$ be its extension by W.*

a) The relation $\overline{\sigma}$ is a monoid ordering on $\mathbb{T}^{m+n}$ which is compatible with $\deg_{\overline{W}}$.
b) If W is non-negative and the restriction of σ to the terms in P_0 is a term ordering, then $\overline{\sigma}$ is a term ordering on $\mathbb{T}^{m+n}$.
c) If W is positive, then $\overline{\sigma}$ is a term ordering on $\mathbb{T}^{m+n}$.
d) If σ is of the form $\sigma = \mathtt{Ord}(V)$ for a non-singular matrix $V \in \mathrm{Mat}_n(\mathbb{Z})$, then we have $\overline{\sigma} = \mathtt{Ord}\left(\begin{smallmatrix} \mathcal{I}_m & W \\ 0 & V \end{smallmatrix}\right)$.

Proof. First we prove a). In order to check antisymmetry, we assume that $t = y_1^{\alpha_1} \cdots y_m^{\alpha_m} x_1^{\beta_1} \cdots x_n^{\beta_n}$ and $t' = y_1^{\alpha'_1} \cdots y_m^{\alpha'_m} x_1^{\beta'_1} \cdots x_n^{\beta'_n}$ satisfy $t \geq_{\overline{\sigma}} t'$ and $t' \geq_{\overline{\sigma}} t$. Then we have $\deg_{\overline{W}}(t) = \deg_{\overline{W}}(t')$ and $t^{\mathrm{deh}} = (t')^{\mathrm{deh}}$, and therefore $\overline{W} \cdot (\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)^{\mathrm{tr}} = \overline{W} \cdot (\alpha'_1, \ldots, \alpha'_m, \beta'_1, \ldots, \beta'_n)^{\mathrm{tr}}$ and $(\beta_1, \ldots, \beta_n) = (\beta'_1, \ldots, \beta'_n)$. By plugging the second equation into the first one, we find $\mathcal{I}_m \cdot (\alpha_1, \ldots, \alpha_m)^{\mathrm{tr}} = \mathcal{I}_m \cdot (\alpha'_1, \ldots, \alpha'_m)^{\mathrm{tr}}$, and hence $t = t'$. The other axioms for monoid orderings are easy to check, and the compatibility of $\overline{\sigma}$ with $\deg_{\overline{W}}$ is an immediate consequence of the definition.

Now we show b). Since $\overline{\sigma}$ is compatible with $\deg_{\overline{W}}$, we have $y_i >_{\overline{\sigma}} 1$ for $i = 1, \ldots, m$. For the same reason, if $i \in \{1, \ldots, n\}$ is such that $\deg_{\overline{W}}(x_i) = \deg_W(x_i) >_{\mathtt{Lex}} 0$, then $x_i >_{\overline{\sigma}} 1$. Finally, if $i \in \{1, \ldots, n\}$ is such that $\deg_W(x_i) = 0$, then the hypothesis implies $x_i >_\sigma 1$. By definition of $\overline{\sigma}$, we obtain $x_i >_{\overline{\sigma}} 1$.

Claim c) follows from b), because if W is positive, we have $P_0 = K$. Finally, claim d) follows from the definition of $\overline{\sigma}$ in a straightforward manner. □

Let us clarify the details of this proposition using an example.

Example 4.3.15. Let $P = \mathbb{Q}[x_1, x_2, x_3]$ be graded by $W = (1\ 1\ 0)$, and let $\sigma = \mathtt{Ord}(V)$ be the monoid ordering on $\mathbb{T}^3$ given by $V = \left(\begin{smallmatrix} -1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. Notice that the grading given by W is not positive, and that σ is not a term ordering. However, the extension $\overline{\sigma}$ of σ by W is a term ordering by part b) of the proposition, and we have $\overline{\sigma} = \mathtt{Ord}\left(\begin{smallmatrix} 1 & W \\ 0 & V \end{smallmatrix}\right)$ by d).

The following lemma will prove to be a useful tool.

Lemma 4.3.16. *Let $G \in \overline{P}$ be a non-zero homogeneous polynomial, and let $f \in P$ be a non-zero polynomial. Then*

a) There exist $s_1, \ldots, s_m \in \mathbb{N}$ such that $\mathrm{LT}_{\overline{\sigma}}(G) = y_1^{s_1} \cdots y_m^{s_m} \, \mathrm{LT}_\sigma(G^{\mathrm{deh}})$. Hence we have $(\mathrm{LT}_{\overline{\sigma}}(G))^{\mathrm{deh}} = \mathrm{LT}_\sigma(G^{\mathrm{deh}})$.

b) If σ is compatible with $\deg_W$, then

$$\mathrm{LT}_{\overline{\sigma}}(f^{\mathrm{hom}}) = y^{\mu - d_1} \, \mathrm{LT}_\sigma(\mathrm{DF}_W(f)) = y^{\mu - d_1} \, \mathrm{LT}_\sigma(f)$$

where $\mu = \mathrm{topdeg}(f)$ and $d_1 = \deg_W(\mathrm{DF}_W(f))$.

c) If σ is compatible with $\deg_W$ and $W \in \mathrm{Mat}_{1,n}(\mathbb{Z})$ is a one-row matrix, then

$$\mathrm{LT}_{\overline{\sigma}}(f^{\mathrm{hom}}) = \mathrm{LT}_\sigma(\mathrm{DF}_W(f)) = \mathrm{LT}_\sigma(f)$$

Proof. The proof of a) follows from the definition of $\overline{\sigma}$. The proof of b) follows from $f = (f^{\mathrm{hom}})^{\mathrm{deh}}$ and Proposition 4.3.2.a. The proof of c) follows from b) and the fact that $W \in \mathrm{Mat}_{1,n}(\mathbb{Z})$ implies $\mu = d_1$. □

The assumption that σ is degree compatible cannot be dropped in part b) of this lemma, as the following example shows.

Example 4.3.17. Let $P = K[x_1, x_2]$ graded by $W = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, let $f = x_1 + x_2$, and let $G = f^{\mathrm{hom}} = y_2 x_1 + y_1 x_2$. The term ordering $\sigma = \mathtt{Ord}(\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right))$ is clearly not compatible with $\deg_W$. Nevertheless, we have $\mathrm{LT}_{\overline{\sigma}}(G) = y_1 x_2 = y_1 \, \mathrm{LT}_\sigma(G^{\mathrm{deh}})$ in accord with a). But $\mathrm{LT}_{\overline{\sigma}}(f^{\mathrm{hom}}) = y_1 x_2$ does not agree with the right-hand side, since $\mu = (1,1)$ and $d_1 = (1,0)$ and $\mathrm{DF}_W(f) = x_1$ yield $y^{\mu - d_1} \, \mathrm{LT}_\sigma(\mathrm{DF}_W(f)) = y_2 x_1$.

If we use the lexicographic term ordering instead, it is clearly compatible with $\deg_W$, and we obtain $\mathrm{LT}_{\overline{\mathtt{Lex}}}(f^{\mathrm{hom}}) = y_2 x_1 = y^{\mu - d_1} \, \mathrm{LT}_{\mathtt{Lex}}(\mathrm{DF}_W(f))$ in agreement with claim b).

Our next proposition shows how Gröbner bases behave under dehomogenization. Notice that under the hypotheses of the following proposition, the ordering $\overline{\sigma}$ is a term ordering by Proposition 4.3.14.b.

Proposition 4.3.18. (Dehomogenization of Gröbner Bases)
Let P be non-negatively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let σ be a term ordering on $\mathbb{T}^n$, let $J \subseteq \overline{P}$ be a non-zero homogeneous ideal, and let $\{G_1, \ldots, G_s\}$ be a homogeneous $\overline{\sigma}$-Gröbner basis of J. Then $\{G_1^{\mathrm{deh}}, \ldots, G_s^{\mathrm{deh}}\}$ is a σ-Gröbner basis of J^{deh}.

Proof. It suffices to show for every non-zero polynomial $f \in J^{\mathrm{deh}}$ that there exists an index $i \in \{1, \ldots, s\}$ such that $\mathrm{LT}_\sigma(f)$ is a multiple of $\mathrm{LT}_\sigma(G_i^{\mathrm{deh}})$. Since $f^{\mathrm{hom}} \in (J^{\mathrm{deh}})^{\mathrm{hom}}$, Proposition 4.3.5.c yields a number $\ell \in \mathbb{N}$ such that $(y_1 \cdots y_m)^\ell f^{\mathrm{hom}} \in J$. By assumption, there exist an index $i \in \{1, \ldots, s\}$ and a term $t \in \mathbb{T}^n$ such that $(y_1 \cdots y_m)^\ell \, \mathrm{LT}_{\overline{\sigma}}(f^{\mathrm{hom}}) = y_1^{\alpha_1} \cdots y_m^{\alpha_m} \, t \, \mathrm{LT}_{\overline{\sigma}}(G_i)$.

By part a) of the lemma, there exist numbers $s_1, \ldots, s_m \in \mathbb{N}$ such that $\mathrm{LT}_{\overline{\sigma}}(f^{\mathrm{hom}}) = y_1^{s_1} \cdots y_m^{s_m} \mathrm{LT}_\sigma(f)$. If we dehomogenize the two expressions for $\mathrm{LT}_{\overline{\sigma}}(f^{\mathrm{hom}})$ and use part a) of the lemma again, we obtain the equality $\mathrm{LT}_\sigma(f) = t\,(\mathrm{LT}_{\overline{\sigma}}(G_i))^{\mathrm{deh}} = t\,\mathrm{LT}_\sigma(G_i^{\mathrm{deh}})$, as claimed. □

4.3.B Macaulay Bases and Homogenization

In this subsection we consider different aspects of the process of homogenizing an ideal, specifically its relation to Macaulay bases and its geometric interpretation. Since it turns out that the results we are going to discuss do not hold in general, we restrict to the case when $m = 1$ and the polynomial ring $P = K[x_1, \ldots, x_n]$ is graded by a row of positive integers $W = (w_1 \ \cdots \ w_n) \in \mathrm{Mat}_{1,n}(\mathbb{Z})$. Moreover, since we now have only one homogenizing indeterminate, it is customary to denote it by x_0 rather than by y_1. Hence we let $\overline{P} = K[x_0, \ldots, x_n]$ be graded by the matrix $\overline{W} = (1 \ w_1 \ \cdots \ w_n)$. Notice that we have $\deg_W(f) = \deg_{\overline{W}}(f^{\mathrm{hom}})$ and $f^{\mathrm{hom}}(0, x_1, \ldots, x_n) = \mathrm{DF}_W(f)$ for every non-zero polynomial $f \in P$.

In Example 4.3.9 we saw that, to compute the homogenization of an ideal (see Corollary 4.3.8.a), it is usually not sufficient to homogenize a system of generators. Sometimes it is essential to perform the saturation with respect to x_0. This suggests the following natural question. Which systems of generators of I have the property that their homogenizations generate I^{hom}? Our next theorem says that the answer to this question is "Macaulay bases".

Theorem 4.3.19. (Macaulay Bases and Homogenization)
Let I be a proper ideal of P, and let $\{f_1, \ldots, f_r\} \subset P \setminus \{0\}$ be a system of generators of I. Then the following conditions are equivalent.

a) We have $I^{\mathrm{hom}} = (f_1^{\mathrm{hom}}, \ldots, f_r^{\mathrm{hom}})$.
b) The set $\{f_1, \ldots, f_r\}$ is a Macaulay basis of I with respect to the grading given by W.

Proof. First we show that a) implies b). Given a polynomial $f \in I \setminus \{0\}$, we use the hypothesis to find a representation $f^{\mathrm{hom}} = \sum_{i=1}^r G_i f_i^{\mathrm{hom}}$, where G_i is a homogeneous polynomial in $\overline{P}$ of degree $\deg_W(f) - \deg_W(f_i)$. If we substitute $x_0 \mapsto 0$ in this equation and use Proposition 4.3.2, we obtain $\mathrm{DF}_W(f) = \sum_{i=1}^r G_i(0, x_1, \ldots, x_n)\ \mathrm{DF}_W(f_i)$, as we had to show.

Now we prove that b) implies a). The ideal $J = (f_1^{\mathrm{hom}}, \ldots, f_r^{\mathrm{hom}})$ is a homogeneous ideal in $\overline{P}$ which is contained in I^{hom}. Using induction on the degree d, we shall prove $J_d = I_d^{\mathrm{hom}}$ for all $d \geq 0$. For $d = 0$, we have $I_0^{\mathrm{hom}} = J_0 = (0)$, since $I \subset P$ means that I contains no non-zero constant polynomial. For $d > 0$, we let $G \in I_d^{\mathrm{hom}}$. By Proposition 4.3.2.h, the polynomial G is of the form $G = x_0^s (G^{\mathrm{deh}})^{\mathrm{hom}}$ for some $s \geq 0$, and Proposition 4.3.5.e implies $(G^{\mathrm{deh}})^{\mathrm{hom}} \in I_{d-s}^{\mathrm{hom}}$. Thus the claim follows from the induction hypothesis $I_{d-s}^{\mathrm{hom}} = J_{d-s}$ if $s > 0$. Hence we may assume that $s = 0$, i.e. that $G = (G^{\mathrm{deh}})^{\mathrm{hom}}$.

By assumption and Corollary 1.7.11, there are homogeneous polynomials $g_1, \ldots, g_r \in P$ of degree $\deg_W(g_i) = \deg_W(G^{\mathrm{deh}}) - \deg_W(f_i)$ such that $\mathrm{DF}_W(G^{\mathrm{deh}}) = \sum_{i=1}^r g_i \, \mathrm{DF}_W(f_i)$. Hence the polynomial $G^{\mathrm{deh}} \in P$ is of the form $G^{\mathrm{deh}} = \sum_{i=1}^r g_i f_i + h$ with a polynomial $h \in P$ whose degree is $\deg_W(h) < \deg_W(G^{\mathrm{deh}}) = d$. Using Proposition 4.3.2.c, we obtain $G = (G^{\mathrm{deh}})^{\mathrm{hom}} = \sum_{i=1}^r g_i f_i^{\mathrm{hom}} + x_0^t H$ with $t > 0$ and a homogeneous polynomial $H \in \overline{P}$ which is not divisible by x_0. Consequently, we have $H = (H^{\mathrm{deh}})^{\mathrm{hom}}$ and $x_0^t H \in I_d^{\mathrm{hom}}$. Therefore Proposition 4.3.5.e and the induction hypothesis show $H \in I_{d-t}^{\mathrm{hom}} = J_{d-t}$. Altogether, we find $G \in J_d$ as claimed. □

For instance, for a principal ideal $I = (f)$ in P, this theorem shows $I^{\mathrm{hom}} = (f^{\mathrm{hom}})$, since $\{f\}$ is a Macaulay basis of I. Exercises 8 and 9 show that both implications of this theorem can fail in the case $m \geq 2$.

Recall that Corollary 4.3.8 provides a method for computing the homogenization of an ideal using saturation. Theorem 4.3.19 can be used to compute homogenizations in another way if $m = 1$ and P is positively graded.

Corollary 4.3.20. *Given an ideal I in P, consider the following sequence of instructions.*

1) *Choose a non-singular matrix $V \in \mathrm{Mat}_n(\mathbb{Z})$ of the form $\binom{W}{W'}$, where $W' \in \mathrm{Mat}_{n-1,n}(\mathbb{Z})$.*
2) *Compute a Gröbner basis $\{g_1, \ldots, g_s\}$ of I with respect to $\mathtt{Ord}(V)$.*
3) *Return the ideal $(g_1^{\mathrm{hom}}, \ldots, g_s^{\mathrm{hom}})$ and stop.*

This is an algorithm which computes $I^{\mathrm{hom}} = (g_1^{\mathrm{hom}}, \ldots, g_s^{\mathrm{hom}})$.

Proof. It suffices to combine Corollary 4.2.16 and the theorem. □

Proposition 4.3.21. (Homogenization of Gröbner Bases) *Let σ be a term ordering on $\mathbb{T}^n$ which is compatible with $\deg_W$, let I be an ideal in P, and let $\{g_1, \ldots, g_s\}$ be a σ-Gröbner basis of I. Then $\{g_1^{\mathrm{hom}}, \ldots, g_s^{\mathrm{hom}}\}$ is a $\overline{\sigma}$-Gröbner basis of I^{hom}.*

Proof. It suffices to show that, for every non-zero homogeneous polynomial $G \in I^{\mathrm{hom}}$, there exists an index $i \in \{1, \ldots, s\}$ such that $\mathrm{LT}_{\overline{\sigma}}(G)$ is a multiple of $\mathrm{LT}_{\overline{\sigma}}(g_i^{\mathrm{hom}})$. Since $G^{\mathrm{deh}} \in I \setminus \{0\}$ by Proposition 4.3.5, and since $\{g_1, \ldots, g_s\}$ is a σ-Gröbner basis of I, we know that $\mathrm{LT}_\sigma(G^{\mathrm{deh}})$ is a multiple of $\mathrm{LT}_\sigma(g_i)$ for some $i \in \{1, \ldots, s\}$. By Lemma 4.3.16.c, it follows that $\mathrm{LT}_{\overline{\sigma}}((G^{\mathrm{deh}})^{\mathrm{hom}})$ is a multiple of $\mathrm{LT}_{\overline{\sigma}}(g_i^{\mathrm{hom}})$. Now the claim is a consequence of Proposition 4.3.2.h. □

By this proposition, the polynomials $g_1^{\mathrm{hom}}, \ldots, g_s^{\mathrm{hom}}$ computed by the algorithm of Corollary 4.3.20 are actually a Gröbner basis of I^{hom} with respect to $\overline{\sigma}$, where $\sigma = \mathtt{Ord}\binom{W}{W'}$. On the other hand, Exercise 9 shows that the proposition can fail in the case $m \geq 2$.

Our next topic is another interpretation of the homogenization process which has a decidedly more geometric flavor. The basic result is part b) of the following theorem. Notice that there exists a natural homomorphism of K-algebras $K[x_0] \longrightarrow \overline{P}/I^{\mathrm{hom}}$ which allows us to consider $\overline{P}/I^{\mathrm{hom}}$ as a $K[x_0]$-module.

Theorem 4.3.22. (Homogenization as a Free Module)
Let I be a proper ideal in P.

a) We have isomorphisms of K-algebras $\overline{P}/(I^{\mathrm{hom}} + (x_0)) \cong P/\operatorname{DF}_W(I)$ and $\overline{P}/(I^{\mathrm{hom}} + (x_0 - c)) \cong P/I$ for every $c \in K \setminus \{0\}$.

b) The ring $\overline{P}/I^{\mathrm{hom}}$ is a free $K[x_0]$-module.

Proof. First we construct the two isomorphisms in a). By Proposition 4.3.2.a, we have $f^{\mathrm{hom}}(0, x_1, \ldots, x_n) = \operatorname{DF}_W(f)$ for all $f \in P \setminus \{0\}$. Thus the preimage of $\operatorname{DF}_W(I)$ under the homomorphism $\overline{P} \longrightarrow \overline{P}$ defined by $x_0 \mapsto 0$ and $x_i \mapsto x_i$ for $i = 1, \ldots, n$ is the ideal $I^{\mathrm{hom}} + (x_0)$. This proves the first claim in a). The second isomorphism is induced by the homomorphism $\varphi : \overline{P} \longrightarrow P$ defined by $\varphi(x_0) = c$ and $\varphi(x_i) = c^{w_i} x_i$ for $i = 1, \ldots, n$. Using Proposition 4.3.2.a, we see that φ maps $f^{\mathrm{hom}} \in I^{\mathrm{hom}}$ to $c^d f$ for $f \in I \setminus \{0\}$ and $d = \deg_W(f)$. Hence φ maps $I^{\mathrm{hom}} + (x_0 - c)$ onto I.

It remains to prove that $\varphi^{-1}(I)$ is contained in $I^{\mathrm{hom}} + (x_0 - c)$. Let $f \in \overline{P}$ be a non-zero polynomial such that $g = \varphi(f) \in I$. Then the polynomial $h = c^{\deg_W(g)} f - g^{\mathrm{hom}}$ satisfies $\varphi(h) = c^{\deg_W(g)} g - c^{\deg_W(g)} g = 0$, and therefore $h = c^{\deg_W(g)} f - g^{\mathrm{hom}} \in \operatorname{Ker}(\varphi) = (x_0 - c)$. Since $c \neq 0$, we obtain $f \in I^{\mathrm{hom}} + (x_0 - c)$, as we wanted to show. Thus φ induces the desired isomorphism.

Now we prove b). We choose a term ordering σ on $\mathbb{T}^n$ which is compatible with $\deg_W$ and let $\{f_1, f_2, \ldots, f_s\}$ be a σ-Gröbner basis of I. By Macaulay's Basis Theorem 1.5.7, the residue classes of the terms in $B = \mathbb{T}^n \setminus \operatorname{LT}_\sigma\{I\}$ form a K-basis of P/I. Our goal is to show that the residue classes of the elements of B in $\overline{P}/I^{\mathrm{hom}}$ form a $K[x_0]$-basis. By Proposition 4.3.21, the set $\{f_1^{\mathrm{hom}}, \ldots, f_s^{\mathrm{hom}}\}$ is a $\overline{\sigma}$-Gröbner basis of I^{hom}. By Lemma 4.3.16.b, we have $\operatorname{LT}_\sigma(f_i) = \operatorname{LT}_{\overline{\sigma}}(f_i^{\mathrm{hom}})$ for $i = 1, \ldots, s$. Therefore it follows that the set $\mathbb{T}(x_0, \ldots, x_n) \setminus \operatorname{LT}_{\overline{\sigma}}\{I^{\mathrm{hom}}\}$ equals $\cup_{i=0}^{\infty} x_0^i B$. Hence the residue classes of the elements of this set form a K-basis of $\overline{P}/I^{\mathrm{hom}}$. Clearly, this implies that B is a basis of $\overline{P}/I^{\mathrm{hom}}$ as a $K[x_0]$-module. □

In the language of algebraic geometry, the preceding theorem says that, for any ideal $I \subset P$, the algebra homomorphism $K[x_0] \longrightarrow \overline{P}/I^{\mathrm{hom}}$ defines a **flat family** whose **special fiber** is $P/\operatorname{DF}_W(I)$ and whose **general fiber** is P/I. Since the ring $K[x_0]$ is a principal ideal domain, flatness (a concept not defined here) is equivalent to freeness (as in part b) of the theorem). Theorem 4.3.19 allows us to characterize Macaulay bases by their behaviour with respect to this flat family.

Proposition 4.3.23. (Macaulay Bases and the Flat Family)
Let I be a proper ideal in P, and let $\{f_1, \ldots, f_s\} \subseteq P$ be a system of generators of I. Then the following conditions are equivalent.

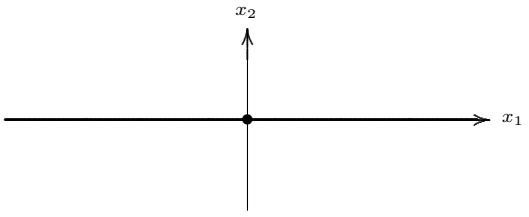
a) The set $\{f_1, \ldots, f_s\}$ is a Macaulay basis of I.
b) For every $c \in K$, the residue classes of $\{f_1^{\text{hom}}, \ldots, f_s^{\text{hom}}\}$ in the ring $\overline{P}/(x_0 - c)$ generate the ideal $(I^{\text{hom}} + (x_0 - c))/(x_0 - c)$.

Proof. By Theorem 4.3.19, condition a) implies $I^{\text{hom}} = (f_1^{\text{hom}}, \ldots, f_s^{\text{hom}})$, and hence b). Conversely, if we assume b) and apply it to the case $c = 0$, we see that $\{\text{DF}_W(f_1), \ldots, \text{DF}_W(f_s)\}$ generates $\text{DF}_W(I)$. Thus $\{f_1, \ldots, f_s\}$ is a Macaulay basis of I. □

Another way to phrase the above statement is that if these conditions hold, then the residue classes of $\{f_1^{\text{hom}}, \ldots, f_s^{\text{hom}}\}$ generate the defining ideal of every fiber of the flat family $K[x_0] \longrightarrow \overline{P}/I^{\text{hom}}$. Let us explain the geometric content of this proposition with a few examples.

Example 4.3.24. Let $P = \mathbb{Q}[x_1, x_2]$ be graded by the matrix $W = (1\ 2)$, let $f_1 = x_1^2 + x_2^2$, let $f_2 = x_1 x_2$, and let $I = (f_1, f_2)$. Then we obtain $f_1^{\text{hom}} = x_0^2 x_1^2 + x_2^2$ and $f_2^{\text{hom}} = x_1 x_2$. The ideal I corresponds geometrically to the origin $\mathcal{Z}(I) = \{(0,0)\} \subseteq \mathbb{A}^2_{\mathbb{Q}}$.

Now we look at the ideal $\tilde{I} = (f_1^{\text{hom}}, f_2^{\text{hom}})$ in $\overline{P}$ and at its residue class ideals $(\tilde{I} + (x_0 - c))/(x_0 - c) \subseteq \overline{P}/(x_0 - c) \cong P$ for various $c \in \mathbb{Q}$. If $c \neq 0$, then that residue class ideal is isomorphic to the ideal $I_c = (c^2 x_1^2 + x_2^2,\ x_1 x_2) \subseteq P$ which corresponds to $\mathcal{Z}(I_c) = \{(0,0)\}$. But if $c = 0$, then the residue class ideal is $I_0 = (x_2^2,\ x_1 x_2)$ and corresponds to the line $\mathcal{Z}(I_0) = \{(\lambda, 0) \mid \lambda \in \mathbb{Q}\}$.

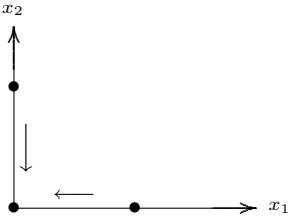


Thus the family $K[x_0] \longrightarrow \overline{P}/\tilde{I}$ has general fiber $\{(0,0)\}$, i.e. a point, and a special fiber which is a line. This means that the family is not flat. The reason is that $\{f_1, f_2\}$ is not a Macaulay basis of I. If we add the third polynomial $f_3 = x_1^3$, then $\{f_1, f_2, f_3\}$ is a Macaulay basis of I and the family $K[x_0] \longrightarrow \overline{P}/(f_1^{\text{hom}}, f_2^{\text{hom}}, f_3^{\text{hom}})$ is flat. Its special fiber $\overline{P}/(I^{\text{hom}} + (x_0)) \cong P/(x_1^3,\ x_1 x_2,\ x_2^2)$ corresponds again to the origin only, because $\mathcal{Z}((x_1^3,\ x_1 x_2,\ x_2^2)) = \{(0,0)\}$.

Example 4.3.25. Let $P = \mathbb{Q}[x_1, x_2]$ be standard graded, let $f_1 = x_1 x_2$, let $f_2 = x_1^2 - x_1$, let $f_3 = x_2^2 - x_2$, and let $I = (f_1, f_2, f_3)$. Geometrically, the ideal I corresponds to three points $\mathcal{Z}(I) = \{(0,0),\ (1,0),\ (0,1)\} \subseteq \mathbb{A}^2_{\mathbb{Q}}$.

It is easy to check that $\{f_1, f_2, f_3\}$ is a Macaulay basis of I. Thus we have $I^{\text{hom}} = (f_1^{\text{hom}}, f_2^{\text{hom}}, f_3^{\text{hom}})$.

Let us look at the family $K[x_0] \longrightarrow \overline{P}/I^{\text{hom}}$. For $c \in \mathbb{Q} \setminus \{0\}$, the fiber $\overline{P}/(I^{\text{hom}} + (x_0 - c))$ corresponds to $\mathcal{Z}((x_1x_2, x_1^2 - cx_1, x_2^2 - cx_2)) = \{(0,0), (c,0), (0,c)\}$. For $c = 0$, the fiber $\overline{P}/(I^{\text{hom}} + (x_0))$ corresponds to $\{(0,0)\}$.



Thus we can interpret the process of letting $c \longrightarrow 0$ as the process of moving the two points $(c,0)$, $(0,c)$ towards the origin. In the special fiber, the three points come together at the origin. This suggests that we should consider the special fiber as a point of **multiplicity** three, a topic which we shall examine more closely in Chapter 5.

Exercise 1. Let K be a field and $P = K[x_1, \ldots, x_n]$. Find a matrix $W \in \text{Mat}_{m,n}(\mathbb{Z})$ such that the grading defined by W is of positive type, but the grading on $K[y_1, \ldots, y_m, x_1, \ldots, x_n]$ defined by $\overline{W} = (\mathcal{I}_m | W)$ is not of positive type.

Exercise 2. Let K be an algebraically closed field, let $\overline{P} = K[x_0, x_1]$ be standard graded, let $d \geq 1$, and let $F \in \overline{P}$ be a non-zero homogeneous polynomial of degree d. Show that F admits a factorization $F = F_1 \cdots F_d$ with homogeneous polynomials $F_1, \ldots, F_d \in P_1$.

Exercise 3. In the context of Subsection 4.3.A, let $f_1, \ldots, f_s \in P$ and $I = (f_1, \ldots, f_s)$. Prove that $I^{\text{hom}} = (f_1^{\text{hom}}, \ldots, f_s^{\text{hom}}) \cdot \overline{P}_{y_1 \cdots y_m} \cap \overline{P}$ where $\overline{P}_{y_1 \cdots y_m}$ is the localization of $\overline{P}$ in the element $y_1 \cdots y_m$.

Exercise 4. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be graded by a matrix $W \in \text{Mat}_{m,n}(\mathbb{Z})$, let I_1 and I_2 be two ideals in P, and let $\overline{P} = K[y_1, \ldots, y_m, x_1, \ldots, x_n]$.

a) Show that $(I_1 + I_2)^{\text{hom}} = (I_1^{\text{hom}} + I_2^{\text{hom}}) :_{\overline{P}} (y_1 \cdots y_m)^\infty$.
b) Show that $I_1^{\text{hom}} \cdot I_2^{\text{hom}} = (I_1 \cdot I_2)^{\text{hom}}$ if I_1 and I_2 are principal ideals.

Exercise 5. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let $I \subseteq P$ be an ideal, let $f \in P$ be a non-zerodivisor for P/I, and let $\overline{P} = K[x_0, \ldots, x_n]$.

a) Show that f^{hom} is a non-zerodivisor for $\overline{P}/I^{\text{hom}}$.
b) Find an example in which the inclusion $I^{\text{hom}} + (f^{\text{hom}}) \subseteq (I + (f))^{\text{hom}}$ is strict. Under which additional hypothesis on f is this an equality?

Exercise 6. Let K be a field, and let J be a homogeneous ideal in $K[y_1, \ldots, y_m, x_1, \ldots, x_n]$. Show that J^{deh} can be a prime ideal without J having this property.

Exercise 7. In the situation of Subsection 4.3.B, let $I \subset P$ be a proper ideal in P, and let $\varphi : K[x_0] \longrightarrow \overline{P}/I^{\text{hom}}$ be the canonical ring homomorphism.

a) Show that φ is injective.
b) Prove that, for every non-zero polynomial $f \in K[x_0]$, the image $\varphi(f)$ is a non-zerodivisor in $\overline{P}/I^{\text{hom}}$.

Exercise 8. Let K be a field, and let $P = K[x_1, x_2, x_3, x_4]$ be graded by $W = \left(\begin{smallmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{smallmatrix}\right)$.

a) Using CoCoA, show that the homogenizations of the polynomials $f_1 = x_1x_2 - x_3^2$ and $f_2 = x_2^2 - x_4^2$ generate the ideal $(f_1, f_2)^{\text{hom}}$.
b) Use the polynomial $f_3 = x_1x_4^2 - x_2x_3^2$ to show that $\{f_1, f_2\}$ is not a Macaulay basis of (f_1, f_2) with respect to the grading given by W.

Exercise 9. Let K be a field, and let $P = K[x_1, x_2, x_3, x_4]$ be graded by $W = \left(\begin{smallmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{smallmatrix}\right)$.

a) Show that the polynomials $f_1 = x_1 - x_3$ and $f_2 = x_2 - x_4$ form a Macaulay basis of the ideal $I = (f_1, f_2)$ with respect to the grading given by W.
b) Use the polynomial $f_3 = x_1x_4 - x_2x_3$ to prove that $(f_1^{\text{hom}}, f_2^{\text{hom}})$ is strictly contained in I^{hom}.

Exercise 10. In the setting of Proposition 4.3.21, let G be the reduced σ-Gröbner basis of I. Prove that $G^{\text{hom}} = \{g_1^{\text{hom}}, \ldots, g_s^{\text{hom}}\}$ is the reduced $\overline{\sigma}$-Gröbner basis of I^{hom}.

Exercise 11. Let $P = \mathbb{Q}[x_1, x_2]$ be graded by the identity matrix, let $I = (x_1 + x_2, x_1^2, x_2^2)$, and let $\overline{P} = \mathbb{Q}[y_1, y_2, x_1, x_2]$. Consider $\overline{P}/I^{\text{hom}}$ as a $K[y_1, y_2]$-module via the natural homomorphism $K[y_1, y_2] \longrightarrow \overline{P}/I^{\text{hom}}$ and show that is not free.

Tutorial 49: Homogenization of Modules

I'm against a homogenized society,
because I want the cream to rise.
(Robert Frost)

The definitions in this section require only slight modification and extension in order to generalize the process of homogenization to vectors of polynomials contained in submodules of graded free modules over a graded polynomial ring. If you work out the following problems, you attain a theory of homogenization which has the same level of generality as the remainder of this chapter.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, and let F be the graded free P-module $F = \bigoplus_{i=1}^r P(-\delta_i)$. We introduce homogenizing indeterminates $y_1, \ldots, y_m$ and equip the polynomial ring $\overline{P} = K[y_1, \ldots, y_m, x_1, \ldots, x_n]$ with the grading defined by $\overline{W} = (\mathcal{I}_m \mid W)$. Then $\overline{F} = \bigoplus_{i=1}^r \overline{P}(-\delta_i)$ is a graded free $\overline{P}$-module in the natural way.

Given a vector $v \in F \setminus \{0\}$, we decompose it into its homogeneous components $v = v_1 + \cdots + v_s$, where v_i is homogeneous of degree $d_i \in \mathbb{Z}^m$. Then we let $d \in \mathbb{Z}^m$ be the componentwise maximum of $\{d_1, \ldots, d_s\}$, call it the **top degree** of v, and denote it by $\mathrm{topdeg}_W(v)$. The vector $v^{\mathrm{hom}} = y^{d-d_1}v_1 + \cdots + y^{d-d_s}v_s \in \overline{F}$ is called the **homogenization** of v with respect to the grading given by W. For $v = 0$, we set $v^{\mathrm{hom}} = 0$.

Similarly, given a vector $\overline{v} \in \overline{F}$, we write $\overline{v} = (\bar{f}_1, \ldots, \bar{f}_r)$ with polynomials $\bar{f}_1, \ldots, \bar{f}_r \in \overline{P}$. Then we call $\overline{v}^{\,\mathrm{deh}} = (\bar{f}_1^{\,\mathrm{deh}}, \ldots, \bar{f}_r^{\,\mathrm{deh}}) \in F$ the **dehomogenization** of $\overline{v}$.

a) Discuss how this definition generalizes Definition 4.3.1. In particular, show that it behaves as if the canonical basis elements e_i were *true* indeterminates of degrees δ_i for $i = 1, \ldots, r$.

b) Write a CoCoA function `IsWHomog(...)` which takes a vector in F, checks whether it is homogeneous, and returns the corresponding Boolean value.

c) Implement a CoCoA function `WDegree(...)` which takes a homogeneous vector in F or in $\overline{F}$ and returns its degree.

d) Prove the following rules for homogenizing vectors of polynomials.

   1) For all $v \in F$, we have $(v^{\mathrm{hom}})^{\mathrm{deh}} = v$.
   2) For $f \in P \setminus \{0\}$ and $v \in F \setminus \{0\}$, we have $\mathrm{topdeg}_W(fv) = \mathrm{topdeg}_W(f) + \mathrm{topdeg}_W(v)$ as well as $(fv)^{\mathrm{hom}} = (f^{\mathrm{hom}})(v^{\mathrm{hom}})$.
   3) Let $v, w, v+w \in F \setminus \{0\}$, and let d be the componentwise maximum of $d' = \mathrm{topdeg}_W(v)$ and $d'' = \mathrm{topdeg}_W(w)$. Then we have
   $$y^{d-\mathrm{topdeg}_W(v+w)} \cdot (v+w)^{\mathrm{hom}} = y^{d-d'} \cdot v^{\mathrm{hom}} + y^{d-d''} \cdot w^{\mathrm{hom}}$$
   4) For $\bar{f} \in \overline{P}$ and $\overline{v}, \overline{w} \in \overline{F}$, we have $(\bar{f}\,\overline{v})^{\mathrm{deh}} = (\bar{f}^{\mathrm{deh}})(\overline{v}^{\,\mathrm{deh}})$ and $(\overline{v} + \overline{w})^{\mathrm{deh}} = \overline{v}^{\mathrm{deh}} + \overline{w}^{\mathrm{deh}}$.
   5) Let $\overline{v} \in \overline{F} \setminus \{0\}$ be homogeneous and $s_j = \max\{i \geq 0 \mid y_j^i \text{ divides } \overline{v}\}$ for $j = 1, \ldots, m$. Then we have
   $$y_1^{s_1} \cdots y_m^{s_m} \cdot (\overline{v}^{\,\mathrm{deh}})^{\mathrm{hom}} = \overline{v}$$
   In particular, we have $\overline{v}^{\,\mathrm{deh}} \neq 0$.

e) Write CoCoA functions `WHomogenize(...)` and `WDehomogenize(...)` which take vectors in F and $\overline{F}$, respectively, and perform the appropriate operation. Use your functions to compute the following homogenizations and dehomogenizations, where we assume that $P = \mathbb{Q}[x_1, \ldots, x_n]$ is graded by W.

1) v^{hom} for $v = (x_1^2 + x_2^2,\, x_2^3) \in \mathbb{Q}[x_1, x_2] \oplus \mathbb{Q}[x_1, x_2]((-1, 0))$ graded by the matrix $W = \left(\begin{smallmatrix} 1 & 1 \\ 2 & 3 \end{smallmatrix}\right)$
2) w^{hom} for $w = (x_1^2 x_2^2,\, x_2^3 x_3^3,\, x_1 x_3) \in \mathbb{Q}[x_1, x_2, x_3]^3$ graded by the matrix $W = \left(\begin{smallmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \end{smallmatrix}\right)$
3) $\overline{v}^{\,\mathrm{deh}}$ for $\overline{v} = (x_1x_2 + x_1y_2,\, y_1^2y_2^4x_1x_2 + y_1^3y_2^4x_2) \in \mathbb{Q}[x_1, x_2]((0, -1)) \oplus \mathbb{Q}[x_1, x_2]((2, 3))$ graded by the matrix $W = \left(\begin{smallmatrix} 1 & 0 \\ -2 & 1 \end{smallmatrix}\right)$

f) Let M be a submodule of F and $\overline{M}$ a graded submodule of $\overline{F}$. Imitate Definition 4.3.4 and introduce the homogenization M^{hom} of M and the dehomogenization $\overline{M}^{\,\mathrm{deh}}$ of $\overline{M}$. Then prove the following rules governing these processes.
   1) We have $(M^{\mathrm{hom}})^{\mathrm{deh}} = M$.
   2) For a homogeneous vector $\overline{v} \in \overline{P}$, we have $\overline{v} \in M^{\mathrm{hom}}$ if and only if there exist a vector $v \in M$ and numbers $s_1, \ldots, s_m \in \mathbb{N}$ such that $\overline{v} = y_1^{s_1} \cdots y_m^{s_m}\, v^{\mathrm{hom}}$.
   3) For a homogeneous vector $\overline{v} \in \overline{P}$, we have $\overline{v}^{\,\mathrm{deh}} \in \overline{M}^{\,\mathrm{deh}}$ if and only if $(y_1 \cdots y_m)^s \cdot \overline{v} \in \overline{M}$ for some $s \geq 0$.
   4) We have $\overline{M} \subseteq (\overline{M}^{\,\mathrm{deh}})^{\mathrm{hom}} = \overline{M} :_{\overline{F}} (y_1 \cdots y_m)^\infty$.
   5) If $M \neq 0$, then $y_1 \cdots y_m$ is a non-zerodivisor for $\overline{F}/M^{\mathrm{hom}}$.
   6) If M is a proper graded submodule of F, then $M^{\mathrm{hom}} = \overline{P} \cdot M$.

g) Use these rules to derive algorithms for computing the homogenization and dehomogenization of submodules of F and $\overline{F}$, respectively. Implement these algorithms in two CoCoA functions `HomogModule`(...) and `DehomogModule`(...).

h) Using your function `HomogModule`(...), compute the homogenization of the following submodules.
   1) $M_1 = \langle (x_1x_2+1,\, x_1+x_2), (x_1^3,\, x_2^3), (x_2,\, x_1+1) \rangle \subseteq \mathbb{Q}[x_1, x_2]((-1, 0)) \oplus \mathbb{Q}[x_1, x_2]((0, -2))$ graded by $W = \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right)$
   2) $M_2 = \langle (x_1^2 + 1, 0, 0),\, (0, x_2^2 + 1, 0),\, (0, 0, x_3^2 + 1) \rangle \subseteq \mathbb{Q}[x_1, x_2, x_3]^3$ graded by $W = \left(\begin{smallmatrix} 1 & 1 & 1 \\ 1 & 2 & -1 \end{smallmatrix}\right)$

i) Let M_1, M_2 be submodules of F and $\overline{M}_1, \overline{M}_2$ graded submodules of $\overline{F}$. Prove the following rules.
   1) If $M_1 \subseteq M_2$, then we have $M_1^{\mathrm{hom}} \subseteq M_2^{\mathrm{hom}}$.
   2) We have $(M_1 \cap M_2)^{\mathrm{hom}} = M_1^{\mathrm{hom}} \cap M_2^{\mathrm{hom}}$.
   3) If $\overline{M}_1 \subseteq \overline{M}_2$, then we have $\overline{M}_1^{\mathrm{deh}} \subseteq \overline{M}_2^{\mathrm{deh}}$.
   4) We have $(\overline{M}_1 \cap \overline{M}_2)^{\mathrm{deh}} = \overline{M}_1^{\mathrm{deh}} \cap \overline{M}_2^{\mathrm{deh}}$.
   5) We have $(\overline{M}_1 + \overline{M}_2)^{\mathrm{deh}} = \overline{M}_1^{\mathrm{deh}} + \overline{M}_2^{\mathrm{deh}}$.

He who asks is a fool for five minutes,
but he who does not ask remains a fool forever.
(Chinese Proverb)

Tutorial 50: The Homogeneous Part of an Ideal

The idea of homogenization is to approximate an arbitrary polynomial ideal by a homogeneous ideal. The price we have to pay is the introduction of a number of additional indeterminates. Another way to achieve the same goal is to look at the ideal generated by the homogeneous elements in the given ideal. Using this approach we avoid extra indeterminates, but the disadvantage is that the approximation might be very bad, e.g. that the only homogeneous element inside the ideal might be zero. Nevertheless, let us see what we can do, and let us do it effectively.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let I be an ideal in P. Then the ideal I_W generated by the homogeneous polynomials in I is called the **W-homogeneous part** of I, or simply the **homogeneous part** of I if it is clear which grading we are considering.

a) Prove that $I_W = I^{\mathrm{hom}} \cap P$.
Hint: Show that both ideals are homogeneous and have the same homogeneous elements.
b) Using a), show that if I is a prime ideal, then I_W too is a prime ideal.
c) Let σ be a term ordering on $\mathbb{T}^n$. Generalize Tutorial 22.c by showing that I is a homogeneous ideal if and only if its reduced σ-Gröbner basis is homogeneous with respect to the grading given by W.
d) Let $P = K[x_1, \ldots, x_n]$ be standard graded. Find an ideal $I \subseteq P$ such that I_W strictly contains the ideal generated by the homogeneous elements in some reduced Gröbner basis of I.
e) Combine the results obtained so far and develop an algorithm for computing I_W. Implement this algorithm in a CoCoA function `HomogPart(...)` which computes the homogeneous part of an ideal.
Hint: Use the reduced Gröbner basis of I^{hom} with respect to an elimination ordering for $\{y_1, \ldots, y_m\}$.
f) Apply your function `HomogPart(...)` to compute the homogeneous parts of the following ideals with respect to the gradings given by the stated matrices.
   1) $I_1 = (x_1^2 - x_1,\ x_2^2 - x_1) \subseteq \mathbb{Q}[x_1, x_2]$ graded by $W = (1\ 1)$
   2) $I_2 = (x_1x_2 - 1,\ 2x_1^3x_2 + x_2^3 - x_1^2) \subseteq \mathbb{Q}[x_1, x_2]$ graded by $W = \left(\begin{smallmatrix} 3 & 2 \\ 1 & 0 \end{smallmatrix}\right)$
   3) $I_3 = (x_1x_2x_3 + x_1 + x_2,\ x_1x_2 + x_2^2 + x_2x_3,\ x_1^2x_2^2x_3 + 2x_1 + 2x_2) \subseteq \mathbb{Q}[x_1, x_2, x_3]$ graded by $W = \left(\begin{smallmatrix} 1 & 1 & 2 \\ 3 & 3 & -1 \end{smallmatrix}\right)$
g) The ideal generated by the terms in I is called the **monomial part** of I and will be denoted by I_{mon}. Explain how one can use the preceding results in order to compute I_{mon}. Write a CoCoA function `MonomialPart(...)` which does this.
h) Compute the monomial parts of the following ideals.
   1) $J_1 = (x_1x_2 + x_1,\ x_1^2x_2^2 + x_1^2x_2 + x_1^2) \subseteq \mathbb{Q}[x_1, x_2]$
   2) $J_2 = (x_1^2 + 2x_2^2,\ 2x_1^2 + 2x_1x_2 + x_2^2,\ x_1x_2 + 2x_2^2) \subseteq \mathbb{Q}[x_1, x_2]$

3) $J_3 = (x_1x_2^2x_3 + x_1x_2x_3,\ x_1x_2^2x_3 + x_2^2x_3,\ x_1^2x_2^3x_3 + x_1^2x_2 + x_1x_2x_3,\ x_1^5x_2^5x_3) \subseteq \mathbb{Q}[x_1, x_2, x_3]$

i) Let $w_1, \ldots, w_m$ be the the rows of W. We can consider them as matrices in $\mathrm{Mat}_{1,n}(\mathbb{Z})$. Show that we have $I_W = (\cdots((I_{w_1})_{w_2})\cdots)_{w_m}$.

j) Prove that $I_W \subseteq \bigcap_{i=1}^m I_{w_i}$ and that this inclusion may be strict. (*Hint:* Consider the ideal $(x^2 + y,\ x + y^2)$ in $\mathbb{Q}[x, y]$.)

k) Using i), implement a second function `HomogPart2(...)`, apply it in the cases of f), and compare the results.

l) Compute the determinant of the matrix

$$W = \begin{pmatrix} 2 & 1 & \ldots & 1 \\ 1 & 2 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & 2 \end{pmatrix} \in \mathrm{Mat}_n(\mathbb{Z})$$

Use this matrix together with i) to write a function `MonomialPart2(...)` which computes I_{mon} in an alternative way. Apply your function in the cases of h) and compare the results.

Tutorial 51: Implicitization and Homogenization

In the current chapter it has been one of our dicta that many computations can be performed more efficiently in a homogeneous setting. To make this principle come alive, we now look at the computation of implicitizations using the technique of homogenizing, performing a homogeneous computation, and dehomogenizing again. In Section 3.6 we defined the implicitization of a tuple of polynomials $(f_1, \ldots, f_n) \in K[y_1, \ldots, y_m]^n$ as the ideal of all algebraic relations among them. Corollary 3.6.3 gives us a concrete method for computing this ideal: form the diagonal ideal $J = (x_1 - f_1, \ldots, x_n - f_n)$ in $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and use elimination to get the implicitization $J \cap K[x_1, \ldots, x_n]$.

Now we propose another way of computing such implicitizations. We introduce a homogenizing indeterminate x_0 and equip the polynomial ring $\overline{Q} = K[x_0, \ldots, x_n, y_1, \ldots, y_m]$ with a suitable grading which makes the ideal $\overline{J} = (x_1 - f_1^{\mathrm{hom}}, \ldots, x_n - f_n^{\mathrm{hom}})$ homogeneous. The we compute a homogeneous Gröbner basis of $\overline{J} \cap K[x_0, \ldots, x_n]$ and find $J \cap K[x_1, \ldots, x_n]$ by dehomogenizing it. We will guide you through a proof of the correctness of this technique, ask you to implement it and to compare it to the former method. In the second part of the tutorial, we introduce a variation of this algorithm which computes the homogenization of the implicitization with respect to the standard grading. An optimization of this algorithm is contained in Tutorial 69.

Let K be a field, let $P = K[x_1, \ldots, x_n]$, let $P' = K[y_1, \ldots, y_m]$, and let $f_1, \ldots, f_n \in P' \setminus \{0\}$. We equip P with the grading given by the matrix

$W = (d_1 \ \cdots \ d_n)$, where d_i is the degree of f_i with respect to the standard grading. Our goal is to show that we can compute the implicitization of $f_1, \ldots, f_n$ by performing the following steps.

1) Form the polynomial ring $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and the ideal $J = (x_1 - f_1, \ldots, x_n - f_n)$ in Q.
2) Form the polynomial ring $\overline{P} = K[x_0, \ldots, x_n]$ and equip it with the grading given by $\overline{W} = (1 \ d_1 \ \cdots \ d_n)$.
3) Form the polynomial ring $\overline{Q} = K[x_0, \ldots, x_n, y_1, \ldots, y_m]$ and equip it with the grading given by $\widetilde{W} = (1 \ d_1 \ d_2 \ \cdots \ d_n \ 1 \ \cdots 1)$.
4) For $i = 1, \ldots, n$, compute the homogenization f_i^{hom} of f_i with respect to x_0. Then form the ideal $\overline{J} = (x_1 - f_1^{\text{hom}}, \ldots, x_n - f_n^{\text{hom}})$ in $\overline{Q}$.
5) Compute the elimination ideal $\overline{I} = \overline{J} \cap \overline{P}$.
6) Return the ideal $I = \overline{I}^{\text{deh}}$.

In the following, you will prove that $I = J \cap P$, i.e. that I is the implicitization of J. Moreover, we shall see that $\overline{I}$ is the homogenization of I with respect to the grading given by W.

a) Show that $\overline{J} \cap \overline{P}$ is a homogeneous ideal in $\overline{P}$.
b) Using Proposition 3.6.1.a, prove that $\overline{J}$ is a prime ideal.
c) Using b), show that the ideal $\overline{J} \cap \overline{P}$ is saturated with respect to x_0.
d) Prove that the homogenization of J with respect to x_0 is given by $\overline{J}$. (*Hint:* Use Corollary 4.3.8.)
e) Finally, use Corollary 4.3.7 to prove that $(J \cap P)^{\text{hom}} = \overline{J} \cap \overline{P}$, where P is graded by W and x_0 is the homogenizing indeterminate.
f) Write a CoCoA function `Implicit(...)` which takes $(f_1, \ldots, f_n)$ and computes the implicitization $J \cap P$ using the above method.
g) Apply your function `Implicit(...)` to compute the implicitizations of the following tuples of polynomials. Compare the timings of your function to the timings of the built-in CoCoA command `Elim`.
   1) $(y_1^5 + y_1y_2 + y_2, \ y_1^4 + y_1y_2^2 - y_1 - 1, \ y_1^3 + y_2)$ in $\mathbb{Z}/(101)[y_1, y_2]$
   2) $(y_1^7 + y_1y_2 + y_2, \ y_1^4 + y_1y_2^2 - y_1 - 1, \ y_1^3 + y_2)$ in $\mathbb{Z}/(101)[y_1, y_2]$
   3) $(y_1^5 + y_1y_2 + y_2, \ y_1^4 + y_1y_2^2 - y_1 - 1, \ y_1^3 + y_2)$ in $\mathbb{Q}[y_1, y_2]$
   4) $(y_1^7 + y_1y_2 + y_2, \ y_1^4 + y_1y_2^2 - y_1 - 1, \ y_1^3 + y_2)$ in $\mathbb{Q}[y_1, y_2]$

In the second part of this tutorial, we start with the same setting, but we want to compute the homogenization of the implicitization $J \cap P$ with respect to the standard grading on P. In this case, we can modify the above steps as follows.

1') Form the polynomial ring $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and the ideal $J = (x_1 - f_1, \ldots, x_n - f_n)$ in Q.
2') Form the polynomial ring $\overline{P} = K[x_0, \ldots, x_n]$ and equip it with the standard grading.
3') Form the polynomial ring $\overline{Q} = K[x_0, \ldots, x_n, y_0, \ldots, y_m]$ and equip it with the grading given by the matrix $\widetilde{W} = (d \ d \ \cdots \ d \ 1 \ \cdots 1)$, where $d = \max\{d_1, \ldots, d_n\}$ is repeated $n + 1$ times.

4') For $i = 1, \ldots, n$, compute the homogenization f_i^{hom} of f_i with respect to y_0. Form the ideal $\overline{J} = (x_0 - y_0^d, x_1 - y_0^{d-d_1} f_1^{\text{hom}}, \ldots, x_n - y_0^{d-d_n} f_n^{\text{hom}})$ in $\overline{Q}$.
5') Compute the elimination ideal $\overline{I} = \overline{J} \cap \overline{P}$.

In a manner which is similar to the method above we want to show the formula $\overline{I} = (J \cap P)^{\text{hom}}$. This gives us an efficient way of computing the homogenization with respect to the standard grading of the implicitization $J \cap P$, since we have to compute only one Gröbner basis in a homogeneous setting.

h) Show that $\overline{J} \cap \overline{P}$ is homogeneous with respect to the standard grading.
i) Using b), show that the ideal $\overline{J} \cap \overline{P}$ is saturated with respect to x_0.
j) Prove that the homogenization of J with respect to y_0 is the ideal $(x_1 - y_0^{d-d_1} f_1^{\text{hom}}, \ldots, x_n - y_0^{d-d_n} f_n^{\text{hom}})$. (*Hint:* Use Corollary 4.3.8.)
k) Now show that $J \cap P = (\overline{J} \cap \overline{P})^{\text{deh}}$, where the dehomogenization is formed with respect to x_0.
Hint: Prove the two inclusions. For the proof of "$\subseteq$", equip P with the grading given by $(d \cdots d)$, homogenize $f \in J \cap P$ with respect to y_0 and substitute $y_0^d \mapsto x_0$ in f^{hom}. For the proof of "$\supseteq$", use the substitution $x_0 \mapsto 1,\ y_0 \mapsto 1$.
l) Finally, use Corollary 4.3.7 to prove that $(J \cap P)^{\text{hom}} = \overline{J} \cap \overline{P}$, where P is standard graded and x_0 is the homogenizing indeterminate.
m) Write a CoCoA function `HomImplicit(...)` which takes $(f_1, \ldots, f_n)$ and computes the homogenization of the implicitization $J \cap P$ with respect to the standard grading using steps 1') – 5').
n) Apply your function `HomImplicit(...)` to the examples in g) and measure the timings.

Tutorial 52: Projective Closure

The geometric interpretation of the process of homogenizing a polynomial ideal under the standard grading is the process of forming the projective closure of an affine variety. Furthermore, the geometric interpretation of the process of dehomogenizing a polynomial ideal is the process of passing to the affine part of a projective variety. In this tutorial, we want to study these processes from the geometric point of view.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ and $\overline{P} = K[x_0, \ldots, x_n]$ be standard graded, let $\overline{K}$ be the algebraic closure of K, and let $\mathbb{A}^n$ (resp. $\mathbb{P}^n$) be the n-dimensional affine (resp. projective) space over $\overline{K}$.

a) Show that, for $i = 0, \ldots, n$, there exists an injective map $\imath_i : \mathbb{A}^n \longrightarrow \mathbb{P}^n$ defined by $(p_1, \ldots, p_n) \mapsto (p_1 : \ldots : p_i : 1 : p_{i+1} : \ldots : p_n)$, where the "1" occurs in the $(i+1)^{\text{st}}$ position.
b) Prove that $\mathbb{P}^n$ is covered by the images of $\imath_0, \ldots, \imath_n$.

In the following, we shall identify $\mathbb{A}^n$ with its image U under the map $\imath_0$. Thus, for a projective variety $W \subseteq \mathbb{P}^n$, we can consider $W \cap U$ as a subset of $\mathbb{A}^n$. We call $W \cap U$ the **affine part** of W.

c) Let $J \subseteq \overline{P}$ be a homogeneous ideal which defines a non-empty projective variety $W = \mathcal{Z}^+(J) \subseteq \mathbb{P}^n$. Prove that the affine part of W is the affine variety defined by J^{deh}.

Now let I be an ideal in P, and let $V = \mathcal{Z}(I)$ be the affine variety in $\mathbb{A}^n$ defined by I. Then the projective variety $\overline{V} = \mathcal{Z}^+(I^{\mathrm{hom}}) \subseteq \mathbb{P}^n$ is called the **projective closure** of V.

d) Show that $\overline{V} \cap U = V$ and that $\overline{V}$ is the smallest projective variety whose affine part contains V.

e) Prove that the homogeneous vanishing ideal of $\overline{V}$ is $\mathcal{I}(V)^{\mathrm{hom}}$.

f) Write a CoCoA function `ProjClosure(...)` which takes I and computes the ideal I^{hom} which defines the projective closure of $\mathcal{Z}(I)$. Use your function to compute the projective closure of the following affine varieties. (In each case, you will have to find the vanishing ideal first.)

1) $V_1 = \{(t^3, t^4, t^5) \mid t \in \overline{K}\} \subseteq \mathbb{A}^3$
2) $V_2 = \{(t, u, t^2, tu, u^2) \mid t, u \in \overline{K}\} \subseteq \mathbb{A}^5$ (This is the **Veronese surface** which we first met in Tutorial 39.g.)
3) $V_3 = \{(t, u, v, tu, tv) \mid t, u, v \in \overline{K}\} \subseteq \mathbb{A}^5$

The variety $H^{\mathrm{inf}} = \mathcal{Z}^+(x_0)$ in $\mathbb{P}^n$ is called the **hyperplane at infinity**. Let $W \subseteq \mathbb{P}^n$ be a non-empty projective variety defined by a homogeneous ideal $J \subseteq \overline{P}$. The points in $W^{\mathrm{inf}} = W \cap H^{\mathrm{inf}}$ are called the **points at infinity** of W.

g) Show that H^{inf} is the complement of U in $\mathbb{P}^n$, and that it can be identified with $\mathbb{P}^{n-1}$.

h) Prove that W^{inf} is the projective variety in $\mathbb{P}^{n-1}$ defined by the ideal obtained by setting $x_0 = 0$ in the polynomials in J.

i) Compute the points at infinity of the projective closure of the **twisted cubic curve** $C = \mathcal{Z}((x_1^2 - x_2, x_1^3 - x_3)) \subseteq \mathbb{A}^3$. Then determine the set of points at infinity of the projective variety $\mathcal{Z}^+((x_1^2 - x_0x_2, x_1^3 - x_0^2x_3))$ in $\mathbb{P}^3$ obtained by homogenizing the generators of the defining ideal of C. Compare and explain your findings.

4.4 Term Orderings of DegRev Type

Mathematics is ...
the systematic misuse of a nomenclature
developed for that specific purpose
(Anonymous)

In the previous section we saw that if we want to homogenize an ideal in a standard graded polynomial ring, we need an extra indeterminate which then plays a special role. In Volume 1 we encountered several other situations where a particular indeterminate becomes the focus of our attention. For instance, in Sections 3.4 and 3.5 we computed intersections, colon modules, and saturations by introducing a *tag variable*. In Tutorials 37 and 38 we found an efficient way to calculate toric ideals using the saturation with respect to an indeterminate.

What is the common thread connecting these phenomena? Is there any advantage if we want to perform such operations and know that we are dealing with a graded situation? Of course, there is. Otherwise, would we be asking such rhetorical questions? In fact, we shall introduce a new nomenclature for that specific purpose: a module term ordering is of x_i-DegRev type if it acts with respect to x_i in the same way as `DegRevLex` does with respect to x_n. In other words, if the leading term of some homogeneous vector v is divisible by x_i, all terms in the support of v should be divisible by x_i. Notice that this generalizes the corresponding property of `DegRevLex` (see Corollary 1.5.12).

So, what are the advantages of this new terminology? Is it merely intended to misuse you, our kind reader? Our answer is an unequivocal "no". After presenting you with a plethora of examples of term orderings of x_i-DegRev type, we show how we can use them in many common cases to compute colon ideals and saturations in a simple manner. Applications include a homogeneous non-zerodivisor test, yet another way of computing homogenizations, and a homogeneous radical membership test.

Moreover, we can quickly add an indeterminate to a graded submodule (see Proposition 4.4.17) or reduce it modulo some indeterminate (see Proposition 4.4.18). Geometrically, the last process corresponds to taking a hyperplane section of an algebraic variety. This is one of the reasons for the popularity of `DegRevLex` among algebraic geometers. But even a *pure* computational commutative algebraist (i.e. a personified oxymoron) will enjoy our final Corollary 4.4.19 which says that if you plug $x_i = 0$ into a reduced Gröbner basis and if your module term ordering is of x_i-DegRev type, the result is again a reduced Gröbner basis.

After all this advertising hype, it is high time to get going and offer our new nomenclature for your delectation.

Let K be a field, let $m, n, r \geq 1$, let $P = K[x_1, \ldots, x_n]$ be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of rank m, let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, and let M be a graded P-submodule of the graded free P-module $F = \bigoplus_{i=1}^{r} P(-\delta_i)$. The

canonical basis of this graded free module will be denoted by $\{e_1, \ldots, e_r\}$. We have $\deg_W(e_i) = \delta_i$ for $i = 1, \ldots, r$.

In the following we shall denote the exponent of an indeterminate x_i in a term $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathbb{T}^n$ by $\log_{x_i}(t)$. In other words, for $i = 1, \ldots, n$, we let $\log_{x_i}(t) = \alpha_i$. The following definition introduces the central notion of this section.

Definition 4.4.1. Let $i \in \{1, \ldots, n\}$. We say that a module term ordering σ on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ is of $\boldsymbol{x_i}$**-DegRev type** if it satisfies the following conditions:

a) The ordering σ is compatible with $\deg_W$.
b) Let $t, t' \in \mathbb{T}^n$ and $j, k \in \{1, \ldots, r\}$. If the terms $te_j, t'e_k \in \mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ satisfy $\deg_W(te_j) = \deg_W(t'e_k)$ and $\log_{x_i}(t) < \log_{x_i}(t')$, then we have $te_j >_\sigma t'e_k$.

This definition implies that for two terms of the same degree, one of which is divisible by x_i and one of which is not, the former one is the *smaller* one. Furthermore, recall that a term ordering compatible with $\deg_W$, and hence a term ordering of DegRev type exists only if the grading given by W is non-negative (see Proposition 4.2.3 and Exercise 2).

To get a feeling for this new notion, we consider a few examples. The archetypal term ordering of DegRev type is `DegRevLex`.

Example 4.4.2. Let P be standard graded. The term ordering `DegRevLex` on $\mathbb{T}^n$ is of x_n-DegRev type, since it is degree compatible and, for all terms $t, t' \in \mathbb{T}^n$ of the same degree, $\log_{x_n}(t) < \log_{x_n}(t')$ implies $t >_{\texttt{DegRevLex}} t'$.

The term ordering `DegRevLex` can be generalized to a module term ordering in the following way.

Example 4.4.3. For $r \geq 1$, we can define an ordering τ on the set of terms $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ of the graded free module F by defining $te_j \geq_\tau t'e_k$ if we have

1) $\deg_W(te_j) > \deg_W(t'e_k)$, or
2) $\deg_W(te_j) = \deg_W(t'e_k)$ and $t >_{\texttt{RevLex}} t'$, or
3) $\deg_W(te_j) = \deg_W(t'e_k)$ and $t = t'$ and $j \leq k$.

It is easy to check that this defines a module term ordering τ on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. It is of x_n-DegRev type, since for two terms $te_j, t'e_k$ of the same degree we have that $\log_{x_n}(t) < \log_{x_n}(t')$ implies $t >_{\texttt{RevLex}} t'$, and therefore $te_j >_\tau t'e_k$. We shall call τ the **degree-reverse-lexicographic module term ordering** with respect to the grading given by W.

Other examples of term orderings of DegRev type follow from Definition 4.3.13.

Example 4.4.4. Let P be non-negatively graded by $W \in \mathrm{Mat}_{1,n}(\mathbb{Z})$, let $\overline{P} = K[x_0, \ldots, x_n]$ be graded by $\overline{W} = (1 \mid W)$, and let σ be a term ordering

on $\mathbb{T}(x_1, \ldots, x_n)$ which is compatible with $\deg_W$. Then the extension $\overline{\sigma}$ of σ by W is a term ordering of x_0-DegRev type on $\mathbb{T}(x_0, \ldots, x_n)$.

Firstly, $\overline{\sigma}$ is a term ordering by Proposition 4.3.14.b. Secondly, it is compatible with $\deg_{\overline{W}}$ by Proposition 4.3.14.a. Finally, given two terms $t_1, t_2 \in \mathbb{T}(x_0, \ldots, x_n)$ such that $\deg_{\overline{W}}(t_1) = \deg_{\overline{W}}(t_2)$ and such that $\log_{x_0}(t_1) < \log_{x_0}(t_2)$, it follows that $\deg_W({t_1}^{\mathrm{deh}}) > \deg_W({t_2}^{\mathrm{deh}})$. Then we have $t_1 >_\sigma t_2$, since σ is compatible with $\deg_W$.

It is easy to construct term orderings of x_i-DegRev type on $\mathbb{T}^n$ for various $i \in \{1, \ldots, n\}$ as follows.

Example 4.4.5. Let $r = 1$ and $\delta_1 = 0$.

a) Let $w_1, \ldots, w_n$ be positive integers, and let V be the matrix

$$V = \begin{pmatrix} w_1 & w_2 & \cdots & w_{n-1} & w_n \\ -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

Then the term ordering $\sigma = \mathtt{Ord}(V)$ is of x_1-DegRev type with respect to the grading given by $W = (w_1, \ldots, w_n)$.

b) On $\mathbb{T}^2$, the term ordering represented by the matrix $V = \left(\begin{smallmatrix} 1 & 2 \\ 1 & 0 \end{smallmatrix}\right)$ is of x_2-DegRev type with respect to the grading given by $W = (1\ 2)$.

By Proposition 4.2.3, a degree compatible module term ordering exists only if the grading given by W is non-negative. But the existence of a degree compatible module term ordering is not enough to guarantee that there is a term ordering of DegRev type (see Exercise 3). On the other hand, given a degree compatible module term ordering, we can characterize whether it is of DegRev type in analogy with the characterization of `DegRevLex` in Corollary 1.5.12.

Proposition 4.4.6. *Let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ which is compatible with $\deg_W$, and let $i \in \{1, \ldots, n\}$. Then the following conditions are equivalent.*

a) The ordering σ is of x_i-DegRev type.

b) If a homogeneous vector $v \in F \setminus \{0\}$ has a leading term $\mathrm{LT}_\sigma(v)$ which is divisible by x_i^ℓ for some positive integer ℓ, the entire vector v is divisible by x_i^ℓ, i.e. it is contained in $x_i^\ell F$.

Proof. First we show that a) implies b). Let $\mathrm{LT}_\sigma(v) = te_j$ with $t \in \mathbb{T}^n$ and $j \in \{1, \ldots, r\}$, and let $s \geq 1$ be the largest number such that $x_i^s \mid t$. For $t'e_k \in \mathrm{Supp}(v)$, we have $t'e_k \leq_\sigma \mathrm{LT}_\sigma(v)$ and $\deg_W(t'e_k) = \deg_W(\mathrm{LT}_\sigma(v))$. Therefore it follows that $\log_{x_i}(t') \geq \log_{x_i}(t) = s$, i.e. that $x_i^s \mid t'$. Altogether, this shows that v is a multiple of x_i^s.

Conversely, let $te_j, t'e_k \in \mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ be two terms of the same degree $\deg_W(te_j) = \deg_W(t'e_k)$. Moreover, let $s = \log_{x_i}(t)$ and $s' = \log_{x_i}(t')$. We have to show that $s < s'$ implies $te_j >_\sigma t'e_k$. By dividing both sides of this inequality by x_i^s, we see that we may assume $s = 0$. Then $v = te_j + t'e_k$ satisfies $x_i \nmid t$ and $x_i \mid t'$. By assumption, this yields $\mathrm{LT}_\sigma(v) = te_j$. Hence we get $te_j >_\sigma t'e_k$, as we had claimed. □

One of the main uses of module term orderings of DegRev type is to compute certain colon modules and saturations in a particularly simple way. Notice that, given a submodule $M \subseteq F$ and an ideal I, we always have $\mathrm{LT}_\sigma(M :_F I) \subseteq \mathrm{LT}_\sigma(M) :_F I$, but this containment is generally strict (see Exercise 5). In part b) of the following theorem and in several other results of this section, we assume that we are given a homogeneous Gröbner basis of a graded module. This is not a restrictive assumption, because, as we shall see in the next section, the application of Buchberger's Algorithm 2.5.5 to a homogeneous system of generators yields a homogeneous Gröbner basis.

Theorem 4.4.7. (Colon by a Power of an Indeterminate)
Let M be a non-zero graded submodule of F, let $i \in \{1, \ldots, n\}$, let σ be a module term ordering of x_i-DegRev type on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$, and let $\ell \in \mathbb{N}$.

a) We have $\mathrm{LT}_\sigma(M :_F (x_i^\ell)) = \mathrm{LT}_\sigma(M) :_F (x_i^\ell)$.
b) Let $G = \{g_1, \ldots, g_s\}$ be a homogeneous σ-Gröbner basis of M. Then let $a_j = \max\{\alpha \mid x_i^\alpha$ divides $g_j\}$, let $b_j = \min\{a_j, \ell\}$, and let $g'_j = g_j/x_i^{b_j}$ for $j = 1, \ldots, s$. Under these conditions $\{g'_1, \ldots, g'_s\}$ is a homogeneous σ-Gröbner basis of $M :_F (x_i^\ell)$.

Proof. First we show a). Since "$\subseteq$" holds generally, we only need to show the inclusion "$\supseteq$". Let $v \in F$ be a non-zero homogeneous vector such that $x_i^\ell v \in \mathrm{LT}_\sigma(M)$. Since $\mathrm{LT}_\sigma(M)$ is a monomial module, we have $x_i^\ell te_k \in \mathrm{LT}_\sigma(M)$ for all terms $te_k \in \mathrm{Supp}(v)$. Let te_k be one of those terms. By Proposition 1.5.6.a, there exists a homogeneous element $w \in M$ such that $x_i^\ell te_k = \mathrm{LT}_\sigma(w)$. By Proposition 4.4.6, the vector w is divisible by x_i^ℓ, i.e. it is of the form $w = x_i^\ell w'$ for some $w' \in F$. Then $x_i^\ell te_k = \mathrm{LT}_\sigma(w) = \mathrm{LT}_\sigma(x_i^\ell w') = x_i^\ell \mathrm{LT}_\sigma(w')$ shows that $te_k = \mathrm{LT}_\sigma(w') \in \mathrm{LT}_\sigma(M :_F (x_i^\ell))$. Since te_k was an arbitrary element of $\mathrm{Supp}(v)$, it follows that $v \in \mathrm{LT}_\sigma(M :_F (x_i^\ell))$.

In order to show b), we first prove that $\langle \mathrm{LT}_\sigma(g_j)\rangle :_F (x_i^\ell) = \langle \mathrm{LT}_\sigma(g'_j)\rangle$ for $j = 1, \ldots, s$. Since $x_i^\ell \mathrm{LT}_\sigma(g'_j) = \mathrm{LT}_\sigma(x_i^\ell g'_j) \in \langle \mathrm{LT}_\sigma(g_j)\rangle$, only the inclusion "$\subseteq$" needs to be shown. Let $te_k \in \mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ be a term such that we have $x_i^\ell te_k \in \langle \mathrm{LT}_\sigma(g_j)\rangle$, where $t \in \mathbb{T}^n$ and $k \in \{1, \ldots, r\}$. Thus there exists a term $t' \in \mathbb{T}^n$ such that $x_i^\ell te_k = t' \mathrm{LT}_\sigma(g_j)$, and there are two possibilities. If $\ell \leq a_j$, we have $te_k = t' x_i^{a_j - \ell} \mathrm{LT}_\sigma(g'_j)$. Otherwise $\ell > a_j$, and we have $x_i^{\ell - a_j} te_k = t' \mathrm{LT}_\sigma(g'_j)$. In this case x_i does not divide g'_j. Therefore it does not divide $\mathrm{LT}_\sigma(g'_j)$ by Proposition 4.4.6. Hence we have $te_k = t'' \mathrm{LT}_\sigma(g'_j)$, where t'' is defined by $t' = x_i^{\ell - a_j} t''$. In both cases it follows that we have

$te_k \in \langle \mathrm{LT}_\sigma(g'_j)\rangle$. Since $\langle \mathrm{LT}_\sigma(g_j)\rangle :_F (x_i^\ell)$ is a monomial module, this proves the desired inclusion.

At this point we prove claim b) by showing that $\mathrm{LT}_\sigma(M :_F (x_i^\ell)) = \langle \mathrm{LT}_\sigma(g'_1), \ldots, \mathrm{LT}_\sigma(g'_s)\rangle$. Using a), we get $\mathrm{LT}_\sigma(M :_F (x_i^\ell)) = \mathrm{LT}_\sigma(M) :_F (x_i^\ell)$. The latter coincides with $\langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\rangle :_F (x_i^\ell)$, since $\{g_1, \ldots, g_s\}$ is a σ-Gröbner basis of M. This module in turn equals $\langle \mathrm{LT}_\sigma(g'_1), \ldots, \mathrm{LT}_\sigma(g'_s)\rangle$ by what we proved above and the fact that $\langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\rangle$ is a monomial module. □

The case when $\ell = 1$ in this theorem deserves special mention. It yields a simple test for deciding when an indeterminate is a non-zerodivisor for a graded P-module of the form F/M.

Corollary 4.4.8. (Colon by an Indeterminate)
Let M be a non-zero, graded submodule of F, let $i \in \{1, \ldots, n\}$, and let σ be a module term ordering of x_i-DegRev type on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. Moreover, let $G = \{g_1, \ldots, g_s\}$ be a homogeneous σ-Gröbner basis of M, and for each $j \in \{1, \ldots, s\}$ let

$$g'_j = \begin{cases} g_j/x_i & \text{if } g_j \text{ is a multiple of } x_i, \\ g_j & \text{otherwise.} \end{cases}$$

a) The set $\{g'_1, \ldots, g'_s\}$ is a homogeneous σ-Gröbner basis of $M :_F (x_i)$.
b) Let G be the reduced σ-Gröbner basis of M. The indeterminate x_i is a non-zerodivisor for the graded P-module F/M if and only if none of the elements in G is divisible by x_i.

Proof. Claim a) is a special case of the theorem. To prove b), it suffices to note that x_i is a non-zerodivisor for F/M if and only if $M :_F (x_i) = M$ and to apply a). □

In a similar manner we can use term orderings of DegRev type to compute the saturation of a module by an indeterminate.

Corollary 4.4.9. (Saturation by an Indeterminate)
Let M be a non-zero graded submodule of F, let $i \in \{1, \ldots, n\}$, and let σ be a module term ordering of x_i-DegRev type on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$.

a) We have $\mathrm{LT}_\sigma(M :_F (x_i)^\infty) = \mathrm{LT}_\sigma(M) :_F (x_i)^\infty$.
b) Let $G = \{g_1, \ldots, g_s\}$ be a homogeneous σ-Gröbner basis of M. For $j = 1, \ldots, s$, let $a_j = \max\{\alpha \in \mathbb{N} \mid x_i^\alpha \text{ divides } g_j\}$ and $g'_j = g_j/x_i^{a_i}$. Then $\{g'_1, \ldots, g'_s\}$ is a homogeneous σ-Gröbner basis of $M :_F (x_i)^\infty$.

Proof. By Proposition 3.5.9, we have $M :_F (x_i)^\infty = M :_F (x_i)^\ell$ for sufficiently large $\ell \in \mathbb{N}$. Thus claim a) follows from Theorem 4.4.7.a. To prove b), we let $\ell \in \mathbb{N}$ be large enough so that $M :_F (x_i)^\infty = M :_F (x_i)^\ell$. Then we have $\ell \geq \max\{a_1, \ldots, a_s\}$, and the claim follows from Theorem 4.4.7.b. □

More generally, we can use the same idea to compute the colon module of M by the principal ideal generated by a homogeneous polynomial. The necessary module term ordering of DegRev type is provided by the following lemma. (For a special case of this lemma, see Example 4.4.4.)

Lemma 4.4.10. *Let P be non-negatively graded by W, let $d \in \mathbb{Z}^m$ be a degree vector which satisfies $d >_{\mathtt{Lex}} 0$, and let $\overline{P} = K[x_0, \ldots, x_n]$ be graded by $\overline{W} = (d \mid W)$. Then there exists a module term ordering on the set of terms of the graded free $\overline{P}$-module $\overline{F} = \bigoplus_{i=1}^{r} \overline{P}(-\delta_i)$ which is of x_0-DegRev type.*

Proof. Since W has $\mathbb{Z}$-linearly independent rows, the same holds for the row vectors $\overline{w}_1, \ldots, \overline{w}_m$ of $\overline{W}$, and also for the set $\{\overline{w}_1, \ldots, \overline{w}_m, -e_1\}$. Therefore we can find indices $i_1, \ldots, i_{n-m} \in \{2, \ldots, n+1\}$ such that the matrix $V \in \mathrm{Mat}_{n+1}(\mathbb{Z})$ whose rows are $\overline{w}_1, \ldots, \overline{w}_m, -e_1, e_{i_1}, \ldots, e_{i_{n-m}}$ is non-singular. By the hypotheses on W and d, the ordering $\tau = \mathtt{Ord}(V)$ is a term ordering on $\mathbb{T}^{n+1} = \mathbb{T}(x_0, \ldots, x_n)$. Moreover, the term ordering τ is clearly of x_0-DegRev type.

Generalizing Example 4.4.3, we now define a module ordering σ on $\mathbb{T}^{n+1}\langle e_1, \ldots, e_r\rangle$ by $te_j \geq_\sigma t'e_k$ for $t, t' \in \mathbb{T}^{n+1}$ and $j, k \in \{1, \ldots, r\}$ if we have

1) $\deg_W(te_j) > \deg_W(t'e_k)$, or
2) $\deg_W(te_j) = \deg_W(t'e_k)$ and $t >_\tau t'$, or
3) $\deg_W(te_j) = \deg_W(t'e_k)$ and $t = t'$ and $j \leq k$.

As in Example 4.4.3, we see that σ is a module term ordering of x_0-DegRev type with respect to the grading on $\overline{F}$ defined by $\overline{W}$. □

In view of this lemma, the assumptions of the following theorem can always be satisfied.

Theorem 4.4.11. (Colon by a Power of a Polynomial)
Let P be non-negatively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let M be a non-zero graded submodule of F, let $f \in P$ be a homogeneous polynomial whose degree satisfies $d = \deg_W(f) >_{\mathtt{Lex}} 0$, and let $\ell \in \mathbb{N}$. We equip $\overline{P} = K[x_0, \ldots, x_n]$ with the grading defined by $\overline{W} = (d \mid W) \in \mathrm{Mat}_{m,n+1}(\mathbb{Z})$. Then we choose a module term ordering σ on the terms of the graded free $\overline{P}$-module $\overline{F} = \bigoplus_{i=1}^{r} \overline{P}(-\delta_i)$ which is of x_0-DegRev type. Consider the following instructions.

1) Compute a homogeneous σ-Gröbner basis $G = \{g_1, \ldots, g_s\}$ of the graded $\overline{P}$-submodule $\overline{M} = M\overline{P} + (f - x_0)\overline{F}$ of $\overline{F}$.
2) For $i = 1, \ldots, s$, let $a_i = \max\{\alpha \in \mathbb{N} \mid x_0^\alpha$ divides $g_i\}$, let $b_i = \min\{a_i, \ell\}$, and let $g_i' = g_i / x_0^{b_i}$.
3) Substitute $x_0 \mapsto f$ in g_i', i.e. form the vector $g_i'' = g_i'(f, x_1, \ldots, x_n)$ in F. Return $G'' = \{g_1'', \ldots, g_s''\}$ and stop.

This is an algorithm which compute a homogeneous system of generators G'' of $M :_F (f^\ell)$.

Proof. By Theorem 4.4.7, the set $\{g'_1, \ldots, g'_s\}$ is a homogeneous σ-Gröbner basis of the $\overline{P}$-module $\overline{M} :_{\overline{F}} (x_0^\ell)$. Upon substituting $x_0 \mapsto f$, we see that $g''_1, \ldots, g''_s \in M :_F (f^\ell)$. To show the reverse inclusion, let $v \in F$ be a homogeneous vector such that $f^\ell v \in M$. Then the equation

$$x_0^\ell v = f^\ell v - (f - x_0)(f^{\ell-1} + f^{\ell-2}x_0 + \cdots + x_0^{\ell-1})\, v \in \overline{M}$$

shows $v \in \overline{M} :_{\overline{F}} (x_0^\ell)$. We substitute $x_0 \mapsto f$ and get $v \in \langle g''_1, \ldots, g''_s \rangle$. □

Regarding the hypothesis $\deg_W(f) >_{\mathtt{Lex}} 0$, we note that, in the $\mathbb{N}$-graded case, a term ordering of x_0-DegRev type exists on $\mathbb{T}^{n+1}$ if and only if $\deg_W(f) > 0$ (see Exercise 4).

The theorem can be used to compute the colon module and the saturation of M with respect to a homogeneous polynomial. The next corollary corresponds to the case $\ell = 1$ of the theorem.

Corollary 4.4.12. (Colon by a Homogeneous Polynomial)
Assume the hypotheses of the theorem. For $i = 1, \ldots, s$, let g'_i be defined by

$$g'_i = \begin{cases} g_i/x_0 & \text{if } g_i \text{ is a multiple of } x_0, \\ g_i & \text{otherwise.} \end{cases}$$

and let $g''_i = g'_i(f, x_1, \ldots, x_n)$. Then $G'' = \{g''_1, \ldots, g''_s\}$ is a homogeneous system of generators of the colon module $M :_F (f)$.

If we apply the theorem for large enough ℓ, the colon module $M :_F (f^\ell)$ coincides with the saturation of M by (f).

Corollary 4.4.13. (Saturation by a Homogeneous Polynomial)
Assume the hypotheses of the theorem. For $i = 1, \ldots, s$, let a_i be the number $\max\{\alpha \in \mathbb{N} \mid x_0^\alpha$ divides $g_i\}$, let $g'_i = g_i/x_0^{a_i}$, and let $g''_i = g'_i(f, x_1, \ldots, x_n)$. Then $G'' = \{g''_1, \ldots, g''_s\}$ is a homogeneous system of generators of the saturation $M :_F (f)^\infty$.

Let us compare the two algorithms for computing $M :_F (f)^\infty$ provided by Theorem 3.5.13.a and the preceding corollary.

Remark 4.4.14. Suppose that P is non-negatively graded by W. Let M be a graded submodule of F as above, and let $f \in P$ be a homogeneous polynomial of degree $d = \deg_W(f) >_{\mathtt{Lex}} 0$.

a) If we use Theorem 3.5.13.a to compute the saturation $M :_F (f)^\infty$, we have to calculate the elimination module

$$[M\overline{P} + (1 - fx_0)\overline{F}] \cap F$$

For this we need to find a Gröbner basis of the module in square brackets with respect to an elimination ordering.

b) If we use Corollary 4.4.13 to compute the saturation $M :_F (f)^\infty$, we have to calculate a Gröbner basis of the graded $\overline{P}$-submodule

$$\overline{M} = M\overline{P} + (f - x_0)\overline{F}$$

of $\overline{F}$ with respect to a module term ordering σ of x_0-DegRev type.

The second method is in general more efficient, since it *preserves the homogeneity*, i.e. we need just the Gröbner basis of a graded submodule with respect to a degree compatible term ordering, and we can use the efficient algorithms of Section 4.5 and Tutorial 59.

Corollary 4.4.13 has two nice applications. In Corollary 4.3.8.a we saw that the computation of the homogenization of an ideal is equivalent to saturating a certain ideal by the product of the homogenizing indeterminates. This saturation can be performed one indeterminate at a time (see Exercise 6) or in one step using Corollary 4.4.13.

Corollary 4.4.15. (Homogenization Via DegRev Type Orderings) *Let P be non-negatively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let I be an ideal in P which is generated by non-zero polynomials $f_1, \ldots, f_s$. We form the polynomial ring $\overline{P} = K[y_0, y_1, \ldots, y_m, x_1, \ldots, x_n]$ and equip it with the grading defined by $\overline{W} = (d \mid \mathcal{I}_m \mid W)$, where $d = (1\ 1\ \cdots\ 1)^{\mathrm{tr}}$. Let σ be a term ordering of y_0-DegRev type on $\mathbb{T}(y_0, \ldots, y_m, x_1, \ldots, x_n)$. Consider the following instructions.*

1) Compute the homogenizations $f_1^{\mathrm{hom}}, \ldots, f_s^{\mathrm{hom}}$ and form the homogeneous ideal $J = (f_1^{\mathrm{hom}}, \ldots, f_s^{\mathrm{hom}}, y_1 \cdots y_m - y_0)$ in $\overline{P}$.
2) Calculate a homogeneous σ-Gröbner basis $\{g_1, \ldots, g_t\}$ of J.
3) For $i = 1, \ldots, t$, let $a_i = \max\{\alpha \mid y_0^\alpha \text{ divides } g_i\}$ and $g_i' = g_i / y_0^{a_i}$.
4) For $i = 1, \ldots, t$, let $g_i'' = g_i(y_1 \cdots y_m, y_1, \ldots, y_m, x_1, \ldots, x_n)$. Return $G'' = \{g_1'', \ldots, g_t''\}$ and stop.

This is an algorithm which computes a homogeneous system of generators G'' of I^{hom}.

Proof. This result follows by combining Corollaries 4.3.8 and 4.4.13. □

In the case $m = 1$ the algorithm of this corollary can be simplified substantially (see Exercise 7). One of the applications of computing the saturation by a polynomial is the Radical Membership Test 3.5.15. Corollary 4.4.13 enables us to write down a homogeneous version of this test.

Corollary 4.4.16. (Homogeneous Radical Membership Test) *Let P be non-negatively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let I be a homogeneous ideal in P, and let $f \in P$ be a homogeneous polynomial of degree $d >_{\mathtt{Lex}} 0$. We equip the ring $\overline{P} = K[x_0, \ldots, x_n]$ with the grading defined by the matrix $(d \mid W) \in \mathrm{Mat}_{m,n+1}(\mathbb{Z})$. Let σ be a term ordering of x_0-DegRev type on $\mathbb{T}(x_0, \ldots, x_n)$, and let $G = \{g_1, \ldots, g_s\}$ be the reduced σ-Gröbner basis of the ideal $I\overline{P} + (f - x_0)\overline{P}$ in $\overline{P}$. Then the following conditions are equivalent.*

a) We have $f \in \sqrt{I}$.
b) There exists a number $i \in \mathbb{N}$ *such that* $x_0^i \in G$.

If these conditions are satisfied, then f^i *is the lowest power of* f *contained in* I.

Proof. First we prove that a) implies b). Let $i \in \mathbb{N}$ be such that $f^i \in I$. Then we have $x_0^i = f^i - (f - x_0)(f^{i-1} + f^{i-2}x_0 + \cdots + x_0^{i-1}) \in I\overline{P} + (f - x_0)\overline{P}$, whence $x_0^j \in G$ for some $j \leq i$. Conversely, let $x_0^i \in G$ for some $i \geq 0$. Thus we have $I :_P (f)^\infty = (1)$ by Corollary 4.4.13, and therefore $f \in \sqrt{I}$.

To prove the additional claim, let $i = \min\{j \in \mathbb{N} \mid f^j \in I\}$. We have to show $x_0^j \notin G$ for $j < i$. Suppose that $x_0^j \in G$ for some $j < i$. Then Theorem 4.4.11 yields $1 \in I :_P (f^j)$, and therefore $f^j \in I$, in contradiction to the minimality of i. □

In the last part of this section we examine two further operations which can be performed efficiently using module term orderings of DegRev type: addition of an indeterminate to a submodule, and reduction of a submodule modulo an indeterminate.

In the next proposition we are going to use the following notation. If $g \in M$ is a non-zero element, we write $g = g' + x_i g''$ in the unique way so that x_i does not divide any monomial in the support of g'.

Proposition 4.4.17. (Addition of an Indeterminate)
Let M *be a graded submodule of* F, *let* $i \in \{1, \ldots, n\}$, *and let* σ *be a module term ordering of* x_i*-DegRev type on* $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$.

a) We have $\mathrm{LT}_\sigma(M + x_i F) = \mathrm{LT}_\sigma(M) + x_i F$.
b) Let G *be a homogeneous* σ*-Gröbner basis of the module* M. *Then the set* $G \cup \{x_i e_1, \ldots, x_i e_r\}$ *is a homogeneous* σ*-Gröbner basis of* $M + x_i F$.
c) Let $G = \{g_1, \ldots, g_s\}$ *be the reduced* σ*-Gröbner basis of* M. *Then the set* $\{g_1', \ldots, g_s', x_i e_1, \ldots, x_i e_r\} \setminus \{0\}$ *is the reduced* σ*-Gröbner basis of the module* $M + x_i F$.

Proof. Since b) is an immediate consequence of a), and since in a) the containment "$\supseteq$" holds obviously, we prove only "$\subseteq$". Let $v = v' + x_i v''$ be a non-zero homogeneous element of $M + x_i F$, where $v' \in M$ and $v'' \in F$. If $\mathrm{LT}_\sigma(v)$ is divisible by x_i, we obviously have $\mathrm{LT}_\sigma(v) \in \mathrm{LT}_\sigma(M) + x_i F$. Otherwise we have $\mathrm{LT}_\sigma(v) \in \mathrm{Supp}(v')$. Since σ is of x_i-DegRev type, the term $\mathrm{LT}_\sigma(v)$ is larger than any term of the same degree which is divisible by x_i. Hence we have $\mathrm{LT}_\sigma(v) = \mathrm{LT}_\sigma(v') \in \mathrm{LT}_\sigma(M)$.

To prove c), we observe that $\{g_1', \ldots, g_s', x_i e_1, \ldots, x_i e_r\} \setminus \{0\}$ is certainly monic and minimal. It is also interreduced, since G is interreduced. □

For the next proposition, we need additional notation. Let $n > 1$, let $i \in \{1, \ldots, n\}$ and let $\widehat{P} = K[x_1, \ldots, x_{i-1}, x_{i+1} \ldots, x_n]$. The restriction of a term ordering σ on $\mathbb{T}^n$ to the monoid of terms $\mathbb{T}(x_1, \ldots, x_{i-1}, x_{i+1} \ldots, x_n)$ in $\widehat{P}$ will be denoted by $\hat{\sigma}$. Notice that we can identify $P/(x_i)$ with $\widehat{P}$ via

the surjective K-algebra homomorphism $\varphi : P \longrightarrow \widehat{P}$ defined by $x_i \mapsto 0$ and $x_j \mapsto x_j$ for $j \neq i$. The image of a polynomial $f \in P$ under φ will be denoted by $\hat{f}$.

Given a grading on P by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, we consider $\widehat{P}$ graded by the matrix $\widehat{W}$ which is obtained by deleting the i^{th} column from W. For every graded free P-module F, the map φ induces a homomorphism of graded P-modules $\Phi : F \longrightarrow \bigoplus_{j=1}^{r} \widehat{P}(-\delta_j)$. The image of a graded submodule M of F under Φ will be denoted by $\widehat{M}$.

Proposition 4.4.18. (Reduction Modulo an Indeterminate)
Let M be a graded submodule of F, let $i \in \{1, \ldots, n\}$, and let σ be a module term ordering of x_i-DegRev type on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. Let $G = \{g_1, \ldots, g_s\}$ be a homogeneous σ-Gröbner basis of M.

a) The set $\widehat{G} = \{\hat{g}_1, \ldots, \hat{g}_s\} \setminus \{0\}$ is a homogeneous $\hat{\sigma}$-Gröbner basis of $\widehat{M}$. In particular, we have $\mathrm{LT}_{\hat{\sigma}}(\widehat{M}) = (\mathrm{LT}_\sigma(M))\widehat{\ }$.

b) Assume that G is the reduced σ-Gröbner basis of M. Then $\widehat{G}$ is the reduced $\hat{\sigma}$-Gröbner basis of $\widehat{M}$.

Proof. For the proof of a), we need to show $\mathrm{LT}_{\hat{\sigma}}(\widehat{M}) = \langle \mathrm{LT}_{\hat{\sigma}}(\hat{g}_j) \mid \hat{g}_j \neq 0\rangle$. The inclusion "$\supseteq$" holds trivially. If we have $\widehat{M} = \langle 0\rangle$, it follows that $M \subseteq x_i F$ and $\widehat{G} = \emptyset$. Thus we may assume that there exists a non-zero homogeneous vector $u \in \widehat{M}$. Since Φ is surjective, there exists a homogeneous vector $v \in M \setminus x_i F$ such that $\Phi(v) = u$. Then Proposition 4.4.6 implies that the leading term $\mathrm{LT}_\sigma(v)$ is not divisible by x_i, and therefore $\Phi(\mathrm{LT}_\sigma(v)) \neq 0$. All terms in $\mathrm{Supp}(u)$ are images under Φ of the same terms in $\mathrm{Supp}(v)$. Thus we have $\mathrm{LT}_{\hat{\sigma}}(u) = \Phi(\mathrm{LT}_\sigma(v))$. Since $\mathrm{LT}_\sigma(v) \in \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\rangle$, we obtain $\mathrm{LT}_{\hat{\sigma}}(u) \in \langle \mathrm{LT}_{\hat{\sigma}}(\hat{g}_j) \mid \hat{g}_j \neq 0\rangle$, i.e. the claim.

Next we prove b). We have just seen that $\mathrm{LT}_{\hat{\sigma}}(\hat{g}_j) = \Phi(\mathrm{LT}_\sigma(g_j))$ for all $\hat{g}_j \neq 0$. Hence the set $\{\mathrm{LT}_{\hat{\sigma}}(\hat{g}_j) \mid \hat{g}_j \neq 0\}$ is a minimal system of generators of $\mathrm{LT}_{\hat{\sigma}}(\widehat{M})$. Since the leading coefficients of the elements of $\widehat{G}$ are the same as those of the corresponding elements of G, it remains to show that the elements of $\widehat{G}$ are interreduced. Again we use the fact that every term in $\mathrm{Supp}(\hat{g}_j - \mathrm{LT}_{\hat{\sigma}}(\hat{g}_j))$ is the image of the same term in $\mathrm{Supp}(g_j - \mathrm{LT}_\sigma(g_j))$ under Φ. We conclude that none of these terms is a multiple of one of the terms in $\{\mathrm{LT}_{\hat{\sigma}}(\hat{g}_j) \mid g_j \neq 0\}$. □

One consequence of this proposition is that certain reduced Gröbner bases behave well under reduction modulo an indeterminate.

Corollary 4.4.19. *In the situation of the proposition, let $G = \{g_1, \ldots, g_s\}$ be the reduced σ-Gröbner basis of M, and assume that x_i is a non-zerodivisor for F/M. Then $\widehat{G} = \{\hat{g}_1, \ldots, \hat{g}_s\}$ is the reduced $\hat{\sigma}$-Gröbner basis of $\widehat{M}$.*

Proof. By Corollary 4.4.8.b, the indeterminate x_i does not divide an element of G. Hence we have $\hat{g}_j \neq 0$ for $j = 1, \ldots, s$, and we can apply the proposition. □

Exercise 1. Prove that the term orderings defined in Example 4.4.5 are indeed of x_i-DegRev type. More generally, given a positive grading by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ on P with $m < n$ and a number $i \in \{1, \ldots, n\}$, construct a term ordering which is of x_i-DegRev type .

Exercise 2. Prove that there exists no degree compatible term ordering for the grading on $P = K[x_1, x_2, x_3]$ given by $W = \left(\begin{smallmatrix} 1 & -1 & 0 \\ 2 & -3 & 1 \end{smallmatrix}\right)$. In particular, there exists no term ordering of DegRev type.

Exercise 3. Find a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ which defines a grading on $P = K[x_1, \ldots, x_n]$ such that a degree compatible term ordering exists, but no term ordering of x_i-DegRev type for any $i \in \{1, \ldots, n\}$.

Exercise 4. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by $W = (w_1 \ \cdots \ w_n) \in \mathrm{Mat}_{1,n}(\mathbb{Z})$, let $d \in \mathbb{Z}$, and let $\overline{P} = K[x_0, \ldots, x_n]$ be $\mathbb{Z}$-graded by $\overline{W} = (d \ \ w_1 \ \cdots \ w_n)$. Show that there exists a term ordering of x_0-DegRev type on $\mathbb{T}(x_0, \ldots, x_n)$ with respect to the grading given by $\overline{W}$ if and only if $d > 0$.

Exercise 5. Let K be a field, let $P = K[x_1, \ldots, x_n]$, let F be a finitely generated free P-module, let M be a submodule of F, let I be an ideal of P, and let σ be a module term ordering on the terms in F.

a) Show that $\mathrm{LT}_\sigma(M :_F I) \subseteq \mathrm{LT}_\sigma(M) :_F I$.
b) Prove by example that the containment in a) can be strict.

Exercise 6. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let I be an ideal in P which is generated by non-zero polynomials $f_1, \ldots, f_s$. Explain how one can use the formula in Tutorial 37.g and Corollary 4.4.9 in order to compute I^{hom}. Formulate an algorithm and implement it in a CoCoA function `IteratedHomog(...)`. Use your function to compute the homogenizations of the following ideals.

a) $I_1 = (x_1 - x_2^2,\ x_1x_2 - x_1)$ in $\mathbb{Q}[x_1, x_2]$ graded by $W = \left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$
b) $I_2 = (x_1^3 - x_2x_3,\ x_2^3 - x_1x_3,\ x_3^3 - x_1x_2)$ in $\mathbb{Q}[x_1, x_2, x_3]$ graded by $W = \left(\begin{smallmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \end{smallmatrix}\right)$
c) $I_3 = (x_1x_2 - 1,\ x_2x_3 - 1,\ x_3x_4 - 1,\ x_4x_1 - 1)$ in $\mathbb{Q}[x_1, x_2, x_3, x_4]$ graded by $W = \mathcal{I}_4$.

Exercise 7. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by $W \in \mathrm{Mat}_{1,n}(\mathbb{Z})$, and let I be an ideal in P which is generated by non-zero polynomials $f_1, \ldots, f_s$. Equip the polynomial ring $\overline{P} = K[x_0, \ldots, x_n]$ with the grading defined by $(1 \mid W)$, and let σ be a term ordering of x_0-DegRev type on $\mathbb{T}(x_0, \ldots, x_n)$. Consider the following instructions.

1) Compute $f_1^{\mathrm{hom}}, \ldots, f_s^{\mathrm{hom}}$ and form the ideal $J = (f_1^{\mathrm{hom}}, \ldots, f_s^{\mathrm{hom}})$ in $\overline{P}$.
2) Calculate a homogeneous σ-Gröbner basis $G = \{g_1, \ldots, g_t\}$ of J.
3) For $i = 1, \ldots, t$, let $g_i' = (g_i^{\mathrm{deh}})^{\mathrm{hom}}$. Return $G' = \{g_1', \ldots, g_t'\}$ and stop.

Show that this is an algorithm which computes a homogeneous system of generators G' of I^{hom}.

Tutorial 53: Reduced Gröbner Bases and Homogenization

In Proposition 4.3.18 we saw that Gröbner bases behave well under dehomogenization, but in the light of Theorem 4.3.19 it is clear that their behaviour under homogenization is more subtle. The situation becomes even more intricate when we are interested in the properties of reduced Gröbner bases with respect to homogenization and dehomogenization. In this tutorial we want to face that challenge in the $\mathbb{Z}$-graded case, i.e. when $m = 1$. As an application, we shall be able to complement the methods of Corollaries 4.3.8 and 4.3.20 with another way of computing the homogenization of an ideal. The idea is to compute the reduced Gröbner basis of the ideal with respect to a suitable term ordering and to homogenize it.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by a matrix $W = (w_1 \ \cdots \ w_n) \in \mathrm{Mat}_{1,n}(\mathbb{Z})$, and let σ be a term ordering on $\mathbb{T}^n$ which is compatible with $\deg_W$. We equip the polynomial ring $\overline{P} = K[x_0, \ldots, x_n]$ with the grading defined by $\overline{W} = (1 \mid W)$ and let τ be a term ordering of x_0-DegRev type on $\mathbb{T}(x_0, \ldots, x_n)$ which restricts to σ on $\mathbb{T}(x_1, \ldots, x_n)$. Finally, let I be an ideal in P and $G = \{g_1, \ldots, g_s\}$ its reduced σ-Gröbner basis.

a) Show that $\mathrm{LT}_\tau(f^{\mathrm{hom}}) = \mathrm{LT}_\sigma(f)$ for all polynomials $f \in P$ and that $(\mathrm{LT}_\tau(F))^{\mathrm{deh}} = \mathrm{LT}_\sigma(F^{\mathrm{deh}})$ for all homogeneous polynomials $F \in \overline{P}$.

b) Let $H = \{h_1, \ldots, h_t\}$ be the reduced τ-Gröbner basis of I^{hom}. Prove that $H^{\mathrm{deh}} = G$.
Hint: Use a) and Proposition 4.3.5.e to show that $\mathrm{LT}_\tau(h_i) = \mathrm{LT}_\sigma(h_i^{\mathrm{deh}})$ for $i = 1, \ldots, t$.

c) Find an example of a homogeneous ideal $J \subseteq \overline{P}$ for which the dehomogenization of the reduced τ-Gröbner basis of J is not the reduced σ-Gröbner basis of J^{deh}.

d) Prove that $G^{\mathrm{hom}} = \{g_1^{\mathrm{hom}}, \ldots, g_s^{\mathrm{hom}}\}$ is the reduced τ-Gröbner basis of I^{hom}.
Hint: Use Proposition 4.3.5.b to show that, for every homogeneous polynomial $F \in \overline{P}$, there exist $r \geq 0$, $T \in \mathbb{T}(x_1, \ldots, x_n)$, and $i \in \{1, \ldots, s\}$ such that $\mathrm{LT}_\tau(F) = x_0^r T \, \mathrm{LT}_\tau(g_i^{\mathrm{hom}})$. To prove that G^{hom} is interreduced, write $T' \in \mathrm{Supp}(g_i^{\mathrm{hom}}) \cap \mathrm{LT}_\tau(I^{\mathrm{hom}})$ in the form $T' = x_0^r T''$, where $T'' \in \mathrm{Supp}(g_i)$, and in the form $T' = x_0^{r'} \, \mathrm{LT}_\tau(f^{\mathrm{hom}})$, where $f \in I$. Then compare the two expressions.

In what follows, we shall assume that σ is of the form $\sigma = \mathtt{Ord}(V)$ with a matrix $V \in \mathrm{Mat}_n(\mathbb{Z})$ whose first row is W. Similarly, we let τ be of the form $\tau = \mathtt{Ord}(\overline{V})$ with a matrix $\overline{V} \in \mathrm{Mat}_{n+1}(\mathbb{Z})$ whose first row is $\overline{W}$.

e) Write a CoCoA function `Homog1(...)` which combines the algorithm of Corollary 4.3.8.a for computing I^{hom} with the proof of Theorem 2.4.13 to compute the reduced τ-Gröbner basis of I^{hom}.

f) Write a CoCoA function `Homog2(...)` which combines the algorithm of Corollary 4.3.20 for computing I^{hom} with the proof of Theorem 2.4.13 to compute the reduced τ-Gröbner basis of I^{hom}.

g) Next, write a CoCoA function `Homog3(...)` which computes the reduced τ-Gröbner basis of I^{hom} using the method implicit in part d).

h) Finally, write a CoCoA function `Homog4(...)` which computes the reduced τ-Gröbner basis of I^{hom} using an adaptation of the algorithm given in Corollary 4.4.15.

i) Apply your four functions for computing G^{hom} to the following cases and compare their timings for $\sigma = \texttt{Ord}(V)$ and $\tau = \texttt{Ord}(\overline{V})$, where

$$V = \begin{pmatrix} 1 & \cdots & 1 & 1 \\ -1 & 0 & 0 & 0 \\ & \ddots & & \\ 0 & & 0 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix} \in \text{Mat}_n(\mathbb{Z})$$

and $\overline{V}$ is the analogous matrix of size $(n{+}1) \times (n{+}1)$.

1) $I_1 = (4x_1^4 - x_3,\ 5x_1^5 - x_2)$ in $\mathbb{Q}[x_1, x_2, x_3]$
2) $I_2 = (x_1^2x_2 + 2x_1x_2 + x_1,\ x_1^2 + x_2^2 + 1,\ -2x_1x_2 - x_1 + x_2^3 + x_2,\ -x_2^5 - x_2^4 + x_2^2 + x_2 - 2)$ in $\mathbb{Q}[x_1, x_2]$
3) $I_3 = (2x_1^3 - x_1^2x_2x_3 - 1,\ x_1^2 - x_3,\ x_1x_2 - x_1x_3 + x_3)$ in $\mathbb{Q}[x_1, x_2, x_3]$

Tutorial 54: Regular Sequences of Indeterminates

Corollary 4.4.8 provides a simple criterion for an indeterminate to be a nonzerodivisor for a finitely generated, graded module. If we want to generalize this to a criterion for a list of indeterminates to be a regular sequence, we have to use a special module term ordering of DegRev type, namely the degree-reverse-lexicographic module term ordering τ introduced in Example 4.4.3. Our goal is to show that $x_i, x_{i+1}, \ldots, x_n$ is a regular sequence for a module of the form F/M, where F is a graded free module and M a graded submodule of F, if and only if it is a regular sequence for $F/\operatorname{LT}_\tau(M)$. Then we will find an elementary criterion for the last condition. Finally, the case of an arbitrary sequence of indeterminates can be handled by renaming the indeterminates suitably.

Let K be a field, let $m, n, r \geq 1$, let $P = K[x_1, \ldots, x_n]$ be graded by a matrix $W \in \text{Mat}_{m,n}(\mathbb{Z})$, let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, let F be the graded free P-module $F = \bigoplus_{i=1}^r P(-\delta_i)$, and let τ be the degree-reverse-lexicographic module term ordering defined in Example 4.4.3.

a) Show that τ has the following property. Whenever a homogeneous vector $v \in F \setminus \{0\}$ satisfies $\operatorname{LT}_\tau(v) \in (x_i, x_{i+1}, \ldots, x_n) \cdot F$ for some $i \in \{1, \ldots, n\}$, we have $v \in (x_i, x_{i+1}, \ldots, x_n) \cdot F$.

b) Now let σ be an arbitrary module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ and ϱ a term ordering on $\mathbb{T}^n$. Prove that the following conditions are equivalent.
   1) The module term ordering σ is compatible with ϱ (see Definition 1.4.17).
   2) For all $f \in P \setminus \{0\}$ and all $v \in F \setminus \{0\}$, we have the equality $\mathrm{LT}_\sigma(f\,v) = \mathrm{LT}_\varrho(f) \cdot \mathrm{LT}_\sigma(v)$.
   3) Given two terms $t_1 e_i, t_2 e_i$, where $t_1, t_2 \in \mathbb{T}^n$ and $i \in \{1, \ldots, r\}$, we have $t_1 e_i \geq_\sigma t_2 e_i$ if and only if $t_1 \geq_\varrho t_2$.

c) Let ϱ be a term ordering on $\mathbb{T}^n$ and σ a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ which is compatible with ϱ. Moreover, let M be a submodule of F, and let $f_1, \ldots, f_s \in P$ be polynomials such that $\mathrm{LT}_\varrho(f_1), \ldots, \mathrm{LT}_\varrho(f_s)$ is a regular sequence for $F/\mathrm{LT}_\sigma(M)$ (see Definition 3.2.23.b). Prove that $f_1, \ldots, f_s$ is a regular sequence for F/M.
Hint: Using induction, reduce the claim to the case $s = 1$. Then argue by contradiction starting from a counterexample with minimal leading term.

d) In the setting of c), show that

$$\mathrm{LT}_\sigma(M + (f_1, \ldots, f_s) \cdot F) = \mathrm{LT}_\sigma(M) + (\mathrm{LT}_\varrho(f_1), \ldots, \mathrm{LT}_\varrho(f_s)) \cdot F$$

Hint: Using induction again, reduce the claim to the case $s = 1$. Then argue by contradiction starting from a vector $v = v' + f_1\, v''$ such that $\mathrm{LT}_\sigma(v) \notin \mathrm{LT}_\sigma(M) + \mathrm{LT}_\varrho(f_1) \cdot F$ and $\mathrm{LT}_\sigma(v'')$ is minimal.

e) Let $i \in \{1, \ldots, n\}$, and let M be a graded submodule of F. Prove that $x_i, x_{i+1}, \ldots, x_n$ is a regular sequence for F/M if and only if it is a regular sequence for $F/\mathrm{LT}_\tau(M)$.
Hint: Use descending induction on i, Proposition 4.4.17 and Corollary 4.4.8.

f) Now let M be a monomial submodule of F, let $v_1, \ldots, v_s$ be the minimal monomial system of generators of M (see Proposition 1.3.11), and let $t_1, \ldots, t_u \in \mathbb{T}^n$. Show that $t_1, \ldots, t_u$ is a regular sequence for F/M if and only if no indeterminate divides both t_i and an element of $\{t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_u, v_1, \ldots, v_s\}$ for $i = 1, \ldots, u$.

g) Using f), write a CoCoA function `IsMonRegSeq(...)` which takes a list L of terms and a minimal monomial system of generators of a monomial submodule M of F and checks whether L is a regular sequence for F/M.

h) Use your function `IsMonRegSeq(...)` to find out whether the following lists of terms are regular sequences for $\mathbb{Q}[x_1, x_2, x_3]^3/\langle x_1^2 e_1,\, x_2^2 e_2,\, x_1 x_2 e_3\rangle$: $L_1 = (x_3^2,\, x_4^2)$, $L_2 = (x_2 x_3,\, x_1 x_4)$, and $L_3 = (x_3^4, x_3^2 x_4^2, x_4^4)$.

i) Implement a CoCoA function `IsIndetRegSeq(...)` which takes a list L of indeterminates and a system of generators of a graded submodule M of F and checks whether L is a regular sequence for F/M.
Hint: By renaming the indeterminates suitably, you can reduce the task to the case $L = (x_i, x_{i+1}, \ldots, x_n)$ for some $i \in \{1, \ldots, n\}$.

j) Use your function `IsIndetRegSeq(...)` to check whether the following lists of indeterminates are regular sequences for the stated modules.
   1) $L_1 = (x_1, x_2)$, $L_2 = (x_1, x_3)$, and $L_3 = (x_3, x_4)$ for the ring $\mathbb{Q}[x_1, x_2, x_3, x_4]/(x_1^2 - x_2^2, x_3^2 - x_4^2)$
   2) $L_4 = (x_1, x_2)$, $L_5 = (x_2, x_4)$, and $L_6 = (x_4, x_3)$ for the module $\mathbb{Q}[x_1, x_2, x_3, x_4]^3/\langle (x_3^2 + x_4^2)e_1, x_1e_2 - x_3e_3 \rangle$

Tutorial 55: Set-Theoretic Complete Intersections

Hi! I'm in a phone booth
at the intersection of
`WALK` *and* `DON'T WALK`.
(Anonymous)

Many of the techniques we have learned in this chapter can be applied in algebraic geometry. Here we present a first case in point. Throughout this tutorial we have to assume that you are acquainted with affine and projective varieties (see Tutorials 27 and 46). For a projective variety, its homogeneous vanishing ideal has a unique minimal number of generators by Proposition 4.1.22.b. But frequently there are smaller homogeneous ideals which define the same projective variety and which have fewer generators. The extremal case for this behaviour is the case of set-theoretic complete intersections defined below.

Let K be a field, let $P = K[x_1, x_2, x_3]$ and $\overline{P} = K[x_0, x_1, x_2, x_3]$ both be standard graded, and let $C = \{(t, t^2, t^3) \mid t \in K\} \subseteq \mathbb{A}^3_K$ be the twisted cubic curve we met in Exercise 10 of Section 3.4.

a) Prove that C is an affine variety whose vanishing ideal $I = \mathcal{I}(C) \subseteq P$ is a prime ideal $I = (f, g)$ generated by the two polynomials $f = x_1^2 - x_2$ and $g = x_1x_2 - x_3$.
   Hint: First show that I is the kernel of the K-algebra homomorphism $\varphi : K[x_1, x_2, x_3] \longrightarrow K[y]$ defined by $x_i \mapsto y^i$ for $i = 1, 2, 3$.

b) Use the methods provided by Corollaries 4.3.8.a, 4.3.20, and 4.4.15 to compute the homogenization I^{hom} of I in three ways. In all three cases show that I^{hom} is generated by the three 2×2-minors $d_1 = x_1x_3 - x_2^2$, $d_2 = x_1x_2 - x_0x_3$, and $d_3 = x_0x_2 - x_1^2$ of the matrix

$$\begin{pmatrix} x_0 & x_1 & x_2 \\ x_1 & x_2 & x_3 \end{pmatrix}$$

c) Prove that I^{hom} is a prime ideal and that the above three minors are in fact a minimal system of generators of I^{hom}. (*Hint:* Use the graded version of Nakayama's lemma 1.7.15.)

d) Let $D \in K[x_0, x_1, x_2, x_3]$ be the determinant of the matrix

$$\begin{pmatrix} x_0 & x_1 & x_2 \\ x_1 & x_2 & x_3 \\ x_2 & x_3 & 0 \end{pmatrix}$$

Show that $I^{\mathrm{hom}} = \sqrt{(d_3, D)}$. More specifically, prove that $d_1^2 \in (d_3, D)$ and $d_2^2 \in (d_3, D)$ by finding the corresponding expressions.

Let us interpret these algebraic facts in the language of algebraic geometry. The projective variety $\overline{C} = \mathcal{Z}^+(I^{\mathrm{hom}}) \subseteq \mathbb{P}^3$ is the projective closure of C. It is a **curve**, i.e. it is 1-dimensional in the sense of the definition which we shall discuss in Chapter 5. Since C is contained in the 3-dimensional space $\mathbb{P}^3$, it has codimension two. It is known that in order to generate the homogeneous vanishing ideal, one needs at least $\mathrm{codim}(C) = 2$ polynomials. In our case, we have seen that one actually needs at least three polynomials. But there exists another ideal, namely (d_3, D), which defines the same variety and is indeed generated by only two polynomials. A variety with the property that it can be defined by an ideal whose number of generators is the codimension is called a **set-theoretic complete intersection**.

In the remainder of this tutorial, we shall generalize this result to find more set-theoretic complete intersections. Let both $P = K[x_1, \ldots, x_4]$ and $\overline{P} = K[x_0, \ldots, x_4]$ be standard graded.

f) Let $C = \{(t, t^2, t^3, t^4) \mid t \in K\} \subseteq \mathbb{A}^4_K$. Prove that C is an affine variety whose vanishing ideal $I = \mathcal{I}(C) \subseteq P$ is a prime ideal generated by three polynomials $f = x_1^2 - x_2$, $g = x_1x_2 - x_3$, and $h = x_1x_3 - x_4$.

g) As in part b), compute the homogenization I^{hom} of I in three ways. Show that I^{hom} is minimally generated by the six 2×2-minors of the matrix

$$\begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}$$

h) Let J be the ideal generated by the leading principal minors of size > 1 of the matrix

$$M = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 & x_4 \\ x_2 & x_3 & x_4 & 0 \\ x_3 & x_4 & 0 & 0 \end{pmatrix}$$

i.e. the ideal generated by $\{\det \left(\begin{smallmatrix} x_0 & x_1 \\ x_1 & x_2 \end{smallmatrix}\right), \det \left(\begin{smallmatrix} x_0 & x_1 & x_2 \\ x_1 & x_2 & x_3 \\ x_2 & x_3 & x_4 \end{smallmatrix}\right), \det(M)\}$. Show that $I^{\mathrm{hom}} = \sqrt{J}$. Conclude that the projective closure $\overline{C} = \mathcal{Z}^+(I^{\mathrm{hom}})$ of C in $\mathbb{P}^4$ is a set-theoretic complete intersection.

If you are very brave (and skilful), you might try to generalize the previous examples as follows. Let $n \geq 2$, let $P = K[x_1, \ldots, x_n]$ and $\overline{P} = K[x_0, \ldots, x_n]$ be standard graded, and let I be the ideal in $\overline{P}$ generated by the 2×2-minors of the matrix

$$M = \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_1 & x_2 & \cdots & x_n \end{pmatrix} \in \mathrm{Mat}_{2,n}(\overline{P})$$

i) Show that I is a prime ideal which is minimally generated by those minors and that $C = \mathcal{Z}^+(I)$ is a set-theoretic complete intersection in $\mathbb{P}^n$. This variety is called the **rational normal curve** in $\mathbb{P}^n$.
Hint: Show that $I = \sqrt{J}$, where J is the ideal generated by the leading principal minors of size > 1 of the matrix

$$\begin{pmatrix} x_0 & x_1 & \cdots & x_{n-2} & x_{n-1} \\ x_1 & x_2 & \cdots & x_{n-1} & x_n \\ x_2 & x_3 & \cdots & x_n & 0 \\ \vdots & \vdots & & & \vdots \\ x_{n-1} & x_n & 0 & \cdots & 0 \end{pmatrix}$$

4.5 Homogeneous Gröbner Bases

No problem is so formidable
that you can't walk away from it.
(Charles Schulz)

The topic of the current chapter is homogeneity. Given the presence of a grading on our objects of study, we want to take computational advantage of it. But so far we have computed precious little. We have not yet even considered the computation of Gröbner bases. What happens if we apply Buchberger's algorithm to a homogeneous ideal? Is the reduced Gröbner basis of a graded submodule homogeneous? Can one write down a homogeneous version of Buchberger's algorithm which computes the desired Gröbner basis degree by degree? As you know by now, these are rhetorical questions and the answer is usually "yes". In the first part of this section we shall explain why.

After showing that Buchberger's algorithm preserves homogeneity, we characterize graded submodules by the property that their reduced Gröbner bases are homogeneous (see Corollary 4.5.2). Then we actually try to compute a homogeneous Gröbner basis. We reorganize Buchberger's algorithm to make it proceed degree by degree (see Theorem 4.5.5). In each degree there are two phases: first we process the S-vectors, and then we treat the input vectors of that degree. Although this strategy is not strictly necessary here, we will be able to reap a nice reward in the next section. A long, detailed illustrative run of this algorithm in Example 4.5.6 should make it clear that there is no reason for you to walk out on us at this point.

Expanding on the idea of proceeding degree by degree, we examine in the second subsection what happens if we stop our calculation at a given degree. The name of this game is *calculus interruptus* and its result is called a *truncated* Gröbner basis. A d-truncated Gröbner basis consists of the vectors of degree less than or equal to d of some homogeneous Gröbner basis. Truncated Gröbner bases have a characterization which is analogous to Buchberger's criterion for ordinary Gröbner bases (see Proposition 4.5.11). One consequence of this characterization is Corollary 4.5.14 which explains what happens when we add an element of degree d into a d-truncated Gröbner basis and this will come in handy later. More practical applications of truncated Gröbner bases are contained in Tutorial 57.

Naturally, computing a Gröbner basis degree by degree is neither a deep nor a new idea. Therefore we were surprised to find that the problem of writing down the algorithms in full detail is rarely addressed in the literature. When we tried to tame the subtleties of this topic, we quickly understood why. But instead of avoiding these uncharted waters, we stayed the course and sailed into the perilous seas. We believe we reached our desired destination, and we are offering you our maps as proof. Before leaving port, you still have to endure a briefing on our assumptions and hypotheses.

Positiveness, Effectiveness, Finiteness, and All That

Starting from this section, we are going to assume that our polynomial ring $P = K[x_1, \ldots, x_n]$ is positively graded. Why is this condition so important?

The first property of a grading we need is that there is a well-ordering on the degrees. It guarantees the descending chain condition 1.4.18.b, and consequently, if a procedure produces a list of terms in strictly decreasing degrees, it has to stop eventually. This is the archetype of all finiteness proofs in Computational Commutative Algebra.

Generally speaking, the whole section, and in fact the entire chapter, can be written up for modules over polynomial rings which are graded by a commutative monoid possessing a monoid ordering which is a well-ordering. In this way, we could furnish you with nicely honed theoretical arguments, most of which are essentially impossible to implement in a true computer algebra system. Just how should one practically realize an arbitrary commutative monoid? And which monoids carry an effectively computable well-ordering? A purely theoretical approach like this would clearly violate the concrete and hands-on spirit of this book.

Thus we need to specialize to an effectively computable monoid and a natural ordering on the degrees. Many applications of the homogeneous case use the standard grading. In Chapter 5 we shall encounter some problems where bigradings are truly useful, and the most general monoid we have ever used is $\mathbb{Z}^m$. For a $\mathbb{Z}^m$-grading on the polynomial ring of the type considered in this book, i.e. a grading given by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, a well-ordering on the monoid of degrees $\Gamma = \{d \in \mathbb{Z}^m \mid P_d \neq 0\}$ exists if W is of non-negative type (see Proposition 4.1.21).

However, as we explained in Section 4.1, gradings of non-negative type are not yet good enough to satisfy further reasonable requirements, such as finite dimensional homogeneous components and a well-behaved minimal number of homogeneous generators. These properties are satisfied for gradings of positive type (see Propositions 4.1.19 and 4.1.22). But this is still not concrete enough for us. Although there exists a term ordering on the degrees in the case of gradings of positive type (and even in the case of gradings of non-negative type), there is no canonical choice for that ordering. Computers absolutely hate that. Consequently, programmers dislike it, too. And we join in and ask for a definite and easily computable answer to the question which of two degrees is larger.

Moreover, having an explicit ordering σ on Γ with $\deg_W(x_i) >_\sigma 0$ for $i = 1, \ldots, n$ (as is guaranteed by a grading of positive type) has further advantages for computing a homogeneous Gröbner basis degree by degree. If Buchberger's algorithm generates a new critical pair (i, j), it will have a degree which is larger than the current degree. Namely, a non-zero S-vector of the form $S_{ij} = t_{ij}g_i - t_{ji}g_j$ has a degree larger than g_i, because we have $\deg_W(t_{ij}) >_\sigma 0$ for any term $t_{ij} \neq 1$. In this way, we never have to go back in degree and apply reductions to elements of smaller degree.

The second advantage is related to the efficiency of homogeneous Gröbner basis computations. During the computation in degree d, the normal remainder of a homogeneous vector with respect to some list of homogeneous vectors may have to be computed. If we know that $\deg_W(t) > 0$ for every term $t \neq 1$, we can exclude reductors of larger degree. Therefore we can speed up the reduction process.

So, why are we not working with a grading of positive type together with an explicitly given ordering σ on Γ such that $\deg_W(x_i) >_\sigma 0$ for $i = 1, \ldots, n$? There are at least two reasons. According to Remark 4.2.7, it is easy to switch from a grading of positive type to a positive grading. And, for a positive grading, the ordering on the degree with the above mentioned property is simply `Lex`. This fact allows us to avoid many unnecessary complications and to describe many algorithms in a more natural way.

But there is a more important reason. Ordering the degrees lexicographically has the added advantage that degree compatible term orderings exist (see Proposition 4.2.3), so that we can study the interplay between non-graded and graded settings. In conclusion, if `Lex` is to be a well-ordering on the degrees such that $\deg_W(x_i) >_{\texttt{Lex}} 0$ for $i = 1, \ldots, n$, there remains but one choice: P has to be positively graded. Voilà!

So, henceforth we let K be a field, we assume that $P = K[x_1, \ldots, x_n]$ is positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, we let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, and we consider the graded free P-module $F = \bigoplus_{i=1}^r P(-\delta_i)$ together with a module term ordering σ on the monomodule $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ of terms in F.

4.5.A The Homogeneous Buchberger Algorithm

First of all, let us have another look at the behaviour of Buchberger's Algorithm 2.5.5 in this graded situation. Given two non-zero homogeneous vectors $v, w \in F$ and a term $t \in \mathbb{T}^n$ such that $t \cdot \mathrm{LT}_\sigma(w) \in \mathrm{Supp}(v)$, we can perform the reduction step $v \xrightarrow{w} v'$. Notice that this can happen only if $\deg_W(tw) = \deg_W(v)$. Hence v' is again a homogeneous vector of degree $\deg_W(v)$. This simple observation is the key to the proof of the following proposition.

Proposition 4.5.1. *Let M be a graded submodule of F and $\{g_1, \ldots, g_s\}$ a set of non-zero homogeneous vectors which generate M.*

a) Buchberger's Algorithm 2.5.5, applied to the tuple $\mathcal{G} = (g_1, \ldots, g_s)$, returns a homogeneous σ-Gröbner basis of M.

b) The reduced σ-Gröbner basis of M consists of homogeneous vectors.

Proof. First we prove claim a). During the execution of Buchberger's Algorithm 2.5.5, only elements of the form $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$ are appended to $\mathcal{G}$. Let $\mathrm{LM}_\sigma(g_i) = c_i t_i e_{\gamma_i}$ for $i = 1, \ldots, s$, where $c_i \in K \setminus \{0\}$ and $t_i \in \mathbb{T}^n$ and $\gamma_i \in \{1, \ldots, r\}$. For all $1 \leq i < j \leq s$ such that $\gamma_i = \gamma_j$, the

element $S_{ij} = \frac{\mathrm{lcm}(t_i,t_j)}{c_i t_i}\, g_i - \frac{\mathrm{lcm}(t_i,t_j)}{c_j t_j}\, g_j$ is homogeneous and its degree is $\deg_W(\mathrm{lcm}(t_i,t_j)) + \delta_{\gamma_i}$. As we have noted above, the reduction steps during the computation of the normal remainder of S_{ij} preserve homogeneity and degree. Therefore only homogeneous elements are appended to $\mathcal{G}$ and the resulting Gröbner basis is homogeneous.

To prove b), we look at the construction of the reduced Gröbner basis in the proof of Theorem 2.4.13. Starting with a homogeneous Gröbner basis, we see that all operations preserve the homogeneity of the elements, since the normal form operation is again composed of reduction steps and reduction steps preserve homogeneity. □

An easy but important application of this proposition is the following criterion for checking whether a given module is graded (see also Tutorial 22.c).

Corollary 4.5.2. (Characterization of Graded Submodules)
Let M be a submodule of F. Then the following conditions are equivalent.

a) The module M is a graded submodule of F.
b) For every term ordering σ on $\mathbb{T}^n\langle e_1,\ldots,e_r\rangle$, the reduced σ-Gröbner basis of M consists of homogeneous vectors.
c) There exists a term ordering σ on $\mathbb{T}^n\langle e_1,\ldots,e_r\rangle$ and a σ-Gröbner basis of M which consists of homogeneous vectors.

Proof. Claim a) implies b) by part b) of the proposition, and claim b) obviously implies c). The remaining implication is an immediate consequence of Proposition 1.7.10. □

Our next goal is to state and prove a homogeneous version of Buchberger's Algorithm. To ease the notation, we shall use the following convention. Whenever a non-zero vector g_i appears, we write $\mathrm{LM}_\sigma(g_i) = c_i t_i e_{\gamma_i}$ where $c_i \in K$ and $t_i \in \mathbb{T}^n$ and $\gamma_i \in \{1,\ldots,r\}$. Let us recall the basic objects occurring in Buchberger's Algorithm 2.5.5, examine whether they are homogeneous, and determine their degrees in that case.

Remark 4.5.3. Let $\mathcal{G} = (g_1,\ldots,g_s)$ be a tuple of non-zero homogeneous vectors in F, and let $d_i = \deg_W(g_i)$ for $i = 1,\ldots,s$.

a) The syzygy modules $\mathrm{Syz}_P(\mathcal{G})$ and $\mathrm{Syz}_P(\mathrm{LM}_\sigma(\mathcal{G}))$ are graded submodules of the graded free P-module $\bigoplus_{i=1}^s P(-d_i)$ (see Exercise 3). The canonical basis of this module will be denoted by $\{\varepsilon_1,\ldots,\varepsilon_s\}$.
b) For two indices $i,j \in \{1,\ldots,s\}$ such that $i \neq j$ and $\gamma_i = \gamma_j$, the element $\sigma_{ij} = \frac{\mathrm{lcm}(t_i,t_j)}{c_i t_i}\,\varepsilon_i - \frac{\mathrm{lcm}(t_i,t_j)}{c_j t_j}\,\varepsilon_j$ is called the **fundamental syzygy** of $(\mathrm{LM}_\sigma(g_i), \mathrm{LM}_\sigma(g_j))$ (see Theorem 2.3.7 and Proposition 3.1.3). Then σ_{ij} is homogeneous of degree $\deg_W(\sigma_{ij}) = \deg_W(\mathrm{lcm}(t_i,t_j)) + \delta_{\gamma_i}$. We note that $\deg_W(\sigma_{ij}) \geq_{\mathtt{Lex}} \max_{\mathtt{Lex}}\{d_i,d_j\}$.
c) For all pairs (i,j) such that $1 \leq i < j \leq s$ and $\gamma_i = \gamma_j$, the S-vector $S_{ij} = \frac{\mathrm{lcm}(t_i,t_j)}{c_i t_i}\, g_i - \frac{\mathrm{lcm}(t_i,t_j)}{c_j t_j}\, g_j$ of g_i and g_j is a homogeneous element of F of degree $\deg_W(\mathrm{lcm}(t_i,t_j)) + \delta_{\gamma_i} = \deg_W(\sigma_{ij})$.

d) The set $B = \{(i,j) \mid 1 \leq i < j \leq s,\ \gamma_i = \gamma_j\}$ is called the **set of critical pairs** of $\mathcal{G}$. For $(i,j) \in B$, we define the **degree of the critical pair** (i,j) to be $\deg_W((i,j)) = \deg_W(S_{ij})$.

The following definition provides a few more abbreviations which will make it easier to formulate and study algorithms in the homogeneous case.

Definition 4.5.4. Let M be a graded P-module, let S be a subset of M, and let $\mathcal{V} = (v_1, \ldots, v_s)$ be a tuple of non-zero homogeneous elements of M.

a) The tuple $\mathcal{V}$ is called **deg-ordered** if $\deg_W(v_1) \leq_{\mathtt{Lex}} \cdots \leq_{\mathtt{Lex}} \deg_W(v_s)$.

b) Given a degree $d \in \mathbb{Z}^m$, we let $S_{\leq d} = \{v \in S \mid v \text{ homogeneous}, \deg_W(v) \leq_{\mathtt{Lex}} d\}$ and $S_d = \{v \in S \mid v \text{ homogeneous}, \deg_W(v) = d\}$.

c) Likewise, given a degree $d \in \mathbb{Z}^m$, we let $\mathcal{V}_{\leq d}$ be the subtuple of $\mathcal{V}$ consisting of the elements v_i such that $\deg_W(v_i) \leq_{\mathtt{Lex}} d$, and we let $\mathcal{V}_d$ be the subtuple of $\mathcal{V}$ consisting of the elements v_i such that $\deg_W(v_i) = d$.

Now we are ready to formulate and prove the homogeneous version of Buchberger's algorithm. Notice that, unlike in Algorithm 2.5.5, here we shall keep the input tuple untouched.

Theorem 4.5.5. (The Homogeneous Buchberger Algorithm)
Let $P = K[x_1, \ldots, x_n]$ be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let M be a graded submodule of F, and let $\mathcal{V} = (v_1, \ldots, v_s)$ be a deg-ordered tuple of non-zero homogeneous vectors which generate M. Furthermore, let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. Consider the following sequence of instructions.

1) Let $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, and $s' = 0$.
2) Let d be the smallest degree with respect to Lex *of an element in B or in $\mathcal{W}$. Form the subset B_d of B, form the subtuple $\mathcal{W}_d$ of $\mathcal{W}$, and delete their entries from B and $\mathcal{W}$, respectively.*
3) If $B_d = \emptyset$, continue with step 6). Otherwise, choose a pair $(i,j) \in B_d$ and remove it from B_d.
4) Compute the S-vector S_{ij} and its normal remainder $S'_{ij} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$. If $S'_{ij} = 0$, continue with step 3).
5) Increase s' by one, append $g_{s'} = S'_{ij}$ to the tuple $\mathcal{G}$, and append the set $\{(i,s') \mid 1 \leq i < s',\ \gamma_i = \gamma_{s'}\}$ to the set B. Continue with step 3).
6) If $\mathcal{W}_d = \emptyset$, continue with step 9). Otherwise, choose a vector $v \in \mathcal{W}_d$ and remove it from $\mathcal{W}_d$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v)$. If $v' = 0$, continue with step 6).
8) Increase s' by one, append $g_{s'} = v'$ to the tuple $\mathcal{G}$, and append the set $\{(i,s') \mid 1 \leq i < s',\ \gamma_i = \gamma_{s'}\}$ to the set B. Continue with step 6).
9) If $B = \emptyset$ and $\mathcal{W} = \emptyset$, return the tuple $\mathcal{G}$ and stop. Otherwise, continue with step 2).

This is an algorithm which returns a deg-ordered tuple $\mathcal{G} = (g_1, \ldots, g_{s'})$ whose elements are a homogeneous σ-Gröbner basis of M.

Proof. First we prove finiteness. Every time step 3) is executed, we remove an element from the set B_d if it is non-empty, and every time step 6) is executed, we remove an element from the tuple $\mathcal{W}_d$ if it is non-empty. The tuple $\mathcal{W}$ is never enlarged. The set B is enlarged only in steps 5) and 8). Notice that a pair (i,j) which is added to B in step 5) or in step 8) has a degree d' greater than d because the grading given by W is positive. Thus, for each degree d, the execution of steps 3) to 8) is finite. When the set B is enlarged, an element $g_{s'}$ is appended to $\mathcal{G}$ which has a leading term outside $\langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_{s'-1})\rangle$. Since every ascending chain of monomial submodules of F becomes eventually stationary, steps 5) and 8) can be executed only finitely many times. Thus we reach eventually a point where $\mathcal{W} = \emptyset$ and $B = \emptyset$, and the procedure terminates in step 9).

Now we show that the algorithm returns a homogeneous σ-Gröbner basis of M. For every new element $g_{s'}$ which is added to $\mathcal{G}$, the set of pairs $\{(i,s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$ is added to B in steps 5) and 8). Hence all pairs in $\{(i,j) \mid 1 \leq i < j \leq s', \gamma_i = \gamma_j\}$ are added to B at some point during the execution of the algorithm.

Every time a pair (i,j) is deleted in step 3), steps 4) and 5) guarantee that the corresponding syzygy σ_{ij} has a lifting in $\mathrm{Syz}(\mathcal{G})$. Therefore $\mathcal{G}$ is a σ-Gröbner basis of $\langle g_1, \ldots, g_{s'}\rangle$ by Buchberger's criterion 2.5.3. Since all generators $\{v_1, \ldots, v_s\}$ of M are eventually treated by steps 6), 7), and 8), we have $M = \langle g_1, \ldots, g_{s'}\rangle$ when the algorithm stops.

Moreover, the elements S'_{ij} or v' in steps 4) and 7) are normal remainders of homogeneous elements with respect to reduction by a list of homogeneous vectors. Thus it follows by induction on s' that $\mathcal{G}$ continues to consist of homogeneous vectors throughout. Finally, the fact that the degrees of the elements of $\mathcal{G}$ are ordered non-decreasingly follows from the choice of the next degree d in step 2), because an element $g_{s'}$ which is appended to $\mathcal{G}$ in step 5) or 8) has the current degree d. □

The best way to come to grips with a complicated algorithm like this one is to try it out on some example. Let us go through a complete computation on a step-by-step basis.

Example 4.5.6. Let $P = K[x_1, x_2, x_3, x_4]$ be graded by $W = \left(\begin{smallmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{smallmatrix}\right)$, let $\mathcal{V}$ be the tuple of polynomials $\mathcal{V} = (v_1, v_2)$, where $v_1 = x_1x_3 - x_2x_4$ and $v_2 = x_1^2 - x_2^2$, and let I be the ideal generated by the polynomials in $\mathcal{V}$. We note that v_1 is homogeneous of degree $\binom{2}{1}$ and v_2 is homogeneous of degree $\binom{2}{2}$. Therefore $\mathcal{V}$ is a deg-ordered list.

Our goal is to compute a σ-Gröbner basis of I, where $\sigma = \texttt{DegRevLex}$. We follow the algorithm explained in Theorem 4.5.5.

1) Let $B = \emptyset$, $\mathcal{W} = (v_1, v_2)$, $\mathcal{G} = \emptyset$, and $s' = 0$.
2) Let $d = \binom{2}{1}$, $\mathcal{W}_{\binom{2}{1}} = (v_1)$, $\mathcal{W} = (v_2)$, and $B_{\binom{2}{1}} = \emptyset$.
3) Since $B_{\binom{2}{1}} = \emptyset$, we continue with step 6).

6) Choose $v = v_1$ and let $\mathcal{W}_{\binom{2}{1}} = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = v_1$.
8) Let $s' = 1$, $\mathcal{G} = (g_1)$ with $g_1 = v_1$, and $B = \emptyset$.
6) Since $\mathcal{W}_{\binom{2}{1}} = \emptyset$, we continue with step 9).
9) Since $\mathcal{W} \neq \emptyset$, we continue with step 2).
2) Let $d = \deg_W(v_2) = \binom{2}{2}$, $\mathcal{W}_{\binom{2}{2}} = (v_2)$, $\mathcal{W} = \emptyset$, $B_{\binom{2}{2}} = \emptyset$, and $B = \emptyset$.
3) Since $B_{\binom{2}{2}} = \emptyset$, we continue with step 6).
6) Choose $v = v_2$ and let $\mathcal{W}_{\binom{2}{2}} = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = v_2$.
8) Let $s' = 2$, $\mathcal{G} = (g_1, g_2)$ with $g_2 = v_2$, and $B = \{(1,2)\}$.
6) Since $\mathcal{W}_{\binom{2}{2}} = \emptyset$, we continue with step 9).
9) Since $B \neq \emptyset$, we continue with step 2).
2) Let $d = \deg_W((1,2)) = \binom{3}{2}$, $B_{\binom{3}{2}} = \{(1,2)\}$, $\mathcal{W}_{\binom{3}{2}} = \emptyset$, $\mathcal{W} = \emptyset$, and $B = \emptyset$.
3) Choose $(1,2) \in B_{\binom{3}{2}}$ and let $B_{\binom{3}{2}} = \emptyset$.
4) Compute $S_{12} = -x_2^2x_3 + x_1x_2x_4$ and $S'_{12} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{12}) = -x_2^2x_3 + x_1x_2x_4$.
5) Let $s' = 3$, $\mathcal{G} = (g_1, g_2, g_3)$ with $g_3 = -x_2^2x_3 + x_1x_2x_4$, and $B = \{(1,3),(2,3)\}$. We note that $\deg_W((1,3)) = \binom{5}{4}$ and $\deg_W((2,3)) = \binom{4}{3}$.
2) Let $d = \deg_W((2,3)) = \binom{4}{3}$, $B_{\binom{4}{3}} = \{(2,3)\}$, $\mathcal{W}_{\binom{4}{3}} = \emptyset$, $\mathcal{W} = \emptyset$, and $B = \{(1,3)\}$.
3) Choose $(2,3) \in B_{\binom{4}{3}}$ and let $B_{\binom{4}{3}} = \emptyset$.
4) Compute $S_{23} = x_1^2x_2x_4 - x_2^3x_4$ and $S'_{23} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{23}) = 0$.
3) Since $B_{\binom{4}{3}} = \emptyset$, we continue with step 6).
6) Since $\mathcal{W}_{\binom{4}{3}} = \emptyset$, we continue with step 9).
9) Since $B \neq \emptyset$, we continue with step 2).
2) Let $d = \deg_W((1,3)) = \binom{5}{4}$, $B_{\binom{5}{4}} = \{(1,3)\}$, $\mathcal{W}_{\binom{5}{4}} = \emptyset$, $\mathcal{W} = \emptyset$, and $B = \emptyset$.
3) Choose $(1,3) \in B_{\binom{5}{4}}$ and let $B_{\binom{5}{4}} = \emptyset$.
4) Compute $S_{13} = x_1^3x_2x_4 - x_2^4x_3$ and $S'_{13} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{13}) = 0$.
3) Since $B_{\binom{5}{4}} = \emptyset$, we continue with step 6).
6) Since $\mathcal{W}_{\binom{5}{4}} = \emptyset$, we continue with step 9).
9) Since $B = \emptyset$ and $\mathcal{W} = \emptyset$, we return $\mathcal{G} = (g_1, g_2, g_3)$ and stop.

The result of this algorithm is that $\mathcal{G} = (g_1, g_2, g_3)$ is a homogeneous σ-Gröbner basis of I.

To conclude this subsection, we collect a few remarks about the hypothesis of the homogeneous Buchberger algorithm.

Remark 4.5.7. This algorithm does not require that σ be degree compatible because during the computation of the Gröbner basis only comparisons

of terms in the support of a homogeneous vector are made. Thus these terms have the same degree, and it does not matter whether σ is degree compatible or not.

Remark 4.5.8. If we drop the hypothesis that the grading by W be positive, the homogeneous Buchberger algorithm still computes a homogeneous Gröbner basis of M (see also Exercise 5). But the resulting tuple will in general not be deg-ordered anymore, and the algorithm may have to go back in degree occasionally. The reason for this phenomenon is that a critical pair (i, j) can have a smaller degree than g_i or g_j.

For instance, if we use the grading given by $W = \left(\begin{smallmatrix} -1 & -1 & 1 & 1 \\ 1 & & 1 & 0 & 0 \end{smallmatrix}\right)$ in the previous example, the algorithm starts to work in degree $\deg_W(v_2) = \binom{-2}{2}$, then treats degree $\deg_W(v_1) = \binom{0}{1}$, and next goes back to the smaller degree $\deg_W((1,2)) = \binom{-1}{2}$.

In particular, this shows that if we interrupt the execution of the algorithm after some degree d is finished, the tuple $\mathcal{G}$ need not contain a truncated Gröbner basis of M in the sense of the following subsection.

4.5.B Truncated Gröbner Bases

Given a homogeneous system of generators G of a graded module M and a degree $d \in \mathbb{Z}^m$, the set $G_{\leq d}$ generates the module $\langle M_{\leq d} \rangle$ by Corollary 1.7.11. This simple observation lies at the heart of *calculus interruptus*. If, for some reason, we happen to know ahead of time the maximum degree of an element in a Gröbner basis, can we use that to simplify the computation?

To answer this question, we start from the same situation as above, i.e. we let $P = K[x_1, \ldots, x_n]$ be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, we let $F = \bigoplus_{i=1}^r P(-\delta_i)$ be a graded free P-module, and we let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r \rangle$. Furthermore, we assume that we are given a set of non-zero homogeneous vectors $G = \{g_1, \ldots, g_s\}$ in F. Then we let $M = \langle g_1, \ldots, g_s \rangle$ and $\mathcal{G} = (g_1, \ldots, g_s)$.

Definition 4.5.9. Suppose that the set G is a homogeneous σ-Gröbner basis of M, and let $d \in \mathbb{Z}^m$. Then the set $G_{\leq d}$ (or the tuple $\mathcal{G}_{\leq d}$) is called a **d-truncated σ-Gröbner basis** of M, or a σ-Gröbner basis of M which has been **truncated at degree** d.

If we interrupt the Homogeneous Buchberger Algorithm 4.5.5 after some degree d is finished, the elements of the tuple $\mathcal{G}$ at that moment form a d-truncated Gröbner basis of M. Consequently, we can compute truncated Gröbner bases efficiently as follows.

Proposition 4.5.10. (Computation of Truncated Gröbner Bases) *In the situation of Theorem 4.5.5, let a degree $d_0 \in \mathbb{Z}^m$ be given. We replace steps 2), 5), 8) by the following instructions.*

2') Let d be the smallest degree with respect to Lex *of an element in B or in $\mathcal{W}$. If $d >_{\mathtt{Lex}} d_0$, return the tuple $\mathcal{G}$ and stop. Otherwise, form the subset B_d of B and the subtuple $\mathcal{W}_d$ of $\mathcal{W}$, and delete their entries from B and $\mathcal{W}$, respectively.*

5') Increase s' by one, append $g_{s'} = S'_{ij}$ to the tuple $\mathcal{G}$, and append the set $\{(i,s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}, \deg_W((i,s')) \leq_{\mathtt{Lex}} d_0\}$ to the set B. Continue with step 3).

8') Increase s' by one, append $g_{s'} = v'$ to the tuple $\mathcal{G}$, and append the set $\{(i,s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}, \deg_W((i,s')) \leq_{\mathtt{Lex}} d_0\}$ to the set B. Continue with step 6).

Then the resulting set of instructions defines an algorithm. It returns a deg-ordered tuple $\mathcal{G}$ of homogeneous vectors forming a d_0-truncated Gröbner basis of M.

Proof. While the Homogeneous Buchberger Algorithm computes in some current degree d, only elements of degree d are added to the Gröbner basis in steps 5) and 8). Hence, after finishing all degrees $d \leq_{\mathtt{Lex}} d_0$, the elements of the tuple $\mathcal{G}$ are precisely the elements of degree $\leq_{\mathtt{Lex}} d_0$ of the final Gröbner basis. It is clearly not necessary to append critical pairs of degree larger than d_0 to B in steps 5) and 8), since those pairs would never be processed anyway. □

For theoretical applications of truncated Gröbner bases, we need a generalization of Buchberger's Criterion 2.5.3. The following proposition says that d-truncated Gröbner bases are characterized by the property that their S-vectors of degree $\leq_{\mathtt{Lex}} d$ reduce to zero.

Proposition 4.5.11. (Characterization of Truncated Gröbner Bases) *Let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of non-zero homogeneous vectors which generate a graded submodule M of F, and let $d \in \mathbb{Z}^m$. Then the following conditions are equivalent.*

a) The tuple $\mathcal{G}_{\leq d}$ is a d-truncated σ-Gröbner basis of M.
b) Every non-zero element $v \in M_{\leq d}$ satisfies $\mathrm{LT}_\sigma(v) \in \mathrm{LT}_\sigma(\mathcal{G})_{\leq d}$.
c) For all critical pairs (i,j) of degree $\leq d$, we have $\mathrm{NR}_{\sigma,\mathcal{G}_{\leq d}}(S_{ij}) = 0$.

Proof. Without loss of generality, we may assume that $\mathcal{G}$ is a deg-ordered tuple. Hence we have $\mathcal{G}_{\leq d} = (g_1, \ldots, g_{s'})$ for some $s' \leq s$.

It is clear that a) implies b). Let us show that b) implies a). The assumption implies that we can find terms $t'_1, \ldots, t'_{s''}$ of degree greater than d such that

$$\mathrm{LT}_\sigma(M) = \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_{s'}), t'_1, \ldots, t'_{s''} \rangle$$

Using Proposition 1.5.6.a, we may choose homogeneous elements $h_1, \ldots, h_{s''}$ in M such that $\mathrm{LT}_\sigma(h_i) = t'_i$ for $i = 1, \ldots, s''$. Then $(g_1, \ldots, g_{s'}, h_1, \ldots, h_{s''})$ is a homogeneous σ-Gröbner basis of M. If we truncate it at degree d, we get $\mathcal{G}_{\leq d}$.

Next we show that a) implies c). Let $\mathcal{H} = (g_1, \ldots, g_{s'}, h_1, \ldots, h_{s''})$ be a homogeneous σ-Gröbner basis of M for which we have $\deg_W(h_i) >_{\mathtt{Lex}} d$ for $i = 1, \ldots, s''$. By Buchberger's Criterion 2.5.3, we have $\mathrm{NR}_{\sigma,\mathcal{H}}(S_{ij}) = 0$ for all $1 \leq i < j \leq s'$ such that $\gamma_i = \gamma_j$. But since critical pairs (i, j) of degree $\leq_{\mathtt{Lex}} d$ satisfy $i, j \in \{1, \ldots, s'\}$ and $\deg_W(S_{ij}) = \deg_W((i, j)) \leq_{\mathtt{Lex}} d$, only the elements of $\mathcal{G}_{\leq d}$ can be involved in the reduction steps which show $S_{ij} \xrightarrow{\mathcal{H}} 0$. This yields condition c).

Finally, it remains to prove that c) implies a). We need to show that there exists a σ-Gröbner basis $\mathcal{H}$ of M such that $\mathcal{H}_{\leq d} = \mathcal{G}_{\leq d}$. To this end we may replace $\mathcal{G}$ by a subtuple such that no leading term of an element of $\mathcal{G}$ is a multiple of another one. Now we use the algorithm of Proposition 4.5.10, applied to the system of generators $\mathcal{V} = \mathcal{G}$ and $d_0 = d$. In step 7) of this algorithm it suffices to reduce only the leading term of v (see Remark 2.5.6.a). Then the assumption implies that the algorithm puts the elements of $\mathcal{V}_{\leq d}$ one by one into the computed truncated Gröbner basis and no critical pair yields a new element. Hence the result of the algorithm is $\mathcal{V}_{\leq d} = \mathcal{G}_{\leq d}$. □

This characterization has several useful applications. Let us start with an easy one.

Corollary 4.5.12. *Let $\mathcal{G} = (g_1, \ldots, g_s)$ be a homogeneous σ-Gröbner basis of M, and let $d \in \mathbb{Z}^m$. Then $\mathcal{G}_{\leq d}$ is a d-truncated σ-Gröbner basis of the module $\langle M_{\leq d} \rangle$.*

Proof. Since $\mathcal{G}$ generates M, the tuple $\mathcal{G}_{\leq d}$ generates the P-module $\langle M_{\leq d} \rangle$. From Buchberger's Criterion 2.5.3 we know that, for all critical pairs (i, j), we have $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij}) = 0$. If we have $\deg_W((i, j)) \leq_{\mathtt{Lex}} d$ here, the elements of $\mathcal{G}$ involved in the reduction steps $S_{ij} \xrightarrow{\mathcal{G}} 0$ all have degrees less than or equal to d. Hence we see that $\mathrm{NR}_{\sigma,\mathcal{G}_{\leq d}}(S_{ij}) = 0$, and the Proposition yields the claim. □

Example 4.5.13. Let $P = \mathbb{Q}[x, y, z]$ be standard graded, let $\sigma = \mathtt{DegLex}$, and let $I \subseteq P$ be the ideal generated by $\mathcal{G} = (g_1, g_2, g_3)$, where $g_1 = xy - z^2$ and $g_2 = y^2$ and $g_3 = z^3$. Then $\mathcal{G}_{\leq 2} = (g_1, g_2)$ is a 2-truncated σ-Gröbner basis of both the ideal I and the ideal $\langle I_{\leq 2} \rangle = (g_1, g_2)$, since the only critical pair has degree 3. But the tuple $\mathcal{G}_{\leq 3} = (g_1, g_2, g_3)$ is not a 3-truncated Gröbner basis of $I = \langle I_{\leq 3} \rangle$, because $\mathrm{NR}_{\sigma,\mathcal{G}_{\leq 3}}(S_{12}) = -yz^2$ is a new Gröbner basis element in degree 3.

Corollary 4.5.14. *Let $d \in \mathbb{Z}^m$, let the elements of $\mathcal{G} = (g_1, \ldots, g_s)$ form a d-truncated σ-Gröbner basis of M, and let $g_{s+1} \in F$ be a non-zero homogeneous element of degree d such that $\mathrm{LT}_\sigma(g_{s+1}) \notin \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s) \rangle$. Then $\{g_1, \ldots, g_{s+1}\}$ is a d-truncated Gröbner basis of $M + \langle g_{s+1} \rangle$.*

Proof. To prove the claim, we check condition c) of the proposition. For all $1 \leq i < j \leq s$ such that $\gamma_i = \gamma_j$ and $\deg_W(S_{ij}) \leq_{\mathtt{Lex}} d$, we have

$\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij}) = 0$ by the assumption and the proposition. Now the claim follows from the proposition and the observation that there are no pairs $(i, s+1)$ of degree d. Indeed, suppose that there were an index $i \in \{1, \ldots, s\}$ such that $\gamma_i = \gamma_{s+1}$ and $\deg_W((i, s+1)) = d$. Since $\deg_W(g_{s+1}) = d$, the term $\mathrm{LT}_\sigma(g_{s+1})$ would have to be a multiple of $\mathrm{LT}_\sigma(g_i)$, in contradiction to one of the hypotheses. □

Exercise 1. Let $P = K[x, y, z]$ be standard graded and $I = (x^2 - y^2 + z^2,\ xy - z^2,\ y^3 + xz^2 - yz^2 + 2z^3 + xy - z^2,\ -y^2z^2 + 2z^4 + x^2 - y^2 + z^2,\ xy^3 - y^2z^2 + x^3 - xy^2 + xz^2,\ x^3y^3 - 3x^2y^2z^2 + 3xyz^4 - z^6 - yz^3 - z^4,\ y^3z^9 + 3y^2z^{10} + 3yz^{11} + z^{12} - y^2z^2 + 2z^4)$. Show that I is homogeneous.

Exercise 2. Let K be a field, and let $P = K[x, y, z]$ be graded by a non-singular matrix $W \in \mathrm{Mat}_3(\mathbb{Z})$.

a) Let $I = (f_1, f_2, f_3)$ be the ideal in P generated by the polynomials $f_1 = xy$, $f_2 = y^4 - xyz^2 - z^4$, and $f_3 = xz^2$. Show that I is not W-homogeneous.

b) Let $J = (f_1, f_2, f_3)$ be the ideal in P generated by $f_1 = xy$, $f_2 = xz^2$, and $f_3 = c_1x^3 + c_2x^2y + c_3x^2z + c_4xy^2 + c_5xyz + c_6xz^2 + c_7y^3 + c_8y^2z + c_9yz^2 + c_{10}z^3$, where $c_1, \ldots, c_{10} \in K$. Find necessary and sufficient conditions on $c_1, \ldots, c_{10}$ for J to be W-homogeneous.

Exercise 3. Let Γ be a monoid, let R be a Γ-graded ring, let M be a Γ-graded R-module, and let $v_1, \ldots, v_s \in M$ be homogeneous elements. Show that the syzygy module $\mathrm{Syz}_R(v_1, \ldots, v_s)$ is a graded submodule of a suitable Γ-graded free R-module.

Exercise 4. Formulate and prove a homogeneous version of the Extended Buchberger Algorithm 2.5.11.

Exercise 5. Generalize the homogeneous Buchberger algorithm in the following ways.

a) From the assumptions of Theorem 4.5.5, drop the hypothesis that the grading defined by W is positive. Show that the sequence of instructions given in the theorem still computes a homogeneous σ-Gröbner basis of M.

b) Modify Theorem 4.5.5 as follows. Let P be graded by a commutative monoid Γ, let τ be a term ordering on Γ, and let F be a Γ-graded free P-module. Use τ to compare degrees in step 2). Formulate and prove a version of the homogeneous Buchberger algorithm which applies to this situation.

Exercise 6. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let $f_1, \ldots, f_r \in P \setminus \{0\}$ be homogeneous of degrees $d_1, \ldots, d_r$, respectively. Assume that $d_1 < d_2 \leq d_3 \leq \cdots \leq d_r$, and let σ be a term ordering on $\mathbb{T}^n$. Show that $\{f_1\}$ is a d-truncated σ-Gröbner basis of the ideal generated by $\{f_1, \ldots, f_r\}$ for every d such that $d_1 \leq d < d_2$.

Exercise 7. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let $f_1, \ldots, f_r \in P_1$. Furthermore, let $I = (f_1, \ldots, f_r)$, let σ be a term ordering on $\mathbb{T}^n$, and assume that $\{f_1, \ldots, f_r\}$ is a 1-truncated σ-Gröbner basis of I. Prove that $\{f_1, \ldots, f_r\}$ is a σ-Gröbner basis of I.

Tutorial 56: Computation of Homogeneous Gröbner Bases

```
Runtime Error 6D at 417A:32CF: Incompetent User
```
(Anonymous)

When we start practical Gröbner basis computations using the Homogeneous Buchberger Algorithm 4.5.5, we quickly notice that it becomes very slow as soon as we consider some non-trivial examples. This phenomenon is not due to the incompetence of the user, but to the intrinsic complexity of Gröbner basis computations. Nevertheless, there are some easy ways we can improve the performance of our algorithm, and in this tutorial we study a few of them.

As a byproduct, we shall show that the optimization for the usual Buchberger algorithm we stated in Tutorial 25.h is in fact correct. Further optimizations of the homogeneous Buchberger algorithm are contained in Tutorial 59.

Let K be a field, let the polynomial ring $P = K[x_1, \ldots, x_n]$ be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, let F be the graded free P-module $F = \bigoplus_{i=1}^{r} P(-\delta_i)$, and let $\mathcal{V} = (v_1, \ldots, v_s)$ be a deg-ordered tuple of non-zero homogeneous vectors in F which generate a graded submodule M of F. For $i = 1, \ldots, s$, we let $d_i = \deg_W(v_i)$. Moreover, let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$.

a) Implement the Homogeneous Buchberger Algorithm 4.5.5 in a CoCoA function `HomBA(...)`. Apply your function to compute the Gröbner bases of the graded submodules generated by the following tuples with respect to the given module term orderings.
   1) $M_1 \subseteq P = \mathbb{Q}[x_1, x_2, x_3, x_4]$, graded by $W = \left(\begin{smallmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{smallmatrix}\right)$, generated by $\mathcal{V}_1 = (x_1x_3 - x_2x_4,\ x_1^2 - x_2^2)$, with respect to $\sigma =$ `DegRevLex` (see Example 4.5.6)
   2) $M_2 \subseteq P = \mathbb{Q}[x_1, x_2, x_3, x_4]$, graded by $W = (1\ 1\ 1\ 1)$, generated by $\mathcal{V}_2 = (x_1^3 - 4x_2^3,\ x_1^5 - 7x_3^5,\ x_1^7 - 11x_4^7)$, with respect to $\sigma =$ `DegRevLex` and also to $\sigma =$ `Lex`
   3) $M_3 \subseteq P = \mathbb{Q}[x_1, x_2, x_3, x_4]$, graded by $W = (1\ 1\ 1\ 1)$, generated by $\mathcal{V}_3 = (x_1^2x_4 + x_2^3 + x_3^3 - x_4^3,\ x_1^3x_4^2 + x_2^4x_4 + x_3^5 - x_4^5)$, with respect to $\sigma =$ `DegRevLex` and also to $\sigma =$ `Lex`
   4) $M_4 \subseteq P = \mathbb{Q}[x_1, \ldots, x_5]$, graded by $W = (1\ \cdots\ 1)$, generated by $\mathcal{V}_4 = (x_1^5 - x_1x_5^4 - x_4x_5^4,\ x_1^6 - x_1x_5^5 - x_3x_5^5,\ x_1^{51} + x_1^{16}x_5^{35} + x_1x_5^{50} - x_2x_5^{50})$, with respect to $\sigma =$ `Lex`
   5) $M_5 \subseteq P = \mathbb{Q}[x_1, \ldots, x_5]$, graded by $W = (1\ \cdots\ 1)$, generated by $\mathcal{V}_5 = (7x_2x_3^6x_4^2 + 4x_1^6x_2x_5^2 + 9x_1^3x_3^2x_4x_5^3 + 6x_2^2x_3x_5^6,\ 8x_1x_2^5x_3^3 + 2x_1^3x_2^3x_3^2x_5 + 4x_1^6x_4x_5^2 + 3x_2x_5^8,\ 5x_1^3x_2^8x_3^2x_4 + x_1^5x_2^2x_3x_5^6 + 2x_2^2x_3x_5^{11} + 5x_1x_5^{13})$, with respect to $\sigma =$ `DegRevLex`
   6) $M_6 \subseteq P \oplus P(-2)$, where $P = \mathbb{Q}[x, y, z]$ is graded by $W = (1\ 1\ 1)$ and M_6 is generated by $\mathcal{V}_6 = ((x^2 + y^2 - xz,\ 0),\ (y^2 + 2yz - z^2, 1))$, with respect to $\sigma =$ `DegRevLexPos`

7) $M_7 \subseteq P(-1) \oplus P \oplus P$, where $P = \mathbb{Q}[x,y,z]$ is graded by $W = (1\ 1\ 1)$ and M_7 is generated by $\mathcal{V}_7 = ((0,z,y),(0,xy,xy-yz),(y,z^2,0),(z,0,y^2))$, with respect to $\sigma = \texttt{DegLexPos}$

In the following, we use the additional notation introduced before Theorem 4.5.5. Let $\mathcal{G} = (g_1,\ldots,g_{s'})$ be the deg-ordered σ-Gröbner basis of M computed by the algorithm. For $i = 1,\ldots,s'$, we write $\mathrm{LM}_\sigma(g_i) = c_i\, t_i\, e_{\gamma_i}$ with $c_i \in K \setminus \{0\}$ and $t_i \in \mathbb{T}^n$ and $\gamma_i \in \{1,\ldots,r\}$. For $i,j \in \{1,\ldots,s'\}$, we let $t_{ij} = \mathrm{lcm}(t_i,t_j)/t_i$, and $\sigma_{ij} = \frac{1}{c_i}\, t_{ij}\, \varepsilon_i - \frac{1}{c_j}\, t_{ji}\, \varepsilon_j \in \bigoplus_{k=1}^{s'} P(-d_k)$. Furthermore, the set of critical pairs of $\mathcal{G}$ is $B = \{(i,j) \mid 1 \le i < j \le s',\ \gamma_i = \gamma_j\}$, and the corresponding set of fundamental syzygies is $\Sigma = \{\sigma_{ij} \mid (i,j) \in B\}$.

b) Let $\Sigma' \subseteq \Sigma$ be a subset which generates $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. Show that Theorem 4.5.5 remains correct if we apply steps 3) – 5) only to those critical pairs (i,j) such that $\sigma_{ij} \in \Sigma'$.

c) Prove that there exists a subset Σ' of Σ which is a minimal set of generators of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$.

In Tutorial 59 we shall optimize the homogeneous Buchberger algorithm by finding a set Σ' as in c) and applying steps 3) – 5) only to critical pairs (i,j) corresponding to $\sigma_{ij} \in \Sigma'$. Here we make a few steps in this direction by isolating certain critical syzygies which are not minimal generators of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. To do this systematically, it will prove to be convenient to modify Definition 3.1.1 by setting $t\varepsilon_i \ge_\tau t'\varepsilon_j$ if $\mathrm{LT}_\sigma(tg_i) >_\sigma \mathrm{LT}_\sigma(t'g_j)$ or if $\mathrm{LT}_\sigma(tg_i) = \mathrm{LT}_\sigma(t'g_j)$ and $i \ge j$. We shall call τ the **ordering induced by** $(\sigma,\mathcal{G})$ again.

d) Prove that Lemma 3.1.2 and Proposition 3.1.3 continue to hold with this new definition, i.e. that τ is a module term ordering and Σ is a τ-Gröbner basis of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$.

e) Determine $\mathrm{LT}_\tau(\sigma_{ij})$ for $(i,j) \in B$. Then consider the following rules.

1') Delete in Σ all elements σ_{ij} such that there exists an element $\sigma_{i'j}$ for which $\mathrm{LT}_\tau(\sigma_{ij})$ is a proper multiple of $\mathrm{LT}_\tau(\sigma_{i'j})$, i.e. a multiple of and different from $\mathrm{LT}_\tau(\sigma_{i'j})$.

2') If, among the remaining elements, there are $\sigma_{ij}, \sigma_{i'j}$ with $i' > i$ and $\mathrm{LT}_\tau(\sigma_{ij}) = \mathrm{LT}_\tau(\sigma_{i'j})$, then delete $\sigma_{i'j}$.

Prove that the set Σ'' of elements surviving these two rules is a minimal τ-Gröbner basis of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$.

f) Show that the result of applying Rules 1') and 2') is the same as the result of applying the following two rules.

1) Delete in Σ all elements σ_{jk} such that there exists $i \in \{1,\ldots,j-1\}$ such that t_{ki} divides t_{kj}.

2) Delete in the resulting set all elements σ_{ik} such that there exists $j \in \{i+1,\ldots,k-1\}$ such that t_{kj} properly divides t_{ki}.

g) Now we subject the elements of Σ'' to a further rule.

3') Delete in Σ'' all elements σ_{ij} such that there exists $k \in \{j+1, \ldots, s'\}$ for which t_{ik} properly divides t_{ij} and t_{jk} properly divides t_{ji}.

Show that the resulting set Σ''' still generates $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$.
Hint: Prove that $\sigma_{ij} = t\sigma_{ik} + t'\sigma_{jk}$ with $t, t' \in \mathbb{T}^n \setminus \{1\}$.

h) Prove that Rule 3') is equivalent to the following rule.

3) Delete in Σ'' all elements σ_{ij} for which there exists $k \in \{j+1, \ldots, s'\}$ with the properties that t_{ki} does not divide t_{kj}, that t_{kj} does not divide t_{ki}, and that $\gcd(t_{ik}, t_{jk}) = 1$.

Hint: Look at the coefficients of $\sigma_{ij} = t\sigma_{ik} + t'\sigma_{jk}$ and analyze their exponents one indeterminate at a time.

i) Prove that the CoCoA function `GoodGB(...)` which you wrote in Tutorial 25.h correctly computes a σ-Gröbner basis.

j) Write a CoCoA function `Update(...)` which implements the following steps.

U1) Form the set $C = \{(i, s') \mid 1 \leq i < s',\ \gamma_i = \gamma_{s'}\}$.
U2) Delete from C all pairs (j, s') for which there exists $i \in \{1, \ldots, j-1\}$ such that $t_{s'i}$ divides $t_{s'j}$.
U3) Delete from C all pairs (i, s') for which there is $j \in \{i+1, \ldots, s'-1\}$ such that $t_{s'j}$ properly divides $t_{s'i}$.
U4) Find in C all pairs (i, s') and (j, s') such that $1 \leq i < j \leq s'$ and $\gcd(t_{is'}, t_{js'}) = 1$. In each case, delete the pair (i, j) in B if possible.
U5) Append the elements of C to B and stop.

Show that the Homogeneous Buchberger Algorithm 4.5.5 remains correct if we substitute steps 5) and 8) by

5') Increase s' by one, append $g_{s'} = S'_{ij}$ to the tuple $\mathcal{G}$, and apply `Update(...)`. Continue with step 3).
8') Increase s' by one, append $g_{s'} = v'$ to the tuple $\mathcal{G}$, and apply `Update(...)`. Continue with step 6).

Implement the resulting algorithm in a CoCoA function `NewHomBA(...)`.

k) Apply your function `NewHomBA(...)` in the examples of a). Compare its efficiency with the efficiency of `HomBA(...)` by using timings and by counting the numbers of calls to `NR(...)` in every example.

Tutorial 57: Some Applications of Truncated Gröbner Bases

The possibility of truncating a Gröbner basis computation at some degree has many uses. Every time we have some idea of the degree or the structure of the answer we are looking for, we can try to abort the computation of the Homogeneous Buchberger Algorithm 4.5.5 as soon as we have finished treating the degree where we expect our result. In this way we can frequently obtain good bounds on the time it takes to compute that result. Let us study some instances in which this strategy works well.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, let $F = \bigoplus_{i=1}^r P(-\delta_i)$, and let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$.

a) Write a CoCoA program `TruncGB(...)` which takes a tuple $\mathcal{V} = (v_1, \ldots, v_s)$ of non-zero homogeneous vectors which generate a graded submodule M of F and a degree $d \in \mathbb{Z}^m$ and computes a d-truncated Gröbner basis of M using the algorithm of Proposition 4.5.10.

b) Apply your program `TruncGB(...)` to the following cases. Use $K = \mathbb{Q}$, the standard grading, and the module term ordering $\sigma =$ `DegRevLexPos`.

1) $M_1 = (x_1^2 - 2x_2^2,\ x_1^3 - 3x_3^3,\ x_1^4 - x_4^4) \subseteq \mathbb{Q}[x_1, \ldots, x_4],\ d = 3$
2) $M_2 = \langle (x_1x_2,\ x_1x_3,\ x_2x_3),\ (x_2^2 + x_2x_3,\ x_1x_3 + x_2^2,\ x_1x_3),$ $(-x_1,\ x_2,\ x_1),\ (x_2^2,\ x_2x_3,\ x_1x_3)\rangle \subseteq \mathbb{Q}[x_1, x_2, x_3]^3,\ d = 2$
3) $M_3 = \langle (0,\ x_2x_3,\ x_1x_3),\ (0,\ x_1x_3,\ x_1x_2 - x_1x_3),\ (x_2x_3,\ x_1x_3,\ 0),$ $(x_2^2,\ x_2x_3,\ 0)\rangle \subseteq \mathbb{Q}[x_1, x_2, x_3]^3,\ d = 3$

c) Explain how one can use a truncated Gröbner basis computation to develop an efficient homogeneous submodule membership test. Then implement your algorithm in a CoCoA function `HomogIsIn(...)` which takes a homogeneous system of generators of a graded submodule M of F and a homogeneous vector $v \in F$ and checks whether or not we have $v \in M$.

d) Use your function `HomogIsIn(...)` to find out which of the following homogeneous vectors are contained in the module M_3 defined above.

1) $v_1 = (x_2^2x_3,\ x_1^2x_3,\ x_1x_2x_3 - x_1x_3^2)$
2) $v_2 = (x_2^3 - x_1x_2x_3,\ x_1x_2x_3,\ x_1^2x_2 - x_1x_2x_3)$
3) $v_3 = (x_1x_2^2x_3,\ x_1x_2^3 - x_2^3x_3,\ x_1^2x_3^2)$

e) Let $f, g \in P$ be two non-zero homogeneous polynomials. Show that $\mathrm{Syz}_P(f, g)$ is the graded submodule of $P(-\deg_W(f)) \oplus P(-\deg_W(g))$ generated by $(g/\gcd(f, g),\ -f/\gcd(f, g))$.

f) Let $1 \leq m < n$, and let I be a homogeneous ideal in P. Suppose it is known that the elimination ideal $I \cap K[x_1, \ldots, x_m]$ is a principal ideal generated by a homogeneous polynomial $f \in I$. Describe a variant of your function `TruncGB(...)` which computes f. Implement it in a CoCoA function `HomogElimPoly(...)` and apply it to the following cases, where $P = \mathbb{Q}[x_1, \ldots, x_6]$ is standard graded and $m = 4$.

1) $I_1 = (x_1x_6 - 2x_4^2,\ x_1^2 - 2x_1x_5 - x_2^2 + x_5^2 + x_6^2,\ x_3^2 - x_5^2 - x_6^2)$
2) $I_2 = (x_1x_4^3 - \frac{1}{2}x_4^3x_5 - x_6^4,\ x_2x_4 - 2x_5^2 - x_4x_6,\ x_3 - \frac{1}{3}x_6)$
3) $I_3 = (x_1^3 - 3x_4^2x_6 - 3x_5^2x_6 + x_6^3,\ x_2^3 - 3x_4^2x_5 + x_5^3 - 3x_5x_6^2,\ x_3^2 - 3x_5^2 + 3x_6^2)$

4.6 Minimal Homogeneous Systems of Generators

The Pythagorean Theorem employed 24 words,
the Lord's Prayer has 66 words,
Archimedes' Principle has 67 words,
the 10 Commandments have 179 words,
the Gettysburg Address had 286 words,
the Declaration of Independence 1,300 words,
and finally,
the European Commission's regulation on the sale of cabbage: 26,911 words.
(Dennis Gartman)

In Proposition 4.1.22 we saw that finitely generated graded modules over polynomial rings with gradings of positive type have the property that all irredundant systems of generators have the same number of elements. Hence every homogeneous system of generators contains a minimal one. Given a system of homogeneous generators of a module, is there a good method to compute a minimal one? What do we mean by a *good method?*

We have already addressed a similar problem in Corollary 3.1.12, where we suggested that syzygies be used. Here we can do much better, but in order to realize the benefit of using the grading we need some preparatory work which, in turn, requires a lot of sweat. Fortunately, half the job has already been done in Subsection 4.5.B, where we studied the behaviour of truncated Gröbner bases under the process of adding one homogeneous generator at a time. The second half of the job is based on Proposition 4.6.1, where we prove a nice characterization of minimal homogeneous systems of generators. In particular, we get a better insight into the problem of deciding whether the addition of an element to a minimal system of generators produces a minimal system of generators of the enlarged module (see Corollary 4.6.2).

Then we describe a variation of the Homogeneous Buchberger Algorithm 4.5.5 which allows us to compute efficiently a minimal set of generators while also computing a homogeneous Gröbner basis. This is the main result of the entire section. Therefore we illustrate it by working through one example in full detail (see Example 4.6.6). We conclude the section with Theorem 4.6.7. It treats the special case where the input set of generators is already a reduced Gröbner basis. Besides being an interesting application of the methods previously described, it serves as a basis for the optimizations of Buchberger's algorithm developed in Tutorial 59.

In this second volume we usually have longer sections than in the first one. However, we decided to make this section a little shorter. Indeed, we are proud to announce that, after minimalizing here and truncating there, the number of words in this section is about 4,300, far fewer than the European Commission's regulation on the sale of cabbage ... even if you include the words in this sentence.

Let K be a field, let $m, n, r \geq 1$, let $P = K[x_1, \ldots, x_n]$ be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type, let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, and let M

be a non-zero graded P-submodule of $F = \bigoplus_{i=1}^{r} P(-\delta_i)$. Furthermore, let $\{g_1, \ldots, g_s\} \subseteq M \setminus \{0\}$ be a homogeneous system of generators of M, and let $d_i = \deg_W(g_i)$ for $i = 1, \ldots, s$.

Using the Graded Version of Nakayama's Lemma 1.7.15, we have seen in Proposition 4.1.22 that the irredundant homogeneous systems of generators of the graded submodule M of F are all minimal. Hence they have the same number of elements which we shall denote by $\mu(M)$. Our first task is to describe explicitly a subset of $\{g_1, \ldots, g_s\}$ which is a minimal system of generators of M.

Recall that in Section 4.1 we showed that the set $\Gamma = \{d \in \mathbb{Z}^m \mid P_d \neq 0\}$ is a submonoid of $\mathbb{Z}^m$ on which we have a term ordering τ, and that on the Γ-monomodule Σ generated by all degrees of non-zero elements of M we have a module ordering σ which is a well-ordering and compatible with τ. The following proposition will be a useful tool for solving our task.

Proposition 4.6.1. (Characterization of Minimal Homogeneous Systems of Generators)
Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type, let M be a graded submodule of F generated by non-zero homogeneous vectors $\{g_1, \ldots, g_s\}$, and assume that $\deg_W(g_1) \leq_\sigma \deg_W(g_2) \leq_\sigma \cdots \leq_\sigma \deg_W(g_s)$.

a) The set $\{g_1, \ldots, g_s\}$ is a minimal system of generators of M if and only if we have $g_i \notin \langle g_1, \ldots, g_{i-1}\rangle$ for $i = 1, \ldots, s$.
b) The set $\{g_i \mid i \in \{1, \ldots, s\}, g_i \notin \langle g_1, \ldots, g_{i-1}\rangle\}$ is a minimal system of generators of M.

Proof. First we prove a). If $\{g_1, \ldots, g_s\}$ is a minimal set of generators of M, then no relation of the form $g_i \in \langle g_1, \ldots, g_{i-1}\rangle$ can hold, since otherwise we would have $M = \langle g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_s\rangle$. Conversely, if $\{g_1, \ldots, g_s\}$ is not a minimal set of generators of M, then there exists an index $i \in \{1, \ldots, s\}$ such that $g_i \in \langle g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_s\rangle$. Using Corollary 1.7.11, we obtain a representation $g_i = \sum_{j \neq i} f_j g_j$, where each $f_j \in P$ is a homogeneous polynomial of degree $\deg_W(g_i) - \deg_W(g_j)$.

We have already recalled that there exists a term ordering τ on the monoid $\Gamma = \{d \in \mathbb{Z}^m \mid P_d \neq 0\}$ such that σ is compatible with τ. Therefore we have $\deg_W(f_j) \geq_\tau 0$ whenever $f_j \neq 0$. So, if $\deg_W(g_j) >_\sigma \deg_W(g_i)$, it follows that $f_j = 0$. Hence there are two possibilities. Either we have $\deg_W(g_i) >_\sigma \deg_W(g_j)$ for all j such that $f_j \neq 0$. In this case, those indices j satisfy $j < i$ by the assumption that the degrees of $g_1, \ldots, g_s$ are ordered increasingly, and therefore we get $g_i \in \langle g_1, \ldots, g_{i-1}\rangle$. Or there exist some indices j with $f_j \neq 0$ such that $\deg_W(g_j) = \deg_W(g_i)$. In that case, the polynomials f_j corresponding to those indices j are non-zero constants by Proposition 4.1.19.a. We define $j_{\max} = \max\{j \in \{1, \ldots, s\} \mid f_j \in K \setminus \{0\}\}$ and get $g_{j_{\max}} \in \langle g_1, \ldots, g_{j_{\max}-1}\rangle$. In both cases, we obtain a contradiction to our hypothesis.

Now let us show b). Let $S = \{g_i \mid i \in \{1, \ldots, s\}, g_i \notin \langle g_1, \ldots, g_{i-1}\rangle\}$. We see that the elements of S form a system of generators of M, because

an element g_i such that $g_i \in \langle g_1, \ldots, g_{i-1} \rangle$ is also contained in the module $\langle g_j \in S \mid 1 \leq j \leq i-1 \rangle$. The fact that this system of generators is minimal follows from a). □

Later we shall use this proposition to construct minimal systems of generators of M by adding one element at a time. The following result is an immediate consequence of a).

Corollary 4.6.2. *Let M be a graded submodule of F, let $\{g_1, \ldots, g_s\}$ be a minimal homogeneous system of generators of M, and let $g \in F \setminus M$ be a homogeneous vector such that $\deg_W(g) \geq_\sigma \max_\sigma\{\deg_W(g_i) \mid i = 1, \ldots, s\}$.*

Then $\{g_1, \ldots, g_s, g\}$ is a minimal system of generators of the graded module $M + \langle g \rangle$. In particular, we have $\mu(M + \langle g \rangle) = \mu(M) + 1$.

Clearly part b) of the proposition could be applied to compute a minimal system of generators of M from a given homogeneous system of generators, since module membership can be effectively checked. But this method would require a large number of Gröbner basis computations. Therefore we will now look for something better.

The following extension of the Homogeneous Buchberger Algorithm computes a minimal system of generators of M contained in that given while also computing a Gröbner basis. This variant is an efficient way to find a minimal system of generators. If one is not interested in the Gröbner basis, one can speed it up even more by truncating the computation in the appropriate degree.

Theorem 4.6.3. (Buchberger's Algorithm with Minimalization) *Let $P = K[x_1, \ldots, x_n]$ be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let M be a graded submodule of F, and let $\mathcal{V} = (v_1, \ldots, v_s)$ be a deg-ordered tuple of non-zero homogeneous vectors which generate M. Furthermore, let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r \rangle$. Consider the following sequence of instructions.*

1) *Let $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, $s' = 0$, and $\mathcal{V}_{\min} = \emptyset$.*
2) *Let d be the smallest degree with respect to* `Lex` *of an element in B or in $\mathcal{W}$. Form the subset B_d of B, form the subtuple $\mathcal{W}_d$ of $\mathcal{W}$, and delete their entries from B and $\mathcal{W}$, respectively.*
3) *If $B_d = \emptyset$, continue with step 6). Otherwise, choose a pair $(i, j) \in B_d$ and remove it from B_d.*
4) *Compute the S-vector S_{ij} and its normal remainder $S'_{ij} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$. If $S'_{ij} = 0$, continue with step 3).*
5) *Increase s' by one, append $g_{s'} = S'_{ij}$ to the tuple $\mathcal{G}$, and append the set $\{(i, s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$ to the set B. Continue with step 3).*
6) *If $\mathcal{W}_d = \emptyset$, continue with step 9). Otherwise, choose a vector $v \in \mathcal{W}_d$ and remove it from $\mathcal{W}_d$.*
7) *Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v)$. If $v' = 0$, continue with step 6).*

8) Increase s' by one, append $g_{s'} = v'$ to the tuple $\mathcal{G}$, append v to the tuple $\mathcal{V}_{\min}$, and append $\{(i, s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$ to the set B. Continue with step 6).

9) If $B = \emptyset$ and $\mathcal{W} = \emptyset$, return the pair $(\mathcal{G}, \mathcal{V}_{\min})$ and stop. Otherwise, continue with step 2).

This is an algorithm which returns a pair $(\mathcal{G}, \mathcal{V}_{\min})$ such that $\mathcal{G}$ is a deg-ordered tuple forming a homogeneous σ-Gröbner basis of M, and $\mathcal{V}_{\min}$ is a subtuple of $\mathcal{V}$ whose elements are a minimal system of generators of M.

Proof. In the light of Theorem 4.5.5, we only have to show that the elements in $\mathcal{V}_{\min}$ are a minimal set of generators of M. Since the algorithm is finite, it operates in only finitely many degrees d. Therefore it suffices to prove degree by degree that $\mathcal{V}_{\min}$ is a minimal system of generators of $\langle M_{\leq d} \rangle$ after the algorithm has finished working on elements of degree d.

This is the case after step 1), i.e. when $\mathcal{V}_{\min} = \emptyset$ is a minimal system of generators of the zero module. Suppose it is true for the last degree treated before d. Inductively, we can show that the elements of $\mathcal{G}$ continue to be contained in the module $\langle M_{<d} \rangle$ while we are looping through steps 3), 4), and 5) of the algorithm. Namely, every time an element of the form $\mathrm{NF}_{\sigma,\mathcal{G}}(S_{ij})$ is added to $\mathcal{G}$, it is clearly contained in the module generated by the previous elements of $\mathcal{G}$. Furthermore, by Proposition 4.5.10, the tuple $\mathcal{G}$ forms a d-truncated Gröbner basis of $\langle M_{<d} \rangle$ after we have finished looping through steps 3), 4), and 5), i.e. when we have treated all pairs of degree d.

Now let $\mathcal{W}_d = (w_1, \ldots, w_\ell)$, and let the numbering of these vectors correspond to the order in which they are chosen in step 6). We show that, for each application of steps 6), 7), and 8), the elements of $\mathcal{V}_{\min}$ continue to be a minimal system of generators of the module they generate, and that this module always is equal to the one generated by the elements of $\mathcal{G}$. Furthermore, the elements of $\mathcal{G}$ are always a d-truncated σ-Gröbner basis of that module.

When a new vector $v = w_i$ is chosen in step 6), there are two possibilities. If $v' = 0$ in step 7), then v is already contained in the module M' generated by the elements of $\mathcal{V}_{\min}$. Otherwise, both v' and v lie outside M': since $\mathcal{G}$ is a d-truncated σ-Gröbner basis of M', we can apply the Submodule Membership Test 2.4.10.a. In this case, the tuple $\mathcal{V}_{\min}$, augmented by v, is a minimal system of generators of the module $M' + \langle v \rangle = M' + \langle v' \rangle$ by Corollary 4.6.2. Moreover, the tuple $\mathcal{G}$, augmented by v', is a d-truncated σ-Gröbner basis of $M' + \langle v' \rangle$ by Corollary 4.5.14.

Altogether, it follows that, after degree d is finished, the elements of the tuple $\mathcal{V}_{\min}$ are a minimal system of generators of $\langle M_{\leq d} \rangle$, as we wanted to show. □

It is easy to see that Buchberger's Algorithm with Minimalization also works if the initial tuple $\mathcal{V}$ is not deg-ordered. In this case, the tuple $\mathcal{V}_{\min}$ may not be a subtuple of $\mathcal{V}$, but will be a permutation of some subtuple.

As we mentioned above, if we are only interested in the minimal system of generators, this algorithm can be speeded up as follows.

Remark 4.6.4. In the setting of the theorem, suppose that we stop the execution of the algorithm after degree $d_{\max} = \deg_W(v_s)$ is finished and that we append only the pairs $\{(i,s') \mid 1 \leq i < s',\ \gamma_i = \gamma_{s'},\ \deg_W((i,s')) \leq_{\texttt{Lex}} d_{\max}\}$ to the set B in steps 5) and 8). Then the resulting tuple $\mathcal{V}_{\min}$ is still a subtuple of $\mathcal{V}$ which contains a minimal homogeneous system of generators of M.

In step 8) of Buchberger's Algorithm with Minimalization 4.6.3, we can append the vector v', instead of v, to $\mathcal{V}_{\min}$. The resulting tuple still generates M minimally. However, these generators are contained in the computed Gröbner basis $\mathcal{G}$ instead of in the initial tuple $\mathcal{V}$. They have the additional property that each vector is fully reduced against the previous ones. For later reference, let us spell out this version of the algorithm.

Corollary 4.6.5. *Modify the theorem by replacing steps 1), 8), and 9) with the following instructions.*

1') Let $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, $s' = 0$, and $\mathcal{G}_{\min} = \emptyset$.
8') Increase s' by one, append $g_{s'} = v'$ to the tuples $\mathcal{G}$ and $\mathcal{G}_{\min}$, and append $\{(i,s') \mid 1 \leq i < s',\ \gamma_i = \gamma_{s'}\}$ to the set B. Continue with step 6).
9') If $B = \emptyset$ and $\mathcal{W} = \emptyset$, return the pair $(\mathcal{G}, \mathcal{G}_{\min})$ and stop. Otherwise, continue with step 2).

Then the resulting set of instructions defines an algorithm. It returns a pair $(\mathcal{G}, \mathcal{G}_{\min})$ such that $\mathcal{G}$ is a deg-ordered tuple which forms a homogeneous σ-Gröbner basis of M, and $\mathcal{G}_{\min}$ is a subtuple of $\mathcal{G}$ which minimally generates M.

Let us apply the Buchberger Algorithm with Minimalization 4.6.3 to a concrete case and follow its computations on a step-by-step basis.

Example 4.6.6. Let $P = \mathbb{Q}[x,y,z]$ be standard graded, i.e. graded by $W = (1 \ \cdots \ 1)$, let $\mathcal{V}$ be the tuple of polynomials $\mathcal{V} = (v_1, v_2, v_3, v_4)$, where $v_1 = x^2 - xy$, $v_2 = x^2 - yz$, $v_3 = x^3 - yz^2$, and $v_4 = y^5 - z^5$, and let I be the ideal generated by the polynomials in $\mathcal{V}$.

Our goal is to compute a minimal set of generators of I. We choose the term ordering $\sigma = \texttt{DegRevLex}$ and follow Buchberger's Algorithm with Minimalization 4.6.3. However, we stop the computation after degree $d_{\max} = \deg_W(v_4) = 5$ is finished.

1) Let $B = \emptyset$, $\mathcal{W} = (v_1, v_2, v_3, v_4)$, $\mathcal{G} = \emptyset$, $s' = 0$, and $\mathcal{V}_{\min} = \emptyset$.
2) Let $d = \deg(v_1) = 2$, $\mathcal{W}_2 = (v_1, v_2)$, $\mathcal{W} = (v_3, v_4)$, and $B_2 = \emptyset$.
3) Since $B_2 = \emptyset$, we continue with step 6).
6) Choose $v = v_1$ and let $\mathcal{W}_2 = (v_2)$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = v_1$.

8) Let $s' = 1$, $\mathcal{G} = (g_1)$ with $g_1 = v_1$, $\mathcal{V}_{\min} = (v_1)$, and $B = \emptyset$.
6) Choose $v = v_2$ and let $\mathcal{W}_2 = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = xy - yz$.
8) Let $s' = 2$, $\mathcal{G} = (g_1, g_2)$ with $g_2 = xy - yz$, $\mathcal{V}_{\min} = (v_1, v_2)$, and $B = \{(1,2)\}$.
6) Since $\mathcal{W}_2 = \emptyset$, we continue with step 9).
9) Since $\mathcal{W} \neq \emptyset$, we continue with step 2).
2) Let $d = \deg(v_3) = 3$. Since $d \leq d_{\max} = 5$, we let $\mathcal{W}_3 = (v_3)$, $\mathcal{W} = (v_4)$, $B_3 = \{(1,2)\}$, and $B = \emptyset$. (Notice that $\deg_W((1,2)) = 3$.)
3) Choose $(1,2) \in B_3$ and let $B_3 = \emptyset$.
4) Compute $S_{12} = xyz - xy^2$ and $S'_{12} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{12}) = -y^2z + yz^2$.
5) Let $s' = 3$, let $\mathcal{G} = (g_1, g_2, g_3)$ with $g_3 = -y^2z + yz^2$, and let $B = \{(1,3), (2,3)\}$.
3) Since $B_3 = \emptyset$, we continue with step 6).
6) Choose $v = v_3$ and let $\mathcal{W}_3 = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = 0$ and continue with step 6).
6) Since $\mathcal{W}_3 = \emptyset$, we continue with step 9).
9) Since $\mathcal{W} \neq \emptyset$, we continue with step 2).
2) Let $d = \deg_W((2,3)) = 4$. Since $d \leq d_{\max} = 5$, we let $\mathcal{W}_4 = \emptyset$, $B_4 = \{(2,3)\}$, and $B = \{(1,3)\}$.
3) Choose $(2,3) \in B_4$, and let $B_4 = \emptyset$.
4) Compute $S_{23} = xyz^2 - y^2z^2$ and $S'_{23} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{23}) = 0$. Since $S'_{23} = 0$, we continue with step 3).
3) Since $B_4 = \emptyset$, we continue with step 6).
6) Since $\mathcal{W}_4 = \emptyset$, we continue with step 9).
9) Since $\mathcal{W} \neq \emptyset$, we continue with step 2).
2) Let $d = \deg(v_4) = 5$. Since $d \leq d_{\max} = 5$, we let $\mathcal{W}_5 = (v_4)$, $\mathcal{W} = \emptyset$, $B_5 = \{(1,3)\}$, and $B = \emptyset$.
3) Choose $(1,3) \in B_5$, and let $B_5 = \emptyset$.
4) Compute $S_{13} = -xy^3z + x^2yz^2$ and $S'_{13} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{13}) = 0$. Since we have $S'_{13} = 0$, we continue with step 3).
3) Since $B_5 = \emptyset$, we continue with step 6).
6) Choose $v = v_4$ and let $\mathcal{W}_5 = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = v_4$.
8) Let $s' = 4$, $\mathcal{G} = (g_1, g_2, g_3, g_4)$ with $g_4 = v_4$, let $\mathcal{V}_{\min} = (v_1, v_2, v_4)$, and let $B = \{(1,4), (2,4), (3,4)\}$.
6) Since $\mathcal{W}_5 = \emptyset$, we continue with step 9).
9) Since $B \neq \emptyset$, we continue with step 2).
2) Let $d = \deg_W((2,4)) = 6$. Since $d > d_{\max} = 5$, we return $(\mathcal{G}, \mathcal{V}_{\min})$ and stop.

The result of this algorithm is that $\mathcal{V}_{\min} = (v_1, v_2, v_4)$ is a minimal system of generators of I. Notice that the returned tuple $\mathcal{G}$ is a 5-truncated σ-Gröbner basis of I. If we are interested in a true σ-Gröbner basis of I, we have to continue the algorithm in degree ≥ 6 until we get $B = \emptyset$ in step 2).

The minimal homogeneous system of generators computed by Corollary 4.6.5 is $\mathcal{H} = (g_1, g_2, g_4)$, where $g_1 = v_1$, $g_2 = v_2 - v_1$, and $g_4 = v_4$.

Finally, we end this section with an application of the preceding theorem which will be essential for optimizing the Homogeneous Buchberger Algorithm 4.5.5 in Tutorial 59. More precisely, we want to apply the Buchberger Algorithm with Minimalization 4.6.3 to a reduced Gröbner basis and improve it significantly in that case.

Theorem 4.6.7. (Minimal Generators in a Reduced Gröbner Basis) *Let $P = K[x_1, \ldots, x_n]$ be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let M be a graded submodule of F, let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$, and let the deg-ordered tuple $\mathcal{V} = (v_1, \ldots, v_s)$ be the reduced σ-Gröbner basis of M. Finally, let $d_{\max} = \deg_W(v_s)$, and consider the following instructions.*

1) *Let $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, $s' = 0$, and $\mathcal{V}_{\min} = \emptyset$.*
2) *Let d be the smallest degree with respect to* `Lex` *of an element in B or in $\mathcal{W}$. Form the subset B_d of B, the subtuple $\mathcal{W}_d$ of $\mathcal{W}$, and delete their entries from B and $\mathcal{W}$, respectively.*
3) *If $B_d = \emptyset$, continue with step 6). Otherwise, choose a pair $(i, j) \in B_d$ and remove it from B_d.*
4) *Compute $S'_{ij} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$. If $S'_{ij} = 0$, continue with step 3).*
5) *Increase s' by one, append the element $g_{s'} = S'_{ij}$ to $\mathcal{G}$, and append the set $\{(i, s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}, \deg_W((i, s')) \leq_{\mathtt{Lex}} d_{\max}\}$ to the set B. Continue with step 3).*
6) *If $\mathcal{W}_d = \emptyset$, continue with step 9). Otherwise, choose a vector $v \in \mathcal{W}_d$ and remove it from $\mathcal{W}_d$.*
7) *If $\mathrm{LT}_\sigma(v) = \mathrm{LT}_\sigma(g)$ for some $g \in \mathcal{G}$, then replace the element g in $\mathcal{G}$ by v, and continue with step 6).*
8) *Increase s' by one, append $g_{s'} = v$ to $\mathcal{G}$ and $\mathcal{V}_{\min}$, and append the set $\{(i, s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}, \deg_W((i, s')) \leq_{\mathtt{Lex}} d_{\max}\}$ to the set B. Continue with step 6).*
9) *If $B = \emptyset$ and $\mathcal{W} = \emptyset$, return the tuple $\mathcal{V}_{\min}$ and stop. Otherwise, continue with step 2).*

This is an algorithm which computes a subtuple $\mathcal{V}_{\min}$ of $\mathcal{V}$ such that $\mathcal{V}_{\min}$ is a minimal homogeneous system of generators of M.

Proof. It suffices to show that this procedure has the same effect as running the Buchberger Algorithm with Minimalization 4.6.3 on $\mathcal{V}$. The main difference occurs in step 7).

First we use induction on d to show that, after we have finished some degree d, the tuple $\mathcal{G}$ has the same elements as $\mathcal{V}_{\leq d}$. Every element of $\mathcal{V}_d$ is put into $\mathcal{G}$ at some point in step 7) or 8). On the other hand, if an element $g_{s'}$ is put into $\mathcal{G}$ in step 5), it has a leading term which is not a multiple of an element of $\mathcal{V}_{<d}$. Hence it is replaced in $\mathcal{G}$ at some point in step 7).

Next we note that, after we have finished cycling through steps 3), 4), and 5) in degree d, the tuple $\mathcal{G}$ is a d-truncated minimal σ-Gröbner basis of $\langle M_{<d} \rangle$. Here minimal means that no proper subtuple of $\mathcal{G}$ is a d-truncated σ-Gröbner basis of $\langle M_{<d} \rangle$.

Now we turn our attention to the loop described in steps 6), 7) and 8). Notice that the effect of steps 7) and 8) is essentially independent of the order in which we choose the elements $v \in \mathcal{W}_d$ in step 6). Hence we can assume for the purposes of this proof that we always choose the vector v in $\mathcal{W}_d$ which has the minimal leading term with respect to σ. With this assumption, we show inductively that when we run steps 7) and 8) for some element $v \in \mathcal{W}_d$, at each point the elements in $\mathcal{G}$ are a minimal σ-Gröbner basis of the module they generate, and the elements of $\mathcal{V}_{\min}$ are a minimal system of generators of that module.

For the induction step, we have to consider two cases: either v replaces an existing element of $\mathcal{G}$ in step 7) or is appended to both $\mathcal{G}$ and $\mathcal{V}_{\min}$ in step 8). In the first case, it suffices to show that the module generated by the elements of $\mathcal{G}$ does not change when we perform the swap, i.e. that the difference $v - g$ is contained in this module. This follows from the observations that $\mathrm{LT}_\sigma(v-g) <_\sigma \mathrm{LT}_\sigma(v)$ and all elements v' in $\mathcal{V}$ such that $\mathrm{LT}_\sigma(v') <_\sigma \mathrm{LT}_\sigma(v)$ are already in $\mathcal{G}$. Since $v - g \xrightarrow{\mathcal{V}} 0$, we have $v - g \xrightarrow{\mathcal{G}} 0$. In the second case, it is clear that $\mathcal{G}$ continues to be a minimal Gröbner basis of the module it generates by Corollary 4.5.14, and $\mathcal{V}_{\min}$ continues to be a minimal system of generators of that module by Corollary 4.6.2.

Finally, we note that in step 8) we can append v to $\mathcal{G}$ without passing to the normal remainder, since v is an element of a reduced Gröbner basis and thus irreducible. □

Remark 4.6.8. Let us make some observations about this algorithm.

a) The proof of the theorem shows that the algorithm reconstructs the given reduced Gröbner basis inside $\mathcal{G}$, and that $\mathcal{G}_{\leq d}$ has the same elements as $\mathcal{V}_{\leq d}$ after some degree d is finished.
b) In step 4) it is not essential to compute the normal remainder $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$. Rather, it suffices to reduce the leading term of S_{ij} as far as possible.
c) The non-zero elements $\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$ computed in step 4) and the elements $v \in \mathcal{V}_d$ which replace values already in $\mathcal{G}$ in step 7) are in $1-1$ correspondence, since every new element computed in step 4) must have a new leading term in the leading term module of M. This new leading term must be the leading term of an element in the reduced Gröbner basis, hence it is replaced.

We conclude this section by applying Theorem 4.6.7 to a concrete case.

Example 4.6.9. Let $P = K[x, y, z]$ be standard graded, let $\mathcal{V}$ be the tuple of polynomials $\mathcal{V} = (v_1, v_2, v_3, v_4, v_5)$, where $v_1 = x^2 - yz$, $v_2 = xy - yz$, $v_3 = y^2z - yz^2$, $v_4 = y^3$, and $v_5 = yz^3$, and let I be the ideal generated by the polynomials in $\mathcal{V}$.

We assume that we know in advance that $\mathcal{V}$ is the reduced σ-Gröbner basis of I, where $\sigma = \texttt{DegRevLex}$. Our goal is to compute a minimal set of generators of I. To this end, we follow the algorithm explained in Theorem 4.6.7. We note that $d_{\max} = 4$.

1) Let $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, $s' = 0$, and $\mathcal{V}_{\min} = \emptyset$.
2) Let $d = 2$, $B_2 = \emptyset$, $\mathcal{W}_2 = (v_1, v_2)$, and $\mathcal{W} = (v_3, v_4, v_5)$.
3) Since $B_2 = \emptyset$, we continue with step 6).
6) Choose $v = v_1$ and let $\mathcal{W}_2 = (v_2)$.
8) Let $s' = 1$, $\mathcal{G} = (v_1)$, $\mathcal{V}_{\min} = (v_1)$, and $B = \emptyset$.
6) Choose $v = v_2$, and let $\mathcal{W}_2 = \emptyset$.
8) Let $s' = 2$, $\mathcal{G} = (v_1, v_2)$, $\mathcal{V}_{\min} = (v_1, v_2)$, and $B = \{(1, 2)\}$.
6) Since $\mathcal{W}_2 = \emptyset$, we continue with step 9).
9) Since $B \neq \emptyset$ and $\mathcal{W} \neq \emptyset$, we continue with step 2).
2) We note that $\deg_W(v_3) = 3$ and $\deg_W((1, 2)) = 3$. Hence we let $d = 3$, $\mathcal{W}_3 = (v_3, v_4)$, $\mathcal{W} = (v_5)$, $B_3 = \{(1, 2)\}$, and $B = \emptyset$.
3) Choose $(1, 2) \in B_3$, and let $B_3 = \emptyset$.
4) Compute $S'_{12} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{12}) = -y^2z + yz^2$.
5) Let $s' = 3$, $\mathcal{G} = (v_1, v_2, g_3)$ with $g_3 = -y^2z + yz^2$, and $B = \{(2, 3)\}$. (Notice that $\deg_W((1, 3)) = 5 > 4 = d_{\max}$.)
3) Since $B_3 = \emptyset$, we continue with step 6).
6) Choose $v = v_3$, and let $\mathcal{W}_3 = (v_4)$.
7) Since $\mathrm{LT}_\sigma(v) = \mathrm{LT}_\sigma(g_3)$, we replace g_3, i.e. we let $\mathcal{G} = (v_1, v_2, v_3)$.
6) Choose $v = v_4$, and let $\mathcal{W}_3 = \emptyset$.
8) Let $s' = 4$, $\mathcal{G} = (v_1, v_2, v_3, v_4)$, $\mathcal{V}_{\min} = (v_1, v_2, v_4)$, and $B = \{(2, 3), (2, 4), (3, 4)\}$.
6) Since $\mathcal{W}_3 = \emptyset$, we continue with step 9).
9) Since $B \neq \emptyset$ and $\mathcal{W} \neq \emptyset$, we continue with step 2).
2) Note that $\deg_W(v_5) = \deg_W((2, 3)) = \deg_W((2, 4)) = \deg_W((3, 4)) = 4$. Hence we let $d = 4$, $\mathcal{W}_4 = (v_5)$, $\mathcal{W} = \emptyset$, $B_4 = \{(2, 3), (2, 4), (3, 4)\}$, and $B = \emptyset$.
3) Choose $(2, 3) \in B_4$, and let $B_4 = \{(2, 4), (3, 4)\}$.
4) Compute $S'_{23} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{2,3}) = 0$.
3) Choose $(2, 4) \in B_4$, and let $B_4 = \{(3, 4)\}$.
4) Compute $S'_{24} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{2,4}) = -yz^3$.
5) Let $s' = 5$, $\mathcal{G} = (v_1, v_2, v_3, v_4, g_5)$ with $g_5 = -yz^3$, and $B = \emptyset$, since all the pairs $(1, 5)$, $(2, 5)$, $(3, 5)$, and $(4, 5)$ have degree bigger than $d_{\max}$.
3) Choose $(3, 4) \in B_4$, and let $B_4 = \emptyset$.
4) Compute $S'_{34} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{3,4}) = 0$.
3) Since $B_4 = \emptyset$, we continue with step 6).
6) Choose $v = v_5$, and let $\mathcal{W}_4 = \emptyset$.
7) Since $\mathrm{LT}_\sigma(v) = \mathrm{LT}_\sigma(g_5)$, we replace g_5, i.e. we let $\mathcal{G} = (v_1, v_2, v_3, v_4, v_5)$.
6) Since $\mathcal{W}_4 = \emptyset$, we continue with step 9).
9) Since $B = \emptyset$ and $\mathcal{W} = \emptyset$, we return $\mathcal{V}_{\min} = (v_1, v_2, v_4)$ and stop.

The result of this algorithm is that $\mathcal{V}_{\min} = (v_1, v_2, v_4)$ is a minimal homogeneous system of generators of I which is contained in $\mathcal{V}$. Notice how few reduction steps we had to perform. The treatment of the generators $v_1, \ldots, v_5$ was a purely combinatorial affair.

Exercise 1. Let K be a field and $P = K[x, y]$. Find an example of an ideal I in P and an element $f \in P \setminus I$ such that $\mu(I + (f)) < \mu(I)$, and another example such that $\mu(I + (f)) = \mu(I)$.

Exercise 2. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded, let $d \geq 1$, and let $I \subseteq P$ be a homogeneous ideal. Show that $\mu(I^d) \leq \binom{\mu(I)+d-1}{d}$ and give an example in which this inequality is strict.

Exercise 3. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be graded by a positive matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $P_+ = \bigoplus_{d >_{\mathtt{Lex}} 0} P_d$, let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, let $F = \bigoplus_{i=1}^r P(-\delta_i)$, let M be a non-zero graded submodule of F, and let $g \in F \setminus M$ be a homogeneous element. Show that the following conditions are equivalent.

a) $\mu(M + \langle g \rangle) = \mu(M) + 1$
b) $(P_+ \cdot (M + \langle g \rangle)) \cap M = P_+ \cdot M$
c) $(P_+ \cdot \langle g \rangle) \cap M \subseteq P_+ \cdot M$

Hint: Use $\mu(M) = \dim_K(M/(P_+ \cdot M))$.

Exercise 4. Use the previous exercise to give an alternative proof of Theorem 4.6.1.a.
Hint: Show that $\mu(\langle g_1, \ldots, g_i \rangle) = \mu(\langle g_1, \ldots, g_{i-1} \rangle) + 1$ by verifying condition c) of the previous exercise.

Exercise 5. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, and let $F = \bigoplus_{i=1}^r P(-\delta_i)$. Given a module term ordering σ on $\mathbb{T}^n\langle e_1, \ldots, e_r \rangle$ and homogeneous vectors $v_1, \ldots, v_s \in F$ such that no two of them have their leading term in the same position, show that $\{v_1, \ldots, v_s\}$ is a minimal system of generators of the graded submodule $\langle v_1, \ldots, v_s \rangle$ of F.

Exercise 6. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, let M be a non-zero graded submodule of $F = \bigoplus_{i=1}^r P(-\delta_i)$, and let $d \in \mathbb{Z}^m$. Furthermore, assume that $G = \{g_1, \ldots, g_s\}$ is a d-truncated σ-Gröbner basis of M, and H is a minimal homogeneous set of generators of M which consists of elements of degree $\leq d$. Finally, let $g_{s+1}, \ldots, g_{s'} \in F$ be homogeneous elements of degree d such that, for $s + 1 \leq j \leq s'$, the leading term of g_j is not a multiple of a term $\mathrm{LT}_\sigma(g_i)$ with $i < j$.

a) Show that the set $G \cup \{g_{s+1}, \ldots, g_{s'}\}$ is a d-truncated Gröbner basis of the module $M' = M + \langle g_{s+1}, \ldots, g_{s'} \rangle$.
b) Show that the set $H \cup \{g_{s+1}, \ldots, g_{s'}\}$ is a minimal homogeneous set of generators of M'.

Exercise 7. Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let σ be a term ordering on $\mathbb{T}^n$. Furthermore, let $f_1, \ldots, f_s \in P \setminus K$, let I be the ideal generated by $\{f_1, \ldots, f_s\}$, and assume that $\gcd(\mathrm{LT}_\sigma(f_i), \mathrm{LT}_\sigma(f_j)) = 1$ for $1 \leq i < j \leq s$. Prove that $\{f_1, \ldots, f_s\}$ is an irredundant system of generators of I.

Exercise 8. In the ring $\mathbb{Q}[x, y, z]$, consider the polynomials $f_1 = x^2 - yz$, $f_2 = xy - z^2$, $f_3 = y^2z$, $f_4 = xz^2$, $f_5 = yz^3$, and $f_6 = z^4$. Suppose you know that $\{f_1, \ldots, f_6\}$ is the reduced `DegRevLex`-Gröbner basis of the ideal $I = (f_1, f_2, f_3, f_4, f_5, f_6)$. Compute a minimal system of generators of I using Theorem 4.6.7.

Tutorial 58: Computing Some Minimal Systems of Generators

Minimalism is a cheap excuse for laziness.
(Anonymous)

In this section we have seen several methods for computing a minimal homogeneous system of generators of a graded submodule. Here we ask you to implement and compare them. For good measure we throw in another one which is based on a syzygy computation and a smart application of Nakayama's Lemma. Of course, the telling test for these competing methods is their practical performance. The handful of examples we provide here for your perusal is merely meant to serve as a quick check for correctness. To get a thorough grasp of the relative merits of various methods for minimalization you need to overcome your innate laziness and continue to explore their efficiency on your own.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, let $F = \bigoplus_{i=1}^r P(-\delta_i)$, and let $\mathcal{V} = (v_1, \ldots, v_s)$ be a deg-ordered tuple of non-zero vectors in F which generate a graded submodule M of F.

a) Using Proposition 4.6.1.b and the submodule membership test (see Proposition 2.4.10 and Tutorial 57.c), develop an algorithm for computing a subtuple $\mathcal{V}_{\min}$ of $\mathcal{V}$ which generates M minimally.

b) Implement this algorithm in a CoCoA function `Min1(...)`. Apply your function to the following tuples which generate graded submodules of $\mathbb{Q}[x, y, z] \oplus \mathbb{Q}[x, y, z](-2)$ where we use $W = (1\ 1\ 1)$.

1) $\mathcal{V}_1 = ((x^2 - xy, 0), (x^2 - yz, 0), (x^3 - yz^2, 0), (y^5 - z^5, 0))$
2) $\mathcal{V}_2 = ((x^4, y^2), (x^3y, yz), (x^2y^2, z^2), (0, y^3 - xyz), (0, y^2z - xz^2), (0, y^4 - x^2z^2), (x^3y^2 - x^4z, 0))$
3) $\mathcal{V}_3 = ((xyz, x - y), (x^4 + xyz^2, xz), (x^4, yz), (x^6 - x^5y, x^2y^2 - z^4), (x^2y^2z^2, x^2y^2 - z^4), (0, x^4y^2 - y^3z^3 - x^2z^4))$

c) Implement the Buchberger Algorithm with Minimalization 4.6.3 in a CoCoA function `Min2(...)` and apply it to the examples of b). Which function minimalizes the given tuple faster?
d) Modify the algorithm of Corollary 4.6.5 in such a way that it computes the reduced σ-Gröbner basis of M and a minimal system of generators of M contained in it.
e) Write a CoCoA function `Min3(...)` which implements the algorithm of d). The apply your function to the examples of b). Let $\mathcal{G}_1$, $\mathcal{G}_2$, and $\mathcal{G}_3$ be the resulting reduced Gröbner bases.
f) Implement the algorithm of Theorem 4.6.7 in a CoCoA function `Min4(...)`, apply it to the reduced Gröbner bases $\mathcal{G}_1$, $\mathcal{G}_2$, and $\mathcal{G}_3$, and compare the resulting minimal system of generators with the one computed by `Min3(...)`.
g) Now we want to compute a minimal homogeneous system of generators of M in yet another way. For $i = 1, \ldots, s$, let $d_i = \deg_W(v_i)$. Suppose that $\mathcal{W} = (w_1, \ldots, w_t)$ is a deg-ordered tuple of non-zero homogeneous vectors in $\bigoplus_{i=1}^{s} P(-d_i)$ which generate the syzygy module $\mathrm{Syz}_P(\mathcal{V})$. By considering $\mathcal{W}$ as a matrix of homogeneous polynomials and by substituting $x_i \mapsto 0$ for $i = 1, \ldots, n$ in the entries of that matrix, we obtain a matrix $\overline{\mathcal{W}} \in \mathrm{Mat}_{s,t}(K)$. Let $I \subseteq \{1, \ldots, s\}$ be the set of indices of the rows involved in some maximal non-zero minor of $\overline{\mathcal{W}}$. Then show that $\{v_i \mid i \in \{1, \ldots, s\} \setminus I\}$ is a minimal homogeneous system of generators of M.
Hint: Show that the corresponding vectors $\{\overline{v}_i \mid i \in \{1, \ldots, s\} \setminus I\}$ form a K-basis of $M/(x_1, \ldots, x_n)M$ and use the graded version of Nakayama's lemma.
h) Write a CoCoA function `Min5(...)` which implements the method for computing a minimal set of generators of M resulting from i). Apply your function to the examples in b) and discuss its efficiency.
Hint: To find the set I, take a non-zero row of $\overline{\mathcal{W}}$ and keep adding linearly independent rows until their number reaches the rank of that matrix.

Tutorial 59: Optimizing the Homogeneous Buchberger Algorithm

`(D)inner not ready: (A)bort, (R)etry, (P)izza`
(Anonymous)

In Tutorial 56 we saw some straightforward improvements of the Homogeneous Buchberger Algorithm 4.5.5. Since it suffices to treat a subset of all critical pairs for which the corresponding fundamental syzygies generate the syzygy module of the leading terms of the computed Gröbner basis, we were able to state a few simple rules for discovering unnecessary critical pairs. This tutorial is a natural continuation of that process.

After discovering that Rules 1) – 3) of Tutorial 56 do not always minimalize the critical pairs, we set out to achieve that minimalization by applying the algorithm of Theorem 4.6.7 to the minimal Gröbner basis Σ'' of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ we discovered in Tutorial 56.e. The resulting minimalization can be performed during the computation of the original Gröbner basis and is as fast as the application of Rules 1) – 3). In the end, we obtain a version of the Buchberger algorithm which is truly optimal in the sense that only a minimal set of critical pairs is treated.

Let the assumptions and notation be the same as in Tutorial 56. Namely, let K be a field, let the polynomial ring $P = K[x_1, \ldots, x_n]$ be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, let F be the graded free P-module $F = \bigoplus_{i=1}^r P(-\delta_i)$, and let $\mathcal{V} = (v_1, \ldots, v_s)$ be a deg-ordered tuple of non-zero homogeneous vectors in F which generate a graded submodule M of F. For $i = 1, \ldots, s$, we let $d_i = \deg_W(v_i)$. Moreover, let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$.

a) Consider the following example. Let $P = \mathbb{Q}[x, y, z]$ be standard graded, and let $\mathcal{G}$ be a deg-ordered homogeneous σ-Gröbner basis of an ideal $M \subseteq P$ such that $\mathrm{LM}_\sigma(\mathcal{G}) = (t_1, t_2, t_3, t_4)$, where $t_1 = x^3z^2$, $t_2 = x^3y^4$, $t_3 = y^5z^2$, and $t_4 = x^2y^5z$. Compute the set Σ of fundamental syzygies and its subset Σ''' of elements which survive Rules 1), 2), and 3) of Tutorial 56. Show that Σ''' is not a minimal system of generators of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$.

This example shows that the algorithm of Tutorial 56.j is not optimal in the sense that the set of critical pairs it treats does not always correspond to a minimal system of generators of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. To get this property, we now want to apply the algorithm of Theorem 4.6.7 to the minimal Gröbner basis Σ'' of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ we found in Tutorial 56.e.

b) Prove that a **pair of pairs**, i.e. a critical pair between two elements σ_{ij}, $\sigma_{i'j'}$ yields an S-vector of the form $\tilde{c}\,\tilde{t}\,\sigma_{ii'}$, where $\tilde{c} \in K$ and $\tilde{t} \in \mathbb{T}^n$. Show that such a pair of pairs is homogeneous and compute its degree.

c) Define a **head reduction step** and a **tail reduction step** of one fundamental syzygy by another. Describe the results of these reduction steps.

d) Let $i, j, k \in \{1, \ldots, s'\}$ be such that $\gamma_i = \gamma_j = \gamma_k$. Show that we have

$$\frac{\mathrm{lcm}(t_i,t_j,t_k)}{\mathrm{lcm}(t_i,t_j)} \cdot \sigma_{ij} + \frac{\mathrm{lcm}(t_i,t_j,t_k)}{\mathrm{lcm}(t_j,t_k)} \cdot \sigma_{jk} - \frac{\mathrm{lcm}(t_i,t_j,t_k)}{\mathrm{lcm}(t_i,t_k)} \cdot \sigma_{ik} = 0$$

e) Let $i, j, k \in \{1, \ldots, s'\}$ be pairwise distinct numbers with $\gamma_i = \gamma_j = \gamma_k$. Prove that the following conditions are equivalent.

1) $\sigma_{ij} \in \langle \sigma_{ik}, \sigma_{jk} \rangle$
2) $t_{ik} \mid t_{ij}$
3) $t_{jk} \mid t_{ji}$
4) $t_k \mid \mathrm{lcm}(t_i, t_j)$
5) $\mathrm{lcm}(t_i, t_j, t_k) = \mathrm{lcm}(t_i, t_j)$
6) $\gcd(t_{ik}, t_{jk}) = 1$

Conclude that the S-vector $\tilde{c}\,\tilde{t}\,\sigma_{ii'}$ of a pair of pairs satisfies $\tilde{t} = 1$ if and only if $\gcd(t_{ij}, t_{i'j}) = 1$.

f) Let Σ'' be the minimal τ-Gröbner basis of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ constructed in Tutorial 56.e. Consider the following instructions.

1) Let $\mathcal{B}^* = \emptyset$, $\mathcal{W} = \Sigma''$, $\mathcal{A} = \emptyset$, and $\Theta = \emptyset$.
2) For all $\sigma_{ij}, \sigma_{i'j} \in \Sigma''$ such that $1 \le i < i' < j \le s$, form the S-vector $S_{((i,j),(i',j))} = \tilde{c}\,\tilde{t}\,\sigma_{ii'}$ where $\tilde{c} \in K$ and $\tilde{t} \in \mathbb{T}^n$. If $\tilde{t} = 1$, append $\sigma_{ii'}$ to $\mathcal{B}^*$.
3) Let d be the smallest degree with respect to `Lex` of an element of $\mathcal{B}^*$ or $\mathcal{W}$. Form $\mathcal{B}^*_d$ and $\mathcal{W}_d$, and delete their entries from $\mathcal{B}^*$ and $\mathcal{W}$, respectively.
4) If $\mathcal{B}^*_d = \emptyset$, continue with step 11). Otherwise, choose an element $\sigma_{ij} \in \mathcal{B}^*_d$ and remove it from $\mathcal{B}^*_d$.
5) If $\mathrm{LT}_\tau(\sigma_{ij}) \in \mathrm{LT}_\tau(\mathcal{A}_d)$, then continue with step 4).
6) If $\mathrm{LT}_\tau(\sigma_{ij}) = \mathrm{LT}_\tau(\sigma_{i'j})$ for some element $\sigma_{i'j} \in \mathcal{W}_d$, then remove $\sigma_{i'j}$ from $\mathcal{W}_d$, append it to $\mathcal{A}$, and continue with step 4).
7) Find $\sigma_{i'j} \in \mathcal{A}_{<d}$ such that t_{ji} is a multiple of $t_{ji'}$. Then perform the head reduction step $\sigma_{ij} \xrightarrow{\sigma_{i'j}} \tilde{t}\,\sigma_{k\ell}$, where $\tilde{t} \in \mathbb{T}^n$, $k = \min\{i, i'\}$, and $\ell = \max\{i, i'\}$. If $\tilde{t} \neq 1$, continue with step 4).
8) If $\mathrm{LT}_\tau(\sigma_{k\ell}) \in \mathrm{LT}_\tau(\mathcal{A}_d)$, continue with step 4).
9) If $\mathrm{LT}_\tau(\sigma_{k\ell}) = \mathrm{LT}_\tau(\sigma_{k'\ell})$ for some element $\sigma_{k'\ell} \in \mathrm{LT}_\tau(\mathcal{W}_d)$, remove $\sigma_{k'\ell}$ from $\mathcal{W}_d$, append it to $\mathcal{A}$, and continue with step 4).
10) If $\sigma_{k\ell} \in \mathcal{B}^*_d$, delete $\sigma_{k\ell}$ in $\mathcal{B}^*_d$ and continue with step 7), applied to this element. Otherwise continue with step 4).
11) Append $\mathcal{W}_d$ to $\mathcal{A}$ and to Θ.
12) If $\mathcal{B}^* = \emptyset$ and $\mathcal{W} = \emptyset$, return Θ and stop. Otherwise, continue with step 3).

Assume that this is an algorithm which computes a subset Θ of Σ'' such that Θ is a minimal system of generators of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. (If you are very adventurous, you may try to prove this. At the end of this tutorial we give an extended hint on how you can proceed.)
Implement this algorithm in a CoCoA function `MinCritPairs(...)`.

g) Using both a direct calculation and your function `MinCritPairs(...)`, apply this algorithm to the following cases.

1) Let Σ'' be the set you computed in part a).
2) Let $P = \mathbb{Q}[x_1, \ldots, x_5]$ be standard graded, and let $\mathrm{LM}_\sigma(\mathcal{G}) = (t_1, t_2, t_3, t_4)$, where $t_1 = x_2^2 x_3^6 x_4 x_5^2$, $t_2 = x_1^8 x_2 x_4 x_5^4$, $t_3 = x_1^8 x_2^2 x_3^6$, and $t_4 = x_1^8 x_3^6 x_5^4$. Compute Σ, Σ'', and Σ''', and show that Σ''' is not minimal.

h) Modify the Homogeneous Buchberger Algorithm 4.5.5 by replacing steps 1), 2), 5), and 8) with the following.

1') Let $\mathcal{W} = \mathcal{V}$, $A = \emptyset$, $B = \emptyset$, $B^* = \emptyset$, $\mathcal{G} = \emptyset$, and let $s' = 0$.

2') Let d be the smallest degree with respect to `Lex` of an element of B or $\mathcal{W}$. Form B_d, B_d^*, $\mathcal{W}_d$, and delete their entries from B, B^*, and $\mathcal{W}$, respectively. Apply the function `MinPairs`(A, B_d, B_d^*) defined below.

5') Increase s' by one, append $g_{s'} = S'_{ij}$ to $\mathcal{G}$, perform the procedure `Update`$(B, B^*, g_{s'})$, and continue with step 3).

8') Increase s' by one, append $g_{s'} = v'$ to $\mathcal{G}$ and perform the procedure `Update`$(B, B^*, g_{s'})$. Then continue with step 6).

Here `Update`$(B, B^*, g_{s'})$ is the same as the procedure described in Tutorial 56.j, except for the substitution of

U4') Find in C all pairs (i, s') and (j, s') with $1 \leq i < j < s'$ such that $\gcd(t_{is'}, t_{js'}) = 1$. For each of these, check if (i, j) is already contained in B^* and append it if it isn't.

The procedure `MinPairs`(A, B_d, B_d^*) is defined as follows.

M1) If $B_d^* = \emptyset$ then stop. Otherwise, choose a pair (i, j) in B_d^* and remove it from B_d^*.

M2) If $t_{ji} = t_{ji'}$ for some pair $(i', j) \in A$, continue with step M1).

M3) If $t_{ji} = t_{ji'}$ for some pair $(i', j) \in B_d$, remove this pair from B_d and append it to A. Continue with step M1).

M4) Find $(i', j) \in A$ such that $t_{ji'}$ divides t_{ji}. Let $(k, \ell) = (\min\{i, i'\}, \max\{i, i'\})$. If $\gcd(t_{ij}, t_{i'j}) \neq 1$, then continue with M1).

M5) If $t_{\ell k} = t_{\ell k'}$ for some pair $(k', \ell) \in A$, continue with M1).

M6) If $t_{\ell k} = t_{\ell k'}$ for some pair $(k', \ell) \in B_d$, delete this pair from B_d, append it to A, and continue with M1).

M7) If $(k, \ell) \in B_d^*$, delete (k, ℓ) in B_d^* and continue with M4), applied to this pair.

M8) Continue with step M1).

Show that, altogether, we obtain a new algorithm which computes a deg-ordered homogeneous σ-Gröbner basis $\mathcal{G}$ of M. Moreover, the set of pairs treated in steps 3) – 5') corresponds to a minimal system of generators of $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$.

i) Apply this algorithm to the following case and follow its computations on a step-by-step basis. Let $P = \mathbb{Q}[x, y, z]$ be standard graded, and let $M \subseteq P$ be the homogeneous ideal generated by $\mathcal{V} = (v_1, v_2, v_3)$, where $v_1 = x^3z^2 + x^2y^2z$, $v_2 = x^3y^8$, and $v_3 = y^{10}z^2$. Use $\sigma =$ `DegLex`.

j) Implement this new algorithm in a CoCoA function `OptimalBA`$(\ldots)$. Apply your function to the examples given in i) and in Tutorial 56.a. Compare its efficiency with `NewHomBA`$(\ldots)$ by using timings and counting the number of calls of `NR`$(\ldots)$.

k) (*Note:* The following task requires a substantial effort on your part. Attempt it only if you are *very* bored.) Prove the finiteness and correctness of the algorithm underlying `MinCritPairs`$(\ldots)$. You could try to apply Theorem 4.6.7 to Σ'' and proceed as follows.

1) Suppose the element σ_{ij} chosen in step 4) of the algorithm in f) is not in $\mathcal{A}_d$ but its leading term is in $\mathrm{LT}_\sigma(\mathcal{A}_d)$. Show that $\sigma_{ij} \xrightarrow{\mathcal{A}} 0$ by considering the three cases $\mathrm{LT}_\tau(\sigma_{ij}) \in \mathrm{LT}_\tau(\mathcal{A}_d)$, $\mathrm{LT}_\tau(\sigma_{ij})$ irreducible with respect to $\mathcal{A}$, and $\mathrm{LT}_\tau(\sigma_{ij})$ reducible by $\mathcal{A}_{<d}$, separately.
2) Let $1 \leq i < j < m \leq s$ and $i' \in \{1, \ldots, j-1\} \setminus \{i\}$. Suppose there are terms $t, t', t'' \in \mathbb{T}^n \setminus \{1\}$ such that $\sigma_{ij} = \sigma_{ii'} + t\,\sigma_{i'j} = t'\,\sigma_{im} - t''\,\sigma_{jm}$ and $\sigma_{i'm} = t\,\sigma_{i'j} + t''\,\sigma_{jm}$. Show that t, t', and t'' are pairwise coprime.
3) In the algorithm in f), suppose that the element σ_{ij} reduces to $\sigma_{k\ell}$ in step 7) and that steps 8), 9), and 10) do not apply. Then show that $\sigma_{k\ell}$ is one of the elements of B_d^* which has been dealt with already. (Write $\sigma_{ij} = t'\sigma_{im} + t''\sigma_{jm} = t\sigma_{i'j} \pm \sigma_{k\ell}$ and conclude that $t\,\mathrm{lcm}(t_{i'}, t_j) = t''\,\mathrm{lcm}(t_j, t_m) = \tilde{t}\,\mathrm{lcm}(t_{i'}, t_m)$. Using 2), prove that $\tilde{t} = 1$ does not happen.)

4.7 Minimal Homogeneous Presentations

I have made this letter longer than usual,
because I lack the time to make it short.
(Blaise Pascal)

What is a good presentation? Some people might answer that first you say what you're going to say, then you say it, and then you say what you said. In this sense the presentation in this book is not good, because we lack the third part. However, when the subject of the presentation is presentations, our intention is completely different, because we want to make the presentation *minimal*. Although it has been claimed that minimalism is a cheap excuse for laziness, this is all wrong for presentations, because it takes a lot of time and effort to make them short.

In Computational Commutative Algebra, the computation of the minimal homogeneous presentation of a module is the first step in the computation of a minimal graded free resolution. Since many invariants of ideals and modules can be derived from such a resolution, computing one is a crucial achievement. It is also a formidable challenge, and to surmount the obstacles, we have to select our *strategy* carefully. The first component of our strategy is to divide and conquer. Therefore we divided the section into three subsections.

Firstly, we examine the existence and uniqueness of minimal homogeneous presentations. If they didn't exist, this section would never have been written and you wouldn't be reading these lines. This is the cheap way to settle the existence question. And if they are not unique (spoiler: they aren't) we should at least find out how the different minimal homogeneous presentations of the same module are related to each other and which invariants they share. In this context it is useful to represent presentations by homogeneous matrices of polynomials (see Definition 4.7.1 and Proposition 4.7.4) and to study how the minimality of a presentation is reflected in the degrees of the rows and the columns of the corresponding homogeneous matrix (see Propositions 4.7.8 and 4.7.10). These results allow us to associate two sets of invariants to a graded module, namely its 0^{th} and 1^{st} graded Betti numbers.

Having defined these invariants, we could proceed as follows: give a hint about a possible algorithm for the computation of minimal homogeneous presentations and ask you to work out the details in the exercises. But as you know, this is not what is going to happen here. We are going the extra mile for you, dear reader, and will describe several algorithms. In fact, this extra mile starts with a huge detour in the second subsection.

For more than 400 pages we have been stressing that computer algebra is really about modules rather than ideals. Now we turn round and embed a module in a suitable ring such that it becomes an ideal in that ring. This process is called *idealization*. For graded submodules, we construct explicit idealizations (see Proposition 4.7.14) and show how Gröbner bases and minimal systems of generators behave under this embedding (see Propositions 4.7.16 and 4.7.19). Moreover, by constructing an even bigger surround-

ing ring, we can idealize a whole presentation and compute a minimal homogeneous presentation by minimalizing suitable homogeneous ideals (see Proposition 4.7.23).

Finally, in the third subsection we present several ways to compute minimal homogeneous presentations. The obvious and inefficient strategy of applying Theorem 4.6.3 to minimalize the generators of the module, Theorem 3.1.8 to compute the syzygies, and then Theorem 4.6.3 again to minimalize the syzygies can be improved using the idealization technique to obtain the *vertical strategy* for computing minimal presentations (see Theorem 4.7.26). A more natural and efficient strategy is to compute the entire minimal homogeneous presentation degree-by-degree. This is called the *horizontal strategy* and is explained in Theorem 4.7.29. It is particularly interesting to see how strategies which look so different are simply variants of the classical Buchberger Algorithm applied to the idealization of the given module.

Before inviting you to read the section, we want to point out a choice of notation we decided upon. In Subsection A we treat arbitrary finitely presented modules. Their presentation has the shape $F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$, where F_0 and F_1 are free modules. However, in Subsection C we deal with a submodule M of a free module. The name of the free module is F_0, and the presentation of M has the shape $F_2 \longrightarrow F_1 \longrightarrow M \longrightarrow 0$.

You will notice that this section is longer than usual although we certainly did not lack the time to make it shorter. Quite to the contrary, we tried to give a careful account of the subtleties involved. Now, having said what we are going to say, it is high time to start saying it.

4.7.A Existence and Uniqueness of Minimal Presentations

There can be only one.
(Movie Tagline)

Let K be a field, let $m, n, r \geq 1$, let $P = K[x_1, \ldots, x_n]$ be positively graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let M be a graded P-module generated by a tuple of non-zero homogeneous elements $\mathcal{G} = (g_1, \ldots, g_r)$. The tuple $(\deg_W(g_1), \ldots, \deg_W(g_r))$ of their degrees will be denoted by $\deg_W(\mathcal{G})$. In Definition 3.2.5 we said that a presentation of M is an exact sequence

$$F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

where F_0 and F_1 are free P-modules. Under our hypotheses we have additional information. The syzygy module $\mathrm{Syz}_P(\mathcal{G})$ is a graded P-module. Let $\mathcal{S} = (v_1, \ldots, v_s)$ be a tuple of non-zero homogeneous vectors which generate $\mathrm{Syz}_P(\mathcal{G})$, let $d_{0i} = \deg_W(g_i)$ for $i = 1, \ldots, r$, and let $d_{1j} = \deg_W(v_j)$ for $j = 1, \ldots, s$. We consider the graded free P-modules $F_0 = \bigoplus_{i=1}^{r} P(-d_{0i})$ and $F_1 = \bigoplus_{j=1}^{s} P(-d_{1j})$, and we denote the canonical bases of F_0 and F_1

by $(e_1, \ldots, e_r)$ and $(\varepsilon_1, \ldots, \varepsilon_s)$, respectively. Finally, we define two homomorphisms of P-modules $\varphi: F_0 \longrightarrow M$ and $\psi: F_1 \longrightarrow F_0$ by $\varphi(e_i) = g_i$ for $i = 1, \ldots, r$ and $\psi(\varepsilon_j) = v_j$ for $j = 1, \ldots, s$. Then the exact sequence of graded P-modules

$$F_1 \xrightarrow{\psi} F_0 \xrightarrow{\varphi} M \longrightarrow 0$$

is called a **homogeneous presentation** of M. Notice that $\deg_W(e_i) = d_{0i}$ for $i = 1, \ldots, r$ and $\deg_W(\varepsilon_j) = d_{1j}$ for $j = 1, \ldots, s$.

In the following we choose $\mathcal{G}$ and $\mathcal{S}$ to be minimal and examine which aspects of such a minimal homogeneous presentation are uniquely determined. As a first step, we are going to see that the map ψ is associated to the following kind of matrix.

Definition 4.7.1. Let $\mathcal{M} = (f_{ij})$ be a matrix in $\mathrm{Mat}_{r,s}(P)$. We say that $\mathcal{M}$ is a **homogeneous matrix** (or simply **homogeneous**) if there exist two tuples $d_0 = (d_{01}, \ldots, d_{0r})$ and $d_1 = (d_{11}, \ldots, d_{1s})$ of elements in $\mathbb{Z}^m$ such that the polynomial f_{ij} is homogeneous of degree $\deg_W(f_{ij}) = d_{1j} - d_{0i}$ for $i = 1, \ldots, r$ and $j = 1, \ldots, s$. In this case, the pair $(d_0, d_1) \in (\mathbb{Z}^m)^r \times (\mathbb{Z}^m)^s$ is called a **degree pair** of $\mathcal{M}$.

We can think of a degree pair as a pair of tuples of degrees which mark the rows and columns of a homogeneous matrix. Then the entry in position (i, j) of the matrix is a homogeneous element whose degree is the difference of the degree of the j^{th} column and the degree of the i^{th} row. Even if this entry is zero, we have to consider it as a homogeneous element of that degree. Degree pairs are not uniquely determined. We can add a vector $d \in \mathbb{Z}^m$ to all the d_{ij} and obtain $d_0' = (d_{01} + d, \ldots, d_{0r} + d)$ and $d_1' = (d_{11} + d, \ldots, d_{1s} + d)$. Then also (d_0', d_1') is a degree pair of $\mathcal{M}$. Clearly, fixing one of the components of either d_0 or d_1 uniquely determines the degree pair of $\mathcal{M}$.

Example 4.7.2. Let $P = K[x_1, x_2, x_3, x_4]$ be graded by $W = \left(\begin{smallmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \end{smallmatrix}\right)$. The matrix $\left(\begin{smallmatrix} x_3 & x_2 & x_4 \\ x_2 & x_1 & x_2 \end{smallmatrix}\right)$ has homogeneous entries, but it is easy to see that it is not homogeneous. However, the matrix $\left(\begin{smallmatrix} x_3 & x_2 & x_4 \\ x_2 & x_1 & x_3 \end{smallmatrix}\right)$ is homogeneous and one of its degree pairs is (d_0, d_1), where $d_0 = \big((-2,-1),(-2,0)\big)$ and $d_1 = \big((-1,2),(-1,1),(-1,3)\big)$. Another one is (d_0', d_1'), where $d_0' = \big((0,0),(0,1)\big)$ and $d_1' = \big((1,3),(1,2),(1,4)\big)$.

An immediate consequence of the definition is that the determinant of a homogeneous square matrix of size $r \times r$ is a homogeneous polynomial of degree $\sum_{i=1}^{r}(d_{1i} - d_{0i})$. In particular, if a homogeneous matrix is invertible in $\mathrm{Mat}_r(P)$, its determinant is a non-zero constant. Another immediate consequence is that Corollary 1.7.11 can be rephrased as follows.

Remark 4.7.3. For any homogeneous element $u \in M$, there exists a homogeneous matrix $\mathcal{U} \in \mathrm{Mat}_{r,1}(P)$ with degree pair $(\deg_W(\mathcal{G}), \deg_W(u))$ such that $u = \mathcal{G} \cdot \mathcal{U}$.

The next step is to investigate how homogeneous matrices are related to maps of graded free modules.

Proposition 4.7.4. (Characterization of Homogeneous Matrices) *Let* $\mathcal{M} = (f_{ij}) \in \mathrm{Mat}_{r,s}(P)$, *let* $d_{01}, \ldots, d_{0r}, d_{11}, \ldots, d_{1s} \in \mathbb{Z}^m$, *and let* $d_0 = (d_{01}, \ldots, d_{0r})$ *as well as* $d_1 = (d_{11}, \ldots, d_{1s})$. *Denote the canonical bases of* $F_0 = \bigoplus_{i=1}^r P(-d_{0i})$ *and* $F_1 = \bigoplus_{j=1}^s P(-d_{1j})$ *by* $(e_1, \ldots, e_r)$ *and* $(\varepsilon_1, \ldots, \varepsilon_s)$, *respectively. Then the following conditions are equivalent.*

a) The matrix $\mathcal{M}$ *is homogeneous with degree pair* (d_0, d_1).
b) For $j = 1, \ldots, s$, *the vector* $v_j = (f_{1j}, \ldots, f_{rj}) \in F_0$ *is homogeneous of degree* $\deg_W(v_j) = d_{1j}$.
c) The P*-linear map* $\psi : F_1 \longrightarrow F_0$ *defined by* $\psi(\varepsilon_j) = v_j$ *for* $j = 1, \ldots, s$ *is homogeneous.*

Proof. The equivalence of a) and b) follows from the following fact. Given $j \in \{1, \ldots, s\}$, the vector $v_j = f_{1j}e_1 + \cdots + f_{rj}e_r$ is homogeneous of degree d_{1j} if and only if f_{ij} is homogeneous and $\deg_W(f_{ij}e_i) = \deg_W(f_{ij}) + d_{0i} = d_{1j}$ for $i = 1, \ldots, r$. The equivalence of b) and c) is obviously true. □

Now we imitate the definition of a deg-ordered tuple (see Definition 4.5.4) and extend it to homogeneous matrices.

Definition 4.7.5. Let $d_0 = (d_{01}, \ldots, d_{0r})$, $d_1 = (d_{11}, \ldots, d_{1s})$, and let $\mathcal{M}$ be a homogeneous matrix with degree pair (d_0, d_1). We say that $\mathcal{M}$ is a **deg-ordered matrix** (or simply **deg-ordered**) if $d_{01} \leq_{\mathtt{Lex}} \cdots \leq_{\mathtt{Lex}} d_{0r}$ and $d_{11} \leq_{\mathtt{Lex}} \cdots \leq_{\mathtt{Lex}} d_{1s}$.

In other words, the degrees of the *entries* of a deg-ordered matrix are non-decreasing from left to right and from bottom to top. Now we examine matrices which are invertible in the sense that there exists an inverse matrix with polynomial entries. What can we say about deg-ordered invertible matrices? Clearly, invertible matrices correspond to isomorphisms of graded free modules, but we can say a bit more. In the following, when we say that a P-linear map of graded free P-modules is defined by a matrix without specifying the bases, we mean with respect to the canonical bases.

Proposition 4.7.6. *Let* $\mathcal{M} \in \mathrm{Mat}_{r,s}(P)$ *be a homogeneous deg-ordered matrix with degree pair* $(d_0, d_1) = ((d_{01}, \ldots, d_{0r}), (d_{11}, \ldots, d_{1s}))$. *Furthermore, let* $F_0 = \bigoplus_{i=1}^r P(-d_{0i})$, *let* $F_1 = \bigoplus_{j=1}^s P(-d_{1j})$, *and let* $\varphi : F_1 \longrightarrow F_0$ *be defined by* $\mathcal{M}$. *Then the following conditions are equivalent.*

a) The matrix $\mathcal{M}$ *is invertible.*
b) The matrix $\mathcal{M}$ *is a block matrix of the form*

$$\mathcal{M} = \begin{pmatrix} \mathcal{M}_{11} & \mathcal{M}_{12} & \cdots & \mathcal{M}_{1q} \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathcal{M}_{q-1\,q} \\ 0 & \cdots & 0 & \mathcal{M}_{qq} \end{pmatrix}$$

with square matrices $\mathcal{M}_{11}, \ldots, \mathcal{M}_{qq}$ *which are invertible matrices with constant entries.*

c) The P*-linear map* φ *is an isomorphism of graded* P*-modules.*

If these conditions are satisfied, we have $r = s$ *and* $d_0 = d_1$*.*

Proof. First, we observe that if $\mathcal{M}$ is invertible, we have $r = s$. Moreover, we claim that every entry on the main diagonal of $\mathcal{M}$ has to have degree zero. To see why this is true, we write $\mathcal{M} = (f_{ij})$ and $\mathcal{M}^{-1} = (\tilde{f}_{ij})$ with $f_{ij}, \tilde{f}_{ij} \in P$. Then we use the fact that the degrees of the i^{th} elements $f_{ii}, \tilde{f}_{ii}$ on the main diagonals of $\mathcal{M}$ and $\mathcal{M}^{-1}$ have to add up to zero. If we have $\deg_W(f_{ii}) >_{\texttt{Lex}} 0$, we get $\deg_W(\tilde{f}_{ii}) <_{\texttt{Lex}} 0$, and vice versa. Suppose that $\deg_W(f_{ii}) <_{\texttt{Lex}} 0$. Then the degree of every element f_{jk} with $j \in \{i, \ldots, r\}$ and $k \in \{1, \ldots, i\}$ is negative, and therefore we have $f_{jk} = 0$. Hence we can consider $\mathcal{M}$ as a block matrix with two square blocks on the diagonal of size i and $r - i$. Since the last row of the upper left block it zero, it follows that $\det(\mathcal{M}) = 0$, in contradiction to the hypothesis. From this claim we conclude that $d_0 = d_1$.

Now we observe that below the main diagonal of $\mathcal{M}$ only non-positive degrees are allowed. By combining the rows and columns whose indices i, j satisfy $d_{0i} = d_{0j}$, we see that $\mathcal{M}$ and $\mathcal{M}^{-1}$ are block matrices with square blocks on the main diagonal. Below these square blocks the degrees of all entries are negative. Hence these entries are all zero. Since $\det(\mathcal{M})$ is the product of the determinants of the blocks on the main diagonal, these blocks are invertible matrices. Thus we have shown that a) implies b). The implications "b)⇒c)" and "c)⇒a)" are obviously true. □

Now we go one step further in our discussion of generators and syzygies and assume that $\mathcal{G}$ and $\mathcal{S}$ are minimal homogeneous systems of generators. Recall that every finite homogeneous system of generators of a module contains a minimal one, because the polynomial ring P is positively graded (see Proposition 4.1.22.b and Corollary 4.2.6.b).

Definition 4.7.7. Let $\mathcal{G} = (g_1, \ldots, g_r)$ be a minimal homogeneous system of generators of M, and let $\mathcal{S} = (v_1, \ldots, v_s)$ be a minimal homogeneous system of generators of $\mathrm{Syz}_P(\mathcal{G})$. Then the presentation

$$F_1 \xrightarrow{\psi} F_0 \xrightarrow{\varphi} M \longrightarrow 0$$

where $\varphi(e_i) = g_i$ for $i = 1, \ldots, r$, and $\psi(\varepsilon_j) = v_j$ for $j = 1, \ldots, s$, is called a **minimal homogeneous presentation** of M.

Notice that, given $\mathcal{G}$, a homogeneous presentation of M is uniquely determined by the homogeneous matrix $\mathcal{S}$. From the Graded Version of Nakayama's Lemma 1.7.15 it follows that a homogeneous presentation is minimal if and only if $\mathcal{S}$ contains no non-zero constant polynomials. A degree pair of $\mathcal{S}$ is given by $(\deg_W(\mathcal{G}), \deg_W(\mathcal{S}))$.

Now we turn to the main goal of this subsection which is to show that, up to permutations, the pair $(\deg_W(\mathcal{G}), \deg_W(\mathcal{S}))$ is uniquely determined by M if the homogeneous presentation is minimal. Recall that, by Proposition 4.1.22.b, any two minimal sets of generators of a finitely generated graded P-module have the same number of elements.

Proposition 4.7.8. *Let $\mathcal{G} = (g_1, \ldots, g_r)$ and $\mathcal{G}' = (g'_1, \ldots, g'_r)$ be deg-ordered tuples of non-zero homogeneous elements of M which are minimal homogeneous systems of generators of M.*

a) We have $\deg_W(\mathcal{G}) = \deg_W(\mathcal{G}')$. So the tuple $\deg_W(\mathcal{G})$ is uniquely determined by the module M and does not depend on the choice of the homogeneous minimal system of generators.

b) There are deg-ordered homogeneous matrices $\mathcal{A}, \mathcal{B} \in \mathrm{Mat}_r(P)$ such that the following conditions are satisfied.

1) We have $\mathcal{G}' = \mathcal{G}\,\mathcal{A}$ and $\mathcal{G} = \mathcal{G}'\,\mathcal{B}$.

2) The matrices $\mathcal{A}$ and $\mathcal{B}$ are invertible.

Proof. First we prove a). Let $\deg_W(\mathcal{G}) = (d_1, \ldots, d_r)$ and $\deg_W(\mathcal{G}') = (d'_1, \ldots, d'_r)$. Suppose there exists an index $i \in \{1, \ldots, r\}$ such that $d_j = d'_j$ for $j < i$ and $d_i <_{\mathtt{Lex}} d'_i$. By Proposition 4.1.22.a, the set of residue classes $\{\overline{g}'_1, \ldots, \overline{g}'_{i-1}\}$ modulo $(x_1, \ldots, x_n)$ is a K-basis of $\overline{M}_{\leq d_i}$. On the other hand, by the same proposition, the set of residue classes $\{\overline{g}_1, \ldots, \overline{g}_i\}$ is contained in a K-basis of the same vector space. Since the two bases have different numbers of elements, this yields a contradiction. A similar argument shows that we cannot have $d_i >_{\mathtt{Lex}} d'_i$. Altogether, we must have $d_i = d'_i$ for $i = 1, \ldots, r$, as claimed.

Now we prove b). By a) and Remark 4.7.3, there exist homogeneous deg-ordered square matrices $\mathcal{A}, \mathcal{B}$ such that $\mathcal{G}' = \mathcal{G}\,\mathcal{A}$ and $\mathcal{G} = \mathcal{G}'\,\mathcal{B}$. From these equations we deduce that $\mathcal{G}\,(\mathcal{I}_r - \mathcal{A}\,\mathcal{B}) = 0$, where $\mathcal{I}_r$ is the identity matrix of size $r \times r$. Since the residue classes $\{\overline{g}_1, \ldots, \overline{g}_r\}$ form a K-basis of $\overline{M}$ by Proposition 4.1.22.b, the matrix of residue classes $\overline{\mathcal{I}}_r - \overline{\mathcal{A}}\,\overline{\mathcal{B}}$ is the zero matrix. Hence the matrices $\overline{\mathcal{A}}$ and $\overline{\mathcal{B}}$ are inverse to each other. It follows that the constant terms of $\det(\mathcal{A})$ and $\det(\mathcal{B})$ are non-zero. But since $\mathcal{A}$ and $\mathcal{B}$ are homogeneous matrices, this implies that their determinants are non-zero constants, i.e. that they are invertible. □

In light of this result, we have a new set of invariants of a finitely generated graded P-module.

Definition 4.7.9. Let $\mathcal{G} = (g_1, \ldots, g_r)$ be a deg-ordered tuple of non-zero homogeneous elements of M which form a minimal system of generators. For $i = 1, \ldots, r$, let $d_{0i} = \deg_W(g_i)$.

a) The tuple $(d_{01}, \ldots, d_{0r}) \in (\mathbb{Z}^m)^r$ is called the **degree sequence** of M. It does not depend on the choice of the minimal homogeneous system of generators.

b) For all $d \in \mathbb{Z}^m$, we let $\beta_{0d}(M)$ be the number of times d occurs in the degree sequence of M. Then the numbers $\beta_{0d}(M)$, or simply β_{0d}, are called the **0^{th} graded Betti numbers** of M.
c) For later use, we call the number $d_{01} = \deg_W(g_1)$ the **initial degree** of M and denote it by $\alpha(M)$.

In the final part of this subsection we explain how passing from one homogeneous minimal system of generators of M to another affects their syzygies.

Proposition 4.7.10. *Let $\mathcal{G} = (g_1, \ldots, g_r)$ and $\mathcal{G}' = (g'_1, \ldots, g'_r)$ be deg-ordered tuples of non-zero homogeneous elements of M which are also minimal homogeneous systems of generators of M. Let $d_{0i} = \deg_W(g_i)$ for $i = 1, \ldots, r$, let $\mathcal{A} \in \mathrm{Mat}_r(P)$ be a deg-ordered, homogeneous, invertible matrix such that $\mathcal{G}' = \mathcal{G}\,\mathcal{A}$, and let $\mathcal{S} = (v_1, \ldots, v_s)$ be a deg-ordered tuple of homogeneous vectors in $F_0 = \bigoplus_{i=1}^r P(-d_{0i})$ which minimally generate $\mathrm{Syz}_P(\mathcal{G})$.*

a) The tuple $\mathcal{S}' = \mathcal{A}^{-1}\,\mathcal{S}$ is a deg-ordered tuple of homogeneous vectors in F_0 which minimally generate $\mathrm{Syz}_P(\mathcal{G}')$.
b) We have $\deg_W(\mathcal{S}) = \deg_W(\mathcal{S}')$. Thus the pair $(\deg_W(\mathcal{S}), \deg_W(\mathcal{G}))$ is uniquely determined by the module M.

Proof. Let us prove a) first. Since we have $\mathcal{G}'\,(\mathcal{A}^{-1}\,\mathcal{S}) = (\mathcal{G}\,\mathcal{A})\,(\mathcal{A}^{-1}\,\mathcal{S}) = \mathcal{G}\,\mathcal{S} = 0$, the columns of $\mathcal{S}'$ are syzygies of $\mathcal{G}'$. Given any homogeneous element $u \in \mathrm{Syz}_P(\mathcal{G}')$, we compute $\mathcal{G}\,(\mathcal{A}\,u) = \mathcal{G}'\,u = 0$. Hence the homogeneous vector $\mathcal{A}\,u$ is a syzygy of $\mathcal{G}$. Since $\mathcal{S}$ generates $\mathrm{Syz}_P(\mathcal{G})$, there exists a homogeneous matrix $\mathcal{H} = (h_1, \ldots, h_s)^{\mathrm{tr}}$ such that $\mathcal{A}\,u = h_1 v_1 + \ldots + h_s v_s = \mathcal{S}\,\mathcal{H}$. Therefore we have $u = \mathcal{A}^{-1}\,(\mathcal{A}\,u) = (\mathcal{A}^{-1}\,\mathcal{S})\,\mathcal{H} = \mathcal{S}'\,\mathcal{H}$, and it follows that $\mathcal{S}'$ generates $\mathrm{Syz}_P(\mathcal{G}')$.

Moreover, by Proposition 4.7.4.c, the matrix $\mathcal{A}^{-1}$ corresponds to a bijective homogeneous P-linear map $\varphi : F_0 \longrightarrow F_0$. Therefore the tuple $\mathcal{S}' = (\varphi(v_1), \ldots, \varphi(v_s)) = \mathcal{A}^{-1}\,\mathcal{S}$ is also deg-ordered and a minimal system of generators of $\mathrm{Syz}_P(\mathcal{G}')$. Using Proposition 4.7.6, we see that the tuple $\mathcal{S}'$ satisfies $\deg_W(\mathcal{S}') = \deg_W(\mathcal{S})$ which proves b). □

The statement of this proposition can be visualized using the following commutative diagram with exact rows, where $F_1 = \bigoplus_{j=1}^s P(-d_{1j})$ with $d_{1j} = \deg_W(v_j)$, and where homogeneous tuples are used to label the homogeneous P-linear maps they define.

$$\begin{array}{ccccccc} F_1 & \xrightarrow{\mathcal{S}} & F_0 & \xrightarrow{\mathcal{G}} & M & \longrightarrow & 0 \\ \| & & {\scriptstyle\mathcal{A}^{-1}}\downarrow\uparrow{\scriptstyle\mathcal{A}} & & \| & & \\ F_1 & \xrightarrow{\mathcal{S}'} & F_0 & \xrightarrow{\mathcal{G}'} & M & \longrightarrow & 0 \end{array}$$

As a consequence of this proposition, we can attach further invariants to a finitely generated graded P-module.

Definition 4.7.11. Let M be a finitely generated graded P-module, let $\mathcal{G} = (g_1, \ldots, g_r)$ be a deg-ordered tuple which minimally generates M, and let $\mathcal{S} = (v_1, \ldots, v_s)$ be a deg-ordered tuple which minimally generates $\mathrm{Syz}_P(\mathcal{G})$.

a) The degree pair $(\deg_W(\mathcal{G}), \deg_W(\mathcal{S}))$ of the homogeneous matrix $\mathcal{S}$ does not depend on the choice of $\mathcal{G}$ and $\mathcal{S}$. It is called the **degree pair** of the module M.

b) For every $d \in \mathbb{Z}^m$, we let $\beta_{1d}(M)$ be the number of times the degree d occurs in the tuple $(\deg_W(v_1), \ldots, \deg_W(v_s))$. The numbers $\beta_{1d}(M)$, or simply β_{1d}, are called the **1st graded Betti numbers** of the module M.

Using the graded Betti numbers, a minimal homogeneous presentation of M can be written in the form

$$\bigoplus_{d\in\mathbb{Z}^m} P(-d)^{\beta_{1d}} \longrightarrow \bigoplus_{d\in\mathbb{Z}^m} P(-d)^{\beta_{0d}} \longrightarrow M \longrightarrow 0$$

Before we plunge into actual computations of such presentations, we embark on an extended detour.

4.7.B Idealization of Graded Modules and Presentations

If you can't realize your ideal,
idealize the real.
(Stewart's Marriage Counsel Homily)

On a multitude of occasions we have emphasized the importance of modules. One of our main arguments was that to confine our theory to the realm of ideals would be far too limiting. In other words, we have been trying to suggest that the ideal setting for our book is the category of finitely generated modules over affine algebras. But in this section we realize that modules are not the ideal objects we pretended them to be. In order to compute minimal homogeneous presentations in a compact way, it turns out to be more efficient to idealize graded submodules, i.e. to identify them with ideals in suitably enlarged polynomial rings. The purpose of this subsection is to provide the necessary mathematical background for that idea.

Definition 4.7.12. Let R be a ring and M an R-module. Let us equip the product set $R \times M$ with two operations, namely

$$\begin{array}{rccc} & + : (R\times M)\times(R\times M) & \longrightarrow & R\times M \\ & ((r,m),\,(r',m')) & \longmapsto & (r+r', m+m') \\ \text{and} & \cdot : (R\times M)\times(R\times M) & \longrightarrow & R\times M \\ & ((r,m),\,(r',m')) & \longmapsto & (rr', rm'+r'm) \end{array}$$

In this way, the set $R \times M$ becomes a commutative ring with identity element $(1, 0)$. We call this ring the **idealization** of M and denote it by $R \ltimes M$.

The ring $R \ltimes M$ is an R-algebra via the ring homomorphism $R \longrightarrow R \ltimes M$ given by $r \mapsto (r, 0)$. The canonical map $\imath : M \longrightarrow R \ltimes M$ defined by $\imath(m) = (0, m)$ is injective and R-linear. Its image is an ideal in $R \ltimes M$. We shall denote this ideal by $\imath(M)$ and identify the elements of M with their images under $\imath$.

Let us collect some basic properties of the idealization of a module.

Remark 4.7.13. Let R be a ring and M an R-module.

a) The ideal $\imath(M)$ satisfies $\imath(M)^2 = 0$.
b) Given an R-submodule $N \subseteq M$, the inclusion $R \times N \subseteq R \times M$ defines an injective ring homomorphism $R \ltimes N \longrightarrow R \ltimes M$. The image of N in $R \ltimes M$ is an ideal which is contained in the ideal $\imath(M)$.
c) Let Γ be a monoid, let R be Γ-graded, and let M be a Γ-graded R-module. Then $R \ltimes M$ is a Γ-graded ring via $(R \ltimes M)_\gamma = R_\gamma \times M_\gamma$ for all $\gamma \in \Gamma$, and $\imath(M)$ is a homogeneous ideal in this ring.

In the following we want to study the idealization of a graded submodule of a graded free P-module, since this is the most interesting case for the applications to minimal presentations and minimal free resolutions.

As usual, we let $P = K[x_1, \ldots, x_n]$ be positively graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $d_{01}, \ldots, d_{0r} \in \mathbb{Z}^m$, let $F_0 = \bigoplus_{i=1}^r P(-d_{0i})$, and let M be a graded submodule of F_0. The canonical basis vectors of F_0 will be denoted by $e_1, \ldots, e_r$. By considering $e_1, \ldots, e_r$ as indeterminates, we form the polynomial ring $\overline{P} = K[x_1, \ldots, x_n, e_1, \ldots, e_r] = P[e_1, \ldots, e_r]$. We equip $\overline{P}$ with the grading given by $\overline{W} = (W \mid d_{01} \ \cdots \ d_{0r}) \in \mathrm{Mat}_{m,n+r}(\mathbb{Z})$. A vector $v = f_1 e_1 + \cdots + f_r e_r \in F_0$ will be identified with the corresponding polynomial in $\overline{P}$.

Moreover, we let $\mathfrak{e}$ be the ideal generated by $E = \{e_i e_j \mid 1 \leq i \leq j \leq r\}$ in $\overline{P}$, and let $\mathcal{E}$ be the tuple

$$\mathcal{E} = (e_1e_1, e_1e_2, \ldots, e_1e_r, e_2e_2, e_2e_3, \ldots, e_2e_r, \ldots, e_re_r) \in \overline{P}^{\,r(r+1)/2}$$

In this situation we can represent the idealization of M as follows.

Proposition 4.7.14. (Idealization of a Graded Submodule)
Let $\mathcal{V} = (v_1, \ldots, v_s)$ be a deg-ordered tuple of homogeneous vectors which generate M.

a) The map $\varphi : P \ltimes F_0 \longrightarrow \overline{P}/\mathfrak{e}$ which sends $(f, (g_1, \ldots, g_r))$ to the residue class of $f + g_1 e_1 + \cdots + g_r e_r$ is an isomorphism of graded rings.
b) Under the composition $M \xrightarrow{\imath} P \ltimes M \hookrightarrow P \ltimes F_0 \xrightarrow{\varphi} \overline{P}/\mathfrak{e}$, the module M is identified with the residue class ideal of $I_M = (v_1, \ldots, v_s) + \mathfrak{e} \subseteq \overline{P}$.

Proof. First we prove a). Since φ is clearly a well-defined R-linear map, we check that φ is compatible with multiplication. Let $(f, (g_1, \ldots, g_r))$ and $(f', (g'_1, \ldots, g'_r))$ be two elements of $R \ltimes M$. Computing modulo $\mathfrak{e}$, we get

$$\begin{aligned}\varphi((f,(g_1,\ldots,g_r)) \cdot (f',(g'_1,\ldots,g'_r))) &= \varphi((ff',(fg'_1+f'g_1,\ldots,fg'_r+f'g_r)))\\ &= ff'+(fg'_1+f'g_1)e_1+\cdots+(fg'_r+f'g_r)e_r\\ &= (f+g_1e_1+\cdots+g_re_r)\cdot(f'+g'_1e_1+\cdots+g'_re_r)\\ &= \varphi((f,(g_1,\ldots,g_r)))\cdot\varphi((f',(g'_1,\ldots,g'_r)))\end{aligned}$$

Since φ is clearly both injective and surjective, it remains to show that φ is homogeneous. The monomial ideal $\mathfrak{e}$ is homogeneous (see Proposition 4.1.8), and given a homogeneous element $(f,(g_1,\ldots,g_r))$ of $R\ltimes M$, the residue class of $f+g_1e_1+\cdots+g_re_r$ is homogeneous of the same degree. Therefore φ is a homomorphism of graded rings.

To prove b), we combine the descriptions of the maps in Definition 4.7.12.b, Remark 4.7.13.b, and part a). For $i=1,\ldots,s$, we see that v_i is mapped to the residue class $v_i+\mathfrak{e}$ by the composition. From this the claim follows immediately. □

Definition 4.7.15. In the above setting, the ideal $I_M=(v_1,\ldots,v_s)+\mathfrak{e}$ of $\overline{P}$ is called the **idealization ideal**, or simply the **ideal** of M.

Gröbner bases of graded submodules and Gröbner bases of their ideals are related as follows. Recall that a module term ordering σ on $\mathbb{T}^n\langle e_1,\ldots,e_r\rangle$ is compatible with a term ordering τ on $\mathbb{T}^n$ if $t\geq_\tau t'$ implies $te_i\geq_\sigma t'e_i$ for all $t,t'\in\mathbb{T}^n$ and $i\in\{1,\ldots,r\}$ (see Definition 1.4.17 and Tutorial 54.b). We shall say that a term ordering $\overline{\sigma}$ on $\mathbb{T}(x_1,\ldots,x_n,e_1,\ldots,e_r)$ extends both σ and τ if the restriction of $\overline{\sigma}$ to $\mathbb{T}^n$ is τ and its restriction to $\mathbb{T}^n\langle e_1,\ldots,e_r\rangle$ is σ.

Proposition 4.7.16. (Gröbner Bases and Idealization)
Let $I_M\subseteq\overline{P}$ be the ideal of M. Furthermore, let τ be a term ordering on $\mathbb{T}^n$, let σ be a module term ordering on $\mathbb{T}^n\langle e_1,\ldots,e_r\rangle$ which is compatible with τ, and let $\overline{\sigma}$ be a term ordering on $\mathbb{T}(x_1,\ldots,x_n,e_1,\ldots,e_r)$ which extends both σ and τ.

a) Let G be a σ-Gröbner basis of M. Then $G\cup E$ is a $\overline{\sigma}$-Gröbner basis of I_M.
b) Let G be the reduced σ-Gröbner basis of M. Then the reduced $\overline{\sigma}$-Gröbner basis of I_M is $G\cup\{e_ie_j\in E\mid e_i,e_j\notin \mathrm{LT}_\sigma(M)\}$.

Proof. To prove a), we let $G=\{g_1,\ldots,g_{s'}\}$ and $f\in I_M$. By subtracting suitable multiples of polynomials e_ie_j, we see that we may reduce f to the form $h=h_0+h_1e_1+\cdots+h_re_r$ with $h_0,\ldots,h_r\in P$. Since I_M is contained in $(e_1,\ldots,e_r)$, we have $h_0=0$. The polynomial $h=h_1e_1+\cdots+h_re_r\in I$ is linear in $e_1,\ldots,e_r$. The only generators of I_M which are linear in $e_1,\ldots,e_r$ are $v_1,\ldots,v_s$. Hence h is a P-linear combination of those generators. Thus we have $(h_1,\ldots,h_r)\in\langle v_1,\ldots,v_s\rangle$ and $\mathrm{LT}_\sigma((h_1,\ldots,h_r))=t\,\mathrm{LT}_\sigma(g_i)$ for some $t\in\mathbb{T}^n$ and $i\in\{1,\ldots,s'\}$. Since the term ordering $\overline{\sigma}$ extends σ, we get $\mathrm{LT}_{\overline{\sigma}}(h)=t\,\mathrm{LT}_{\overline{\sigma}}(g_i)$. Therefore we can reduce h by G. After several

such reduction steps we eventually get zero, because G is a σ-Gröbner basis of M. Altogether, the polynomial f reduces to zero using $G \cup E$.

To show claim b), we let $\overline{G}$ be the reduced $\overline{\sigma}$-Gröbner basis of I_M. Since we have $e_i e_j \in I_M$, we know $e_i e_j \in \mathrm{LT}_{\overline{\sigma}}(I_M)$ for all $1 \leq i \leq j \leq r$. Now it follows from the additional condition $e_i, e_j \notin \mathrm{LT}_\sigma(M)$ that $e_i e_j$ is a minimal generator of $\mathrm{LT}_{\overline{\sigma}}(I_M)$, and therefore $e_i e_j$ is contained in $\overline{G}$. Thus $\overline{G}$ has the form $\overline{G} = G \cup \{e_i e_i \in E \mid e_i, e_j \notin \mathrm{LT}_\sigma(I)\}$ for some set of polynomials $G \subseteq \overline{P}$. The fact that the polynomials in G are irreducible with respect to E implies that they have degree ≤ 1 in the indeterminates $e_1, \ldots, e_r$. Since we have $I_M \subseteq (e_1, \ldots, e_r)$, this shows that the polynomials in G are linear forms in $e_1, \ldots, e_r$. By Proposition 4.5.1.b, they are homogeneous with respect to the grading given by $\overline{W}$. Hence they are actually images of homogeneous vectors in M. Their leading terms generate all elements in $\mathrm{LT}_\sigma(I_M)$ of degree one in $e_1, \ldots, e_r$. Thus the leading terms of the corresponding elements of M generate $\mathrm{LT}_\sigma(M)$. Finally, since the elements of G are fully reduced against each other, the corresponding elements of M are fully reduced, too. Hence G is the image of the reduced σ-Gröbner basis of M in $\overline{P}$. □

In particular, notice that the reduced $\overline{\sigma}$-Gröbner basis of I_M is $G \cup E$ if we have $M \subseteq (x_1, \ldots, x_n) F_0$ and where G denotes the reduced σ-Gröbner basis of M. In the following, we give some typical examples of simultaneous extensions $\overline{\sigma}$ of σ and τ as required by this proposition.

Remark 4.7.17. Let $\tau = \mathtt{Ord}(V)$ be a term ordering on $\mathbb{T}^n$ given by a non-singular matrix $V \in \mathrm{Mat}_n(\mathbb{Z})$.

a) Let σ be the module term ordering τ−$\mathtt{Pos}$ on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ (see Example 1.4.16.a). Then $\overline{\sigma} = \mathtt{Ord}\left(\begin{smallmatrix} V & 0 \\ 0 & \mathcal{I}_r \end{smallmatrix}\right)$ is a term ordering on the monoid $\mathbb{T}^n(x_1, \ldots, x_n, e_1, \ldots, e_r)$ which extends both τ and σ.

b) Let σ be the module term ordering $\mathtt{Pos}$−τ on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ (see Example 1.4.16.b). Then $\overline{\sigma} = \mathtt{Ord}\left(\begin{smallmatrix} 0 & \mathcal{I}_r \\ V & 0 \end{smallmatrix}\right)$ is a term ordering on the monoid $\mathbb{T}^n(x_1, \ldots, x_n, e_1, \ldots, e_r)$ which extends both τ and σ.

c) Suppose that τ is a degree compatible term ordering of the form $\tau = \mathtt{Ord}\left(\begin{smallmatrix} W \\ W' \end{smallmatrix}\right)$ with $W' \in \mathrm{Mat}_{n-m,n}(\mathbb{Z})$ and that $d_{0i} >_{\mathtt{Lex}} 0$ for $i = 1, \ldots, r$. Then the module term ordering $\sigma = \mathtt{Deg}$−τ−$\mathtt{Pos}$ is compatible with τ, and the term ordering $\overline{\sigma} = \begin{pmatrix} W & d_{01} \cdots d_{0r} \\ W' & 0 \cdots 0 \\ 0 & \mathcal{I}_r \end{pmatrix}$ on $\mathbb{T}(x_1, \ldots, x_n, e_1, \ldots, e_r)$ extends both τ and σ.

Example 4.7.18. Let $P = K[x, y, z]$ be standard graded, and let τ be the term ordering $\mathtt{DegRevLex}$ on $\mathbb{T}^3$. Then $\sigma = \mathtt{PosDegRevLex}$ is a module term ordering on $\mathbb{T}^3\langle e_1, e_2, e_3\rangle$ which is compatible with τ. Moreover, the term ordering $\overline{\sigma} = \mathtt{Ord}\left(\begin{smallmatrix} 0 & \mathcal{I}_3 \\ V & 0 \end{smallmatrix}\right)$ with $V = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$ extends both σ and τ.

Now let M be the graded submodule of $P(-1)^3$ generated by the set of vectors $\{(x, y, 0), (0, 1, 0), (0, z^2, xy)\}$. Then the reduced σ-Gröbner basis

of M is $\{e_2, xe_1, xye_3\}$. By applying the proposition, we see that the reduced $\overline{\sigma}$-Gröbner basis of the ideal I_M is $\{e_2, xe_1, xye_3, e_1^2, e_1e_3, e_3^2\}$.

After clarifying the behaviour of Gröbner bases with respect to idealization, we turn to minimal homogeneous system of generators.

Proposition 4.7.19. (Minimal Generators and Idealization)
Let M be a graded submodule of a graded free P-module $F_0 = \bigoplus_{i=1}^{r} P(-d_{0i})$ such that $M \subseteq (x_1, \ldots, x_n) F_0$ and where $d_{0i} >_{\mathtt{Lex}} 0$ for $i = 1, \ldots, r$. Furthermore, let $\mathcal{V} = (v_1, \ldots, v_s)$ be a deg-ordered tuple of non-zero homogeneous vectors which generate M.

a) Assume that $\mathcal{V}$ is a minimal homogeneous system of generators of M. Then the set $\{v_1, \ldots, v_s\} \cup E$ is a minimal homogeneous system of generators of I_M.

Now let τ be a term ordering on $\mathbb{T}^n$, let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ which is compatible with τ, and let $\overline{\sigma}$ be a term ordering on $\mathbb{T}(x_1, \ldots, x_n, e_1, \ldots, e_r)$ which extends both σ and τ.

b) If we apply Buchberger's Algorithm with Minimalization 4.6.3 to the tuple $(\mathcal{V} \mid \mathcal{E})$, it computes a minimal system of generators of the ideal $I_M \subseteq \overline{P}$ of the form $(\mathcal{V}_{\min} \mid \mathcal{E})$, where $\mathcal{V}_{\min}$ is a minimal homogeneous system of generators of M.

c) If we apply the algorithm of Corollary 4.6.5 to the tuple $(\mathcal{V} \mid \mathcal{E})$, it computes a homogeneous $\overline{\sigma}$-Gröbner basis of I_M of the form $(\mathcal{G} \mid \mathcal{E})$ and a minimal system of generators of the form $(\mathcal{G}_{\min} \mid \mathcal{E})$, where $\mathcal{G}$ is a σ-Gröbner basis of M and $\mathcal{G}_{\min}$ is a minimal homogeneous system of generators of M which is contained in $\mathcal{G}$.

Proof. First we show a). By definition, the set $\{v_1, \ldots, v_s\} \cup E$ generates I_M. Consider the grading on $\overline{P}$ defined by $\deg(x_i) = 0$ and $\deg(e_j) = 1$ for $i = 1, \ldots, n$ and $j = 1, \ldots, r$. Then I_M is a homogeneous ideal with respect to this grading. Its homogeneous component of degree one is $Pv_1 + \cdots + Pv_s$, so that it follows from the minimality of $\mathcal{V}$ that we cannot drop any of these generators in $(\mathcal{V} \mid \mathcal{E})$. Next we consider the image of I_M under the substitution $x_i \mapsto 0$ for $i = 1, \ldots, n$. Since $M \subseteq (x_1, \ldots, x_n) F_0$, we have $v_i \mapsto 0$ for $i = 1, \ldots, s$. The images of the elements e_ie_j are minimal generators. Therefore the elements e_ie_j are minimal generators of I_M.

Now we prove b). The hypothesis $d_{0i} >_{\mathtt{Lex}} 0$ implies that $\overline{P}$ is positively graded. Hence we can apply Buchberger's Algorithm with Minimalization. Since $(\mathcal{V} \mid \mathcal{E})$ generates I_M, the algorithm computes a minimal system of generators of I_M which is contained in $(\mathcal{V} \mid \mathcal{E})$. By considering the grading $\deg(x_i) = 0$, $\deg(e_j) = 1$ again, we see that the vectors in $\mathcal{V}$ chosen by the algorithm correspond to a minimal system of generators of M. Moreover, the algorithm has to choose all polynomials e_ie_j because they are all minimal generators of I_M.

To show c), we claim that the $\overline{\sigma}$-Gröbner basis of I_M computed by the algorithm has the form $(\mathcal{G} \mid \mathcal{E})$. Clearly, a critical pair (i,j) such that $\mathrm{LT}_{\overline{\sigma}}(v_i) = c_i t_i e_{\gamma_i}$ and $\mathrm{LT}_{\overline{\sigma}}(v_j) = c_j t_j e_{\gamma_j}$ satisfy $\gamma_i = \gamma_j$ corresponds to a critical pair of the vectors $v_1, \ldots, v_s$ in M. However, if we have $\gamma_i \neq \gamma_j$, then the corresponding S-vector has degree two in the indeterminates $e_1, \ldots, e_r$. It reduces to zero, because the terms in its support are of the form te_ke_ℓ where e_ke_ℓ has a smaller degree and has been appended to the Gröbner basis already. Moreover, every time the algorithm encounters a term e_ke_ℓ, that term is irreducible with respect to the part of the Gröbner basis computed so far and is appended to the Gröbner basis and to the minimal system of generators. Altogether, we see that the algorithm computes a Gröbner basis of the form $(\mathcal{G} \mid \mathcal{E})$. As above, it follows that the minimal set of generators it finds is of the form $(\mathcal{G}_{\min} \mid \mathcal{E})$. □

Let us briefly discuss the hypotheses of this proposition.

Remark 4.7.20. Suppose we are in the setting of the proposition.

a) The assumption $M \subseteq (x_1, \ldots, x_n)\, F_0$ is essential for the proposition to be true. Otherwise, S-vectors of the form $e_{\gamma_i} v_j - e_{\gamma_j} v_i$ could be appended to the Gröbner basis, because they contain terms of the form $c\, e_k e_\ell$ with $c \in K$ which have not yet been treated, i.e. which are not yet in the Gröbner basis.

b) The assumption $d_{0i} >_{\mathtt{Lex}} 0$ for $i = 1, \ldots, r$ is used to conclude that the grading on $\overline{P}$ given by $\overline{W}$ is positive, but it is not essential for the correctness of the algorithm (see also the discussion below).

Next we want to idealize not only a graded submodule, but a whole homogeneous presentation. We continue to assume that M is a graded submodule of a graded free P-module $F_0 = \bigoplus_{i=1}^r P(-d_{0i})$, where $d_{01}, \ldots, d_{0r} \in \mathbb{Z}^m$, and that $\mathcal{V} = (v_1, \ldots, v_s)$ is a deg-ordered tuple of non-zero homogeneous elements which generate M. Then we form the graded free P-module $F_1 = \bigoplus_{j=1}^s P(-d_{1j})$ where $d_{1j} = \deg_W(v_j)$ for $j = 1, \ldots, s$. We let $\{\varepsilon_1, \ldots, \varepsilon_s\}$ be the canonical basis of F_1, and we consider a homogeneous presentation

$$F_2 \xrightarrow{\psi} F_1 \xrightarrow{\varphi} M \longrightarrow 0$$

of M, where $\varphi(\varepsilon_j) = v_j$ for $j = 1, \ldots, s$ and where F_2 is a another graded free P-module.

Remark 4.7.21. For every $d \in \mathbb{Z}^m$, a homogeneous presentation of the shifted module $M(d)$ is given by

$$F_2(d) \xrightarrow{\tilde{\psi}} F_1(d) \xrightarrow{\tilde{\varphi}} M(d) \longrightarrow 0$$

where $F_1(d)$ and $F_2(d)$ are graded free P-modules, and where the homogeneous P-linear maps $\tilde{\varphi}$ and $\tilde{\psi}$ are given by the same homogeneous matrices

as φ and ψ, respectively. Therefore the computation of a minimal homogeneous presentation of M is equivalent to the computation of a minimal homogeneous presentation of $M(d)$.

In view of this remark, we shall from now on assume that $d_{0i} >_{\mathtt{Lex}} 0$ for $i = 1, \ldots, r$. Notice that this implies $d_{1j} >_{\mathtt{Lex}} 0$ for $j = 1, \ldots, s$. This assumption will prove useful in our theoretical discussion below. In an actual implementation it is not really necessary, because shifting the entire computation by a fixed degree does not change its correctness.

In order to idealize the above presentation of M, we introduce the polynomial ring $\widetilde{P} = P[e_1, \ldots, e_r, \varepsilon_1, \ldots, \varepsilon_s] = K[x_1, \ldots, x_n, e_1, \ldots, e_r, \varepsilon_1, \ldots, \varepsilon_s]$ and equip it with the grading given by $\widetilde{W} = (W \mid d_{01} \cdots d_{0r} \mid d_{11} \cdots d_{1s})$. Notice that, because of our assumption, this grading is positive. By Proposition 4.7.14.a, the idealization of the module $F_0 \oplus F_1$ is the ring $\widetilde{P}/\tilde{\mathfrak{e}}$, where $\tilde{\mathfrak{e}}$ is the homogeneous ideal generated by the union of $\{e_i e_j \mid i, j = 1, \ldots, r\}$, $\{e_i \varepsilon_j \mid i \in \{1, \ldots, r\}, j \in \{1, \ldots, s\}\}$, and $\{\varepsilon_i \varepsilon_j \mid i, j = 1, \ldots, s\}$.

Let $\imath_0 : F_0 \longrightarrow \widetilde{P}/\tilde{\mathfrak{e}}$ be the homogeneous injective P-linear map given by $\imath_0((f_1, \ldots, f_r)) = f_1 e_1 + \cdots f_r e_r + \tilde{\mathfrak{e}}$, and let $\imath_1 : F_1 \longrightarrow \widetilde{P}/\tilde{\mathfrak{e}}$ be the homogeneous injective P-linear map given by $\imath_1((f_1, \ldots, f_s)) = f_1 \varepsilon_1 + \cdots f_s \varepsilon_s + \tilde{\mathfrak{e}}$. By Proposition 3.6.1, if $(f_1, \ldots, f_s) \in \mathrm{Syz}_P(\mathcal{V})$ is a homogeneous syzygy of $\mathcal{V}$, then the corresponding element $f_1 \varepsilon_1 + \cdots + f_s \varepsilon_s$ of $\widetilde{P}$ is contained in the ideal $(v_1 - \varepsilon_1, \ldots, v_s - \varepsilon_s)$.

Definition 4.7.22. The ideal $\tilde{I}_M = (v_1 - \varepsilon_1, \ldots, v_s - \varepsilon_s) + \tilde{\mathfrak{e}}$ in $\widetilde{P}$ is called the **ideal of the presentation** of M given above.

Our next proposition serves to justify this name.

Proposition 4.7.23. (Idealization of a Homogeneous Presentation) *Let $\tilde{I}_M \subseteq \widetilde{P}$ be the ideal of the presentation of M.*

a) There exists a unique P-algebra homomorphism

$$\Phi : P[\varepsilon_1, \ldots, \varepsilon_s]/(\varepsilon_i \varepsilon_j)_{i,j=1,\ldots,s} \longrightarrow \overline{P}/\mathfrak{e}$$

which maps the residue class of ε_i to $v_i + \mathfrak{e}$ for $i = 1, \ldots, s$.

b) The image of Φ is the residue class ideal of the ideal of M.

c) The kernel of Φ is the residue class ideal of the ideal of $\mathrm{Syz}_P(\mathcal{V})$.

d) The ideal of $\mathrm{Syz}_P(\mathcal{V})$ *is given by $\tilde{I}_M \cap P[\varepsilon_1, \ldots, \varepsilon_s]$.*

Proof. To prove a), it suffices to note that Φ is well-defined, because we have $v_i v_j \in \mathfrak{e}$ for $i, j = 1, \ldots, s$. Claim b) follows from Proposition 4.7.14.b.

To show c), we note that Φ is induced by the substitution homomorphism $\Psi : P[\varepsilon_1, \ldots, \varepsilon_s] \longrightarrow \overline{P}/\mathfrak{e}$ with $\varepsilon_k \mapsto v_k + \mathfrak{e}$ for $k = 1, \ldots, s$. The ideal $(\varepsilon_k \varepsilon_\ell)_{k,\ell=1,\ldots,s}$ is contained in $\mathrm{Ker}(\Psi)$. Since $v_1, \ldots, v_s \in (e_1, \ldots, e_r)$, the kernel of the composition of Ψ with the canonical surjection $\overline{P}/\mathfrak{e} \longrightarrow P$

is $(\varepsilon_1, \ldots, \varepsilon_s)$, and therefore we have $\mathrm{Ker}(\Psi) \subseteq (\varepsilon_1, \ldots, \varepsilon_s)$. Furthermore, we have $f_1\varepsilon_1 + \cdots + f_s\varepsilon_s \in \mathrm{Ker}(\Psi)$ if and only if $f_1v_1 + \cdots + f_sv_s = 0$. Hence $\{f_1\varepsilon_1 + \cdots + f_s\varepsilon_s \mid (f_1, \ldots, f_s) \in \mathrm{Syz}_P(\mathcal{V})\} \cup \{\varepsilon_k\varepsilon_\ell \mid k, \ell = 1, \ldots, s\}$ generates $\mathrm{Ker}(\Psi)$, and the claim follows from Proposition 4.7.14.b.

Finally, part d) follows from c) by a slight generalization of Proposition 3.6.2, but the proof of that proposition still applies without modifications. □

4.7.C Computation of Minimal Homogeneous Presentations

There are two basic strategies for success
in computing minimal homogeneous presentations:
1. Never reveal your strategy.
2.
(Anonymous)

Knowing that a finitely generated graded P-module has a unique minimal homogeneous presentation is not the same thing as being able to find it. In principle, a couple of applications of Buchberger's Algorithm with Minimalization 4.6.3 should do the trick, but not in an efficient way. Thus we are looking for better strategies. In this subsection, we shall reveal two good strategies for computing minimal homogeneous presentations: the vertical and the horizontal strategy. In fact, we shall explain how our strategies can be successful without needing to be secretive.

What does it mean to compute a minimal homogeneous presentation? To be able to compute anything, we have to assume that M is somehow given explicitly. Many times we assume that M is given by generators and relations, i.e. that we have an isomorphism $M \cong \bigoplus_{i=1}^{r} P(-d_{0i})/\langle v_1, \ldots, v_s\rangle$. In this case, it is easy to find a minimal homogeneous presentation.

Proposition 4.7.24. *Let $d_{01}, \ldots, d_{0r} \in \mathbb{Z}^m$, let $F_0 = \bigoplus_{i=1}^{r} P(-d_{0i})$, and let $v_1, \ldots, v_s \in F_0$ be homogeneous vectors such that we have an isomorphism of graded P-modules $M \cong F_0/\langle v_1, \ldots, v_s\rangle$. For $i = 1, \ldots, r$, let $\bar{e}_i$ be the residue class of e_i in M.*

a) The set of generators $\{\bar{e}_1, \ldots, \bar{e}_r\}$ of M is minimal if and only if we have $e_i \notin \langle e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_r, v_1, \ldots, v_s\rangle$ for $i = 1, \ldots, r$.

b) Consider the following instructions.

1) Let $r' = r$, let $d'_{0i} = d_{0i}$ for $i = 1, \ldots, r$, let $\mathcal{W} = (v_1, \ldots, v_s)$, let $s' = s$, and let $i = 1$.

2) Check whether $\mathcal{W}$ contains a zero column. If so, delete that column in $\mathcal{W}$, decrease s' by one, and repeat step 2).

3) Check whether the i^{th} row of $\mathcal{W}$ contains a non-zero constant. If so, continue with step 5).

4) Increase i by one. If $i > r'$, return $\mathcal{W}$ and stop. Otherwise, continue with step 3).

5) Let $j \in \{1, \ldots, s'\}$ be such that the entry of $\mathcal{W}$ in position (i, j) is a non-zero constant. Use this entry and row operations on $\mathcal{W}$ to produce zeros everywhere else in the j^{th} column. Delete the i^{th} row and the j^{th} column of the new matrix and replace $\mathcal{W}$ by the resulting matrix.

6) Decrease r' and s' by one. Replace d'_{0j} by $d'_{0\,j+1}$ for $j = i, \ldots, r'$. Then continue with step 2).

This is an algorithm which computes a tuple of homogeneous vectors $\mathcal{W} = (w_1, \ldots, w_{s'})$ such that we have a homogeneous presentation $M \cong \bigoplus_{i=1}^{r'} P(-d'_{0i})/\langle w_1, \ldots, w_{s'} \rangle$, and such that $\bar{e}_1, \ldots, \bar{e}_{r'}$ is a minimal homogeneous system of generators of M.

Proof. The first claim follows immediately from the graded version of Nakayama's lemma (see Proposition 4.1.22). The procedure defined in b) is clearly finite, because we either increase i in step 4) or decrease r' in step 6). It remains to show that the algorithm is correct.

Obviously, if some column of $\mathcal{W}$ is zero, the corresponding vector is not a minimal generator of $\langle w_1, \ldots, w_{s'} \rangle$ and can be deleted. This is done in step 2). Let $i \in \{1, \ldots, r'\}$ and $j \in \{1, \ldots, s'\}$ be such that the entry in position (i, j) of $\mathcal{W}$ is a non-zero constant. Without loss of generality we may assume that it is 1. Hence there exists an element of the form $v'_j = e_i + \sum_{k \neq i} a_k e_k$ with $a_k \in P$ which is contained in the module generated by the current column vectors $v'_1, \ldots, v'_{s'}$ of $\mathcal{W}$. The row operations performed in step 5) correspond to using this element to rewrite $v'_1, \ldots, v'_{j-1}, v'_{j+1}, \ldots, v'_{s'}$ in such a way that the result does not involve e_i anymore. Consequently, the residue class $\bar{e}_i$ is not a minimal generator of M and the syzygies of the system of generators $\{\bar{e}_1, \ldots, \bar{e}_{i-1}, \bar{e}_{i+1}, \ldots, \bar{e}_{s'}\}$ of M are generated by the columns of the new matrix $\mathcal{W}$ computed by step 5). Clearly, step 6) conducts the necessary adjustments to r', s', and F_0.

Altogether, we have shown that step 3) correctly recognizes non-minimal generators $\bar{e}_i$ of M and steps 5) and 6) correctly remove them and modify the presentation accordingly. □

Using this proposition, it is easy to compute a minimal homogeneous presentation of M. In fact, it suffices to apply Buchberger's Algorithm with Minimalization 4.6.3 to the tuple $\mathcal{W}$ returned by the algorithm of part b) of the proposition.

Done! Or are we? Is this really all there is to it? Not quite! The situation becomes more interesting if we assume that M is a submodule of a graded free module $F_0 = \bigoplus_{i=1}^{r} P(-d_{0i})$ and that it is given by a deg-ordered homogeneous system of generators $\mathcal{V} = (v_1, \ldots, v_s)$. In view of Proposition 4.1.22, the preceding proposition says that in order to compute a minimal homogeneous presentation of M, we may assume that $M \subseteq (x_1, \ldots, x_n) F_0$. Based

on the results of Sections 3.1 and 4.6, there is again an obvious method to solve our task.

Remark 4.7.25. Consider the following instructions.

1) Using the Buchberger Algorithm with Minimalization 4.6.3, compute a subtuple $\mathcal{V}_{\min}$ of $\mathcal{V}$ of homogeneous vectors which generate M minimally.
2) Using Theorem 3.1.8, compute a matrix $\mathcal{S}$ whose columns generate the module $\mathrm{Syz}_P(\mathcal{V}_{\min})$. (Notice that all computations involved here keep the homogeneity of the input by Proposition 4.5.1. Thus $\mathcal{S}$ is a homogeneous matrix.)
3) Using the Buchberger Algorithm with Minimalization 4.6.3, compute a subtuple $\mathcal{S}_{\min}$ of $\mathcal{S}$ of homogeneous vectors which generate $\mathrm{Syz}_P(\mathcal{S}_{\min})$ minimally.
4) Return $\mathcal{V}_{\min}$ and $\mathcal{S}_{\min}$ and stop.

This is an algorithm which computes two tuples $\mathcal{V}_{\min}$ and $\mathcal{S}_{\min}$ of homogeneous vectors such that $\mathcal{V}_{\min}$ minimally generates M and $\mathcal{S}_{\min}$ minimally generates $\mathrm{Syz}_P(\mathcal{V}_{\min})$. In particular, we have a minimal homogeneous presentation

$$F_2 \xrightarrow{\psi} F_1 \xrightarrow{\varphi} M \longrightarrow 0$$

where F_1 and F_2 are graded free P-modules, where ψ is given by $\mathcal{S}_{\min}$ and where φ is given by $\mathcal{V}_{\min}$.

Notice that this algorithm is rather wasteful, because the reduction steps involved in computing the Gröbner basis of M in Theorem 4.6.3 have to be done again by Theorem 3.1.8 (see Tutorial 61). Using the idealization of the presentation discussed in the previous subsection, we can proceed in a more efficient way. The method we use in the next theorem is called the **vertical strategy**. The reason is that we compute first a minimal system of generators $\mathcal{G}_{\min}$ of M by looping through all necessary degrees (which we think of as being on top of each other) and then a minimal system of generators of $\mathrm{Syz}_P(\mathcal{G}_{\min})$ by a similar loop.

To ease the notation, we shall continue to resort to the following convention introduced in Section 4.5. Given a tuple $\mathcal{G} = (g_1, \ldots, g_{s'})$, we write $\mathrm{LT}_\sigma(g_i) = t_i\, e_{\gamma_i}$ with $t_i \in \mathbb{T}^n$ and $\gamma_i \in \{1, \ldots, r\}$ for $i = 1, \ldots, s'$. Moreover, we identify the elements of the graded free P-module $F_0 = \bigoplus_{i=1}^r P(-d_{0i})$ with their canonical images in the polynomial ring $\overline{P} = P[e_1, \ldots, e_r]$ and equip $\overline{P}$ with the grading given by $\overline{W} = (W \mid d_{01} \cdots d_{0r})$.

Theorem 4.7.26. (Computing Minimal Presentations Vertically) *Let M be a graded submodule of a graded free P-module $F_0 = \bigoplus_{i=1}^r P(-d_{0i})$ where $d_{0i} >_{\mathtt{Lex}} 0$ for $i = 1, \ldots, r$. Let $\mathcal{V} = (v_1, \ldots, v_s)$ be a deg-ordered tuple of non-zero homogeneous vectors which generate M. Consider the following instructions.*

1) Choose a term ordering σ on $\mathbb{T}^n(e_1,\ldots,e_r)$. Let $B=\emptyset$, $\mathcal{W}=\mathcal{V}$, $\mathcal{G}=\emptyset$, $s'=0$, $\mathcal{G}_{\min}=\emptyset$, $\mu=0$, and $\mathcal{S}=\emptyset$.

2) Let d be the smallest degree with respect to `Lex` *of an element in B or in $\mathcal{W}$. Form the subset B_d and the subtuple $\mathcal{W}_d$, and delete their entries from B and $\mathcal{W}$, respectively.*

3) If $B_d=\emptyset$, continue with step 6). Otherwise, chose a pair $(i,j)\in B_d$ and remove it from B_d.

4) Compute the S-vector S_{ij} of g_i and g_j. Then compute $S'_{ij}=\mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$. If $S'_{ij}=0$ continue with step 3). If $S'_{ij}\neq 0$ and it does not involve the indeterminates $e_1,\ldots,e_r$, append it to $\mathcal{S}$ and continue with step 3).

5) Increase s' by one, append $g_{s'}=S'_{ij}$ to the tuple $\mathcal{G}$, and append the set $\{(i,s') \mid 1\leq i<s',\ \gamma_i=\gamma_{s'}\}$ to B, where $\mathrm{LT}_\sigma(g_{s'})=t_{s'}e_{\gamma_{s'}}$ with $t_{s'}\in\mathbb{T}^n$ and $\gamma_{s'}\in\{1,\ldots,r\}$. Then continue with step 3).

6) If $\mathcal{W}_d=\emptyset$, continue with step 9). Otherwise, choose a vector $v\in\mathcal{W}_d$ and remove it from $\mathcal{W}_d$.

7) Compute $v'=\mathrm{NR}_{\sigma,\mathcal{G}}(v)$ and $\bar{v}=v'(x_1,\ldots,x_n,e_1,\ldots,e_r,0,\ldots,0)$. If $\bar{v}=0$, continue with step 6).

8) Increase s' and μ by one. Adjoin a new indeterminate ε_μ to $\overline{P}$ and extend the grading to this new ring by defining $\deg_{\overline{W}}(\varepsilon_\mu)=\deg_{\overline{W}}(\bar{v})$. Extend the term ordering σ to the new ring in such a way that the extension is an elimination ordering for $\{e_1,\ldots,e_r\}$. Append $g_{s'}=\bar{v}-\varepsilon_\mu$ to $\mathcal{G}$ and $\bar{v}$ to $\mathcal{G}_{\min}$. Append the set $\{(i,s') \mid 1\leq i<s',\ \gamma_i=\gamma_{s'}\}$ to B. Continue with step 6).

9) If $B\neq\emptyset$ or $\mathcal{W}\neq\emptyset$, continue with step 2).

10) Apply the Buchberger Algorithm with Minimalization 4.6.3 to the module generated by $\mathcal{S}$ and obtain a subtuple $\mathcal{S}_{\min}$ of $\mathcal{S}$ which minimally generates that module. Return the pair $(\mathcal{G}_{\min},\mathcal{S}_{\min})$ and stop.

This is an algorithm which computes a pair $(\mathcal{G}_{\min},\mathcal{S}_{\min})$ where $\mathcal{G}_{\min}$ is a deg-ordered tuple of homogeneous vectors in F_0 which generate M minimally, and $\mathcal{S}_{\min}$ is a deg-ordered tuple of homogeneous vectors in $\bigoplus_{i=1}^{\mu}P(-d_{1i})$ which generate $\mathrm{Syz}_P(\mathcal{G}_{\min})$ minimally. Here μ is the number of elements in $\mathcal{G}_{\min}$ and d_{1i} is the degree of the i^{th} element in $\mathcal{G}_{\min}$ for $i=1,\ldots,\mu$.

Proof. In order to prove the finiteness of this procedure, we note that elements are appended to $\mathcal{G}$ and B only in steps 5) and 8). By induction on s', we see that all elements of $\mathcal{G}$ are of the form $a_1e_1+\cdots+a_re_r+b_1\varepsilon_1+\cdots+b_\mu\varepsilon_\mu$ with $a_i,b_j\in P$. Moreover, the checks in step 4) and step 7) make sure that at least one polynomial a_i is non-zero. Since B is enlarged only when an element is appended to $\mathcal{G}$ which has a new leading term, and since Corollary 1.3.10 implies that this can happen only finitely many times, the procedure terminates after finitely many steps.

Now we prove correctness. If we substitute $\varepsilon_1\mapsto 0,\ \ldots,\ \varepsilon_\mu\mapsto 0$ everywhere, the algorithm reduces to the Buchberger Algorithm with Minimalization 4.6.5. Thus the resulting tuple $\mathcal{G}_{\min}$ is a minimal homogeneous set of generators of M. To show that $\mathcal{S}_{\min}$ is correct, we use Proposition 4.7.23. Notice

that the elements $g_{s'} = \bar{v} - \varepsilon_\mu$ appended to $\mathcal{G}$ in step 8) are exactly the generators of $\tilde{I}_M$ corresponding to the minimal system of generators $\mathcal{G}_{\min}$ of M. Thus Proposition 4.7.23.e says that $\mathrm{Syz}_P(\mathcal{G}_{\min})$ corresponds to the residue class ideal of $\tilde{I}_M \cap P[\varepsilon_1, \ldots, \varepsilon_\mu]$ in $P[\varepsilon_1, \ldots, \varepsilon_\mu]/(\varepsilon_1\varepsilon_j \mid i, j = 1, \ldots, \mu)$. Since all extensions of σ are elimination orderings for $\{e_1, \ldots, e_r\}$, the σ-Gröbner basis of $\tilde{I}_M$ contains a system of generators of $\mathrm{Syz}_P(\mathcal{G}_{\min})$.

In fact, we claim that the elements of $\mathcal{S}$ are a σ-Gröbner basis of $\mathrm{Syz}_P(\mathcal{G}_{\min})$ when the algorithm stops. This follows by inspecting the effect of step 4): a σ-Gröbner basis element S'_{ij} of $\tilde{I}_M$ corresponds to a syzygy of $\mathcal{G}_{\min}$ if and only if it is contained in $P[\varepsilon_1, \ldots, \varepsilon_\mu]$. Finally, we note that $\mathcal{S}_{\min}$ is indeed a minimal system of generators of $\mathrm{Syz}_P(\mathcal{G}_{\min})$ because we apply Theorem 4.6.3 in step 10). □

The algorithm described in this theorem gives us another way to compute the degree pair $(\deg_W(\mathcal{G}_{\min}), \deg_W(\mathcal{S}_{\min}))$ of the module M effectively. But unlike Remark 4.7.25, it returns a minimal system of generators which is not necessarily contained in the given set of generators. Our next remark shows how we can modify the theorem to get this property as well.

Remark 4.7.27. In the algorithm of the theorem, the elements v of the tuple $\mathcal{V}$ for which the corresponding v' does not involve the indeterminates $e_1, \ldots, e_r$ form a subtuple $\mathcal{V}_{\min}$ of $\mathcal{V}$ which minimally generates M. By keeping track of the representations of new Gröbner basis elements in terms of the elements in $\mathcal{V}_{\min}$, we compute a homogeneous matrix $\mathcal{A}$ such that $\mathcal{G} = \mathcal{V}_{\min}\mathcal{A}$. Since $\mathcal{G}_{\min}$ is a subtuple of $\mathcal{G}$, the columns corresponding to the elements of $\mathcal{G}_{\min}$ in this matrix equality yield a matrix $\mathcal{B}$ such that $\mathcal{G}_{\min} = \mathcal{V}_{\min}\mathcal{B}$. Then the exact sequence $F_2 \xrightarrow{\psi'} F_1 \xrightarrow{\varphi'} M \longrightarrow 0$, where ψ' is given by the matrix $\mathcal{B}\mathcal{S}_{\min}$ and where φ' is given by $\mathcal{V}_{\min}$, is a minimal homogeneous presentation of M by Proposition 4.7.10.

To get a better understanding of the algorithm of the theorem, we apply to in a concrete case and monitor its workings carefully.

Example 4.7.28. Let $P = \mathbb{Q}[x_1, x_2, x_3, x_4]$ be graded by $W = \left(\begin{smallmatrix}1&1&1&1\\0&1&3&4\end{smallmatrix}\right)$, and let I be the homogeneous ideal in P generated by $\{f_1, f_2, f_3, f_4\}$ where $f_1 = x_1x_4 - x_2x_3$, $f_2 = x_1^2x_3 - x_2^3$, $f_3 = x_1x_3^2 - x_2^2x_4$, and $f_4 = x_2x_4^2 - x_3^3$. We would like to compute a minimal homogeneous presentation of I. Since the degree of the canonical basis vector $e = 1$ of $F'_0 = P$ is $\deg_W(1) = \binom{0}{0}$, the theorem is not immediately applicable. We apply Remark 4.7.21 and consider the graded P-submodule $M = I(-\binom{1}{0})$ of $F_0 = P(-\binom{1}{0})$ instead, where the canonical basis vector e of F_0 has degree $\deg_W(e) = \binom{1}{0}$. As we said already, in an actual implementation this is not really necessary.

The P-module M is generated by the homogeneous deg-ordered tuple $\mathcal{V} = (f_1e, f_2e, f_3e, f_4e)$, where $\deg_W(f_1e) = \binom{3}{4}$, $\deg_W(f_2e) = \binom{4}{3}$,

$\deg_W(f_3) = \binom{4}{6}$, and $\deg_W(f_4) = \binom{4}{9}$. Let us follow the steps of the algorithm. To unclutter the presentation, we only note those steps where something happens. For the term ordering σ, we always choose the lexicographic term ordering such that

$$e >_{\mathtt{Lex}} \varepsilon_1 >_{\mathtt{Lex}} \cdots >_{\mathtt{Lex}} \varepsilon_\mu >_{\mathtt{Lex}} x_1 >_{\mathtt{Lex}} \cdots >_{\mathtt{Lex}} x_n$$

1) Let $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, $s' = 0$, $\mathcal{G}_{\min} = \emptyset$, $\mu = 0$, and $\mathcal{S} = \emptyset$.
2) Let $d = \binom{3}{4}$, $B_d = \emptyset$, $\mathcal{W}_d = (f_1 e)$, and $\mathcal{W} = (f_2 e, f_3 e, f_4 e)$.
6) Choose $v = f_1 e$ and set $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = f_1 e$ and $\bar{v} = f_1 e$.
8) Let $s' = 1$ and $\mu = 1$. Adjoin ε_1 to $\overline{P}$ and let $\deg_{\overline{W}}(\varepsilon_1) = \binom{3}{4}$. Let $g_1 = f_1 e - \varepsilon_1$, let $\mathcal{G} = (g_1)$, and let $\mathcal{G}_{\min} = (f_1 e)$.
2) Let $d = \binom{4}{3}$, $B_d = \emptyset$, $\mathcal{W}_d = (f_2 e)$, and $\mathcal{W} = (f_3 e, f_4 e)$.
6) Choose $v = f_2 e$ and set $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = f_2 e$ and $\bar{v} = f_2 e$.
8) Let $s' = 2$ and $\mu = 2$. Adjoin ε_2 to $\overline{P}$ and let $\deg_{\overline{W}}(\varepsilon_2) = \binom{4}{3}$. Let $g_2 = f_2 e - \varepsilon_2$, let $\mathcal{G} = (g_1, g_2)$, let $\mathcal{G}_{\min} = (f_1 e, f_2 e)$, and let $B = \{(1,2)\}$. Observe that $\deg_{\overline{W}}((1,2)) = \binom{5}{7}$.
2) Let $d = \binom{3}{6}$, $B_d = \emptyset$, $\mathcal{W}_d = (f_3 e)$, and $\mathcal{W} = (f_4 e)$.
6) Choose $v = f_3 e$ and set $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = f_3 e$ and $\bar{v} = f_3 e$.
8) Let $s' = 3$ and $\mu = 3$. Adjoin ε_3 to $\overline{P}$ and let $\deg_{\overline{W}}(\varepsilon_3) = \binom{4}{6}$. Let $g_3 = f_3 e - \varepsilon_3$, let $\mathcal{G} = (g_1, g_2, g_3)$, let $\mathcal{G}_{\min} = (f_1 e, f_2 e, f_3 e)$, and let $B = \{(1,2), (1,3), (2,3)\}$. Observe that $\deg_{\overline{W}}((1,3)) = \binom{5}{10}$ and $\deg_{\overline{W}}((2,3)) = \binom{5}{6}$.
2) Let $d = \binom{4}{9}$, $B_d = \emptyset$, $\mathcal{W}_d = (f_4 e)$, and $\mathcal{W} = \emptyset$.
6) Choose $v = f_4 e$ and set $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = f_4 e$ and $\bar{v} = f_4 e$.
8) Let $s' = 4$ and $\mu = 4$. Adjoin ε_4 to $\overline{P}$ and let $\deg_{\overline{W}}(\varepsilon_4) = \binom{4}{9}$. Then let $g_4 = f_4 e - \varepsilon_4$, let $\mathcal{G} = (g_1, g_2, g_3, g_4)$, let $\mathcal{G}_{\min} = (f_1 e, f_2 e, f_3 e, f_4 e)$, and let $B = \{(1,2), (1,3), (2,3), (1,4), (2,4), (3,4)\}$. Notice that we have $\deg_{\overline{W}}((1,4)) = \binom{5}{9}$, $\deg_{\overline{W}}((2,4)) = \binom{7}{12}$, and $\deg_{\overline{W}}((3,4)) = \binom{7}{15}$.
2) Let $d = \binom{5}{6}$, $B_d = \{(2,3)\}$, and $B = \{(1,2), (1,3), (1,4), (2,4), (3,4)\}$.
3) Choose $(2,3) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{23} = x_3 g_2 - x_1 g_3 = x_1 x_2^2 x_4 e - x_2^3 x_3 e - x_3 \varepsilon_2 + x_1 \varepsilon_3$ and $S'_{23} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{23}) = x_2^2 \varepsilon_1 - x_3 \varepsilon_2 + x_1 \varepsilon_3$. Set $\mathcal{S} = (S'_{23})$.
2) Let $d = \binom{5}{7}$, $B_d = \{(1,2)\}$, and $B = \{(1,3), (1,4), (2,4), (3,4)\}$.
3) Choose $(1,2) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{12} = x_1 x_3 g_1 - x_4 g_2 = x_2^3 x_4 e - x_1 x_2 x_3^2 e - x_1 x_3 \varepsilon_1 + x_4 \varepsilon_2$ and $S'_{12} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{12}) = -x_1 x_3 \varepsilon_1 + x_4 \varepsilon_2 - x_2 \varepsilon_3$. Set $\mathcal{S} = (S'_{23}, S'_{12})$.
2) Let $d = \binom{5}{9}$, $B_d = \{(1,4)\}$, and $B = \{(1,3), (2,4), (3,4)\}$.
3) Choose $(1,4) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{14} = x_2 x_4 g_1 - x_1 g_4 = x_1 x_3^3 e - x_2^2 x_3 x_4 e - x_2 x_4 \varepsilon_1 + x_1 \varepsilon_4$ and $S'_{14} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{14}) = -x_2 x_4 \varepsilon_1 + x_3 \varepsilon_3 + x_1 \varepsilon_4$. Set $\mathcal{S} = (S'_{23}, S'_{12}, S'_{14})$.

2) Let $d = \binom{5}{10}$, $B_d = \{(1,3)\}$, and $B = \{(2,4), (3,4)\}$.
3) Choose $(1,3) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{13} = x_3^2 g_1 - x_4 g_3 = x_2^2 x_4^2 e - x_2 x_3^3 e - x_3^2 \varepsilon_1 + x_4 \varepsilon_3$, and then $S'_{13} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{13}) = -x_3^2 \varepsilon_1 + x_4 \varepsilon_3 + x_2 \varepsilon_4$. Set $\mathcal{S} = (S'_{23}, S'_{12}, S'_{14}, S'_{13})$.
2) Let $d = \binom{7}{12}$, $B_d = \{(2,4)\}$, and $B = \{(3,4)\}$.
3) Choose $(2,4) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{24} = x_2 x_4^2 g_2 - x_1^2 x_3 g_4 = x_1^2 x_3^4 e - x_2^4 x_4^2 e - x_2 x_4^2 \varepsilon_2 + x_1^2 x_3 \varepsilon_4$ and $S'_{24} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{24}) = -x_2 x_4^2 \varepsilon_2 + x_3^3 \varepsilon_2 + x_1^2 x_3 \varepsilon_4 - x_2^3 \varepsilon_4$.
2) Let $d = \binom{7}{15}$, $B_d = \{(3,4)\}$, and $B = \emptyset$.
3) Choose $(3,4) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{34} = x_2 x_4^2 g_3 - x_1 x_3^2 g_4 = x_1 x_3^5 e - x_2^3 x_4^3 e + x_1 x_3^2 \varepsilon_4 - x_2 x_4^2 \varepsilon_3$ and $S'_{34} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{24}) = -x_2 x_4^2 \varepsilon_3 + x_3^3 \varepsilon_3 + x_1 x_3^2 \varepsilon_4 - x_2^2 x_4 \varepsilon_4$.

At this point we have computed a minimal set of generators $\mathcal{G}_{\min}$ of M and a homogeneous set of generators $\mathcal{S}$ of $\mathrm{Syz}_P(\mathcal{G}_{\min})$. Step 10) now requires us to apply the Buchberger Algorithm with Minimalization 4.6.3 to the tuple $\mathcal{V} = (v_1, \ldots, v_6) = \mathcal{S} = (S'_{23}, S'_{12}, S'_{14}, S'_{13}, S'_{24}, S'_{34})$, where $v_1 = S'_{23} = x_2^2 \varepsilon_1 - x_3 \varepsilon_2 + x_1 \varepsilon_3$, $v_2 = S'_{12} = -x_1 x_3 \varepsilon_1 + x_4 \varepsilon_2 - x_2 \varepsilon_3$, $v_3 = S'_{14} = -x_2 x_4 \varepsilon_1 + x_3 \varepsilon_3 + x_1 \varepsilon_4$, $v_4 = S'_{13} = -x_3^2 \varepsilon_1 + x_4 \varepsilon_3 + x_2 \varepsilon_4$, $v_5 = S'_{24} = -x_2 x_4^2 \varepsilon_2 + x_3^3 \varepsilon_2 + x_1^2 x_3 \varepsilon_4 - x_2^3 \varepsilon_4$, and $v_6 = S'_{34} = -x_2 x_4^2 \varepsilon_3 + x_3^3 \varepsilon_3 + x_1 x_3^2 \varepsilon_4 - x_2^2 x_4 \varepsilon_4$. Notice that $\deg_{\overline{W}}(v_1) = \binom{5}{6}$, $\deg_{\overline{W}}(v_2) = \binom{5}{7}$, $\deg_{\overline{W}}(v_3) = \binom{5}{9}$, $\deg_{\overline{W}}(v_4) = \binom{5}{10}$, $\deg_{\overline{W}}(v_5) = \binom{7}{12}$, and $\deg_{\overline{W}}(v_6) = \binom{7}{15}$.

In this case, the situation is particularly favourable. The reason is that the first component of the degree of the first four elements in $\mathcal{S}$ is five and the second components are pairwise different. Since the first component of the degree of every indeterminate is positive, the first four elements of $\mathcal{S}$ are already interreduced. The last two elements are easily seen to be contained in the ideal generated by the first four. Therefore we get $\mathcal{S}_{\min} = (v_1, v_2, v_3, v_4)$.

For the sake of completeness, we list the steps of Theorem 4.6.3 in the idealized setting. We work in the polynomial ring $K[x_1, x_2, x_3, x_4, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4]$ which is graded by $\overline{W} = \binom{1\ 1\ 1\ 1\ 5\ 5\ 5\ 5}{0\ 1\ 3\ 4\ 6\ 7\ 9\ 10}$. We use an elimination ordering σ for $\varepsilon_1, \ldots, \varepsilon_4$. Since we are only interested in a minimal system of generators contained in $\mathcal{S}$, we may use Remark 4.6.4 and truncate the computation after we have finished degree $d_{\max} = \binom{7}{15}$ and we may ignore pairs of higher degree.

1) Let $B = \emptyset$, $v_1 = S'_{23}$, $v_2 = S'_{12}$, $v_3 = S'_{14}$, $v_4 = S'_{13}$, $v_5 = S'_{24}$, $v_6 = S'_{34}$, $\mathcal{W} = (v_1, v_2, v_3, v_4, v_5, v_6)$, $\mathcal{G} = \emptyset$, $s' = 0$, and $\mathcal{V}_{\min} = \emptyset$.
2) Let $d = \binom{5}{6}$, $\mathcal{W}_d = (v_1)$, and $\mathcal{W} = (v_2, v_3, v_4, v_5, v_6)$.
6) Choose $v = v_1$ and let $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = v_1$.
8) Let $s' = 1$, $\mathcal{G} = (v_1)$, and $\mathcal{V}_{\min} = (v_1)$.
2) Let $d = \binom{5}{7}$, $\mathcal{W}_d = (v_2)$, and $\mathcal{W} = (v_3, v_4, v_5, v_6)$.
6) Choose $v = v_2$ and let $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = v_2$.

8) Let $s' = 2$, $\mathcal{G} = (v_1, v_2)$, $\mathcal{V}_{\min} = (v_1, v_2)$, and $B = \{(1,2)\}$. Notice that $\deg_{\overline{W}}((1,2)) = \binom{7}{9}$.
2) Let $d = \binom{5}{9}$, $\mathcal{W}_d = (v_3)$, and $\mathcal{W} = (v_4, v_5, v_6)$.
6) Choose $v = v_3$ and let $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = v_3$.
8) Let $s' = 3$, $\mathcal{G} = (v_1, v_2, v_3)$, $\mathcal{V}_{\min} = (v_1, v_2, v_3)$, and $B = \{(1,2), (1,3), (2,3)\}$. Notice that $\deg_{\overline{W}}((1,3)) = \binom{6}{10}$ and $\deg_{\overline{W}}((2,3)) = \binom{7}{12}$.
2) Let $d = \binom{5}{10}$, $\mathcal{W}_d = (v_4)$, and $\mathcal{W} = (v_5, v_6)$.
6) Choose $v = v_4$ and let $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = v_4$.
8) Let $s' = 4$, $\mathcal{G} = (v_1, v_2, v_3, v_4)$, $\mathcal{V}_{\min} = (v_1, v_2, v_3, v_4)$, and $B = \{(1,2), (1,3), (2,3), (1,4), (2,4), (3,4)\}$. We observe that $\deg_{\overline{W}}((1,4)) = \binom{7}{12}$, $\deg_{\overline{W}}((2,4)) = \binom{6}{10}$, and $\deg_{\overline{W}}((3,4)) = \binom{7}{15}$.
2) Let $d = \binom{6}{10}$, $\mathcal{W}_d = \emptyset$, $\mathcal{W} = (v_5, v_6)$, $B_d = \{(1,3), (2,4)\}$, and let $B = \{(1,2), (2,3), (1,4), (3,4)\}$.
3) Choose $(1,3) \in B_d$ and let $B_d = \{(2,4)\}$.
4) Compute $S_{13} = x_4 v_1 + x_2 v_3 = -x_3 x_4 \varepsilon_2 + x_1 x_4 \varepsilon_3 + x_2 x_3 \varepsilon_3 + x_1 x_2 \varepsilon_4$ and $S'_{13} = S_{13}$.
5) Append $g_5 = S_{13}$ to $\mathcal{G}$. No pairs need to be appended to B.
3) Choose $(2,4) \in B_d$ and let $B_d = \emptyset$.
4) Compute $S_{24} = x_3 v_2 - x_1 v_4 = x_3 x_4 \varepsilon_2 - x_2 x_3 \varepsilon_3 - x_1 x_4 \varepsilon_3 - x_1 x_2 \varepsilon_4$ and $S'_{24} = 0$.
2) Let $d = \binom{7}{9}$, $B_d = \{(1,2)\}$, and $B = \{(2,3), (1,4), (3,4)\}$.
3) Choose $(1,2) \in B_d$ and let $B_d = \emptyset$.
4) Compute $S_{12} = x_1 x_3 v_1 + x_2^2 v_2 = -x_1 x_3^2 \varepsilon_2 + x_2^2 x_4 \varepsilon_2 + x_1^2 x_3 \varepsilon_3 - x_2^3 \varepsilon_3$ and $S'_{12} = S_{12}$.
5) Append $g_6 = S'_{12}$ to $\mathcal{G}$. From now on, no new pairs have to be created since they all have too large degree.
2) Let $d = \binom{7}{12}$, $B_d = \{(2,3), (1,4)\}$, $B = \{(3,4)\}$, $\mathcal{W}_d = (v_5)$, and $\mathcal{W} = v_6$.
3) Choose $(2,3) \in B_d$ and let $B_d = \{(1,4)\}$.
4) Compute $S_{23} = x_2 x_4 v_2 - x_1 x_3 v_3 = x_2 x_4^2 \varepsilon_2 - x_2^2 x_4 \varepsilon_3 - x_1 x_3^2 \varepsilon_3 - x_1^2 x_3 \varepsilon_4$ and $S'_{23} = S_{23}$.
5) Append $g_7 = S'_{23}$ to $\mathcal{G}$.
3) Choose $(1,4) \in B_d$ and let $B_d = \emptyset$.
4) Compute $S_{14} = x_3^2 g_1 + x_2^2 g_4 = -x_3^3 \varepsilon_2 + x_1 x_3^2 \varepsilon_3 + x_2^2 x_4 \varepsilon_3 + x_2^3 \varepsilon_4$ and $S'_{14} = S_{14}$.
5) Append $g_8 = S_{14}$ to $\mathcal{G}$.
6) Choose $v = v_5$ and let $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NF}_{\sigma,\mathcal{G}}(v) = 0$. (Notice that $v_5 = -g_7 - g_8$.)
2) Let $d = \binom{7}{15}$, $B_d = \{(3,4)\}$, $B = \emptyset$, $\mathcal{W}_d = (v_6)$, and $\mathcal{W} = \emptyset$.
3) Choose $(3,4) \in B_d$ and let $B_d = \emptyset$.
4) Compute $S_{34} = x_3^2 v_3 - x_2 x_4 v_4 = x_3^3 \varepsilon_3 - x_2 x_4^2 \varepsilon_3 + x_1 x_3^2 \varepsilon_4 - x_2^2 x_4 \varepsilon_4$ and $S'_{34} = S_{34}$.

5) Append $g_9 = S'_{34}$ to $\mathcal{G}$.
6) Choose $v = v_6$ and let $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NF}_{\sigma,\mathcal{G}}(v) = 0$. (Notice that $v = g_9$.)

Now we have finished degree $d_{\max} = \binom{7}{15}$ and we may stop the computation. Altogether, we have computed a minimal homogeneous presentation

$$F_2 \xrightarrow{\psi} F_1 \xrightarrow{\varphi} M \longrightarrow 0$$

of M, where $F_1 = P\big(-\binom{3}{4}\big) \oplus P\big(-\binom{4}{3}\big) \oplus P\big(-\binom{4}{6}\big) \oplus P\big(-\binom{4}{9}\big)$ and where $F_2 = P\big(-\binom{5}{6}\big) \oplus P\big(-\binom{5}{7}\big) \oplus P\big(-\binom{5}{9}\big) \oplus P\big(-\binom{5}{10}\big)$. The map $\varphi : F_1 \longrightarrow F_0$ is defined by the homogeneous matrix (f_1, f_2, f_3, f_4), and the map ψ is defined by the homogeneous matrix

$$\begin{pmatrix} x_2^2 & -x_1x_3 & -x_2x_4 & -x_3^2 \\ -x_3 & x_4 & 0 & 0 \\ x_1 & -x_2 & x_3 & x_4 \\ 0 & 0 & x_1 & x_2 \end{pmatrix}$$

Thus the minimal homogeneous presentation of I is $F'_2 \xrightarrow{\psi'} F'_1 \xrightarrow{\varphi'} I \longrightarrow 0$ where we have $F'_1 = P\big(-\binom{2}{4}\big) \oplus P\big(-\binom{3}{3}\big) \oplus P\big(-\binom{3}{6}\big) \oplus P\big(-\binom{3}{9}\big)$ and where $F'_2 = P\big(-\binom{4}{6}\big) \oplus P\big(-\binom{4}{7}\big) \oplus P\big(-\binom{4}{9}\big) \oplus P\big(-\binom{4}{10}\big)$. The maps φ', ψ' are defined by the same matrices.

Sometimes the vertical strategy is not the most efficient way to compute a minimal homogeneous presentation. For instance, suppose that we have some information about the highest degrees occurring in the degree pair of M. In this case, it is desirable to compute the minimal generators and their minimal syzygies degree by degree, and to truncate the computation at the appropriate degree. A method which proceeds degree by degree and determines both the minimal generators and their minimal syzygies simultaneously for each degree is called a **horizontal strategy**. Our next theorem shows how we can implement it effectively.

To ease the notation, we shall again resort to the convention $\mathrm{LT}_\sigma(g_i) = t_i e_{\gamma_i}$ with $t_i \in \mathbb{T}^n$ and $\gamma_i \in \{1, \ldots, r\}$. Moreover, we let $\mathrm{LT}_\sigma(h_j) = \tilde{t}_j e_{\eta_j}$ with $\tilde{t}_j \in \mathbb{T}^n$ and $\eta_j \in \{1, \ldots, \mu\}$.

Theorem 4.7.29. (Computing Minimal Presentations Horizontally) *Let M be a graded submodule of a graded free P-module $F_0 = \bigoplus_{i=1}^r P(-d_{0i})$, where $d_{0i} >_{\mathtt{Lex}} 0$ for $i = 1, \ldots, r$, and let $\mathcal{V} = (v_1, \ldots, v_s)$ be a deg-ordered tuple of non-zero homogeneous vectors which generate M. Consider the following instructions.*

1) *Choose a term ordering σ on the monoid $\mathbb{T}^n(e_1, \ldots, e_r)$. Let $B = \emptyset$, $B' = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, $s' = 0$, $\mathcal{G}_{\min} = \emptyset$, $\mu = 0$, $\mathcal{S} = \emptyset$, $s'' = 0$, and $\mathcal{S}_{\min} = \emptyset$.*

2) Let d be the smallest degree with respect to Lex *of an element in $B \cup B'$ or in $\mathcal{W}$. Form the subset B_d of B, the subset B'_d of B', the subtuple $\mathcal{W}_d$ of $\mathcal{W}$, and delete their entries from B, B', and $\mathcal{W}$, respectively.*

3) If $B'_d = \emptyset$, continue with step 6). Otherwise, choose a pair $(i,j) \in B'_d$ and remove it from B'_d.

4) Compute the S-vector of h_i and h_j and call it S_{ij}. Then compute the normal remainder $S'_{ij} = \mathrm{NR}_{\sigma,\mathcal{S}}(S_{ij})$. If $S'_{ij} = 0$, continue with step 3).

5) Increase s'' by one, append $h_{s''} = S'_{ij}$ to the tuple $\mathcal{S}$, append the set $\{(i,s'') \mid 1 \le i < s'',\ \eta_i = \eta_{s''}\}$ to B', and continue with step 3).

6) If $B_d = \emptyset$, continue with step 10). Otherwise, choose a pair $(i,j) \in B_d$ and remove it from B_d.

7) Compute the S-vector of g_i and g_j and call it S_{ij}. Then compute the normal remainder $S'_{ij} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{ij})$. If S'_{ij} involves one of the indeterminates $e_1, \ldots, e_r$ then increase s' by one, append $g_{s'} = S'_{ij}$ to $\mathcal{G}$, append $\{(i,s') \mid 1 \le i < s', \gamma_i = \gamma_{s'}\}$ to B, and continue with step 6).

8) Compute the normal remainder $S''_{ij} = \mathrm{NR}_{\sigma,\mathcal{S}}(S'_{ij})$. If $S''_{ij} = 0$, continue with step 6).

9) Increase s'' by one. Append $h_{s''} = S''_{ij}$ to the tuples $\mathcal{S}$ and $\mathcal{S}_{\min}$. Append $\{(i,s'') \mid 1 \le i < s'',\ \eta_i = \eta_{s''}\}$ to B'. Continue with step 6).

10) If $\mathcal{W}_d = \emptyset$, continue with step 13). Otherwise, choose a vector $v \in \mathcal{W}_d$ and remove it from $\mathcal{W}_d$.

11) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v)$ and $\bar{v} = v'(x_1, \ldots, x_n, e_1, \ldots, e_r, 0, \ldots, 0)$. If $\bar{v} = 0$, continue with step 10).

12) Increase s' and μ by one. Adjoin a new indeterminate ε_μ to $\overline{P}$ and extend the grading to this new ring by defining $\deg_{\overline{W}}(\varepsilon_\mu) = \deg_{\overline{W}}(v')$. Extend the term ordering σ to the new ring in such a way that the extension is an elimination ordering for $\{e_1, \ldots, e_r\}$. Append $g_{s'} = \bar{v} - \varepsilon_\mu$ to the tuple $\mathcal{G}$ and $\bar{v}$ to $\mathcal{G}_{\min}$. Append $\{(i,s') \mid 1 \le i < s',\ \gamma_i = \gamma_{s'}\}$ to B. Continue with step 10).

13) If $B = B' = \emptyset$ and $\mathcal{W} = \emptyset$, return the pair $(\mathcal{G}_{\min}, \mathcal{S}_{\min})$ and stop. Otherwise, continue with step 2).

This is an algorithm which computes a pair $(\mathcal{G}_{\min}, \mathcal{S}_{\min})$ where $\mathcal{G}_{\min}$ is a deg-ordered tuple of homogeneous vectors in F_0 which generate M minimally, and where $\mathcal{S}_{\min}$ is a deg-ordered tuple of homogeneous vectors in $\bigoplus_{i=1}^{\mu} P(-d_{1i})$ which generate $\mathrm{Syz}_P(\mathcal{G}_{\min})$ minimally. Here μ is the number of elements in $\mathcal{G}_{\min}$ and d_{1i} is the degree of the i^{th} element in $\mathcal{G}_{\min}$ for $i = 1, \ldots, \mu$.

Proof. First we show finiteness. The procedure terminates when B, B', and $\mathcal{W}$ are empty. Only B and B' are enlarged during the computation. Each time the loop in steps 3)–5) is executed, one pair is removed from B_d (and thus from B). Similarly, performing the loops in steps 6)–9) and 10)–12) removes one element from B_d and $\mathcal{W}_d$, respectively. Hence it suffices to show that B and B' are enlarged only finitely many times.

The set B is enlarged in steps 7) and 12) only if an element $g_{s'}$ is appended to $\mathcal{G}$ whose normal remainder with respect to the previous elements

of $\mathcal{G}$ is non-zero. In this case, $\langle \mathrm{LT}_\sigma(\mathcal{G})\rangle$ is enlarged, and this can happen only finitely many times. Similarly, the set B' is enlarged in steps 5) and 9) only if an element $h_{s''}$ is appended to S which has a new leading term. Again this can happen only finitely many times.

Now we prove correctness. We consider the entire computation as a computation in $\widetilde{P} = K[x_1, \ldots, x_n, e_1, \ldots, e_r, \varepsilon_1, \ldots, \varepsilon_\mu]$. We claim that the elements of $\mathcal{W}$, $\mathcal{G}$, $\mathcal{G}_{\min}$, $\mathcal{S}$, and $\mathcal{S}_{\min}$ are always of the form $f_1e_1 + \cdots + f_re_r + \tilde{f}_1\varepsilon_1 + \cdots + \tilde{f}_\mu\varepsilon_\mu$ with $f_i, \tilde{f}_j \in P$. This is clearly true at the outset. By the manner in which B and B' are enlarged in steps 5), 7), 9), and 12), the new S-vectors continue to have this shape. Furthermore, reducing one such vector using another one preserves the shape. Hence the elements of $\mathcal{G}$ and $\mathcal{S}$ have the desired form. Clearly the construction of $\mathcal{G}_{\min}$ in step 12) and $\mathcal{S}_{\min}$ in step 9) also preserves the given shape.

By induction on s'' it follows that elements $h_{s''}$ which are appended to $\mathcal{S}$ in step 5) and 9) do not involve the indeterminates $\{e_1, \ldots, e_r\}$. In particular, their leading position is an element $\eta_j \in \{1, \ldots, \mu\}$.

If we set $\varepsilon_1 \mapsto 0$, $\ldots$, $\varepsilon_\mu \mapsto 0$ in the entire algorithm and ignore the instructions concerning $\mathcal{S}$ and $\mathcal{S}_{\min}$, we see that we are applying Buchberger's Algorithm with Minimalization 4.6.3 to the tuple $\mathcal{V}$. Therefore the tuple $\overline{\mathcal{G}} = (\bar{g}_1, \ldots, \bar{g}_{s'})$ where $\bar{g}_i = g_i(x_1, \ldots, x_n, e_1, \ldots, e_r, 0, \ldots, 0)$ is a σ-Gröbner basis of M and $\mathcal{G}_{\min}$ is a subtuple of $\overline{\mathcal{G}}$ whose elements are a minimal system of generators of M.

Next we let $\mathcal{G}_{\min} = (\tilde{g}_1, \ldots, \tilde{g}_\mu)$. We claim that the elements of $\mathcal{G}$ map to zero under the homomorphism defined by $\varepsilon_1 \mapsto \tilde{g}_1$, $\ldots$, $\varepsilon_\mu \mapsto \tilde{g}_\mu$. This follows by induction on s' because in step 5) an element of $\langle g_1, \ldots, g_{s'-1}\rangle$ is appended to $\mathcal{G}$ and in step 8) we have

$$g_{s'}(x_1, \ldots, x_n, e_1, \ldots, e_r, \tilde{g}_1, \ldots, \tilde{g}_{\mu-1}) = \bar{v} - g_\mu = 0$$

Hence the elements of $\mathcal{G}$ are contained in the ideal $(\tilde{g}_1 - \varepsilon_1, \ldots, \tilde{g}_\mu - \varepsilon_\mu)$ of $\overline{P}$. Since we know already that $\mathcal{G}_{\min}$ is a minimal system of generators of M, it follows that $\tilde{I}_M = (\tilde{g}_1 - \varepsilon_1, \ldots, \tilde{g}_\mu - \varepsilon_\mu) + \widetilde{E}$ is the ideal of a homogeneous presentation of M. Therefore, by Proposition 4.7.23, it suffices to prove that $\mathcal{S} \cup \{\varepsilon_i\varepsilon_j \mid i, j = 1, \ldots, \mu\}$ is a σ-Gröbner basis of $\tilde{I}_M \cap P[\varepsilon_1, \ldots, \varepsilon_\mu]$ and $\mathcal{S}_{\min} \cup \{\varepsilon_i\varepsilon_j \mid i, j = 1, \ldots, \mu\}$ is a minimal set of generators of this ideal.

Since σ is an elimination ordering for $\{e_1, \ldots, e_r\}$, steps 3), 4), 5), 8), and 9) correspond to the application of Buchberger's Algorithm with Minimalization 4.6.3 to this ideal. Hence the claim follows from Propositions 4.7.16.a and 4.7.19.a,b. Altogether, we have shown that $\mathcal{G}_{\min}$ is a minimal system of generators of M and $\mathcal{S}_{\min}$ is a minimal system of generators of $\mathrm{Syz}_P(\mathcal{G}_{\min})$. □

Let us add a few remarks about the inner workings of this algorithm.

Remark 4.7.30. Assume that we are in the setting of Theorems 4.7.26 and 4.7.29.

a) If we view the vertical and the horizontal strategy for computing a minimal homogeneous presentation as algorithms in $\overline{P}$, they are nothing but two concrete versions of the same general algorithm, namely the Homogeneous Buchberger Algorithm 4.5.5. The difference lies in the particular strategies for choosing the next pair to work on, and that we do not have to consider critical pairs (i, s') with $\gamma_i \neq \gamma_{s'}$ because $e_i\, e_{s'}$ maps to zero in the idealization of M.

b) The proof of Theorem 4.7.29 shows that when the algorithm stops the tuple $\overline{\mathcal{G}} = (\bar{g}_1, \ldots, \bar{g}_{s'})$ where $\bar{g}_i = g_i(x_1, \ldots, x_n, e_1, \ldots, e_r, 0, \ldots, 0)$ is a σ-Gröbner basis of M, and the tuple $\mathcal{S}$ is a σ-Gröbner basis of the module $\mathrm{Syz}_P(\mathcal{G}_{\min})$

c) Note that one can choose the term ordering on $\mathbb{T}^n\langle\varepsilon_1, \ldots, \varepsilon_\mu\rangle$ freely, as long as it extends σ. Hence the algorithm can be used to compute a Gröbner basis of the syzygy module $\mathrm{Syz}(\mathcal{G}_{\min})$ with respect to an arbitrary term ordering.

Example 4.7.31. The sheer length of this section forces us to ask you, dear reader, to redo Example 4.7.28 with the horizontal strategy on your own. In this particular case, the vertical strategy is superior, because it avoids the computation of the critical pairs among syzygies, as we noticed before.

Exercise 1. Let K be a field, and let $P = K[x_1, x_2, x_3, x_4]$ be graded by $W = \left(\begin{smallmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \end{smallmatrix}\right)$.

a) Show that $\mathcal{M} = \left(\begin{smallmatrix} x_2 & x_3 & x_4 \\ x_2 & x_1 & x_2 \end{smallmatrix}\right)$ is not a homogeneous matrix.

b) Find all matrices $W \in \mathrm{Mat}_{2,4}(\mathbb{Z})$ for which $\mathcal{M}$ is homogeneous with respect to the grading given by W.

Exercise 2. Let $P = \mathbb{Q}[x, y, z]$ be standard graded, let $v_1 = x^2 - xy$, $v_2 = xy^2 - y^2z$, and $v_3 = x^3 + y^3 + y^2z$.

a) Show that $\mathcal{V} = (v_1, v_2, v_3)$ minimally generates the homogeneous ideal $I = (v_1, v_2, v_3)$.

b) Let $v_1' = xy - x^2$, $v_2' = y^2z - x^2y$, and $v_3' = x^2y + xy^2 + y^3$. Prove that $\mathcal{V}' = (v_1', v_2', v_3')$ is another homogeneous minimal system of generators of I.

c) Find homogeneous matrices $\mathcal{A}$, $\mathcal{B}$ for which $\mathcal{V}' = \mathcal{V}\,\mathcal{A}$ and $\mathcal{V} = \mathcal{V}'\,\mathcal{B}$.

d) Compute $\det(\mathcal{A})$, $\det(\mathcal{B})$, and $\mathcal{I}_3 - \mathcal{A}\,\mathcal{B}$.

Exercise 3. Let $P = \mathbb{Q}[x_1, \ldots, x_n]$ be standard graded.

a) Write a CoCoA function which computes the degree sequence of a monomial ideal in P.

b) Find the maximum number of elements in a minimal set of generators of a monomial ideal in the ring $P = \mathbb{Q}[x, y]$ whose degree sequence starts with 2.
c) More generally, given $d \in \mathbb{N}$, find the maximum number of elements in a minimal set of generators of a monomial ideal in the ring $P = \mathbb{Q}[x, y]$ whose degree sequence starts with d.

Exercise 4. Let R be a ring, and let $r \geq 1$. Given a square matrix $\mathcal{M} = (a_{ij}) \in \mathrm{Mat}_r(R)$, define its **adjoint matrix** $\mathcal{M}^{\mathrm{adj}} = (b_{ij})^{\mathrm{tr}}$ by $b_{ij} = (-1)^{i+j} \det(\mathcal{M}_{ij})$, where $\mathcal{M}_{ij}$ is obtained from $\mathcal{M}$ by deleting the i^{th} row and the j^{th} column.

a) Show that $\mathcal{M}\,\mathcal{M}^{\mathrm{adj}} = \det(\mathcal{M})\,\mathcal{I}_r$.
Hint: For $i \neq j$, consider the matrix $\mathcal{M}'$ obtained by replacing the i^{th} row of $\mathcal{M}$ by the j^{th} row.
b) Conclude that if vectors $v_1, \ldots, v_s \in R^r$ satisfy $(v_1, \ldots, v_s) \cdot \mathcal{M} = 0$, then $\det(\mathcal{M}) \cdot v_i = 0$ for $i = 1, \ldots, s$. This result is sometimes called **Dedekind's Lemma**.
c) Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let M be a finitely generated graded P-module, and let $\mathcal{V} = (v_1, \ldots, v_s)$ and $\mathcal{V}' = (v'_1, \ldots, v'_s)$ be two homogeneous systems of generators of M. Given matrices $\mathcal{A}$, $\mathcal{B}$ such that $\mathcal{V}' = \mathcal{V}\,\mathcal{A}$ and $\mathcal{V} = \mathcal{V}'\,\mathcal{B}$, prove that $\det(\mathcal{I}_s - \mathcal{A}\,\mathcal{B}) \cdot M = 0$.
d) Find an example where $\mathcal{V}, \mathcal{V}'$ are minimal and the matrices $\mathcal{A}$, $\mathcal{B}$ above satisfy $\mathcal{A}\,\mathcal{B} \neq \mathcal{I}_s$.

Exercise 5. In the setting of Proposition 4.7.14, find all graded submodules $M \subseteq F_0$ for which the ideal I_M is a prime ideal.

Exercise 6. Suppose we are in the setting of Proposition 4.7.14.

a) Exhibit an ideal in $\overline{P}$ which contains $\mathfrak{e}$ but is not of the form I_M for any graded submodule M of F_0.
b) Characterize the ideals of $\overline{P}$ which are of the form I_M for some graded submodule M of F_0.

Exercise 7. Let $P = K[x_1, x_2, x_3, x_4]$ be standard graded, and let N be the graded P-submodule of $P(-2)^2 \oplus P(-1)^2$ generated by the vectors $(0, x_1, x_1x_2 - x_4^2, x_1x_2 + x_4^2)$, $(x_2, 0, x_1x_3, -x_1x_3)$, $(0, 1, x_2, x_2)$, and $(0, 0, 1, -1))$. Using the algorithm of Proposition 4.7.24.b, compute a minimal homogeneous presentation of $M = (P(-2)^2 \oplus P(-1)^2)/N$.

Exercise 8. Let $P = \mathbb{Q}[x, y, z]$ be standard graded, and let I be the ideal $(x^2,\ xy+xz,\ y^2)$ in P. Compute a minimal homogeneous presentation of I using both the vertical and the horizontal strategy. Compare the efficiency of both methods.

Exercise 9. Work out Example 4.7.31!

Tutorial 60: Computing Some Idealizations

idealization, idealisation (noun)
1. the representation of something as ideal.
2. a conception of something that dwells on its advantages and ignores its deficiencies.
3. a general theoretical account of natural phenomena that ignores features that are difficult to accommodate within a theory.
(English dictionary)

In Tutorial 34 we studied elimination of module components. The idea we had in mind was to consider the canonical basis vectors $e_1, \ldots, e_r$ as "indeterminates". Using the idealization technique of Subsection B, we can now realize this idea and dwell on its advantages.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $d_{0i} \in \mathbb{Z}^m$ for $i = 1, \ldots, r$, and consider the graded free P-module $F_0 = \bigoplus_{i=1}^{r} P(-d_{0i})$. The canonical basis of F_0 is denoted by $\{e_1, \ldots, e_r\}$. By applying a suitable shift, we may assume that $d_{0i} >_{\mathtt{Lex}} 0$ for $i = 1, \ldots r$ (see Remark 4.7.21).

According to Proposition 4.7.14.a, the polynomial ring $\overline{P} = P[e_1, \ldots, e_r]$ represents the idealization $\overline{P}/E$ of F_0. We equip $\overline{P}$ with the grading given by $\overline{W} = (W \mid d_{01} \cdots d_{0r})$ and identify the elements of F_0 with their canonical images in $\overline{P}$. Let M be graded submodule of F_0, and let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of homogeneous vectors which generate M.

a) Let $\varepsilon_1, \ldots, \varepsilon_s$ be further indeterminates. Equip the polynomial ring $\overline{P}[\varepsilon_1, \ldots, \varepsilon_s]$ with the grading obtained by extending the grading by $\overline{W}$ using $\deg_{\overline{W}}(\varepsilon_i) = \deg_W(g_i)$ for $i = 1, \ldots, s$. Prove that the ideal $(g_1 - \varepsilon_1, \ldots, g_s - \varepsilon_s) \cap P[\varepsilon_1, \ldots, \varepsilon_s]$ is the ideal of the module $\mathrm{Syz}_P(\mathcal{G})$.
b) Write a CoCoA function `IdealSyz(...)` which implements the method for computing $\mathrm{Syz}_P(\mathcal{G})$ you found in a). Apply your function to the homogenizations of the modules given in Tutorial 34.d with respect to the standard grading and suitable shifts.
c) Let N be another graded P-submodule of F_0, and let $\mathcal{H} = (h_1, \ldots, h_t)$ be homogeneous system of generators of N. Introduce further indeterminates $\varepsilon_1, \ldots, \varepsilon_r$ and equip the polynomial ring $\overline{P}[\varepsilon_1, \ldots, \varepsilon_r]$ with the grading obtained by extending the grading by $\overline{W}$ with $\deg_{\overline{W}}(\varepsilon_i) = d_{0i}$ for $i = 1, \ldots, r$. Moreover, let h_i' be the polynomial obtained by substituting $e_1 \mapsto \varepsilon_1, \ldots, e_r \mapsto \varepsilon_r$ in h_i. Prove that the ideal $(h_1 - h_1', \ldots, h_s - h_s') \cap P[\varepsilon_1, \ldots, \varepsilon_r]$ is the ideal of the module $M \cap N$.
d) Write a CoCoA function `IdealIntersect(...)` which implements the method for computing $M \cap N$ you found in c). Apply your function to the homogenizations of the modules given in Tutorial 30.b with respect to the standard grading and suitable shifts.
e) Let $v \in F_0 \setminus \{0\}$ be a homogeneous vector. Introduce a further indeterminate ε and equip the polynomial ring $\overline{P}[\varepsilon]$ with the grading obtained

by extending the grading by $\overline{W}$ with $\deg_{\overline{W}}(\varepsilon) = \deg_W(v)$. Prove that the ideal $(g_1, \ldots, g_s, v-\varepsilon) \cap P[\varepsilon]$ is the ideal of the colon ideal $M :_P \langle v \rangle$.

f) Write a CoCoA function `IdealColon(...)` which implements the method for computing $M \cap N$ you found in e). Apply your function to the homogenizations of the modules and vectors given in Tutorial 34.h with respect to the standard grading and suitable shifts.

g) As the last job, we ask you to generalize Propositions 4.7.14 and 4.7.16 to the non-graded case, and then to do as many as you can of the preceding items in this situation.

Tutorial 61: Computing Some Minimal Presentations

The 10 computational commandments:
1. Always use the binary system.
10. Never use the symbol 2.
(Anonymous)

What would a section like this one be without a tutorial which requires you to do some actual computer implementations? Surely, your fingers are already itching to follow this computational commandment and start hitting the keys. Plenty of competing algorithms and strategies require intense practical testing to reveal their respective merits.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by the matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $d_{01}, \ldots, d_{0r} \in \mathbb{Z}^m$, let $F_0 = \bigoplus_{i=1}^r P(-d_{0i})$, and let M be a graded P-submodule of F_0 which is generated by a deg-ordered tuple of non-zero vectors $\mathcal{V} = (v_1, \ldots, v_s)$.

a) Write a CoCoA function `MinPres1(...)` which takes $\mathcal{V}$ and uses the built-in procedures of CoCoA to compute a pair of homogeneous matrices $(\mathcal{V}_{\min}, \mathcal{S}_{\min})$ which give a minimal homogeneous presentation

$$F_2 \xrightarrow{\psi} F_1 \xrightarrow{\varphi} M \longrightarrow 0$$

of M, where φ is given by $\mathcal{V}_{\min}$ and ψ is given by $\mathcal{S}_{\min}$. (In the following, you can use this function to check the correctness of your other programs.) *Hint:* You may want to pass to the idealization of M and use Proposition 4.7.23.

b) Apply your function `MinPres1(...)` to compute a minimal homogeneous presentation of the following ideals and modules.

1) $M_1 = (x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_2x_4, x_3x_4)$ in $\mathbb{Q}[x_1, x_2, x_3, x_4]$ using the standard grading
2) $M_2 = \langle (x_1+x_2, x_3-x_4), (x_1^2-x_2^2, x_3^2+x_4^2), (x_1x_2x_3+x_4^3, 2x_1x_2x_4-x_3^3) \rangle$ in $\mathbb{Q}[x_1, x_2, x_3, x_4]^2$ using the standard grading
3) $M_3 = (x_1x_4 - x_2x_3,\ x_2x_4^2 - x_3^3,\ x_1x_3^2 - x_2^2x_4,\ x_1^2x_3 - x_2^3)$ in the ring $\mathbb{Q}[x_1, x_2, x_3, x_4]$ graded by $\left(\begin{smallmatrix} 5 & 4 & 2 & 1 \\ 1 & 1 & 1 & 1 \end{smallmatrix}\right)$

4) $M_4 = (x_1x_4 - x_2x_3,\ x_1x_5 - x_2x_4,\ x_1x_6 - x_2x_5,\ x_3x_5 - x_4^2,\ x_3x_6 - x_4x_5,\ x_4x_6 - x_5^2)$ in $\mathbb{Q}[x_1, \ldots, x_6]$ graded by $\left(\begin{smallmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 6 \end{smallmatrix}\right)$
5) $M_5 = \langle x_ie_j - x_je_i \mid 1 \leq i < j \leq 6 \rangle$ in $\bigoplus_{i=1}^{6} \mathbb{Q}[x_1, \ldots, x_6](-i)$ graded by $(1\ 2\ \cdots\ 6)$

c) Write a CoCoA function `MinPres2(...)` which performs the same task as `MinPres1(...)` but uses the algorithm of Remark 4.7.25. If possible, use the function `Min2(...)` you wrote in Tutorial 58.c in steps 1) and 3).
d) Apply your function `MinPres2(...)` to the examples in b). Compare the results and the timings with those of `MinPres1(...)`. For this purpose, write a CoCoA function `IsIsomPres(...)` which checks whether two minimal homogeneous presentations of a module are isomorphic. (*Hint:* Use Proposition 4.7.10.)
e) Implement a CoCoA function `MinPresVert(...)` which computes a minimal homogeneous presentation of M using the vertical strategy of Theorem 4.7.26. Apply it to the examples given in b) and compare it to `MinPres2(...)` by counting the number of calls to the normal remainder function. Which strategy is more efficient and why?
f) Let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r \rangle$. Consider the following sequence of instructions.
   1) Let $\mathcal{A} = \emptyset$, $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, $s' = 0$, $\mathcal{G}_{\min} = \emptyset$, and let $\mathcal{S} = \emptyset$.
   2) Let d be the smallest degree with respect to `Lex` of an element in B or in $\mathcal{W}$. Form the subset B_d and the subtuple $\mathcal{W}_d$, and delete their entries from B and $\mathcal{W}$, respectively.
   3) If $B_d = \emptyset$, continue with step 7). Otherwise, chose a pair $(i, j) \in B_d$ and remove it from B_d.
   4) Compute the S-vector S_{ij} of g_i and g_j. Then apply the Division Algorithm 1.6.4 to compute a homogeneous representation $S_{ij} = q_1g_1 + \cdots + q_{s'}g_{s'} + p$, where $q_1, \ldots, q_{s'} \in P$ and $p \in F_0$ satisfy the conditions of Theorem 1.6.4.
   5) If $p = 0$, append the column vector $\sigma_{ij} - \sum_{k=1}^{s'} q_ke_k$ to the matrix $\mathcal{S}$ and continue with 3).
   6) Increase s' by one, append $g_{s'} = p$ to the tuple $\mathcal{G}$, append the set $\{(i, s') \mid 1 \leq i < s',\ \gamma_i = \gamma_{s'}\}$ to B, and append the column vector
   $$\tfrac{1}{c_i}\, t_{ij}a_i - \tfrac{1}{c_j}\, t_{ji}a_j - q_1a_1 - \cdots - q_{s'-1}a_{s'-1}$$
   to the matrix $\mathcal{A}$, where $a_1, \ldots, a_{s'-1}$ denote the previous columns of $\mathcal{A}$. Continue with step 3).
   7) If $\mathcal{W}_d = \emptyset$, continue with step 10). Otherwise, choose a vector $v \in \mathcal{W}_d$ and remove it from $\mathcal{W}_d$.
   8) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v)$. If $v' = 0$, continue with step 7).
   9) Increase s' by one, append $g_{s'} = v'$ to the tuple $\mathcal{G}$ and to the tuple $\mathcal{G}_{\min}$, append a row of zeros to $\mathcal{S}$ and $\mathcal{A}$, append the column vector $(0, \ldots, 0, 1)^{\mathrm{tr}}$ to $\mathcal{A}$, and append $\{(i, s') \mid 1 \leq i < s',\ \gamma_i = \gamma_{s'}\}$ to the set B. Continue with step 7).

10) If $B = \emptyset$ and $\mathcal{W} = \emptyset$, then apply the Buchberger Algorithm with Minimalization 4.6.3 to the module generated by the column vectors of $\mathcal{A}\mathcal{S}$ and obtain a subtuple $\mathcal{S}_{\min}$ of $\mathcal{A}\mathcal{S}$ which minimally generates that module. Otherwise, continue with step 2).
11) Return the pair $(\mathcal{G}_{\min}, \mathcal{S}_{\min})$ and stop.

Prove that this is an algorithm which returns a pair of deg-ordered tuples of homogeneous vectors $(\mathcal{G}_{\min}, \mathcal{S}_{\min})$ where $\mathcal{G}_{\min}$ minimally generates M and $\mathcal{S}_{\min}$ is a homogeneous minimal system of generators of $\mathrm{Syz}_P(\mathcal{G}_{\min})$.

g) Write a CoCoA function `MinPres3(...)` which implements the preceding algorithm. Try your function in the cases given in b) and compare its efficiency to the earlier ones.

h) Finally, implement the horizontal strategy for computing minimal homogeneous presentations explained in Theorem 4.7.29 in a CoCoA function `HorMinPres(...)`. Apply this function again in the cases of b) and check its correctness using `IsIsomPres(...)`.

i) Compare the efficiency of the functions you wrote by constructing a table which contains the timings, the number of calls to `NR(...)`, and the number of critical pairs which had to be treated for the examples given in b). Try to explain the results.

4.8 Minimal Graded Free Resolutions

You know, we just used so many metaphors
I forgot what the hell we were talking about.
(From "The Odd Couple II")

The closing section of this chapter is both its climax and its time of fruition. After extensive preparations in the previous section, we are ready to harvest the fruits of our labour and compute minimal graded free resolutions. Given a finitely generated graded module M over a positively graded polynomial ring $P = K[x_1, \ldots, x_n]$, we defined a finite minimal graded free resolution of M to be an exact sequence

$$0 \longrightarrow F_\ell \xrightarrow{\varphi_\ell} F_{\ell-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

where $F_0, \ldots, F_\ell$ are finitely generated graded free P-modules and where for every $i \in \{1, \ldots, \ell\}$ the homogeneous homomorphism φ_i maps the canonical basis of F_i to a minimal homogeneous system of generators of $\mathrm{Ker}(\varphi_{i-1})$. With the support of Section 4.7, we shall tackle the tasks ahead in two phases: first we examine the existence and uniqueness of such resolutions, and then we conjure up some algorithms to compute them.

The basic existence result for graded free resolutions is the graded version of Hilbert's Syzygy Theorem 4.8.4: for a proof, we simply follow in the wake of Tutorial 29. However, the resolutions produced in this way are not minimal by a long shot. Far from this being our undoing, we save ourselves by fabricating Theorem 4.8.6, a tool for minimalizing non-minimal resolutions. By applying this universal remedy time and time again, we not only get out of a tight spot, but we actually find an effective method for computing minimal graded free resolutions. But we're getting ahead of ourselves! If we want to develop meaningful algorithms, the objects of our striving had better be unique – or, at least, essentially unique. For want of a better idea, we look over the preceding section and rediscover Proposition 4.7.10, a variant of which enables us to prove that the minimal graded free resolution of M is uniquely determined up to a homogeneous isomorphism. Then things are really looking up, and we witness the debut of the graded Betti numbers, a whole array of important invariants.

In the second part of this section we exhibit concrete algorithms for computing minimal graded free resolutions and graded Betti numbers. One method for treating this slippery topic could be to explain in every last detail the use of the built-in CoCoA command `Res(...)` and leave it at that. Instead, we present and explain ... not one ... not two ... but actually three separate algorithms. The first one is obtained by overhauling the vertical strategy of Theorem 4.7.26 and looping a loop around it. Though simple and straightforward to implement, this vertical strategy for computing resolutions is sometimes not optimal.

The second algorithm we present has its roots in the existence proof we sketched above. In essence, we use the pruning technique of Theorem 4.8.6

and apply it to the non-minimal resolution constructed during the proof of Theorem 4.8.4. As we shall see, it all comes down to identifying a minimal system of generators $\mathcal{G}_{\min}$ inside a homogeneous Gröbner basis $\mathcal{G}$ and expressing $\mathcal{G}$ in terms of $\mathcal{G}_{\min}$. Since we have already cooked from several recipes for doing this, we could start feasting. However, we still have one ace up our sleeves. By building on the horizontal strategy for computing minimal homogeneous presentations, we can assemble a very compact algorithm which computes a minimal graded free resolution degree by degree. The formulation of this algorithm in Theorem 4.8.16 requires merely seven instructions. Brevity is the soul of wit, and hand in hand with it one can achieve a very satisfactory efficiency.

Free resolutions do not provide light reading. They wreak havoc on your mind. Although we have steadfastly stayed the course and proffer a generous sprinkling of examples, it is easy to get lost in a muddled computation. But in the end, we hope that you will know exactly what we were talking about.

4.8.A Existence and Uniqueness of Minimal Free Resolutions

This subsection provides the mathematical background for dealing with minimal graded free resolutions. Our first task is to show that finite graded free resolutions do indeed exist. The emphasis here is on the word finite, since the construction of a free resolution is straightforward.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by the matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let M be a non-zero finitely generated graded P-module.

Definition 4.8.1. A **graded free resolution** of M is an exact sequence of the form

$$\cdots \xrightarrow{\varphi_3} F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

where $F_0, F_1, \ldots$ are finitely generated graded free P-modules. If there exists a number $\ell \in \mathbb{N}$ such that $F_\ell \neq 0$ and $F_i = 0$ for $i > \ell$, we say that it is a **finite graded free resolution** of M of **length** ℓ.

Clearly, the module M is a graded free P-module if and only if it has a graded free resolution of length 0. Is there always a finite graded free resolution of M? A quick reply would be to simply state that an easy generalization of Tutorial 29 yields an affirmative answer to this question. However, even if we risk being criticized for filling too many pages, we prefer to give the full proofs. If you were diligent and worked out the details of Tutorial 29, it will help you to digest everything here with little effort.

In the following, we assume that M is generated by a tuple of non-zero homogeneous elements $\mathcal{G} = (g_1, \ldots, g_r)$. For $i = 1, \ldots, r$, let $d_{0i} = \deg_W(g_i)$. The canonical basis of the graded free P-module $F_0 = \bigoplus_{i=1}^{r} P(-d_{0i})$ is denoted by $\{e_1, \ldots, e_r\}$. Thus the P-linear map $\varphi_0 : F_0 \longrightarrow M$ sending

$e_i \mapsto g_i$ for $i = 1, \ldots, r$ is homogeneous and surjective. Our first result enables us to recognize a graded free module by looking at a Gröbner basis of the syzygy module of a homogeneous tuple of generators.

Proposition 4.8.2. *Let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ and $\mathcal{S} = (v_1, \ldots, v_s)$ be a σ-Gröbner basis of $\mathrm{Syz}_P(\mathcal{G})$. If $\mathrm{LT}_\sigma(v_i) \in \{e_1, \ldots, e_r\}$ for $i = 1, \ldots, s$ then M is a graded free P-module.*

Proof. After possibly deleting some of the syzygies in $\mathcal{S}$, we may assume that $\mathrm{LT}_\sigma(v_i) \neq \mathrm{LT}_\sigma(v_j)$ for $i \neq j$. Then we use the syzygies in $\mathcal{S}$ to delete the corresponding elements in the tuple $\mathcal{G}$ as described in Proposition 4.7.24.b. The remaining elements of $\mathcal{G}$ still generate M. There are no syzygies among them, since otherwise the leading term of such a syzygy would be a multiple of an element of $\mathrm{LT}_\sigma(\mathcal{S})$, but the syzygy has a zero in that position. Therefore the remaining elements of $\mathcal{G}$ are a homogeneous basis of the P-module M. □

The following lemma is the key to the existence proof for finite graded free resolutions.

Lemma 4.8.3. *Let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$, let N be a graded P-submodule of F_0, and let $\mathcal{V} = (v_1, \ldots, v_s)$ be a tuple of homogeneous vectors which form a σ-Gröbner basis of N. Furthermore, assume that $\mathrm{LT}_\sigma(v_1) >_{\mathtt{PosLex}} \cdots >_{\mathtt{PosLex}} \mathrm{LT}_\sigma(v_s)$, and that there exists a number $m \in \{1, \ldots, n\}$ such that $\mathrm{LT}_\sigma(v_i) \in \mathbb{T}(x_m, \ldots, x_n)\langle e_1, \ldots, e_r\rangle$ for $i = 1, \ldots, s$. Then the leading terms of the fundamental syzygies σ_{ij} of $\mathcal{V}$ satisfy $\mathrm{LT}_\tau(\sigma_{ij}) \in \mathbb{T}(x_{m+1}, \ldots, x_n)\langle \varepsilon_1, \ldots, \varepsilon_s\rangle$ for all i, j. Here τ is the ordering induced by $(\sigma, \mathcal{V})$ according to Definition 3.1.1.*

Proof. Let $1 \leq i < j \leq s$ and $\mathrm{LT}_\sigma(v_i) = t_i e_{\gamma_i}$ as well as $\mathrm{LT}_\sigma(v_j) = t_j e_{\gamma_j}$ with $t_i, t_j \in \mathbb{T}(x_m, \ldots, x_n)$ and $\gamma_i, \gamma_j \in \{1, \ldots, r\}$. A fundamental syzygy exists only if $\gamma_i = \gamma_j$. In this case, the hypothesis $\mathrm{LT}_\sigma(v_i) >_{\mathtt{PosLex}} \mathrm{LT}_\sigma(v_j)$ implies $\log_{x_m}(t_i) \geq \log_{x_m}(t_j)$. Hence x_m does not divide $\mathrm{lcm}(t_i, t_j)/t_i$ and we have $\mathrm{LT}_\tau(\sigma_{ij}) = (\mathrm{lcm}(t_i, t_j)/t_i)\,\varepsilon_i \in \mathbb{T}(x_{m+1}, \ldots, x_n)\langle \varepsilon_1, \ldots, \varepsilon_s\rangle$, as claimed. □

Now we are ready to settle the existence question for finite graded resolutions. Notice that we even get a global bound for the length of a particular resolution of an arbitrary finitely generated graded P-module.

Theorem 4.8.4. (Graded Version of Hilbert's Syzygy Theorem) *Let M be a finitely generated graded P-module. Then M has a finite graded free resolution of length at most n.*

Proof. Let $\mathcal{G} = (g_1, \ldots, g_r)$ be a tuple of non-zero homogeneous elements which generate M, let $\deg_W(g_i) = d_{0i}$ for $i = 1, \ldots, r$, and let $F_0 = \bigoplus_{i=1}^r P(-d_{0i})$. Then we have an exact sequence of graded P-modules

$$0 \longrightarrow N \xrightarrow{\psi} F_0 \xrightarrow{\varphi} M \longrightarrow 0$$

where $N = \mathrm{Syz}_P(\mathcal{G})$. It suffices to show that there is a graded free resolution

$$0 \longrightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \xrightarrow{\varphi_{n-1}} \cdots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} N \longrightarrow 0$$

since then the sequence

$$0 \longrightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \xrightarrow{\varphi_{n-1}} \cdots \xrightarrow{\varphi_2} F_1 \xrightarrow{\psi\circ\varphi_1} F_0 \longrightarrow M \longrightarrow 0$$

is a graded free resolution of M of length $\leq n$.

Let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ and $\mathcal{V} = (v_1, \ldots, v_s)$ be a homogeneous σ-Gröbner basis of N. Without loss of generality we may assume that $\mathrm{LT}_\sigma(v_1) >_{\mathtt{PosLex}} \cdots >_{\mathtt{PosLex}} \mathrm{LT}_\sigma(v_s)$. For $i = 1, \ldots, s$, let $d_{1i} = \deg_W(v_i)$. The canonical basis of $F_1 = \bigoplus_{i=1}^s P(-d_{1i})$ is denoted by $\{\varepsilon_1, \ldots, \varepsilon_s\}$. Let τ be the module term ordering on $\mathbb{T}^n\langle \varepsilon_1, \ldots, \varepsilon_s\rangle$ induced by $(\sigma, \mathcal{V})$.

By Corollary 3.1.5, the set of fundamental syzygies of $\mathcal{V}$ can be lifted to a τ-Gröbner basis $\mathcal{S}_1$ of the graded P-submodule $S_1 = \mathrm{Syz}_P(\mathcal{V})$ of F_1. By Lemma 4.8.3, the τ-leading terms of the elements of $\mathcal{S}_1$ are contained in $\mathbb{T}(x_2, \ldots, x_n)\langle \varepsilon_1, \ldots, \varepsilon_s\rangle$. Moreover, the elements of $\mathcal{S}_1$ are homogeneous elements of F_1, and we may assume that their τ-leading terms are ordered decreasingly with respect to `PosLex`.

This shows that we can repeat the same argument for S_1 in place of N and construct a graded submodule S_2 of a graded free P-module F_2 with a Gröbner basis whose leading terms involve only the indeterminates $x_3, \ldots, x_n$. After $\ell \leq n$ steps we reach a situation where the leading terms of the Gröbner basis of S_ℓ do not involve any indeterminate anymore, i.e. where they are elements in the canonical basis of F_ℓ. Hence we can apply Proposition 4.8.2 to the sequence

$$0 \longrightarrow S_\ell \longrightarrow F_\ell \xrightarrow{\varphi_\ell} F_{\ell-1}$$

and conclude that $S_{\ell-1}$, the image of φ_ℓ, is a graded free P-module. Consequently, the homogeneous exact sequence

$$0 \longrightarrow S_{\ell-1} \longrightarrow F_{\ell-1} \xrightarrow{\varphi_{\ell-1}} \cdots \xrightarrow{\varphi_1} F_1 \xrightarrow{\varphi_0} N \longrightarrow 0$$

is a graded free resolution and the proof is complete. □

Now we know how to make a finite graded free resolution of a finitely generated graded module. However, as the title of this section suggests, we want more.

Definition 4.8.5. Let M be a finitely generated graded P-module. A graded free resolution

$$\cdots \xrightarrow{\varphi_3} F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

of M is called a **minimal graded free resolution** of M if the images of the canonical basis vectors of F_i are a minimal system of generators of $\mathrm{Ker}(\varphi_{i-1})$ for every $i \geq 1$.

By the Graded Version of Nakayama's Lemma 1.7.15, the graded free resolution of M in the definition is minimal if and only if none of the homogeneous matrices representing $\varphi_1, \varphi_2, \ldots$ contains a non-zero constant polynomial. By choosing a minimal homogeneous presentation of $\mathrm{Ker}(\varphi_i)$ for every $i \geq 0$ and combining the resulting short exact sequences, we can easily construct a minimal graded free resolution for a given module M. However, despite their promising name, it is not yet clear that finite minimal graded free resolutions exist. The finite graded free resolution constructed in the proof of the Graded Version of Hilbert's Syzygy Theorem 4.8.4 is usually non-minimal, because the Gröbner basis of $\mathrm{Ker}(\varphi_i)$ constructed at each step is rarely a minimal set of generators. Thus we are led to the idea of trying to trim a given free resolution until it becomes a minimal one. The following tool does the trick.

Theorem 4.8.6. (Local Minimalization of Resolutions)
Let $F_3 \xrightarrow{\varphi_3} F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0$ *be an exact sequence of finitely generated graded free* P*-modules and homogeneous* P*-linear maps. Then there exists a homogeneous exact sequence of finitely generated graded free modules* $F_3 \xrightarrow{\varphi'_3} F'_2 \xrightarrow{\varphi'_2} F'_1 \xrightarrow{\varphi'_1} F_0$ *such that the matrix associated to* φ'_2 *has no non-zero constant entries and also* $\mathrm{Im}(\varphi_1) = \mathrm{Im}(\varphi'_1)$ *and* $\mathrm{Ker}(\varphi_3) = \mathrm{Ker}(\varphi'_3)$.

Proof. Without loss of generality, we may assume that the canonical bases of all graded free modules involved are deg-ordered. Let $\mathcal{G}$ be the matrix which defines φ_1, and denote $\mathrm{Im}(\varphi_1)$ by M. Considered as a tuple of vectors, $\mathcal{G}$ generates M. We pick a subtuple $\mathcal{G}'$ of $\mathcal{G}$ which minimally generates M and construct the corresponding homomorphism of graded free modules $\varphi'_1 : F'_1 \longrightarrow F_0$. It follows that there exist two matrices $\mathcal{A}_1$ and $\mathcal{B}_1$ such that $\mathcal{G} = \mathcal{G}'\mathcal{A}_1$ and $\mathcal{G}' = \mathcal{G}\,\mathcal{B}_1$ and $\mathcal{A}_1\mathcal{B}_1 = \mathcal{I}$, where $\mathcal{I}$ denotes an identity matrix. The matrix $\mathcal{A}_1$ yields a surjective homomorphism of graded free modules $\alpha_1 : F_1 \longrightarrow F'_1$.

Now let $\mathcal{S}$ be the homogeneous matrix corresponding to φ_2. Thus $\mathcal{S}$ is a tuple of vectors which generate $\mathrm{Syz}_P(\mathcal{G})$. As in the proof of Proposition 4.7.10.a (using $\mathcal{A}_1$ for $\mathcal{A}^{-1}$ and $\mathcal{B}_1$ for $\mathcal{A}$), it follows that $\mathcal{A}_1\mathcal{S}$ generates $\mathrm{Syz}_P(\mathcal{G}')$. Next, we let $\mathcal{S}'$ be a subtuple of $\mathcal{A}_1\mathcal{S}$ which generates $\mathrm{Syz}_P(\mathcal{G}')$ minimally and $\varphi'_2 : F'_2 \longrightarrow F'_1$ be the homomorphism of graded free modules defined by $\mathcal{S}'$. Since $\mathcal{S}'$ is a tuple of generators, there exists a homogeneous matrix $\mathcal{A}_2$ such that $\mathcal{A}_1\mathcal{S} = \mathcal{S}'\mathcal{A}_2$. Since $\mathcal{S}'$ is a subtuple of $\mathcal{A}_1\mathcal{S}$, the homogeneous map $\alpha_2 : F_2 \longrightarrow F'_2$ defined by $\mathcal{A}_2$ is injective.

Altogether, we obtain a commutative diagram of homogeneous P-linear maps with exact rows

$$\begin{array}{ccccccc} F_3 & \xrightarrow{\varphi_3} & F_2 & \xrightarrow{\varphi_2} & F_1 & \xrightarrow{\varphi_1} & F_0 \\ \| & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_1} & & \| \\ F_3 & \xrightarrow{\varphi_3'} & F_2' & \xrightarrow{\varphi_2'} & F_1' & \xrightarrow{\varphi_1'} & F_0 \end{array}$$

where we define $\varphi_3' = \alpha_2 \circ \varphi_3$. Since α_1 is surjective, we have $\mathrm{Im}(\varphi_1) = \mathrm{Im}(\varphi_1')$ and since α_2 is injective, we have $\mathrm{Ker}(\varphi_3) = \mathrm{Ker}(\varphi_3')$, as claimed. By construction, the matrix $\mathcal{S}'$ representing the map φ_2' corresponds to a minimal system of generators and therefore does not contain non-zero constant polynomials. □

Corollary 4.8.7. (Existence of Minimal Graded Free Resolutions) *Let M be a finitely generated graded P-module. Then M has a minimal graded free resolution of length at most n.*

Proof. Using Theorem 4.8.4 we find a finite graded free resolution of M of length $\ell \leq n$. Then we apply Theorem 4.8.6 repeatedly and replace pieces of the resolution until none of the matrices corresponding to $\varphi_1, \varphi_2, \ldots, \varphi_\ell$ contains a non-zero constant polynomial anymore. □

After settling the existence question, we now study whether and in what sense the minimal graded free resolution of a module is uniquely determined. The following lemma, a variant of Proposition 4.7.10, provides essential aid.

Lemma 4.8.8. *Let M be a graded submodule of a graded free P-module F_0, let $\psi_0 : F_0 \longrightarrow F_0$ be a homogeneous isomorphism, let $F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} M \longrightarrow 0$ and $F_2 \xrightarrow{\varphi_2'} F_1 \xrightarrow{\varphi_1'} \psi_0(M) \longrightarrow 0$ be two minimal homogeneous presentations, and let $\psi_1 : F_1 \longrightarrow F_1$ be a homogeneous isomorphism which satisfies $\psi_0 \circ \varphi_1 = \varphi_1' \circ \psi_1$. Furthermore, assume that the matrices $\mathcal{A}, \mathcal{B}, \mathcal{G}, \mathcal{G}', \mathcal{S}, \mathcal{S}'$ representing the maps $\psi_0, \psi_1, \varphi_1, \varphi_1', \varphi_2, \varphi_2'$, respectively, are deg-ordered.*

a) The tuple $\mathcal{B}\,\mathcal{S}$ is deg-ordered and generates $\mathrm{Syz}_P(\mathcal{G}')$ minimally.

b) There exists a deg-ordered invertible matrix $\mathcal{C}$ such that $\mathcal{B}\,\mathcal{S} = \mathcal{S}'\,\mathcal{C}$. In other words, we have a commutative diagram

$$\begin{array}{ccccccc} F_2 & \xrightarrow{\varphi_2} & F_1 & \xrightarrow{\varphi_1} & F_0 \\ \downarrow{\scriptstyle \psi_2} & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_0} \\ F_2 & \xrightarrow{\varphi_2'} & F_1 & \xrightarrow{\varphi_1'} & F_0 \end{array}$$

where ψ_2 is the homogeneous isomorphism defined by $\mathcal{C}$.

Proof. The proof of a) is very similar to the proof of Proposition 4.7.10.a. Since we have $\mathcal{G}'\,\mathcal{B}\,\mathcal{S} = \mathcal{A}\,\mathcal{G}\,\mathcal{S} = 0$, the columns of $\mathcal{B}\,\mathcal{S}$ are syzygies of $\mathcal{G}'$. Given any homogeneous element $u \in \mathrm{Syz}_P(\mathcal{G}')$, we compute $\mathcal{A}\,\mathcal{G}\,\mathcal{B}^{-1}\,u = \mathcal{G}'\,u = 0$. This shows that $\mathcal{G}\,\mathcal{B}^{-1}\,u = 0$. Hence the homogeneous vector $\mathcal{B}^{-1}\,u$ is a syzygy of $\mathcal{G}$. Since $\mathcal{S}$ generates $\mathrm{Syz}_P(\mathcal{G})$, there exists a homogeneous

matrix $\mathcal{H}$ such that $\mathcal{B}^{-1}\,u = \mathcal{S}\,\mathcal{H}$. Therefore we have $u = \mathcal{B}\,(\mathcal{B}^{-1}\,u) = \mathcal{B}\,\mathcal{S}\,\mathcal{H}$, and it follows that $\mathcal{B}\,\mathcal{S}$ generates $\mathrm{Syz}_P(\mathcal{G}')$. Moreover, since the matrix $\mathcal{B}$ is deg-ordered and invertible, the matrix $\mathcal{B}\,\mathcal{S}$ is deg-ordered too, and is also a minimal system of generators of $\mathrm{Syz}_P(\mathcal{G}')$.

To prove b), we observe that $\mathcal{S}'$ and $\mathcal{B}\,\mathcal{S}$ both generate $\mathrm{Syz}_P(\mathcal{G}')$ minimally. By Proposition 4.7.8, there exists a deg-ordered invertible matrix $\mathcal{C}$ such that $\mathcal{B}\,\mathcal{S} = \mathcal{S}'\,\mathcal{C}$. □

Our next theorem shows that the minimal graded free resolution of a finitely generated graded P-module is uniquely determined up to some homogeneous isomorphisms of graded free modules.

Theorem 4.8.9. (Uniqueness of Minimal Graded Free Resolutions) *Let M be a finitely generated graded P-module, and let*

$$0 \longrightarrow F_\ell \xrightarrow{\varphi_\ell} \cdots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

and

$$\cdots \longrightarrow F'_\ell \xrightarrow{\varphi'_\ell} \cdots \xrightarrow{\varphi'_2} F'_1 \xrightarrow{\varphi'_1} F'_0 \xrightarrow{\varphi'_0} M \longrightarrow 0$$

be two minimal graded free resolutions of M. Assume that the canonical bases of the graded free modules F_i, F'_j are deg-ordered.

a) For every $i \geq 0$, we have $F_i = F'_i$. In particular, we have $F'_i = 0$ for $i > \ell$.

b) For $i = 0, \ldots, \ell$ there exist deg-ordered invertible matrices $\mathcal{A}_i$ defining isomorphisms $\psi_i : F_i \longrightarrow F_i$ yielding the commutative diagram

$$\begin{array}{ccccccccccccc}
0 & \longrightarrow & F_\ell & \xrightarrow{\varphi_\ell} & \cdots & \xrightarrow{\varphi_3} & F_2 & \xrightarrow{\varphi_2} & F_1 & \xrightarrow{\varphi_1} & F_0 & \xrightarrow{\varphi_0} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi_\ell} & & & & \downarrow{\scriptstyle \psi_2} & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_0} & & \| & & \\
0 & \longrightarrow & F_\ell & \xrightarrow{\varphi'_\ell} & \cdots & \xrightarrow{\varphi'_3} & F_2 & \xrightarrow{\varphi'_2} & F_1 & \xrightarrow{\varphi'_1} & F_0 & \xrightarrow{\varphi'_0} & M & \longrightarrow & 0
\end{array}$$

Proof. By Proposition 4.7.8.a, we have $F_0 = F'_0$, and by Proposition 4.7.8.b, there exists a deg-ordered invertible matrix $\mathcal{A}_0$ giving a homogeneous isomorphism $\psi_0 : F_0 \longrightarrow F_0$ which satisfies $\varphi'_0 \circ \psi_0 = \varphi_0$. Let $\mathcal{G}, \mathcal{G}', \mathcal{S}, \mathcal{S}'$ be the deg-ordered matrices corresponding to $\varphi_0, \varphi'_0, \varphi_1, \varphi'_1$, respectively. Since we have $\mathcal{G} = \mathcal{G}'\,\mathcal{A}_0$, Proposition 4.7.10 implies that $\mathcal{A}_0^{-1}\,\mathcal{S}'$ is a deg-ordered minimal homogeneous system of generators of $\mathrm{Syz}_P(\mathcal{G})$ and that $F_1 = F'_1$. Using Proposition 4.7.8.b again, we find a deg-ordered invertible homogeneous matrix $\mathcal{A}_1$ such that $\mathcal{S} = \mathcal{A}_0^{-1}\,\mathcal{S}'\,\mathcal{A}_1$. Therefore the homogeneous isomorphism $\psi_1 : F_1 \longrightarrow F_1$ defined by $\mathcal{A}_1$ satisfies $\varphi'_1 \circ \psi_1 = \psi_0 \circ \varphi_1$.

Now we are in a position to apply Lemma 4.8.8 to the commutative diagram

$$\begin{array}{ccccc}
F_2 & \xrightarrow{\varphi_2} & F_1 & \xrightarrow{\varphi_1} & F_0 \\
 & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_0} \\
F'_2 & \xrightarrow{\varphi'_2} & F_1 & \xrightarrow{\varphi'_1} & F_0
\end{array}$$

and we get $F_2 = F_2'$ and a homogeneous isomorphism $\psi_2 : F_2 \longrightarrow F_2$ such that $\varphi_2' \circ \psi_2 = \psi_1 \circ \varphi_2$. By applying the lemma repeatedly in this way, we prove both parts of the theorem. □

If the canonical bases of the graded free modules in a minimal graded free resolution of M are not deg-ordered, we can pass to an isomorphic resolution in which this is the case by permuting them suitably. Therefore we can attach another set of invariants to a finitely generated graded P-module as follows.

Definition 4.8.10. Let M be a finitely generated graded P-module, and let

$$0 \longrightarrow F_\ell \xrightarrow{\varphi_\ell} \cdots \xrightarrow{\varphi_3} F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

be a minimal graded free resolution of M. For every $i \in \mathbb{N}$, let $\mathcal{E}_i$ be the tuple of the canonical basis vectors of F_i. By passing to an isomorphic resolution, we may assume that the tuples $\mathcal{E}_0, \mathcal{E}_1, \ldots$ are deg-ordered.

a) The degree sequence $(\deg_W(\mathcal{E}_0), \deg_W(\mathcal{E}_1), \ldots, \deg_W(\mathcal{E}_\ell))$ does not depend on the choice of the minimal free resolution of M. It is called the **degree sequence** of the module M.
b) Let $i \in \{0, \ldots, \ell\}$. For every $d \in \mathbb{Z}^m$, we let β_{id} be the number of times the degree d occurs in $\deg_W(\mathcal{E}_i)$. The numbers β_{id} are called the **i^{th} graded Betti numbers** of the module M.

Using the graded Betti numbers, a graded minimal free resolution of M can be written in the form

$$0 \to \bigoplus_{d\in\mathbb{Z}^m} P(-d)^{\beta_{nd}} \to \cdots \to \bigoplus_{d\in\mathbb{Z}^m} P(-d)^{\beta_{1d}} \to \bigoplus_{d\in\mathbb{Z}^m} P(-d)^{\beta_{0d}} \to M \to 0$$

Using the algorithms discussed in the next subsection, the graded Betti numbers of a finitely generated graded P-module can be computed effectively. In the standard graded case, they are usually displayed in a particularly compact and expressive form which is called the **Betti diagram** and introduced in Tutorial 63.

4.8.B Computation of Minimal Graded Free Resolutions

When the going gets tough, the tough get going.
(Pop music lyrics)

When the going gets tough, the tough go shopping.
(T-shirt slogan)

This is the point of no return. We are now going *where few men have gone before:* down into the nitty-gritty details of computing minimal graded free resolutions. Using Proposition 4.7.24, we can reduce the task to the case of a submodule of a free module. As explained in the introduction of

Section 4.7, it is convenient to denote the graded free module by F_0 and its graded submodule by M. The minimal graded free resolution of M we are looking for is then of the form

$$0 \longrightarrow F_\ell \xrightarrow{\varphi_\ell} F_{\ell-1} \xrightarrow{\varphi_{\ell-1}} \cdots \xrightarrow{\varphi_3} F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} M \longrightarrow 0$$

So, let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let M be a graded P-submodule of a graded free P-module $F_0 = \bigoplus_{i=1}^{r_0}(-d_{0i})$, and let $\mathcal{V} = (v_1, \ldots, v_s)$ be a tuple of non-zero homogeneous vectors which generate M. For $d \in \mathbb{Z}^m$, the minimal graded free resolutions of M and $M(d)$ differ only by the shift d. Therefore we shall henceforth assume that we have $d_{0i} >_{\mathtt{Lex}} 0$ for $i = 1, \ldots, r_0$. To facilitate the formulation of our algorithms, we introduce a number of conventions.

The i^{th} graded free module F_i is always of the form $F_i = \bigoplus_{j=0}^{r_i}(-d_{ij})$. Its canonical basis is denoted by $(\varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)})$ and is always kept deg-ordered. The idealization of the module $F_0 \oplus \cdots \oplus F_n$ is a residue class ring of the ring $\widetilde{P} = P[\varepsilon_j^{(i)} \mid i \in \{0, \ldots, n\}, j \in \{1, \ldots, r_i\}]$. As in the previous section, the entire computation can be viewed as computation in $\widetilde{P}$. In particular, the elements of each F_i are identified with their images in this ring.

The first algorithm we present is a straightforward generalization of the vertical strategy for computing minimal presentations (see Theorem 4.7.26).

Proposition 4.8.11. (Computing Minimal Resolutions Vertically) *Let M be a graded submodule of a graded free P-module $F_0 = \bigoplus_{i=1}^{r_0} P(-d_{0i})$, where $d_{0i} >_{\mathtt{Lex}} 0$ for $i = 1, \ldots, r_0$. Let $\mathcal{V} = (v_1, \ldots, v_s)$ be a deg-ordered tuple of non-zero homogeneous vectors which generate M. Consider the following sequence of instructions.*

1) *Let $i = 0$. Equip $\overline{P} = P[\varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)}]$ with the grading defined by $\overline{W} = (W \mid d_{i1} \ \cdots \ d_{ir_i})$. Choose a term ordering σ on $\mathbb{T}^n(\varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)})$. Let $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, $s' = 0$, $\mathcal{G}_{\min}^{(i)} = \emptyset$, $r_{i+1} = 0$, and $\mathcal{S} = \emptyset$.*
2) *Let d be the smallest degree with respect to* Lex *of an element in B or in $\mathcal{W}$. Form the subset B_d and the subtuple $\mathcal{W}_d$, and delete their entries from B and $\mathcal{W}$, respectively.*
3) *If $B_d = \emptyset$, continue with step 6). Otherwise, chose a pair $(j, k) \in B_d$ and remove it from B_d.*
4) *Form the S-vector S_{jk} of g_j and g_k. Then compute $S'_{jk} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{jk})$. If $S'_{jk} = 0$ continue with step 3). Otherwise, if $S'_{jk} \neq 0$ and it does not involve the indeterminates $\varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)}$, append it to $\mathcal{S}$ and continue with step 3).*
5) *Increase s' by one, append $g_{s'} = S'_{jk}$ to the tuple $\mathcal{G}$, and append the set $\{(j, s') \mid 1 \leq j < s',\ \gamma_j = \gamma_{s'}\}$ to B, where $\mathrm{LT}_\sigma(g_{s'}) = t_{s'}\varepsilon_{\gamma_{s'}}^{(i)}$ with $t_{s'} \in \mathbb{T}^n$ and $\gamma_{s'} \in \{1, \ldots, r_i\}$. Then continue with step 3).*
6) *If $\mathcal{W}_d = \emptyset$, continue with step 9). Otherwise, choose a vector $v \in \mathcal{W}_d$ and remove it from $\mathcal{W}_d$.*

7) *Compute* $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v)$ *and* $\bar{v} = v'(x_1, \ldots, x_n, \varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)}, 0, \ldots, 0)$. *If* $\bar{v} = 0$, *continue with step 6).*

8) *Increase* s' *and* r_{i+1} *by one. Adjoin a new indeterminate* $\varepsilon_{r_{i+1}}^{(i+1)}$ *to* $\overline{P}$ *and extend the grading to this new ring by defining* $\deg_{\overline{W}}(\varepsilon_{r_{i+1}}^{(i+1)}) = \deg_{\overline{W}}(\bar{v})$. *Extend the term ordering* σ *to the new ring in such a way that the extension is an elimination ordering for* $\{\varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)}\}$. *Append the element* $g_{s'} = \bar{v} - \varepsilon_{r_{i+1}}^{(i+1)}$ *to* $\mathcal{G}$ *and the element* $\bar{v}$ *to* $\mathcal{G}_{\min}^{(i)}$. *Append the set* $\{(j, s') \mid 1 \leq j < s', \gamma_j = \gamma_{s'}\}$ *to* B. *Continue with step 6).*

9) *If* $B \neq \emptyset$ *or* $\mathcal{W} \neq \emptyset$, *continue with step 2).*

10) *If* $\mathcal{S} \neq 0$, *increase* i *by one, form the ring* $\overline{P} = P[\varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)}]$, *and equip it with the grading defined by* $\overline{W} = (W \mid d_{i1} \ \cdots \ d_{ir_i})$. *Restrict the term ordering* σ *to* $\mathbb{T}^n(\varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)})$. *Let* $B = \emptyset$, $\mathcal{W} = \mathcal{S}$, $\mathcal{G} = \emptyset$, $s' = 0$, $\mathcal{G}_{\min}^{(i)} = \emptyset$, $r_{i+1} = 0$, *and* $\mathcal{S} = \emptyset$. *Then continue with step 2).*

11) *Let* $\ell = i + 1$. *Return the list* $(\mathcal{G}_{\min}^{(0)}, \ldots, \mathcal{G}_{\min}^{(\ell-1)})$ *and stop.*

This is an algorithm which computes a list of deg-ordered homogeneous matrices $(\mathcal{G}_{\min}^{(0)}, \ldots, \mathcal{G}_{\min}^{(\ell-1)})$ *with the property that the linear maps* $\varphi_j : F_j \longrightarrow F_{j-1}$ *given by* $\mathcal{G}_{\min}^{(j-1)}$ *for* $j = 1, \ldots, \ell$ *yield a minimal graded free resolution*

$$0 \longrightarrow F_\ell \xrightarrow{\varphi_\ell} F_{\ell-1} \xrightarrow{\varphi_{\ell-1}} \cdots \xrightarrow{\varphi_3} F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} M \longrightarrow 0$$

Proof. The loop defined by steps 2) – 9) mirrors the main loop used in Theorem 4.7.26 to compute a minimal homogeneous presentation of M vertically. In the proof of that theorem we saw that, at the end of the i^{th} iteration, the tuple $\mathcal{G}_{\min}^{(i)}$ contains a minimal set of generators of the module generated by $\mathcal{W}$, and the tuple $\mathcal{S}$ contains a σ-Gröbner basis of $\mathrm{Syz}_P(\mathcal{G}_{\min}^{(i)})$. Thus, if we feed $\mathcal{S}$ as the new input tuple $\mathcal{W}$ into the next iteration of the loop, we compute a minimal system of generators $\mathcal{G}_{\min}^{(i+1)}$ of $\mathrm{Syz}_P(\mathcal{G}_{\min}^{(i)})$ and a Gröbner basis of $\mathrm{Syz}_P(\mathcal{G}_{\min}^{(i+1)})$. By Theorem 4.8.9, this process stops after at most $n - 1$ steps, i.e. after at most $n - 1$ steps we have $\mathcal{S} = \emptyset$ and the algorithm stops. □

Although the vertical strategy for computing minimal graded free resolutions is in general rather crude, it has some merits.

Remark 4.8.12. Suppose we are in the setting of the theorem.

a) If we do not want to know the whole minimal graded free resolution of M, or if we discover during the computation that the going is getting too tough, we can stop the execution of the algorithm after the loop of steps 2) – 9) is finished for a particular value of i and get the correct first $i + 1$ graded free modules and maps.

b) When $i \geq 1$, we can save some applications of step 4), since we know that $\mathcal{S}$ is a Gröbner basis after the loop 2) – 9) for $i - 1$ is finished and this is the new input tuple $\mathcal{W}$.

c) In step 10) we could choose σ freely, but would then lose the knowledge that $\mathcal{W}$ is a Gröbner basis. So, the optimization of b) cannot be used. However, we will get in $\mathcal{G}^{(i)}$ a σ-Gröbner basis of $\mathrm{Syz}_P(\mathcal{G}_{\min}^{(i-1)})$ for the chosen term ordering σ.

Following on from Example 4.7.28, we now compute the whole minimal graded free resolution. Of course, we do not repeat the first iteration of the loop in steps 2) – 9), since this has already been done.

Example 4.8.13. As in Example 4.7.28, we let $P = \mathbb{Q}[x_1, x_2, x_3, x_4]$ be graded by $W = \left(\begin{smallmatrix}1&1&1&1\\0&1&3&4\end{smallmatrix}\right)$, and we let M be the graded P-submodule of $F_0 = P(-\binom{1}{0})$ generated by the homogeneous tuple $\mathcal{V} = (f_1e, f_2e, f_3e, f_4e)$, where $f_1 = x_1x_4 - x_2x_3$, $f_2 = x_1^2x_3 - x_2^3$, $f_3 = x_1x_3^2 - x_2^2x_4$, $f_4 = x_2x_4^2 - x_3^3$, and e is the canonical basis vector of F_0.

When we compute the minimal graded free resolution of M vertically, the first execution of the loop in steps 2) – 9) mimics the first part of Example 4.7.28. After this iteration is finished, we have computed $\mathcal{G}_{\min}^{(0)}$ and a tuple $\mathcal{S} = (S'_{23}, S'_{12}, S'_{14}, S'_{13}, S'_{24}, S'_{34})$, where $S'_{23} = x_2^2\varepsilon_1^{(1)} - x_3\varepsilon_2^{(1)} + x_1\varepsilon_3^{(1)}$, $S'_{12} = -x_1x_3\varepsilon_1^{(1)} + x_4\varepsilon_2^{(1)} - x_2\varepsilon_3^{(1)}$, $S'_{14} = -x_2x_4\varepsilon_1^{(1)} + x_3\varepsilon_3^{(1)} + x_1\varepsilon_4^{(1)}$, $S'_{13} = -x_3^2\varepsilon_1^{(1)} + x_4\varepsilon_3^{(1)} + x_2\varepsilon_4^{(1)}$, $S'_{24} = -x_2x_4^2\varepsilon_2 + x_3^3\varepsilon_2 + x_1^2x_3\varepsilon_4 - x_2^3\varepsilon_4$, and $S'_{34} = -x_2x_4^2\varepsilon_3 + x_3^3\varepsilon_3 + x_1x_3^2\varepsilon_4 - x_2^2x_4\varepsilon_4$. Notice that $\deg_{\overline{W}}(S'_{23}) = \binom{5}{6}$, $\deg_{\overline{W}}(S'_{12}) = \binom{5}{7}$, $\deg_{\overline{W}}(S'_{14}) = \binom{5}{9}$, $\deg_{\overline{W}}(S'_{13}) = \binom{5}{10}$, $\deg_{\overline{W}}(S'_{24}) = \binom{7}{12}$, and $\deg_{\overline{W}}(S'_{34}) = \binom{7}{15}$.

Let us join the action and follow the further calculations step-by-step. We continue to choose σ to be the lexicographic term ordering which satisfies

$$e >_\sigma \varepsilon_1^{(1)} >_\sigma \cdots >_\sigma \varepsilon_{r_1}^{(1)} >_\sigma \cdots >_\sigma \varepsilon_1^{(i)} >_\sigma \cdots >_\sigma \varepsilon_{r_i}^{(i)} >_\sigma x_1 >_\sigma \cdots >_\sigma x_n$$

10) Let $i = 1$, let $\overline{P} = K[\varepsilon_1^{(1)}, \ldots, \varepsilon_4^{(1)}]$ be graded by $\overline{W} = \left(\begin{smallmatrix}1&1&1&1&5&5&5&5\\0&1&3&4&6&7&9&10\end{smallmatrix}\right)$, let $B = \emptyset$, and let $\mathcal{W} = (w_1, w_2, w_3, w_4, w_5, w_6)$ where $w_1 = S'_{23}$, $w_2 = S'_{12}$, $w_3 = S'_{14}$, $w_4 = S'_{13}$, $w_5 = S'_{24}$, and $w_6 = S'_{34}$. Furthermore, let $\mathcal{G} = \emptyset$, $s' = 0$, $\mathcal{G}_{\min}^{(1)} = \emptyset$, $r_1 = 0$, and $\mathcal{S} = \emptyset$.
2) Let $d = \binom{5}{6}$, $B_d = \emptyset$, $\mathcal{W}_d = (w_1)$, and $\mathcal{W} = (w_2, w_3, w_4, w_5, w_6)$.
6) Choose $v = w_1$ and set $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(w_1) = w_1$ and $\overline{v} = w_1$.
8) Let $s' = 1$ and $r_1 = 1$. Append $\varepsilon_1^{(2)}$ to $\overline{P}$ and extend the grading by $\deg_{\overline{W}}(\varepsilon_1^{(2)}) = \binom{5}{6}$. Let $g_1 = w_1 - \varepsilon_1^{(2)}$, $\mathcal{G} = (g_1)$, and $\mathcal{G}_{\min}^{(1)} = (w_1)$.
2) Let $d = \binom{5}{7}$, $B_d = \emptyset$, $\mathcal{W}_d = (w_2)$, and $\mathcal{W} = (w_3, w_4, w_5, w_6)$.
6) Choose $v = w_2$ and set $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(w_2) = w_2$ and $\overline{v} = w_2$.
8) Let $s' = 2$ and $r_1 = 2$. Append $\varepsilon_2^{(2)}$ to $\overline{P}$ and extend the grading by $\deg_{\overline{W}}(\varepsilon_2^{(2)}) = \binom{5}{7}$. Let $g_2 = w_2 - \varepsilon_2^{(2)}$, $\mathcal{G} = (g_1, g_2)$, $\mathcal{G}_{\min}^{(1)} = (w_1, w_2)$, and $B = \{(1,2)\}$. Observe that $\deg_{\overline{W}}((1,2)) = \binom{7}{9}$.

2) Let $d = \binom{5}{9}$, $B_d = \emptyset$, $\mathcal{W}_d = (w_3)$, and $\mathcal{W} = (w_4, w_5, w_6)$.
6) Choose $v = w_3$ and set $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(w_3) = w_3$ and $\overline{v} = w_3$.
8) Let $s' = 3$ and $r_1 = 3$. Append $\varepsilon_3^{(2)}$ to $\overline{P}$ and extend the grading by $\deg_{\overline{W}}(\varepsilon_1^{(2)}) = \binom{5}{9}$. Let $g_3 = w_3 - \varepsilon_3^{(2)}$, $\mathcal{G} = (g_1, g_2, g_3)$, $\mathcal{G}_{\min}^{(1)} = (w_1, w_2, w_3)$, and $B = \{(1,2), (1,3), (2,3)\}$. Observe that $\deg_{\overline{W}}((1,3)) = \binom{6}{10}$ and $\deg_{\overline{W}}((2,3)) = \binom{7}{12}$.
2) Let $d = \binom{5}{10}$, $B_d = \emptyset$, $\mathcal{W}_d = (w_4)$, and $\mathcal{W} = (w_5, w_6)$.
6) Choose $v = w_4$ and set $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(w_4) = w_4$ and $\overline{v} = w_4$.
8) Let $s' = 4$ and $r_1 = 4$. Append $\varepsilon_4^{(2)}$ to $\overline{P}$ and extend the grading by $\deg_{\overline{W}}(\varepsilon_4^{(2)}) = \binom{5}{10}$. Let $g_4 = w_4 - \varepsilon_4^{(2)}$, $\mathcal{G} = (g_1, g_2, g_3, g_4)$, $\mathcal{G}_{\min}^{(1)} = (w_1, w_2, w_3, w_4)$, and $B = \{(1,2), (1,3), (2,3), (1,4), (2,4), (3,4)\}$. We note $\deg_{\overline{W}}((1,4)) = \binom{7}{12}$, $\deg_{\overline{W}}((2,4)) = \binom{6}{10}$ and $\deg_{\overline{W}}((3,4)) = \binom{7}{15}$.
2) Let $d = \binom{6}{10}$, $B_d = \{(1,3), (2,4)\}$, and $B = \{(1,2), (2,3), (1,4), (3,4)\}$.
3) Choose $(1,3) \in B_d$ and set $B_d = \{(2,4)\}$.
4) Compute $S_{13} = x_4 g_1 + x_2^2 g_3 = -x_3 x_4 \varepsilon_2^{(1)} + (x_1 x_4 + x_2 x_3)\varepsilon_3^{(1)} + x_1 x_2 \varepsilon_4^{(1)} - x_4 \varepsilon_1^{(2)} - x_2 \varepsilon_3^{(2)}$ and $S'_{13} = \mathrm{NR}_{\sigma,\mathcal{G}}(S_{13}) = S_{13}$.
5) Let $s' = 5$, $g_5 = S'_{13}$, and $\mathcal{G} = (g_1, \ldots, g_5)$. (The set B does not change, because the leading term of g_5 is in a new position.)
3) Choose $(2,4) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{24} = x_3 g_2 - x_1 g_4$ and $S'_{24} = S_{24} + g_5 = -x_4 \varepsilon_1^{(2)} - x_3 \varepsilon_2^{(2)} - x_2 \varepsilon_3^{(2)} + x_1 \varepsilon_4^{(2)}$. Set $\mathcal{S} = (S'_{24})$.
2) Let $d = \binom{7}{9}$, $B_d = \{(1,2)\}$, and $B = \{(2,3), (1,4), (3,4)\}$.
3) Choose $(1,2) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{12} = x_1 x_3 g_1 + x_2^2 g_2 = (-x_1 x_3^2 + x_2^2 x_4)\varepsilon_2^{(1)} + (x_1^2 x_3 - x_2^3)\varepsilon_3^{(1)} - x_1 x_3 \varepsilon_1^{(2)} - x_2^2 \varepsilon_2^{(2)}$ and $S'_{12} = S_{12}$.
5) Let $s' = 6$, $g_6 = S'_{12}$, and $\mathcal{G} = (g_1, \ldots, g_6)$. Append $(5,6)$ to B. Note that $\deg_{\overline{W}}((5,6)) = \binom{8}{13}$.
2) Let $d = \binom{7}{12}$, $B_d = \{(2,3), (1,4)\}$, $B = \{(3,4), (5,6)\}$, $\mathcal{W}_d = (w_5)$, and $\mathcal{W} = (w_6)$.
3) Choose $(2,3) \in B_d$ and set $B_d = \{(1,4)\}$.
4) Compute $S_{23} = x_2 x_4 g_2 - x_1 x_3 g_3 = x_2 x_4^2 \varepsilon_2^{(1)} - (x_2^2 x_4 + x_1 x_3^2)\varepsilon_3^{(1)} - x_1^2 x_3 \varepsilon_4^{(1)} - x_2 x_4 \varepsilon_2^{(2)} + x_1 x_3 \varepsilon_3^{(2)}$ and $S'_{23} = S_{23}$.
5) Let $s' = 7$, $g_7 = S'_{23}$, and $\mathcal{G} = (g_1, \ldots, g_7)$. Append $(5,7)$ and $(6,7)$ to B. Note that $\deg_{\overline{W}}((5,7)) = \binom{8}{15}$ and $\deg_{\overline{W}}((6,7)) = \binom{10}{18}$.
3) Choose $(1,4) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{14} = x_3^2 g_1 + x_2^2 g_4 = -x_3^3 \varepsilon_2^{(1)} + (x_1 x_3^2 + x_2^2 x_4)\varepsilon_3^{(1)} + x_2^3 \varepsilon_4^{(1)} - x_3^2 \varepsilon_1^{(2)} - x_2^2 \varepsilon_4^{(2)}$ and $S'_{14} = S_{14}$.

5) Let $s' = 8$, $g_8 = S'_{14}$, and $\mathcal{G} = (g_1, \ldots, g_8)$. Append $(5,8)$, $(6,8)$, and $(7,8)$ to B. Note that $\deg_{\overline{W}}((5,8)) = \binom{8}{16}$, $\deg_{\overline{W}}((6,8)) = \binom{8}{12}$, and $\deg_{\overline{W}}((7,8)) = \binom{10}{21}$.
6) Choose $v = w_5$ and let $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = 0$.
2) Let $d = \binom{7}{15}$, $B_d = \{(3,4)\}$, $B = \{(5,6), (5,7), (6,7), (5,8), (6,8), (7,8)\}$, $\mathcal{W}_d = (w_6)$, and $\mathcal{W} = \emptyset$.
3) Choose $(3,4) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{34} = x_3^2 g_3 - x_2 x_4 g_4 = (x_3^3 - x_2 x_4^2)\varepsilon_3^{(1)} + (x_1 x_3^2 - x_2^2 x_4)\varepsilon_4^{(1)} - x_3^2 \varepsilon_3^{(2)} + x_2 x_4 \varepsilon_4^{(2)}$ and $S'_{34} = S_{34}$.
5) Let $s' = 9$, $g_9 = S'_{34}$, and $\mathcal{G} = (g_1, \ldots, g_9)$. (There are no new pairs.)
6) Let $v = w_6$ and $\mathcal{W}_d = \emptyset$.
7) Compute $v' = \mathrm{NR}_{\sigma,\mathcal{G}}(v) = 0$.
2) Let $d = \binom{8}{12}$, $B_d = \{(6,8)\}$, and $B = \{(5,6), (5,7), (6,7), (5,8), (7,8)\}$.
3) Choose $(6,8) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{68} = x_3 g_6 - x_1 g_8$ and $S'_{68} = -x_2^2 x_4 \varepsilon_1^{(2)} - x_2^2 x_3 \varepsilon_2^{(2)} - x_2^3 \varepsilon_3^{(2)} + x_1 x_2^2 \varepsilon_4^{(2)}$. Let $\mathcal{S} = (S'_{24}, S'_{68})$.
2) Let $d = \binom{8}{13}$, $B_d = \{(5,6)\}$, and $B = \{(5,7), (6,7), (5,8), (7,8)\}$.
3) Choose $(5,6) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{56} = x_1 x_3 g_5 - x_4 g_6$ and $S'_{56} = 0$.
2) Let $d = \binom{8}{15}$, $B_d = \{(5,7)\}$, and $B = \{(6,7), (5,8), (7,8)\}$.
3) Choose $(5,7) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{57} = x_2 x_4 g_5 + x_3 g_7$ and $S'_{57} = -x_2 x_4^2 \varepsilon_1^{(2)} - x_2 x_3 x_4 \varepsilon_2^{(2)} - x_2^2 x_4 \varepsilon_3^{(2)} + x_1 x_2 x_4 \varepsilon_4^{(2)}$. Let $\mathcal{S} = (S'_{24}, S'_{68}, S'_{57})$.
2) Let $d = \binom{8}{16}$, $B_d = \{(5,8)\}$, and $B = \{(6,7), (7,8)\}$.
3) Choose $(5,8) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{58} = x_3^5 g_5 - x_4 g_8$ and $S'_{58} = 0$.
2) Let $d = \binom{10}{18}$, $B_d = \{(6,7)\}$, and $B = \{(7,8)\}$.
3) Choose $(6,7) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{67} = x_2 x_4^2 g_6 + x_1 x_3^2 g_7$ and $S'_{67} = 0$.
2) Let $d = \binom{10}{21}$, $B_d = \{(7,8)\}$, and $B = \emptyset$.
3) Choose $(7,8) \in B_d$ and set $B_d = \emptyset$.
4) Compute $S_{78} = x_3^2 g_7 + x_2 x_4^2 g_8$ and $S'_{78} = 0$.

Here we turn off the computer and turn on our brain again. We have finished the loop in steps 2) – 9) for $i = 1$. The next round will use the tuple $\mathcal{S} = (S'_{24}, S'_{68}, S'_{57})$ as its input tuple. Since we have $S'_{68} = x_2^2 S'_{24}$ and $S'_{57} = x_2 x_4 S'_{24}$, the result will be $\mathcal{G}^{(2)}_{\min} = (S'_{24})$ and there will be no syzygies.

Finally, the algorithm returns the triple $(\mathcal{G}^{(0)}_{\min}, \mathcal{G}^{(1)}_{\min}, \mathcal{G}^{(2)}_{\min})$ where $\mathcal{G}^{(0)}_{\min}$ and $\mathcal{G}^{(1)}_{\min}$ are the tuples computed in Example 4.7.28 and $\mathcal{G}^{(2)}_{\min} = (S'_{24})$. Therefore the module M has the minimal graded free resolution

$$0 \longrightarrow P\big(-\tbinom{6}{10}\big) \xrightarrow{\lambda} P\big(-\tbinom{5}{6}\big) \oplus P\big(-\tbinom{5}{7}\big) \oplus P\big(-\tbinom{5}{9}\big) \oplus P\big(-\tbinom{5}{10}\big) \xrightarrow{\psi}$$
$$\xrightarrow{\psi} P\big(-\tbinom{3}{4}\big) \oplus P\big(-\tbinom{4}{3}\big) \oplus P\big(-\tbinom{4}{6}\big) \oplus P\big(-\tbinom{4}{9}\big) \xrightarrow{\varphi} M \longrightarrow 0$$

where the matrices defining φ and ψ are the ones given in Example 4.7.28 and the matrix defining λ is $(-x_4\ -x_3\ -x_2\ \ x_1)^{\mathrm{tr}}$.

The second algorithm for computing minimal graded free resolutions we present is based on combining the resolution given in the proof of Theorem 4.8.4 with the minimalization procedure of Theorem 4.8.6.

Proposition 4.8.14. (Schreyer's Resolution Algorithm)
Let M be a graded submodule of a graded free P-module $F_0 = \bigoplus_{i=1}^{r_0} P(-d_{0i})$, let $\{\varepsilon_1^{(0)}, \ldots, \varepsilon_{r_0}^{(0)}\}$ denote the canonical basis of F_0, and let $\mathcal{V} = (v_1, \ldots, v_s)$ be a deg-ordered tuple of non-zero homogeneous vectors which generate M. Consider the following sequence of instructions.

1) *Let $i = 0$. Choose a module term ordering σ_0 on $\mathbb{T}^n\langle\varepsilon_1^{(0)}, \ldots, \varepsilon_{r_0}^{(0)}\rangle$.*
2) *Using Corollary 3.1.5, compute a σ_0-Gröbner basis $\mathcal{G}_0 = (g_1^{(0)}, \ldots, g_{r_1}^{(0)})$ of M. Reorder it so that $\mathrm{LT}_{\sigma_0}(g_1^{(0)}) >_{\mathtt{PosLex}} \cdots >_{\mathtt{PosLex}} \mathrm{LT}_{\sigma_0}(g_{r_1}^{(0)})$.*
3) *Increase i by one. Let $\{\varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)}\}$ be the canonical basis of the graded free P-module $F_i = \bigoplus_{j=1}^{r_i} P(-\deg_W(g_j^{(i)}))$, and let σ_i be the module term ordering induced by $(\sigma_{i-1}, \mathcal{G}_{i-1})$ on $\mathbb{T}^n\langle\varepsilon_1, \ldots, \varepsilon_{r_i}^{(i)}\rangle$. Using Corollary 3.1.5, compute a σ_i-Gröbner basis $\mathcal{G}_i = (g_1^{(i)}, \ldots, g_{r_{i+1}}^{(i)})$ of $\mathrm{Syz}_P(\mathcal{G}_{i-1})$. Reorder it so that $\mathrm{LT}_{\sigma_i}(g_1^{(i)}) >_{\mathtt{PosLex}} \cdots >_{\mathtt{PosLex}} \mathrm{LT}_{\sigma_i}(g_{r_{i+1}}^{(i)})$.*
4) *If $r_{i+1} \neq 0$ and $i < n$, continue with step 2). Otherwise, let $j = 0$.*
5) *Compute a homogeneous minimal system of generators $\mathcal{G}_0'$ of M and a homogeneous matrix $\mathcal{A}_0$ such that $\mathcal{G}_0 = \mathcal{G}_0'\,\mathcal{A}_0$.*
6) *Increase j by one. Compute a homogeneous minimal system of generators $\mathcal{G}_j'$ of the module generated by the column vectors of $\mathcal{A}_{j-1}\,\mathcal{G}_j$ and a homogeneous matrix $\mathcal{A}_j$ satisfying $\mathcal{A}_{j-1}\,\mathcal{G}_j = \mathcal{G}_j'\,\mathcal{A}_j$.*
7) *If $\mathcal{A}_j\,\mathcal{G}_{j+1} \neq 0$, continue with step 6). Otherwise, let $\ell = j$, return $(\mathcal{G}_0', \ldots, \mathcal{G}_\ell')$ and stop.*

This is an algorithm which returns a tuple $(\mathcal{G}_0', \ldots, \mathcal{G}_\ell')$ of homogeneous matrices for which the P-linear maps $\varphi_j : F_j' \longrightarrow F_{j-1}'$ given by $\mathcal{G}_{j-1}'$ for $j = 1, \ldots, \ell$ yield a minimal graded free resolution

$$0 \longrightarrow F_\ell' \xrightarrow{\varphi_\ell} F_{\ell-1}' \xrightarrow{\varphi_{\ell-1}} \cdots \xrightarrow{\varphi_3} F_2' \xrightarrow{\varphi_2} F_1' \xrightarrow{\varphi_1} M \longrightarrow 0$$

Proof. Clearly, steps 2) and 3) correspond to the computation of the graded free resolution of M which is constructed in the proof of Theorem 4.8.4. It remains to show that steps 5) – 7) correspond to the repeated application of Theorem 4.8.6 in order to minimalize that resolution.

In step 5), we minimalize $\mathcal{G}_0$. By Theorem 4.8.6, we have to replace the syzygy matrix $\mathcal{G}_1$ by $\widetilde{\mathcal{G}}_1 = \mathcal{A}_0\mathcal{G}_1$. Next we want to minimalize the resolution

at the map defined by $\widetilde{\mathcal{G}}_1$. By Theorem 4.8.6, we have to compute a minimal homogeneous system of generators $\mathcal{G}'_1$ of $\langle \widetilde{\mathcal{G}}_1 \rangle$ and to replace the syzygy matrix $\mathcal{G}_2$ by $\widetilde{G}_2 = \mathcal{A}_1 \mathcal{G}_2$. If we continue in this way, Theorem 4.8.9 guarantees that we stop after at most n steps and arrive at the minimal graded free resolution of M. □

Remark 4.8.15. Although it is clear that we can use Explicit Membership 3.1.9 to compute the matrices $\mathcal{A}_0, \ldots, \mathcal{A}_\ell$ in steps 5) and 6) of the algorithm in the theorem, this does not appear to be an efficient method. One improvement is to perform the minimalization step-by-step as in Proposition 4.7.24 and to adjust the syzygy matrices accordingly. Another solution is to combine Corollary 4.6.5 with the book keeping technique of Proposition 2.5.11 .

The drawback of Schreyer's Algorithm is that the Gröbner bases defining the initial resolution may be very large. Then a huge number of minimalization steps is necessary and the algorithm becomes slow. However, experience shows that it performs well in many cases.

All good things come in threes.
(German Proverb)

Our third algorithm for computing minimal graded free resolutions generalizes the horizontal strategy for computing minimal homogeneous presentations (see Theorem 4.7.29). As before, we consider the entire computation as a computation in a large polynomial ring $\widetilde{P} = P[\varepsilon_1^{(0)}, \ldots, \varepsilon_{r_n}^{(n)}]$ a residue class ring of which is the idealization of $F_0 \oplus \cdots \oplus F_n$, and we identify all vectors with their images in $\widetilde{P}$. For the purposes of this theorem it will be convenient to replace the Division Algorithm 1.6.4 with a procedure that merely head reduces a given polynomial f with respect to a list of polynomials $\mathcal{G}$. We shall denote the result of such a reduction procedure by $\mathrm{HR}_{\sigma,\mathcal{G}}(f)$ and call it a **head reduction remainder** of f.

Theorem 4.8.16. (Computing Minimal Resolutions Horizontally) *Let M be a graded submodule of a graded free P-module $F_0 = \bigoplus_{i=1}^{r_0} P(-d_{0i})$ where $d_{0i} >_{\mathtt{Lex}} 0$ for $i = 1, \ldots, r_0$. Let $\mathcal{V} = (v_1, \ldots, v_s)$ be a deg-ordered tuple of non-zero homogeneous vectors which generate M. Consider the following sequence of instructions.*

1) *Let σ be a term ordering on $\mathbb{T}^n(\varepsilon_1^{(0)}, \ldots, \varepsilon_{r_0}^{(0)})$, let $\overline{P} = P[\varepsilon_1^{(0)}, \ldots, \varepsilon_{r_0}^{(0)}]$ be graded by $\overline{W} = (W \mid d_{01} \ \cdots \ d_{0r_0})$, let $r_1 = \cdots = r_n = 0$, let $B = \{v_1, \ldots, v_s\}$, let $\mathcal{G} = \emptyset$, and let $\mathcal{G}_{\min} = \emptyset$.*
2) *Let d be the smallest degree with respect to* Lex *of an element of B. Form the subset B_d of B and remove its entries from B.*
3) *If $B_d = \emptyset$, continue with step 7). Otherwise, let i be the largest upper index of an indeterminate $\varepsilon_k^{(j)}$ occurring in a polynomial of B_d. Let*

$f \in B_d$ be a polynomial which involves that indeterminate. Remove f from B_d.

4) *Compute $f' = \mathrm{HR}_{\sigma,\mathcal{G}}(f)$. If $i \geq 1$ and one of the indeterminates $\varepsilon_1^{(i-1)}, \ldots, \varepsilon_{r_{i-1}}^{(i-1)}$ occurs in f', append f' to $\mathcal{G}$, append to B all S-polynomials of f' and a polynomial g in $\mathcal{G}$ such that $\mathrm{LT}_\sigma(f')$ and $\mathrm{LT}_\sigma(g)$ involve the same indeterminate $\varepsilon_j^{(i-1)}$, and continue with step 3).*

5) *If none of the indeterminates $\{\varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)}\}$ occurs in f', continue with step 3).*

6) *Increase r_{i+1} by one. Adjoin a new indeterminate $\varepsilon_{r_{i+1}}^{(i+1)}$ to $\overline{P}$ and extend the grading to this new ring by defining $\deg_{\overline{W}}(\varepsilon_{r_{i+1}}^{(i+1)}) = d$. Extend the term ordering σ to the new ring in such a way that the extension is an elimination ordering for $\{\varepsilon_1^{(0)}, \ldots, \varepsilon_{r_i}^{(i)}\}$. Compute the polynomial*

$$\overline{f} = f'(x_1, \ldots, x_n, \varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)}, 0, \ldots, 0)$$

Append $g = \overline{f} - \varepsilon_{r_{i+1}}^{(i+1)}$ to $\mathcal{G}$ and $\overline{f}$ to $\mathcal{G}_{\min}$. For all $h \in B$ such that $\mathrm{LT}_\sigma(g)$ and $\mathrm{LT}_\sigma(h)$ involve the same indeterminate $\varepsilon_j^{(i)}$, compute the S-polynomial of g and h and append it to B. Then continue with step 3).

7) *If $B = \emptyset$, return the tuple $\mathcal{G}_{\min}$ and stop. Otherwise, continue with step 2).*

This is an algorithm which computes a deg-ordered tuple $\mathcal{G}_{\min}$ of homogeneous polynomials in $\overline{P} = P[\varepsilon_1^{(0)}, \ldots, \varepsilon_{r_0}^{(0)}, \ldots, \varepsilon_1^{(\ell)}, \ldots, \varepsilon_{r_\ell}^{(\ell)}]$ for which the homogeneous maps of graded free P-modules $\varphi_i : F_i \longrightarrow F_{i-1}$ defined by the elements of $\mathcal{G} \cap P[\varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)}]$ yield a minimal graded free resolution

$$0 \longrightarrow F_\ell \xrightarrow{\varphi_\ell} F_{\ell-1} \xrightarrow{\varphi_{\ell-1}} \cdots \xrightarrow{\varphi_3} F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} M \longrightarrow 0$$

Proof. First we prove that the procedure is well-defined, i.e. that all instructions can be executed. For this purpose it suffices to show the following claim: For a polynomial f which is contained in B or in $\mathcal{G}$ at some point during the computation, there exists a number $i \geq 0$ such that f is of the shape

$$f = a_1\varepsilon_1^{(i)} + \cdots + a_{r_i}\varepsilon_{r_i}^{(i)} + b_1\varepsilon_1^{(i+1)} + \cdots + b_{r_{i+1}}\varepsilon_{r_{i+1}}^{(i+1)}$$

with $a_j, b_k \in P$. This is clearly the case at the outset when $v_1, \ldots, v_s$ involve only the indeterminates $\varepsilon_1^{(0)}, \ldots, \varepsilon_{r_0}^{(0)}$. Later B and $\mathcal{G}$ are enlarged only in steps 4) and 6).

When $f' = \mathrm{HR}_{\sigma,\mathcal{G}}(f)$ is appended to $\mathcal{G}$ in step 4), the element $f \in B$ has been head reduced using only elements of the shape shown above. Thus also f' has this shape. When $g = \overline{f'} - \varepsilon_{r_{i+1}}^{(i+1)}$ is appended to $\mathcal{G}$ in step 6), the element f' involves only indeterminates $\varepsilon_k^{(j)}$ with upper index $j \in \{i, i+1\}$. Consequently, the polynomial $\overline{f'} = f'(x_1, \ldots, x_n, \varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)}, 0, \ldots, 0)$ involves only indeterminates $\varepsilon_k^{(j)}$ with upper index $j = i$, and so g has the

claimed shape. When B is enlarged in step 4) or 6), the new elements are S-polynomials of polynomials of the claimed shape. By the construction of σ, the leading term of a polynomial involves one of the indeterminates $\varepsilon_k^{(j)}$ with the smaller of the two upper indices. Since both leading terms are required to involve the same indeterminate $\varepsilon_k^{(j)}$, it follows that the S-polynomials appended to B have the claimed shape, and the claim is proved.

Now we turn to proving finiteness and correctness of the procedure. The procedure stops when B becomes empty. New S-polynomials are appended to B in step 4) or 6) only if a new element is appended to $\mathcal{G}$ in the same step. The new element of $\mathcal{G}$ has a leading term which is not contained in the ideal generated by $\mathrm{LT}_\sigma(\mathcal{G})$. Hence finiteness will follow if we can show that only finitely many new indeterminates $\varepsilon_{r_{i+1}}^{(i+1)}$ are introduced in step 6).

To prove this and the correctness of the algorithm, it is sufficient to prove the following claim by induction on i: After finitely many steps, all elements $f \in B$ involving indeterminates $\varepsilon_k^{(i)}$ with upper index i have been treated, and at that point the tuple $\mathcal{G}_i = \mathcal{G}_{\min} \cap P[\varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)}]$ is a minimal system of generators of $\mathrm{Syz}(\mathcal{G}_{i-1})$. To this end, we set $\varepsilon_k^{(j)} \mapsto 0$ for $j > i$ everywhere and show that the resulting algorithm reduced to the horizontal strategy for computing minimal homogeneous presentations (see Theorem 4.7.29). The choice of f in step 3) ensures that S-polynomials involving only the indeterminates $\varepsilon_1^{(i)}, \ldots, \varepsilon_{r_i}^{(i)}$ are treated first. This corresponds to doing the loop in steps 3) – 5) before the loops in steps 6) – 9) and 10) – 12) in Theorem 4.7.29. The fact that we replaced the normal remainder computation by a head reduction remainder does not affect the correctness of the algorithm by Remark 2.5.6.a. The elements $f \in B$ which produce an f' appended to $\mathcal{G}$ in step 4) correspond to the pairs treated in steps 6) – 9) in Theorem 4.7.29. The elements f' discarded by step 5) correspond to the vectors v' discarded in step 11) in Theorem 4.7.29. Finally, step 6) corresponds to step 12) in Theorem 4.7.29. Altogether, it follows inductively from Theorem 4.7.29 that the algorithm is correct. In particular, by Theorem 4.8.9, the tuple $\mathcal{G}_{\min}$ is finite and the computation stops after finitely many steps. □

The preceding algorithm admits several further optimizations.

Remark 4.8.17. Suppose that we are in the setting of the theorem.

a) Because of the checks performed in steps 4) and 5), the procedure $\mathrm{HR}_{\sigma,\mathcal{G}}(f)$ can stop when all indeterminates $\varepsilon_k^{(i-1)}, \varepsilon_\ell^{(i)}$ are eliminated from f.

b) Let W be a matrix of non-negative integers. Then the head reduction procedure can be further optimized by noting that a polynomial f can be head reduced by $g \in \mathcal{G}$ only if $\deg_{\overline{W}}(f)$ is componentwise larger than or equal to $\deg_{\overline{W}}$. For instance, a homogeneous polynomial f of degree $\binom{4}{3}$ cannot be reduced by a homogeneous polynomial of degree $\binom{3}{4}$. This observation restricts the set of possible reductors in $\mathcal{G}$.

Last, but not least, we now apply the horizontal strategy for computing minimal resolutions to the module discussed in Examples 4.7.28 and 4.8.13.

Example 4.8.18. Let $P = \mathbb{Q}[x_1, x_2, x_3, x_4]$ be graded by $W = \left(\begin{smallmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 3 & 4 \end{smallmatrix}\right)$, and let M be the graded P-submodule of $F_0 = P(-\binom{1}{0})$ generated by the homogeneous tuple $\mathcal{V} = (f_1\varepsilon_1^{(0)}, f_2\varepsilon_1^{(0)}, f_3\varepsilon_1^{(0)}, f_4\varepsilon_1^{(0)})$, where $f_1 = x_1x_4 - x_2x_3$, $f_2 = x_1^2x_3 - x_2^3$, $f_3 = x_1x_3^2 - x_2^2x_4$, $f_4 = x_2x_4^2 - x_3^3$, and $\varepsilon_1^{(0)}$ is the canonical basis vector of F_0. Thus we have $\deg_W(f_1\varepsilon_1^{(0)}) = \binom{3}{4}$, $\deg_W(f_2\varepsilon_1^{(0)}) = \binom{4}{3}$, $\deg_W(f_3\varepsilon_1^{(0)}) = \binom{4}{6}$, and $\deg_W(f_4\varepsilon_1^{(0)}) = \binom{4}{9}$. We always choose σ to be the lexicographic term ordering which satisfies

$$\varepsilon_1^{(0)} >_\sigma \varepsilon_1^{(1)} >_\sigma \cdots >_\sigma \varepsilon_{r_1}^{(1)} >_\sigma \cdots >_\sigma \varepsilon_1^{(i)} >_\sigma \cdots >_\sigma \varepsilon_{r_i}^{(i)} >_\sigma x_1 >_\sigma \cdots >_\sigma x_n$$

O.k., now let's get going, not shopping!

1) Let $\overline{P} = P[\varepsilon_1^{(0)}]$ be graded by $\overline{W} = (W \mid \binom{1}{0})$, let $B = \{f_1\varepsilon_1^{(0)}, f_2\varepsilon_1^{(0)}, f_3\varepsilon_1^{(0)}, f_4\varepsilon_1^{(0)}\}$, let $\mathcal{G} = \emptyset$, and let $\mathcal{G}_{\min} = \emptyset$.
2) Let $d = \binom{3}{4}$, $B_d = \{f_1\varepsilon_1^{(0)}\}$, and $B = \{f_2\varepsilon_1^{(0)}, f_3\varepsilon_1^{(0)}, f_4\varepsilon_1^{(0)}\}$.
3) Let $i = 0$, $f = f_1\varepsilon_1^{(0)}$, and $B_d = \emptyset$.
4) Compute $f' = \mathrm{HR}_{\sigma,\mathcal{G}}(f) = f$.
6) Let $r_1 = 1$. Adjoin $\varepsilon_1^{(1)}$ to $\overline{P}$. Extend the grading by $\deg_{\overline{W}}(\varepsilon_1^{(1)}) = \binom{3}{4}$. Let $\bar{g}_1 = f'$, $g_1 = \bar{g}_1 - \varepsilon_1^{(1)}$, $\mathcal{G} = (g_1)$, and $\mathcal{G}_{\min} = (\bar{g}_1)$.
2) Let $d = \binom{4}{3}$, $B_d = \{f_2\varepsilon_1^{(0)}\}$, and $B = \{f_3\varepsilon_1^{(0)}, f_4\varepsilon_1^{(0)}\}$.
3) Let $i = 0$, $f = f_2\varepsilon_1^{(0)}$, and $B_d = \emptyset$.
4) Compute $f' = \mathrm{HR}_{\sigma,\mathcal{G}}(f) = f$.
6) Let $r_1 = 2$. Adjoin $\varepsilon_2^{(1)}$ to $\overline{P}$. Extend the grading by $\deg_{\overline{W}}(\varepsilon_2^{(1)}) = \binom{4}{3}$. Let $\bar{g}_2 = f'$, $g_2 = \bar{g}_2 - \varepsilon_2^{(1)}$, $\mathcal{G} = (g_1, g_2)$, and $\mathcal{G}_{\min} = (\bar{g}_1, \bar{g}_2)$. Append $S_{12} = x_1x_3g_1 - x_4g_4$ to B and note that $\deg_{\overline{W}}(S_{12}) = \binom{5}{7}$.
2) Let $d = \binom{4}{6}$, $B_d = \{f_3\varepsilon_1^{(0)}\}$, and $B = \{f_4\varepsilon_1^{(0)}, S_{12}\}$.
3) Let $i = 0$, $f = f_3\varepsilon_1^{(0)}$, and $B_d = \emptyset$.
4) Compute $f' = \mathrm{HR}_{\sigma,\mathcal{G}}(f) = f$.
6) Let $r_1 = 3$. Adjoin $\varepsilon_3^{(1)}$ to $\overline{P}$. Extend the grading by $\deg_{\overline{W}}(\varepsilon_3^{(1)}) = \binom{4}{6}$. Let $\bar{g}_3 = f'$, $g_3 = \bar{g}_3 - \varepsilon_3^{(1)}$, $\mathcal{G} = (g_1, g_2, g_3)$, and $\mathcal{G}_{\min} = (\bar{g}_1, \bar{g}_2, \bar{g}_3)$. Append $S_{13} = x_3^2g_1 - x_4g_3$ and $S_{23} = x_3g_2 - x_1g_3$ to B. Note that $\deg_{\overline{W}}(S_{13}) = \binom{5}{10}$ and $\deg_{\overline{W}}(S_{23}) = \binom{5}{6}$.
2) Let $d = \binom{4}{9}$, $B_d = \{f_4\varepsilon_1^{(0)}\}$, and $B = \{S_{23}, S_{12}, S_{13}\}$.
3) Let $i = 0$, $f = f_4\varepsilon_1^{(0)}$, and $B_d = \emptyset$.
4) Compute $f' = \mathrm{HR}_{\sigma,\mathcal{G}}(f) = f$.
6) Let $r_1 = 4$. Adjoin $\varepsilon_4^{(1)}$ to $\overline{P}$. Extend the grading by $\deg_{\overline{W}}(\varepsilon_4^{(1)}) = \binom{4}{9}$. Let $\bar{g}_4 = f'$, $g_4 = \bar{g}_4 - \varepsilon_4^{(1)}$, $\mathcal{G} = (g_1, \ldots, g_4)$, and $\mathcal{G}_{\min} = (\bar{g}_1, \ldots, \bar{g}_4)$. Append $S_{14} = x_2x_4g_1 - x_1g_4$, $S_{24} = x_2x_4^2g_2 - x_1^2x_3g_4$, and $S_{34} =$

$x_2x_4^2g_3 - x_1x_3^2g_4$ to B. Note that $\deg_{\overline{W}}(S_{14}) = \binom{5}{9}$, $\deg_{\overline{W}}(S_{24}) = \binom{7}{12}$, and $\deg_{\overline{W}}(S_{34}) = \binom{7}{15}$.

2) Let $d = \binom{5}{6}$, $B_d = \{S_{23}\}$, and $B = \{S_{12}, S_{14}, S_{13}, S_{24}, S_{34}\}$.
3) Let $i = 1$, $f = S_{23}$, and $B_d = \emptyset$.
4) Compute $f' = \mathrm{HR}_{\sigma,\mathcal{G}}(S_{23}) = S_{23} - x_2^2g_1 = x_2^2\varepsilon_1^{(1)} - x_3\varepsilon_2^{(1)} - x_3\varepsilon_3^{(1)} + x_1\varepsilon_4^{(1)}$. Notice that $\varepsilon_1^{(0)}$ does not occur in f'.
6) Let $r_2 = 1$. Adjoin $\varepsilon_1^{(2)}$ to $\overline{P}$. Extend the grading by $\deg_{\overline{W}}(\varepsilon_1^{(2)}) = \binom{5}{6}$. Let $\bar{g}_5 = f'$, $g_5 = \bar{g}_5 - \varepsilon_1^{(2)}$, $\mathcal{G} = (g_1, \ldots, g_5)$, and $\mathcal{G}_{\min} = (\bar{g}_1, \ldots, \bar{g}_5)$. No S-polynomial is appended to B.
2) Let $d = \binom{5}{7}$, $B_d = \{S_{12}\}$, and $B = \{S_{14}, S_{13}, S_{24}, S_{34}\}$.
3) Let $i = 1$, $f = S_{12}$, and $B_d = \emptyset$.
4) Compute $f' = S_{12} + x_2g_3 = -x_1x_3\varepsilon_1^{(1)} + x_4\varepsilon_2^{(1)} - x_2\varepsilon_3^{(1)}$.
6) Let $r_2 = 2$. Adjoin $\varepsilon_2^{(2)}$ to $\overline{P}$. Extend the grading by $\deg_{\overline{W}}(\varepsilon_2^{(2)}) = \binom{5}{7}$. Let $\bar{g}_6 = f'$, $g_6 = \bar{g}_6 - \varepsilon_2^{(2)}$, $\mathcal{G} = (g_1, \ldots, g_6)$, and $\mathcal{G}_{\min} = (\bar{g}_1, \ldots, \bar{g}_6)$. Append $S_{56} = x_1x_3g_5 + x_2^2g_6$ to B. Note that $\deg_{\overline{W}}(S_{56}) = \binom{7}{9}$.
2) Let $d = \binom{5}{9}$, $B_d = \{S_{14}\}$, and $B = \{S_{13}, S_{56}, S_{24}, S_{34}\}$.
3) Let $i = 1$, $f = S_{14}$, and $B_d = \emptyset$.
4) Compute $f' = S_{14} - x_3g_3 = -x_2x_4\varepsilon_1^{(1)} + x_2\varepsilon_3^{(1)} + x_1\varepsilon_4^{(1)}$.
6) Let $r_2 = 3$. Adjoin $\varepsilon_3^{(2)}$ to $\overline{P}$. Extend the grading by $\deg_{\overline{W}}(\varepsilon_3^{(2)}) = \binom{5}{9}$. Let $\bar{g}_7 = f'$, $g_7 = \bar{g}_7 - \varepsilon_3^{(2)}$, $\mathcal{G} = (g_1, \ldots, g_7)$, and $\mathcal{G}_{\min} = (\bar{g}_1, \ldots, \bar{g}_7)$. Append $S_{57} = x_4g_5 + x_2g_7$ and $S_{67} = x_2x_4g_6 - x_1x_3g_7$ to B. Note that $\deg_{\overline{W}}(S_{57}) = \binom{6}{10}$ and $\deg_{\overline{W}}(S_{67}) = \binom{7}{12}$.
2) Let $d = \binom{5}{10}$, $B_d = \{S_{13}\}$, and $B = \{S_{57}, S_{56}, S_{24}, S_{67}, S_{34}\}$.
3) Let $i = 1$, $f = S_{13}$, and $B_d = \emptyset$.
4) Compute $f' = S_{13} - x_2g_4 = -x_3^2\varepsilon_1^{(1)} + x_4\varepsilon_3^{(1)} + x_2\varepsilon_4^{(1)}$.
6) Let $r_2 = 4$. Adjoin $\varepsilon_4^{(2)}$ to $\overline{P}$. Extend the grading by $\deg_{\overline{W}}(\varepsilon_4^{(2)}) = \binom{5}{10}$. Let $\bar{g}_8 = f'$, $g_8 = \bar{g}_8 - \varepsilon_4^{(2)}$, $\mathcal{G} = (g_1, \ldots, g_8)$, and $\mathcal{G}_{\min} = (\bar{g}_1, \ldots, \bar{g}_8)$. Append $S_{58} = x_3^2g_5 + x_2^2g_8$, $S_{68} = x_3g_6 - x_1g_8$, and $S_{78} = x_3^2g_7 - x_2x_4g_8$ to B. Note $\deg_{\overline{W}}(S_{58}) = \binom{7}{12}$, $\deg_{\overline{W}}(S_{68}) = \binom{6}{10}$, and $\deg_{\overline{W}}(S_{78}) = \binom{7}{15}$.
2) Let $d = \binom{6}{10}$, $B_d = \{S_{57}, S_{68}\}$, and $B = \{S_{56}, S_{24}, S_{67}, S_{58}, S_{34}, S_{78}\}$.
3) Let $i = 2$, $f = S_{57}$, and $B_d = \{S_{68}\}$.
4) Compute $f' = \mathrm{HR}_{\sigma,\mathcal{G}}(f) = S_{57}$. Observe that this polynomial involves $\varepsilon_2^{(1)}$ with upper index $i - 1$. Append $g_9 = S_{57}$ to $\mathcal{G}$.
3) Let $i = 2$, $f = S_{68}$, and $B_d = \emptyset$.
4) Compute $f' = S_{68} + g_9 = -x_4\varepsilon_1^{(2)} - x_3\varepsilon_2^{(2)} - x_2\varepsilon_3^{(2)} + x_1\varepsilon_4^{(2)}$.
6) Let $r_3 = 1$. Adjoin $\varepsilon_1^{(3)}$ to $\overline{P}$. Extend the grading by $\deg_{\overline{W}}(\varepsilon_1^{(3)}) = \binom{6}{10}$. Let $\bar{g}_{10} = f'$, $g_{10} = \bar{g}_{10} - \varepsilon_1^{(3)}$, $\mathcal{G} = (g_1, \ldots, g_{10})$, and notice that we have to set $\mathcal{G}_{\min} = (\bar{g}_1, \ldots, \bar{g}_8, \bar{g}_{10})$.
2) Let $d = \binom{7}{9}$, $B_d = \{S_{56}\}$, and $B = \{S_{24}, S_{67}, S_{58}, S_{34}, S_{78}\}$.
3) Let $i = 2$, $f = S_{56}$, and $B_d = \emptyset$.

4) Compute $f' = \mathrm{HR}_{\sigma,\mathcal{G}}(f) = S_{56}$. Append $g_{11} = S_{56}$ to $\mathcal{G}$. Append $S_{9\,11} = x_1x_3g_9 - x_4g_{11}$ to B. Note that $\deg_{\overline{W}}(S_{9\,11}) = \binom{8}{13}$.
2) Let $d = \binom{7}{12}$, $B_d = \{S_{24}, S_{67}, S_{58}\}$, and $B = \{S_{34}, S_{78}, S_{9\,11}\}$.
3) Let $i = 2$, $f = S_{67}$, and $B_d = \{S_{24}, S_{58}\}$. (Notice that we may not choose $f = S_{24}$ here.)
4) Compute $f' = \mathrm{HR}_{\sigma,\mathcal{G}}(f) = S_{67}$. Append $g_{12} = S_{67}$ to $\mathcal{G}$. Append $S_{9\,12} = x_2x_4g_9 + x_3g_{12}$ and $S_{11,\,12} = x_2x_4^2g_{11} - x_1x_3^2g_{12}$ to B. Note that $\deg_{\overline{W}}(S_{9\,12}) = \binom{8}{15}$ and $\deg_{\overline{W}}(S_{11\,12}) = \binom{10}{18}$.
3) Let $i = 2$, $f = S_{58}$, and $B_d = \{S_{24}\}$.
4) Compute $f' = \mathrm{HR}_{\sigma,\mathcal{G}}(f) = S_{58}$. Append $g_{13} = S_{58}$ to $\mathcal{G}$. Append $S_{9\,13} = x_3^2g_9 - x_4g_{13}$, $S_{11\,13} = x_3g_{11} + x_1g_{13}$, and $S_{12\,13} = x_3^3g_{12} + x_2x_4^2g_{13}$ to B. Note that $\deg_{\overline{W}}(S_{9\,13}) = \binom{8}{16}$, $\deg_{\overline{W}}(S_{11\,13}) = \binom{8}{12}$, and $\deg_{\overline{W}}(S_{12\,13}) = \binom{10}{21}$.
2) Let $d = \binom{7}{15}$, $B_d = \{S_{34}, S_{78}\}$, and $B = \{S_{11\,13}, S_{9\,11}, S_{9\,12}, S_{11\,12}, S_{12\,13}\}$.
3) Let $i = 2$, $f = S_{78}$, and $B_d = \{S_{34}\}$.
4) Compute $f' = \mathrm{HR}_{\sigma,\mathcal{G}}(f) = S_{78}$. Append $g_{14} = S_{78}$ to $\mathcal{G}$. No new S-polynomials are appended to B.
3) Let $i = 1$, $f = S_{34}$, and $B_d = \emptyset$.
4) Compute $f' = \mathrm{HR}_{\sigma,\mathcal{G}}(f) = 0$.

Here we stop tracing through the computation. All the elements of B of higher degree head reduce to zero. After that the algorithm stops and returns the result $\mathcal{G}_{\min} = (\bar{g}_1, \ldots, \bar{g}_8, \bar{g}_{10})$. When we sort the polynomials in $\mathcal{G}_{\min}$ according to the upper indices of their indeterminates $\varepsilon_k^{(j)}$, we get the tuples $\mathcal{G}_0 = (\bar{g}_1, \bar{g}_2, \bar{g}_3, \bar{g}_4) = (f_1\varepsilon_1^{(0)}, f_2\varepsilon_1^{(0)}, f_3\varepsilon_1^{(0)}, f_4\varepsilon_1^{(0)})$, $\mathcal{G}_1 = (\bar{g}_5, \bar{g}_6, \bar{g}_7, \bar{g}_8)$, and $\mathcal{G}_2 = (\bar{g}_{10})$. Thus we have calculated a minimal graded free resolution

$$0 \longrightarrow P\big(-\tbinom{6}{10}\big) \xrightarrow{\lambda} P\big(-\tbinom{5}{6}\big) \oplus P\big(-\tbinom{5}{7}\big) \oplus P\big(-\tbinom{5}{9}\big) \oplus P\big(-\tbinom{5}{10}\big) \xrightarrow{\psi}$$
$$\xrightarrow{\psi} P\big(-\tbinom{3}{4}\big) \oplus P\big(-\tbinom{4}{3}\big) \oplus P\big(-\tbinom{4}{6}\big) \oplus P\big(-\tbinom{4}{9}\big) \xrightarrow{\varphi} M \longrightarrow 0$$

where the maps φ, ψ, and λ are given by the matrices $\mathcal{G}_0$, $\mathcal{G}_1$, and $\mathcal{G}_2$, respectively. Wow! We have got the same result as in Example 4.8.13!

Exercise 1. Let K be a field and $R = K[x]/(x^2)$. We equip R with the grading induced by the standard grading on $K[x]$. Find the minimal graded free R-resolution of the homogeneous ideal $I = (x)$ in R.

Exercise 2. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let M be a finitely generated graded P-module. Given two homogeneous tuples $\mathcal{G} = (g_1, \ldots, g_r)$ and $\mathcal{H} = (h_1, \ldots, h_s)$ of non-zero elements which generate M, we let $F = \bigoplus_{i=1}^{r} P(-\deg_W(g_i))$ and $F' = \bigoplus_{j=1}^{s} P(-\deg_W(h_j))$.

a) **(Graded Version of Schanuel's Lemma)** Prove that there exists an isomorphism of graded P-modules $\mathrm{Syz}_P(\mathcal{G}) \oplus F' \cong F \oplus \mathrm{Syz}_P(\mathcal{G}')$. *Hint:* Let $\mathcal{A}, \mathcal{B}$ be homogeneous matrices such that $\mathcal{G} = \mathcal{G}'\mathcal{A}$ and $\mathcal{G}' = \mathcal{G}\mathcal{B}$. Then consider $\varrho(v, w) = (v + \mathcal{B}w,\ w - \mathcal{A}(v + \mathcal{B}w))$ and $\varrho'(v, w) = (v - \mathcal{B}(w + \mathcal{A}v), w + \mathcal{A}v)$.
b) Using a), show that there is an isomorphism of graded P-modules $\mathrm{Syz}_P(\mathcal{G}) \cong \mathrm{Syz}_P(\mathcal{G}')$ if $\mathcal{G}$ and $\mathcal{G}'$ are minimal systems of generators of M.
c) Give a new proof for the uniqueness of the minimal graded free resolution of M (see Theorem 4.8.9).

Exercise 3. Let K be a field, and let $P = K[x, y, z]$ be standard graded. Find a minimal graded free resolution of the graded P-module $K \cong P/(x, y, z)$.
Repeat this exercise with four, five or more indeterminates. Can you guess the general shape of the minimal graded free resolution?

Exercise 4. Let $P = \mathbb{Q}[x, y, z]$ be standard graded. Compute the minimal graded free resolution of the ideal $I = (x^2,\ x(y + z),\ y^2)$ using

a) the vertical strategy (see Proposition 4.8.11),
b) Schreyer's algorithm (see Proposition 4.8.14), and
c) the horizontal strategy (see Theorem 4.8.16).

Exercise 5. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let $f_1, f_2 \in P$ be non-zero homogeneous polynomials, and let $I = (f_1, f_2)$. Show that the graded Betti numbers of P/I are uniquely determined by $\deg(f_1)$, $\deg(f_2)$, and $\deg(\gcd(f_1, f_2))$.

Exercise 6. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded, and let I be a homogeneous ideal in P. Find the graded Betti numbers of $P \oplus I$ in terms of the graded Betti numbers of I.

Exercise 7. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $f_1, f_2, f_3 \in P$ be homogeneous polynomials which form a regular sequence, and let $d_i = \deg_W(f_i)$ for $i = 1, 2, 3$. Show that the graded free resolution of the ideal $I = (f_1, f_2, f_3)$ has the shape

$$0 \longrightarrow P(-d_1 - d_2 - d_3) \xrightarrow{\varphi} P(-d_1 - d_2) \oplus P(-d_2 - d_3) \oplus P(-d_1 - d_3) \longrightarrow$$
$$\xrightarrow{\psi} P(-d_1) \oplus P(-d_2) \oplus P(-d_3) \xrightarrow{\varepsilon} I \longrightarrow 0$$

and determine the matrices defining the maps φ and ψ.

Exercise 8. Let K be a field, let $P = K[x_1, x_2, x_3]$ be graded by $\mathcal{I}_3$, and let $I = (x_1x_2, x_2x_3, x_1x_3)$. Compute the minimal graded free resolution of I with respect to this grading.

Tutorial 62: The Hilbert-Burch Theorem

Is this the real McCoy?

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let I be a proper homogeneous ideal in P. In this section we proved that the length ℓ of the minimal graded free resolution of P/I satisfies $\ell \in \{1, \ldots, n\}$. It is easy to see that this length is one if and only if I is a principal ideal. Thus the first non-trivial case occurs when $\ell = 2$. In this tutorial we guide you through a structure theorem for such ideals. More precisely, let $\mathcal{G}$ be a minimal homogeneous system of generators of I. You will prove that $\mathcal{G}$ is (up to signs) a multiple of the tuple of maximal minors of a homogeneous matrix of size $r \times (r-1)$, and that this matrix is the syzygy matrix of $\mathcal{G}$. The first ingredient of this proof is the following linear algebra result.

a) **(McCoy's Theorem)** Let R be a ring, let $1 \leq r \leq s$, and let an R-linear map $\varphi : R^r \longrightarrow R^s$ be given by a matrix $\mathcal{M} \in \mathrm{Mat}_{s,r}(R)$. For every $1 \leq i \leq r$ we denote the ideal generated by the $i \times i$-minors of $\mathcal{M}$ by I_i. Show that the following conditions are equivalent.

   1) The homomorphism φ is injective.
   2) We have $\mathrm{Ann}_R(I_1) = \mathrm{Ann}_R(I_2) = \cdots = \mathrm{Ann}_R(I_r) = 0$.
   3) We have $\mathrm{Ann}_R(I_r) = (0)$.

   Hint: To prove "1)⇒2)", assume that $\mathrm{Ann}_R(I_q) = 0$ and $\mathrm{Ann}_R(I_{q+1}) \neq 0$ for some $q \in \{1, \ldots, r-1\}$. Let $f \in \mathrm{Ann}_R(I_{q+1}) \setminus \{0\}$. W.l.o.g. let $fd \neq 0$ for the minor d defined by the first q rows and columns of $\mathcal{M}$. Now let $\mathcal{N}$ be the submatrix of $\mathcal{M}$ consisting of the first $q+1$ rows and q columns, and let $d_1, \ldots, d_{q+1}$ be the maximal minors of $\mathcal{N}$. Show that $(fd_1, -fd_2, \ldots, \pm fd_{q+1}, 0, \ldots, 0)$ is a non-zero element of $\mathrm{Ker}(\varphi)$.
   To prove "3)⇒1)", use Dedekind's Lemma (see Exercise 4 in Section 4.7).

In the following we let I be a homogeneous ideal in P whose minimal graded free resolution has the form

$$0 \longrightarrow \bigoplus_{i=1}^{r-1} P(-d_{1i}) \xrightarrow{\psi} \bigoplus_{j=1}^{r} P(-d_{0j}) \xrightarrow{\varphi} I \longrightarrow 0$$

Let $\mathcal{G} = (g_1, \ldots, g_r)$ and $\mathcal{S} = (v_1, \ldots, v_{r-1})$ be the homogeneous matrices defining φ and ψ, respectively.

c) For $i \in \{1, \ldots, r\}$, let $\mathcal{S}_i$ be the matrix obtained by deleting the i^{th} row of $\mathcal{S}$. Use a) to show that there is an index i such that $\det(\mathcal{S}_i) \neq 0$.

d) Let L be the field of rational functions $L = K(x_1, \ldots, x_n)$. For the L-linear map $\tilde{\psi} : L^r \longrightarrow L^{r-1}$ given by $\mathcal{S}^{\mathrm{tr}}$, prove

$$\mathrm{Ker}(\tilde{\psi}) = L \cdot (\det(\mathcal{S}_1), -\det(\mathcal{S}_2), \ldots, (-1)^{r-1} \det(\mathcal{S}_r))$$

e) Using c), show that $g_i \det(\mathcal{S}_j) = (-1)^{i-j} g_j \det(\mathcal{S}_i)$ for $i, j \in \{1, \ldots, r\}$.

f) Assume that $f = \det(S_1) \neq 0$. Show that the P-linear map

$$\overline{\psi} : \bigoplus_{i=1}^{r-1} P/(f)(-d_{1i}) \longrightarrow \bigoplus_{j=1}^{r} P/(f)(-d_{0j})$$

induced by ψ is injective.
Hint: Assume that $u \in \bigoplus_{i=1}^{r-1} P(-d_{1i})$ satisfies $\overline{\psi}(\bar{u}) = 0$. There exists a vector w such that $\psi(u) = fw$. Hence $0 = \varphi(\psi(u)) = \varphi(fw) = f\varphi(w)$ implies $\varphi(w) = 0$.

g) Prove that $\mathcal{G}$ is a multiple of $(\det(\mathcal{S}_1), -\det(\mathcal{S}_2), \ldots, (-1)^{r-1}\det(\mathcal{S}_r))$.
Hint: Assume that $f = \det(S_1) \neq 0$. Let $\bar{I}_{r-1}$ be the ideal in $P/(f)$ generated by the maximal minors of the matrix $\overline{\mathcal{S}}$. Using d), deduce $\bar{g}_1 \in \mathrm{Ann}_{P/(f)}(\bar{I}_{r-1})$. Now apply a).

h) Find an example where $\mathcal{G}$ is a proper multiple of the tuple

$$(\det(\mathcal{S}_1), -\det(\mathcal{S}_2), \ldots, (-1)^{r-1}\det(\mathcal{S}_r))$$

i) Suppose that $\mathcal{G}$ is deg-ordered and that $\deg(g_1) = r - 1$. Prove that $\deg(g_2) = \cdots = \deg(g_r)$.

j) Let $\mathcal{M} = (m_{ij}) \in \mathrm{Mat}_{3,2}(\mathbb{Z})$ be a matrix with positive entries such that $m_{11} + m_{22} = m_{12} + m_{21}$ and $m_{11} + m_{32} = m_{12} + m_{31}$. Show that there exists a homogeneous ideal $I \subseteq K[x_1, \ldots, x_6]$ whose minimal graded free resolution has the form given above and whose graded Betti numbers are $d_{01} = m_{21} + m_{32}$, $d_{02} = m_{11} + m_{32}$, $d_{03} = m_{11} + m_{22}$, $d_{11} = m_{11} + m_{21} + m_{32}$, and $d_{12} = m_{12} + m_{21} + m_{32}$.
Hint: Consider the matrix $\begin{pmatrix} x_1^{m_{11}} & x_2^{m_{21}} & x_3^{m_{31}} \\ x_4^{m_{12}} & x_5^{m_{22}} & x_6^{m_{32}} \end{pmatrix}^{\mathrm{tr}}$. Find a term ordering such that its three maximal minors are a Gröbner basis.

Tutorial 63: Computing Some Graded Betti Numbers

The most important information contained in a minimal graded free resolution of a module are its graded Betti numbers. In this tutorial we want to implement algorithms for computing minimal graded free resolutions and graded Betti numbers. A particularly efficient way to display all graded Betti numbers is the graded Betti diagram which we define and study below.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be graded by $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let $F_0 = \bigoplus_{i=1}^{r_0} P(-d_{0i})$ where $d_{01}, \ldots, d_{0r_0} \in \mathbb{Z}^m$. We denote the canonical basis of F_0 by $\{\varepsilon_1^{(0)}, \ldots, \varepsilon_{r_0}^{(0)}\}$. Let $\mathcal{V} = (v_1, \ldots, v_s)$ be a tuple of non-zero homogeneous vectors in F_0, and let M be the graded submodule of F_0 generated by $\mathcal{V}$. The minimal graded free resolution of M has the shape

$$0 \to \bigoplus_{d \in \mathbb{Z}^m} P(-d)^{\beta_{nd}} \to \cdots \to \bigoplus_{d \in \mathbb{Z}^m} P(-d)^{\beta_{1d}} \to \bigoplus_{d \in \mathbb{Z}^m} P(-d)^{\beta_{0d}} \to M \to 0$$

where the numbers β_{ij} are the graded Betti numbers of M.

a) Write a CoCoA function `BettiNo(...)` which takes $\mathcal{V}$ and uses the built-in CoCoA routines to compute a list of lists which contains the graded Betti numbers of M.

b) Using your function `BettiNo(...)`, compute the graded Betti numbers of the following modules.

1) $M_1 = \langle (x_1x_4 - x_2x_3)\,\varepsilon_1^{(0)},\ (x_1^2x_3 - x_2^3)\,\varepsilon_1^{(0)},\ (x_1x_3^2 - x_2^2x_4)\,\varepsilon_1^{(0)},\ (x_2x_4^2 - x_3^3)\,\varepsilon_1^{(0)}\rangle \subseteq P\big(-\binom{1}{0}\big)$ where $P = \mathbb{Q}[x_1, x_2, x_3, x_4]$ is graded by the matrix $W = \left(\begin{smallmatrix}1&1&1&1\\0&1&3&4\end{smallmatrix}\right)$ (see Examples 4.8.13 and 4.8.18)
2) $M_2 = \langle x_1\varepsilon_1^{(0)}, \ldots, x_5\varepsilon_1^{(0)}\rangle \subseteq P\big(-\binom{2}{3}\big)$ where $P = \mathbb{Q}[x_1, \ldots, x_5]$ is graded by $W = \left(\begin{smallmatrix}1&1&1&1&1\\1&2&3&4&5\end{smallmatrix}\right)$
3) $M_3 = \langle x_ix_j\varepsilon_1^{(0)} \mid i, j = 1, \ldots, 6\rangle \subseteq P(-1)$ where $P = \mathbb{Q}[x_1, \ldots, x_6]$ is standard graded
4) $M_4 = \langle (x_1x_3 - x_2^2)\,\varepsilon_1^{(0)},\ (x_1x_4 - x_2x_3)\,\varepsilon_1^{(0)},\ (x_1x_5 - x_3x_4)\,\varepsilon_1^{(0)},\ (x_2x_4 - x_3^2)\,\varepsilon_1^{(0)},\ (x_2x_5 - x_3x_4)\,\varepsilon_1^{(0)},\ (x_3x_5 - x_4^2)\,\varepsilon_1^{(0)}\rangle \subset P\big(-\binom{1}{0}\big)$ where $P = \mathbb{Q}[x_1, \ldots, x_5]$ is graded by $W = \left(\begin{smallmatrix}1&1&1&1&1\\0&1&2&3&4\end{smallmatrix}\right)$
5) $M_5 = \langle (x_1^2 - x_2)\,\varepsilon_1^{(0)},\ (x_2^2 - x_4)\,\varepsilon_1^{(0)},\ (x_3^2 - x_6)\,\varepsilon_1^{(0)},\ (x_4^2 - x_8)\,\varepsilon_1^{(0)},\ (x_5^2 - x_8x_2)\,\varepsilon_1^{(0)},\ (x_6^2 - x_8x_4)\,\varepsilon_1^{(0)},\ (x_7^2 - x_8x_6)\,\varepsilon_1^{(0)}\rangle \subset P(-1)$ where $P = \mathbb{Q}[x_1, \ldots, x_8]$ is graded by $W = (1\ 2\ \cdots\ 8)$

c) Implement a CoCoA function `VMinRes(...)` which computes a minimal graded free resolution of M using the vertical strategy (see Proposition 4.8.11). Apply this function to the examples in b) and compare the results.

d) Implement a CoCoA function `SMinRes(...)` computes a minimal graded free resolution of M using Schreyer's Algorithm (see Proposition 4.8.14). Apply this function to the examples in b) and compare the results.

e) Implement a CoCoA function `HMinRes(...)` which computes a minimal graded free resolution of M using the horizontal strategy (see Proposition 4.8.16). Apply this function to the examples in b) and compare the results.

f) Compare your functions `VMinRes(...)`, `SMinRes(...)`, and `HMinRes(...)` by counting the number of calls to $\mathrm{NR}_{\sigma,\mathcal{G}}$ and $\mathrm{HR}_{\sigma,\mathcal{G}}$ respectively, in the examples of b).

g) Suppose that $P = K[x_1, \ldots, x_n]$ is standard graded. Prove that we have $\min\{j \in \mathbb{Z} \mid \beta_{ij} \neq 0\} \geq \min\{j \in \mathbb{Z} \mid \beta_{i-1\,j} \neq 0\}$ for $i = 1, \ldots, n$.

In the following we assume that the polynomial rings are standard graded. In view of g), it makes sense to store the numbers $\{\beta_{i\,j-i} \mid i \geq 0, j \geq \alpha + 1\}$, where $\alpha = \alpha(M)$. The matrix $\mathcal{B} = (\beta_{i\,j-i})$ consisting of these numbers is called the **Betti diagram** of M.

h) Using calculation by hand, show that the Betti diagram of the ideal $I = (xy, xz, yz)$ in $\mathbb{Q}[x, y, z]$ is $\begin{pmatrix}1&0\\0&3\\0&2\end{pmatrix}$.

i) Write a CoCoA function `BettiDiagram(...)` which takes the output of `BettiNo(...)` and computes the Betti diagram of M.

j) Apply your function `BettiDiagram(...)` to compute the Betti diagrams of the following homogeneous ideals.

1) $I_1 = (x_1^5 - x_2^5,\ x_2^5 - x_3^5,\ x_3^5 - x_4^5,\ x_4^5 - x_5^5,\ x_1^4x_2 + x_2^4x_3 + x_3^4x_4 + x_4^4x_5 + x_5^4x_1)$ in $\mathbb{Q}[x_1, \ldots, x_5]$

2) $I_2 = (x_2x_8^2 - x_4^3,\ x_2^3 - x_4x_6^2,\ x_1x_7^2 - x_3^3,\ x_1^3 - x_3x_5^2,\ x_2x_4 - x_6x_8,\ x_1x_3 - x_5x_7,\ x_2^2x_8 - x_4^2x_6,\ x_1^2x_7 - x_3^2x_5)$ in $\mathbb{Q}[x_1, \ldots, x_8]$

3) I_3, the vanishing ideal of 11 randomly chosen points in $\mathbb{P}^7$, obtained by taking `I := IdealOfProjectivePoints(GenericPoints(11));` in $\mathbb{Z}/(101)[x_1, \ldots, x_7]$.

5. Hilbert Functions

The mathematicians' function should be
to simplify the intricate.
Instead they do just the opposite,
and complicate what is simple,
and call it 'generalizing'.
(David Hilbert)

An amateur mathematician and two of his friends, a gardener and a chess player, are walking on a *passeggiata* along the sea shore. He is holding a copy of this book in his hands. Let us drop in on their animated discussion.

A: Recently I bought this book. I was intrigued by the introduction of Chapter 5.

G: What is it about?

A: The authors call it *Hilbert functions.*

C: Can you explain what that is?

A: In a nutshell, the basic idea is to measure the size of a graded module by considering $\dim_K(M_i)$ for every $i \in \mathbb{Z}$.

G: I heard that it has something to do with what Italian geometers at the beginning of the twentieth century called *formule di postulazione.* I always thought that *postulante* meant beggar. Is there any connection?

A: Yes, there is. *Postulazione* comes from the latin word *postulatio* which means claim or demand. Those Italian geometers were considering the vector space of all homogeneous polynomials of a fixed degree which vanish at a given set of points. The codimension of this vector space is the number of linearly independent conditions the point set demands from the forms when they are required to contain it. On the other hand, this codimension is a value of the Hilbert function of a ring $K[x_1, \ldots, x_n]/I$ with a homogeneous ideal I.

C: But why are they called Hilbert functions? What is the German contribution here?

A: David Hilbert was one of the greatest mathematicians around that time. While studying invariant theory, he was able to simplify an intricate maze of invariants attached to a graded module by combining them into a single function which now bears his name.

C: Very well, but that doesn't impress me much. This Hilbert function still has infinitely many values, hasn't it? How would you ever get hold of all of them?

A: Indeed, you are right. This is where the story gets interesting. In Section 5.1 the authors prove that Hilbert functions are *integer functions of polynomial type.* In other words, there exists a polynomial in $\mathbb{Q}[t]$ which takes the same values as the Hilbert function of a graded module M in large enough degrees. Thus Hilbert functions are finitely describable in the sense that it suffices to determine the first few values and that polynomial.

G: Finitely describable? Maybe. But what an ugly description is this? Is that what you call simplifying the intricate?

A: Not really. But that chapter does not end with Section 5.1 either. You have to read on! In the next section the authors use one of the most fruitful ideas in all of mathematics: *generating functions.*

G: This sounds enticing. How does this fertilizer work?

A: Instead of considering the individual values $\mathrm{HF}_M(i)$ of the Hilbert function of a graded module M, you combine them into a single object, namely the power series $\mathrm{HS}_M(z) = \sum_{i\in\mathbb{Z}} \mathrm{HF}_M(i)\, z^i$ which is (surprise, surprise!) called the *Hilbert series* of M.

C: Power series? Is it powerful?

A: It is. In fact, it is shown here that a Hilbert series is a very special kind of power series. First of all, we should call it a Laurent series, since there can be finitely many negative exponents. But more importantly, it is a rational series of the particularly simple form $\mathrm{HS}_M(z) = \frac{z^\alpha\, \mathrm{HN}_M(z)}{(1-z)^n}$, where α is the initial degree of the module, $\mathrm{HN}_M(z)$ is a polynomial with integer coefficients, and n is the number of indeterminates in the polynomial ring.

G: O.k., so it looks pretty simple. But why did you call it fruitful?

A: Hilbert series are convenient to handle. They are additive on homogeneous short exact sequences, invariant under passing to a leading term module, invariant under field extensions, and are explicitly computable for graded free modules.

C: Computable? Did you say computable? This interests me a lot. You know, I always like to compute as many variations as possible. For instance, how would you compute the Hilbert series of the polynomial ring itself?

A: Ah! This is not so difficult. By playing a little with binomial coefficients, you can count the terms of a fixed degree. You get $\mathrm{HF}_P(i) = \binom{i+n-1}{n-1}$ for a polynomial ring $P = K[x_1, \ldots, x_n]$ and all $i \geq 0$. Then you have to switch your point of view; what looks complicated from one angle may sometimes look simple from another. In the case at hand, these nasty binomial coefficients turn out to be nothing but the coefficients of the power series expansion of $\frac{1}{(1-z)^n}$. Do you see how elegant this description is?

G: Indeed, this is beautiful. To capture a huge amount of data in such a compact formula reminds me of the efficiency of nature.

At this point the three men leave the promenade and turn into a gorgeous Italian *parco*.

C: Now, how can one compute Hilbert series for more complicated modules?
A: In Section 5.3, the authors lay out a number of strategies for doing this.
C: Strategies? How wonderful! What is the best strategy?
A: Well, basically you first reduce the computation of Hilbert series to modules of the form P/I, where I is monomial ideal in $P = K[x_1, \ldots, x_n]$. Then you have to apply the *multiplication sequence* to decompose the monomial ideal into smaller ones. That's where those strategies come in. It is like choosing the right path in the maze of paths in this park. The best strategy is called the CoCoA strategy.
C: CoCoA? Isn't that a computer program? Can I use it to play chess?
A: Not really. But you may enjoy Tutorials 65 and 71 where the theory of Hilbert functions is used to solve several kinds of chess puzzles.
G: Besides those games, are there any *true* applications? I wonder whether this CoCoA program would have been useful for those Italian geometers and their *postulazione*. For instance, I wonder what happens if we mark the positions of those three palm trees over there on map of this park? Can you compute the postulation?
A: Hm, I am not sure. Let us give it a try. To have a homogeneous vanishing ideal, we should consider the points as points in the projective plane. One point p_1 corresponds to one condition for curves of degree $i \geq 1$, i.e. the Hilbert function of $R_1 = K[x_0, x_1, x_2]/\mathcal{I}(p_1)$ is $\mathrm{HF}_{R_1}(i) = 1$ for $i \geq 0$ and the Hilbert series is $\mathrm{HS}_{R_1}(z) = \sum_{i \geq 0} z^i = \frac{1}{1-z}$.
G: I see. Then the Hilbert function of two points ought to be $\mathrm{HF}_{R_2}(i) = 2$ for $i \geq 1$, where $R_2 = K[x_0, x_1, x_2]/\mathcal{I}(\{p_1, p_2\})$. Similarly, the Hilbert function of three points ought to be $\mathrm{HF}_{R_3}(i) = 3$ for $i \geq 1$, where $R_3 = K[x_0, x_1, x_2]/\mathcal{I}(\{p_1, p_2, p_3\})$, and so on.
A: Wait, wait! Not so quick! Who tells us that the conditions posed by those points on curves of degree i are really linearly independent? For two points, we can choose the coordinate system such that they are $p_1 = (1 : 0 : 0)$ and $p_2 = (0 : 1 : 0)$. We get $\mathcal{I}(\{p_1, p_2\}) = (x_2, x_0x_1)$ and $R_2 \cong K[x_0, x_1](x_0x_1)$. This yields $\mathrm{HF}_{R_2}(i) = 2$ for $i \geq 1$, as you guessed. However, for three points the situation depends on whether they lie on a line or not.
G: What?
A: If the three points are not collinear, we can choose the coordinate system such that they are $p_1 = (1 : 0 : 0)$, $p_2 = (0 : 1 : 0)$, and $p_3 = (0 : 0 : 1)$. We get $\mathcal{I}(\{p_1, p_2, p_3\}) = (x_0x_1, x_0x_2, x_1x_2)$ and therefore an isomorphism $R_3 \cong K \oplus \bigoplus_{i \geq 1}(Kx_0^i \oplus Kx_1^i \oplus Kx_2^i)$. This yields $\mathrm{HF}_{R_3}(i) = 3$ for $i \geq 1$, again in agreement with your guess. But if the three points are collinear, we choose the coordinate system such that

$p_1 = (1 : 0 : 0)$, $p_2 = (0 : 1 : 0)$, and $p_3 = (1 : 1 : 0)$. We get $\mathcal{I}(\{p_1, p_2, p_3\}) = (x_2, x_0x_1(x_1 - x_0))$ and $\mathrm{HF}_{R_3}(1) = 2$, $\mathrm{HF}_{R_3}(i) = 3$ for $i \geq 3$.

G: That's great! The Hilbert function tells me the geometry of my three palm trees. It distinguishes whether they are planted in a row or not! I start believing that this theory can be truly useful.

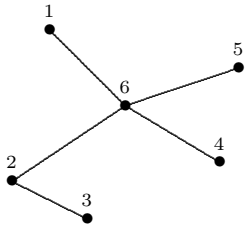
C: Are there other areas besides geometry where Hilbert function can be applied? What about those chess problems I like so much?

A: Do you know the 8-queens problem? It asks in how many ways eight queens can be placed on a chessboard so that no two of them attack each other.

C: Of course! This is a famous problem. It was published in 1850 in a newspaper, and while Carl F. Gauß was still working on it, an amateur mathematician had already found all solutions. Can you actually do it using Hilbert functions?

A: Believe it or not, you can. If we ask how many queens you can place on a chessboard such that no two of them attack each other, we are really studying the graph whose vertices are the squares of the chessboard and whose edges indicate queen moves. And we are asking for the maximal cardinality of a *totally disconnected* subgraph, i.e. a subgraph such that no two of its vertices are connected by an edge. The 8-queens problem is to find the number of maximal, totally disconnected subgraphs. Let us consider this easy example instead.

Using his walking stick, the mathematician starts to draw the following picture in an empty flower-bed.



C: In this case I can tell you right away that a maximal, totally disconnected subgraph has four vertices.

A: True. But for more complicated situations like the 8-queens problem we need a systematic method for getting this answer. Let x_i be an indeterminate corresponding to vertex i for $i = 1, \ldots, 6$. Then the edges of the graph correspond to the terms in $L = \{x_1x_6, x_2x_3, x_2x_6, x_4x_6, x_5x_6\}$. Thus we can attach to our graph the graded ring $K[x_1, \ldots, x_6]/I$ where K is a field and I is the monomial ideal generated by L.

C: So what? Does the Hilbert function of this ring contain any information about our problem?

A: Slow down, please! Let's do one step at a time. The ideal I has the *primary decomposition* $I = (x_1, x_2, x_4, x_5) \cap (x_2, x_6) \cap (x_3, x_6)$. What is the meaning of these three ideals? For instance, let us consider (x_2, x_6). In the graph this means that every edge contains at least one of the two vertices $\{2, 6\}$. Therefore the complementary set of vertices $\{1, 3, 4, 5\}$ is totally disconnected. Likewise, $\{1, 2, 4, 5\}$ and $\{3, 6\}$ are totally disconnected. In conclusion, a maximal, totally disconnected subgraph has four vertices.

G: I think there is a geometric side of this story. The polynomial ring $K[x_1, \ldots, x_6]$ corresponds to the 6-dimensional affine space, and the subvariety $\mathcal{Z}(x_2, x_6)$ is a 4-dimensional linear subspace. Similarly, $\mathcal{Z}(x_3, x_6)$ and $\mathcal{Z}(x_1, x_2, x_4, x_5)$ are 4- and 2-dimensional linear subspaces, respectively. Altogether, the variety $\mathcal{Z}(I)$ is the union of these three linear spaces and therefore 4-dimensional. But what has all of this to do with Hilbert functions?

A: Well, you two should really read Section 5.4. Do you remember that I said Hilbert functions were of polynomial type? The polynomial giving their values in high degree is called, you guessed it, the *Hilbert polynomial* of the graded module in question. Its degree is one less than the dimension you mentioned, and its leading coefficient is related to the multiplicity of the module which corresponds to the number of totally disconnected subgraphs of maximal cardinality in our combinatorial example.

C: Can we calculate this stuff? I think we'll need a computer in any but the most trivial examples.

A: Oh, yes. The Hilbert polynomial can easily be computed from the Hilbert series. As I just said, read Section 5.4 and you'll get the full story.

C: Do you know that you haven't told us so far which integer functions are Hilbert functions?

A: Yes, and I had a good reason: the answer to this question is pretty complicated.

G: I think the path we just took is of dubious value. The designers of this garden call it the *path of maximal irony*, because it requires a lot of effort and in the end it doesn't take you anywhere. Is that true for Hilbert functions as well?

A: No, no! In Sections 5.5, for instance, the authors guide you through a labyrinth full of strange binomial representations of integers, even stranger operations on those representations, weird monomial ideals generated by `Lex`-segments, and an abstruse proof by a bold double induction involving generic linear forms. But the reward for these efforts are sharp bounds for the growth of homogeneous ideals and their Hilbert functions which had been considered rather inaccessible until recently.

C: Which brings us to another question. You mentioned Hilbert functions only for graded modules. What do we do if we are not in a graded situa-

tion? Do we have to just forget about all these nice computational tricks we discussed today?

A: Quite the contrary! In Section 5.6 you can see that Hilbert functions exist for arbitrary affine algebras. Hilbert polynomials, dimension, multiplicity, everything carries over from the graded situation if we replace the vector space of homogeneous polynomials of degree i in an ideal by the space of arbitrary polynomials of degree $\leq i$ in that ideal.

G: Once again you mention dimensions. Is your notion of dimension, i.e. the degree of the affine Hilbert polynomial, really the same as my concept, namely the geometric notion based on chains of irreducible varieties?

A: This question is thoroughly warranted. And as you can see in this book, the authors have to spend a lot of energy and to go through an extended detour to answer it affirmatively.

C: By the way, did you know that there is also a combinatorial notion of dimension?

A: I didn't, but after studying Section 5.7 in here, I know what you mean. Fortunately enough, it also agrees with my Hilbert function approach. In fact, you can even interpret this dimension as a transcendence degree!

G: Ho, ho! Aren't we getting a little carried away? And where does that gate over there lead us?

At the far end of the park, our three strollers enter a blooming rose garden.

C: Wow! This is what I call *dulcis in fundo*.

A: This seems to be one the mottos of the authors of this book. For instance, the last section of this chapter we were talking about contains the whole theory of Hilbert functions, Hilbert series, and so on, in the multigraded setting.

G: Is there any advantage of having a multigrading at hand? Aren't you complicating what is simple and calling it 'generalizing'?

A: For one, the individual homogeneous components tend to be smaller.

C: Which aids the computation, of course!

A: Secondly, we can pass from a finer grading to a coarser one by means of a *change of grading*. This allows us to treat Rees ring, Segre products, Hadamard products, etc., effectively. You name it, we've got it!

Returning from the rose garden, the threesome pass a playground.

C: Recently my children brought home a nice new toy. It consists of coloured 90 degree arcs, four of which can be put together to form a ring. After playing a while, we were able to use the six colours they had to form 231 different rings. I challenge you to explain this number.

A: I can't. But if you solve Tutorial 83, you can do it yourself.

G: I wonder what else is in there. Somehow I began to realize that I knew all of this already, but I did not know anymore that I knew it.

C: Fortunately the book remembers what we have already forgotten ...

5.1 Basic Properties of Hilbert Functions

Besides it is an error to believe
that rigor in the proof
is the enemy of simplicity. [...]
The very effort of rigor forces us
to find out simpler methods of proof.
(David Hilbert)

As in the previous chapter, let us begin at the beginning, and let us proceed in a systematic and rigorous way. For a start, let the polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K be standard graded. Given a finitely generated graded module M over P, we attach many *numerical invariants* to M by considering the function $\mathrm{HF}_M : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $i \mapsto \dim_K(M_i)$. This function is called the *Hilbert function* of M. It is the central object of study in this chapter. The very effort of treating the theory of Hilbert functions rigorously forces us to begin by simplifying the matter and looking at the $\mathbb{Z}$-module of all maps $\mathbb{Z} \longrightarrow \mathbb{Z}$ first. Such maps will be called *integer functions*.

Thus the first subsection is a collection of results about certain classes of integer functions with special regard to properties which turn out to hold for Hilbert functions. For instance, one such class is the set of *integer functions of polynomial type*. Those functions $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ have the property that, for large integers i, their value $f(i)$ is given by the value $p(i)$ of an *integer valued polynomial*, i.e. of a polynomial $p \in \mathbb{Q}[t]$ such that $p(i) \in \mathbb{Z}$ for all $i \in \mathbb{Z}$. The interplay between integer functions of polynomial type and integer valued polynomials is quite intricate. Hence we take great pains to present it as simply as possible (but not simpler).

For instance, the $\mathbb{Z}$-module of all integer valued polynomials has a nice, simple basis, specifically the set $\{\binom{t+a}{b} \mid b \in \mathbb{N}\}$, where a is a fixed integer (see Proposition 5.1.7). These polynomials will turn out to be associated to the Hilbert functions of particularly simple modules, namely polynomial rings and their shifts. As we mentioned above, the values of an integer function f of polynomial type and its associated integer valued polynomial agree for large enough arguments. Indeed, the first integer such that they agree from that point on is another useful invariant. It is called the *regularity index* of f. Many remarkable properties of integer functions of polynomial type and their regularity indices are collected in Proposition 5.1.10 and Corollary 5.1.11 and given simple, rigorous proofs.

Why do we bother to spend several pages playing with such general stuff? There are a number of reasons. The most obvious one is that this material is important for later use. But even more than that, we wanted to have a clear distinction between the general properties of integer functions and the specific properties of Hilbert functions. Following this guideline, the second subsection starts with the definition of Hilbert functions and moves quickly to their basic properties. Let us point out three of them.

Firstly, Hilbert functions are additive on short exact sequences (see Proposition 5.1.14). Speaking on a higher level, this says that HF_M is an additive functor on the category of finitely generated graded P-modules, something homological algebraists crave for. A more down to earth meaning is that we can compute HF_M using the Hilbert functions of simpler modules as building blocks, a fact which is going to enhance our later algorithms. Secondly, the *multiplication sequence* 5.1.16 allows us to reduce the module modulo an element, preferably a regular one. And thirdly, Theorem 5.1.18 says that the Hilbert function of a graded submodule agrees with the Hilbert function of its leading term module with respect to a module term ordering. Clearly, this simplifies things even further and allows us to reduce the computation of Hilbert functions to the case of monomial ideals.

The highlight of the section, like the highlight of a good show, appears at the very end when we prove that Hilbert functions are indeed integer functions of polynomial type (see Theorem 5.1.21). Using the extensive machinery developed in the first part, the task of providing a rigorous proof of this result becomes so straightforward and simple that you should be able to do it in your head. Simplicity and rigor: two ingredients which combine perfectly to ensure the continued success of Hilbert function theory.

5.1.A Integer Functions of Polynomial Type

Theorem: All positive integers are interesting.
Proof: Assume the contrary.
Then there is a smallest
non-interesting positive integer.
But, hey, that's pretty interesting!
A contradiction. QED
(Anonymous)

In this subsection we define integer functions, introduce some general operations and study their properties. In this way, we want to show that integer functions are interesting without having to argue by contradiction.

Definition 5.1.1. A map $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ is called an **integer function**. Given an integer function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, we define the following operators.

a) The integer function $\Delta f : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $\Delta f(i) = f(i) - f(i-1)$ for $i \in \mathbb{Z}$ is called the **(first) difference function** of f.
b) Let $\Delta^0 f = f$. For $r \geq 1$, we inductively define an integer function $\Delta^r f : \mathbb{Z} \longrightarrow \mathbb{Z}$ by $\Delta^r f = \Delta(\Delta^{r-1} f)$ and call it the $\mathbf{r^{th}}$ **difference function** of f.
c) Given a number $q \in \mathbb{Z}$, we define an integer function $\Delta_q f : \mathbb{Z} \longrightarrow \mathbb{Z}$ by $\Delta_q f(i) = f(i) - f(i-q)$ for $i \in \mathbb{Z}$ and call it the **q-difference function** of f.
d) An integer function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ is called an **integer Laurent function** if there exists a number $i_0 \in \mathbb{Z}$ such that $f(i) = 0$ for all $i < i_0$.

e) Given an integer Laurent function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, we define another integer Laurent function $\Sigma f : \mathbb{Z} \longrightarrow \mathbb{Z}$ by $\Sigma f(i) = \sum_{j \leq i} f(j)$ and call it the **summation function** of f.

Some authors use the expression "numerical function" to denote integer functions. The difference and summation operations define bijections on the set of integer Laurent functions which are inverse to each other.

Proposition 5.1.2. *Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be an integer Laurent function. Then we have $\Sigma \Delta f = \Delta \Sigma f = f$.*

Proof. For every $i \in \mathbb{Z}$, we have $\Sigma \Delta f(i) = \sum_{j \leq i} (\Delta f(j)) = \sum_{j \leq i} (f(j) - f(j-1)) = f(i)$ and $\Delta \Sigma f(i) = \Sigma f(i) - \Sigma f(i-1) = \sum_{j \leq i} f(j) - \sum_{j \leq i-1} f(j) = f(i)$. □

As we shall see, Hilbert functions are integer Laurent functions. But they have another important property, namely that their values agree with the values of some rational univariate polynomial from some point on. The following definition introduces a subset of $\mathbb{Q}[t]$ containing precisely the rational univariate polynomials we are concerned with.

Definition 5.1.3. A polynomial $p \in \mathbb{Q}[t]$ is called an **integer valued polynomial** if we have $p(i) \in \mathbb{Z}$ for all $i \in \mathbb{Z}$. The set of all integer valued polynomials will be denoted by $\mathbb{IP}$. Furthermore, for every $r \geq 0$, we let $\mathbb{IP}_{\leq r}$ be the set of all integer valued polynomials of degree $\leq r$.

Some authors use the expression "numerical polynomial" to denote integer valued polynomials. Clearly, for every $r \geq 0$, the set $\mathbb{IP}_{\leq r}$ is a $\mathbb{Z}$-submodule of $\mathbb{Q}[t]$. Notice that $\mathbb{IP}$ is not contained in $\mathbb{Z}[t]$, as evidenced by the integer valued polynomial $\frac{1}{2}t(t+1)$.

Remark 5.1.4. To every integer valued polynomial $p \in \mathbb{IP}$ we can associate an integer function $\mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $i \mapsto p(i)$ for all $i \in \mathbb{Z}$. The difference function of this integer function is associated to the integer valued polynomial $\Delta p(t) = p(t) - p(t-1)$. If $p \neq 0$, the associated integer function is not an integer Laurent function. Therefore we cannot define its summation function.

The following example highlights some very important integer valued polynomials. Later we shall see that they are related to Hilbert functions of polynomial rings. Recall that, for $a \in \mathbb{N}$ and $i \in \mathbb{Z}$, the binomial coefficient $\binom{i}{a}$ is defined by

$$\binom{i}{a} = \begin{cases} \frac{1}{a!}\, i\,(i-1)\cdots(i-a+1) & \text{if } a \geq 1, \\ 1 & \text{if } a = 0. \end{cases}$$

Example 5.1.5. Let $a, b \in \mathbb{Z}$ with $b \geq 1$, and let $p \in \mathbb{Q}[t]$ be the polynomial defined by $p(t) = \binom{t+a}{b} = \frac{1}{b!}(t+a)(t+a-1)\cdots(t+a-b+1)$. We claim

that p is an integer valued polynomial. To this effect we have to show that, for every $i \in \mathbb{Z}$, the number $(i+a)(i+a-1)\cdots(i+a-b+1)$ is divisible by $b!$. For all $m \geq 1$, it is congruent to $(i+a+mb!)(i+a-1+mb!)\cdots \cdots(i+a-b+1+mb!)$ modulo $b!$. Hence the claim follows from the observation that, for a sufficiently big m, the usual binomial coefficient $\binom{i+a+mb!}{b}$ is an integer.

Clearly, we have $\deg(p) = b$. Using Lemma 5.1.6.b below we see that $\Delta(\binom{t+a}{b}) = \binom{t+a-1}{b-1}$. Repeating this process, we obtain $\Delta^b p(t) = 1$. For $b > 1$, the polynomial p is not contained in $\mathbb{Z}[t]$, since we have $\mathrm{LC}_{\mathtt{Deg}}(p) = \frac{1}{b!}$.

In order to examine integer valued polynomials of the form $\binom{t+a}{b}$ more carefully, we need to collect a few useful properties of binomial coefficients.

Lemma 5.1.6. *Let $a \in \mathbb{N}$ and $i \in \mathbb{Z}$.*

a) For all $i \in \mathbb{Z}$, we have $\binom{-i}{a} = (-1)^a \binom{a+i-1}{a}$.
b) If $i \geq a \geq 1$, then we have $\binom{i}{a} - \binom{i-1}{a} = \binom{i-1}{a-1}$.
c) If $i \geq a \geq 1$, then we have $\sum_{j=a-1}^{i-1} \binom{j}{a-1} = \binom{i}{a}$.
d) If $i \geq a \geq 0$, then we have $\sum_{j=0}^{a} \binom{i-1-j}{a-j} = \binom{i}{a}$.

Proof. Claim a) follows from $\binom{-i}{a} = \frac{1}{a!}(-i)(-i-1)\cdots(-i-a+1) = (-1)^a \frac{1}{a!} i(i+1)\cdots(i+a-1) = (-1)^a \binom{i+a-1}{a}$. To prove b), we calculate $\binom{i}{a} - \binom{i-1}{a} = \frac{1}{a!}[i(i-1)\cdots(i-a+1) - (i-1)(i-2)\cdots(i-a)] = \frac{1}{a!}(i-1)\cdots \cdots(i-a+1)[i-(i-a)] = \frac{1}{(a-1)!}(i-1)\cdots(i-a+1) = \binom{i-1}{a-1}$. Claim c) follows by repeatedly applying b), since $\binom{i}{a} = \binom{i-1}{a-1} + \binom{i-1}{a} = \binom{i-1}{a-1} + \binom{i-2}{a-1} + \binom{i-2}{a} = \cdots = \sum_{j=a-1}^{i-1} \binom{j}{a-1}$. Finally, also claim d) follows by repeatedly applying b), since $\binom{i}{a} = \binom{i-1}{a} + \binom{i-1}{a-1} = \binom{i-1}{a} + \binom{i-2}{a-1} + \binom{i-2}{a-2} = \cdots = \sum_{j=0}^{a} \binom{i-1-j}{a-j}$. □

Now we collect some basic properties of integer valued polynomials.

Proposition 5.1.7. (Basic Properties of Integer Valued Polynomials) *Let $a \in \mathbb{Z}$, $r \in \mathbb{N}$, and let $(a_0, a_1, a_2, \ldots)$ be a sequence of integers.*

a) For an integer valued polynomial p, we have $\deg(p) = r$ if and only if $\Delta^r p(t) \in \mathbb{Z} \setminus \{0\}$. If this holds true, we have $\Delta^r p(t) = r!\,\mathrm{LC}_{\mathtt{Deg}}(p) \in \mathbb{Z}$.
b) Let p be an integer valued polynomial of degree r. Then the polynomial $q = p - r!\,\mathrm{LC}_{\mathtt{Deg}}(p)\binom{t+a}{r}$ is an integer valued polynomial of degree $< r$.
c) For every $r \geq 0$, the set of polynomials $\{\binom{t+a_i}{i} \mid 0 \leq i \leq r\}$ is a $\mathbb{Z}$-basis of $\mathbb{IP}_{\leq r}$. Consequently, the set $\{\binom{t+a_i}{i} \mid i \in \mathbb{N}\}$ is a $\mathbb{Z}$-basis of $\mathbb{IP}$.
d) For a map $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, the following conditions are equivalent.
  1) There exists an integer valued polynomial $p \in \mathbb{IP}$ with $f(i) = p(i)$ for all $i \in \mathbb{Z}$.
  2) There exist a number $i_0 \in \mathbb{Z}$ and an integer valued polynomial $q \in \mathbb{IP}$ such that $f(i_0) \in \mathbb{Z}$ and $\Delta f(i) = q(i)$ for all $i \in \mathbb{Z}$.

Proof. Claim a) follows from the observation that, given an integer valued polynomial $p(t) = c_r\, t^r$ + *(terms of lower degree)*, we obtain $\Delta p(t) = c_r(t^r-(t-1)^r)+$*(terms of lower degree)* $= r\, c_r\, t^{r-1}+$*(terms of lower degree)*. To prove b), we observe that q is clearly an integer valued polynomial of degree $\leq r$. Since $\Delta^r q(t) = \Delta^r p(t) - c\,\Delta^r(\binom{t+a}{r}) = r!\,(\mathrm{LC}_{\mathtt{Deg}}(p) - c) = 0$, the claim follows from a).

Next we show c). Let $p_i = \binom{t+a_i}{i}$ for $i \geq 0$. Suppose there is an $r \geq 0$ and a relation $b_0p_0+\cdots+b_rp_r = 0$ with $b_0, \ldots, b_r \in \mathbb{Q}$ and $b_r \neq 0$. Equating the r^{th} homogeneous components in this relation yields $b_r\,\mathrm{LC}_{\mathtt{Deg}}(p_r) = 0$, a contradiction. Hence the polynomials p_i are $\mathbb{Z}$-linearly independent. The fact that they generate $\mathbb{IP}_{\leq r}$ as a $\mathbb{Z}$-module follows from a) and b).

It remains to prove claim d). The implication "1)$\Rightarrow$2)" follows from $\Delta f(i) = p(i) - p(i-1)$ for all $i \in \mathbb{Z}$, so that the integer valued polynomial $q(t) = p(t) - p(t-1)$ does the job. Conversely, we note that we have $f(i) = f(i_0) + \sum_{j=i_0+1}^{i} \Delta f(j)$ for $i > i_0$ and $f(i) = f(i_0) - \sum_{j=i+1}^{i_0} \Delta f(j)$ for $i < i_0$. By b), we can write the integer valued polynomial q in the form $q(t) = c_1\binom{t-1}{0}+\cdots+c_m\binom{t-1}{m-1}$, where $c_1, \ldots, c_m \in \mathbb{Z}$. Then also $p(t) = c_1\binom{t}{1}+\cdots+c_m\binom{t}{m}$ is an integer valued polynomial, and Lemma 5.1.6.b yields $q(t) = p(t)-p(t-1)$. Thus we obtain $f(i) = f(i_0)+\sum_{j=i_0+1}^{i}(p(j)-p(j-1)) = f(i_0) - p(i_0) + p(i)$ for $i > i_0$ and $f(i) = f(i_0) - \sum_{j=i+1}^{i_0}(p(j) - p(j-1)) = f(i_0) - p(i_0) + p(i)$ for $i < i_0$. Altogether, we see that the integer valued polynomial $p(t) - p(i_0) + f(i_0)$ has the desired property. □

The importance of integer valued polynomials derives from the fact that they determine the eventual behaviour of the following kind of integer functions.

Definition 5.1.8. Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be an integer function.

a) The map $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ is called an integer function **of polynomial type** if there exists a number $i_0 \in \mathbb{Z}$ and an integer valued polynomial $p \in \mathbb{IP}$ such that $f(i) = p(i)$ for all $i \geq i_0$. This polynomial is uniquely determined and denoted by HP_f.

b) For an integer function f of polynomial type, the number

$$\mathrm{ri}(f) = \min\{i \in \mathbb{Z} \mid f(j) = \mathrm{HP}_f(j) \text{ for all } j \geq i\}$$

is called the **regularity index** of f. Whenever $f(i) = \mathrm{HP}_f(i)$ for all $i \in \mathbb{Z}$, we let $\mathrm{ri}(f) = -\infty$.

The integer functions of polynomial type we study later are called Hilbert functions and their associated integer valued polynomials are called Hilbert polynomials. This is the reason why we use the notation HP_f. By definition, not all values of an integer function f of polynomial type have to agree with the corresponding values of HP_f. The following example introduces a family of integer functions of polynomial type which will turn out to be fundamentally important.

Example 5.1.9. For every $i \in \mathbb{N}$, we define a map $\mathrm{bin}_i : \mathbb{Z} \longrightarrow \mathbb{Z}$ by $\mathrm{bin}_i(j) = \binom{j}{i}$ for $j \geq i$ and by $\mathrm{bin}_i(j) = 0$ for $j < i$. Clearly, the map bin_i is an integer Laurent function of polynomial type. It satisfies $\mathrm{HP}_{\mathrm{bin}_i}(t) = \binom{t}{i}$ and $\mathrm{ri}(\mathrm{bin}_i) = 0$. Moreover, if $i > 0$, then Lemma 5.1.6.b shows $\Delta \mathrm{bin}_i(j) = \mathrm{bin}_{i-1}(j-1)$ for all $j \in \mathbb{Z}$.

But there is no integer valued polynomial $p \in \mathbb{IP}$ such that $\mathrm{bin}_i(j) = p(j)$ for all $j \in \mathbb{Z}$, because in this case we would get $p = \mathrm{HP}_{\mathrm{bin}_i}$ and $p(-1) = \binom{-1}{i} = (-1)^i$, in contradiction to $\mathrm{bin}_i(-1) = 0$.

Our next result says that integer functions of polynomial type behave well under the difference and summation operations.

Proposition 5.1.10. *Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be an integer function. Then the following conditions are equivalent.*

a) The integer function f is of polynomial type.
b) The integer function Δf is of polynomial type.

Moreover, if f is an integer Laurent function, then these conditions are equivalent to the following one.

c) The integer function Σf is of polynomial type.

Proof. Let f be of polynomial type and $p = \mathrm{HP}_f$. Then the polynomial $q(t) = \Delta p(t)$ is an integer valued polynomial, and we have $\Delta f(i) = \Delta p(i) = q(i)$ for $i \geq \mathrm{ri}(f) + 1$. Hence Δf is an integer function of polynomial type. Conversely, let $q = \mathrm{HP}_{\Delta f}$, and let $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ be the integer function of polynomial type defined by $g(i) = q(i)$ for all $i \in \mathbb{Z}$. Now we choose a number $i_0 \geq \mathrm{ri}(\Delta f)$ and define an integer function $h : \mathbb{Z} \longrightarrow \mathbb{Z}$ by

$$h(i) = \begin{cases} \sum\limits_{j=i_0+1}^{i} g(j) & \text{for } i > i_0, \\ 0 & \text{for } i = i_0, \\ -\sum\limits_{j=i+1}^{i_0} g(j) & \text{for } i < i_0. \end{cases}$$

It is easy to check that we have $g = \Delta h$. By Proposition 5.1.7.d, there exists an integer valued polynomial $p \in \mathbb{IP}$ such that $h(i) = p(i)$ for all $i \in \mathbb{Z}$. Since $i_0 \geq \mathrm{ri}(f)$, this implies $f(i) = f(i_0) + \sum_{j=i_0+1}^{i} \Delta f(j) = f(i_0) + \sum_{j=i_0+1}^{i} g(j) = f(i_0) + h(i) - h(i_0) = f(i_0) + h(i)$ for all $i > i_0$. Thus f is of polynomial type, as claimed.

To prove the equivalence of a) and c) it suffices to apply "a)$\Leftrightarrow$b)" to the integer function $g = \Sigma f$ and to note that $f = \Delta g$ by Proposition 5.1.2. $\square$

If all conditions of this proposition are satisfied, i.e. if the given map $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ is an integer Laurent function of polynomial type, we can compute the integer valued polynomials corresponding to Δf and to Σf. Recall that, for a polynomial $p \in \mathbb{IP}$, we let Δp be the polynomial defined by $\Delta p(t) = p(t) - p(t-1)$.

Corollary 5.1.11. *Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be an integer Laurent function of polynomial type.*

a) We have $\mathrm{HP}_{\Delta f}(t) = \Delta \mathrm{HP}_f(t)$. In particular, if $\deg(\mathrm{HP}_f) > 0$, then we have $\deg(\mathrm{HP}_{\Delta f}) = \deg(\mathrm{HP}_f) - 1$.

b) For every $q \geq 1$, we have $\mathrm{ri}(\Delta_q f) = \mathrm{ri}(f) + q$. In particular, we have $\mathrm{ri}(\Delta f) = \mathrm{ri}(f) + 1$.

c) If we write $\mathrm{HP}_f(t) = c_1\binom{t-1}{0} + \cdots + c_m\binom{t-1}{m-1}$ and choose $i_0 \geq \mathrm{ri}(f)$, then we have $\mathrm{HP}_{\Sigma f}(t) = c_1\binom{t}{1} + \cdots + c_m\binom{t}{m} + f(i_0)$.

d) We have $\mathrm{ri}(\Sigma f) = \mathrm{ri}(f) - 1$.

Proof. Claim a) was shown in the first part of the proof of the proposition. To show b), we let $i_0 = \mathrm{ri}(f)$. Then we have $\Delta_q f(i) = f(i) - f(i-q) = \mathrm{HP}_f(i) - \mathrm{HP}_f(i-q) = \Delta_q \mathrm{HP}_f(i)$ for all $i \geq i_0 + q$. For $i = i_0 + q - 1$, we get $\Delta_q f(i) \neq \Delta \mathrm{HP}_f(i)$, because we have $f(i) = \mathrm{HP}_f(i)$ and $f(i-q) = f(i_0 - 1) \neq \mathrm{HP}_f(i_0 - 1) = \mathrm{HP}_f(i-q)$ by the definition of $\mathrm{ri}(f)$.

Claim c) follows from the second part of the proof of the proposition, and d) follows from b) because of $\mathrm{ri}(f) = \mathrm{ri}(\Delta\Sigma f) = \mathrm{ri}(\Sigma f) + 1$. □

5.1.B Hilbert Functions in the Standard Graded Case

I hate quotations.
Tell me what you know.
(Ralph W. Emerson)

After all these preparations, it is time for us to tell you what Hilbert functions really are. Specifically, we prove that they are examples of integer functions of polynomial type. In fact, they are easily the most interesting and important integer functions of polynomial type you will encounter in this book. Let K be a field, and let $P = K[x_1, \ldots, x_n]$ be standard graded.

Definition 5.1.12. Let M be a finitely generated graded P-module. Since the grading given by W on P is of positive type, Proposition 4.1.19 shows that we have a well-defined map

$$\begin{array}{rcl} \mathrm{HF}_M : \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ i & \longmapsto & \dim_K(M_i) \end{array}$$

This map is called the **Hilbert function** of M.

The Hilbert function is an **invariant** of M in the following sense. By Proposition 1.1.12, an isomorphism of vector spaces $\varphi : P_1 \longrightarrow P_1$ extends uniquely to an isomorphism $\Phi : P \longrightarrow P$ of graded K-algebras. Such a map Φ is called a **homogeneous linear change of coordinates**. If we choose a presentation $M = F/U$ with a graded free P-module F and a

graded submodule U of F, the map Φ extends uniquely to an isomorphism of graded P-modules $F/U \longrightarrow F/U$. We express this fact by saying that the Hilbert function of M is invariant under a homogeneous linear change of coordinates.

To get an idea of the kind of integer function this is, let us compute it in the simplest case $M = P$.

Proposition 5.1.13. *For every $i \in \mathbb{N}$, we have $\mathrm{HF}_P(i) = \binom{i+n-1}{n-1}$.*

Proof. We shall use induction on n. For the case $n = 1$, we have $\mathrm{HF}_P(i) = 1 = \binom{i}{0}$ for all $i \in \mathbb{N}$. Now we consider the case $n > 1$. For each $i \in \mathbb{N}$, we let $\mathbb{T}^n_i$ be the set of all terms of degree i in $\mathbb{T}^n$, and for $j = 0, \ldots, i$ we let $\mathbb{T}^n_{ij}$ be the set of terms in $\mathbb{T}^n_i$ which are divisible by x^j_n but not by x^{j+1}_n. Hence we have a decomposition $\mathbb{T}^n_i = \cup^i_{j=0} \mathbb{T}^n_{ij}$ of $\mathbb{T}^n_i$ into pairwise disjoint subsets. Moreover, the elements in $\mathbb{T}^n_{ij}$ are in 1–1 correspondence with the elements of $\mathbb{T}^{n-1}_{i-j}$. Using the induction hypothesis and Lemma 5.1.6.d, we obtain $\mathrm{HF}_P(i) = \#\mathbb{T}^n_i = \sum^i_{j=0} \#\mathbb{T}^n_{ij} = \sum^i_{j=0} \#\mathbb{T}^{n-1}_{i-j} = \sum^i_{j=0} \binom{(i-j)+(n-1)-1}{(n-1)-1} = \sum^i_{j=0} \binom{i+n-2-j}{i-j} = \binom{i+n-1}{i}$. □

Since it is clear that $\mathrm{HF}_P(i) = 0$ for $i < 0$, we can rephrase this proposition by saying that $\mathrm{HF}_P(i) = \mathrm{bin}_{n-1}(i+n-1)$ for all $i \in \mathbb{Z}$, where bin_{n-1} is the function introduced in Example 5.1.9. Our next proposition enables us to reduce the computation of the Hilbert function of more complicated graded P-modules to this case.

Proposition 5.1.14. (Basic Properties of Hilbert Functions) *Let M, M', and M'' be three finitely generated graded P-modules.*

a) Let $j \in \mathbb{Z}$. Then the Hilbert function of the module $M(j)$ obtained by shifting degrees by j is given by $\mathrm{HF}_{M(j)}(i) = \mathrm{HF}_M(i+j)$ for all $i \in \mathbb{Z}$.

b) Given a homogeneous exact sequence of graded P-modules

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

we have $\mathrm{HF}_M(i) = \mathrm{HF}_{M'}(i) + \mathrm{HF}_{M''}(i)$ for all $i \in \mathbb{Z}$.

c) Given finitely many finitely generated graded P-modules $M_1, \ldots, M_r$, we have $\mathrm{HF}_{M_1 \oplus \cdots \oplus M_r}(i) = \mathrm{HF}_{M_1}(i) + \cdots + \mathrm{HF}_{M_r}(i)$ for all $i \in \mathbb{Z}$.

d) Let $\delta_1, \ldots, \delta_r \in \mathbb{Z}$. The Hilbert function of the graded free P-module $F = \bigoplus^r_{j=1} P(-\delta_j)$ is given by

$$\mathrm{HF}_F(i) = \sum_{j=1}^{r} \mathrm{HF}_P(i - \delta_j) = \sum_{j=1}^{r} \mathrm{bin}_{n-1}(i - \delta_j + n - 1) \quad \text{for all } i \in \mathbb{Z}.$$

e) Given homogeneous generators $\{g_1, \ldots, g_s\}$ of M, we let $\delta_j = \deg(g_j)$ for $j = 1, \ldots, s$. Then we have $\mathrm{HF}_M(i) \leq \sum^s_{j=1} \mathrm{bin}_{n-1}(i - \delta_j + n - 1)$ for all $i \in \mathbb{Z}$. In particular, HF_M is an integer Laurent function.

Proof. The first claim follows from the definition of $M(j)$, since we have $M(j)_i = M_{i+j}$ for all $i \in \mathbb{Z}$. Now we prove b). Since the P-linear maps in the exact sequence are homogeneous, we have for every $i \in \mathbb{Z}$ an exact sequence of finite dimensional K-vector spaces $0 \longrightarrow M'_i \longrightarrow M_i \longrightarrow M''_i \longrightarrow 0$. Counting dimensions yields $\dim_K(M_i) = \dim_K(M'_i) + \dim_K(M''_i)$, i.e. the claim.

Next we prove c) by induction on r. Since the case $r = 1$ is clear, we may assume $r > 1$. Then the homogeneous exact sequence

$$0 \longrightarrow \textstyle\bigoplus_{j=1}^{r-1} M_j \longrightarrow \bigoplus_{j=1}^{r} M_j \longrightarrow M_r \longrightarrow 0$$

together with b) and the induction hypothesis yields the claim.

Part d) follows by combining a) and c). Finally, claim e) is a consequence of d) and of the fact that the P-linear map $\bigoplus_{j=1}^{s} P(-\delta_j) \longrightarrow M$ defined by $e_j \mapsto g_j$ for $j = 1, \ldots, s$ is homogeneous and surjective. □

Using these rules, we can already compute the Hilbert function of many interesting graded P-modules (see also Exercise 5).

Example 5.1.15. Let f be a non-zero homogeneous polynomial of degree d. Then the Hilbert function of the graded P-module $P/(f)$ is given by $\mathrm{HF}_{P/(f)}(i) = \Delta_d \mathrm{HF}_P(i)$ for all $i \in \mathbb{Z}$. In order to see why this holds, it suffices to apply the proposition to the homogeneous exact sequence

$$0 \longrightarrow P(-d) \xrightarrow{\varphi} P \longrightarrow P/(f) \longrightarrow 0$$

where the map φ is "multiplication by f".

More generally, we can consider multiplication by a homogeneous polynomial on an arbitrary finitely generated graded P-module.

Proposition 5.1.16. (The Multiplication Sequence)
Let M be a finitely generated graded P-module, and let $f \in P$ be a non-zero homogeneous polynomial of degree d.

a) There is a homogeneous exact sequence of graded P-modules

$$0 \longrightarrow [M/(0 :_M (f))](-d) \xrightarrow{\varphi} M \longrightarrow M/fM \longrightarrow 0$$

where the map φ is induced by multiplication by f.

b) For all $i \in \mathbb{Z}$, we have $\mathrm{HF}_{M/fM}(i) = \mathrm{HF}_M(i) - \mathrm{HF}_{M/(0:_M(f))}(i-d)$.

c) The polynomial f is a non-zerodivisor for the module M if and only if $\mathrm{HF}_{M/fM}(i) = \Delta_d \mathrm{HF}_M(i)$ for all $i \in \mathbb{Z}$.

Proof. In order to prove a), we note that multiplication by f defines a homogeneous P-linear map $M(-d) \longrightarrow M$ whose kernel is $[0 :_M (f)](-d)$ and whose cokernel is M/fM. By dividing out the kernel we get the desired exact sequence. Claim b) follows by applying parts a) and b) of

Proposition 5.1.14 to this sequence. Finally, let us prove c). If f is a non-zerodivisor for M then $0 :_M (f) = 0$ and the conclusion follows from b). Conversely, if we assume that $\mathrm{HF}_{M/fM}(i) = \Delta_d \mathrm{HF}_M(i)$ for all $i \in \mathbb{Z}$, then $\mathrm{HF}_{M/fM}(i) = \mathrm{HF}_M(i) - \mathrm{HF}_M(i-d)$ for all $i \in \mathbb{Z}$. Using b), we see that $\mathrm{HF}_{M/(0:_M(f))}(i-d) = \mathrm{HF}_M(i-d)$ and hence $\mathrm{HF}_{(0:_M(f))}(i-d) = 0$ for all $i \in \mathbb{Z}$ which implies that $0 :_M (f)$ is the zero module, and concludes the proof. □

For modules of the form $M = P/I$, this proposition can be simplified as follows.

Corollary 5.1.17. *Let I be a homogeneous ideal in P, and let $f \in P$ be a non-zero homogeneous polynomial of degree d. Then we have a homogeneous exact sequence*

$$0 \longrightarrow [P/(I :_P (f))](-d) \xrightarrow{\varphi} P/I \longrightarrow P/(I + (f)) \longrightarrow 0$$

and therefore $\mathrm{HF}_{P/(I+(f))}(i) = \mathrm{HF}_{P/I}(i) - \mathrm{HF}_{P/(I:_P(f))}(i-d)$ for all $i \in \mathbb{Z}$.

In particular, f is a non-zerodivisor for P/I if and only if we have $\mathrm{HF}_{P/(I+(f))}(i) = \Delta_d \mathrm{HF}_{P/I}(i)$ for all $i \in \mathbb{Z}$.

Proof. It suffices to observe that $0 :_{P/I} (f) = (I :_P (f))/I$ and to apply the proposition. □

In order to be able to compute the Hilbert function for arbitrary finitely generated graded P-modules, we need one more result.

Theorem 5.1.18. (Hilbert Functions and Leading Term Modules) *Let $\delta_1, \ldots, \delta_r \in \mathbb{Z}$, let F be the graded free P-module $F = \bigoplus_{j=1}^r P(-\delta_j)$, let M be a graded submodule of F, and let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. Then we have $\mathrm{HF}_M(i) = \mathrm{HF}_{\mathrm{LT}_\sigma(M)}(i)$ for all $i \in \mathbb{Z}$.*

Proof. By Macaulay's Basis Theorem 1.5.7, the residue classes of the terms in $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle \setminus \mathrm{LT}_\sigma\{M\}$ form a K-basis of both F/M and $F/\mathrm{LT}_\sigma(M)$. For every $i \in \mathbb{Z}$, the residue classes of the terms of degree i of the set $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle \setminus \mathrm{LT}_\sigma\{M\}$ are therefore K-bases of both $(F/M)_i$ and $(F/\mathrm{LT}_\sigma(M))_i$. Hence we can use Proposition 5.1.14.b and get $\mathrm{HF}_M(i) = \mathrm{HF}_F(i) - \mathrm{HF}_{F/M}(i) = \mathrm{HF}_F(i) - \mathrm{HF}_{F/\mathrm{LT}_\sigma(M)}(i) = \mathrm{HF}_{\mathrm{LT}_\sigma(M)}(i)$ for all $i \in \mathbb{Z}$. □

By combining the preceding results, we obtain an effective method for computing individual values of Hilbert functions of finitely generated graded P-modules.

Corollary 5.1.19. (Computation of Hilbert Function Values) *Let $i \in \mathbb{Z}$, let M be a finitely generated graded P-module, and assume that we are given a presentation $M = F/N$ where N is a graded submodule of F. Consider the following instructions.*

1) Choose a module term ordering σ on $\mathbb{T}^n\langle e_1,\ldots,e_r\rangle$ and compute $\mathrm{LT}_\sigma(N)$ using Buchberger's Algorithm 2.5.5.
2) Using the Structure Theorem for Monomial Modules 1.3.9, write $\mathrm{LT}_\sigma(N)$ in the form $\mathrm{LT}_\sigma(N) = \bigoplus_{j=1}^r I_j\, e_j$ with monomial ideals $I_1,\ldots,I_r$ of P.
3) For $j = 1,\ldots,r$, determine $\mathrm{HF}_P(i-\delta_j)$ by applying Proposition 5.1.13.
4) For $j = 1,\ldots,r$, determine $\mathrm{HF}_{I_j}(i-\delta_j)$ by counting the terms of degree $i-\delta_j$ in $\mathbb{T}^n$ which are contained in I_j.
5) Return the number $\sum_{j=1}^r(\mathrm{HF}_P(i-\delta_j) - \mathrm{HF}_{I_j}(i-\delta_j))$ and stop.

This is an algorithm which computes the value $\mathrm{HF}_M(i)$ of the Hilbert function of M.

Proof. The given presentation implies $\mathrm{HF}_M(i) = \dim_K(F_i) - \dim_K(N_i)$. Now we use Proposition 5.1.14.d to compute $\dim_K(F_i) = \sum_{j=1}^r \mathrm{HF}_P(i-\delta_j)$. By the theorem, we have $\mathrm{HF}_N(i) = \mathrm{HF}_{\mathrm{LT}_\sigma(N)}(i)$. Next we apply Proposition 5.1.14.c to $\mathrm{LT}_\sigma(N) = \bigoplus_{j=1}^r I_j\, e_j$. Since $\deg_W(e_j) = \delta_j$ for $j = 1,\ldots,r$, we obtain $\dim_K(N_i) = \mathrm{HF}_{\mathrm{LT}_\sigma(N)}(i) = \sum_{j=1}^r \mathrm{HF}_{I_j}(i-\delta_j)$ for the second dimension in the expression above. □

Unfortunately, this algorithm is not very efficient. In the next two sections, we shall develop a method which is much more suitable for practical applications. Next we apply the theorem to show that Hilbert functions do not change under base fields extensions.

Given any finitely generated graded P-module M, we can choose a presentation $M \cong F/N$ where F is a finitely generated graded free P-module and N a graded submodule of F. If we then have a field extension $K \subseteq L$, we let $\overline{P} = L[x_1,\ldots,x_n]$ and $\overline{F} = \bigoplus_{j=1}^r \overline{P}(-\delta_j)$. The graded $\overline{P}$-module $\overline{F}/N\overline{F}$ will be denoted by $M \otimes_K L$. We say that $M \otimes_K L$ is obtained from M by **base field extension**. This notation indicates that $M \otimes_K L$ is a special case of a more general construction called tensor product. It is easy to see that the $\overline{P}$-module $M \otimes_K L$ does not depend on the choice of the presentation $M = F/N$ (see also Exercise 7). Using the theorem, we can determine the Hilbert function of $M \otimes_K L$ as follows.

Corollary 5.1.20. *Let M be a finitely generated graded P-module, and let $K \subseteq L$ be a field extension. Then we have $\mathrm{HF}_M(i) = \mathrm{HF}_{M\otimes_K L}(i)$ for all $i \in \mathbb{Z}$.*

Proof. We choose a homogeneous presentation $M = F/N$ with a graded free P-module $F = \bigoplus_{j=1}^r P(-\delta_j)$, where $\delta_1,\ldots,\delta_r \in \mathbb{Z}$, and a graded submodule N of F. Then we let $\overline{P} = L[x_1,\ldots,x_n]$ and $\overline{F} = \bigoplus_{j=1}^r \overline{P}(-\delta_j)$. By definition, we have $M \otimes_K L = \overline{F}/N\,\overline{F}$. Since Lemma 2.4.16 yields $\mathrm{LT}_\sigma\{N\} = \mathrm{LT}_\sigma\{N\,\overline{F}\}$, the theorem shows $\mathrm{HF}_N(i) = \mathrm{HF}_{N\,\overline{F}}(i)$ for all $i \in \mathbb{Z}$. Together with Proposition 5.1.14.b, this equality implies the claim. □

Let us finish this section by showing that Hilbert functions are actually integer functions of polynomial type in the sense of Definition 5.1.8.

Theorem 5.1.21. *Let M be a finitely generated graded P-module. Then its Hilbert function $\mathrm{HF}_M : \mathbb{Z} \longrightarrow \mathbb{Z}$ is an integer function of polynomial type.*

Proof. Let $\{g_1, \ldots, g_r\}$ be a homogeneous system of non-zero generators of M, and let $\delta_i = \deg(g_i)$ for $i = 1, \ldots, r$. Letting $F = \bigoplus_{j=1}^r P(-\delta_i)$, we have a homogeneous surjective P-linear map $\varphi : F \longrightarrow M$ defined by $\varphi(e_i) = g_i$ for $i = 1, \ldots, r$. Let N be its kernel. Thus we have a homogeneous presentation $M \cong F/N$. We choose a module term ordering σ on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ and write $\mathrm{LT}_\sigma(N) = \bigoplus_{j=1}^r I_j\, e_j$ with monomial ideals $I_1, \ldots, I_r$. By Corollary 5.1.19, we have $\mathrm{HF}_M(i) = \sum_{j=1}^r (\mathrm{HF}_P(i - \delta_j) - \mathrm{HF}_{I_j}(i - \delta_j))$ for all $i \in \mathbb{Z}$.

Since HF_P is an integer function of polynomial type by Proposition 5.1.13 and Example 5.1.9, and since the set of integer functions of polynomial type is a $\mathbb{Z}$-module, it suffices to show that the Hilbert function HF_I of any monomial ideal $I \subseteq P$ is an integer function of polynomial type. We write $I = (t_1, \ldots, t_s)$ with terms $t_1, \ldots, t_s \in \mathbb{T}^n$ and proceed by induction on s. For $s = 0$, we have $I = (0)$ and $\mathrm{HF}_I(i) = 0$ for all $i \in \mathbb{Z}$.

Now suppose $s > 0$, and let $d = \deg(t_s)$. By Corollary 5.1.17, we have a homogeneous exact sequence

$$0 \to [P/((t_1, \ldots, t_{s-1}) :_P (t_s))]\,(-d) \to P/(t_1, \ldots, t_{s-1}) \to P/(t_1, \ldots, t_s) \to 0$$

Furthermore, it is easy to check that $(t_1, \ldots, t_{s-1}) :_P (t_s) = (t_{s1}, \ldots, t_{s\,s-1})$, where $t_{sj} = \mathrm{lcm}(t_s, t_j)/t_s$ for $j = 1, \ldots, s-1$. Hence we have

$$\begin{aligned} \mathrm{HF}_I(i) &= \mathrm{HF}_P(i) - \mathrm{HF}_{P/I}(i) \\ &= \mathrm{HF}_P(i) - \mathrm{HF}_{P/(t_1,\ldots,t_{s-1})}(i) + \mathrm{HF}_{P/(t_{s1},\ldots,t_{s\,s-1})}(i-d) \\ &= \mathrm{HF}_{(t_1,\ldots,t_{s-1})}(i) + \mathrm{HF}_P(i-d) - \mathrm{HF}_{(t_{s1},\ldots,t_{s\,s-1})}(i-d) \end{aligned}$$

and the claim follows from the induction hypothesis. □

Exercise 1. Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be the integer function defined by $f(i) = i!$ for $i > 0$ and $f(i) = 0$ for $i \leq 0$. Show that f is not of polynomial type.

Exercise 2. Let K be a field, and let $P = K[x_1, \ldots, x_n]$ be standard graded. Describe all homogeneous ideals $I \subseteq P$ such that $\mathrm{HF}_{P/I}(i) = 1$ for every $i \geq 0$.

Exercise 3. Let $i \in \mathbb{N}$. Find an ideal I in a polynomial ring P such that the regularity index of $\mathrm{HF}_{P/I}$ is i.

Exercise 4. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let $\varphi : P_1 \longrightarrow P_1$ be an isomorphism of K-vector spaces.

a) Show that there exists a bijective homogeneous K-algebra homomorphism $\Phi : P \longrightarrow P$ which extends φ.
b) Prove that $\mathrm{HF}_{P/I} = \mathrm{HF}_{P/\Phi(I)}$ for every homogeneous ideal $I \subseteq P$.

Exercise 5. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let $f_1, f_2 \in P \setminus \{0\}$ be two coprime homogeneous polynomials of degrees d_1, d_2, respectively. Show that, for all $i \in \mathbb{Z}$, we have

$$\mathrm{HF}_{P/(f_1,f_2)}(i) = \mathrm{HF}_P(i) - \mathrm{HF}_P(i-d_1) - \mathrm{HF}_P(i-d_2) + \mathrm{HF}_P(i-d_1-d_2)$$

Exercise 6. Let $P = \mathbb{Q}[x, y]$, let $p = x^2 + y^2$, and consider the integer function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $f(i) = \#\,\mathrm{Supp}(p^i)$ for $i \geq 0$ and $f(i) = 0$ for $i < 0$. Show that f is of polynomial type and determine its associated polynomial and regularity index.

Exercise 7. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let M be a finitely generated graded P-module. Suppose that we have two presentations $M \cong F/N$ and $M \cong F'/N'$, where $F = \bigoplus_{i=1}^{r} P(-\delta_i)$ and $F' = \bigoplus_{j=1}^{r'} P(-\delta'_j)$ are two finitely generated graded free P-modules, where N is a graded submodule of F, and where N' is a graded submodule of F'. Let $\varphi : F/N \longrightarrow F'/N'$ be the corresponding isomorphism of graded P-modules. Given a field extension $K \subseteq L$, let $\overline{P} = L[x_1, \ldots, x_n]$ and $\overline{F} = \bigoplus_{i=1}^{r} \overline{P}(-\delta_i)$ as well as $\overline{F'} = \bigoplus_{j=1}^{r'} \overline{P}(-\delta'_j)$.

a) Show that the map φ induces an isomorphism of graded P-modules $\overline{\varphi} : \overline{F}/N\,\overline{F} \longrightarrow \overline{F'}/N'\,\overline{F'}$.
b) Conclude that the module $M \otimes_K L$ is well-defined.

Tutorial 64: Hilbert Functions and Graded Free Resolutions

A good resolution is like an old horse,
which is often saddled but rarely ridden.
(Mexican Proverb)

Using the fact that Hilbert functions are additive on short exact sequences, we can derive relations between the Hilbert function of a graded module and its graded Betti numbers. In the following we examine those relations more closely. In particular, we ask you to prove that the graded Betti numbers determine the Hilbert function, but that the converse is not true in general.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let M be a finitely generated graded P-module, and let

$$0 \longrightarrow F_\ell \xrightarrow{\varphi_\ell} F_{\ell-1} \xrightarrow{\varphi_{\ell-1}} \cdots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

be its minimal graded free resolution, where $F_i = \bigoplus_{j\in\mathbb{Z}} P(-j)^{\beta_{ij}}$ is a graded free P-module and the numbers β_{ij} are the graded Betti numbers of M.

a) Prove that the Hilbert functions satisfy $\mathrm{HF}_M(i) = \sum_{j=0}^{\ell} (-1)^j \,\mathrm{HF}_{F_j}(i)$ for all $i \in \mathbb{Z}$. (*Hint:* Split the resolution into short exact sequences

$$0 \longrightarrow \mathrm{Ker}(\varphi_j) \longrightarrow F_j \xrightarrow{\varphi_j} \mathrm{Ker}(\varphi_{j-1}) \longrightarrow 0$$

and use Proposition 5.1.14.b.)

b) Conclude that $\mathrm{HF}_M(i) = \sum_{j=0}^{\ell} \sum_{k\in\mathbb{Z}} (-1)^j \beta_{jk} \operatorname{bin}_{n-1}(i-k+n-1)$ for all $i \in \mathbb{Z}$.

c) Find the minimal graded free resolutions of the following ideals and modules and use them to compute their Hilbert functions.

1) $M_1 = (x_1x_2,\, x_1x_3,\, x_2x_3) \subseteq \mathbb{Q}[x_1, x_2, x_3]$ (see Tutorial 63.h)
2) $M_2 = (x_1^2 - x_2x_3,\, x_1x_2 - x_3^2,\, x_1x_3 - x_2^2) = I_2\left(\left(\begin{smallmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{smallmatrix}\right)\right) \subseteq \mathbb{Q}[x_1, x_2, x_3]$ (see Tutorial 62). This is the homogeneous vanishing ideal of the **twisted cubic curve** in $\mathbb{P}^3_{\mathbb{Q}}$.
3) $M_3 = (x_1x_4 - x_2x_3,\, x_1^2x_3 - x_2^3,\, x_1x_3^2 - x_2^2x_4,\, x_2x_4^2 - x_3^3) \subseteq \mathbb{Q}[x_1, \ldots, x_4]$ (see Example 4.8.13)
4) $M_4 = \langle (x_1^2, x_1),\, (0, x_2 - x_3) \rangle \subseteq \mathbb{Q}[x_1, x_2, x_3](-1) \oplus \mathbb{Q}[x_1, x_2, x_3]$

d) Let $I = (f, g) \subseteq P$ be an ideal generated by two coprime homogeneous polynomials $f, g \in P$. We say that I is a **complete intersection ideal of type** (a, b), where $a = \deg(f)$ and $b = \deg(g)$. Find the minimal graded free resolution of P/I and use it to give a formula for the Hilbert function of this ring involving only a and b. Moreover, determine the regularity index of P/I.

e) Let $I = (f, g, h) \subseteq P$ be an ideal generated by a homogeneous regular sequence (f, g, h) of length three in P. We say that I is a **complete intersection ideal of type** (a, b, c), where $a = \deg(f)$, $b = \deg(g)$, and $c = \deg(h)$. Find the minimal graded free resolution of P/I and use it to give a formula for the Hilbert function of this ring involving only a, b, and c. Moreover, determine the regularity index of P/I.

f) Consider the graded $\mathbb{Q}[x, y]$-modules $M_1 = \mathbb{Q}[x, y]/(x^2, y^2)$, $M_2 = \mathbb{Q}[x, y]/(x^2, xy, y^3)$, and $M_3 = \mathbb{Q}[x, y]/(xy, x^2 - y^2)$. Show that M_1 and M_2 have the same Hilbert function, but different graded Betti numbers. Furthermore, show that M_1 and M_3 have the same Hilbert function and the same graded Betti numbers, but there is no isomorphism of graded $\mathbb{Q}[x, y]$-modules between them.

The following parts of this tutorial require much more sophisticated algebraic techniques. We advise you to attempt to solve them only if you feel sufficiently comfortable with homological algebra (see Tutorial 33) and localizations (see Section 3.5.a).

g) Let $I \subseteq P$ be a homogeneous ideal such that $\mathrm{HF}_{P/I}(i) = 0$ for $i \geq 2$. Show that this condition uniquely determines the graded Betti numbers of P/I. Find them.
Hint: First reduce the task to the case $\mathrm{HF}_{P/I}(1) = n$. Then dualize the graded free resolution of P/I and show that the dual complex is a minimal graded free resolution of the graded P-module $\operatorname{Hom}_P(P/I, K)(n)$. Now determine the graded Betti numbers β_{n-1j}, β_{nj}.

h) Let $d_1 \ldots, d_\ell \in \mathbb{Z}$, and let $I \subseteq P$ be a homogeneous ideal such that the graded Betti numbers of P/I satisfy $\beta_{ij} = 0$ for $i = 1, \ldots, \ell$ and $j \neq d_i$, and for $i \geq \ell + 1$. Prove that the non-zero graded Betti numbers of I

are given by $\beta_{i\,d_i} = (-1)^{i+1} \prod_{j \neq i} d_j/(d_j - d_i)$.
Hint: Localize the graded free resolution of P/I at $S = P \setminus \{0\}$ and show that $\sum_{i=1}^{\ell} (-1)^i \beta_{i\,d_i} = -1$. Then solve the resulting linear system of equations for the numbers $\beta_{i\,d_i}$ using Vandermonde's determinant and Cramer's rule.

5.2 Hilbert Series

We hear within us the perpetual call:
There is the problem. Seek its solution.
You can find it by pure reason,
for in mathematics there is no ignorabimus.
(David Hilbert)

I would like to call your attention
to a frequently neglected point,
namely the fact that Hilbert's scheme
for the foundation of mathematics
remains highly interesting and important
in spite of my negative results.
(Kurt Gödel)

In the preceding section we were highly successful. We found not merely one numerical invariant attached to a graded module, but infinitely many. Now we risk becoming victims of our own success, because it is not clear how we could ever know all those invariants. Is there a way to get a finite description of those infinitely many numbers or is there some *ignorabimus* after all? A first hint as to how we can seek a solution to this problem is given by Theorem 5.1.21 where we proved that the Hilbert function of a finitely generated graded P-module is an integer function of polynomial type. Hence we could try to determine the regularity index, the associated polynomial, and the first few values of this function in order to completely describe it. Clearly, this would be a rather cumbersome approach, both from the computational and from the conceptual point of view. But it shows that there is hope!

Mathematics is full of wonderful ideas, so let us use one of them. A strikingly powerful method for getting infinity under control is the method of *generating functions*. In the situation at hand, it means that we use the values of the Hilbert function as the coefficients of a univariate power series, or, if the module has some components of negative degree, of a univariate Laurent series. At first glance this seems to gain nothing at all, but then Theorem 5.2.6 comes into play which says that if the coefficients of a power series satisfy some recurrence relation, then that series is really the power series expansion of a rational function, i.e. of the quotient of two polynomials. By pure reason, we have found the blueprint for this section!

In the first subsection we collect the material we need as the theoretical basis for our further studies. We define the rings of univariate power series and Laurent series and examine their elementary ring-theoretic properties. Then we define and characterize rational power series, and finally we show that the associated Laurent series of an integer Laurent function f of polynomial type has the form $\frac{p(z)}{(1-z)^n}$, where $n \in \mathbb{N}$ and $p(z)$ is a Laurent polynomial over $\mathbb{Z}$.

In the second subsection we apply this theory to Hilbert functions. We define Hilbert series of finitely generated graded modules over standard graded

polynomial rings and derive their basic properties from the corresponding properties of Hilbert functions. In particular, we see that Hilbert series are additive on short exact sequences, and that forming the residue class module with respect to a homogeneous non-zerodivisor of degree d corresponds to multiplying the Hilbert series by $1 - z^d$. One useful consequence of the latter property is that, in the homogeneous case, permutations of regular sequences are again regular (see Corollary 5.2.17). Moreover, Hilbert series do not change under passage to the leading term module (see Theorem 5.2.18) and under extensions of the base field (see Corollary 5.2.19). Finally, as indicated by the general theory, we show that Hilbert series of finitely generated graded P-modules are rational power series, and we determine their shape as closely as possible (see Theorem 5.2.20). Although the proof of this theorem provides us with a first insight into how one can actually compute Hilbert series, the hard work of formulating and optimizing concrete algorithms is deferred to the next section.

5.2.A Univariate Power Series

The Power Series instruments
are weatherproof, simple to use,
and give you the information you want
in a package that is small enough
to place where you want it.
(Marine Equipment Advertisement)

In order to introduce power series rings, we shall mimic the construction of polynomial rings in Section 1.1. Besides being weatherproof, they will turn out to be simple to use instruments fundamental to the development of our theory. Later we shall see that some of them are computable such as Hilbert series of finitely generated graded modules. The construction of a package for their computation is an important task in the design of every computer algebra system.

Let R be a ring. Recall that, for us, this always means a commutative ring with identity element. We consider the set $R^{\mathbb{N}}$ of all sequences $(r_0, r_1, \ldots)$ of elements $r_0, r_1, r_2 \ldots$ of R. Using componentwise addition and scalar multiplication, this set becomes an R-module. Next, we equip the R-module $R^{\mathbb{N}}$ with a multiplication. Given two elements $(r_0, r_1, \ldots)$ and $(s_0, s_1, \ldots)$ of $R^{\mathbb{N}}$, we define

$$(r_0, r_1, r_2, \ldots) \cdot (s_0, s_1, s_2, \ldots) = \Big(\sum_{i+j=0} r_i s_j, \sum_{i+j=1} r_i s_j, \sum_{i+j=2} r_i s_j, \ldots \Big)$$

It is easy to check that the set $R^{\mathbb{N}}$, together with componentwise addition and this multiplication, is a commutative ring with identity $(1, 0, 0, \ldots)$.

Definition 5.2.1. Let R be a ring. We equip $R^{\mathbb{N}}$ with the ring structure defined above.

a) If we let $z = (0, 1, 0, 0, \ldots)$, the ring $R^{\mathbb{N}}$ is called the **(formal) power series ring** in the indeterminate z over R and is denoted by $R[[z]]$.
b) For $n \geq 1$, we recursively define $R[[z_1, \ldots, z_n]] = (R[[z_1, \ldots, z_{n-1}]])[[z_n]]$ and call it the **(formal) power series ring** in n indeterminates over R.
c) The elements of a power series ring are called **power series**. Power series in $R[[z]]$ are often called **univariate power series**, while power series in several indeterminates are called **multivariate power series**.

Next we describe some properties of univariate power series.

Proposition 5.2.2. *Let $R[[z]]$ be the univariate power series ring over a ring R.*

a) Every element $f \in R[[z]]$ has a unique representation $f = \sum_{i \geq 0} c_i z^i$ with $c_i \in R$ for all $i \geq 0$.
b) The units in $R[[z]]$ are the power series $f = \sum_{i \geq 0} c_i z^i$ such that c_0 is a unit in R.
c) If R is an integral domain, then $R[[z]]$ is an integral domain, too.

Proof. By induction on i, we see that $z^i = (0, \ldots, 0, 1, 0, 0, \ldots)$ for $i \geq 0$, where 1 is the $(i+1)^{\text{st}}$ entry of the tuple. Given an element $f = (c_0, c_1, \ldots)$ of $R[[z]]$, the sequence of power series $c_0 z^0, c_1 z^1, \ldots$ has the property that there is at most one non-zero component in each position. Therefore its componentwise sum $\sum_{i \geq 0} c_i z^i$ is well-defined. The sum is exactly f, and this representation is clearly unique.

Next we prove b). Given a power series $f = \sum_{i \geq 0} c_i z^i$ which is a unit, there exists a power series $g = \sum_{j \geq 0} d_i z^i$ such that $fg = 1$. Then the representation of fg is

$$f\,g = c_0 d_0 + (c_0 d_1 + c_1 d_0)\, z + (c_0 d_2 + c_1 d_1 + c_2 d_0)\, z^2 + \cdots$$

Therefore we have $c_0 d_0 = 1$. Hence c_0 is a unit of R.

Conversely, let $f = \sum_{i \geq 0} c_i z^i$ be a power series in $R[[z]]$ such that c_0 is a unit of R, and let $d_0 \in R$ be such that $c_0 d_0 = 1$. By induction on i, we can define elements $d_i = -d_0 \cdot \sum_{j=1}^{i} c_j d_{i-j}$ of R for $i > 0$. Then the power series $g = \sum_{j \geq 0} d_j z^j$ satisfies $fg = 1$, i.e. f is a unit in $R[[z]]$.

To prove c), we let $f = \sum_{i \geq 0} c_i z^i$ and $g = \sum_{j \geq 0} d_j z^j$ be non-zero power series. Let $i_0 = \min\{i \in \mathbb{N} \mid c_i \neq 0\}$ and $j_0 = \min\{j \in \mathbb{N} \mid d_j \neq 0\}$. Hence the representation of fg is $c_{i_0} d_{j_0}\, z^{i_0 + j_0} + (c_{i_0} d_{j_0 + 1} + c_{i_0 + 1} d_{j_0})\, z^{i_0 + j_0 + 1} + \cdots$. Thus $c_{i_0} d_{j_0} \neq 0$ implies $fg \neq 0$. □

From now on we shall always denote power series using the representation provided by part a) of this proposition. If the base ring is a field K, we can form both the field of fractions $K(z)$ of $K[z]$ and the localization $K[[z]]_z$. The following proposition describes the way those two rings are related.

Proposition 5.2.3. *Let $K[[z]]$ be the univariate power series ring over a field K.*

a) The localization $K[[z]]_z$ is a field. It is isomorphic to the field of fractions of $K[[z]]$.
b) There is a canonical injective ring homomorphism $\varphi : K(z) \longrightarrow K[[z]]_z$. In other words, the field $K[[z]]_z$ is an extension field of $K(z)$.

Proof. To prove a), we write an element f of $K[[z]]_z \setminus \{0\}$ in the form $f = \frac{g}{z^i}$, where $i \geq 0$ and $g = \sum_{j \geq 0} c_j z^j \in K[[z]]$. Let $m = \min\{j \geq 0 \mid c_j \neq 0\}$ and $h = \sum_{j \geq 0} c_{j+m} z^j$. So, h is a unit of $K[[z]]$ by Proposition 5.2.2.b. Thus the equations $g = z^m h$ and $f \cdot (z^{i-m} h^{-1}) = g \cdot (z^m h)^{-1} = 1$ finish the proof of the first claim of a). To show the second claim of a), it suffices to take a fraction $\frac{f}{g}$ such that $f, g \in K[[z]] \setminus \{0\}$, to write $\frac{1}{g} = \frac{h}{z^i}$ with $i \geq 0$ and $h \in K[[z]]$ using the first claim, and to note that $\frac{f}{g} = \frac{fh}{z^i}$.

An abstract way to prove b) would be to appeal to the universal property of the localization of $K[z]$ in $K[z] \setminus \{0\}$ (see Exercise 3 of Section 3.5). Here we construct the map φ explicitly instead. Every non-zero element of $K(z)$ can be uniquely written in the form $z^i \frac{f}{g}$, where $i \in \mathbb{Z}$ and $f, g \in K[z]$ are coprime polynomials such that $g(0) \neq 0$. By Proposition 5.2.2.b, there exists a power series $h \in K[[z]]$ satisfying $gh = 1$. Now we set $\varphi(z^i \frac{f}{g}) = z^i fh$. It is easy to check that this defines an injective ring homomorphism. □

Based on our characterization of rational power series in Theorem 5.2.6, it is easy to see that the field extension $K(z) \longrightarrow K[[z]]_z$ is not an isomorphism (see also Exercise 2).

Given an integral domain R with field of fractions K, we have further canonical injective ring homomorphisms, namely $R[[z]] \subseteq K[[z]]$ and $R[[z]]_z \subseteq K[[z]]_z$. In particular, we can view $R[[z]]$ and $R[[z]]_z$ and $K(z)$ as subrings of the field $K[[z]]_z$, and their intersections $R[[z]] \cap K(z)$ and $R[[z]]_z \cap K(z)$ are also subrings of $K[[z]]_z$. In order to facilitate our navigation through this tangle of rings, we introduce the following names.

Definition 5.2.4. Let R be an integral domain and K its field of fractions.

a) The subring $R[[z]] \cap K(z)$ of the field $K[[z]]_z$ is called the **ring of rational power series** over R.
b) The localization $R[[z]]_z$ of the power series ring $R[[z]]$ in the element z is called the **ring of Laurent series** in one indeterminate z over R.
c) Finally, the ring $R[z]_z$ is called the **ring of Laurent polynomials** over R. It is sometimes also denoted by $R[z, z^{-1}]$.

Notice that a Laurent series f can be written as $f = \sum_{j \geq -i} c_j z^j$ for some $i \in \mathbb{N}$ with elements $c_j \in R$ for $j \geq -i$. Subsequently, we shall mainly use power series and Laurent series over the ring $R = \mathbb{Z}$. In this case, rational power series can be represented as the quotient of two polynomials of specific

type. Before delving further into this topic, we need some auxiliary results about the ring $\mathbb{Z}[[z]]$.

Lemma 5.2.5. *Let $c_i \in \mathbb{Z}$ for $i \geq 0$, let $f = \sum_{i\geq 0} c_i z^i \in \mathbb{Z}[[z]]$, and let $p \in \mathbb{Z}$ be a prime number.*

a) The number p divides f if and only if $p \mid c_i$ for all $i \geq 0$.
b) The canonical map $\mathbb{Z}[[z]] \longrightarrow \mathbb{Z}/(p)[[z]]$ induces a bijective ring homomorphism $\mathbb{Z}[[z]]/(p \cdot \mathbb{Z}[[z]]) \longrightarrow \mathbb{Z}/(p)[[z]]$.
c) The element $p \in \mathbb{Z}[[z]]$ is a prime element.

Proof. Part a) follows from the fact that, for a power series $g = \sum_{i\geq 0} d_i z^i$, we have $p \cdot g = \sum_{i\geq 0}(p\, d_i)\, z^i$. Part b) is an immediate consequence of a), since the canonical map $\mathbb{Z}[[z]] \longrightarrow \mathbb{Z}/(p)[[z]]$ is obviously a surjective ring homomorphism, and by a) its kernel is precisely $p \cdot \mathbb{Z}[[z]]$. Finally, part c) follows from b), because $\mathbb{Z}/(p)[[z]]$ is an integral domain by Proposition 5.2.2.c. □

Using this lemma, we can characterize rational power series over $\mathbb{Z}$ as follows.

Theorem 5.2.6. (Characterization of Rational Power Series) *Let $c_i \in \mathbb{Z}$ for $i \geq 0$, and let $f = \sum_{i\geq 0} c_i z^i \in \mathbb{Z}[[z]]$. Then the following conditions are equivalent.*

a) The power series f is rational.
b) There exist a polynomial $g \in \mathbb{Z}[z]$ and integers $a_1, \ldots, a_m \in \mathbb{Z}$ such that $f = g/(1 - a_1 z - a_2 z^2 - \cdots - a_m z^m)$.
c) There are natural numbers $m, n \in \mathbb{N}$ and integers $a_1, \ldots, a_m \in \mathbb{Z}$ such that $c_i = a_1 c_{i-1} + a_2 c_{i-2} + \cdots + a_m c_{i-m}$ for all $i > n$.

Proof. First we show that a) implies b). Let $g, h \in \mathbb{Z}[z]$ be polynomials with $h \neq 0$ and $f = g/h$. Without loss of generality we may assume that g and h are coprime. By considering g and h as elements of $\mathbb{Q}[z]$, we can apply Proposition 1.2.8.c and find polynomials $\tilde{g}, \tilde{h} \in \mathbb{Q}[z]$ such that $g\,\tilde{g} + h\,\tilde{h} = 1$. Now we clear denominators and obtain an equation $g\,g^* + h\,h^* = n$ with $g^*, h^* \in \mathbb{Z}[z]$ and $n > 0$. Next we multiply $fh - g = 0$ by g^* and use our equation to get $h(fg^* + h^*) = n$.

Suppose that there is a prime number p dividing n. Then p divides $fg^* + h^*$, because otherwise we have $p \mid h$ by part c) of the lemma, and then p divides $g = fh$, contradicting the coprimality of g and h. By dividing out p and repeating the argument, we see that n divides $fg^* + h^*$. Therefore there exists a power series $f^* \in \mathbb{Z}[[z]]$ such that $nf^* = fg^* + h^*$, and hence $hf^* = 1$. Now Proposition 5.2.2.b yields $h(0) \in \{1, -1\}$, which implies that the representation $f = h(0)g/(h(0)h)$ has the desired form.

To prove that b) implies c), we use the fact that $h = 1 - a_1 z - \cdots - a_m z^m$ is a unit in $\mathbb{Z}[[z]]$ by Proposition 5.2.2.b and write $h^{-1} = \sum_{i\geq 0} b_i z^i$ with $b_0, b_1, \ldots \in \mathbb{Z}$. If we then compare coefficients in $h\,h^{-1} = 1$, we find

$$b_i - a_1 b_{i-1} - a_2 b_{i-2} - \cdots - a_m b_{i-m} = 0 \tag{1}$$

for $i \geq m$. By setting $b_i = 0$ for $i < 0$, we achieve that equation (1) holds for all $i > 0$. But it obviously does not hold for $i = 0$. Next we write $g = d_0 + d_1 z + \cdots + d_n z^n$ with $d_0, \ldots, d_n \in \mathbb{Z}$. We determine the coefficients in $f = g\, h^{-1}$ and find

$$c_i = d_0 b_i + d_1 b_{i-1} + \cdots + d_m b_{i-m} \tag{2}$$

for all $i \in \mathbb{Z}$, where we set $c_i = 0$ for $i < 0$. Now we plug the equations (1) into (2) and obtain $c_i = a_1 c_{i-1} + \cdots + a_m c_{i-m}$ for $i > n$.

Since b) obviously implies a), it remains to show that c) implies b). Let n be the smallest number for which the hypothesis holds, and let $g = \sum_{i \geq 0} d_i z^i$ with $d_i \in \mathbb{Z}$. We compare coefficients in $f \cdot (1 - a_1 z - \cdots - a_m z^m) = g$ and get

$$\begin{aligned}
d_0 &= c_0 \\
d_1 &= c_1 - c_0 a_1 \\
d_2 &= c_2 - c_1 a_1 - c_0 a_2 \\
&\vdots \\
d_n &= c_n - c_{n-1} a_1 - \cdots - c_0 a_n \\
d_i &= c_i - c_{i-1} a_1 - \cdots - c_{i-m} a_m \qquad \text{for } i > n
\end{aligned}$$

where we set $a_i = 0$ for $i > m$. The assumption implies $d_i = 0$ for $i > 0$. Hence $g = d_0 + d_1 z + \cdots + d_n z^n$ satisfies the claim. □

Let us examine the power of this theorem in a well-known case.

Example 5.2.7. Let $c_0, c_1, \ldots$ be the **Fibonacci sequence**, i.e. let $c_0 = c_1 = 1$ and $c_i = c_{i-1} + c_{i-2}$ for $i \geq 2$. Then we have $m = 2$, $n = 1$, and $a_1 = a_2 = 1$ in condition c) of the theorem. Therefore the Fibonacci numbers are the coefficients of the power series $1/(1 - z - z^2) = c_0 + c_1 z + c_2 z^2 + \cdots$.

Furthermore, if we set $c_i = 0$ for $i < 0$, we can consider the integer Laurent function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $f(i) = c_i$ for $i \in \mathbb{Z}$. We note that this is not an integer function of polynomial type, because if a polynomial $p \in \mathbb{IP}$ satisfies $p(i) = c_i$ for large enough i, then $p(i) = p(i-1) + p(i-2)$ implies $\Delta p(i) = p(i-2)$ for large i. But then we have $\deg(\Delta p) = \deg(p)$, contradicting Corollary 5.1.11.a.

This example leads us to the question of how one can recognize Laurent series whose coefficients form an integer function of polynomial type. This is the topic of the remainder of this subsection. Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be a non-zero integer Laurent function. The number $\min\{i \in \mathbb{Z} \mid f(i) \neq 0\}$ will be denoted by α_f or simply α. Moreover, the associated Laurent series $\sum_{i \geq \alpha} f(i)\, z^i$ will be denoted by $\mathrm{HS}_f(z)$. In the next subsection the integer Laurent function f

we consider will be a Hilbert function and its associated Laurent series will be called a Hilbert series.

Let us collect some elementary rules for dealing with Laurent series associated to integer Laurent functions.

Proposition 5.2.8. *Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be a non-zero integer Laurent function.*

a) For every $q \geq 1$, we have $\mathrm{HS}_{\Delta_q f}(z) = (1 - z^q) \cdot \mathrm{HS}_f(z)$.
In particular, we have $\mathrm{HS}_{\Delta f}(z) = (1 - z) \cdot \mathrm{HS}_f(z)$.
b) We have $\mathrm{HS}_{\Sigma f}(z) = \mathrm{HS}_f(z)/(1 - z)$.

Proof. To prove a), we calculate $(1 - z^q)\,\mathrm{HS}_f(z) = (1 - z^q) \sum_{i \geq \alpha} f(i)\, z^i = \sum_{i \geq \alpha} f(i)\, z^i - \sum_{i \geq \alpha + q} f(i - q)\, z^i = \mathrm{HS}_{\Delta_q f}(z)$. Claim b) follows from a), because we have $\mathrm{HS}_f(z) = \mathrm{HS}_{\Delta(\Sigma f)}(z) = (1 - z)\,\mathrm{HS}_{\Sigma f}(z)$. □

For the proof of our next theorem, we need the power series expansion of $(1 - z)^{-n}$ for all $n \geq 1$.

Lemma 5.2.9. *For all $n \geq 1$, we have $(1 - z)^{-n} = \sum_{i \geq 0} \binom{i+n-1}{n-1} z^i$.*

Proof. We proceed by induction on n. For $n = 1$, the geometric series yields $(1 - z)^{-1} = \sum_{i \geq 0} z^i$. Now let $n > 1$. Using the induction hypothesis and Lemma 5.1.6.c, we calculate $(1 - z)^{-n} = (1 - z)(1 - z)^{-n+1} = (\sum_{i \geq 0} z^i)(\sum_{j \geq 0} \binom{j+n-2}{n-2} z^j) = \sum_{i \geq 0} \left[\sum_{j=0}^{i} \binom{j+n-2}{n-2}\right] z^i = \sum_{i \geq 0} \binom{i+n-1}{n-1} z^i$. □

At this point we are ready to characterize those Laurent series which are associated to integer functions of polynomial type.

Theorem 5.2.10. (Characterization of Laurent Series of Integer Functions of Polynomial Type)
For a non-zero integer Laurent function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, the following conditions are equivalent.

a) The integer function f is of polynomial type.
b) The associated Laurent series of f is of the form $\mathrm{HS}_f(z) = \frac{p(z)}{(1-z)^m}$ where $m \in \mathbb{N}$ and $p(z) \in \mathbb{Z}[z, z^{-1}]$ is a Laurent polynomial over $\mathbb{Z}$.

If these conditions are satisfied, we have $m = \deg(\mathrm{HP}_f(t)) + 1$.

Proof. First we prove that a) implies b). Let $m = \deg(\mathrm{HP}_f(t)) + 1$. By Corollary 5.1.11.a, the associated polynomial of the integer function $\Delta^m f$ is $\mathrm{HP}_{\Delta^m f}(t) = \Delta^m\,\mathrm{HP}_f(t) = 0$. Thus the Laurent series $p(z) = \mathrm{HS}_{\Delta^m f}(z)$ is actually a Laurent polynomial, and Proposition 5.2.8 shows that we have $\mathrm{HS}_f(z) = p(z)/(1 - z)^m$.

Conversely, we can use the hypothesis and Proposition 5.2.8 to conclude that the associated Laurent series of $\Delta^m f$ is the Laurent polynomial

$\mathrm{HS}_{\Delta^m f}(z) = p(z) \in \mathbb{Z}[z, z^{-1}]$. In particular, we see that $\Delta^m f(i) = 0$ for all sufficiently large integers i. Thus $\Delta^m f$ is an integer function of polynomial type, and the claim follows from Proposition 5.1.10. □

Notice that the proof of this theorem shows that the Laurent polynomial $p(z)$ in b) is nothing but $\mathrm{HS}_{\Delta^m f}(z)$. Given an integer Laurent function of polynomial type, we relate its associated polynomial, Laurent series, and regularity index as follows.

Corollary 5.2.11. *Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be a non-zero integer Laurent function of polynomial type, and let $\alpha = \min\{i \in \mathbb{Z} \mid f(i) \neq 0\}$.*

a) The associated Laurent series of f has the form $\mathrm{HS}_f(z) = p(z)/(1-z)^m$, where $m \in \mathbb{N}$ and $p(z) \in \mathbb{Z}[z, z^{-1}]$ is a Laurent polynomial of the form $p(z) = \sum_{i=\alpha}^{\beta} c_i z^i$ with $\beta \geq \alpha$, $c_\alpha, \ldots, c_\beta \in \mathbb{Z}$, $c_\alpha \neq 0$, and $c_\beta \neq 0$.

b) If $m > 0$, then we have $\mathrm{HP}_f(t) = \sum_{i=\alpha}^{\beta} c_i \binom{t-i+m-1}{m-1}$, and if $m = 0$, then we have $\mathrm{HP}_f(t) = 0$.

c) We have $\mathrm{ri}(f) = \beta - m + 1$.

Proof. In the light of the theorem, to prove a) we have to show that the Laurent polynomial $p(z)$ starts in degree α. Since we have $p(z) = \mathrm{HS}_{\Delta^m f}(z)$, this follows from the fact that the first non-zero value of $\Delta^m f$ is $\Delta^m f(\alpha)$.

In order to prove claim b), we note that the case $m = 0$ is trivially true. For $m > 0$, we use the lemma and calculate

$$\begin{aligned} \mathrm{HS}_f(z) &= p(z) \cdot (1-z)^{-m} \\ &= \Big(\sum_{i=\alpha}^{\beta} c_i z^i\Big)\Big(\sum_{j \geq 1-m} \tbinom{j+m-1}{m-1} z^j\Big) \\ &= \sum_{i \geq \alpha+1-m} \Big(\sum_{j=\alpha}^{\min\{\beta, i+m-1\}} c_j \tbinom{i-j+m-1}{m-1}\Big) z^i \end{aligned}$$

For $i \geq \beta+1-m$, we therefore get $f(i) = \sum_{j=\alpha}^{\beta} c_j \binom{i-j+m-1}{m-1}$, and the claim follows.

For the proof of c), we use Proposition 5.2.8. We have $\mathrm{HS}_{\Delta^m f}(z) = p(z)$, and therefore $\mathrm{ri}(\Delta^m f) = \beta + 1$. Now Corollary 5.1.11.b shows $\mathrm{ri}(f) = \mathrm{ri}(\Delta^m f) - m = \beta - m + 1$. □

Finally, we apply the preceding results to a concrete case.

Example 5.2.12. Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be the integer Laurent function defined by $f(i) = 0$ for $i < -1$, $f(-1) = f(0) = 4$, $f(1) = 8$, $f(2) = 9$, and $f(i) = 2i^2 - i$ for $i \geq 3$.

Clearly, we have $\mathrm{HP}_f(t) = 2t^2 - t$ and $\mathrm{ri}(f) = 3$. Thus the number m in the preceding corollary equals $m = \deg(\mathrm{HP}_f(t)) + 1 = 3$, and we get $\alpha = -1$ as well as $\beta = \mathrm{ri}(f) + m - 1 = 5$. Hence the associated polynomial of f is of the form $\mathrm{HP}_f(t) = c_{-1}\binom{t+3}{2} + c_0\binom{t+2}{2} + \cdots + c_5\binom{t-3}{2}$, where $c_{-1}, \ldots, c_5 \in \mathbb{Z}$.

In order to find the numbers $c_{-1}, \ldots, c_5$, we could substitute some values ≥ 3 for t and solve the resulting linear system of equations.

Another method follows from the corollary. First we compute $\Delta^3 f$ and get $\Delta^3 f(-1) = 4$, $\Delta^3 f(0) = -8$, $\Delta^3 f(1) = 8$, $\Delta^3 f(2) = -7$, $\Delta^3 f(3) = 8$, $\Delta^3 f(4) = 2$, and $\Delta^3 f(5) = -3$. Therefore we have $p(z) = 4z^{-1} - 8 + 8z - 7z^2 + 8z^3 + 2z^4 - 3z^5$ and $\mathrm{HS}_f(z) = p(z)/(1-z)^3$. The corresponding representation of $\mathrm{HP}_f(t)$ is

$$\mathrm{HP}_f(t) = 4\binom{t+3}{2} - 8\binom{t+2}{2} + 8\binom{t+1}{2} - 7\binom{t}{2} + 8\binom{t-1}{2} + 2\binom{t-2}{2} - 3\binom{t-3}{2}$$

Notice that the integer function $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $g(i) = 0$ for $i < 0$ and $g(i) = 2i^2 - i$ for $i \geq 0$ has the same associated polynomial as f. But since $\mathrm{ri}(g) = 0$ and $g(1)$ is the first non-zero value of g, the representation $\mathrm{HS}_g(z) = (z + 3z^2)/(1-z)^3$ is much easier to compute. Since the difference between f and g is given by $f(-1) - g(-1) = 4$, $f(0) - g(0) = 4$, $f(1) - g(1) = 7$, and $f(2) - g(2) = 3$, we can use HS_g to calculate HS_f by $\mathrm{HS}_f(z) = 4z^{-1} + 4 + 7z + 3z^2 + \frac{z+3z^3}{(1-z)^3}$.

5.2.B Hilbert Series in the Standard Graded Case

Two thirds of the people can't do fractions.
The other half just doesn't care.
(Anonymous)

After filling two thirds of this section with generalities about power series and Laurent series, we now use the other half to apply this theory to the case of Hilbert series. Starting from here, we operate again under the assumptions that K is a field and $P = K[x_1, \ldots, x_n]$ a standard graded polynomial ring. Recall that the Hilbert function of a finitely generated graded P-module is an integer Laurent function by Proposition 5.1.14.c.

Definition 5.2.13. For a finitely generated graded P-module M, the associated Laurent series of the Hilbert function of M is called the **Hilbert series** of M and is denoted by HS_M. In other words, the Hilbert series of M is the Laurent series $\mathrm{HS}_M(z) = \sum_{i \geq \alpha} \mathrm{HF}_M(i)\, z^i \in \mathbb{Z}[[z]]_z$, where $\alpha = \alpha(M)$ is the initial degree of M (see Definition 4.7.9.c).

Since the coefficients of this Laurent series are the values of the Hilbert function of M, the results of Section 5.1.B can be translated into statements about Hilbert series of finitely generated graded modules. This task is accomplished by the following four propositions.

Proposition 5.2.14. *The Hilbert series of P is given by* $\mathrm{HS}_P(z) = \frac{1}{(1-z)^n}$.

Proof. By Proposition 5.1.13, the Hilbert function of P is given by $\mathrm{HF}_P(i) = \mathrm{bin}_{n-1}(i + n - 1)$ for all $i \in \mathbb{Z}$, and by Lemma 5.2.9, these numbers are precisely the coefficients of the power series expansion of $1/(1-z)^n$. □

Proposition 5.2.15. (Basic Properties of Hilbert Series)
Let M, M', M'' be three finitely generated graded P-modules.

a) For all $j \in \mathbb{Z}$, we have $\mathrm{HS}_{M(j)}(z) = z^{-j}\ \mathrm{HS}_M(z)$.
b) Given a homogeneous exact sequence $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$, we have $\mathrm{HS}_M(z) = \mathrm{HS}_{M'}(z) + \mathrm{HS}_{M''}(z)$.
c) Let $M = M_1 \oplus \cdots \oplus M_r$ with finitely generated graded P-modules $M_1, \ldots, M_r$. Then we have $\mathrm{HS}_M(z) = \mathrm{HS}_{M_1}(z) + \cdots + \mathrm{HS}_{M_r}(z)$.
d) Let $\delta_1, \ldots, \delta_r \in \mathbb{Z}$. Then the Hilbert series of the graded free module $F = \bigoplus_{j=1}^r P(-\delta_i)$ is $\mathrm{HS}_F(z) = (\sum_{j=1}^r z^{\delta_j})/(1-z)^n$.

Proof. Part a) follows coefficientwise from Proposition 5.1.14.a, because if we let $\alpha = \min\{i \in \mathbb{Z} \mid M_i \neq 0\}$, we have $\mathrm{HS}_{M(j)}(z) = \sum_{i \geq \alpha - j} \mathrm{HF}_{M(j)}(i)\, z^i = \sum_{i \geq \alpha - j} \mathrm{HF}_M(i+j)\, z^i = z^{-j} \sum_{i \geq \alpha} \mathrm{HF}_M(i)\, z^i = z^{-j}\ \mathrm{HS}_M(z)$. The remaining claims are immediate consequences of the corresponding parts of Proposition 5.1.14.a and of Proposition 5.2.14. □

The Hilbert series version of the multiplication sequence reads as follows.

Proposition 5.2.16. *Let M be a finitely generated graded P-module, and let $f \in P \setminus \{0\}$ be a homogeneous polynomial of degree d. Then we have $\mathrm{HS}_{M/fM}(z) = \mathrm{HS}_M(z) - z^d\ \mathrm{HS}_{M/(0:_M(f))}(z)$.*

In particular, the polynomial f is a non-zerodivisor for the module M if and only if $\mathrm{HS}_{M/fM}(z) = (1-z^d)\ \mathrm{HS}_M(z)$.

Proof. To prove the first claim, it suffices to apply the Multiplication Sequence 5.1.16 and to use the basic properties listed above. The second claim follows from Propositions 5.1.16.c and 5.2.8.a. □

In the case $M = P/I$, this proposition can be rewritten in the spirit of Corollary 5.1.17. We leave this job to the reader and generalize the case of a homogeneous non-zerodivisor to a homogeneous regular sequence instead.

Corollary 5.2.17. *Let M be a finitely generated graded P-module, and let $f_1, \ldots, f_\ell \in P$ be homogeneous polynomials of degrees $d_1, \ldots, d_\ell$ respectively. Then the following conditions are equivalent.*

a) The sequence $f_1, \ldots, f_\ell$ is a regular sequence for M.
b) We have $\mathrm{HS}_{M/(f_1,\ldots,f_\ell)M}(z) = \prod_{i=1}^{\ell}(1-z^{d_i})\ \mathrm{HS}_M(z)$.
c) For every permutation $\sigma(1), \ldots, \sigma(\ell)$ of the sequence $1, \ldots, \ell$, the sequence $f_{\sigma(1)}, \ldots, f_{\sigma(\ell)}$ is a regular sequence for M.

Proof. The equivalence of a) and b) follows from the proposition by induction on ℓ. This equivalence implies that a) and c) are equivalent, too. □

In Tutorial 33.b we saw an example of a non-homogeneous regular sequence where one of its permutations was not regular. Notice that this corollary makes an example like that impossible in the homogeneous case.

Our next two results follow coefficientwise from the analogous properties of Hilbert functions (see Theorem 5.1.18 and Corollary 5.1.20).

Theorem 5.2.18. (Macaulay's Theorem for Hilbert Series) *Let $\delta_1, \ldots, \delta_r \in \mathbb{Z}$, let M be a graded submodule of the graded free P-module $\bigoplus_{i=1}^r P(-\delta_i)$, and let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. Then we have $\mathrm{HS}_M(z) = \mathrm{HS}_{\mathrm{LT}_\sigma(M)}(z)$.*

As for Hilbert functions, we see that Hilbert series do not change under base field extensions.

Corollary 5.2.19. *Let M be a graded P-module, and let $K \subseteq L$ be a field extension. Then we have $\mathrm{HS}_{M\otimes_K L}(z) = \mathrm{HS}_M(z)$.*

The last theorem of this section provides us with a precise description of the shape of the Hilbert series of a finitely generated graded P-module.

Theorem 5.2.20. *Let M be a non-zero finitely generated graded P-module, and let $\alpha(M) = \min\{i \in \mathbb{Z} \mid M_i \neq 0\}$. Then the Hilbert series of M has the form*

$$\mathrm{HS}_M(z) = \frac{z^{\alpha(M)}\,\mathrm{HN}_M(z)}{(1-z)^n}$$

where $\mathrm{HN}_M(z) \in \mathbb{Z}[z]$ and $\mathrm{HN}_M(0) = \mathrm{HF}_M(\alpha(M)) > 0$. Note that n is the number of indeterminates of P.

Proof. By Theorem 5.1.21, the Hilbert function of M is an integer Laurent function of polynomial type. Hence Theorem 5.2.10 shows that $\mathrm{HS}_M(z)$ is of the form $\frac{p(z)}{(1-z)^m}$, where $p(z) \in \mathbb{Z}[z, z^{-1}]$ is a Laurent polynomial and $m-1$ is the degree of the associated polynomial of HF_M. We claim that $m \leq n$.

To prove this claim, we choose a homogeneous presentation $M \cong F/N$ with a graded free P-module F and a graded submodule N of F. Since $\mathrm{HF}_M(i) \leq \mathrm{HF}_F(i)$, we have $\deg(\mathrm{HP}_{\mathrm{HF}_M}) \leq \deg(\mathrm{HP}_{\mathrm{HF}_F})$. The degree of the right-hand side is $n-1$ by Proposition 5.1.14.d. Therefore we have $m = 1 + \deg(\mathrm{HP}_{\mathrm{HF}_M}) \leq 1 + \deg(\mathrm{HP}_{\mathrm{HF}_F}) = n$, as we wanted to show.

Now let $p(z) = c_\alpha z^\alpha + c_{\alpha+1} z^{\alpha+1} + \cdots + c_\beta z^\beta$, where $\alpha, \beta \in \mathbb{Z}$ satisfy $\alpha \leq \beta$ and where $c_\alpha, \ldots, c_\beta \in \mathbb{Z}$. Using $\frac{1}{(1-z)^n} = 1 + nz + \binom{n+1}{2} z^2 + \cdots$, we see that $\mathrm{HS}_M(z) = c_\alpha z^\alpha + (\textit{terms of higher degree})$. Hence α equals the initial degree $\alpha(M)$ of M and $c_\alpha = \mathrm{HF}_M(\alpha) > 0$. □

In other words, the Hilbert series of a graded module M is completely determined by its initial degree α and the polynomial $\mathrm{HN}_M(z) \in \mathbb{Z}[z]$. In order to compute the Hilbert series of M, it is therefore sufficient to compute $\mathrm{HN}_M(z)$. Let us give this polynomial a name.

Definition 5.2.21. Given a finitely generated graded P-module M with initial degree $\alpha = \min\{i \in \mathbb{Z} \mid M_i \neq 0\}$ and Hilbert series $\mathrm{HS}_M(z) = \frac{z^\alpha\,\mathrm{HN}_M(z)}{(1-z)^n}$, the polynomial $\mathrm{HN}_M(z) \in \mathbb{Z}[z]$ is called the **Hilbert numerator** of M.

Exercise 1. Let $R = K[[z_1, \ldots, z_n]]$ be a power series ring over a field K.

a) Show that a power series $f \in R$ is a unit in R if and only if $f(0, \ldots, 0) \neq 0$.
b) Prove that R has exactly one maximal ideal. Describe it!

Exercise 2. Show that the power series $\sum_{i \geq 1} z^{i!} \in \mathbb{Z}[[z]]$ is not rational.

Exercise 3. (A combinatorial identity)
For all $n \geq 1$ and $d > 0$, show that $\binom{d+n-1}{n-1} = \sum_{i=1}^{d} (-1)^{i+1} \binom{n}{i} \binom{d-i+n-1}{n-1}$.

Exercise 4. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let I be a homogeneous ideal in P which is $(x_1, \ldots, x_n)$-primary (see Tutorial 43). Show that $\mathrm{HS}_{P/I}(z)$ is a polynomial.

Exercise 5. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let $1 \leq s \leq n$, and let $f_1, \ldots, f_s$ be a homogeneous regular sequence for P. For $i = 1, \ldots, s$, we let $d_i = \deg(f_i)$. A ring of the form $P/(f_1, \ldots, f_s)$ is called a **homogeneous complete intersection of type** $(d_1, \ldots, d_s)$. Show that the Hilbert series of a homogeneous complete intersection of type $(d_1, \ldots, d_s)$ is given by

$$\mathrm{HS}_{P/(f_1,\ldots,f_s)}(z) = \frac{\prod_{i=1}^{s} (1 + z + z^2 + \cdots + z^{d_i - 1})}{(1-z)^{n-s}}$$

Exercise 6. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let $I, J \subseteq P$ be two homogeneous ideals of P. Prove the following equalities.

a) $\mathrm{HN}_{P/I}(z) + \mathrm{HN}_{P/J}(z) = \mathrm{HN}_{P/(I+J)}(z) + \mathrm{HN}_{P/(I \cap J)}(z)$
b) $z^{\alpha(I)} \mathrm{HN}_I(z) + z^{\alpha(J)} \mathrm{HN}_J(z) = z^{\alpha(I+J)} \mathrm{HN}_{I+J}(z) + z^{\alpha(I \cap J)} \mathrm{HN}_{I \cap J}(z)$

Exercise 7. Find a standard graded polynomial ring P and a finitely generated graded P-module M whose Hilbert series is $\mathrm{HS}_M(z) = \frac{z^{-1}}{(1-z)}$.

Exercise 8. Consider the rational power series $f = \frac{1}{1-z^2} \in \mathbb{Q}[[z]]$.

a) Find a recurrence relation which describes the coefficients of f (see Theorem 5.2.6.c).
b) Is there a standard graded K-algebra whose Hilbert series is f?
c) Find a non-standard graded K-algebra whose Hilbert series is f.

Exercise 9. Find a homogeneous ideal I in a standard graded polynomial ring P such that $\Delta(\mathrm{HF}_{P/I})$ is not the Hilbert function of any ring P/J with a homogeneous ideal $J \subseteq P$.

Exercise 10. Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be a non-zero integer Laurent function of polynomial type, and let $d \in \mathbb{N}$ be the degree of its associated integer valued polynomial. Prove that there are integers $e_0, \ldots, e_d$ such that we have the formula

$$\mathrm{HP}_f(t) = \sum_{i=0}^{d} e_i \binom{t+d-i}{d-i}$$

Tutorial 65: Knight Moves

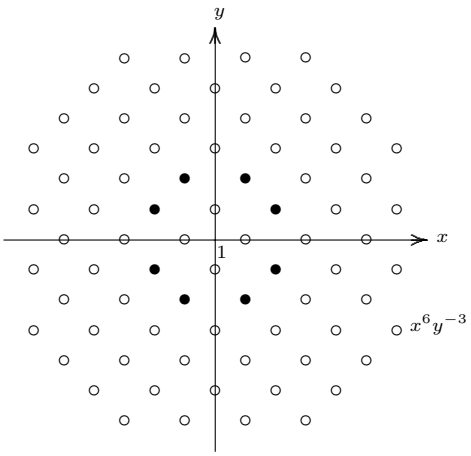
If you can't beat your computer at chess, try kickboxing.
(Anonymous)

How could I lose to such an idiot?
(Aaron Nimzowitch)

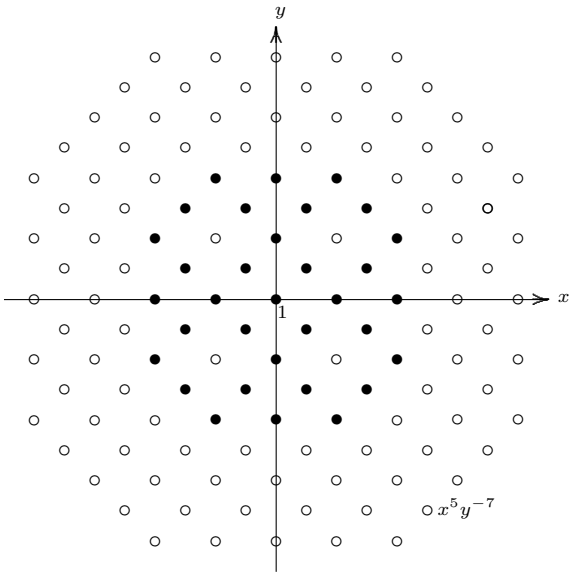
A well-known problem in elementary mathematics asks for the number of squares on an infinite chess board a chess knight can reach in n moves. Here we want to answer this question and similar ones without resorting to complicated induction arguments, but using the power of Computational Commutative Algebra instead.

To begin with, we let K be a field and identify the squares of an infinite chessboard with the (extended) terms in the Laurent polynomial ring $L = K[x, y, x^{-1}, y^{-1}]$. For every $n \in \mathbb{N}$, we let $f(n)$ be the number of squares a chess knight placed at $1 = x^0y^0$ can reach in n moves. Moreover, let $g(n)$ be the number of squares a chess knight placed at 1 can reach in n, but not in fewer moves.

The following picture illustrates the positions contributing to $f(1) = g(1)$ (marked $\bullet$), those contributing to $g(3)$ (marked $\circ$), and to $f(3)$ (all marked positions).



Similarly, we can picture the positions counted in $f(2)$ (marked $\bullet$), in $g(4)$ (marked $\circ$), and in $f(4)$ (all marked positions) as follows.



In the first part of this tutorial, we want to determine the functions $f(n)$ and $g(n)$. Let $M = \{m_1, m_2, \ldots, m_8\}$ be the set of the eight terms in L given by $m_1 = x^2y$, $m_2 = xy^2$, $m_3 = x^{-1}y^2$, $m_4 = x^{-2}y$, $m_5 = x^{-2}y^{-1}$, $m_6 = x^{-1}y^{-2}$, $m_7 = xy^{-2}$, and $m_8 = x^2y^{-1}$.

a) Let $n \in \mathbb{N}$ and $i, j \in \mathbb{Z}$. Show that the square x^iy^j is reachable from 1 in n moves if and only if $x^iy^j \in M^n = \{\mu_1 \cdots \mu_n \mid \mu_j \in M\}$. Conclude that $f(n) = \#M^n$.

b) Prove that $g(n) = \#(M^n \setminus \cup_{i=0}^{n-1} M^i)$ for all $n \in \mathbb{N}$.

c) Compute the first values of $f(n)$ and $g(n)$ by hand. Is it true that we have $g(n) = f(n) - f(n-2)$?

d) Let $P = K[x_1, \ldots, x_8]$ be standard graded, i.e. graded by the matrix $W = (1\ 1\ \cdots\ 1)$. We define a K-algebra homomorphism $\varphi : P \longrightarrow L$ by setting $\varphi(x_i) = m_i$ for $i = 1, \ldots, 8$. Using CoCoA, compute the ideal $I = \ker(\varphi)$. (*Hint:* Use Proposition 3.5.6 to get a presentation of L. Then apply Proposition 3.6.2.)

e) Let $n \in \mathbb{N}$ and $i_1, \ldots, i_n, j_1, \ldots, j_n \in \{1, \ldots, 8\}$. Prove that the two products $m_{i_1} \cdots m_{i_n}$ and $m_{j_1} \cdots m_{j_n}$ are equal in L if and only if the binomial $x_{i_1} \cdots x_{i_n} - x_{j_1} \cdots x_{j_n}$ is contained in I. Conclude that, for every $n \in \mathbb{N}$, the number $\#M^n$ equals $\dim_K(P_n)$ minus the dimension of the space of all such binomials of degree n.

f) Let I_W be the homogeneous part of I (see Tutorial 50). Prove that I and I_W are binomial ideals. Using one of the CoCoA functions from Tutorial 50, compute I_W.

g) Show that f is the Hilbert function of P/I_W. Compute $\mathrm{HS}_{P/I_W}(z)$ and derive a formula for $f(n)$. (*Hint:* Use the method of the proof of Theorem 5.2.6.)

h) Given $n \in \mathbb{N}$ and $i_1, \ldots, i_n \in \{1, \ldots, 8\}$, prove that a product $m_{i_1} \cdots m_{i_n}$ is contained in $M^n \setminus \cup_{i=0}^{n-1} M^i$ if and only if no binomial of the form $x_{i_1} \cdots x_{i_n} - t$ with $t \in \mathbb{T}^8_{\leq n-1}$ is contained in I.

i) Let σ be a degree compatible term ordering on $\mathbb{T}^8$. Show that there is a binomial of the form $t - t' \in I$ with $t, t' \in \mathbb{T}^8$ and $\deg(t) > \deg(t')$ if and only if $t \in \mathrm{LT}_\sigma(I)$. Conclude that g is the Hilbert function of $P/\mathrm{LT}_\sigma(I)$.

j) Using CoCoA, compute the Hilbert series of $P/\mathrm{LT}_\sigma(I)$ and derive a formula for $g(n)$.

In the second part of this tutorial, we want to generalize the above method to count products of **extended terms** or **Laurent terms**, i.e. terms in Laurent polynomial rings. Let K be a field, let $L = K[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}]$ be a Laurent polynomial ring, and let $M = \{m_1, \ldots, m_s\}$ be a finite set of Laurent terms. Our goal is to determine the numbers $f(n) = \#M^n$ and $g(n) = \#(M^n \setminus \cup_{i=0}^{n-1} M^i)$ for every $n \in \mathbb{N}$.

k) Let $P = K[y_1, \ldots, y_s]$ be standard graded. Define a homomorphism of K-algebras $\varphi : P \longrightarrow L$ by setting $\varphi(y_i) = m_i$ for $i = 1, \ldots, s$. Write a CoCoA function `RelationIdeal(...)` which takes the tuple $(\log(m_1), \ldots, \log(m_s))$ and computes the ideal $I = \ker(\varphi)$.

l) Prove that, for every $n \in \mathbb{N}$, the value $f(n)$ is equal to $\mathrm{HF}_{P/I_W}(n)$, where $W = (1\ 1\ \cdots\ 1) \in \mathrm{Mat}_{1,s}(\mathbb{Z})$ and I_W is the homogeneous part of I.

m) Write a CoCoA function `LaurentProducts(...)` which computes the function $f(n)$. (*Hint:* You may use the built-in CoCoA function `Hilbert(...)`.)

n) Prove that, for every $n \in \mathbb{N}$, the value $g(n)$ is equal to $\mathrm{HF}_{P/\mathrm{LT}_\sigma(I)}(n)$, where σ is a degree compatible term ordering on $\mathbb{T}^s$.

o) Write a CoCoA function `NewLaurentProducts(...)` which computes the function $g(n)$.

p) Try your functions for computing $f(n)$ and $g(n)$ in the following cases.

1) $M_1 = \{x, xy, y, x^{-1}y, x^{-1}, x^{-1}y^{-1}, y^{-1}, xy^{-1}\}$ in $K[x, y, x^{-1}, y^{-1}]$ (What does this mean in chess?)
2) $M_2 = \{xy, x^{-1}y, x^{-1}y^{-1}, xy^{-1}\}$ in $K[x, y, x^{-1}, y^{-1}]$ (Picture this!)
3) $M_3 = \{x^i y^j z^k \mid i, j, k \in \mathbb{Z},\ i^2+j^2+k^2 = 5\}$ in $K[x, y, z, x^{-1}, y^{-1}, z^{-1}]$ (The knight in spatial chess!)

Avoid the crowd.
Do your own thinking independently.
Be the chess player, not the chess piece.
(Ralph Charell)

Tutorial 66: Veronese Subrings

In algebraic geometry, Veronese varieties are well-studied objects. In this tutorial we examine the algebraic analog of taking a Veronese embedding of a projective variety. Moreover, we want to understand how this process affects the Hilbert series of the corresponding coordinate rings. Let K be a field, and let R be a standard graded K-algebra, i.e. a K-algebra of the form $R = P/I$, where $P = K[x_1, \ldots, x_n]$ is standard graded and $I \subseteq P$ is a homogeneous ideal.

For every $d > 0$, we let $R^{(d)}$ be the $\mathbb{N}$-graded K-algebra whose i^{th} homogeneous component is $R^{(d)}_i = R_{di}$ for all $i \geq 0$. The ring $R^{(d)}$ is called the d^{th} **Veronese subring** of R.

a) Show that $R^{(d)}$ is a standard graded K-algebra.
b) For the case $R = P$, find an explicit presentation of $P^{(d)}$. More precisely, show that $P^{(d)} \cong K[y_1, \ldots, y_N]/J_d$, where $N = \binom{d+n-1}{n-1}$ and J_d is the following ideal. Let $t_1, \ldots, t_N$ be the terms of degree d in $\mathbb{T}^n$. Then J_d is generated by all polynomials $y_i y_j - y_k y_\ell$ for $i, j, k, \ell \in \{1, \ldots, N\}$ such that $t_i t_j = t_k t_\ell$. (*Hint:* Represent J_d as the kernel of a suitable K-algebra homomorphism. Then show that it is a binomial ideal.)
The projective variety $\mathcal{V}_d(\mathbb{P}^{n-1}) = \mathcal{Z}(J_d) \subseteq \mathbb{P}^{N-1}$ is called the d^{th} **Veronese variety**. Notice that the ideal J_d is a toric ideal (see Tutorials 38 and 45).
c) Write a CoCoA function `VeroneseIdeal(...)` which takes $d > 0$ and a homogeneous ideal I in the current ring P and computes an ideal J in a polynomial ring $K[y_1, \ldots, y_N]$ such that we have $R^{(d)} \cong K[y_1, \ldots, y_N]/J$, where $R = P/I$.

Now suppose we are given a Laurent series $f = \sum_{i \geq i_0} c_i z^i \in \mathbb{Z}[[z]]_z$ and a number $d > 0$. Then we define $f^{(d)} = \sum_{i \in \mathbb{Z}} c_{di} z^{di}$ and $\text{Ver}_d(f) = \sum_{i \in \mathbb{Z}} c_{di} z^i$. The Laurent series $\text{Ver}_d(f)$ is called the d^{th} **Veronese series** associated to f. Our next goal is to compute some Veronese series which are associated to important Hilbert series. For this, we need a few transformation rules. Let $g \in \mathbb{Z}[[z]]_z$ be a further Laurent series, and let $h(z) = f(z^d)g(z)$.

d) Show that $h^{(d)}(z) = f(z^d)g^{(d)}(z)$.
e) Using d), prove that $\text{Ver}_d(h) = f \cdot \text{Ver}_d(g)$.
f) Conclude that if f has the form $f(z) = \frac{p(z)}{(1-z)^n}$ for some Laurent polynomial $p(z) \in \mathbb{Z}[[z]]$, then we have $\text{Ver}_d(f) = \frac{\text{Ver}_d((1+z+\cdots+z^{d-1})^n\, p(z))}{(1-z)^n}$.
g) Using f), compute $\text{Ver}_3(\frac{1+z}{(1-z)^2})$.
h) In the situation of f) let $\tilde{f} : \mathbb{Z} \longrightarrow \mathbb{Z}$ be the integer Laurent function such that $\text{HS}_{\tilde{f}} = \text{Ver}_d(f)$, and let $\delta = \deg(p)$. Then prove that we have $\text{ri}(\tilde{f}) \leq \lfloor \frac{\delta - n}{d} \rfloor + 1$. Here $\lfloor q \rfloor$ is the function which maps a rational number q to the largest integer $\leq q$.

i) Show that the preceding inequality is not always an equality by examining the case $g(z) = (1 + z + z^2 + z^3 - 2z^4 + z^5)/(1 - z)^2$ with $d = 2$.
j) Next suppose $f = \mathrm{HS}_R$. Show that $\mathrm{Ver}_d(f)$ is the Hilbert series of the Veronese subring $R^{(d)}$.
k) Let $Q = K[x_1, x_2]$ and $d \geq 1$. Prove that the Hilbert series of $Q^{(d)}$ is $\mathrm{HS}_{Q^{(d)}}(z) = \frac{1+(d-1)z}{(1-z)^2}$.
l) Write a CoCoA function `VeroneseHS(...)` which takes a number $d > 0$ and a homogeneous ideal I in the current ring P and computes the Hilbert series of the d^{th} Veronese subring of $R = P/I$.
Hint: In order to compute the Hilbert series of R, you may use the built-in CoCoA function `Poincare(...)`. Now apply f).
m) Use your function `VeroneseHS(...)` to compute the Hilbert series of the following Veronese subrings.
   1) $d \in \{2, 3, 4, 5\}$, $I = (0)$, $n \in \{1, 2, 3\}$
   2) $d \in \{2, 3, 4\}$, $I = (x^3 + y^3 + z^3) \subseteq K[x, y, z]$
   3) $d \in \{2, 3\}$, $I = (x_1^2 - x_2x_3,\, x_2^2 - x_3x_4) \subseteq K[x_1, \ldots, x_4]$
n) For $i \in \{0, \ldots, d-1\}$ and $j \in \mathbb{Z}$, we let $(M^{(i)})_j = R_{i+dj}$. Prove that $M^{(i)} = \bigoplus_{j\in\mathbb{N}}(M^{(i)})_j$ is a finitely generated graded $R^{(d)}$-module.
o) Show that R, considered as an $R^{(d)}$-module, satisfies $R \cong \bigoplus_{i=0}^{d-1} M^{(i)}$. Is this an isomorphism of graded $R^{(d)}$-modules?
p) Using f) again, write a CoCoA function `VeroneseModuleHS(...)` which takes $d > 0$, $i \in \{0, \ldots, d-1\}$, and a homogeneous ideal $I \subseteq P$ and computes the Hilbert series of the module $M^{(i)}$ over $R^{(d)} = (P/I)^{(d)}$.
Hint: Show that the Hilbert series of $M^{(i)}$ over $R^{(d)}$ is given by $\mathrm{Ver}_d(z^{-i}\ \mathrm{HS}_{P/I}(z))$.
q) Apply your function `VeroneseModuleHS(...)` to compute the Hilbert series of all possible modules $M^{(i)}$ in the cases of m).

Tutorial 67: Powers of Polynomials and Ehrhart Functions

What is the power of polynomials?
Just look at their powers,
the growth of their size is polynomial.
(Anonymous)

In Tutorial 42 we studied some strange polynomials. Their behaviour was atypical in the sense that the square of each had fewer terms in its support than the polynomial itself. However, to discover such polynomials, we had to look for very special coefficients. In other words, such a property is truly strange, because it is far from being shared by a generic polynomial. So, the current question is: what is the generic size of a power of a polynomial? How many terms are there in the support of these powers? After working for a while in Computational Commutative Algebra, we have grown accustomed

to the expressive power of polynomials. In this tutorial, we are concerned with measuring the *size* of their powers.

Let K be a field, and let $P = K[x_1, \ldots, x_n]$. For a non-zero polynomial $f \in P$, we let $\mathrm{LSupp}(f) = \{\log(t) \mid t \in \mathrm{Supp}(f)\} \subseteq \mathbb{N}^n$ be the **logarithmic support** of f. Recall that in Tutorial 13 we defined the **Newton polytope** of f as the convex hull of $\mathrm{LSupp}(f)$. Moreover, given a subset S of $\mathbb{N}^n$ and a positive integer $i \in \mathbb{N}_+$, we define

$$i\,S = \{p_1 + \cdots + p_i \mid p_1, \ldots, p_i \in S\}$$

a) Show that $i\,\mathrm{conv}(S) = \mathrm{conv}(i\,S)$ for every $i \geq 1$ and every $S \subseteq \mathbb{N}^n$.
b) Prove that $\#\,\mathrm{Supp}(f^i) = \#\mathrm{LSupp}(f^i) \leq \#(i\,\mathrm{LSupp}(f))$ for every $i \geq 1$.

In the following we let $\mathrm{char}(K) = 0$. Given $S = \{t_1, \ldots, t_r\} \subseteq \mathbb{T}^n$, we say that a property holds for **generic polynomials** with support in S if there exists a non-trivial system of polynomial equations in r indeterminates such that the property holds for every polynomial $a_1t_1 + \cdots + a_rt_r$ for which $(a_1, \ldots, a_r) \in K^r$ is not a solution of the system.

c) Let $i \geq 1$, and let $S \subseteq \mathbb{T}^n$ be a non-empty finite subset. Show that we have $\#(\mathrm{LSupp}(g^i)) = \#(i\,\mathrm{LSupp}(g))$ and $\mathrm{Newton}(g^i) = i\,\mathrm{Newton}(g)$ for generic polynomials g with support in S.
d) Let $i \geq 1$ and $S = \{t_1, \ldots, t_r\} \subseteq \mathbb{T}^n$ a non-empty subset. Prove that every polynomial $g = a_1t_1 + \cdots + a_rt_r$ with $a_1, \ldots, a_r \in \mathbb{N}_+$ satisfies $\#\mathrm{LSupp}(g^i) = \#(i\,\mathrm{LSupp}(g))$ and $\mathrm{Newton}(g^i) = i\,\mathrm{Newton}(g)$.

Considering these results, we assume hereinafter that $S = \{t_1, \ldots, t_r\}$ is a non-empty subset of $\mathbb{T}^n$ and that $f \in P$ is a generic polynomial with support in S, or $f = a_1t_1 + \cdots + a_rt_r$ with positive integers $a_1, \ldots, a_r$. To measure the size of $\mathrm{Supp}(f^i)$ for $i \geq 1$, we want to bring Hilbert functions into play. A term in the support of f^i is of the form $t_1^{\alpha_1} \cdots t_r^{\alpha_r}$ with $\alpha_1 + \cdots + \alpha_r = i$. Thus we can view this term as a power product in $t_1, \ldots, t_r$, and if $t_1, \ldots, t_r$ were distinct indeterminates, it would be sufficient to count those power products.

e) For every $i \geq 1$, prove that $\#\,\mathrm{Supp}(f^i) \leq \binom{r+i-1}{i-1}$. Find an example where this is a strict inequality.

So, the terms $t_1, \ldots, t_r$ do not behave like indeterminates. For counting the terms in $\mathrm{Supp}(f^i)$ using a suitable Hilbert function, we need at least the property that $\mathrm{Supp}(f^i) \cap \mathrm{Supp}(f^j) = \emptyset$ for $i \neq j$. Unfortunately, not even this is true in general, as the example $f = x + x^2$ shows, where we have $\mathrm{Supp}(f) \cap \mathrm{Supp}(f^2) = \{x^2\}$. But for this problem there exist remedies, and we shall examine two of them. The first one uses the homogenization of f and is based on the observation that the terms in the support of different powers of a homogeneous polynomial have different degrees. The second remedy is to multiply f by a new indeterminate y_0 and to observe that the terms in $\mathrm{Supp}((y_0 f)^i)$ have degree i in y_0.

To implement the first method, consider the homogenization $F = f^{\text{hom}}$ of f in $\overline{P} = K[x_0, \ldots, x_n]$. Let $\text{Supp}(F) = \{\bar{t}_1, \ldots, \bar{t}_r\}$, and let $I \subseteq \overline{P}$ be the monomial ideal generated by $\{\bar{t}_1, \ldots, \bar{t}_r\}$.

f) For every $i \geq 1$, show that $\#\,\text{Supp}(f^i)$ is the minimal number of generators of I^i.

g) Give an example which shows that f) is not true if $\text{char}(K) > 0$.

Let $y_1, \ldots, y_r$ be further indeterminates, and let $Q = K[y_1, \ldots, y_r]$ be standard graded. In Tutorial 38 we defined the toric ideal associated to the matrix $(\log(\bar{t}_1), \ldots, \log(\bar{t}_r)) \in \text{Mat}_{n+1,r}(\mathbb{N})$ by $J = (y_1 - \bar{t}_1, \ldots, y_r - \bar{t}_r) \cap Q$.

h) Show that J is a homogeneous ideal. Then prove $\#\,\text{Supp}(f^i) = \text{HF}_{Q/J}(i)$ for every $i \geq 1$.

i) Give an example which shows that h) is not true if $\text{char}(K) > 0$.

j) Write a CoCoA function `SuppSize(...)` which takes a non-empty finite subset $S \subseteq \mathbb{T}^n$ and computes the power series $\sum_{i \geq 0} \#\,\text{Supp}(f^i) z^i$, where $f \in \mathbb{Q}[x_1, \ldots, x_n]$ is a generic polynomial with support in S.

k) Apply your function `SuppSize(...)` to the following cases.

1) $S_1 = \{x_1^2,\, x_1x_2, x_2^2\} \subseteq \mathbb{T}^2$
2) $S_2 = \{x_1x_2x_3,\, x_1^4,\, x_2^4,\, x_3^4,\, x_1^3x_2^2,\, x_2^3x_3^2,\, x_1^2x_3^3\} \subseteq \mathbb{T}^3$
3) $S_3 = \{x_{i_1} \cdots x_{i_5} \mid 1 \leq i_1 < \cdots < i_5 \leq 8\} \subseteq \mathbb{T}^8$

l) Now implement the second method for treating the problem mentioned above. More precisely, show that the results of f) and h) remain true if we replace $(\bar{t}_1, \ldots, \bar{t}_r)$ by $(y_0t_1, \ldots, y_0t_r)$.

In the last part of this tutorial we connect the growth of the size of the powers of a polynomial to the problem of counting integral points inside polytopes. Since the latter problem extends well beyond the scope of this tutorial, we must content ourselves with seeing just a few aspects.

Let us start again with a non-empty, finite subset S of $\mathbb{N}^n$. We want to count the number of integral points in $\text{conv}(iS)$ for $i \geq 1$, i.e. we want to determine the function $\text{EF}_S : \mathbb{N} \longrightarrow \mathbb{N}$ given by $\text{EF}_S(i) = \#(\text{conv}(iS) \cap \mathbb{N}^n)$. This function is called the **Ehrhart function** of S.

m) Imitate the construction preceding f) to define a suitable subset $\overline{S}$ of $\mathbb{T}^{n+1}$ which has the property that $\text{EF}_S(i) = \text{EF}_{\overline{S}}(i)$ for all $i \in \mathbb{N}$.

n) Let $I_{\overline{S}} \subseteq \overline{P}$ be the ideal generated by $\{x_0^{\alpha_0} \cdots x_n^{\alpha_n} \mid (\alpha_0, \ldots, \alpha_n) \in \overline{S}\}$. For every $i \geq 1$, prove that $\text{EF}_S(i)$ is the minimal number of generators of $I_{\overline{S}}$.

o) Let $r = \#S$, and let $J_{\overline{S}} \subseteq Q$ be the toric ideal associated to $\overline{S}$. Prove that $J_{\overline{S}}$ is a homogeneous ideal and $\text{EF}_S(i) = \text{HF}_{Q/J_{\overline{S}}}(i)$ for all $i \in \mathbb{N}$.

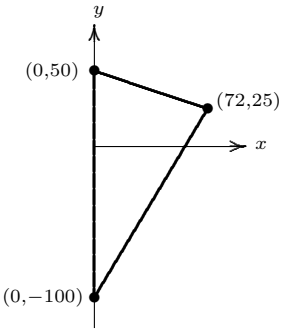
p) Conclude that there exists an integer valued polynomial $\text{EP}_S \in \mathbb{Q}[t]$ such that $\text{EF}_S(i) = \text{EP}_S(i)$ for all sufficiently large i. This polynomial is called the **Ehrhart polynomial** of S.

q) Write a CoCoA function `EhrhartPoly(...)` which computes the Ehrhart polynomial of a non-empty finite subset of $\mathbb{N}^n$.

r) Apply your function `EhrhartPoly(...)` to the following sets.

1) $S_1' = \{(0,0),\ (6,0),\ (5,3)\} \subseteq \mathbb{N}^2$
2) $S_2' = \{(3,3,0),\ (3,0,3),\ (0,3,3),\ (3,6,3),\ (6,3,3),\ (3,3,6)\} \subseteq \mathbb{N}^3$
3) $S_3' = \{(1,0,0,0,0),\ (0,1,0,0,0), (0,0,1,0,0),\ (0,0,0,1,0),$
$(0,0,0,0,1),\ (1,1,1,1,1)\} \subseteq \mathbb{N}^5$

s) How many integral points lie in or on the triangle with vertices $(0,-100)$, $(0,50)$, and $(75,25)$?



5.3 Computation of Hilbert Series

I think there is a world market
for maybe five computers.
(Thomas J. Watson, IBM, 1943)

Computers in the future
may weigh no more than 1.5 tons.
(Popular Mechanics, 1949)

640K ought to be enough for anybody.
(William H. Gates, 1981)

Prediction is very difficult,
especially about the future.
(Niels Bohr)

Nowadays, hundreds of millions of computers have been sold, the opening screen of the Windows operating system alone occupies more than 640 kilobytes of memory, and there are powerful notebook computers weighing no more than 1.5 kilograms. Personal computers offer us tremendous power and with their help we may dare to compute very complicated Hilbert series. However, to achieve that goal we still need a good deal of hard work. Why is this problem so difficult?

First of all, we need an algorithm. More than a century ago, David Hilbert invented graded free resolutions for the purpose of computing the functions which are now called Hilbert functions in his honour. But as we have seen in Chapter IV, the computation of graded free resolutions is a tough job. Fortunately, the theory of Gröbner bases and Buchberger's algorithm have improved the situation dramatically. In the last section we saw that, to compute the Hilbert series of a graded module over the polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K, it is enough to determine its Hilbert numerator. Moreover, the proof of Theorem 5.1.21 contains the outline of an algorithm for doing this: first apply the basic properties to reduce the task to the case of a P-module of the form P/I, where I is a monomial ideal, and then use the multiplication sequence to proceed by induction on the minimal number of generators of I.

This leads to a recursive procedure called the Classical Hilbert Numerator Algorithm 5.3.2 which clearly shows where the difficulties of the problem lie. On the one hand, we need a Gröbner basis of the module under consideration; this part of the task has been discussed in Chapter IV. On the other hand, using the multiplication sequence to break the problem into smaller pieces may lead to an exponential number of branches of the computation. Since we are dealing with monomial ideals, the combinatorial complexity of the task appears here. We need to administer the full force of our cunning in order to do well in *most* cases.

As you know by now, computers are not intelligent. *They only think they are.* Therefore we need to invent good *strategies* in order to convince them

to work efficiently on the challenge posed by the computation of Hilbert numerators. More specifically, given a minimal monomial system of generators $\{t_1, \ldots, t_s\}$ of I, we need to choose a good *pivot*, i.e. a term $p \in \mathbb{T}_d^n$ such that the multiplication sequence

$$0 \to [P/((t_1, \ldots, t_s) :_P (p))](-d) \to P/(t_1, \ldots, t_s) \to P/(p, t_1, \ldots, t_s) \to 0$$

breaks the computation into two well-balanced parts. In this way, we hope to get swiftly down to the *base cases*, i.e. monomial ideals whose Hilbert numerator we know offhand. Are there good strategies for choosing such a pivot? And what does it mean for a strategy to be good?

To answer these questions, we have to leave the firm ground of propositions and theorems. For every strategy, one can invent examples where it performs exceptionally well or particularly badly. What really makes a strategy good or bad is therefore its behaviour with respect to a large number of interesting examples. Viewed from a higher point of view, what a strategy does is to try to predict the future course of the computation. And as we have seen, predictions are notoriously difficult, especially if they concern the future. In this sense we discuss a number of strategies with fancy names such as the indeterminate strategy (which is far from being indeterminate, of course), the GCD strategy, and the CoCoA strategy. The last one is the strategy implemented in CoCoA (where else?), and naturally, it is the one we think is generally the best. Furthermore, these algorithms and strategies lend themselves to a straightforward generalization: in Section 5.8 we shall see how to compute Hilbert series in a $\mathbb{Z}^m$-graded setting.

Obviously, the structure of this section differs from the other ones. Technical terms such as recursive procedure, pivot element, strategies, and base cases abound and the most instructive features are a couple of *running examples* which tie together the whole discussion and come in more installments than a short-lived TV series. Do you see the difference? Like a diamond, a good theorem is forever, but a good algorithm is confronted with an extra looming parameter, a finite life-span. The end of the development is that, using the best available strategies, one can achieve results which are so good that nowadays the computation of Hilbert series can be used as a tool for speeding up the computation of graded free resolutions (see Tutorial 69). In this way, history has come full circle and Hilbert's project is carried out in reverse order!

In this section we let K be a field, $P = K[x_1, \ldots, x_n]$ a standard graded polynomial ring, and M a non-zero finitely generated graded P-module. We assume that we are given a homogeneous presentation $M \cong F/N$, where F is a finitely generated graded free P-module and N is a graded submodule of F. We write $F = \bigoplus_{i=1}^r P(-\delta_i)$ with $\delta_1, \ldots, \delta_r \in \mathbb{Z}$.

Clearly, if $e_i \in N$ for some $i \in \{1, \ldots, r\}$, we can replace the presentation $M = F/N$ by a simpler presentation $M \cong F'/N'$, where F' is a graded free P-module of rank $r-1$ and N' is a graded submodule of F'. Therefore we

shall from now on assume that the presentation of M is chosen in such a way that $e_i \notin N$ for $i = 1, \ldots, r$. Hence the homogeneous system of generators $\{e_1 + N, \ldots, e_r + N\}$ of M consists of non-zero elements.

In Theorem 5.2.20 we saw that the Hilbert series of M is of the form $\mathrm{HS}_M(z) = z^\alpha \, \mathrm{HN}_M(z)/(1-z)^n$, where $\alpha = \min\{i \in \mathbb{Z} \mid M_i \neq 0\}$ is the initial degree of M and $\mathrm{HN}_M(z) \in \mathbb{Z}[z]$. Because of our assumption, we have $\alpha = \min\{\delta_1, \ldots, \delta_r\}$. Our goal of computing the Hilbert series of M immediately reduces to the task of finding the polynomial $\mathrm{HN}_M(z) \in \mathbb{Z}[z]$. The next step is to reduce the problem to the computation of the polynomial $\mathrm{HN}_{P/I}(z)$ for a monomial ideal I. The following proposition does that job.

Proposition 5.3.1. *Let $M \cong F/N$ be a finitely generated graded P-module, where N is given by an explicit set of generators and $e_i \notin N$ for $i = 1, \ldots, r$. Assume that there exists a procedure* `MonHN`(I) *which computes the Hilbert numerator $\mathrm{HN}_{P/I}(z)$ for a monomial ideal I in P. Consider the following instructions.*

1) *Let $\alpha = \min\{\delta_1, \ldots, \delta_r\}$. After choosing a module term ordering σ on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$, compute $\mathrm{LT}_\sigma(N)$ using Buchberger's Algorithm.*
2) *Let $\{t_1 e_{\gamma_1}, \ldots, t_s e_{\gamma_s}\}$ be a system of generators of $\mathrm{LT}_\sigma(N)$, where $t_1, \ldots, t_s \in \mathbb{T}^n$ and $\gamma_1, \ldots, \gamma_s \in \{1, \ldots, r\}$. For $i = 1, \ldots, r$, let $I_i \subseteq P$ be the monomial ideal generated by $\{t_j \mid 1 \leq j \leq s, \gamma_j = i\}$ and compute $\mathrm{HN}_{P/I_i}(z)$ by performing* `MonHN`(I_i).
3) *Return the polynomial $\sum_{i=1}^r z^{\delta_i - \alpha} \, \mathrm{HN}_{P/I_i}(z)$ and stop.*

This is an algorithm which computes the Hilbert numerator $\mathrm{HN}_M(z)$.

Proof. Since the procedure is clearly finite, it remains to prove correctness. Using Properties 5.2.15.b,d and Proposition 5.2.18, we calculate $\mathrm{HS}_M(z) = \sum_{i=1}^r z^{\delta_i} \, \mathrm{HS}_P(z) - \mathrm{HS}_{\mathrm{LT}_\sigma(N)}(z)$. By the Structure Theorem for Monomial Modules 1.3.9, we have $\mathrm{LT}_\sigma(N) = \bigoplus_{i=1}^r I_i e_i$, and therefore $\mathrm{HS}_N(z) = \sum_{i=1}^r z^{\delta_i} \, \mathrm{HS}_{I_i}(z)$. Hence we get $\mathrm{HS}_M(z) = \sum_{i=1}^r z^{\delta_i} \, (\mathrm{HS}_P(z) - \mathrm{HS}_{I_i}(z)) = \sum_{i=1}^r z^{\delta_i} \, \mathrm{HS}_{P/I_i}(z)$. By assumption we have $e_i \notin N$ for $i = 1, \ldots, r$. Thus we have $P/I_i \neq 0$ and $\min\{j \in \mathbb{Z} \mid (P/I_i)_j \neq 0\} = 0$. Now Theorem 5.2.20 yields $\mathrm{HS}_{P/I_i}(z) = \mathrm{HN}_{P/I_i}(z)/(1-z)^n$. Altogether, we get

$$\mathrm{HS}_M(z) = \tfrac{z^\alpha}{(1-z)^n} \cdot \sum_{i=1}^r z^{\delta_i - \alpha} \, \mathrm{HN}_{P/I_i}(z)$$

Since the algorithm returns the sum appearing on the right-hand side, the claim follows from Theorem 5.2.20. □

To develop an algorithm for computing the Hilbert numerator of P/I for a monomial ideal I we shall use a **recursive procedure**, i.e. a procedure which may call itself during its execution. Of course, we have to make sure that this does not lead to an infinite loop.

Recall from Proposition 1.3.11 that, given a monomial ideal I in P, there exists a unique minimal monomial system of generators of I. So, given any

set of terms which generates I, this minimal monomial system of generators is a subset of the given set and can be computed easily (see the proof of Proposition 1.3.11 and Tutorial 8).

Now we are ready to describe the classical algorithm for computing Hilbert numerators.

Theorem 5.3.2. (The Classical Hilbert Numerator Algorithm) *Let I be a non-zero proper monomial ideal in P. Consider the procedure* `MonHN`(I) *defined by the following instructions.*

1) *Let $\{t_1, \ldots, t_s\}$ be the minimal monomial system of generators of I. If $s = 1$, let $d = \deg(t_1)$, return the result $1 - z^d$, and stop. Otherwise, let $p \in \{t_1, \ldots, t_s\}$, and let J be the ideal generated by $\{t_1, \ldots, t_s\} \setminus \{p\}$.*
2) *Call the procedures* `MonHN`(J) *and* `MonHN`$(J:_P(p))$, *and let $f_1(z)$ and $f_2(z)$ be the polynomials which they return.*
3) *Let $d = \deg(p)$. Return the polynomial $f_1(z) - z^d f_2(z)$ and stop.*

This is an algorithm which computes the Hilbert numerator $\mathrm{HN}_{P/I}(z)$.

Proof. First we prove finiteness. In step 2), the procedure `MonHN`$(\ldots)$ calls itself twice. We show that in both instances the minimal number of generators of the ideal passed as argument is smaller than s. This fact is clear for J, and $J :_P (p)$ is the ideal generated by the terms $\mathrm{lcm}(t_i, p)/p$ with $t_i \neq p$. Hence we eventually reach $s = 1$, and the procedure stops in step 1).

To show correctness, we note that when the procedure reaches $s = 1$, we have $I = (t_1)$ and the claim follows from Corollary 5.2.17. Now we use induction on the minimal number of generators and assume that $f_1(z) = \mathrm{HN}_{P/J}(z)$ and $f_2(z) = \mathrm{HN}_{P/(J:_P(p))}(z)$. From Proposition 5.2.16, we get that $\mathrm{HS}_{P/I}(z) = \mathrm{HS}_{P/J}(z) - z^d\ \mathrm{HS}_{P/(J:_P(p))}(z)$. Thus the claim follows from the observation that a P-module of the form P/I with a homogeneous proper ideal I has its first non-zero homogeneous component in degree zero, and from Theorem 5.2.20. □

Notice that the algorithm of this theorem shows that the polynomial it returns always has constant coefficient $\mathrm{HN}_{P/I}(0) = 1$. Moreover, we remark that several choices of p are available, and different choices may lead to different levels of efficiency. Let us have a look at an example.

Example 5.3.3. Let I be the monomial ideal in $K[x_1, x_2, x_3]$ minimally generated by $\{x_1^3x_2,\ x_2^2x_3,\ x_3^4,\ x_2x_3^2\}$. If we choose $p = x_2x_3^2$, we obtain $J = (x_1^3x_2,\ x_2^2x_3,\ x_3^4)$ and $J :_P (p) = (x_1^3,\ x_2,\ x_3^2)$. These ideals have three minimal generators each.

However, if we choose $p = x_3^4$ instead, we get $J = (x_1^3x_2,\ x_2^2x_3,\ x_2x_3^2)$ and $J :_P (p) = (x_1^3x_2,\ x_2^2,\ x_2) = (x_2)$. In this case the second ideal has only one minimal generator, and this branch of the computation stops at the next step. Thus this choice of p is better.

In view of this example the question arises which minimal generator of I we should choose in step 1). The following method works well in practise.

Remark 5.3.4. (The Good Generator Strategy)
Let I be a non-zero proper monomial ideal in P, and let $\{t_1, \ldots, t_s\}$ be its minimal monomial system of generators. Let $i \in \{1, \ldots, n\}$ be such that x_i divides one of the terms $t_1, \ldots, t_s$. Let p be one of the terms in which x_i appears with the highest exponent. Then apply step 1) of the Classical Hilbert Numerator Algorithm.

In this way, not only does the ideal $J :_P (p)$ have at most $s-1$ generators, but also its generators do not involve the indeterminate x_i anymore. Hence one of the branches of the algorithm stops after at most $n-1$ recursions.

A number of further algorithms for computing Hilbert numerators of monomial ideals are based on the idea that we can use the formula

$$\mathrm{HS}_{P/(I+(p))}(z) = \mathrm{HS}_{P/I}(z) - z^d \, \mathrm{HS}_{P/(I:_P(p))}(z)$$

where p is a term and $d = \deg(p)$, in another way, namely by expressing $\mathrm{HN}_{P/I}(z)$ in terms of $\mathrm{HN}_{P/(I+(p))}(z)$ and $\mathrm{HS}_{P/(I:_P(p))}(z)$. In the following we refer to p as the **pivot**. Again we have to make sure that this does not lead to an infinite loop. We need to show that the recursive calls are applied to sets generating *simpler* ideals. The following notion will help us achieve this.

Definition 5.3.5. Let I be a monomial ideal and $\{t_1, \ldots, t_s\}$ its minimal monomial set of generators. Then we define $\Sigma\deg(I) = \deg(t_1) + \cdots + \deg(t_s)$ and call it the **total degree** of I.

The recursion stops when we reach ideals I so simple the we know the Hilbert numerator of P/I without further computation. These very simple ideals are called the **base cases**. For instance, the base cases in the Classical Hilbert Numerator Algorithm are the principal monomial ideals. For our more general procedures a richer collection of base cases is provided by the following proposition.

Proposition 5.3.6. *Let I be a non-zero proper monomial ideal in P whose minimal monomial generators $\{t_1, \ldots, t_s\}$ are pairwise coprime. Then the Hilbert numerator of P/I is given by* $\mathrm{HN}_{P/I}(z) = \prod_{i=1}^{s}(1 - z^{\deg(t_i)})$.

Proof. Using induction on s, we show that $(t_1, \ldots, t_s)$ is a regular sequence for P; then the claim follows from Corollary 5.2.17. Clearly, t_1 is not a zerodivisor in P. Now let $s > 1$, and suppose $f \in P$ is a polynomial for which $f\,t_s \in (t_1, \ldots, t_{s-1})$. It follows that, for every $\tilde{t} \in \mathrm{Supp}(f)$, there exists an index $i \in \{1, \ldots, s-1\}$ such that t_i divides $\tilde{t}\,t_s$. Then $\gcd(t_i, t_s) = 1$ implies $\tilde{t} \in (t_i)$. Altogether, we find $f \in (t_1, \ldots, t_{s-1})$, as desired. □

A monomial ideal which satisfies the hypothesis of this proposition will be called a **monomial complete intersection**. Notice that it cannot have more than n minimal monomial generators. At this point we can formulate a prototype algorithm for computing Hilbert numerators of monomials ideals using different strategies.

Theorem 5.3.7. (Computing Hilbert Numerators Using Strategies) *Suppose there exists a procedure* $\texttt{Pivot}(I)$ *which applies to monomial ideals* I *in* P *that are not monomial complete intersections, and which returns a term* p *such that* $\Sigma\deg(I:_P(p)) < \Sigma\deg(I)$ *and* $\Sigma\deg(I+(p)) < \Sigma\deg(I)$. *Let* I *be a non-zero proper monomial ideal in* P. *Consider the procedure* $\texttt{MonHN}(I)$ *defined by the following instructions.*

1) *Check whether* I *is a monomial complete intersection. If it is, let* $d_1, \ldots, d_s$ *be the degrees of the minimal monomial generators of* I. *Return the result* $\prod_{i=1}^{s}(1 - z^{d_i})$ *and stop. Otherwise, let* p *be the term computed by* $\texttt{Pivot}(I)$.
2) *Call the procedures* $\texttt{MonHN}(I:_P(p))$ *and* $\texttt{MonHN}(I+(p))$, *and let* $f_1(z)$ *and* $f_2(z)$ *be the polynomials which they return.*
3) *Let* $d = \deg(p)$. *Return the polynomial* $z^d f_1(z) + f_2(z)$ *and stop.*

This is an algorithm which computes the Hilbert numerator $\mathrm{HN}_{P/I}(z)$.

Proof. First we prove finiteness. In step 2), the procedure $\texttt{MonHN}(\ldots)$ calls itself twice. In both instances the monomial ideals to which it applies have a smaller total degree. Since the total degree is always non-negative, we eventually arrive at a monomial complete intersection or at total degree zero. We claim that total degree zero never happens. If $\Sigma\deg(I) = 0$, we have either $I = (0)$ or $I = (1)$. Since $I \neq (0)$, it is clear that both $I :_P (p) \neq (0)$ and $I + (p) \neq (0)$. Thus $I = (0)$ never happens. It remains to show that $I = (1)$ never happens.

Initially, this follows from $I \neq P$. Later, the procedure $\texttt{Pivot}(I)$ never chooses $p = 1$, since then the equality $I :_P (p) = I$ contradicts the inequality $\Sigma\deg(I :_P (p)) < \Sigma\deg(I)$. Thus we never get $I + (p) = (1)$. Nor do we ever get $I :_P (p) = (1)$, since in that case $p \in I$ yields $I + (p) = I$, in contradiction with $\Sigma\deg(I + (p)) < \Sigma\deg(I)$. Altogether, we never reach $\Sigma\deg(I) = 0$. Hence the procedure stops in step 1) in every branch of the recursion.

Now we show correctness. When the procedure reaches a monomial complete intersection, the claim follows from Proposition 5.3.6. Next we use induction on the depth of the recursion. Hence we may assume that $f_1(z) = \mathrm{HN}_{P/(I:_P(p))}(z)$ and $f_2(z) = \mathrm{HN}_{P/(I+(p))}(z)$. Proposition 5.2.16 implies

$$\mathrm{HS}_{P/I}(z) = z^d \, \mathrm{HS}_{P/(I:_P(p))}(z) + \mathrm{HS}_{P/(I+(p))}(z)$$

By using Theorem 5.2.20 and multiplying everything by $z^{-\alpha}(1 - z)^n$, we get $\mathrm{HN}_{P/I}(z) = z^d f_1(z) + f_2(z)$. Therefore the algorithm returns the correct result. □

Naturally, we still need to show that a procedure `Pivot`(I) with the desired properties really exists. In fact, we shall now introduce a number of different strategies used in modern computer algebra systems and compare their efficiency by way of two *running examples*.

Remark 5.3.8. (The Indeterminate Strategy)
Far from being indeterminate, this strategy is very concise and simple. The procedure `Pivot`(I) determines $i \in \{1, \ldots, n\}$ such that x_i is a proper divisor of one of the minimal monomial generators of I and returns $p = x_i$.

Let us see why this choice has the desired properties. First of all, an index $i \in \{1, \ldots, n\}$ always exists, because ideals generated by indeterminates are monomial complete intersections and we assumed I not to be one. Now let t_j be a minimal monomial generator of I which is a proper multiple of x_i. Since the exponent of x_i in the corresponding generator $\mathrm{lcm}(x_i, t_j)/x_i = t_j/x_i$ of $I{:}_P(x_i)$ is decreased by one, we have $\Sigma\deg(I{:}_P(x_i)) < \Sigma\deg(I)$. On the other hand, we have $I + (x_i) = J + (x_i)$, where $J = (t_k \mid x_i \nmid t_k)$. Hence the ideal $I + (x_i)$ has total degree $1 + \sum_{x_i \nmid t_k} \deg(t_k) < \Sigma\deg(I)$.

In general, the ideal $I{:}_P(x_i)$ will have about the same minimal number of generators as I. A decrease happens for instance in situations such as $(x_1^2x_2, x_1x_3) :_P (x_3) = (x_1)$. But the ideal $I + (x_i)$ will usually have significantly fewer minimal generators than I, because all minimal generators divisible by x_i are replaced by the single minimal generator x_i. This tends to lead to a somewhat unbalanced situation where the two branches of the computation have substantially different computational costs. Therefore the indeterminate strategy is easy to implement, but not always very efficient. An optimization is contained in Exercise 7.

Now let us immediately start our two running examples.

Example 5.3.9. (Running One)
Let $P = K[x_1, \ldots, x_4]$ and $I = (x_3^3,\ x_2^3x_3x_4^2,\ x_1^2x_2^4x_4^2,\ x_1x_2x_3^2)$. We want to compute the Hilbert numerator of P/I using the indeterminate strategy. In the first step, we choose the indeterminate x_1 as a pivot and obtain $I_1 = I :_P (x_1) = (x_3^3,\ x_2^3x_3x_4^2,\ x_1x_2^4x_4^2,\ x_2x_3^2)$ as well as $I_2 = I + (x_1) = (x_3^3,\ x_2^3x_3x_4^2,\ x_1)$. These ideals have four and three minimal monomial generators, respectively, and further recursive function calls are required.

For I_1, we choose x_2 and find $I_{11} = I_1 :_P (x_2) = (x_3^2,\ x_2^2x_3x_4^2,\ x_1x_2^3x_4^2)$ as well as $I_{12} = I_1 + (x_2) = (x_3^3,\ x_2)$. To treat I_{11}, we choose the pivot x_3 and get $I_{111} = I_{11} :_P (x_3) = (x_3, x_2^2x_4^2)$ as well as $I_{112} = I_{11} + (x_3) = (x_3,\ x_1x_2^3x_4^2)$. Both of these are base cases, so that we get $\mathrm{HN}_{P/I_{111}}(t) = (1-z)(1-z^4)$ and $\mathrm{HN}_{P/I_{112}}(z) = (1-z)(1-z^6)$, and therefore

$$\mathrm{HN}_{P/I_{11}}(z) = z\ \mathrm{HN}_{P/I_{111}}(z) + \mathrm{HN}_{P/I_{112}}(z) = (1-z)(1+z-z^5-z^6)$$

Since I_{12} is a base case, we then compute $\mathrm{HN}_{P/I_{12}}(z) = (1-z)(1-z^3)$ and

$$\mathrm{HN}_{P/I_1}(z) = z\ \mathrm{HN}_{P/I_{11}}(z) + \mathrm{HN}_{P/I_{12}}(z) = (1-z)(1+z+z^2-z^3-z^6-z^7)$$

For I_2, we choose the pivot x_3 and immediately get the base cases $I_{21} = I_2 :_P (x_3) = (x_3^2, x_2^3x_4^2, x_1)$ as well as $I_{22} = I_2 + (x_3) = (x_1, x_3)$. This yields $\mathrm{HN}_{P/I_{21}}(z) = (1-z)(1-z^2)(1-z^5)$ and $\mathrm{HN}_{P/I_{22}}(z) = (1-z)^2$, and therefore $\mathrm{HN}_{P/I_2}(z) = (1-z)(1-z^3-z^6+z^8)$. Altogether, the algorithm returns the result

$$\mathrm{HN}_{P/I}(z) = 1 - z^3 - z^4 + z^5 - z^6 + z^8$$

Our initial choice of the pivot was not the only possible one. By analyzing the support of the minimal monomial generators of I, we may be able to come up with a better choice (see also Exercise 7). In the case at hand, we can take x_3 as a pivot and get $J_1 = I :_P (x_3) = (x_3^2, x_2^3x_4^2, x_1x_2x_3)$ as well as $J_2 = I + (x_3) = (x_3, x_1^2x_2^4x_4^2)$. Here J_2 is already a base case, and J_1 is simpler than I_1.

Example 5.3.10. (Running Two)
Let $P = K[x_1, \ldots, x_4]$ and $I = (x_1x_3^3, x_1^2x_2^2x_3, x_1x_2^3x_3, x_1^3x_2x_3x_4)$. Here the pivot x_1 yields the ideals $I_1 = I :_P (x_1) = (x_3^3, x_1x_2^2x_3, x_2^3x_3, x_1^2x_2x_3x_4)$ and $I_2 = I + (x_1) = (x_1)$. Clearly, this is a *very* unbalanced result and the treatment of I_1 will require much more work than the treatment of I_2 which is a trivial base case. Notwithstanding this observation, we shall later see that, in this very example, the indeterminate strategy is not performing badly at all. So, to really see the difference between various strategies, one usually has to look at much larger examples than we do here.

Our next strategy tries to overcome the deficiencies of the indeterminate strategy by choosing the pivot to maximize the likelihood that the computation is cut into two branches of approximately the same size.

Remark 5.3.11. (The GCD Strategy)
Consider the following strategy which contains some "random" choice: Given a monomial ideal I which is not a complete intersection, having a minimal monomial system of generators $\{t_1, \ldots, t_s\}$, choose an indeterminate x_i such that $\#\{j \mid x_i \text{ divides } t_j\}$ is maximal. Then choose randomly two different terms t_j, t_k which are divisible by x_i, and return $p = \gcd(t_j, t_k)$.

Let us again prove that this strategy has the desired properties. First of all, it always returns a result, because there must be some indeterminate which is contained in at least two of the terms $t_1, \ldots, t_s$, otherwise we would be in a base case. Secondly, since the term p is divisible by x_i, the minimal monomial generators of the ideal $I :_P (p)$ corresponding to the terms t_j which are divisible by x_i have their x_i-exponents reduced by one. Thus the ideal $I :_P (p)$ has smaller total degree than I. Finally, in the ideal $I + (p)$ the two generators t_j, t_k are replaced by p, and thus it, too, has smaller total degree.

Experience shows that the GCD strategy performs well on many types of input ideals. If $\#\{j \mid x_i \text{ divides } t_j\} \geq 3$, it turns out to be even better

to use as pivot the greatest common divisor of three randomly chosen terms t_i, t_j, t_k which are divisible by x_i. Let us apply the GCD strategy to our example "Running One".

Example 5.3.12. (Running Further)
In Example 5.3.9, the indeterminates x_2 and x_3 each appear in three generators. We randomly choose the first and second generators containing x_2 and compute $p = \gcd(x_2^3x_3x_4^2,\ x_1^2x_2^4x_4^2) = x_2^3x_4^2$. Using this term as pivot, we calculate $I_1 = I :_P (p) = (x_3,\ x_1^2x_2)$ and $I_2 = I + (p) = (x_3^3,\ x_2^3x_4^2,\ x_1x_2x_3^2)$. Here I_1 is a base case and yields $\mathrm{HN}_{P/I_1}(z) = (1-z)(1-z^3)$. When we apply the GCD strategy to I_2, we choose $p = x_2$ and get $I_{21} = I_2 :_P (x_2) = (x_3^3,\ x_2^2x_4^2,\ x_1x_3^2)$ as well as $I_{22} = I_2 + (x_2) = (x_3^3, x_2)$. Again I_{22} is a base case and yields $\mathrm{HN}_{P/I_{22}}(z) = (1-z)(1-z^3)$. In order to deal with I_{21}, our strategy chooses $p = x_3^2$ and computes $I_{211} = I_3 :_P (x_3^2) = (x_1, x_3, x_2^2x_4^2)$ as well as $I_{212} = I_3 + (x_3^2) = (x_3^2,\ x_2^2x_4^2)$. Since these are base cases, we get $\mathrm{HN}_{P/I_{211}}(z) = (1-z)^2(1-z^4)$ and $\mathrm{HN}_{P/I_{212}}(z) = (1-z^2)(1-z^4)$, and therefore $\mathrm{HN}_{P/I_{21}}(z) = (1-z)(1-z^4)(1+z+z^2-z^3)$. Putting everything together, we find $\mathrm{HN}_{P/I_2}(z) = (1-z)(1+z+z^2-z^4-z^5-z^6-z^7+z^8)$ and

$$\mathrm{HN}_{P/I}(z) = 1 - z^3 - z^4 + z^5 - z^6 + z^8$$

Even a brief glance at this computation convinces us that it is easier than "Running One". At several junctures there were other possible choices of pivot, depending on random choices in our strategy but, in this example, all of them yield similar computational trees.

Next we hit Example 5.3.10 with the GCD strategy and let the algorithm run its course.

Example 5.3.13. (Hit and Run)
In the ideal $I = (x_1x_3^3,\ x_1^2x_2^2x_3,\ x_1x_2^3x_3,\ x_1^3x_2x_3x_4)$ of Example 5.3.10, the indeterminates x_1 and x_3 occur in all generators. If we randomly take the first two, we obtain the pivot $p = \gcd(x_1x_3^3,\ x_1^2x_2^2x_3) = x_1x_3$. This pivot leads us to consider $I_1 = I :_P (x_1x_3) = (x_3^2,\ x_1x_2^2,\ x_2^3,\ x_1^2x_2x_4)$ and $I_2 = I + (x_1x_3) = (x_1x_3)$ next. Since I_2 is a base case, we apply the GCD strategy to I_1. The indeterminate occurring most often is x_2, and the greatest common divisor of the (randomly chosen) first two generators containing it is $p = x_2^2$.

Therefore the algorithm has to compute $I_{11} = I_1 :_P (x_2^2) = (x_3^2,\ x_1, x_2)$ and $I_{12} = I_1 + (x_2^2) = (x_3^2,\ x_2^2,\ x_1^2x_2x_4)$, where I_{11} is a base case and I_{12} easily reduces to base cases by choosing $p = x_2$. Again the choice of hitting the ideal with the pivot given by the greatest common divisor of two generators has reduced it quickly to some very simple cases.

From these examples, it would appear that the GCD strategy is the best one available. But we have not yet taken into account one operation which

incurs substantial computational cost: after each colon operation, the resulting list of terms has to be minimalized. In the worst case, this means that we have to perform $\binom{s}{2}$ divisibility tests on a list of s terms. Our final strategy is similar to the GCD strategy in that it chooses terms of higher degree dividing at least two minimal generators. But it restricts this choice to pure powers of indeterminates, because for such pivots p the computation of the minimal monomial generators of $I :_P (p)$ can be improved substantially (see Exercise 4). This is the strategy implemented in CoCoA, and it performs really well in practice.

Remark 5.3.14. (The CoCoA Strategy)
As a compromise between the two previous strategies, we introduce the following one. Given a monomial ideal I which is not a complete intersection, let x_i be one of the indeterminates occurring most often in the minimal monomial generators $\{t_1, \ldots, t_s\}$ of I. Then choose randomly two minimal generators t_j, t_k divisible by x_i, and let p be the highest power of x_i dividing both t_j and t_k. Return p and stop.

It follows as in Remark 5.3.11 that this strategy has the properties prescribed by Theorem 5.3.7. Although it sometimes produces slightly more complicated ideals than the GCD strategy while the algorithm is running, it can be implemented very efficiently, so that its higher speed more than makes up for the extra distance it has to go.

Of course, we jump at once into action and run this strategy on our first running Example 5.3.9.

Example 5.3.15. (Jump and Run)
When we apply the CoCoA strategy to Example 5.3.9, we can choose p to be the highest power of x_2 contained in $x_2^3x_3x_4^2$ and $x_1^2x_2^4x_4^2$, i.e. we choose $p = x_2^3$. We obtain the ideals $I_1 = I :_P (x_2^3) = (x_3^3, x_3x_4^2, x_1^2x_2x_4^2, x_1x_3^2)$ and $I_2 = I + (x_2^3) = (x_3^3, x_2^3, x_1x_2x_3^2)$. To treat I_1 further, we choose the indeterminate x_3 and then the first two generators to get the pivot x_3. This yields $I_{11} = I_1 :_P (x_3) = (x_3^2, x_4^2, x_1x_3)$ and $I_{12} = I_1 + (x_3) = (x_3, x_1^2x_2x_4^2)$, where I_{11} can easily be split using $p = x_3$ and I_{12} is a base case.

To treat I_2 further, we choose the indeterminate x_2 and the last two generators to get the pivot x_2. This yields $I_{21} = I_2 :_P (x_2) = (x_3^3, x_2^2, x_1x_3^2)$ and $I_{22} = (x_3^3, x_2)$, where I_{21} can easily be split using $p = x_3^2$ and I_{22} is a base case. By recombining the Hilbert numerators, we get the result. Notice that the computation in the two main branches has exactly the same length. Thus our strategy splits the problem in a very balanced way into two parts.

To end this discussion, we have a look at a really fast example.

Example 5.3.16. (Road Runner)
Let us apply the CoCoA strategy to Example 5.3.10. Since x_1x_3 divides all the generators, we choose $p = x_1$ and get $I_1 = I :_P (x_1) = (x_3^3, x_1x_2^2x_3, x_2^3x_3,$

$x_1^2x_2x_3x_4$) and $I_2 = I + (x_1) = (x_1)$. Then we deal with I_1 by choosing the pivot x_3 and get $I_{11} = I_1 :_P (x_3) = (x_3^2, x_1x_2^2, x_2^3, x_1^2x_2x_4)$ and $I_{12} = I_1 + (x_3) = (x_3)$. Finally, we treat I_{11} by choosing $p = x_2^2$ and get the base case $I_{111} = I_{11} :_P (x_2^2) = (x_3^2, x_1, x_2)$ as well as $I_{112} = I_{11} + (x_2^2) = (x_3^2, x_2^2, x_1^2x_2x_4)$ which is easily split by $p = x_2$. The computation was simple at each step. Using the method of Exercise 4, the implementation yields a fast and efficient algorithm.

All strategies can be enhanced further by enlarging the set of base cases, for instance by using the cases described in Exercise 5 and Tutorial 68.

Exercise 1. Let K be a field, let $P = K[x_1, x_2, x_3]$ be standard graded, let $F = P(-2) \oplus P(-1)^2$, and let M be the graded submodule of F generated by $\{e_1 - x_1e_2,\ x_1x_2e_2,\ x_2^3e_2,\ x_3e_2 - x_2e_3\}$. Compute the Hilbert series of F/M.

Exercise 2. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let $I = (x_1x_2, x_2x_3, \ldots, x_{n-1}x_n)$. Apply the Classical Hilbert Numerator Algorithm 5.3.2 to the ideal I. In step 1) choose the term involving the indeterminate with maximal index. Show that in this way the computation tree has a number of branches which is exponential in n.

Exercise 3. Let K be a field, let $P = K[x_1, \ldots, x_4]$, and let I be the ideal $(x_1x_3^3,\ x_1^2x_2^2x_3,\ x_1x_2^3x_3,\ x_2x_3x_4)$ in P. Consider all possible choices of pivot as the greatest common divisor of two minimal monomial generators and decide which of them is best suited to computing the Hilbert numerator of P/I efficiently.

Exercise 4. Let $T = \{t_1, \ldots, t_s\}$ be the minimal monomial set of generators of a monomial ideal in the polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K, and let $p = x_i^d$ with $i \in \{1, \ldots, n\}$ and $d \geq 1$. Let $j, k \in \{1, \ldots, s\}$, and write $t_j = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ as well as $t_k = x_1^{\beta_1} \cdots x_n^{\beta_n}$. For $1 \leq j \leq s$, we define $t_j : p = x_1^{\alpha_1} \cdots x_{i-1}^{\alpha_{i-1}} x_i^{\max\{0, \alpha_i - d\}} x_{i+1}^{\alpha_{i+1}} \cdots x_n^{\alpha_n}$. For a set of terms L, the list $L : p$ is defined elementwise.

a) Let $j, k \in \{1, \ldots, s\}$ be such that $j \neq k$. Show that $t_j : p$ does not divide $t_k : p$ if $\alpha_i \leq \beta_i$, or if $\min\{\alpha_i, \beta_i\} > d$, or if $\alpha_i > d \geq \beta_i$.
b) For every $\ell \in \{0, \ldots, d\}$, let $L_\ell = \{t_j \in T \mid \alpha_i = \ell\}$, and then let $L_{d+1} = \{t_j \in T \mid \alpha_i > d\}$. Show that the sets $L_\ell : p$ are interreduced, i.e. they contain the minimal monomial generators of the ideals they generate.
c) Prove that a term in $L_\ell : p$ may divide a term in $L_m : p$ only if $\ell < m \leq d$.
d) Explain how one can use these results to drastically reduce the number of divisibility tests needed in order to compute the minimal monomial system of generators of $(t_1, \ldots, t_s) :_P (p)$.

Exercise 5. Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let I be a monomial ideal in P which has a minimal monomial system of generators of the form $\{x_1^{\alpha_1}x_2^{\alpha_2} \cdots x_n^{\alpha_n},\ x_{i_1}^{\beta_1},\ x_{i_2}^{\beta_2}, \ldots,\ x_{i_s}^{\beta_s}\}$, where $\beta_j > 0$ for all $j = 1, \ldots, s$.

a) Show that $\beta_j > \alpha_{i_j}$ for $j = 1, \ldots, s$.
b) Prove that the Hilbert numerator of P/I is given by the formula $\mathrm{HN}_{P/I}(t) = \prod_{j=1}^{s}(1 - t^{\beta_j}) - t^{\alpha_1+\cdots+\alpha_n} \cdot \prod_{j=1}^{s}(1 - t^{\beta_j - \alpha_{i_j}})$

Exercise 6. Let I be a non-zero homogeneous proper ideal in the polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K. Prove that the following conditions are equivalent.

a) The ideal I is zero-dimensional.
b) The Hilbert series $\mathrm{HS}_{P/I}(z)$ is a polynomial.

Exercise 7. Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let I be a non-zero monomial ideal in P.

a) Let $i \in \{1, \ldots, n\}$. Show that there exists a unique decomposition $I = x_i^{\alpha_1} I_1 + \cdots + x_i^{\alpha_m} I_m$ such that
   1) $0 \leq \alpha_1 < \cdots < \alpha_m$
   2) $I_1, \ldots, I_m$ are monomial ideals generated by terms which are not divisible by x_i.
   3) For every $j \in \{1, \ldots, m\}$, let T_j be the minimal monomial set of generators of I_j. Then $x_i^{\alpha_1} T_1 \cup \cdots \cup x_i^{\alpha_m} T_m$ is the minimal monomial set of generators of I.
b) Consider the procedure `NewMonHN`(I) defined by the following instructions.
   1) Check whether we have $I = (1)$. In this case, return 0 and stop.
   2) Choose $i \in \{1, \ldots, n\}$ such that x_i divides one of the minimal monomial generators of I. Write $I = x_i^{\alpha_1} I_1 + \cdots + x_i^{\alpha_m} I_m$ as in a).
   3) For $j = 1, \ldots, m$, let $J_j = I_1 + \cdots + I_j$. Call the procedure `NewMonHN`(J_j) and let $f_j(z)$ be the polynomial it returns.
   4) Return the polynomial $1 - z^{\alpha_1} + (z^{\alpha_1} - z^{\alpha_2}) f_1(z) + \cdots + (z^{\alpha_{m-1}} - z^{\alpha_m}) f_{m-1}(z) + z^{\alpha_m} f_m(z)$ and stop.

   Show that this is an algorithm which computes the Hilbert numerator $\mathrm{HN}_{P/I}(z)$.
c) Prove that the minimal number of generators of I satisfies the equality $\mu(I) = \mu(I_1) + \cdots + \mu(I_m)$.
d) Show that $\mu(I_j) \leq \mu(J_j)$ for $j = 1, \ldots, m$.
e) Let $r \geq 0$ and $I = (x_1, \ldots, x_n)^r$. Show that we have $\mu(I_j) = \mu(J_j)$ for $j = 1, \ldots, m$. Find further examples of monomial ideals with this property.

Tutorial 68: Implementation of the Hilbert Series Algorithm

There are two ways of constructing a software design.
One way is to make it so simple
that there are obviously no deficiencies.
And the other way is to make it so complicated
that there are no obvious deficiencies.
(C.A.R. Hoare)

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let I be a non-zero proper monomial ideal in P. In this tutorial we want to implement the Classical Hilbert Numerator Algorithm 5.3.2 and several other strategies for computing the Hilbert numerator of P/I. Then we compare the efficiency of these algorithms in some concrete cases. One particularly "bad" example leads us to increase the number of base cases by studying tensor products of graded K-algebras and the product formula for Hilbert series.

a) Write a CoCoA function `MinMon(...)` which takes a list of terms generating I and computes the minimal monomial system of generators contained in it. (*Hint:* You may also use the function `MinMonomials(...)` of Tutorial 8 if you wrote it back then!)

b) Now implement a CoCoA function `HNClassical(...)` which takes I and computes the Hilbert numerator of P/I using the Classical Hilbert Numerator Algorithm 5.3.2. Choose the generators according to the good generator strategy described in Remark 5.3.4.

c) Apply your function `HNClassical(...)` to the following cases.
   1) $I_1 = (x_1^5,\ x_1x_2x_3,\ x_2x_3^4,\ x_2^4,\ x_1x_3^2,\ x_3^5)$ in $\mathbb{Q}[x_1, x_2, x_3]$
   2) $I_2 = (x_1^4,\ x_1^3x_2^3,\ x_1^3x_2^2x_3,\ x_1^3x_2x_3^2,\ x_2^2x_4,\ x_2x_3^5)$ in $\mathbb{Q}[x_1, \ldots, x_4]$
   3) $I_3 = (x_2^4x_4^4,\ x_1x_2^3x_3x_4^3x_5,\ x_1^2x_2^2x_3^2x_4^2x_5^2,\ x_1^3x_2x_3^3x_4x_5^3,\ x_1^4x_3^4x_5^4)$ in the ring $\mathbb{Q}[x_1, \ldots, x_5]$
   4) $I_4 = (x_1,\ x_2, \ldots, x_6)^6$ in $\mathbb{Q}[x_1, \ldots, x_6]$
   5) $I_5 = [(x_1, x_2)^5 + (x_1^4x_3,\ x_1^3x_2x_3,\ x_1^2x_2^2x_3,\ x_1^3x_3^2,\ x_1^2x_2x_3^2)]^7$ in the ring $\mathbb{Q}[x_1, x_2, x_3]$
   6) $I_6 = \mathrm{LT}_{\mathtt{Lex}}(x_1^8 - x_1^5x_2^3 - x_3^6x_4^2,\ x_1^6 - x_1^3x_2^3 - x_4^6,\ x_1^7 - x_5^7 - x_3^4x_5^3)$ in the ring $\mathbb{Q}[x_1, \ldots, x_5]$
   7) $I_7 = (x_1x_2,\ x_2x_3, \ldots, x_{n-1}x_n)$ in $\mathbb{Q}[x_1, \ldots, x_n]$, where $n = 10$.

d) Implement two CoCoA functions `HNIndet(...)` and `HNgcd(...)` which compute the Hilbert numerator of P/I using the indeterminate strategy and the GCD strategy, respectively. Apply these functions to the cases of c) and compare the timings.

e) Write a CoCoA function `OptColon(...)` which optimizes the computation of the minimal monomial system of generators of $I :_P (p)$ for the case of a simple power pivot $p = x_i^d$ by using the results of Exercise 4.

f) Implement a CoCoA function `HNCoCoA(...)` which computes the Hilbert numerator of P/I using the CoCoA strategy and the optimization provided by `OptColon(...)`. Apply this function to the cases of c) and compare the timings.

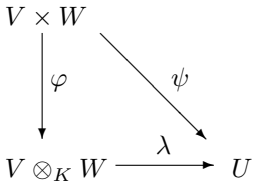
g) Try to apply your functions to computing the Hilbert numerator of P/I_7 for $n = 100$ (instead of $n = 10$). What happens? Why?

In order to remedy the problem underlying the last example, we are led to introduce tensor products of graded K-algebras and use them to increase the number of base cases. Although we hope that you have already seen the tensor product of two K-vector spaces, we shall ask you to work out a few crucial properties and to apply them to the study of graded algebras and Hilbert functions.

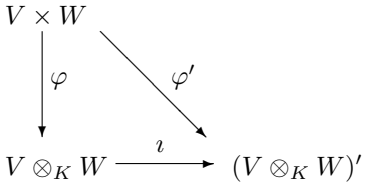
Let V and W be two finite dimensional K-vector spaces, let $\{v_1, \ldots, v_r\}$ be a K-basis of V, and let $\{w_1, \ldots, w_s\}$ be a K-basis of W. We define a new K-vector space of dimension rs which we denote by $V \otimes_K W$ as follows. The basis vectors of the new vector space are denoted by $v_i \otimes w_j$ for $i = 1, \ldots, r$ and $j = 1, \ldots, s$. Moreover, we define a map $\varphi : V \times W \longrightarrow V \otimes_K W$ by $\varphi(v, w) = \sum_{i=1}^{r} \sum_{j=1}^{s} a_i b_j \; v_i \otimes w_j$ for all $v = a_1 v_1 + \cdots + a_r v_r$ and $w = b_1 w_1 + \cdots + b_s w_s$ such that $a_1, \ldots, a_r, b_1, \ldots, b_s \in K$. The K-vector space $V \otimes_K W$ is called the **tensor product** of V and W.

h) Prove that φ is a K-bilinear map.

i) Show that the vector space $V \otimes_K W$ has the following **universal property**. Given a K-vector space U and a K-bilinear map $\psi : V \times W \longrightarrow U$, there exists a unique K-linear map $\lambda : V \otimes_K W \longrightarrow U$ such that $\psi = \lambda \circ \varphi$. In other words, there exists a commutative diagram



j) Show that this universal property determines the pair $(V \otimes_K W, \varphi)$ uniquely up to a unique isomorphism. In other words, given another pair $((V \otimes_K W)', \varphi')$ satisfying the same universal property, there is a unique isomorphism of K-vector spaces $\imath : V \otimes_K W \longrightarrow (V \otimes_K W)'$ such that the following diagram is commutative.



k) Now let I be an arbitrary homogeneous ideal of P, let $Q = K[y_1, \ldots, y_m]$ be a standard graded polynomial ring over K, let J be a homogeneous ideal of Q, and let $R = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ be standard graded. Show that the K-algebra defined by $(P/I) \otimes_K (Q/J) \cong R/(I \cdot R + J \cdot R)$

is standard graded and $[(P/I) \otimes_K (Q/J)]_i \cong \bigoplus_{j=0}^{i} (P/I)_j \otimes_K (Q/J)_{i-j}$ for all $i \geq 0$.
Hint: To prove the second claim, define two K-linear maps which are inverse to each other. One of them is obtained by applying the universal property of the tensor product repeatedly.

l) In the situation of k), conclude that the Hilbert series of $(P/I) \otimes_K (Q/J)$ is $\mathrm{HS}_{P/I}(z) \cdot \mathrm{HS}_{Q/J}(z)$.

m) Taking into account what you have just proved, modify Theorem 5.3.7 by including more base cases. Then alter your function `HNcocoa(...)` accordingly and apply it to the computation of $\mathrm{HN}_{P/I_7}(z)$ in the case $n = 100$.

Tutorial 69: Hilbert Driven Gröbner Basis Computations I

Sometimes it pays to stay in bed on Monday,
rather than spending the rest of the week
debugging Monday's code.
(Dan Salomon)

Sometimes it pays to skip reading the quote rather than to debug its grammar. Fortunately, this tutorial was not written on a Monday. Our plan is to speed up Gröbner basis computations by using a driver: the Hilbert function. Now, what exactly is this supposed to mean?

Assume that we have some *a priori* knowledge about the Hilbert function of a graded ideal or module, e.g. we are given its value in the degree in which we are computing. Then we know how big the leading term module should be in this degree. If the part of the Gröbner basis we have computed so far is not big enough, we know how many Gröbner basis elements we still have to discover, and if it is already big enough, we can skip the remaining pairs and generators in this degree because we know that they will surely reduce to zero.

This strategy clearly gives a powerful boost to most Gröbner basis computations, but you might be tempted to object that to compute the Hilbert function we first need to compute a Gröbner basis of the module, so that our plan makes no sense. However, there are situations in which we do have advance knowledge of the Hilbert series. Let us point out three typical cases. Firstly, suppose you want to compute a Gröbner basis of a module with respect to a term ordering σ which tends to be slow, for instance with respect to $\sigma =$ `Lex`. Then you start by computing a Gröbner basis with respect to a faster term ordering, for instance with respect to `DegRevLex`, use this Gröbner basis to determine the Hilbert series, and then apply the Hilbert driven strategy to compute the other Gröbner basis.

Secondly, suppose your module is part of a homogeneous exact sequence of graded modules and you know the Hilbert series of the other modules, for

instance because they are graded free modules. Then you can use Proposition 5.2.15.b to determine the Hilbert series of the module under consideration and use it to apply the Hilbert driven strategy. Thirdly, to compute an implicitization ideal you have to find a Gröbner basis of an ideal of the form $(x_1 - f_1, \ldots, x_n - f_n)$ with respect to an elimination ordering. By homogenizing the polynomials f_i, raising the indeterminates x_i to the appropriate powers d_i and using a term ordering such that the leading terms are $x_1^{d_1}, \ldots, x_n^{d_n}$, you can immediately read off the Hilbert series of this ideal, and then apply it to drive the computation of the elimination (see also Exercise 80 in Section 5.8).

At this point it is important to make the following observation: given a monomial ideal or module, the computation of its Hilbert series is usually a very fast operation in comparison to the computation of a Gröbner basis. Hence it is frequently possible to compute many Hilbert series to aid the computation of a single Gröbner basis. Enough said, let's jump out of bed and get going! Be it Monday or not, Hilbert series will be our guide at every turn, for a swift and sure journey.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let M be a finitely generated graded P-module, and let $\alpha = \alpha(M)$ be the initial degree of M.

a) Let $j \in \mathbb{Z}$, and let N be a graded submodule of M such that $N_i = M_i$ for $i < j$. Prove that the following conditions are equivalent.
   1) $N_j \subset M_j$
   2) $\dim_K(M_j) - \dim_K(N_j) > 0$
   3) There exists a positive integer c_j such that $\mathrm{HN}_M(z) - \mathrm{HN}_N(z) = c_j z^{j-\alpha} + (\textit{terms of higher degree})$.

   Show that $c_j = \dim_K(M_j) - \dim_K(N_j)$ if these conditions are satisfied.

Now let us try to use this basic observation to drive a Gröbner basis computation. Let M be a graded submodule of $F = \bigoplus_{i=1}^r P(-\delta_i)$, and let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. Assume that we are applying the Homogeneous Buchberger Algorithm 4.5.5 and we have finished the loop in steps 3)–8) for some degree d. At this point the tuple $\mathcal{G}$ is a d-truncated homogeneous σ-Gröbner basis of M. Suppose that we know the Hilbert numerator of M and that a computation of the Hilbert numerator of the module $N = \langle \mathrm{LT}_\sigma(\mathcal{G})\rangle$ yields $\mathrm{HN}_M(z) - \mathrm{HN}_N(z) = c_j z^{j-\alpha} + (\textit{terms of higher degree})$ with $c_j > 0$.

b) Prove that we have $N_i = M_i$ for $i < j$, that $j > d$, and that there are neither reduced σ-Gröbner basis elements nor minimal homogeneous generators of M in degrees $d+1, \ldots, j-1$.

c) Show that we have $c_j \leq \#B_j + \#\mathcal{W}_j$ and that the reduced σ-Gröbner basis of M contains exactly c_j elements of degree j.

d) In the Homogeneous Buchberger Algorithm 4.5.5, replace steps 2), 3) and 6) by the following instructions.

2') Let $N = \langle \mathrm{LT}_\sigma(\mathcal{G}) \rangle$. Compute the polynomial $\mathrm{HN}_M(z) - \mathrm{HN}_N(z)$. If it is zero, return $\mathcal{G}$ and stop. Otherwise, let $d \geq \alpha$ and $c_d > 0$ be such that $\mathrm{HN}_M(z) - \mathrm{HN}_N(z) = c_d z^{d-\alpha} + (\textit{terms of higher degree})$. Form the subset B_d of B, form the subtuple $\mathcal{W}_d$ of $\mathcal{W}$, and delete their entries from B and $\mathcal{W}$, respectively.

3') If $B_d = \emptyset$ or if $\mathcal{G}$ contains c_d elements of degree d, continue with step 6'). Otherwise, choose a pair $(i, j) \in B_d$ and remove it from B_d.

6') If $\mathcal{W}_d = \emptyset$ or if $\mathcal{G}$ contains c_d elements of degree d, continue with step 9). Otherwise, choose a vector $v \in \mathcal{W}_d$ and remove it from $\mathcal{W}_d$.

Show that the resulting sequence of instructions is an algorithm which computes a homogeneous σ-Gröbner basis of M. We call it the **Hilbert Driven Buchberger Algorithm**.

e) Write a CoCoA function `HDrivenBA(...)` which implements the algorithm of d). Apply this function to compute the `PosLex`-Gröbner bases of the following ideals and modules. In each case, use CoCoA first to compute the Hilbert series of M_i via its `DegRevLexPos`-Gröbner basis. Determine how many degrees and how many pairs and generators were skipped because of the Hilbert driven approach.

1) $M_1 = (x_1^2 - x_2^2,\, x_1^3 - x_3^3,\, x_1^4 - x_4^4) \subseteq \mathbb{Q}[x_1, \ldots, x_4]$
2) $M_2 = (x_1^2 x_4 - x_1 x_2^2,\, x_2^2 x_4 - x_2 x_3^2,\, x_3^2 x_1 - x_2 x_4^2) \subseteq \mathbb{Q}[x_1, \ldots, x_4]$
3) $M_3 = \langle (0, x_2x_3, x_1x_3),\, (0, x_1x_3, x_1x_2 - x_1x_3),\, (x_2x_3, x_1x_3 - x_2^2, 0),\, (x_2^2, x_2x_3, 0),\, (x_1x_2, 0, x_2x_3) \rangle \subseteq \mathbb{Q}[x_1, x_2, x_3]^3$

In the last part of this tutorial we want to use the Hilbert driven approach to speed up the computation of implicitizations. We shall apply it to the following variant of the technique explained in Tutorial 51. Notice that the results of Section 5.8 allow us to generalize the Hilbert driven approach for use with more general gradings and to use the technique of Tutorial 51 without modifications (see Exercise 80 in Section 5.8).

Let $P' = K[y_1, \ldots, y_m]$ be standard graded, let $f_1, \ldots, f_n \in P' \setminus \{0\}$, and let $d_i = \deg(f_i)$ for $i = 1, \ldots, n$.

f) Consider the following sequence of instructions.

1) Form the rings $\overline{P} = K[x_0, \ldots, x_n]$ and $\overline{Q} = K[x_0, \ldots, x_n, y_1, \ldots, y_m]$ and equip them with the standard grading.
2) For $i = 1, \ldots, n$, compute the homogenization f_i^{hom} of f_i with respect to x_0. Then form the ideal $\overline{J} = (x_1^{d_1} - f_1^{\mathrm{hom}}, \ldots, x_n^{d_n} - f_n^{\mathrm{hom}})$ in $\overline{Q}$.
3) Using the lexicographic term ordering where $x_1 >_{\mathtt{Lex}} \cdots >_{\mathtt{Lex}} x_n >_{\mathtt{Lex}} x_0 >_{\mathtt{Lex}} y_1 >_{\mathtt{Lex}} \cdots >_{\mathtt{Lex}} y_m$, determine the Hilbert numerator of J.
4) By applying the Hilbert Driven Buchberger Algorithm with respect to an elimination ordering for $y_1, \ldots, y_m$, compute the elimination ideal $\overline{I} = \overline{J} \cap \overline{P}$.

5) Let $\tilde{I} = \overline{I}^{\mathrm{deh}}$ be generated by $\{\tilde{g}_1, \ldots, \tilde{g}_s\}$. For $i = 1, \ldots, s$, write $\tilde{g}_i = g_i(x_1^{d_1}, \ldots, x_n^{d_n})$ with $g_i \in P$. Return $I = (g_1, \ldots, g_s)$ and stop.

Show that this is an algorithm which computes the implicitization of $(f_1, \ldots, f_n)$.

g) Write a CoCoA function `HDrivenImplicit(...)` which implements the algorithm of f). Apply your function to compute the implicitizations of the following tuples of polynomials. In each case, determine the degrees, pairs and generators skipped because of the Hilbert driven approach.

1) $(y_1 - 1,\ y_1^2 - 2y_1,\ y_1^3 - 3y_1^2) \in \mathbb{Q}[y_1]^3$
2) $(y_1^8,\ y_1^{10},\ y_1^{51} + y_1^6 + y_1) \in \mathbb{Q}[y_1]^3$
3) $(y_2y_3 + y_1,\ y_2^2y_3^3 + 2y_1y_2y_3 + y_1^2 + y_3^2 + y_2 - y_3,\ y_2y_3^3 + y_1y_3^2 + y_2^2y_3 - y_2y_3^2 + y_1y_2 - y_1y_3 + y_3) \in \mathbb{Q}[y_1, y_2, y_3]^3$

5.4 Dimension, Multiplicity, and Hilbert Polynomials

Inflation's down
except for what you actually buy.
(Chad Hudson)

In the first volume we had two quotes from David Hilbert, whereas in this volume we have already had three. By applying a suitable hedonic deflator, we can determine that the seasonally adjusted, monthly Hilbert quote core inflation rate is a little over 0.1%. The situation gets trickier if we look at what we actually do: the Hilbert functions we introduced in Section 5 are just the tip of an iceberg. In the last two sections they were joined by Hilbert series, Hilbert numerators, and Hilbert driven algorithms. In this section, we have Hilbert polynomials, simplified Hilbert numerators, and h-vectors in the offering.

What is the point of all this Hilbert theory? Hilbert functions provide us with an infinitude of numbers attached to a homogeneous ideal or graded module. Hilbert series allow us to manage these numbers in a small, simple to use package, and Hilbert numerators are useful for actually computing the essential information for describing Hilbert series. But somewhere hidden in this sea of numbers are some data which really capture the underlying geometric and the deeper algebraic structure of those ideals and modules. In this section we want to extract those data, study their basic properties and look for their true meaning.

In Section 5.2 we saw that the Hilbert series of a finitely generated graded module M is a fraction whose numerator is a Laurent polynomial and whose denominator is a power of $1 - z$. Remembering Hilbert's maxim to simplify the intricate, we reduce the Hilbert series of M as much as possible and use the simplified version to define the *dimension* and the *multiplicity* of M by its pole order and the value of its numerator at $z = 1$, respectively. After proving that the multiplicity is, in fact, always a positive integer, we compute $\dim(P)$ and $\operatorname{mult}(P)$, i.e. the dimension and the multiplicity of the polynomial ring.

In order to get a better feeling for these invariants, we proceed by proving the basic properties of the dimension and the multiplicity. Moreover, we can also encode the information contained in the Hilbert function of a module as its dimension and the tuple of coefficients of the numerator of its simplified Hilbert series. This tuple is called the h-vector of M, and its basic properties are provided as well.

Then the study of dimension is raised to a new level. We show that the dimension of an affine algebra of the form P/I does not change if we replace the ideal I by its radical. This shows that the dimension is really an invariant of geometric nature and depends only on the zero set of I. Further results in this direction are the formula $\dim(P/(I \cap J)) = \max\{\dim(P/I), \dim(P/J)\}$ which connects the dimension of a union of two zero sets to their individual dimensions, and the formula $\dim(M) = \dim(P/\operatorname{Ann}(M))$ contained in Theorem 5.4.10.

Recall that Theorem 5.1.21 said that Hilbert functions of finitely generated graded modules are integer functions of polynomial type. Therefore their associated polynomials are invariants of the module, and every integer we can attach to them is an invariant, too. Thus the second subsection commences by calling the associated polynomial of HF_M the Hilbert polynomial of M and denoting it by $\mathrm{HP}_M(t)$. We compute the Hilbert polynomial in a couple of easy cases and use the results of Section 5.1 to determine its basic properties.

However, a deeper insight is gained only if we connect the Hilbert polynomial to the invariants studied in the first subsection. Theorem 5.4.15 provides this connection and says that, essentially, $\dim(M)$ is the degree and $\mathrm{mult}(M)$ is $(\dim(M)-1)!$ times the leading coefficient of $\mathrm{HP}_M(t)$. Moreover, the same theorem shows how we can compute Hilbert polynomials effectively if we know the Hilbert series. Finally, we show the formula $\mathrm{HP}_{P/(I\cap J)}(t) = \mathrm{HP}_{P/I}(t)$ for homogeneous ideals J having $\sqrt{J} = P_+$. It says that the Hilbert polynomial is really an invariant of the *projective scheme* defined by I. Although that interpretation exceeds the scope of this book, it shows why Hilbert polynomials are popular among algebraic geometers, while computer algebraists usually prefer Hilbert series.

But dimension, multiplicity, and Hilbert polynomials are also versatile tools for applications of Computational Commutative Algebra in other areas besides algebraic geometry. In the tutorials we shall encounter two such areas: graph theory (see Tutorial 71) and photogrammetry (see Tutorial 72). Is this the end of the line? Will the rate of Hilbert inflation be kept under control from here on? Unfortunately not. In Chapter 6 we will introduce Hilbert bases, and it will be *déjà vu* all over again.

5.4.A Dimension and Multiplicity of Standard Algebras

Well and Good. Dreams are a multiplicity.[...]
These dimensions have nothing to do with frequency of dreaming,
but more to do with underlying principles of dream generation.
(Harry Hunt, "The Multiplicity of Dreams")

Throughout this subsection, we let K be a field, we let $P = K[x_1, \ldots, x_n]$ be standard graded, and we let M be a non-zero finitely generated graded P-module. In Theorem 5.2.20 we have seen that the Hilbert series of M is of the form $\mathrm{HS}_M(z) = \frac{z^\alpha \mathrm{HN}_M(z)}{(1-z)^n}$, where $\alpha = \alpha(M)$ is the initial degree of M, and where the Hilbert numerator $\mathrm{HN}_M(z)$ is a polynomial in $\mathbb{Z}[z]$ having $\mathrm{HN}_M(0) > 0$.

Just like the alchemists of yore, mathematicians always dream of distilling the essence of an object. In the case of Hilbert series, we can proceed as follows.

Definition 5.4.1. In the Hilbert series $\mathrm{HS}_M(z) = \frac{z^\alpha\,\mathrm{HN}_M(z)}{(1-z)^n}$, we simplify the fraction by cancelling $1-z$ as often as possible. We obtain a representation $\mathrm{HS}_M(z) = \frac{z^\alpha\,\mathrm{hn}_M(z)}{(1-z)^d}$, where $0 \le d \le n$ and where $\mathrm{hn}_M(z) \in \mathbb{Z}[z]$ satisfies $\mathrm{hn}_M(0) = \mathrm{HF}_M(\alpha) > 0$.

a) The polynomial $\mathrm{hn}_M(z) \in \mathbb{Z}[z]$ is called the **simplified Hilbert numerator** of M.
b) Let $\delta = \deg(\mathrm{hn}_M(z))$, and let $\mathrm{hn}_M(z) = h_0 + h_1 z + \cdots + h_\delta z^\delta$. Then the tuple $\mathrm{hv}(M) = (h_0, h_1, \ldots, h_\delta) \in \mathbb{Z}^{\delta+1}$ is called the **h-vector** of M.
c) The number $\dim(M) = d$ is called the **dimension** of M.
d) The number $\mathrm{mult}(M) = \mathrm{hn}_M(1)$ is called the **multiplicity** of M.

It is clear that the Hilbert series of M is completely determined by the numbers $\alpha(M)$, $\dim(M)$, and the tuple $\mathrm{hv}(M)$. Obviously, the multiplicity of M is nothing but the sum of the elements in the h-vector. By definition, we have $0 \le \dim(M) \le n$. The fact that $\mathrm{mult}(M)$ is a positive integer is not that obvious.

Proposition 5.4.2. *For a non-zero finitely generated graded P-module M, we have* $\mathrm{mult}(M) > 0$.

Proof. Let $d = \dim(M)$, and let $\mathrm{hv}(M) = (h_0, \ldots, h_\delta)$. By Lemma 5.2.9, we have $\mathrm{HS}_M(z) = \frac{z^\alpha\,\mathrm{hn}_M(z)}{(1-z)^d} = z^\alpha\,(h_0 + \cdots + h_\delta z^\delta) \sum_{i\ge 0} \binom{d+i-1}{d-1} z^i$. For $N \gg 0$, the coefficient of $z^{\alpha+N}$ of this power series is $h_0\binom{d+N-1}{d-1} + \cdots + h_\delta\binom{d+N-1-\delta}{d-1} = \frac{1}{(d-1)!}[h_0(N+d-1)\cdots(N+1) + \cdots + h_\delta(N+d-1-\delta)\cdots(N-\delta+1)]$. Since this number equals $\mathrm{HF}_M(N) > 0$ and since it is a polynomial of degree $d-1$ in N, its leading coefficient $\frac{1}{(d-1)!}(h_0 + \cdots + h_\delta)$ is positive. Thus we have $\mathrm{mult}(M) = \mathrm{hn}_M(1) = h_0 + \cdots + h_\delta > 0$. □

The dimension, the h-vector, and the multiplicity of the polynomial ring are easy to determine.

Example 5.4.3. In Proposition 5.2.14 we saw that the Hilbert series of P is $\mathrm{HS}_P(z) = \frac{1}{(1-z)^n}$. Therefore we have $\dim(P) = n$ and $\mathrm{hv}(P) = (1)$ and $\mathrm{mult}(P) = 1$. More generally, given a subset $L \subseteq \{x_1, \ldots, x_n\}$ consisting of m indeterminates, let I be the ideal generated by L. Then we have $\mathrm{HS}_{P/I}(z) = (1-z)^m\,\mathrm{HS}_P(z) = \frac{1}{(1-z)^{n-m}}$ by Corollary 5.2.17, and therefore $\dim(P/I) = n-m$ and $\mathrm{hv}(P/I) = (1)$ and $\mathrm{mult}(P/I) = 1$.

Let us compute the dimension, the h-vector, and the multiplicity in a slightly more complicated case.

Example 5.4.4. Let $f \in P$ be a non-zero homogeneous polynomial of degree $d > 0$. By Proposition 5.2.16, the Hilbert series of $P/(f)$ is given by $\mathrm{HS}_{P/(f)}(z) = \frac{1-z^d}{(1-z)^n} = \frac{1+z+\cdots+z^{d-1}}{(1-z)^{n-1}}$. Since the last fraction cannot be simplified anymore, we have $\dim(P/(f)) = n-1$ and $\mathrm{hv}(P/(f)) = (1, 1, \ldots, 1) \in \mathbb{Z}^d$ and $\mathrm{mult}(P/(f)) = d$.

Using the basic properties of Hilbert series, we can prove a number of basic properties of the dimension, the h-vector, and the multiplicity of a graded module.

Proposition 5.4.5. (Basic Properties of Dim and Mult)
Let M, M', and M'' be non-zero finitely generated graded P-modules.

a) For every $i \in \mathbb{Z}$, we have $\dim(M(i)) = \dim(M)$ and $\mathrm{hv}(M(i)) = \mathrm{hv}(M)$. In particular, we have $\mathrm{mult}(M(i)) = \mathrm{mult}(M)$.

b) Given a homogeneous exact sequence of graded P-modules

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

we have $\dim(M) = \max\{\dim(M'), \dim(M'')\}$ and

$$\mathrm{mult}(M) = \begin{cases} \mathrm{mult}(M') + \mathrm{mult}(M'') & \text{if } \dim(M') = \dim(M''), \\ \mathrm{mult}(M') & \text{if } \dim(M') > \dim(M''), \\ \mathrm{mult}(M'') & \text{if } \dim(M'') > \dim(M'). \end{cases}$$

c) Given non-zero finitely generated graded P-modules $M_1, \ldots, M_r$, the module $M = M_1 \oplus \cdots \oplus M_r$ satisfies $\dim(M) = \max\{\dim(M_1), \ldots, \dim(M_r)\}$ and $\mathrm{mult}(M) = \sum_{\{i \mid \dim(M_i) = \dim(M)\}} \mathrm{mult}(M_i)$.

d) Let $\delta_1, \ldots, \delta_r \in \mathbb{Z}$, and let $I \subset P$ be a homogeneous ideal. Then the finitely generated graded P/I-module $F = \bigoplus_{i=1}^{r} (P/I)(-\delta_i)$ satisfies $\dim(F) = \dim(P/I)$ and $\mathrm{mult}(F) = r \cdot \mathrm{mult}(P/I)$.

e) Let $\delta_1, \ldots, \delta_r \in \mathbb{Z}$, let N be a non-zero graded submodule of the graded free module $F = \bigoplus_{i=1}^{r} P(-\delta_i)$, and let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. Then we have $\dim(\mathrm{LT}_\sigma(N)) = \dim(N)$ and $\mathrm{hv}(\mathrm{LT}_\sigma(N)) = \mathrm{hv}(N)$.
In particular, we have $\mathrm{mult}(\mathrm{LT}_\sigma(N)) = \mathrm{mult}(N)$. Moreover, if $F/N \neq 0$, we have $\dim(F/N) = \dim(F/\mathrm{LT}_\sigma(N))$ and $\mathrm{hv}(F/N) = \mathrm{hv}(F/\mathrm{LT}_\sigma(N))$ and $\mathrm{mult}(F/N) = \mathrm{mult}(F/\mathrm{LT}_\sigma(N))$.

f) Let $K \subseteq L$ be a field extension. Then we have $\dim(M \otimes_K L) = \dim(M)$ and $\mathrm{hv}(M \otimes_K L) = \mathrm{hv}(M)$. Thus we have $\mathrm{mult}(M \otimes_K L) = \mathrm{mult}(M)$.

g) Let $\delta = \deg(\mathrm{hn}_M(z))$. Then the h-vector of M satisfies $\mathrm{hv}(M) = (\Delta^d \mathrm{HF}_M(\alpha), \ldots, \Delta^d \mathrm{HF}_M(\alpha + \delta))$ where $d = \dim(M)$.

Proof. Claim a) follows immediately from Proposition 5.2.15.a. To prove b), we assume that M, M', and M'' have initial degrees α, α', and α'' and dimensions d, d', and d'', respectively. Then Proposition 5.2.15.b yields

$$\mathrm{HS}_M(z) = \frac{z^\alpha \mathrm{hn}_M(z)}{(1-z)^d} = \frac{z^{\alpha'} \mathrm{hn}_{M'}(z)}{(1-z)^{d'}} + \frac{z^{\alpha''} \mathrm{hn}_{M''}(z)}{(1-z)^{d''}} = \mathrm{HS}_{M'}(z) + \mathrm{HS}_{M''}(z)$$

Now we distinguish three cases. If $d' = d''$, then $z^\alpha \mathrm{hn}_M(z)(1-z)^{d'} = [z^{\alpha'} \mathrm{hn}_{M'}(z) + z^{\alpha''} \mathrm{hn}_{M''}(z)](1-z)^d$, and consequently $d' \geq d$. But since $\mathrm{mult}(M') = \mathrm{hn}_{M'}(1)$ and $\mathrm{mult}(M'') = \mathrm{hn}_{M''}(1)$ are positive, the sum in square brackets is not divisible by $1 - z$. Hence we see that $d = d'$

and $\operatorname{mult}(M) = \operatorname{hn}_M(1) = \operatorname{hn}_{M'}(1) + \operatorname{hn}_{M''}(1) = \operatorname{mult}(M') + \operatorname{mult}(M'')$. Now, if $d' > d''$, then the equality $z^\alpha \operatorname{hn}_M(z)(1-z)^{d'} = [z^{\alpha'} \operatorname{hn}_{M'}(z) + z^{\alpha''} \operatorname{hn}_{M''}(z)(1-z)^{d'-d''}](1-z)^d$ shows $d = d'$, because $\operatorname{mult}(M') = \operatorname{hn}_{M'}(1) > 0$ implies that the sum in square brackets is not divisible by $1-z$. It follows that $\operatorname{mult}(M) = \operatorname{hn}_M(1) = \operatorname{hn}_{M'}(1) = \operatorname{mult}(M')$. Finally, if $d'' > d'$, we obtain $d = d''$ and $\operatorname{mult}(M) = \operatorname{mult}(M'')$ analogously.

Claim c) follows from b) by an easy induction on r, and d) follows from c) and a). Moreover, parts e) and f) follow from Theorem 5.2.18 and Corollary 5.2.19 which say that the corresponding Hilbert series are equal. Finally, to prove g), we let $\operatorname{hn}_M(z) = h_0 + \cdots + h_\delta z^\delta$ with $h_0, \ldots, h_\delta \in \mathbb{Z}$. We apply Proposition 5.2.8.a and get $\operatorname{HS}_{\Delta^d \operatorname{HF}_M}(z) = (1-z)^d \operatorname{HS}_{\operatorname{HF}_M}(z) = z^\alpha (h_0 + h_1 z + \cdots + h_\delta z^\delta)$. By the definition of the Hilbert series, this yields $\Delta^d \operatorname{HF}_M(\alpha + i) = h_i$ for $i = 0, \ldots, \delta$, and the claim follows. □

The remainder of this subsection is devoted to providing the reader with some useful properties of the dimension and the multiplicity of a graded module. In particular, we describe the effect of common ideal-theoretic operations on the dimension and the multiplicity of standard graded K-algebras. Our first proposition in this direction says that the dimension of a module M can decrease at most by one when we pass to a residue class module of the form M/fM.

Proposition 5.4.6. *Let M be a non-zero finitely generated graded P-module, and let $f \in P \setminus K$ be a homogeneous polynomial. Then we have*

$$\dim(M) - 1 \leq \dim(M/fM) \leq \dim(M)$$

If f is a non-zero divisor for M, we have $\dim(M/fM) = \dim(M) - 1$.

Proof. Let $d = \dim(M)$ and $\delta = \deg(f)$. Multiplication by f induces the exact sequence of graded P-modules

$$0 \longrightarrow [0 :_M (f)](-\delta) \longrightarrow M(-\delta) \longrightarrow M \longrightarrow M/fM \longrightarrow 0$$

Thus Proposition 5.4.5.b shows the inequality $\dim(M/fM) \leq \dim(M)$. To prove the first inequality, we let $N = [0 :_M (f)](-\delta)$ and use the exact sequence to see that $\operatorname{HS}_{M/fM}(z) = (1-z^\delta) \operatorname{HS}_M(z) + \operatorname{HS}_N(z)$. Next we let $d' = \dim(M/fM)$ and $d'' = \dim(N)$. By Proposition 5.4.5.b, we have $d'' \leq d$. Using the abbreviations $\alpha' = \alpha(M/fM)$ and $\alpha'' = \alpha(N)$, we get

$$\frac{z^{\alpha'} \operatorname{hn}_{M/fM}(z)}{(1-z)^{d'}} = \frac{z^\alpha \operatorname{hn}_M(z) \cdot (1+z+\cdots+z^{\delta-1})}{(1-z)^{d-1}} + \frac{z^{\alpha''} \operatorname{hn}_N(z)}{(1-z)^{d''}}$$

If $d'' = d$, the right-hand side yields $\frac{z^\alpha \operatorname{hn}_M(z) \cdot (1-z^\delta) + z^{\alpha''} \operatorname{hn}_N(z)}{(1-z)^d}$. Since this fraction cannot be simplified further, we have $d' = d$. Similarly, if $d'' \leq d-2$, the right-hand side yields $\frac{z^\alpha \operatorname{hn}_M(z) \cdot (1+z+\cdots+z^{\delta-1}) + z^{\alpha''} \operatorname{hn}_N(z) \cdot (1-z)^{d-1-d''}}{(1-z)^{d-1}}$ and

this fraction cannot be simplified further. Thus we have $d' = d-1$ in this case. Finally, if $d'' = d-1$, the numerator of the combined fraction on the right-hand side has the value $\delta \operatorname{hn}_M(1) + \operatorname{hn}_N(1)$ at $z = 1$, and this value is positive by Proposition 5.4.2. Hence the combined fraction cannot be simplified further and we obtain $d' = d-1$. Altogether, we have shown that we have $d-1 \leq d' \leq d$, as claimed.

If f is a non-zero divisor for M, we have $N = 0$ and $d' = d-1$ because the fraction $\frac{z^\alpha \operatorname{hn}_M(z)\cdot(1+z+\cdots+z^{\delta-1})}{(1-z)^{d-1}}$ cannot be simplified further. □

The following example shows that in this proposition we may have $\dim(M/fM) = \dim(M)$.

Example 5.4.7. Let $P = \mathbb{Q}[x,y]$, let $M = P/(xy)$, and let $f = x$. Then we have $\dim(M/fM) = \dim(P/(x)) = 1 = \dim(P/(xy)) = \dim(M)$. In fact, consider the exact sequence

$$0 \longrightarrow [(y)/(xy)](-1) \longrightarrow [P/(xy)](-1) \longrightarrow P/(xy) \longrightarrow P/(x) \longrightarrow 0$$

Since $[(y)/(xy)](-1) \cong [P/(x)](-2)$, we obtain

$$\operatorname{HS}_{M/fM}(z) = \tfrac{1}{1-z} = (1-z)\tfrac{1+z}{1-z} + z^2\tfrac{1}{1-z} = (1-z)\operatorname{HS}_M(z) + z^2 \operatorname{HS}_{M/fM}(z)$$

Our next result is that the dimension of an affine algebra P/I does not change if we replace I by its radical. Hence the dimension is an invariant which is basically of *geometric* nature, i.e. it depends only on the set of zeros of I.

Proposition 5.4.8. *Let I and J be proper homogeneous ideals in P.*

a) If $I \subseteq J$, then we have $\dim(P/I) \geq \dim(P/J)$.
b) For all $i > 0$, we have $\dim(P/I) = \dim(P/I^i)$.
c) There exists a number $i > 0$ such that $(\sqrt{I})^i \subseteq I$. In particular, we have $\dim(P/I) = \dim(P/\sqrt{I})$.

Proof. In order to show a), it is enough to apply Proposition 5.4.5.b to the canonical surjective P-linear map $P/I \twoheadrightarrow P/J$. Next we prove b) by induction on i, the case $i = 1$ being identically true. For $i > 0$ we consider the homogeneous exact sequence

$$0 \longrightarrow I^{i-1}/I^i \longrightarrow P/I^i \longrightarrow P/I^{i-1} \longrightarrow 0$$

where the maps are the natural ones, and use Propositon 5.4.5.b to see that $\dim(P/I^i) = \max\{\dim(I^{i-1}/I^i), \dim(P/I^{i-1})\}$. The induction hypothesis yields $\dim(P/I^{i-1}) = \dim(P/I)$. Since I^{i-1}/I^i is a finitely generated graded P/I-module, it is a quotient of a finitely generated graded free P/I-module. So, parts b) and d) of Proposition 5.4.5 show $\dim(I^{i-1}/I^i) \leq \dim(P/I)$. Hence it follows that $\dim(P/I^i) = \dim(P/I)$.

For the proof of the first part of c), we choose a system of generators $\{g_1, \dots, g_s\}$ of $\sqrt{I}$, and for $j = 1, \dots, s$ we let $\alpha_j \geq 1$ be such that $g_j^{\alpha_j} \in I$. Given numbers $\beta_1, \dots, \beta_s \in \mathbb{N}$ such that $\beta_1 + \cdots + \beta_s \geq \alpha_1 + \cdots + \alpha_s - s + 1$, we have $g_1^{\beta_1} \cdots g_s^{\beta_s} \in I$, because for at least one index $j \in \{1, \dots, s\}$ we must have $\beta_j \geq \alpha_j$. Let $f_k = h_{k1}g_1 + \cdots + h_{ks}g_s \in \sqrt{I}$ with $h_{k1}, \dots, h_{ks} \in P$. By expanding the product, we see that $f_1 \cdots f_i \in I$ for $i \geq \alpha_1 + \cdots + \alpha_s - s + 1$. This implies $(\sqrt{I})^i \subseteq I \subseteq \sqrt{I}$ for those i. The second part of c) follows by applying a) and b), because $\dim(P/\sqrt{I}) \leq \dim(P/I) \leq \dim(P/(\sqrt{I})^i) = \dim(P/\sqrt{I})$ for $i \gg 0$ implies that we have equality everywhere. □

Our next proposition discusses the dimension and the multiplicity of an affine K-algebra defined by the intersection of two ideals. Geometrically, this corresponds to taking the union of two zero sets.

Proposition 5.4.9. *Let I and J be proper homogeneous ideals in P.*

a) We have $\dim(P/(I \cap J)) = \max\{\dim(P/I), \dim(P/J)\}$.
b) If we have $\dim(P/I) = \dim(P/J) > \dim(P/(I + J))$, *then we find* $\operatorname{mult}(P/(I \cap J)) = \operatorname{mult}(P/I) + \operatorname{mult}(P/J)$.
c) If $\dim(P/I) > \dim(P/J)$, *then we have* $\operatorname{mult}(P/(I \cap J)) = \operatorname{mult}(P/I)$.

Proof. To show a), we construct two homogeneous exact sequences

$$0 \longrightarrow P/(I \cap J) \longrightarrow (P/I) \oplus (P/J) \longrightarrow P/(I + J) \longrightarrow 0 \tag{1}$$

$$0 \longrightarrow P/I \longrightarrow (P/I) \oplus (P/J) \longrightarrow P/J \longrightarrow 0 \tag{2}$$

The first sequence is defined by the map $P/(I \cap J) \longrightarrow (P/I) \oplus (P/J)$ given by $f + (I \cap J) \mapsto (f + I, f + J)$ and the map $(P/I) \oplus (P/J) \longrightarrow P/(I + J)$ given by $(f + I, g + J) \mapsto f - g + I + J$. The second sequence is defined by the natural maps. By applying Proposition 5.4.5.b to these two sequences, we get

$$\dim((P/I) \oplus (P/J)) = \max\{\dim(P/(I \cap J)), \dim(P/(I + J))\}$$

and

$$\dim((P/I) \oplus (P/J)) = \max\{\dim(P/I), \dim(P/J)\}$$

The fact that the former is exactly $\dim(P/(I \cap J))$ follows from Proposition 5.4.8.a, since $I \cap J \subseteq I + J$. Putting together the two pieces of information, we get a).

Claims b) and c) follow from the assumption and Proposition 5.4.5.b applied to the sequences (1) and (2). □

The last result of this subsection combines much of what we have proved above and yields a useful formula for the dimension of a graded module. Recall that a module M over a ring R can be considered as a module over the residue class ring $R/\operatorname{Ann}_R(M)$ because the elements of $\operatorname{Ann}_R(M)$ act trivially on M.

Theorem 5.4.10. *Let M be a non-zero finitely generated graded P-module. Then we have* $\dim(M) = \dim(P/\operatorname{Ann}(M))$.

Proof. Let $\{g_1, \ldots, g_r\}$ be a minimal homogeneous system of generators of M, and let $\delta_i = \deg(g_i)$ for $i = 1, \ldots, r$. We use the notation $\mathfrak{a}_i = \operatorname{Ann}(g_i)$ for $i = 1, \ldots, r$, observe that $\operatorname{Ann}(M) = \cap_{i=1}^r \mathfrak{a}_i$. Without loss of generality, we may assume that $i < j$ implies $\dim(P/\mathfrak{a}_i) \geq \dim(P/\mathfrak{a}_j)$.

Now we use induction on r, the minimal number of homogeneous generators of M. If $r = 1$, then M is isomorphic to $(P/\mathfrak{a}_1)(-\delta_1)$, and the conclusion follows from Proposition 5.4.5.d. If $r > 1$, we let $N = \langle g_1, \ldots, g_{r-1} \rangle$. Consider the canonical exact sequence of graded P-modules

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

By Proposition 5.4.5.b, we have $\dim(M) \geq \dim(N)$. By induction, we have $\dim(N) = \dim(P/\operatorname{Ann}(N)) = \dim(P/(\cap_{i=1}^{r-1} \mathfrak{a}_i))$. This dimension equals $\max\{\dim(P/\mathfrak{a}_1), \ldots, \dim(P/\mathfrak{a}_{r-1})\}$ by Proposition 5.4.9.a. Hence the assumption $\dim(P/\mathfrak{a}_{r-1}) \geq \dim(P/\mathfrak{a}_r)$ implies that the dimension of N equals $\max\{\dim(P/\mathfrak{a}_1), \ldots, \dim(P/\mathfrak{a}_r)\}$. Therefore we can use Proposition 5.4.9.a again to deduce that the maximum is equal to $\dim(P/(\cap_{i=1}^r \mathfrak{a}_i))$, and hence equal to $\dim(P/\operatorname{Ann}(M))$. Altogether, we get $\dim(M) \geq \dim(P/\operatorname{Ann}(M))$. Conversely, we have a canonical surjective homomorphism

$$\textstyle\bigoplus_{i=1}^r (P/\operatorname{Ann}(M))(-\delta_i) \to M \to 0$$

Using parts b) and d) of Proposition 5.4.5, we obtain the other inequality $\dim(M) \leq \dim(P/\operatorname{Ann}(M))$. □

5.4.B Hilbert Polynomials in the Standard Graded Case

Let us continue to use the assumptions introduced at the beginning of the last subsection. From Theorem 5.1.21 we know that the Hilbert function of M is an integer function of polynomial type.

Definition 5.4.11. Let t be an indeterminate over $\mathbb{Q}$.

a) The integer valued polynomial associated to HF_M is called the **Hilbert polynomial** of M and is denoted by $\mathrm{HP}_M(t)$. Therefore we have $\mathrm{HP}_M(t) \in \mathbb{IP} \subset \mathbb{Q}[t]$ and $\mathrm{HF}_M(i) = \mathrm{HP}_M(i)$ for $i \gg 0$.
b) The regularity index of HF_M is called the **regularity index** of M and is denoted by $\operatorname{ri}(M)$.

Since the Hilbert polynomial of M is an invariant of the module, it can be used to define many other invariants of M. For instance its degree and its coefficients are numerical invariants of M. During the course of this subsection, we shall try to understand the relationship of some of those invariants to the invariants defined in the preceding subsection. Let us begin by computing the Hilbert polynomial and the regularity index in some easy cases.

Example 5.4.12. The Hilbert function of P is $\mathrm{HF}_P(i) = \mathrm{bin}_{n-1}(i+n-1)$ for all $i \in \mathbb{Z}$. Therefore the Hilbert polynomial of P is $\mathrm{HP}_P(t) = \binom{t+n-1}{n-1}$. Clearly, we have $\mathrm{HP}_P(i) = \mathrm{HF}_P(i)$ for $i \geq -n+1$ and $\mathrm{HP}_P(-n) = \binom{-1}{n-1} = (-1)^{n-1} \neq \mathrm{HF}_P(-n) = 0$. Thus we have $\mathrm{ri}(P) = -n+1$.

Also rings of the form $P/(f)$ with a non-zero homogeneous polynomial f are easy to handle.

Example 5.4.13. Let $f \in P$ be a non-zero homogeneous polynomial of degree $d > 0$. The Hilbert function of $P/(f)$ is $\mathrm{HF}_{P/(f)}(i) = \Delta_d \mathrm{HF}_P(i)$ for all $i \in \mathbb{Z}$. Therefore we have $\mathrm{HF}_{P/(f)}(i) = \binom{i+n-1}{n-1} - \binom{i-d+n-1}{n-1}$ for $i \geq d$, and thus $\mathrm{HP}_{P/(f)}(t) = \binom{t+n-1}{n-1} - \binom{t-d+n-1}{n-1}$. Since we have $\mathrm{HP}_{P/(f)}(i) = \mathrm{HF}_{P/(f)}(i)$ for $i \geq d-n+1$ and $\mathrm{HP}_{P/(f)}(d-n) = \binom{d-1}{n-1} - (-1)^{n-1} \neq \mathrm{HF}_{P/(f)}(d-n) = \binom{d-1}{n-1}$, it follows that $\mathrm{ri}(P/(f)) = d-n+1 = \mathrm{ri}(P)+d$, in agreement with Corollary 5.1.11.b

It is not difficult to use the basic properties of Hilbert functions shown in Section 5.1.B in order to determine the basic properties of Hilbert polynomials. We leave it to the reader to write down similar properties of the regularity index (see also Exercise 7).

Proposition 5.4.14. (Basic Properties of Hilbert Polynomials)
Let M, M', and M'' be three finitely generated graded P-modules.

a) For every $i \in \mathbb{Z}$, we have $\mathrm{HP}_{M(i)}(t) = \mathrm{HP}_M(t+i)$.
b) Given a homogeneous exact sequence of graded P-modules

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

we have $\mathrm{HP}_M(t) = \mathrm{HP}_{M'}(t) + \mathrm{HP}_{M''}(t)$.
c) Given finitely many finitely generated graded P-modules $M_1, \ldots, M_r$, we have $\mathrm{HP}_{M_1 \oplus \cdots \oplus M_r}(t) = \mathrm{HP}_{M_1}(t) + \cdots + \mathrm{HP}_{M_r}(t)$.
d) Let $\delta_1, \ldots, \delta_r \in \mathbb{Z}$. The Hilbert polynomial of the finitely generated graded free P-module $F = \bigoplus_{i=1}^r P(-\delta_i)$ is $\mathrm{HP}_F(t) = \sum_{i=1}^r \binom{t-\delta_i+n-1}{n-1}$.
e) Let $\delta_1, \ldots, \delta_r \in \mathbb{Z}$, let N be a graded submodule of $F = \bigoplus_{i=1}^r P(-\delta_i)$, and let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. Then we have $\mathrm{HP}_N(t) = \mathrm{HP}_{\mathrm{LT}_\sigma(N)}(t)$ and $\mathrm{HP}_{F/N}(t) = \mathrm{HP}_{F/\mathrm{LT}_\sigma(N)}(t)$.
f) Let $K \subseteq L$ be a field extension. Then we have $\mathrm{HP}_{M \otimes_K L}(t) = \mathrm{HP}_M(t)$.

Proof. Claims a), b), c), and d) follow immediately from the corresponding properties of Hilbert functions shown in Proposition 5.1.14. Similarly, claim e) follows from Theorem 5.1.18 and b), and claim f) is a consequence of Corollary 5.1.20. □

It is clear that we can effectively compute the simplification of the Hilbert series of M required by Definition 5.4.1. Our next theorem says that the simplified Hilbert numerator $\mathrm{hn}_M(z)$ can be used to calculate the Hilbert polynomial of M.

Theorem 5.4.15. (Computation of Hilbert Polynomials)
Let M be a non-zero finitely generated graded P-module with initial degree $\alpha = \min\{i \in \mathbb{Z} \mid M_i \neq 0\}$, and let $d = \dim(M)$.

a) Let $\mathrm{hn}_M(z) = h_0 + h_1 z + \cdots + h_\delta z^\delta$, where $h_0 > 0$ and $h_\delta \neq 0$. We have

$$\mathrm{HP}_M(t) = \begin{cases} \sum_{i=0}^{\delta} h_i \binom{t-\alpha-i+d-1}{d-1} & \text{if } d > 0, \\ 0 & \text{if } d = 0. \end{cases}$$

b) We have $\dim(M) = \begin{cases} 1 + \deg(\mathrm{HP}_M(t)) & \text{if } \mathrm{HP}_M(t) \neq 0, \\ 0 & \text{if } \mathrm{HP}_M(t) = 0. \end{cases}$

c) We have $\mathrm{mult}(M) = \begin{cases} (d-1)!\, \mathrm{LC}_{\mathtt{Deg}}(\mathrm{HP}_M(t)) & \text{if } d > 0, \\ \dim_K(M) & \text{if } d = 0. \end{cases}$

d) The regularity index of M satisfies $\mathrm{ri}(M) = \alpha + \delta - d + 1$.

Proof. To prove a), we invoke Corollary 5.2.11.b in the present situation. Namely, the Hilbert series of M has the form $\mathrm{HS}_M(z) = \frac{z^\alpha \mathrm{hn}_M(z)}{(1-z)^d}$ with $z^\alpha \mathrm{hn}_M(z) = h_0 z^\alpha + \cdots + h_\delta z^{\alpha+\delta}$. For $d = 0$, we have $\mathrm{HP}_M(t) = 0$. For $d > 0$, we have $\mathrm{HP}_M(t) = \sum_{i=\alpha}^{\alpha+\delta} h_{i-\alpha} \binom{t-i+d-1}{d-1} = \sum_{i=0}^{\delta} h_i \binom{t-\alpha-i+d-1}{d-1}$.

Now we show b). If $\mathrm{HP}_M(t) = 0$, the Hilbert series of M is a Laurent polynomial. Therefore it is of the form $\mathrm{HS}_M(z) = \frac{z^\alpha \mathrm{hn}_M(z)}{(1-z)^0}$, and we get $\dim(M) = 0$. If we have $\mathrm{HP}_M(t) \neq 0$, we can use a) to get $\mathrm{HP}_M(t) = \sum_{i=0}^{\delta} h_i \binom{t-\alpha-i+d-1}{d-1}$. We obtain $\frac{1}{(d-1)!}(h_0 + \cdots + h_\delta) = \frac{1}{(d-1)!}\mathrm{hn}_M(1)$ as the coefficient of t^{d-1}. Hence we have $\deg(\mathrm{HP}_M(t)) = d - 1$.

Next we prove c). For $d > 0$, we have just seen that $\mathrm{LC}_{\mathtt{Deg}}(\mathrm{HP}_M(t)) = \frac{1}{(d-1)!}(h_0 + \cdots + h_\delta)$. This yields $(d-1)!\, \mathrm{LC}_{\mathtt{Deg}}(\mathrm{HP}_M(t)) = h_0 + \cdots + h_\delta = \mathrm{hn}_M(1)$. For $d = 0$, we have $\mathrm{HS}_M(z) = \mathrm{hn}_M(z)$ and $\mathrm{mult}(M) = \mathrm{hn}_M(1) = \sum_{i \in \mathbb{Z}} \dim_K(M_i) = \dim_K(M)$.

Finally, we note that the proof of d) follows from Corollary 5.2.11.c. □

As we mentioned above, part a) of this theorem allows us to compute Hilbert polynomials effectively, since we know from the previous section how to compute $\mathrm{HN}_M(z)$, and dividing this polynomial repeatedly by $(1 - z)$ yields $\mathrm{hn}_M(z)$. If we are only interested in the dimension of M, we can use the simpler algorithm described in Tutorial 70. Parts b) and c) of this theorem show that $\dim(M)$ and $\mathrm{mult}(M)$ are related to the degree and the leading coefficient of the Hilbert polynomial of M.

Our last proposition in this subsection provides some rules for the behaviour of Hilbert polynomials under certain ideal-theoretic operations.

Proposition 5.4.16. *Let I and J be proper homogeneous ideals of P.*

a) We have $\mathrm{HP}_{P/(I \cap J)}(t) = \mathrm{HP}_{P/I}(t) + \mathrm{HP}_{P/J}(t) - \mathrm{HP}_{P/(I+J)}(t)$.

b) If $\sqrt{J} = P_+ = (x_1, \ldots, x_n)$, *we have* $\mathrm{HP}_{P/(I \cap J)}(t) = \mathrm{HP}_{P/I}(t)$.

Proof. To prove a), it suffices to apply the additivity of Hilbert polynomials shown in Proposition 5.4.14.b to the exact sequences (1) and (2) constructed in the proof of Proposition 5.4.9.

Now we show b). The assumption on J implies that we also have $\sqrt{I+J} = P_+$. Thus Proposition 5.4.8.c yields $\dim(P/J) = \dim(P/(I+J)) = \dim(P/P_+)$. On the other hand, it is clear that $\mathrm{HP}_{P/P_+}(t) = 0$. Hence $\dim(P/P_+) = 0$, and consequently $\mathrm{HP}_{P/J}(t) = \mathrm{HP}_{P/(I+J)}(t) = 0$ by Theorem 5.4.15.b. Now the conclusion follows from a). □

Exercise 1. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let $I \subseteq P$ be a homogeneous ideal having $\dim(P/I) = d$. Assume that there exist d linear forms $\ell_1, \ldots, \ell_d$ such that $\ell_1, \ldots, \ell_d$ is a regular sequence for P/I. Show that all components of the h-vector $\mathrm{hv}(P/I)$ are positive.

Exercise 2. Let K be a field, and let $P = K[x, y]$ be standard graded. Show that $\frac{1-2z^2}{(1-z)^2}$ cannot be the Hilbert series of any finitely generated graded P-module.

Exercise 3. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let $f, g \in P$ be non-constant homogeneous polynomials. Assume that $\gcd(f, g) = 1$, and let I be the ideal generated by $\{f, g\}$. Show that $\dim(P/I) = n - 2$ and $\mathrm{mult}(P/I) = \deg(f) \cdot \deg(g)$.

Exercise 4. Let K be a field, let $P = K[x, y, z]$ be standard graded, let $f_1, f_2, f_3 \in P$ be pairwise coprime homogeneous polynomials, and let $I = (f_1, f_2, f_3)$.

a) Show that $\dim(P/I) \leq 1$. Find an example for which $\dim(P/I) = 0$ and an example for which $\dim(P/I) = 1$.
b) Find an example for which $\dim(P/I) = 1$ and $\mathrm{mult}(P/I) = 1$.

Exercise 5. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let M be a non-zero finitely generated graded P-module. Moreover, let $f \in P$ be a non-zero homogeneous polynomial which is a non-zero divisor for M.

a) Show that we have $\mathrm{mult}(M/fM) = \deg(f) \cdot \mathrm{mult}(M)$.
b) Show that we have $\mathrm{HP}_{M/fM}(t) = \mathrm{HP}_M(t) - \mathrm{HP}_M(t - \deg(f))$.

Exercise 6. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let $f_1, \ldots, f_n$ be homogeneous polynomials of degree two which form a regular sequence, and let $S = \mathrm{Syz}_P(f_1, \ldots, f_n)$. Compute $\mathrm{HS}_S(z)$, $\mathrm{HP}_S(t)$, $\dim(S)$, and $\mathrm{mult}(S)$.

Exercise 7. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let M, M' be two finitely generated graded P-modules.

a) For $i \in \mathbb{Z}$, prove that $\mathrm{ri}(M(i)) = \mathrm{ri}(M) - i$.
b) Show that $\mathrm{ri}(M \oplus M') \leq \max\{\mathrm{ri}(M), \mathrm{ri}(M')\}$. Find an example in which we have a strict inequality here.

c) Suppose that M is a graded submodule of a graded free P-module $\bigoplus_{i=1}^{r} P(-\delta_i)$. Let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. Prove that $\mathrm{ri}(\mathrm{LT}_\sigma(M)) = \mathrm{ri}(M)$.
d) Let $K \subseteq L$ be a field extension. Show that $\mathrm{ri}(M \otimes_K L) = \mathrm{ri}(M)$.

Exercise 8. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let M be a non-zero finitely generated graded P-module of dimension $d > 0$. Write $\mathrm{HS}_M(z) = \frac{z^\alpha \, \mathrm{hn}_M(z)}{(1-z)^d}$ as in Definition 5.4.1.

a) Prove that $\mathrm{HP}_M(t)$ has a representation $\mathrm{HP}_M(t) = \sum_{i=0}^{d-1} e_i \binom{t+d-1-i}{d-1-i}$ with $e_0, \ldots, e_{d-1} \in \mathbb{Z}$.
b) Show that $e_0 = \mathrm{mult}(M)$.

Tutorial 70: Computing the Dimension of a Module

In 1998, in the biggest incident of its kind,
a Salomon Brothers trader mistakenly sold
1.2 billion dollars worth of French government bonds
when he carelessly leaned on his keyboard.
(BBC news, Sep. 28, 2001)

This tutorial foreshadows some results which will be studied more thoroughly in Section 5.7. So, we give a spoiler warning and continue anyway. Suppose that a finitely generated graded module is given by generators and relations, and that we are interested in computing its dimension, but not necessarily its Hilbert series or its Hilbert polynomial. Can we do better than simply go through the general procedure which follows from the computation of the Hilbert series? Yes, we can, and here we shall find out how it works.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let M be a finitely generated graded P-module which is given by a homogeneous presentation $M = F/N$, where $F = \bigoplus_{i=1}^{r} P(-\delta_i)$ is a graded free P-module and $N \subset F$ a graded submodule.

a) Explain how one can use Theorem 5.4.10 and Proposition 5.4.5 to reduce the problem of computing $\dim(M)$ to the problem of computing $\dim(P/I)$ for a non-zero proper monomial ideal $I \subset P$.
b) Assume that there is a CoCoA function `MonIdDim(...)` which computes $\dim(P/I)$ for a non-zero proper monomial ideal $I \subset P$. Write a CoCoA function `ModuleDim(...)` which takes a homogeneous presentation matrix of M and computes $\dim(M)$.

From now on, let I be a non-zero proper monomial ideal in P, and let $\{t_1, \ldots, t_s\}$ be its minimal monomial system of generators. For $i = 1, \ldots, s$, we write $t_i = x_1^{\alpha_{i1}} \cdots x_n^{\alpha_{in}}$ with $\alpha_{i1}, \ldots, \alpha_{in} \in \mathbb{N}$.

c) For $i = 1, \ldots, s$, let $t'_i = \prod_{\{j \mid \alpha_{ij} > 0\}} x_j$. Show that there exists a number $k \geq 1$ such that $J = (t'_1, \ldots, t'_s)$ satisfies $J^k \subseteq I \subseteq J$. Conclude that $\dim(P/I) = \dim(P/J)$.

d) Prove that the ideal J defined in c) is an intersection of linear ideals, i.e. ideals of the form $(x_{i_1}, \ldots, x_{i_\nu})$, where $1 \leq i_1 < \cdots < i_\nu \leq n$. Find an explicit way to compute a set of linear ideals whose intersection is J. (*Hint:* Consider the minimal monomial system of generators of J. Take one indeterminate from each generator in all possible ways.)

e) Show that $\dim(P/(x_{i_1}, \ldots, x_{i_\nu})) = n - \nu$ for all $1 \leq i_1 < \cdots < i_\nu \leq n$. Use this result to write down a formula for $\dim(P/J)$.

f) Combining the results of c), d), and e), implement a CoCoA function `MonIdDim(...)` which takes a system of generators of a non-zero proper monomial ideal $I \subset P$ and computes $\dim(P/I)$.

g) Apply your function `MonIdDim(...)` to compute $\dim(P/I_i)$ for the following monomial ideals I_i, where $i \in \{1, 2, 3\}$.

1) $I_1 = (x^3, xy^2, xyz, xz^2, x^2y, x^2z, xy^2z)$ in $\mathbb{Q}[x, y, z]$
2) $I_2 = (x_1x_2x_3^2, x_1^2x_2^4x_4^2, x_2^3x_3x_4^2, x_3^3)$ in $\mathbb{Q}[x_1, x_2, x_3, x_4]$
3) $I_3 = (x_ix_j \mid 1 \leq i < j \leq 10)$ in $\mathbb{Q}[x_1, \ldots, x_{10}]$

h) Use your function `ModuleDim(...)` to compute the dimension of the graded modules over $\mathbb{Q}[x, y, z]$ represented by the following homogeneous matrices.

1) $\mathcal{M}_1 = \begin{pmatrix} 0 & yz & 0 \\ xy & y^2 & 0 \\ xz & 0 & z^2 \end{pmatrix}$

2) $\mathcal{M}_2 = \begin{pmatrix} x^2 + xy & y^3 & 0 & xyz \\ y + z & xz + z^2 & x + y & xy + yz \end{pmatrix}$

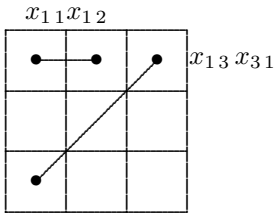
Tutorial 71: Chess Puzzles

The mathematics of chess does not, it is true,
solve the problem of comprehending the contests of life,
but it sets that problem in precise terms,
and points to a solution.
(Emanuel Lasker)

A famous chess puzzle asks in how many ways eight queens can be placed on a chessboard so that no two of them attack one another. We shall solve this question for n queens on a board of size $n \times n$, the classical case corresponding to $n = 8$. We encode an $n \times n$ board as a ring with as many indeterminates as there are squares on the board:

$x_{1\,1}$	$x_{1\,2}$	$x_{1\,3}$
$x_{2\,1}$	$x_{2\,2}$	$x_{2\,3}$
$x_{3\,1}$	$x_{3\,2}$	$x_{3\,3}$

Next we associate to any queen move the product of indeterminates corresponding to the two squares:



Finally, we encode all possible moves of a queen on such a board in an ideal which is generated by those products of indeterminates.

a) Write a CoCoA function `IsMove`(...) which takes two squares (i.e. two indeterminates) and checks whether a queen is allowed to move from the first square to the second.
Hint: You may assume that the base ring is $\mathbb{Z}/(2)[x_{1\,1}, x_{1\,2}, \ldots, x_{n\,n}]$.

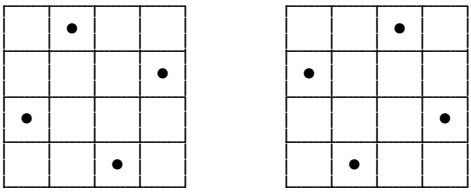
b) Write a CoCoA function `QueenIdeal`(...) which computes the ideal corresponding to all possible queen moves on an $n \times n$ board.

c) Now let $P = \mathbb{Z}/(2)[x_{1\,1}, x_{1\,2}, \ldots, x_{n\,n}]$ for some $n \geq 3$, and let $I \subseteq P$ be the *queen ideal* defined in b). Prove that the dimension of the ring P/I is the maximum number of queens you can place on an $n \times n$ board such that no one attacks another.
Hint: Show that the minimal primes of the queen ideal are precisely the *solution ideals*, i.e. the ideals generated by those indeterminates corresponding to all squares except those occupied by queens in a solution.

d) Prove that the multiplicity of the ring P/I is the number of different ways in which you can place those queens.
Hints: Show that the queen ideal is reduced. Then prove by induction on s that the intersection of s solution ideals has multiplicity s.

e) Write a CoCoA function `Puzzle`(...) which computes the numbers of queens and solutions defined in c) and d) for $n = 3, 4, \ldots$ up to a specified number. Compute the number of solutions for $n = 3, \ldots, 8$.

f) Check your result for $n = 4$ by proving directly that there are only the following two solutions:

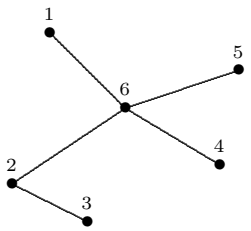


g) If you are adventurous, you may also want to write a CoCoA function `OneByOne`(...) which determines the solutions of our puzzle in the following way:

1) Find all ways to place a queen in the top row.
2) For each of those, find all ways in which one can place a queen in the second row such that it does not attack the first one.
3) Continue in this way, filling the rows one by one. (There is never more than one queen in a row!)
4) Finally, return the list of all solutions to the puzzle.

Can you develop a recursive algorithm?

In the last part of this tutorial we examine a generalization of these ideas from the queen ideal to *graph ideals*. Instead of dealing with the most general case, we shall content ourselves with explaining the method by an example. Consider the graph Γ given by the following picture.



To each vertex i we associate an indeterminate x_i. Then we form the ring $P = K[x_1, \ldots, x_6]$ over a field K. The ideal $I = (x_1x_6, x_2x_3, x_2x_6, x_4x_6, x_5x_6)$ is called the **graph ideal** of Γ. It is generated by the products of the indeterminates corresponding to the edges of Γ. Furthermore, we introduce the standard graded K-algebra $R = P/I$.

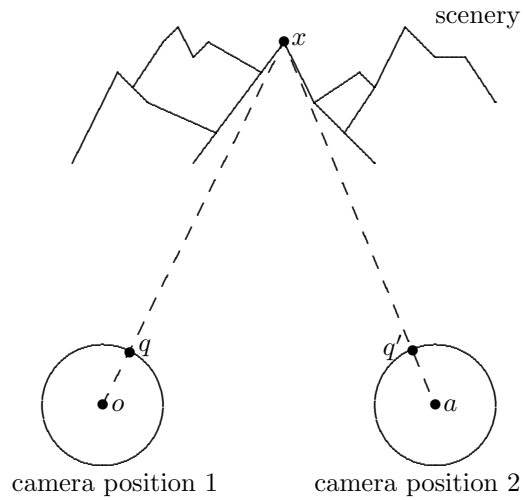
h) Prove that the minimal primes of I are the ideals $\mathfrak{p}_1 = (x_1, x_2, x_4, x_5)$, $\mathfrak{p}_2 = (x_2, x_6)$, and $\mathfrak{p}_3 = (x_3, x_6)$.
i) Show that we have $I = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3$.
j) A **totally disconnected subgraph** of Γ is a subgraph such that no two vertices are connected by an edge. Prove that Γ has exactly three maximal disconnected subgraphs, and that they correspond to the sets of indeterminates outside $\mathfrak{p}_1$, $\mathfrak{p}_2$, and $\mathfrak{p}_3$.
k) Show that $\dim(R)$ is the maximal number of vertices in a totally disconnected subgraph of Γ.
l) Prove that the number of maximal disconnected subgraphs of Γ having $\dim(R)$ vertices is equal to $\mathrm{mult}(R)$.
m) Using CoCoA, show that R satisfies $\dim(R) = 4$ and $\mathrm{mult}(R) = 2$.

A counterattack is never premature.
(Saviely Tartakower)

Tutorial 72: Photogrammetry

Mathematicians are like Frenchmen:
whatever you say to them
they translate into their own language
and forthwith it is something entirely different.
(Johann Wolfgang von Goethe)

Photogrammetry is the theory of reconstructing a 3-D-scene from image motion, i.e. from two or more images of the same object taken from different camera positions. Typical applications include evaluation of satellite images, surveying, and camera calibration. It differs from the related subject of computer vision in that it is typically not time critical and we do not have to deal with a continuous stream of incoming images or motion vectors. Let us consider the following photogrammetric setup.



To describe our goals, we translate this setting into the language of mathematics and hope that it does not become something entirely different.

A **camera position** is a tuple $c_1 = (o, e_1, e_2, e_3)$ such that $o \in \mathbb{R}^3$ and $\{e_1, e_2, e_3\}$ is an orthonormal basis of $\mathbb{R}^3$. We can think of o as the center of the camera and $\{e_1, e_2, e_3\}$ gives us the local coordinate system. In the following we shall assume that we are given two camera positions $c_1 = (o, e_1, e_2, e_3)$ and $c_2 = (a, e_1', e_2', e_3')$ and we shall choose our coordinate system such that $o = (0, 0, 0)$ and $\{e_1, e_2, e_3\}$ is the canonical basis of $\mathbb{R}^3$.

The affine map $\delta : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ such that $\delta(o) = a$ and $\delta(o + e_i) = a + e_i'$ for $i = 1, 2, 3$ is called the **camera displacement**. Using our assumptions, we have $\delta(x) = \mathcal{R}^{\mathrm{tr}}\, x + a$ for all $x \in \mathbb{R}^3$, and we can identify the camera displacement with the pair $(\mathcal{R}, a)$, where $a \in \mathbb{R}^3$ and $\mathcal{R}^{\mathrm{tr}} = (e_1', e_2', e_3')$ is an orthonormal matrix in $\mathrm{Mat}_3(\mathbb{R})$.

The image points inside the camera body will be considered as points on the sphere of radius one around the camera center. The **camera map** corresponding to camera position c_1 is the map $\varphi : \mathbb{R}^3 \setminus \{0\} \longrightarrow S$ given by $x \mapsto x/\|x\|$, where S is the sphere $\{x \in \mathbb{R}^3 \mid \|x\| = 1\}$. Similarly, the camera map corresponding to c_2 is the map $\psi : \mathbb{R}^3 \setminus \{a\} \longrightarrow S'$ given by $x \mapsto (x-a)/\|x-a\|$, where S' is the sphere $\{x \in \mathbb{R}^3 \mid \|x-a\| = 1\}$.

Now we fix a camera displacement. A pair of points $(q, q') \in S \times S'$ is called a **corresponding pair** if there exists a point $x \in \mathbb{R}^3$ such that $q = \varphi(x)$ and $q' = \psi(x)$, i.e. if q and q' are the two images of the same point in $\mathbb{R}^3$ taken from the two camera positions. In this case we write $q \leftrightarrow q'$.

a) For every corresponding pair $q \leftrightarrow q'$ such that $q = \varphi(x)$ and $q' = \psi(x)$ for some $x \in \mathbb{R}^3 \setminus \{o, a\}$, show that we have $\|x-a\| \cdot q' = \mathcal{R}\,(\|x\| \cdot q - a)$.

Given a set of corresponding pairs $Q = \{q_i \leftrightarrow q_i' \mid i = 1, \ldots, n\}$, we say that a camera displacement $(\mathcal{R}, a)$ is a **reconstruction** compatible with Q if there exist points $x_1, \ldots, x_n \in \mathbb{R}^3$ such that $\|x_i - a\|\, q_i' = \mathcal{R}\,(\|x_i\|\, q_i - a)$ for $i = 1, \ldots, n$. The basic photogrammetric problems we shall address in this tutorial are the following:

1) How many corresponding pairs $q_i \leftrightarrow q_i'$ are required in general to reconstruct the camera displacement $(\mathcal{R}, a)$, and therefore the scene, up to a finite number of possibilities?
2) How many different possibilities will there remain in general?

In practice, after we have reduced the compatible reconstructions to a finite number of possibilities, we can resort to other means (such as overlaps, coverings, or shadows) to distinguish between the different cases. The following two ambiguities are innate in the chosen setup.

b) Let $q \leftrightarrow q'$ be a corresponding pair, and let $\lambda \in \mathbb{R}_+$. Show that $q \leftrightarrow q'$ is also a corresponding pair for the camera displacement $(\mathcal{R}, \lambda\, a)$. This phenomenon is called **scaling ambiguity**.

c) Let $q \leftrightarrow q'$ be a corresponding pair, and let $\mathcal{S}$ be the matrix of the 180^o rotation about the axis $\overline{oa}$. Show that $q \leftrightarrow q'$ is also a corresponding pair for the camera displacement $(\mathcal{R}\mathcal{S}, a)$. (*Hint:* Use b) to assume $\|a\| = 1$.) This phenomenon is called the **twisted pair ambiguity**.

d) Let $(q, q') \in S \times S'$, and let $(\mathcal{R}, a)$ be a camera displacement. Prove that the following conditions are equivalent.

   1) There exist $\alpha, \beta \in \mathbb{R}$ such that $\beta q' = \mathcal{R}(\alpha q - a)$.
   2) We have $\langle (\mathcal{R}q \times \mathcal{R}a), q' \rangle = 0$.

   Here $(x_1, x_2, x_3) \times (y_1, y_2, y_3) = (x_2y_3 - x_3y_2,\, x_3y_1 - x_1y_3,\, x_1y_2 - x_2y_1)$ denotes the **vector product** or **cross product** in $\mathbb{R}^3$ and $\langle (x_1, x_2, x_3), (y_1, y_2, y_3) \rangle = x_1y_1 + x_2y_2 + x_3y_3$ is the **standard scalar product** or **inner product**.
   Hint: To show "2)$\Rightarrow$1)", consider the cases $q' \times \mathcal{R}q = 0$ and $q' \times \mathcal{R}q \neq 0$.

Given vectors $a = (a_1, a_2, a_3)$ and $b = (b_1, b_2, b_3)$ in $\mathbb{R}^3$, we define the **associated antisymmetric matrix** $\mathcal{T}_a = \begin{pmatrix} 0 & a_3 & -a_2 \\ -a_3 & 0 & a_1 \\ a_2 & -a_1 & 0 \end{pmatrix}$ of a and the **Kronecker product** $a \otimes b = \begin{pmatrix} a_1 b_1 & a_1 b_2 & a_1 b_3 \\ a_2 b_1 & a_2 b_2 & a_2 b_3 \\ a_3 b_1 & a_3 b_2 & a_3 b_3 \end{pmatrix}$ of a and b.

e) For all $a, b \in \mathbb{R}^3$, prove the following equations.
   1) $\mathcal{T}_a \cdot b = b \times a$
   2) $(a \otimes a) \cdot \mathcal{T}_a = 0$
   3) $\langle a, b \rangle\, a = (a \otimes a) \cdot b$
   4) $\mathcal{R}b \times \mathcal{R}a = \mathcal{R} \cdot (b \times a) = \mathcal{R}\,\mathcal{T}_a \cdot b$

f) Given a camera displacement $(\mathcal{R}, a)$, let $\mathcal{E} = \mathcal{R}\,\mathcal{T}_a$. Conclude that a pair $(q, q') \in S \times S'$ satisfies $\langle \mathcal{E}q, q' \rangle = 0$ if and only if $(q')^{\mathrm{tr}} \mathcal{E}\, q = 0$, and that these equations hold true if $q \leftrightarrow q'$.

A matrix $\mathcal{E} \in \mathrm{Mat}_3(\mathbb{R})$ is called an **essential matrix** if it is of the form $\mathcal{E} = \mathcal{R}\mathcal{T}_a$ for some orthonormal matrix $\mathcal{R} \in \mathrm{Mat}_3(\mathbb{R})$ and some $a \in \mathbb{R}^3$. In the following we let $Q = \{q_i \leftrightarrow q_i' \mid i = 1, \ldots, n\}$ be a set of corresponding pairs.

g) Show that there is a reconstruction compatible with Q if and only if there exists an essential matrix $\mathcal{E} \in \mathrm{Mat}_3(\mathbb{R})$ such that $(q_i')^{\mathrm{tr}} \mathcal{E}\, q_i = 0$ for $i = 1, \ldots, n$.

h) Let $\mathcal{E} = \mathcal{R}\mathcal{T}_a$ be an essential matrix, and let $\mathcal{S} \in \mathrm{Mat}_3(\mathbb{R})$ be the matrix corresponding to the 180^o rotation about the axis $\overline{oa}$. Show that $\mathcal{E} = -\mathcal{R}\mathcal{S}\mathcal{T}_a$ and that every reconstruction $(\mathcal{R}', a')$ having $\mathcal{E} = \mathcal{R}'\mathcal{T}_{a'}$ is either $(\mathcal{R}, a)$ or $(\mathcal{R}\mathcal{S}, -a)$. Conclude that the twisted pair ambiguity corresponds to the substitution $\mathcal{E} \mapsto -\mathcal{E}$.

i) Show that the scaling ambiguity corresponds to a substitution $\mathcal{E} \mapsto \lambda\mathcal{E}$ with $\lambda \in \mathbb{R}_+$.

In the light of these results we shall say that two reconstructions $(\mathcal{R}, a)$ and $(\mathcal{R}', b)$ which are both compatible with Q are **essentially different** if the matrices $\mathcal{R}\mathcal{T}_a$ and $\mathcal{R}'\mathcal{T}_b$ are $\mathbb{R}$-linearly independent. Our next goal is to study the set of all essential matrices more closely. In particular, we want to characterize essential matrices by a finite number of polynomial equations which their entries have to satisfy.

j) Let $\mathcal{E} \in \mathrm{Mat}_3(\mathbb{R})$ be an essential matrix, let $\mathcal{U}, \mathcal{V} \in \mathrm{Mat}_3(\mathbb{R})$ be orthonormal matrices, and let $\lambda \in \mathbb{R}$. Prove that $\lambda\mathcal{E}$, $\mathcal{U}\mathcal{E}\mathcal{V}$, and $\mathcal{E}^{\mathrm{tr}}$ are essential matrices.

k) Let $\mathcal{E} = \mathcal{R}\mathcal{T}_a$ be an essential matrix, and let $b = \mathcal{R}\,a$. Then show that we have $\mathcal{E} = \mathcal{T}_b\mathcal{R}$.

l) For an essential matrix $\mathcal{E} \in \mathrm{Mat}_3(\mathbb{R})$, prove the **characteristic equation**

$$\mathcal{E}\,\mathcal{E}^{\mathrm{tr}}\,\mathcal{E} = \tfrac{1}{2}\,\mathrm{Trace}(\mathcal{E}\,\mathcal{E}^{\mathrm{tr}})\,\mathcal{E}$$

Hint: First write $\mathcal{E} = \mathcal{T}_b\mathcal{R}$ and show that it suffices to prove $\mathcal{T}_b\mathcal{T}_b^{\mathrm{tr}}\mathcal{T}_b = \frac{1}{2}\mathrm{Trace}(\mathcal{T}_b\mathcal{T}_b^{\mathrm{tr}})\mathcal{T}_b$. Then show that $\mathcal{T}_b\mathcal{T}_b^{\mathrm{tr}} = \langle b, b\rangle\mathcal{I}_3 - b \otimes b$.

m) Show that every matrix $\mathcal{E} \in \mathrm{Mat}_3(\mathbb{R})$ which satisfies the characteristic equation has determinant zero.

n) Let $\mathcal{E}$ be a matrix of size 3×3 of rank two having real or complex entries and row vectors z_1, z_2, z_3. Show that if $\mathcal{E}$ satisfies the characteristic equation, then there exists an index $i \in \{1, 2, 3\}$ such that $\langle z_i, z_i\rangle \neq 0$.

o) Now prove that, for a matrix $\mathcal{E} \in \mathrm{Mat}_3(\mathbb{R})$, the following conditions are equivalent:

   1) The matrix $\mathcal{E}$ is an essential matrix.
   2) We have $\mathrm{rk}(\mathcal{E}) = 2$ and $\mathcal{E}$ satisfies the characteristic equation.

   Hint: To prove "2)⇒1)", show that we may assume $(0, 0, 1) \cdot \mathcal{E} = 0$. Then use n) to show that we may assume that the second row of $\mathcal{E}$ is $(0, 1, 0)$. Finally use the characteristic equation to show $\mathcal{E} = (\pm e_1, e_2, 0)$ and decompose this matrix.

p) Let $\mathcal{E} \in \mathrm{Mat}_3(\mathbb{Q})$. Write a CoCoA function `IsEssential(...)` which takes $\mathcal{E}$, uses o) to check whether $\mathcal{E}$ is an essential matrix, and returns the corresponding Boolean value.

q) Let $\mathcal{E} \in \mathrm{Mat}_3(\mathbb{Q})$ be an essential matrix. Write a CoCoA function `Decompose(...)` which computes all possible decompositions $\mathcal{E} = \mathcal{R}\mathcal{T}_a$ where $\mathcal{R} \in \mathrm{Mat}_3(\mathbb{R})$ is an orthonormal matrix and $a \in \mathbb{R}^3$.
   Hint: Consider the entries of $\mathcal{R}$ and a as indeterminates and solve the corresponding polynomial system of equations.

r) Conclude that there exists a reconstruction which is compatible with Q if and only if there exists a matrix $\mathcal{E} \in \mathrm{Mat}_3(\mathbb{R})$ such that the following equations hold true:

   1) $(q_i')^{\mathrm{tr}}\,\mathcal{E}\,q_i = 0$ for $i = 1, \ldots, n$
   2) $\mathcal{E}\mathcal{E}^{\mathrm{tr}}\mathcal{E} = \frac{1}{2}\mathrm{Trace}(\mathcal{E}\mathcal{E}^{\mathrm{tr}})\mathcal{E}$
   3) $\mathrm{rk}(\mathcal{E}) = 2$

For the remaining parts of this tutorial we assume that you have some knowledge of projective spaces and varieties (see Tutorials 35, 46, and 52). We associate a matrix $\mathcal{E} = (z_{ij}) \in \mathrm{Mat}_3(\mathbb{R})$ to the point $p(\mathcal{E}) = (z_{11} : z_{12} : \ldots : z_{33})$ in $\mathbb{P}^8_{\mathbb{R}}$. The set $E = \{p(\mathcal{E}) \in \mathbb{P}^8_{\mathbb{R}} \mid \mathcal{E} \text{ essential matrix}\}$ is called the **essential set** in $\mathbb{P}^8_{\mathbb{R}}$, and the projective variety

$$V = \{(z_{11} : \ldots : z_{33}) \in \mathbb{P}^8_{\mathbb{R}} \mid \mathcal{E} = (z_{ij}) \text{ satisfies the characteristic equation}\}$$

is called the **essential variety** in $\mathbb{P}^8_{\mathbb{R}}$.

s) Write a CoCoA function `EssentialIdeal(...)` which computes the ideal $I_V \subseteq \mathbb{Q}[z_{11}, \ldots, z_{33}]$ defining the essential variety. Then use CoCoA to examine whether the following claims hold true.

   1) The ideal I_V is a homogeneous radical ideal, i.e. it is the homogeneous vanishing ideal of V.

2) The ideal I_V is a prime ideal, i.e. the essential variety is an irreducible projective variety.
3) We have $\dim(V) = 5$ and $\deg(V) = 10$. (*Hint:* Compute the Hilbert polynomial of $\mathbb{Q}[z_{11}, \ldots, z_{33}]/I_V$.)
4) If we intersect V with a randomly chosen linear space $L \subseteq \mathbb{P}^8_{\mathbb{R}}$ of dimension three, we get 10 points of intersection.

t) Show that every matrix of rank one in V is the limit of a sequence of essential matrices. Conclude that V is the projective closure of E.

u) Write a CoCoA function `Reconstruct(...)` which takes a set of corresponding pairs $Q = \{q_i \leftrightarrow q'_i \mid i = 1, \ldots, n\}$ and performs the following steps:

1) Find the equations of the hyperplanes in $\mathbb{P}^8_{\mathbb{R}}$ defined by $(q'_i)^{\mathrm{tr}}\, \mathcal{E}\, q_i = 0$ for $i = 1, \ldots, n$.
2) Intersect V with those hyperplanes.
3) Check whether there are finitely many reconstructions compatible with Q. If this is not the case, return an error message.
4) For every essential matrix in the intersection, compute the corresponding reconstructions using your function `Decompose(...)`.

v) Apply your function `Reconstruct(...)` to the set of five corresponding pairs $Q = \{q_1 \leftrightarrow q'_1, \ldots, q_5 \leftrightarrow q'_5\}$ given by $q_1 = q'_1 = (1, 0, 0)$, $q_2 = q'_2 = (0, 1, 0)$, $q_3 = q'_3 = (0, 0, 1)$, $q_4 = q'_5 = (1, 1, 1)$, and $q_5 = q'_4 = (3, 7, 2)$. Show that there exists a 1-dimensional family of reconstructions compatible with these five corresponding pairs.

w) Apply your function `Reconstruct(...)` to a set of five corresponding pairs $Q = \{q_1 \leftrightarrow q'_1, \ldots, q_5 \leftrightarrow q'_5\}$ obtained by a small perturbation of the pairs in v). Show that there are exactly 10 reconstructions compatible with the perturbed pairs.

x) Finally, conclude that in general one needs at least five corresponding pairs in order to reduce the compatible reconstructions to a finite set of possibilities, and in general this set consists of 10 possibilities which then have to be distinguished by further corresponding pairs or other means.

5.5 Bounds for Hilbert Functions

This proof of the theorem [...]
is given only to place it on record.
It is too long and complicated
to provide any but the most tedious reading.
(F.S. Macaulay)

Mathematics follows the path of maximal irony.
(Mark Green)

At first sight, this section may appear to provide any but the most tedious reading. In fact, already the name "section" is a misnomer according to one of our readers who suggested we call it a "chapter" instead. What is the purpose of going to all this trouble? An astute reader may have observed that, despite the great care taken to describe the properties of Hilbert functions, we still do not know how to characterize them. In other words, given an integer function of polynomial type, how can we know whether it is the Hilbert function of a standard graded K-algebra? Are there any constraints which prevent a given integer function from being a Hilbert function?

Before answering these questions, let us digress for a moment. Is there a good reason to believe that the graph of a Hilbert function exhibits any degree of predictability? Not so long ago, in the roaring nineties, many people were full of *irrational exuberance* and believed they could predict the future behaviour of any graph: stock prices, company profits, economic growth, and budget surpluses were forecast into the distant future. Since mathematicians have proved time and again that many of those graphs represent random walks, it is clear that the efforts of astrologers, fortune tellers, stock market gurus, and technical analysts are mostly in vain. The best we can say is that a high growth rate cannot last for very long, because the earth's resources are limited. The only resource of unlimited supply is paper money which, according to Voltaire, eventually returns to its intrinsic value.

What does this mean for Hilbert functions? Do they have a higher degree of predictability or are they random walks, too? Almost a century ago, F.S. Macaulay found the hidden rule governing the growth of Hilbert functions. But although his result had a reasonably nice formulation, his proof was complicated and tedious. Many decades later, Mark Green followed the path of maximal irony and gave an elegant, short proof of another growth theorem which implies Macaulay's result. So, at the end of this development, the precise formulation of Macaulay's condition and the proof of the basic properties of the functions he used are easily the most intricate parts of the story.

Amazingly, the path which takes us to these results does not begin with gradings, homogeneous ideals, or Gröbner bases. Instead, it begins with the representation of integers in different bases. Since childhood we have been used to representing integers using the decimal system, i.e. in terms of the powers $1, 10, 100, \ldots$. Later on, when learning about computers and pro-

gramming, we get to know the binary and hexadecimal representations. But what we do here is utterly strange: we use the binomial coefficients $\binom{n(i)}{i}, \binom{n(i-1)}{i-1}, \ldots$ to represent n, where $n(i)$, $n(i-1), \ldots$ are chosen maximally. This is called the *binomial representation* of n in base i and its basic properties are explored in the first subsection.

Where is the path connecting those number games to ideal theory? We reveal it in the second subsection by introducing new ideals lying on the border between ideal theory and combinatorics. They are called Lex-segment ideals and, as their name suggests, their homogeneous components are generated in each degree by the largest terms with respect to the lexicographic term ordering. Homogeneous vector spaces having this property are called Lex-segment spaces. Their main feature is that they generate another Lex-segment space in the next degree, and the dimension and codimension of that vector space can be computed from the binomial representation of the dimension of the original vector space (see Proposition 5.5.16). At this point the path of maximal irony takes another turn. If we reduce a Lex-segment space modulo x_n, the dimension and codimension of the resulting residue class vector space are again functions of the binomial representation of the dimension of the space we started with (see Proposition 5.5.18). Thus we have discovered the true meaning of the numerology of binomial representations: they control the growth rate of Lex-segment ideals and their reductions modulo x_n.

What is still lacking is the connection between the growth of Lex-segment ideals and arbitrary ideals. Thus the third subsection starts with one of the most controversial definitions in commutative algebra and algebraic geometry, the notion of genericity. Since we know that this topic can easily turn from being Pandora's box into a can of worms, we tread carefully along this stretch of our path, give a very precise definition, and prove the properties we need in full detail. From there we can proceed with rapid strides and establish Green's Reduction Theorem 5.5.25 with a bold double induction argument. This theorem gives a bound for the codimension of the generic linear reduction of a vector space generated by forms of a given degree by the corresponding number for the Lex-segment space of the same dimension and degree. As a consequence, we obtain a short proof of Macaulay's Growth Theorem 5.5.27 which bounds the codimension of the vector space generated in the next degree. As in Green's theorem, the bound is given by the corresponding number for a Lex-segment space. Thus we have now discovered the true meaning of Lex-segment spaces and Lex-segment ideals: they are the ones which exhibit the extremal growth rate and extremal generic linear reductions.

Finally, we arrive at our destination. After numerous ironic twists and turns, we give a numerical characterization of Hilbert functions among all integer functions (see Theorem 5.5.32). Are we satisfied with this result? Is it time to rest on our laurels? Mathematicians are never satisfied! Using the concept of a Lex-segment ideal associated to a given ideal, we prove that

the growth rate of any ideal equals the growth rate of the corresponding `Lex`-segment ideal in large degrees. Based on this result, we ask you to find another representation of the Hilbert polynomial (see Exercise 11) and to recreate some modern research results which bound the number of generators and the size of the reduced Gröbner basis of a homogeneous ideal in terms of the associated `Lex`-segment ideal. Are you still craving for more? Well, maybe you are ready to do your own research. But remember not to stray from the path of maximal irony!

5.5.A Binomial Representations

The binomial expansion.
Please enter your username and password
to gain access to this resource.
(from "examstutor.com")

Our journey begins with a result which shows how we can represent positive integers via a suitable sum of binomial coefficients. We shall not charge you for this representation, although it is an essential first step on our path to prove Green's Reduction Theorem 5.5.25 and Macaulay's Growth Theorem 5.5.27. The set of positive integers $\{1, 2, 3, \ldots\}$ will be denoted by $\mathbb{N}_+$.

Proposition 5.5.1. *Let $n, i \in \mathbb{N}_+$. The number n has a unique representation of the form*

$$n = \tbinom{n(i)}{i} + \tbinom{n(i-1)}{i-1} + \cdots + \tbinom{n(j)}{j}$$

such that $1 \leq j \leq i$ and such that $n(i), \ldots, n(j) \in \mathbb{N}$ are natural numbers which satisfy $n(i) > n(i-1) > \cdots > n(j) \geq j$.

Proof. Let us use induction on i. For $i = 1$, the representation $n = \binom{n}{1}$ satisfies all requirements, and it is clearly unique.

Now let $i > 1$. There is a unique number $n(i) \in \mathbb{N}$ with the property that $\binom{n(i)}{i} \leq n < \binom{n(i)+1}{i}$. Let $m = n - \binom{n(i)}{i}$. By the induction hypothesis, the number m has a unique representation of the form $m = \binom{n(i-1)}{i-1} + \cdots + \binom{n(j)}{j}$ such that $1 \leq j \leq i-1$, and $n(i-1) > \cdots > n(j) \geq j$. Using the relations $n < \binom{n(i)+1}{i} = \binom{n(i)}{i} + \binom{n(i)}{i-1}$, we see that $m = n - \binom{n(i)}{i} < \binom{n(i)}{i-1}$, and therefore we get the inequality $n(i-1) < n(i)$. Altogether, we see that the representation $n = \binom{n(i)}{i} + \cdots + \binom{n(j)}{j}$ has the desired properties.

It remains to prove uniqueness. Given a representation of the prescribed form, we have the inequality $n(i-k) \leq n(i) - k$ for $k = 1, \ldots, i-j$, and hence it follows from Lemma 5.1.6.d that

$$\tbinom{n(i-1)}{i-1} + \cdots + \tbinom{n(j)}{j} \leq \tbinom{n(i)-1}{i-1} + \tbinom{n(i)-2}{i-2} + \cdots + \tbinom{n(i)-i+1}{1} = \tbinom{n(i)}{i-1} - 1$$

Therefore we have $\binom{n(i)}{i} \leq n < \binom{n(i)}{i} + \binom{n(i)}{i-1} = \binom{n(i)+1}{i}$. This shows that $n(i)$ is uniquely determined by n, and the claim follows inductively. □

The representations provided by this proposition play a central role in this section. Therefore we introduce the following notation.

Definition 5.5.2. Let $n, i \in \mathbb{N}_+$.

a) The representation $n = \binom{n(i)}{i} + \cdots + \binom{n(j)}{j}$ with the property that $1 \leq j \leq i$ and $n(i) > n(i-1) > \cdots > n(j) \geq j$ is called the **binomial representation** of n **in base** i, or the i^{th} **Macaulay representation** of n. We shall also denote it by $n_{[i]}$.

b) The i-tuple $(n(i), \ldots, n(j), 0, \ldots, 0)$ is called the **top binomial representation** of n **in base** i and is denoted by $\operatorname{Top}_i(n)$. We also let $\operatorname{Top}_i(0) = (0, \ldots, 0)$.

Notice that $n(j)$ is really a function which also depends on i, so this notation is slightly imprecise. But it is easy to read, and should not lead to any confusion. The uniqueness of binomial representations also implies that every natural number has a unique top representation in base i. With the purpose of getting accustomed to binomial and top representations, let us compute a few.

Example 5.5.3. The binomial representation of 102 in base 5 satisfies $102_{[5]} = \binom{8}{5} + 46_{[4]}$, since $\binom{8}{5} = 56 \leq 102 < 126 = \binom{9}{5}$. Similarly, $\binom{7}{4} = 35 \leq 46 < 70 = \binom{8}{4}$ yields $46_{[4]} = \binom{7}{4} + 11_{[3]}$. Continuing this way, we finally get $102_{[5]} = \binom{8}{5} + \binom{7}{4} + \binom{5}{3} + \binom{2}{2}$ and thus $\operatorname{Top}_5(102) = (8, 7, 5, 2, 0)$. Similarly, we have $13984_{[10]} = \binom{16}{10} + \binom{15}{9} + \binom{12}{8} + \binom{11}{7} + \binom{9}{6} + \binom{8}{5} + \binom{5}{4} + \binom{3}{3}$ and $\operatorname{Top}_{11}(13984) = (16, 15, 12, 11, 9, 8, 5, 3, 0, 0)$.

Top binomial representations have the nice property that one can compare two numbers in the usual way, i.e. by looking at one "digit" at a time.

Proposition 5.5.4. *Let $m, n \in \mathbb{N}$ and $i \in \mathbb{N}_+$. The following conditions are equivalent.*

a) We have $n > m$.

b) We have $\operatorname{Top}_i(n) >_{\mathtt{Lex}} \operatorname{Top}_i(m)$.

Proof. First we show that a) implies b). Let $\operatorname{Top}_i(n) = (n_i, n_{i-1}, \ldots, n_1)$ and $\operatorname{Top}_i(m) = (m_i, m_{i-1}, \ldots, m_1)$. Suppose there exists an index $\ell \in \{1, \ldots, i\}$ such that $m_k = n_k$ for $k = \ell+1, \ldots, i$ and $m_\ell \neq n_\ell$. By possibly subtracting the same number from m and n, we may assume that $\ell = i$. Thus we now have $n > m$ and $m_i \neq n_i$. Now $\binom{n_i+1}{i} > n > m \geq \binom{m_i}{i}$ implies $n_i \geq m_i$. Together with $m_i \neq n_i$, we get the desired conclusion that $n_i > m_i$.

In order to prove that b) implies a), we may again assume that the two tuples are different in the first place, i.e. we may assume that $n_i > m_i$. We deduce that $n \geq \binom{n_i}{i} \geq \binom{m_i+1}{i} > m$. □

The following operations on binomial representations will be useful for studying the growth of Hilbert functions. Further operations and rules are

given in Tutorial 73. To read the following expressions correctly, remember that by definition we have the equality $\binom{0}{0} = 1$.

Definition 5.5.5. Let $n, i \in \mathbb{N}_+$ and consider the binomial representation $n_{[i]} = \binom{n(i)}{i} + \cdots + \binom{n(j)}{j}$ of n in base i.

a) We let $(n_{[i]})^+ = \binom{n(i)+1}{i} + \cdots + \binom{n(j)+1}{j}$.
b) We let $(n_{[i]})^- = \binom{n(i)-1}{i} + \cdots + \binom{n(j)-1}{j}$.
c) We let $(n_{[i]})^+_+ = \binom{n(i)+1}{i+1} + \cdots + \binom{n(j)+1}{j+1}$.
d) We let $(n_{[i]})^-_- = \binom{n(i)-1}{i-1} + \cdots + \binom{n(j)-1}{j-1}$.

Moreover, we let $(0_{[i]})^+ = 0$, $(0_{[i]})^- = 0$, $(0_{[i]})^+_+ = 0$, and $(0_{[i]})^-_- = 0$.

Clearly, the expressions given for $(n_{[i]})^+$ and $(n_{[i]})^+_+$ are already the binomial representations of those numbers in base i and $i+1$, respectively. The following example shows that this is not necessarily true for $(n_{[i]})^-$ and $(n_{[i]})^-_-$.

Example 5.5.6. The binomial representation of the number 4 in base 2 is $4_{[2]} = \binom{3}{2} + \binom{1}{1}$. Therefore we have $(4_{[2]})^- = \binom{2}{2} + \binom{0}{1} = 1$, but $1_{[2]} = \binom{2}{2}$. Similarly, we have $(4_{[2]})^-_- = \binom{2}{1} + \binom{0}{0} = 3$, but $3_{[1]} = \binom{3}{1}$.

Some rules for the above operations follow easily from the definition.

Remark 5.5.7. Let $n, i \in \mathbb{N}_+$.

a) We have $n = ((n_{[i]})^+)^- = ((n_{[i]})^+_+)^-_-$.
b) Using Lemma 5.1.6.b, we see that we have $n = (n_{[i]})^- + (n_{[i]})^-_-$.

Our next two propositions describe some features of the functions introduced in Definition 5.5.5. More specific results are investigated in Tutorial 73.

Proposition 5.5.8. *Let $n, i \in \mathbb{N}_+$, let $\mathrm{Top}_i(n) = (n_i, \ldots, n_1)$, and let $j = \min\{k \mid n_k \neq 0\}$.*

a) We have $\mathrm{Top}_i((n_{[i]})^+) = (n_i + 1, \ldots, n_j + 1, 0, \ldots, 0)$. Consequently, the map $n \mapsto (n_{[i]})^+$ is increasing.
b) We have $\mathrm{Top}_{i+1}((n_{[i]})^+_+) = (n_i + 1, \ldots, n_j + 1, 0, \ldots, 0, 0)$. Consequently, the map $n \mapsto (n_{[i]})^+_+$ is increasing.
c) If $n_1 > 1$, let $\ell = 1$. Otherwise, let $\ell = 1 + \max\{k \mid n_k \leq k\}$. We have $\mathrm{Top}_i((n_{[i]})^-) = (n_i - 1, \ldots, n_\ell - 1, 0, \ldots, 0)$. Consequently, the map $n \mapsto (n_{[i]})^-$ is non-decreasing.

Proof. The three formulas follow from the definitions of the three operations. The additional claims are then a consequence of Proposition 5.5.4. □

It is not true that the map $n \mapsto (n_{[i]})^-$ is increasing, as the following example shows.

Example 5.5.9. Let $i > 1$. Then we have $1_{[i]} = \binom{i}{i}$ and $2_{[i]} = \binom{i}{i} + \binom{i-1}{i-1}$, and therefore $(1_{[i]})^- = (2_{[i]})^- = 0$.

The following result will be used in the proof of Macaulay's Growth Theorem 5.5.27.

Proposition 5.5.10. *Let $n, i \in \mathbb{N}_+$, $i > 1$. Then we have the inequality $(((n_{[i]})^-_-)_{[i-1]})^+_+ \geq n$.*

Proof. Let $n_{[i]} = \binom{n(i)}{i} + \cdots + \binom{n(j)}{j}$ be the binomial expansion of n in base i. If $j > 1$, the binomial representation of $(n_{[i]})^-_-$ in base $i-1$ is $(n_{[i]})^-_- = \binom{n(i)-1}{i-1} + \cdots + \binom{n(j)-1}{j-1}$, and it is clear that $(((n_{[i]})^-_-)_{[i-1]})^+_+ = n$. Otherwise, when $j = 1$, we have $(n_{[i]})^-_- = \binom{n(i)-1}{i-1} + \cdots + \binom{n(2)-1}{1} + 1$. Let us denote $(n_{[i]})^-_-$ by m, and let $\mathrm{Top}_{i-1}(m) = (m_{i-1}, \ldots, m_1)$. By Proposition 5.5.4, we see that $\mathrm{Top}_{i-1}(m) >_{\mathtt{Lex}} (n(i) - 1, \ldots, n(2) - 1)$, and hence

$$(m_{i-1} + 1, \ldots, m_1 + 1, 0) >_{\mathtt{Lex}} (n(i), \ldots, n(2), 0)$$

Let $\ell \in \{1, \ldots, i-1\}$ be such that $m_k = 0$ for $k = 1, \ldots, \ell - 1$ and such that $m_k = m(k) > 0$ for $k = \ell, \ldots, i-1$. Since the numbers $n(2), \ldots, n(i)$ are positive, the above inequality implies that there is an index $s \in \{\ell, \ldots, i-1\}$ with $m_s = m(s) > n(s+1)$. Hence we get the inequality $\mathrm{Top}_i((((n_{[i]})^-_-)_{[i-1]})^+_+) \geq_{\mathtt{Lex}} \mathrm{Top}_i(n)$. Using Proposition 5.5.4 once again yields the claimed inequality. □

The last result of this subsection can be viewed as the combinatorial part of Green's Reduction Theorem 5.5.25.

Theorem 5.5.11. *Let $m > n > 0$ and $i > 1$.*

a) We have $(n_{[i]})^+ \leq m$ if and only if $n \leq (m_{[i]})^-$.
b) The conditions in a) are satisfied if $n \leq (n_{[i]})^- + ((m-n)_{[i-1]})^-$.

Proof. First we prove a). The implication "⇒" follows by applying the operator $(\ldots)^-$ to both sides of the inequality. To show "⇐", we note that Proposition 5.5.8.c implies that $((m_{[i]})^-)^+ \leq m$. Therefore it suffices to apply the operator $(\ldots)^+$ to both sides of the inequality.

Now we prove b). Let $n = \binom{n(i)}{i} + \cdots + \binom{n(j)}{j}$ be the binomial expansion of n in base i. It suffices to show that we have $N \leq m - n$ for the number $N = \binom{n(i)}{i-1} + \cdots + \binom{n(j)}{j-1}$. Then we can use Lemma 5.1.6.b to deduce that $(n_{[i]})^+ = N + n \leq m$. We distinguish two cases.

If $j > 1$, the sum $\binom{n(i)}{i-1} + \cdots + \binom{n(j)}{j-1}$ is the binomial representation of N in base $i-1$. Therefore we have $(N_{[i-1]})^- = \binom{n(i)-1}{i-1} + \cdots + \binom{n(j)-1}{j-1}$. By the hypothesis and Lemma 5.1.6.b, we see that $(N_{[i-1]})^- \leq ((m-n)_{[i-1]})^-$. Since $n(j) > j - 1$, we have $((N_{[i-1]})^-)^+ = N$. Thus we can apply the operator

$(\dots)^+$ to the above inequality and use Proposition 5.5.8.c to conclude that $N \leq (((m-n)_{[i-1]})^-)^+ \leq m-n$.

Otherwise, when $j = 1$, the sum $\binom{n(i)}{i-1} + \cdots + \binom{n(2)}{1}$ is the binomial representation of $N-1$ in base $i-1$. Therefore we have the relation $((N-1)_{[i-1]})^- = \binom{n(i)-1}{i-1} + \cdots + \binom{n(2)-1}{1}$. By Lemma 5.1.6.b, we see that $((N-1)_{[i-1]})^- = n - (n_{[i]})^- - 1$, and thus the hypothesis yields $((N-1)_{[i-1]})^- < ((m-n)_{[i-1]})^-$. Since the operator $(\dots)^-$ is non-decreasing by Proposition 5.5.8.c, it follows that $N-1 < m-n$, and therefore $N \leq m-n$. This finishes the proof. □

5.5.B Lex-Segment Spaces and Ideals

In this subsection, we let K be a field and $P = K[x_1, \dots, x_n]$ a polynomial ring over K in $n \geq 1$ indeterminates. We equip P with the standard grading. Our goal is to study certain special vector subspaces V of P_d for which $P_1 \cdot V$ will turn out to be as small as possible. They can be described as follows.

Definition 5.5.12. Let $d \in \mathbb{N}$, and let $t \in \mathbb{T}^n$ be a term of degree d.

a) A set of terms of the form $\{t' \in \mathbb{T}^n \mid \deg(t') = d,\ t' \geq_{\mathtt{Lex}} t\}$ is called a **Lex-segment**. The empty set is also considered a Lex-segment.
b) A K-vector subspace V of P_d is called a **Lex-segment space** if $V \cap \mathbb{T}^n$ is both a K-basis of V and a Lex-segment. In this case we denote the K-basis $V \cap \mathbb{T}^n$ by $\mathbb{T}(V)$.

For instance, if $n = 3$ and $d = 2$ then $V = Kx_1^2 + Kx_1x_2 + Kx_1x_3 + Kx_2^2$ is the Lex-segment space generated by the Lex-segment of terms t' of degree 2 such that $t' \geq_{\mathtt{Lex}} t = x_2^2$. For $n = 1$, the only non-zero Lex-segment space in degree d is P_d. Given a non-zero Lex-segment space $V \subset P_d$, we can find explicit formulas for $\dim_K(V)$ and $\operatorname{codim}_K(V)$.

Proposition 5.5.13. (Basic Properties of Lex-Segment Spaces) *Let $n \geq 2$, let $d \in \mathbb{N}$, let $V \subset P_d$ be a non-zero* Lex*-segment space, and let t be the lexicographically biggest term of degree d which is not in $\mathbb{T}(V)$. We write $t = x_1^{\alpha_1} \cdots x_r^{\alpha_r} x_{r+1}^{\alpha_{r+1}}$ where $r \in \{1, \dots, n-1\}$ and $\alpha_{r+1} > 0$, and we let $d_i = d - \sum_{j=1}^{i} \alpha_j$ for $i = 1, \dots, r$.*

a) The K-vector space V is the d^{th} homogeneous component of the ideal

$$x_1^{\alpha_1+1} \cdot (x_1, \dots, x_n)^{d_1-1} + x_1^{\alpha_1} x_2^{\alpha_2+1} \cdot (x_2, \dots, x_n)^{d_2-1} + \cdots + x_1^{\alpha_1} \cdots x_{r-1}^{\alpha_{r-1}} x_r^{\alpha_r+1} \cdot (x_r, \dots, x_n)^{d_r-1}$$

Conversely, the d^{th} homogeneous component of this ideal is the Lex*-segment space such that the biggest term of degree d which is not contained in it is $x_1^{\alpha_1} \cdots x_r^{\alpha_r} x_{r+1}^{\alpha_{r+1}}$.*

b) The binomial representation of $\dim_K(V)$ *in base* $n-1$ *is given by*

$$\dim_K(V) = \tbinom{n-1+d_1-1}{n-1} + \tbinom{n-2+d_2-1}{n-2} + \cdots + \tbinom{n-r+d_r-1}{n-r}$$

c) The binomial representation of $\operatorname{codim}_K(V)$ *in base* d *is given by*

$$\begin{aligned}\operatorname{codim}_K(V) &= \left(\tbinom{n-1+d-1}{d} + \tbinom{n-1+d-2}{d-1} + \cdots + \tbinom{n-1+d_1}{d_1+1}\right)\\ &+ \left(\tbinom{n-2+d_1-1}{d_1} + \tbinom{n-2+d_1-2}{d_1-1} + \cdots + \tbinom{n-2+d_2}{d_2+1}\right)\\ &+ \cdots + \left(\tbinom{n-r+d_{r-1}-1}{d_{r-1}} + \cdots + \tbinom{n-r+d_r-1}{d_r}\right)\end{aligned}$$

Proof. Let I be the monomial ideal in a). Our first goal is to show that $V \subseteq I_d$, so let $t' = x_1^{\beta_1}\cdots x_n^{\beta_n} \in \mathbb{T}(V)$. Since $t' >_{\texttt{Lex}} t$, we can define i to be the minimal index such that $\beta_i > \alpha_i$. By definition of t, we have $i \leq r$. Therefore the term t' is of the form $t' = x_1^{\alpha_1}\cdots x_{i-1}^{\alpha_{i-1}} x_i^{\alpha_i+1}\, t''$ with $t'' \in \mathbb{T}(x_i,\ldots,x_n)$, and hence it is contained in I_d. The other inclusion follows from the observation that every term of degree d in one of the summands of I is clearly Lex-bigger than t.

Now we prove b). The homogeneous component of degree d of the ideal I is given by the formula $I_d = \sum_{i=1}^{r} x_1^{\alpha_1}\cdots x_{i-1}^{\alpha_{i-1}} x_i^{\alpha_i+1} \cdot K[x_i,\ldots,x_n]_{d_i-1}$. By looking at the exponents of $x_1,\ldots,x_i$, we see that this is a direct sum of K-vector spaces. Hence the desired formula follows from the equality $\dim_K(K[x_i,\ldots,x_n]_{d_i-1}) = \binom{n-i+d_i-1}{n-i}$. It is the binomial representation of $\dim_K(V)$ in base $n-1$ because we have the inequalities $n-1+d_1-1 > n-2+d_2-1 > \cdots > n-r+d_r-1 \geq n-r \geq 1$.

Finally, we show c). Using b) and Lemma 5.1.6 we calculate

$$\begin{aligned}\operatorname{codim}_K(V) &= \tbinom{n+d-1}{d} - \sum_{i=1}^{r}\tbinom{n-i+d_i-1}{n-i}\\ &= \tbinom{n+d-1}{d} - \tbinom{n-1+d_1-1}{n-1} - \sum_{i=2}^{r}\tbinom{n-i+d_i-1}{n-i}\\ &= \tbinom{n+d-1}{d} - \tbinom{n-1+d_1-1}{d_1-1} - \sum_{i=2}^{r}\tbinom{n-i+d_i-1}{n-i}\\ &= \left(\tbinom{n-1+d-1}{d} + \cdots + \tbinom{n-1+d_1-1}{d_1}\right) - \sum_{i=2}^{r}\tbinom{n-i+d_i-1}{n-i}\\ &= \left(\tbinom{n-1+d-1}{d} + \cdots + \tbinom{n-1+d_1}{d_1+1}\right) + \tbinom{n-1+d_1-1}{d_1} - \sum_{i=2}^{r}\tbinom{n-i+d_i-1}{n-i}\\ &= \left(\tbinom{n-1+d-1}{d} + \cdots + \tbinom{n-1+d_1}{d_1+1}\right) + \tbinom{n-1+d_1-1}{d_1} - \sum_{i=1}^{r-1}\tbinom{n-1-i+d_{i+1}-1}{n-1-i}\end{aligned}$$

The second part of the last formula has the same shape as the formula we started with, except that n has been replaced by $n-1$ and d by d_1. So, after performing several similar calculations, we end up with the desired result. The

fact that this result is the binomial representation of $\operatorname{codim}_K(V)$ in base d follows from the inequalities $n-1+d-1 > \cdots > n-1+d_1 > n-2+d_1-1 > \cdots > n-r+d_r-1 \geq d_r \geq 1$. □

Let us compute the decomposition of some Lex-segment spaces and evaluate the corresponding dimension and codimension formulas.

Example 5.5.14. Let K be a field and $P = K[x,y,z]$.

a) Let $d = 3$, and let $V \subseteq P_3$ be the Lex-segment space generated by $\{t' \in \mathbb{T}^3 \mid \deg(t') = 3,\ t' \geq_{\mathtt{Lex}} y^2z\}$. The biggest term in the complement is yz^2. It is described by $r = 2$, $\alpha_1 = 0$, $\alpha_2 = 1$. Hence V is the degree 3 component of the ideal $x \cdot (x,y,z)^2 + y^2 \cdot (y,z)^1$, and we have $\dim_K(V) = \binom{4}{2} + \binom{2}{1} = 8$ and $\operatorname{codim}_K(V) = \binom{0}{0} + \left(\binom{3}{3} + \binom{2}{2}\right) = 2$.

b) Let $d = 5$, and let $V \subseteq P_5$ be the Lex-segment space generated by $\{t' \in \mathbb{T}^3 \mid \deg(t') = 5,\ t' \geq_{\mathtt{Lex}} x^3y^2\}$. The biggest term in the complement is x^3yz. Consequently, we have $r = 2$, $\alpha_1 = 3$, and $\alpha_2 = 1$. Therefore V is the degree 5 component of the ideal $x^4 \cdot (x,y,z) + x^3y^2 \cdot (y,z)^0$, and we have $\dim_K(V) = \binom{3}{2} + \binom{1}{1} = 4$ and $\operatorname{codim}_K(V) = \left(\binom{6}{5} + \binom{5}{4} + \binom{4}{3}\right) + \left(\binom{2}{2} + \binom{1}{1}\right) = 17$.

c) Let $d = 6$, and let $V \subseteq P_6$ be the Lex-segment space generated by $\{t' \in \mathbb{T}^3 \mid \deg(t') = 6,\ t' \geq_{\mathtt{Lex}} x^5z\}$. The biggest term in the complement is x^4y^2. Hence we have $r = 1$ and $\alpha_1 = 4$. Therefore V is the degree 6 component of the ideal $x^5 \cdot (x,y,z)$, and we have $\dim_K(V) = \binom{3}{2} = 3$ and $\operatorname{codim}_K(V) = \left(\binom{7}{6} + \binom{6}{5} + \binom{5}{4} + \binom{4}{3} + \binom{3}{2}\right) = 25$.

Example 5.5.15. Let K be a field, let $P = K[x_1,\ldots,x_4]$, let $d = 7$, and let $V \subseteq P_7$ be the Lex-segment space generated by $\{t' \in \mathbb{T}^4 \mid \deg(t') = 7,\ t' \geq_{\mathtt{Lex}} x_1^2x_2^3x_3x_4\}$. The biggest term in the complement is $t = x_1^2x_2^3x_4^2$, and hence $r = 3$, $\alpha_1 = 2$, $\alpha_2 = 3$, and $\alpha_3 = 0$. Therefore V is the degree 7 component of $x_1^3 \cdot (x_1,x_2,x_3,x_4)^4 + x_1^2x_2^4 \cdot (x_2,x_3,x_4)^1 + x_1^2x_2^3x_3 \cdot (x_3,x_4)$, and we have $\dim_K(V) = \binom{7}{3} + \binom{3}{2} + \binom{2}{1} = 40$ and $\operatorname{codim}_K(V) = \left(\binom{9}{7} + \binom{8}{6}\right) + \left(\binom{6}{5} + \binom{5}{4} + \binom{4}{3}\right) + \left(\binom{2}{2}\right) = 80$.

The following proposition shows that we can find explicit expressions for the dimension and codimension of the vector space generated by a Lex-segment space in the next degree.

Proposition 5.5.16. *Let $d \in \mathbb{N}$, let $V \subset P_d$ be a non-zero* Lex*-segment space, and let t be the lexicographically biggest term of degree d which is not in $\mathbb{T}(V)$. We write $t = x_1^{\alpha_1} \cdots x_r^{\alpha_r} x_{r+1}^{\alpha_{r+1}}$ where $r \in \{1,\ldots,n-1\}$ and $\alpha_{r+1} > 0$, and we let $d_i = d - \sum_{j=1}^{i} \alpha_j$ for $i = 1,\ldots,r$.*

a) The K-vector space $P_1 \cdot V$ is the Lex*-segment space in P_{d+1} for which the lexicographically biggest term of degree $d+1$ outside $\mathbb{T}(P_1 \cdot V)$ is $x_1^{\alpha_1} \cdots x_r^{\alpha_r} x_{r+1}^{\alpha_{r+1}+1}$.*

b) We have $\dim_K(P_1 \cdot V) = ((\dim_K(V))_{[n-1]})^+$.

c) We have $\operatorname{codim}_K(P_1 \cdot V) = ((\operatorname{codim}_K(V))_{[d]})^+_+$.

Proof. Using the decomposition of V given in Proposition 5.5.13.a, we see that $P_1 \cdot V$ is the homogeneous component of degree $d+1$ of the ideal

$$x_1^{\alpha_1+1} \cdot (x_1, \ldots, x_n)^{d_1} + x_1^{\alpha_1} x_2^{\alpha_2+1} \cdot (x_2, \ldots, x_n)^{d_2} + \cdots \\ \cdots + x_1^{\alpha_1} \cdots x_{r-1}^{\alpha_{r-1}} x_r^{\alpha_r+1} \cdot (x_r, \ldots, x_n)^{d_r}$$

Now claim a) follows by using Proposition 5.5.13.a the other way around. Moreover, this description of $P_1 \cdot V$ implies b), since we get

$$\dim_K(P_1 \cdot V) = \tbinom{n-1+d_1}{n-1} + \cdots + \tbinom{n-r+d_r}{n-r} = ((\dim_K(V))_{[n-1]})^+$$

Finally, to prove c), we use

$$\operatorname{codim}_K(P_1 \cdot V) = \tbinom{n-1+d+1}{d+1} - \dim_K(P_1 \cdot V) = \tbinom{n-1+d+1}{d+1} - \sum_{i=1}^{r} \tbinom{n-i+d_i}{n-i}$$

and repeat the calculation given in the proof of Proposition 5.5.13.c. The upshot is that all binomial coefficients have their upper and lower entries increased by one, i.e. we obtain the result $((\operatorname{codim}_K(V))_{[d]})^+_+$. □

The last part of this subsection is devoted to determining the properties of reductions of Lex-segment spaces modulo x_n. More generally, we introduce the reduction of V modulo any linear form as follows.

Definition 5.5.17. Let V be a K-vector subspace of P, and let $\ell \in P_1$. Then the image of V in $\overline{P}^{\ell} = P/(\ell)$ is called the **ℓ-reduction** of V, or the **linear reduction** of V modulo ℓ, and is denoted by $\overline{V}^{\ell}$.

For the next proposition, we are only interested in the x_n-reduction of a Lex-segment space. We identify $\overline{P}^{x_n}$ with $K[x_1, \ldots, x_{n-1}]$ and let $\overline{V} = \overline{V}^{x_n}$.

Proposition 5.5.18. *Let $d \in \mathbb{N}$, let $V \subset P_d$ be a non-zero* Lex*-segment space, and let t be the lexicographically biggest term of degree d which is not in $\mathbb{T}(V)$. We write $t = x_1^{\alpha_1} \cdots x_r^{\alpha_r} x_{r+1}^{\alpha_{r+1}}$ where $r \in \{1, \ldots, n-1\}$ and $\alpha_{r+1} > 0$, and we let $d_i = d - \sum_{j=1}^{i} \alpha_j$ for $i = 1, \ldots, r$.*

a) The K-vector space $\overline{V}$ is the Lex*-segment space in $K[x_1, \ldots, x_{n-1}]_d$ for which the* Lex*-biggest term of degree d outside $\mathbb{T}(\overline{V})$ is $x_1^{\alpha_1} \cdots x_r^{\alpha_r} x_{r+1}^{\alpha_{r+1}}$ if $r < n-1$ or $x_1^{\alpha_1} \cdots x_{i-1}^{\alpha_{i-1}} \cdot x_i^{\alpha_i - 1} \cdot x_{n-1}^{\alpha_{n-1}+\alpha_n+1}$ if $r = n-1$ and $i = \max\{j \leq n-2 \mid \alpha_j \geq 1\}$.*

b) We have $\dim_K(\overline{V}) = ((\dim_K(V))_{[n-1]})^-_-$.

c) We have $\operatorname{codim}_K(\overline{V}) = ((\operatorname{codim}_K(V))_{[d]})^-$.

Proof. Using the decomposition of V given in Proposition 5.5.13.a, we see that $\overline{V}$ is the homogeneous component of degree d of the monomial ideal

$\overline{I} = x_1^{\alpha_1+1} \cdot (x_1, \ldots, x_{n-1})^{d_1-1} + \cdots + x_1^{\alpha_1} \cdots x_{r-1}^{\alpha_{r-1}} x_r^{\alpha_r+1} \cdot (x_r, \ldots, x_{n-1})^{d_r-1}$. In order to prove a), we distinguish two cases.

If $r < n-1$ then $\overline{V}$ has the shape described in Proposition 5.5.13.a, and the claim follows. If $r = n-1$ then the last summand of $\overline{I}$ is $x_1^{\alpha_1} \cdots x_{n-2}^{\alpha_{n-2}} \cdot x_{n-1}^{\alpha_{n-1}+\alpha_n}$. Therefore $\overline{V}$ is the Lex-segment space for which the lexicographically biggest term of degree d not contained in $\mathbb{T}(\overline{V})$ is $x_1^{\alpha_1} \cdots x_{i-1}^{\alpha_{i-1}} \cdot x_i^{\alpha_i-1} \cdot x_{n-1}^{\alpha_{n-1}+\alpha_n+1}$ where $i = \max\{j \leq n-2 \mid \alpha_j \geq 1\}$, and the claim follows also in this case. In view of this fact and Proposition 5.5.13.b, we can now compute

$$\dim_K(\overline{V}) = \tbinom{n-2+d_1-1}{n-2} + \cdots + \tbinom{n-r-1+d_r-1}{n-r-1} = ((\dim_K(V))_{[n-1]})^-_-$$

This proves b). Claim c) follows from

$$\operatorname{codim}_K(\overline{V}) = \tbinom{n-2+d}{n-2} - \dim_K(\overline{V}) = \tbinom{n-1+d-1}{d} - \sum_{i=1}^{r} \tbinom{n-1-i+d_i-1}{n-1-i}$$

and the calculation given in the proof of Proposition 5.5.13.c, but replacing n by $n-1$, i.e. where all binomial coefficients have their upper entry decreased by one. □

The formulas for $\dim_K(\overline{V})$ and $\operatorname{codim}_K(\overline{V})$ are also valid for $V = 0$ and $V = P_d$ if we use the conventions $0^- = 0$ and $0^-_- = 0$. But we would like to point out that they do not in general provide us with the binomial representation of $\dim_K(\overline{V})$ in base $n-2$ and of $\operatorname{codim}_K(\overline{V})$ in base d (see Exercise 2).

5.5.C The Theorems of Macaulay and Green

In this subsection we let K be a field, and we let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over K which is equipped with the standard grading. Recall that, given an ideal I of P, the set

$$\mathcal{Z}_K(I) = \{(a_1, \ldots, a_n) \in K^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}$$

is called the set of zeros (or the zero-set) of I in K^n. We can extend the definitions in Tutorial 27 as follows.

Definition 5.5.19. Let S be a subset of K^n.

a) The set S is called **Zariski closed** if there exists an ideal $I \subseteq P$ such that $S = \mathcal{Z}_K(I)$.
b) The set S is called **Zariski open** if there exists an ideal $I \subseteq P$ such that $S = K^n \setminus \mathcal{Z}_K(I)$.
c) Let $\mathcal{P}$ be a property of elements in K^n. We say that $\mathcal{P}$ holds **generically** in K^n, or **for a generic element** of K^n, if there exists a non-empty Zariski open subset U of K^n such that $\mathcal{P}$ holds for all elements of U.

It is easy to see that if K is finite then every subset of K^n is Zariski closed and Zariski open (see Exercise 5). Hence the notion "$\mathcal{P}$ holds for a generic element of K^n" is interesting only if K is infinite. The names "Zariski closed" and "Zariski open" derive their justification from the following fact.

Proposition 5.5.20. *The Zariski closed subsets of K^n are the closed subsets of a topology on K^n. It is called the* **Zariski topology** *on K^n.*

Proof. The empty set and the entire vector space are Zariski closed, because we have $\emptyset = \mathcal{Z}_K((1))$ and $K^n = \mathcal{Z}_K((0))$. Given two Zariski closed subsets $W_1 = \mathcal{Z}_K(I_1)$ and $W_2 = \mathcal{Z}_K(I_2)$, we have $W_1 \cup W_2 = \mathcal{Z}_K(I_1 \cdot I_2)$. Given a family $\{W_\lambda \mid \lambda \in \Lambda\}$ of Zariski closed subsets $W_\lambda = \mathcal{Z}_K(I_\lambda)$, we have $\bigcap_{\lambda\in\Lambda} W_\lambda = \mathcal{Z}_K(\sum_{\lambda\in\Lambda} I_\lambda)$. □

Our next proposition provides us with two basic properties of the Zariski topology.

Proposition 5.5.21. *Let K be an infinite field.*

a) Let $I \subseteq P$ be a non-zero ideal. Then $U = K^n \setminus \mathcal{Z}_K(I)$ has infinitely many elements.

b) Let U_1, U_2 be two non-empty Zariski open subsets of K^n. Then $U_1 \cap U_2$ is non-empty.

Proof. First we prove a). Let $f \in I \setminus \{0\}$. Since we have $\mathcal{Z}_K(I) \subseteq \mathcal{Z}_K(f)$, it suffices to prove the claim for $f \in P \setminus \{0\}$ and $U = K^n \setminus \mathcal{Z}_K(f)$. We use induction on n. For $n = 1$, the polynomial f has at most $\deg(f)$ zeros. Since K is infinite, there are infinitely many points in $K \setminus \mathcal{Z}_K(f)$. Now consider the case $n > 1$. We write $f = f_0 + f_1 x_n + \cdots f_i x_n^i$, where $i \geq 0$ and $f_0, \ldots, f_i \in K[x_1, \ldots, x_{n-1}]$ with $f_i \neq 0$. By the inductive hypothesis, there is a point $(a_1, \ldots, a_{n-1}) \in K^{n-1}$ such that $f_i(a_1, \ldots, a_{n-1}) \neq 0$. Therefore the polynomial $f(a_1, \ldots, a_{n-1}, x_n) \in K[x_n]$ is non-zero. Using the case $n = 1$, we find infinitely many values $a_n \in K$ such that $f(a_1, \ldots, a_n) \neq 0$. Altogether, we have infinitely many points $(a_1, \ldots, a_n)$ in $K^n \setminus \mathcal{Z}_K(f)$.

Next we show b). Let $U_1 = K^n \setminus W_1$ and $U_2 = K^n \setminus W_2$, and let I_1, I_2 be ideals in P such that $W_1 = \mathcal{Z}_K(I_1)$ and $W_2 = \mathcal{Z}_K(I_2)$. Now the claim follows from $W_1 \cup W_2 = \mathcal{Z}_K(I_1 I_2)$ and a). □

The Zariski topology on K^n induces a uniquely determined topology on every n-dimensional K-vector space as follows.

Remark 5.5.22. Let V be a K-vector space of dimension n, and let $\varphi : V \longrightarrow K^n$ be an isomorphism of vector spaces. A subset $U \subseteq V$ is called **Zariski open** if $\varphi(U)$ is a Zariski open subset of K^n. Clearly, this condition does not depend on the choice of the isomorphism φ and we obtain a topology on V which is called the **Zariski topology** on V.

In particular, in this way we can say that a property $\mathcal{P}$ holds for a generic linear form if there exists a Zariski open subset U of P_1 such that the property $\mathcal{P}$ holds for all linear forms in U.

Recall that an isomorphism of K-vector spaces $\varphi : P_1 \longrightarrow P_1$ extends uniquely to an isomorphism of graded K-algebras $\Phi : P \longrightarrow P$ with $\Phi|_{P_1} = \varphi$, and that the map Φ is called a homogeneous linear change of coordinates. In order to better understand the effect of reducing a K-vector subspace $V \subseteq P_d$ modulo a generic linear form, we generalize Proposition 5.5.18 as follows.

Proposition 5.5.23. *Let K be an infinite field, let $d \in \mathbb{N}$, and let $V \subset P_d$ be a* `Lex`*-segment space.*

a) For a generic linear form $\ell \in P_1$, there is a homogeneous linear change of coordinates $\Phi : P \longrightarrow P$ such that $\Phi(V) = V$ and $\Phi(\ell) = x_n$.

b) For a generic linear form $\ell \in P_1$, we have $\dim_K(\overline{V}^{\ell}) = ((\dim_K(V))_{[n-1]})^-_-$ and $\operatorname{codim}_K(\overline{V}^{\ell}) = ((\operatorname{codim}_K(V))_{[d]})^-$.

Proof. To prove claim a), we write $\ell = a_1x_1 + \cdots + a_nx_n$ with $a_1, \ldots, a_n \in K$. Clearly, the subset $U \subset P_1$ of all $\ell \in P_1$ such that $a_n \neq 0$ is Zariski open and not empty. For $\ell \in U$, we define a K-linear map $\varphi : P_1 \longrightarrow P_1$ by setting $\varphi(x_n) = \frac{1}{a_n}(x_n - a_1x_1 - \cdots - a_{n-1}x_{n-1})$ and $\varphi(x_i) = x_i$ for $i = 1, \ldots, n-1$. Then we have $\varphi(\ell) = \sum_{i=1}^{n} a_i\varphi(x_i) = x_n$, and φ is an isomorphism of K-vector spaces. Let $\Phi : P \longrightarrow P$ be the homogeneous linear change of coordinates induced by φ. We have $\Phi(V) \subseteq V$ since for any term $t \in P_d$ the element $\Phi(t)$ is a K-linear combination of terms $t' \geq_{\texttt{Lex}} t$. Moreover, since Φ induces an isomorphism $\Phi|_{P_d} : P_d \longrightarrow P_d$, we have $\dim_K(\Phi(V)) = \dim_K(V)$. Altogether, it follows that $\Phi(V) = V$.

To prove b), we choose $U \subset P_1$ and $\ell \in U$ and $\Phi : P \longrightarrow P$ as in the proof of a). Now, as $\Phi(\ell) = x_n$, we see that Φ induces an isomorphism of graded K-algebras $\overline{\Phi} : P/(\ell) \longrightarrow P/(x_n)$, and $\Phi(V) = V$ implies $\overline{\Phi}(\overline{V}^{\ell}) = \overline{V}^{x_n}$. Thus Proposition 5.5.18 yields $\dim_K(\overline{V}^{\ell}) = \dim_K(\overline{V}^{x_n}) = ((\dim_K(V))_{[n-1]})^-_-$ and $\operatorname{codim}_K(\overline{V}^{\ell}) = \operatorname{codim}_K(\overline{V}^{x_n}) = ((\operatorname{codim}_K(V))_{[d]})^-$. □

Now we are almost ready to prove the first main theorem of this section. We shall avail ourselves of just one more result about generic linear forms.

Lemma 5.5.24. *Let K be an infinite field, let $P = K[x_1, \ldots, x_n]$ be a polynomial ring in $n \geq 2$ indeterminates, let $d \geq 1$, and let $V \subseteq P_d$ be a K-vector subspace.*

a) If $P_{d-1} \cdot \ell \subseteq V$ for a generic linear form $\ell \in P_1$ then $V = P_d$.

b) Let $\mu = \max\{\dim_K(\overline{V}^{m}) \mid m \in P_1 \setminus \{0\}\}$. Then a generic linear form $\ell \in P_1$ satisfies $\dim_K(\overline{V}^{\ell}) = \mu$.

c) Let $\nu = \min\{\operatorname{codim}_K(\overline{V}^{m}) \mid m \in P_1 \setminus \{0\}\}$. Then a generic linear form $\ell \in P_1$ satisfies $\operatorname{codim}_K(\overline{V}^{\ell}) = \nu$.

Proof. First we prove a). Let $U \subseteq P_1$ be a non-empty Zariski open subset such that $P_{d-1} \cdot \ell \subseteq V$ for every linear form $\ell \in U$. It suffices to show that

there exist n linear forms $\ell_1, \ldots, \ell_n$ in U such that $\{\ell_1, \ldots, \ell_n\}$ is a basis of P_1. We construct this basis inductively. Since U is not empty, there exists a linear form $\ell_1 \in U$. Let $i < n$, and let $\{\ell_1, \ldots, \ell_i\}$ be already constructed. Then the set $U' = P_1 \setminus \langle \ell_1, \ldots, \ell_i \rangle_K$ is Zariski open and not empty. Therefore Proposition 5.5.21.b shows that the set $U \cap U'$ is a non-empty Zariski open subset of P_1. Thus there exists a linear form ℓ_{i+1} in $U \cap U'$. Clearly, the elements $\{\ell_1, \ldots, \ell_{i+1}\}$ are K-linearly independent.

Now we prove b). Since we have $\overline{V}^{\ell} = (V + P_{d-1}\ell)/P_{d-1}\ell$, it suffices to show that $\dim_K(V + P_{d-1}\ell)$ is constant and maximal on a non-empty Zariski open subset of P_1. Let $\{v_1, \ldots, v_r\}$ be a K-basis of V and $\{f_1, \ldots, f_s\}$ a K-basis of P_{d-1}. Then the tuple $\mathcal{G} = (v_1, \ldots, v_r, f_1\ell, \ldots, f_s\ell)$ generates the K-vector space $V + P_{d-1}\ell$. We choose a vector space basis $\mathcal{B}$ of P_d and write $\ell = a_1x_1 + \cdots + a_nx_n$ with $a_1, \ldots, a_n \in K$. Then we form the matrix $\mathcal{A}$ whose columns are given by the coordinate tuples of the elements of $\mathcal{G}$ with respect to $\mathcal{B}$. We have $\dim_K(V + P_{d-1}\ell) = \operatorname{rk}(\mathcal{A})$, and this rank is the maximal number i such that not all minors of size i of $\mathcal{A}$ vanish. Those minors are polynomials in $a_1, \ldots, a_n$, and their zero-set is a proper Zariski closed subset of P_1. Hence the maximal rank of $\mathcal{A}$ is attained for a generic linear form.

Finally, to prove c), we observe that the codimension of $\overline{V}^{\ell}$ is given by $\dim_K(P_d/(V + P_{d-1}\ell))$. Therefore the claim follows from b). □

Finally, after all these preparations, we are in a position to prove Mark Green's beautiful formula whose first consequence is that `Lex`-segment spaces have generic linear reductions of minimal dimension.

Theorem 5.5.25. (Green's Reduction Theorem)
Let K be an infinite field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let $d \in \mathbb{N}$, and let $V \subseteq P_d$ be a K-vector subspace. For a generic linear form $\ell \in P_1$, we have

$$\operatorname{codim}_K(\overline{V}^{\ell}) \leq ((\operatorname{codim}_K(V))_{[d]})^{-}$$

Here equality holds if V is a `Lex`*-segment space.*

Proof. Let us denote $\operatorname{codim}_K(V)$ by c. By the lemma, there exists a non-empty Zariski open subset $U_1 \subseteq P_1$ such that $\operatorname{codim}_K(\overline{V}^{\ell})$ attains its minimal value $\overline{c}$ for all $\ell \in U_1$. Thus the inequality to be proved is $\overline{c} \leq (c_{[d]})^{-}$.

If $V = 0$, the claim follows from the equalities $\overline{c} = \dim_K(P/(\ell))_d = \binom{n-2+d}{d} = ((\dim_K(P_d))_{[d]})^{-} = (c_{[d]})^{-}$ which hold for every $\ell \in P_1 \setminus \{0\}$. Furthermore, if $V = P_d$, the claim follows from the simple fact that we have $\overline{c} = 0 = 0^{-} = (c_{[d]})^{-}$. Hence we may assume that V is a non-zero proper vector subspace of P_d.

We proceed by induction on $d + n$. For $d = 0$ or $n = 1$, we have $V = 0$ or $V = P_d$, and the claim has been shown above. If $d = 1$ and $n > 1$, we have $(c_{[1]})^{-} = \binom{c-1}{1} = c - 1$. Since $V \subset P_1$ is Zariski closed, we choose an element $\ell \in P_1 \setminus V$ and get $\dim_K(V \cap K \cdot \ell) = 0$. Consequently, we have $\dim_K(\overline{V}^{\ell}) = \dim_K(V)$ and $\overline{c} = c - 1 = (c_{[1]})^{-}$ as required.

The only remaining case is $d \geq 2$ and $n \geq 2$. For a linear form $\ell \in P_1$, we define $V : \ell = \{f \in P_{d-1} \mid f\,\ell \in V\}$ and observe that the map "multiplication by ℓ" induces an exact sequence of K-vector spaces

$$(1) \qquad 0 \longrightarrow P_{d-1}/(V : \ell) \longrightarrow P_d/V \longrightarrow P_d/(V + P_{d-1} \cdot \ell) \longrightarrow 0$$

Using the isomorphism $P_d/(V + P_{d-1} \cdot \ell) \cong \overline{P}_d^{\ell}/\overline{V}^{\ell}$, we get

$$(2) \qquad \operatorname{codim}_K(V : \ell) = c - \overline{c} \qquad \text{for every } \ell \in U_1$$

Sequence (1) implies that we have $V : \ell = P_{d-1}$ if and only if $P_{d-1} \cdot \ell \subseteq V$. Lemma 5.5.24.a says that if $P_{d-1} \cdot \ell \subseteq V$ for a generic linear form $\ell \in P_1$ then $V = P_d$, a case we have treated above. By Lemma 5.5.24.c, we may therefore assume that there exists a non-empty Zariski open subset $U_2 \subseteq P_1$ such that $\operatorname{codim}_K(V : \ell) > 0$ for all $\ell \in U_2$. Hence equation (2) implies $c > \overline{c}$ for all $\ell \in U_1 \cap U_2$. By Proposition 5.5.21.b, the set $U_1 \cap U_2$ is a non-empty Zariski open subset of P_1.

Now we fix a linear form $L \in U_1 \cap U_2$. Since we have assumed $n \geq 2$, the set $P_1 \setminus K{\cdot}L$ is a non-empty Zariski open subset of P_1. Therefore any linear form ℓ in this set satisfies $K{\cdot}L \cap K{\cdot}\ell = \{0\}$. To simplify the notation, we denote ℓ-reductions by $\overline{P}$, $\overline{V}$, and so on. We have just noted that $\overline{K{\cdot}L} \neq 0$. Multiplication by $\overline{L}$ induces an exact sequence of K-vector spaces

$$0 \longrightarrow \overline{P}_{d-1}/(\overline{V} : \overline{L}) \longrightarrow \overline{P}_d/\overline{V} \longrightarrow \overline{P}_d/(\overline{V} + \overline{P}_{d-1} \cdot \overline{L}) \longrightarrow 0$$

Letting $\widetilde{V}$ be the image of V in $P/(\ell, L)$, this sequence implies that

$$(3) \qquad \operatorname{codim}_K(\widetilde{V}) = \dim_K(\overline{P}_d/(\overline{V} + \overline{P}_{d-1} \cdot \overline{L})) = \overline{c} - \operatorname{codim}_K(\overline{V} : \overline{L})$$

Next we calculate

$$\begin{aligned} \overline{V : L} &= (\{f \in P_{d-1} \mid fL \in V\} + P_{d-2} \cdot \ell)/P_{d-2} \cdot \ell \\ &\subseteq (\{f \in P_{d-1} \mid fL \in V + P_{d-1} \cdot \ell\} + P_{d-2} \cdot \ell)/P_{d-2} \cdot \ell \\ &= \{\overline{f} \in \overline{P}_{d-1} \mid \overline{f}\,\overline{L} \in \overline{V}\} = \overline{V} : \overline{L} \end{aligned}$$

Consequently, we have

$$(4) \qquad \operatorname{codim}_K(\overline{V} : \overline{L}) \leq \operatorname{codim}_K(\overline{V : L})$$

Since $V : L$ is contained in P_{d-1}, we can apply the induction hypothesis to this vector space and obtain

$$(5) \qquad \operatorname{codim}_K(\overline{V : L}) \leq ((\operatorname{codim}_K(V : L))_{[d-1]})^- \qquad \text{for generic } \ell.$$

Moreover, the vector space $\overline{V}^L$ is contained in $\overline{P}_d^L$, and $\overline{P}^L$ is isomorphic to a polynomial ring in $n-1$ indeterminates over K. Therefore we can also apply

the induction hypothesis to the vector space $\overline{V}^L$. Next we observe that $\widetilde{V}$ is the reduction of $\overline{V}^L$ modulo ℓ. So, we obtain

$$\text{(6)} \qquad \operatorname{codim}_K(\widetilde{V}) \leq ((\operatorname{codim}_K(\overline{V}^L))_{[d]})^- = (\overline{c}_{[d]})^- \qquad \text{for generic } \ell\,.$$

By combining all equations and inequalities, we get

$$\begin{array}{rcll} \overline{c} & = & \operatorname{codim}_K(\widetilde{V}) + \operatorname{codim}_K(\overline{V} : \overline{L}) & \text{by (3)} \\ & \leq & (\overline{c}_{[d]})^- + \operatorname{codim}_K(\overline{V} : \overline{L}) & \text{by (6), (4)} \\ & \leq & (\overline{c}_{[d]})^- + ((\operatorname{codim}_K(V : L))_{[d-1]})^- & \text{by (5)} \\ & = & (\overline{c}_{[d]})^- + ((c - \overline{c})_{[d-1]})^- & \text{by (2)} \end{array}$$

Recall that $L \in U_1 \cap U_2$ implies $c > \overline{c}$. Therefore we can apply Theorem 5.5.11.b to get the desired inequality $\overline{c} \leq (c_{[d]})^-$. Finally, we note that Proposition 5.5.23.b shows that we have equality in this formula if V is a `Lex`-segment space. □

In the language of Hilbert functions, Green's Reduction Theorem can be restated as follows.

Corollary 5.5.26. *Let K be an infinite field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let I be a homogeneous ideal in P. For a generic linear form $\ell \in P_1$ and $d \in \mathbb{N}_+$, we have*

$$\operatorname{HF}_{\overline{P}^\ell/\overline{I}^\ell}(d) = \operatorname{HF}_{P/(I+(\ell))}(d) \leq ((\operatorname{HF}_{P/I}(d))_{[d]})^-$$

Here equality holds if I_d is a `Lex`*-segment space.*

Proof. It suffices to observe that $\overline{P}^\ell/\overline{I}^\ell \cong P/(I + (\ell))$ and to apply the theorem to $V = I_d$. □

Using Green's bound for the dimension of the ℓ-reduction of a vector subspace V of P_d, we can now deduce the following bound on the codimension of the vector subspace $P_1 \cdot V$ of P_{d+1}.

Theorem 5.5.27. (Macaulay's Growth Theorem)
Let K be a field, let $d \in \mathbb{N}_+$, and let V be a K-vector subspace of P_d. Then we have

$$\operatorname{codim}_K(P_1 \cdot V) \leq ((\operatorname{codim}_K(V))_{[d]})^+_+$$

Here equality holds if V is a `Lex`*-segment space.*

Proof. Since Hilbert functions do not change under field extensions by Corollary 5.1.20, we may assume that K has infinitely many elements. For every linear form ℓ, the map "multiplication by ℓ" induces an exact sequence of K-vector spaces $P_d/V \longrightarrow P_{d+1}/(P_1 \cdot V) \longrightarrow P_{d+1}/(P_1 \cdot V + P_d \cdot \ell) \longrightarrow 0$. Hence we see that

$$(1) \qquad \begin{aligned} \operatorname{codim}_K(P_1 \cdot V) &\leq \operatorname{codim}_K(V) + \operatorname{codim}_K(P_1 \cdot V + P_d \cdot \ell) \\ &= \operatorname{codim}_K(V) + \operatorname{codim}_K(\overline{P_1 \cdot V}^{\ell}) \end{aligned}$$

Now let ℓ be a generic linear form. We apply Green's Reduction Theorem 5.5.25 and get $\operatorname{codim}_K(\overline{P_1 \cdot V}^{\ell}) \leq ((\operatorname{codim}_K(P_1 \cdot V))_{[d+1]})^-$. Combining this inequality with inequality (1), we obtain

$$(2) \qquad \operatorname{codim}_K(P_1 \cdot V) \leq \operatorname{codim}_K(V) + ((\operatorname{codim}_K(P_1 \cdot V))_{[d+1]})^-$$

Remark 5.5.7.b yields

$$(3) \quad \operatorname{codim}_K(P_1 \cdot V) = ((\operatorname{codim}_K(P_1 \cdot V))_{[d+1]})^- + ((\operatorname{codim}_K(P_1 \cdot V))_{[d+1]})^-_-$$

By (2) and (3), we have $((\operatorname{codim}_K(P_1 \cdot V))_{[d+1]})^-_- \leq \operatorname{codim}_K(V)$. Now we apply Propositions 5.5.8.b and 5.5.10 to obtain

$$\operatorname{codim}_K(P_1 \cdot V) \leq ((((\operatorname{codim}_K(P_1 \cdot V))_{[d+1]})^-_-)_{[d]})^+_+ \leq ((\operatorname{codim}_K(V))_{[d]})^+_+$$

The additional claim follows from Proposition 5.5.16.c. □

Again let us formulate this theorem in the language of Hilbert functions. Notice that this version provides us with a sharp bound on the growth of the Hilbert function of a standard graded K-algebra.

Corollary 5.5.28. *Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let $I \subseteq P$ be a homogeneous ideal, and let $d \in \mathbb{N}_+$. Then we have*

$$\operatorname{HF}_{P/I}(d+1) \leq ((\operatorname{HF}_{P/I}(d))_{[d]})^+_+$$

Here equality holds if I_d is a Lex*-segment space which satisfies $I_{d+1} = P_1 \cdot I_d$.*

Proof. It suffices to note that $P_1 \cdot I_d \subseteq I_{d+1}$ implies $\operatorname{HF}_{P/I}(d+1) = \operatorname{codim}_K(I_{d+1}) \leq \operatorname{codim}_K(P_1 \cdot I_d)$ and to apply the theorem to $V = I_d$. □

Let us demonstrate the power of this corollary with an example.

Example 5.5.29. There is no standard graded K-algebra R for which $\operatorname{HF}_R(1) = 3$ and $\operatorname{HF}_R(2) = 5$ and $\operatorname{HF}_R(3) = 8$. To see why this is true, we suppose that $R = P/I$ is such an algebra, where $P = K[x_1, \ldots, x_n]$ is standard graded and $I \subseteq P$ is a homogeneous ideal. Then the corollary yields $8 = \operatorname{HF}_{P/I}(3) \leq ((\operatorname{HF}_{P/I}(2))_{[2]})^+_+ = (5_{[2]})^+_+ = (\binom{3}{2} + \binom{2}{1})^+_+ = \binom{4}{3} + \binom{3}{2} = 7$, a contradiction.

Definition 5.5.30. An ideal I in P is called a **Lex-segment ideal** if I_d is a Lex-segment space in P_d for every $d \in \mathbb{N}$.

We observe that a Lex-segment ideal is necessarily a monomial ideal. The following lemma provides a necessary and sufficient condition for a collection of Lex-segment spaces to define a Lex-segment ideal.

Lemma 5.5.31. *Let $\{V_d \mid d \in \mathbb{N}\}$ be a collection of vector spaces such that $V_d \subseteq P_d$ for every $d \in \mathbb{N}$, and let $I = \bigoplus_{d\in\mathbb{N}} V_d$. The following conditions are equivalent.*

a) The K-vector space I is an ideal in P.
b) For every $d \in \mathbb{N}$, we have $P_1 \cdot V_d \subseteq V_{d+1}$.

Proof. Since a) clearly implies b), let us prove the reverse implication. According to the definition of a homogeneous ideal in Section 1.7, we need to show that $P_d \cdot V_e \subseteq V_{d+e}$ for all $d, e \in \mathbb{N}$. This follows from the factorization $P_d = P_1 \cdot P_1 \cdots P_1$ and induction on d. □

Finally, we are able to fulfil our promise: we are about to show a characterization for the integer functions which are Hilbert functions of standard graded K-algebras.

Theorem 5.5.32. (Characterization of Hilbert Functions)
Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be an integer function, let $n = f(1)$, and assume that $n > 0$. Then the following conditions are equivalent.

a) The function f satisfies $f(d) = 0$ for $d < 0$, $f(0) = 1$, and

$$0 \leq f(d+1) \leq (f(d)_{[d]})^+_+ \qquad \text{for } d \geq 1.$$

b) There exists a `Lex`*-segment ideal I in the standard graded polynomial ring $P = K[x_1, \ldots, x_n]$ with $I_{\leq 1} = 0$ and $f = \mathrm{HF}_{P/I}$.*
c) There exists a homogeneous ideal I in the standard graded polynomial ring $P = K[x_1, \ldots, x_n]$ with $I_{\leq 1} = 0$ and $f = \mathrm{HF}_{P/I}$.

Proof. First we show that a) implies b). For each $d \geq 0$, let I_d be the `Lex`-segment space in P_d of codimension $f(d)$. Since we have assumed $f(0) = 1$ and $f(1) = n$, we have $I_0 = I_1 = 0$. We want to show that $I = \bigoplus_{d\geq 0} I_d$ is an ideal in P. By the lemma, we need to show $P_1 \cdot I_d \subseteq I_{d+1}$ for all $d \geq 2$. Applying Proposition 5.5.16.a, we see that both vector spaces are `Lex`-segment spaces in P_{d+1}. Hence it suffices to prove $\dim_K(P_1 \cdot I_d) \leq \dim_K I_{d+1}$ for $d \geq 2$. This follows from Macaulay's Growth Theorem 5.5.27 and the hypothesis because together they yield

$$\operatorname{codim}_K(I_{d+1}) = f(d+1) \leq (f(d)_{[d]})^+_+ = (\operatorname{codim}_K(I_d)_{[d]})^+_+ = \operatorname{codim}_K(P_1 \cdot I_d)$$

The implication "b)⇒c)" is clearly true, and "c)⇒a)" follows immediately from Corollary 5.5.28. □

Notice that the `Lex`-segment ideal corresponding to a given Hilbert function is uniquely determined. This motivates the following definition.

Definition 5.5.33. Let $I \subseteq P$ be a homogeneous ideal having $I_{\leq 1} = 0$. Then the uniquely determined `Lex`-segment ideal $J \subseteq P$ with Hilbert function $\mathrm{HF}_{P/J} = \mathrm{HF}_{P/I}$ is called the **`Lex`-segment ideal associated to** I and is denoted by $\mathtt{Lex}(I)$.

Corollary 5.5.34. *Let $I \subseteq P$ be a homogeneous ideal having $I_{\leq 1} = 0$, and let $\delta(I)$ be the maximal degree of a minimal generator of* $\mathtt{Lex}(I)$. *Then we have* $\mathrm{HF}_{P/I}(d+1) = ((\mathrm{HF}_{P/I}(d))_{[d]})^+_+$ *for every* $d \geq \delta$.

Proof. Since $\mathrm{HF}_{P/I} = \mathrm{HF}_{P/\mathtt{Lex}(I)}$, we may assume $I = \mathtt{Lex}(I)$. In this case the claim follows from Corollary 5.5.28. □

Further applications of Lex-segment ideals will be explored in Tutorial 74. A far-reaching generalization of this corollary is **Gotzmann's Persistence Theorem**. It states that if the growth bound for $\mathrm{HF}_{P/I}$ given by Corollary 5.5.28 is achieved in some degree $d > \max\{\beta_{0i}(I) \mid i \in \mathbb{Z}\}$ then it is achieved in all degrees $\geq d$. Gotzmann's Persistence Theorem can be proved using his representation of the Hilbert polynomial (see Exercise 11), but the details exceed the scope of this book.

By persistence even the snail reached Noah's ark.
(Gilbert K. Chesterton)

Exercise 1. Let $a \in \mathbb{N}_+$.

a) Give explicit descriptions of $a_{[a]}$ and $(a+1)_{[a]}$.
b) Now suppose $a > 1$. Give an explicit description of $(a-1)_{[a]}$

Exercise 2. Find a Lex-segment space $V \subset P_d$ for some polynomial ring $P = K[x_1, \ldots, x_n]$ and some $d \in \mathbb{N}$ such that the x_n-reduction $\overline{V}$ of V has the following properties:

1) The formula $\dim_K(\overline{V}) = \binom{n-2+d-\alpha_1-1}{n-2} + \cdots + \binom{n-r-1+d-\alpha_1-\cdots-\alpha_r-1}{n-r-1}$ resulting from Proposition 5.5.18.b is not the binomial representation of $\dim_K(\overline{V})$ in base $n-2$.
2) The formula $\mathrm{codim}_K(\overline{V}) = \binom{n-2+d-1}{d} + \cdots + \binom{n-r-1+d-\alpha_1-\cdots-\alpha_r-1}{d-\alpha_1-\cdots-\alpha_r}$ resulting from Proposition 5.5.18.c is not the binomial representation of $\mathrm{codim}_K(\overline{V})$ in base d.

Exercise 3. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let $d \geq 0$, let $V \subseteq P_d$ be a Lex-segment space, and let $i \in \{1, \ldots, n\}$. Show that the intersection $V_i = V \cap K[x_1, \ldots, x_i]$ is a Lex-segment space. Find the smallest term, the dimension, and the codimension of V_i.

Exercise 4. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let $d \in \mathbb{N}$, let $V \subset P_d$ be the Lex-segment space for which $t = x_1^{\alpha_1} \cdots x_r^{\alpha_r} x_{r+1}^{\alpha_{r+1}}$ with $r < n$ and $\alpha_{r+1} > 0$ is the lexicographically biggest term outside $\mathbb{T}(V)$, and let I be the monomial ideal defined in Proposition 5.5.13.a.

a) Show that $\dim(P/I) = n - \min\{i \geq 1 \mid \alpha_i > 0\}$.
b) Show that $\mathrm{mult}(P/I) = \alpha_j$ where $j = \min\{i \geq 1 \mid \alpha_i > 0\}$.

Exercise 5. Let K be a finite field, let $n > 0$, and let V be an n-dimensional K-vector space. Show that every subset $W \subseteq V$ is Zariski closed.

Exercise 6. Find an example of a proper K-vector subspace $V \subset P_d$ for which we have equality in Green's Reduction Theorem and Macaulay's Growth Theorem, but which is not a `Lex`-segment space.

Exercise 7. Let K be a field and R a standard graded K-algebra.

a) Prove that if $\mathrm{HF}_R(d) \leq 1$ for some $d \geq 1$ then we have $\mathrm{HF}_R(i) \leq 1$ for all $i \geq d$.
b) Suppose that $\mathrm{HF}_R(d) = 2$ for some degree $d \geq 2$. Find all possibilities for $\mathrm{HF}_R(i)$ in degrees $i \geq d$.

Exercise 8. Let K be a field. Suppose that a standard graded K-algebra has one of the following Hilbert functions. (We list the values in degrees ≥ 0.)

a) $1\ 3\ 5\ ?\ 5\ 5\ 5\ \cdots$
b) $1\ 3\ 5\ 5\ ?\ 5\ 5\ \cdots$
c) $1\ 3\ 5\ 5\ 5\ ?\ 5\ \cdots$

Find all possibilities for the missing numbers!

Exercise 9. Let K be a field. Prove that $\frac{1+2z+4z^2}{(1-z)^2}$ cannot be the Hilbert series of a standard graded K-algebra.

Exercise 10. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let $I \subseteq P$ be a non-zero homogeneous ideal. We say that $\mathrm{HF}_{P/I}$ is **unimodal** if there is a degree $d \in \mathbb{N}$ such that

$$\mathrm{HF}_{P/I}(0) \leq \mathrm{HF}_{P/I}(1) \leq \cdots \leq \mathrm{HF}_{P/I}(d) \geq \mathrm{HF}_{P/I}(d+1) \geq \cdots$$

a) Prove that $\mathrm{HF}_{P/I}$ is unimodal for every non-zero ideal $I \subseteq P$ if $n = 2$.
b) Find a homogeneous ideal $I \subset P$ whose Hilbert series is given by $\mathrm{HS}_{P/I}(z) = 1 + 3z + 6z^2 + 5z^3 + 6z^4$.

Exercise 11. In this exercise we ask you to derive a special representation of the Hilbert polynomial which is called the **Gotzmann representation**. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let $I \subseteq P$ be a homogeneous ideal such that $I_{\leq 1} = 0$ and $\dim(P/I) > 0$.

a) Prove that there exist natural numbers s, $a_1, a_2, \ldots, a_s$ such that $a_1 \geq a_2 \geq \cdots \geq a_s \geq 0$ and

$$\mathrm{HP}_{P/I}(t) = \tbinom{t+a_1}{a_1} + \tbinom{t+a_2-1}{a_2} + \cdots + \tbinom{t+a_s-(s-1)}{a_s}$$

b) Show that the representation in a) is uniquely determined.
c) Write a CoCoA function which takes I and computes the Gotzmann representation of the Hilbert polynomial of P/I.
d) In the Gotzmann representation, show that $\dim(P/I) = a_1 + 1$ and that $\mathrm{mult}(P/I)$ is the number of times a_1 appears in $\{a_1, \ldots, a_s\}$.

Tutorial 73: Operations on Binomial Representations

In this tutorial we want to examine very carefully binomial representations and the operations defined on them. We shall see that one can derive many more rules for these operations than the ones given in the first subsection. This allows us to give purely formal proofs of many theorems involving the growth of Hilbert functions and `Lex`-segment ideals.

Let $n, i \in \mathbb{N}_+$, and let $n_{[i]} = \binom{n(i)}{i} + \cdots + \binom{n(j)}{j}$ be the binomial representation of n in base i. In addition to Definition 5.5.5, we define the following two operations:

1) We let $(n_{[i]})_+ = \binom{n(i)}{i+1} + \cdots + \binom{n(j)}{j+1}$.
2) We let $(n_{[i]})_- = \binom{n(i)}{i-1} + \cdots + \binom{n(j)}{j-1}$.

Your first job is to implement binomial representations and their operations in CoCoA.

a) Write two CoCoA functions `BinRep(...)` and `TopBinRep(...)` which take two positive integers n and i and compute the binomial representation of n in base i and the tuple $\mathrm{Top}_i(n)$ (see Definition 5.5.2).
Hint: Look at the proof of Proposition 5.5.1 and Example 5.5.3.
b) Use your function `BinRep(...)` to compute the following binomial representations. Compare your results with the built-in CoCoA command `BinExp(...)`.
   1) $34_{[4]}$
   2) $1000_{[10]}$
   3) $185000_{[10]}$
c) Implement the four operations introduced in Definition 5.5.5 and the two above in CoCoA functions `UpperPlus(...)`, `PlusPlus(...)`, etc. Apply these functions to the examples of b) and compare the results with `BinExp(...)`. (*Hint:* Your functions should return the value of the result of the operation, not its binomial representation.)
d) Using the functions `LowerPlus(...)` and `LowerMinus(...)`, find examples which show that these operations do not preserve binomial representations in general.
e) Show that we always have $(n_{[i]})^+ = n + (n_{[i]})_-$ and $(n_{[i]})^+_+ = n + (n_{[i]})_+$.
f) In the following the numbers $n(2)$ and $n(1)$ denote the last two components of $\mathrm{Top}_i(n)$. Prove the following formulas.
   1) $((n+1)_{[i]})^+_+ = (n_{[i]})^+_+ + n(1) + 1$
   2) $((n+1)_{[i]})^- = \begin{cases} (n_{[i]})^- & \text{if } j > 1, \\ (n_{[i]})^- + 1 & \text{if } j = 1. \end{cases}$
   3) $(((n_{[i]})^-_-)_{[i-1]})^+_+ = \begin{cases} n & \text{if } j > 1, \\ n + n(2) - n(1) & \text{if } j = 1. \end{cases}$
   4) $((n+1)_{[i]})^+ = (n_{[i]})^+ + j$
   5) $((n+1)_{[i]})^-_- = \begin{cases} (n_{[i]})^-_- + 1 & \text{if } j > 1, \\ (n_{[i]})^-_- & \text{if } j = 1. \end{cases}$

6) $((n+1)_{[i]})_- = \begin{cases} (n_{[i]})_- + j - 1 & \text{if } j > 1, \\ (n_{[i]})_- & \text{if } j = 1. \end{cases}$

7) $((n+1)_{[i]})_+ = \begin{cases} (n_{[i]})_+ & \text{if } j > 1, \\ (n_{[i]})_+ + n(1) & \text{if } j = 1. \end{cases}$

Hint: For the proof of 1), consider the case $j = 1$. Let s be the largest number such that $n(k) = n(1)+k-1$ for $1 \leq k \leq s$. Show that $(n+1)_{[i]} = \binom{n(i)}{i} + \cdots + \binom{n(s+1)}{s+1} + \binom{n(1)+s}{s}$ and use it to compute $((n+1)_{[i]})^+_+$. Then show that $(n_{[i]})^+_+ = \binom{n(i)+1}{i+1} + \cdots + \binom{n(s+1)+1}{s+2} + \binom{n(1)+s+1}{s+1} - n(1) - 1$. The proofs of the other formulas follow a similar pattern.

g) Using the same method of proof, show that different compositions of these operations can be evaluated as follows.
   1) $((n_{[i]})^+_+)^- = (n_{[i]})_+ = ((n_{[i]})^-)^+_+ = (n_{[i]})^+_+ - n$
   2) If $i > 1$ then $((n_{[i]})_-)^- = (n_{[i]})^-_-$ and $((n_{[i]})^-_-)^+ = (n_{[i]})_-$.
   3) $((n_{[i]})^-)^+ \leq n = ((n_{[i]})^+)_-$ with equality if and only if $n(j) > j$.

h) Find an example in which we have $((n_{[i]})^-)_- \neq (n_{[i]})^-_-$.

i) Now let m be another positive integer. Prove the following claims.
   1) If $i > 1$ and $(n_{[i]})^-_- \leq (m_{[i-1]})^-$ then we have $(n_{[i]})_- \leq m$.
   2) We have $(n_{[i]})^+ \leq m$ if and only if $n \leq (m_{[i]})^-$.
   3) We have $n \leq (m_{[i]})^+_+$ if and only if $(n_{[i+1]})^-_- \leq m$.

j) Use the preceding claims to give another proof of Theorem 5.5.11.b.

Tutorial 74: Bounds for Minimal Generators

Optimist: "If the economy goes like that any longer, soon we will be begging in the streets."
Pessimist: "I wonder from whom?"
(Anonymous)

One way of interpreting Macaulay's Growth Theorem 5.5.27 is to say that `Lex`-segment ideals are the slowest growing ideals. Therefore, given a Hilbert function H of a standard graded K-algebra, the `Lex`-segment ideal corresponding to H requires the greatest number of minimal generators in each degree among all ideals corresponding to H. This is the basic idea we want to explore further in this tutorial. Unfortunately, it turns out that the bounds on the numbers and the degrees of the minimal generators that we can derive from such a straightforward approach are very pessimistic in general. However, as the example of the `Lex`-segment ideal itself shows, without further information this is the best we can achieve. So, the bounds we derive are useful mainly for theoretical purposes. As far as actual Gröbner basis computations are concerned, it is probably better to follow the optimistic approach: "If this Gröbner basis computation goes up in degree like that any longer, soon we will be running out of memory." (The pessimist's CoCoA command is `Alt+Pause`.)

Let K be a field, and let $P = K[x_1, \ldots, x_n]$ be standard graded. For a homogeneous ideal $I \subseteq P$, we let $\mu(I)$ be its minimal number of homogeneous generators.

a) Let S be a finite subset of $\mathbb{N}$, and let $D = \{d_i \mid i \in S\}$ be a set of natural numbers. Write a CoCoA function `IsRestrHF(...)` which takes S and D and checks whether there exists a standard graded K-algebra R such that $\mathrm{HF}_R(i) = d_i$ for all $i \in S$.
Hint: Use Theorem 5.5.32 and the function `PlusPlus(...)` from the preceding tutorial.

b) Apply your function `IsRestrHF(...)` to check whether a standard graded K-algebra can have the following Hilbert function values.
   1) $\mathrm{HF}_R(1) = 3,\ \mathrm{HF}_R(4) = 16$
   2) $\mathrm{HF}_R(8) = 2,\ \mathrm{HF}_R(9) = 3$
   3) $\mathrm{HF}_R(5) = \mathrm{HF}_R(6) = 3,\ \mathrm{HF}_R(8) = \mathrm{HF}_R(9) = 2$
   4) $\mathrm{HF}_R(i) = (i+1)^2$ for $i = 0, \ldots, 10$.

c) Let $s \geq 0$, let $D = \{d_0, d_1, \ldots, d_s\} \subset \mathbb{N}$, and assume that there exists a standard graded K-algebra R such that $\mathrm{HF}_R(i) = d_i$ for $i = 0, \ldots, s$. Show that there exists a `Lex`-segment ideal $J_D \subseteq P$ such that $\mathrm{HF}_{P/J_D}(i) = d_i$ for $i = 0, \ldots, s$ and $\mathrm{HF}_{P/J_D}(i) = 0$ for $i > s$.

d) Let $J \subseteq P$ be a `Lex`-segment ideal with $J_{\leq 1} = 0$. Show that the 0^{th} graded Betti numbers of J satisfy $\beta_{0d}(J) = (\mathrm{HF}_{P/I}(d)_{[d]})^+_+ - \mathrm{HF}_{P/I}(d+1)$ for every $d \geq 1$.

e) Let $I \subseteq P$ be a homogeneous ideal having $I_{\leq 1} = 0$, and let G be a reduced Gröbner basis of I. Prove the relations

$$\mu(I) \leq \#G \leq \mu(\mathtt{Lex}(I)) = \sum_{d>0} \left((\mathrm{HF}_{P/I}(d)_{[d]})^+_+ - \mathrm{HF}_{P/I}(d+1) \right)$$

Hints: Use that fact that $\#G$ is the minimal number of generators of a leading term ideal of I and compare the growth of this monomial ideal to the growth of $\mathtt{Lex}(I)$.

f) Let $I \subseteq P$ be a homogeneous ideal with $I_{\leq 1} = 0$, and let $p(z) = \mathrm{HN}_{P/I}(z) \in \mathbb{Z}[z]$ be the Hilbert numerator of P/I. Write a CoCoA function `MaxDegRedGB(...)` which takes $p(z)$ and computes a bound for the maximal degree of an element in a reduced Gröbner basis of I. (*Hints:* You may assume Gotzmann's Persistence Theorem. Scour the CoCoA package `HP` for useful commands.)

g) Apply your function `MaxDegRedGB(...)` to the following Hilbert numerators of ideals in $K[x_1, \ldots, x_4]$.
   1) $p_1(z) = z^5 - z^4 - z + 1$
   2) $p_2(z) = z^8 - z^6 + z^5 - z^4 - z^3 - 1$
   3) $p_3(z) = 2z^9 - 7z^8 + 9z^7 - 4z^6 + z^5 - z^4 - z^3 + 1$

Tutorial 75: Gin for the Strongly Stable

VeNoM
Pour $2\frac{1}{2}$ oz *of* gin *into a shaker,*
stir in one tablespoon of CoCoA*,*
mix together and shake.
(from "Favourite Drinks of the Strongly Stable")

Let us take a sip of VeNoM and start meditating a bit about Hilbert functions and leading term ideals from a higher point of view. Right after the definition of Hilbert functions we explained that they are invariants of the ideal or module in question, i.e. that they stay the same under a generic homogeneous linear change of coordinates. But then we used Gröbner bases and leading term ideals to compute Hilbert functions. Alas, the latter objects are anything but invariant under homogeneous linear changes of coordinates. Shouldn't Hilbert functions correspond to some kind of invariant leading term ideal? Given a fixed Hilbert function, there are only finitely many monomial ideals J for which P/J has this Hilbert function. Therefore, at least in characteristic zero, we can hope that generic homogeneous linear changes of coordinates always produce the same leading term ideal. This monomial ideal should be an invariant of the given ideal and should have nice properties. Are we getting a little carried away? Is our meditation turning into levitation? It is time to pin down these high-flying ideas and turn them into concrete mathematics.

Let K be a field, and let $P = K[x_1, \ldots, x_n]$ be standard graded. To every matrix $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_n(K)$ we can associate the K-linear map $\varphi_{\mathcal{A}} : P_1 \longrightarrow P_1$ defined by $\varphi_{\mathcal{A}}(x_j) = \sum_{i=1}^{n} a_{ij} x_i$ for $j = 1, \ldots, n$. The map $\varphi_{\mathcal{A}}$ extends uniquely to a homogeneous K-algebra homomorphism $\Phi_{\mathcal{A}} : P \longrightarrow P$. Recall that the map $\Phi_{\mathcal{A}}$ is called a homogeneous linear change of coordinates if it is bijective.

a) Show that, for a generic matrix $\mathcal{A} \in \mathrm{Mat}_n(K)$, the homomorphism $\Phi_{\mathcal{A}}$ is a homogeneous linear change of coordinates.

In the following we let $\{y_{ij} \mid i, j = 1, \ldots, n\}$ be new indeterminates, we let L be the field $K(y_{11}, y_{12}, \ldots, y_{nn})$, and we let $L[x_1, \ldots, x_n]$ be standard graded. Then the matrix $\mathcal{Y} = (y_{ij}) \in \mathrm{Mat}_n(L)$ defines a homogeneous linear change of coordinates $\Psi_{\mathcal{Y}} : L[x_1, \ldots, x_n] \longrightarrow L[x_1, \ldots, x_n]$. Every specific matrix $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_n(K)$ is obtained by substituting $y_{ij} \mapsto a_{ij}$ in $\mathcal{Y}$. Let $\Psi_{\mathcal{A}} : L[x_1, \ldots, x_n] \longrightarrow L[x_1, \ldots, x_n]$ be the homogeneous L-algebra homomorphism defined by $\mathcal{A}$. Given a homogeneous ideal $I \subseteq P$ and a term ordering σ on $\mathbb{T}^n$, we define the **generic initial ideal** of I with respect to σ by $\mathrm{gin}_\sigma(I) = \mathrm{LT}_\sigma(\Psi_{\mathcal{Y}}(I))$.

b) Write a CoCoA function `TrueGin(...)` which takes I and computes $\mathrm{gin}_\sigma(I)$. Apply your function to the following cases.
   1) $\sigma =$ `DegRevLex`, $I_1 = (x_1^2 + x_1x_2 + x_2^2,\ x_1^3 + x_2^3) \subseteq \mathbb{Q}[x_1, x_2]$
   2) $\sigma =$ `Lex`, $I_2 = (x_1^2,\ x_2^2,\ x_3^2,\ x_1x_2x_3) \subseteq \mathbb{Q}[x_1, x_2, x_3]$

3) $\sigma = \texttt{DegLex}$, $I_3 = (x_1^2 - x_2^2,\, x_2^2 - x_3^2) \subseteq \mathbb{Q}[x_1, x_2, x_3]$

c) Try taking `TrueGin(...)` in larger samples.
(*Hint:* Remember the meaning of `Alt+Pause`.)

d) Let K be an infinite field. Prove that we have $\text{gin}_\sigma(I) = \text{LT}_\sigma(\Psi_\mathcal{A}(I))$ for a generic $\mathcal{A} \in \text{Mat}_n(K)$.

e) Implement a CoCoA function `SubstituteGin(...)` which takes I and computes $\text{LT}_\sigma(\Psi_\mathcal{A}(I))$ for a random choice of $\mathcal{A} \in \text{Mat}_n(K)$.

f) Apply your function `SubstituteGin(...)` repeatedly to the examples in b). Use the results to provide some evidence for the claim that this function computes $\text{gin}_\sigma(I)$ with "high probability".

g) Write a CoCoA function `TripleGin(...)` which uses `SubstituteGin(...)` to compute three ideals $\text{LT}_\sigma(\Psi_\mathcal{A}(I))$ with randomly chosen $\mathcal{A} \in \text{Mat}_n(K)$ and returns the result if they all agree. If not, the function repeats the procedure using three new random matrices $\mathcal{A}$.

h) Apply your function `TripleGin(...)` to compute a probable candidate for $\text{gin}_{\texttt{DegRevLex}}(\ldots)$ of the following ideals.

1) $I_4 = (x_1^{10}, x_2^{10}) \subseteq \mathbb{Q}[x_1, x_2]$
2) $I_5 = (f, g, h) \subseteq \mathbb{Q}[x_1, x_2, x_3]$, where $f, g, h \in \mathbb{Q}[x_1, x_2, x_3]$ are randomly chosen homogeneous polynomials of degree three
3) $I_6 = (x_1^5, \ldots, x_5^5) \subseteq \mathbb{Q}[x_1, \ldots, x_5]$

In the remaining part of this tutorial we study a strong stability property of $\text{gin}_\sigma(I)$. A monomial ideal $J \subseteq P$ is called **strongly stable** if it satisfies the following requirement: for any term $t \in J$ and any indeterminate x_j dividing t, we have $(x_i\, t)/x_j \in J$ for all $1 \leq i < j$. In other words, if we replace an indeterminate in a term $t \in J$ by an indeterminate having a smaller index, the result is still contained in J. A well-known theorem due to A. Galligo implies that if $\text{char}(K) = 0$ then $\text{gin}_\sigma(I)$ is strongly stable for every homogeneous ideal $I \subseteq P$ and every term ordering σ on $\mathbb{T}^n$.

If after these first sips you are still strongly stable, we invite you to work out the following parts of this tutorial.

j) Prove that in positive characteristic there exist homogeneous ideals I for which $\text{gin}_\sigma(I)$ is not strongly stable. (*Hint:* Use $I = (x_1^p, x_2^p)$ where $p = \text{char}(K)$.)

k) Show that `Lex`-segment ideals are strongly stable, but the converse is not true in general.

l) Let $n = 2$. Show that strongly stable ideals are `Lex`-segment ideals. Deduce that the ideal $\text{gin}_\sigma(I)$ is the same for every term ordering σ which satisfies $x_1 \geq_\sigma x_2$.

m) Assume $\text{char}(K) = 0$, let $d_1, d_2 \geq 1$, let $f_i \in K[x_1, x_2]_{d_i}$ for $i = 1, 2$, let $f_3 = \gcd(f_1, f_2)$, and let $I = (f_1, f_2)$.

1) Find the Hilbert function of P/I depending on d_1, d_2, and $d_3 = \deg(f_3)$.

2) Use l) and Galligo's Theorem to determine the two possible generic initial ideals of I.

n) Consider the ideal $I_7 = (x_1^2, x_1x_2 + x_2^2, x_1x_3) \subseteq \mathbb{Q}[x_1, x_2, x_3]$. Show that the ideal $\mathrm{LT}_{\texttt{DegRevLex}}(I_7)$ is strongly stable, but that it differs from $\mathrm{gin}_{\texttt{DegRevLex}}(I_7)$.

o) Find an example of a strongly stable monomial ideal which is neither a `Lex`-segment ideal nor a `DegRevLex`-segment ideal. (First you have to choose a reasonable definition of `DegRevLex`-segment ideals.)

p) Show that the monomial ideal $J = (x_1^3, x_1^2x_2, x_1x_2^2, x_1^2x_3, x_1x_2x_3, x_2^3)$ in $K[x_1, x_2, x_3]$ is strongly stable, but is not a `Lex`-segment ideal.

q) Assume char(K) $\neq 2$. Show that the ideal $I_8 = \big(x_1(x_1{-}x_3)(x_1{-}2x_3), x_1(x_1{-}x_3)x_2, x_1x_2(x_2{-}x_3), x_1(x_1{-}x_3)x_3, x_1x_2x_3, x_2(x_2{-}x_3)(x_2{-}2x_3)\big)$ in $K[x_1, x_2, x_3]$ satisfies $\mathrm{gin}_{\texttt{DegRevLex}}(I_8) = J$.

Did you like this taste of gin? Avoid hangovers. Stay intoxicated.

5.6 Affine Hilbert Functions and Krull Dimension

A mathematician is ...
a device for turning coffee into theorems.
(Paul Erdös)

A mathematician is ...
a blind man in a dark room
looking for a black cat which isn't there.
(Charles Darwin)

Writing this section required a huge amount of coffee. At several junctures we almost thought we were hunting for a ghost. The beginning of this story is innocent enough. So far in this chapter we have restricted our attention to standard graded K-algebras, i.e. to algebras of the form P/I where I is a homogeneous ideal in the standard graded polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K. The reason for this choice is clear: it provides us with a natural setting for studying Hilbert functions, Hilbert series, Hilbert polynomials, and so on. Remembering that in the first volume we were able to prove many theorems for rings of the form P/I with an arbitrary ideal $I \subseteq P$, we develop the desire to generalize Hilbert functions to arbitrary affine K-algebras.

A few cups of coffee later the solution is at hand: instead of speaking of the vector space of homogeneous polynomials in I of degree i, we consider arbitrary polynomials in I of degree $\leq i$. Then we define the *affine Hilbert function* of P/I by $\mathrm{HF}^a_{P/I}(i) = \dim_K(P_{\leq i}/I_{\leq i})$ for all $i \in \mathbb{Z}$. The first subsection is the result of building upon this simple idea. The affine Hilbert function of P/I is equal to the affine Hilbert function of $P/\operatorname{LT}_\sigma(I)$ for any degree compatible term ordering σ, and to the usual Hilbert function of $\overline{P}/I^{\mathrm{hom}}$ where $\overline{P} = K[x_0, \ldots, x_n]$ (see Proposition 5.6.3). This allows us to compute affine Hilbert functions (see Corollary 5.6.4) and it shows that they are integer functions of polynomial type. Thus we can define affine Hilbert series, affine Hilbert polynomials, the affine regularity index, the dimension, and the multiplicity of P/I, and each notion coincides with the corresponding notion for $\overline{P}/I^{\mathrm{hom}}$ (see Proposition 5.6.12).

But something strange occurs when we compare different presentations of the same affine algebra. Whereas the affine Hilbert function and the affine multiplicity depend on the choice of the presentation (as expected, see Tutorial 76), the dimension miraculously always gives the same number. Slightly bemused, we start the coffee percolator and investigate.

The name "dimension" for this invariant provides a first clue. Of course we have an intuitive notion of dimension: a point has dimension zero, a line is 1-dimensional, a plane is 2-dimensional, and the space surrounding us is frequently referred to as 3-dimensional. In algebraic geometry, we can formalize this idea by considering chains of irreducible subvarieties $V_0 \subset V_1 \subset \cdots \subset V_d$ where V_0 is a point, V_1 is a curve, and V_d is the d-dimensional variety under consideration. Here "irreducible" means that a variety should not be the

union of two proper subvarieties, e.g. the union of two points would still be 0-dimensional. Translating this definition back into the language of commutative algebra, we arrive at the concept of *Krull dimension:* a ring R is said to have Krull dimension d if the longest chain of prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_d$ in R has length d.

Now it is clearer what we are looking for. We want to prove that the dimension of an affine algebra defined via the degree of its affine Hilbert polynomial is equal to its Krull dimension. The first steps in this direction are easily taken. Using the results of Section 5.4 and some basic properties of minimal primes in Noetherian rings (see Proposition 5.6.15), we can reduce the task to the case of an integral domain P/I (see Proposition 5.6.32). Then we would like to compute everything modulo a non-zero element and proceed by induction. Indeed, this process necessarily lowers the Krull dimension (see Lemma 5.6.35). But when we try to demonstrate the same behaviour for the degree of the affine Hilbert polynomial, all our previous knowledge proves to be inapplicable and a cloud of darkness descends on us. What can we do?

Aha! We need more coffee and more theorems! Subsection B is filled with results about prime and primary ideals. In particular, it is shown that every ideal in a Noetherian ring has a primary decomposition (see Proposition 5.6.18) and that prime avoidance holds true (see Proposition 5.6.19). Then everything is adapted to the case of standard graded algebras (see Propositions 5.6.21 and 5.6.22). This allows us to introduce a very refined tool: the existence of almost non-zerodivisors in standard graded rings (see Proposition 5.6.26). So equipped, we find what we were looking for: the missing inequality in the proof of Theorem 5.6.36 about the equality of dimensions and Krull dimensions.

Now the cloud has lifted, it has become evident that we were not looking for a black cat which wasn't there. Rather, we have stumbled upon a gorgeous cat (namely primary decomposition) which will greatly enhance our further alchemical endeavors of coffee transformation (see Tutorials 77 and 79).

Coffee (n.), *a person who is coughed upon.*
(Anonymous Dictionary)

5.6.A The Hilbert Function of an Affine Algebra

In this subsection we let K be a field, we let $P = K[x_1, \ldots, x_n]$ be standard graded, and we let I be an ideal in P. Recall that a K-algebra of the form P/I is said to be an affine K-algebra. For such algebras we use the following notation.

Let $i \in \mathbb{Z}$. In Definition 4.5.4.b, we introduced the set $P_{\leq i}$ consisting of all homogeneous polynomials of degree $\leq i$. By $\langle P_{\leq i} \rangle$ we shall denote the K-vector space spanned by those polynomials, i.e. the set of *all* polynomials of degree $\leq i$, including the zero polynomial. The K-vector space $\langle I_{\leq i} \rangle$ is

the vector subspace of $\langle P_{\leq i}\rangle$ which consists of the polynomials of degree $\leq i$ in I. Since $\langle I_{\leq i}\rangle = \langle P_{\leq i}\rangle \cap I$, we can view the vector space $\langle P_{\leq i}\rangle/\langle I_{\leq i}\rangle$ as a vector subspace of P/I. In the following we shall frequently use this identification.

Definition 5.6.1. The map $\mathrm{HF}^a_{P/I} : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $\mathrm{HF}^a_{P/I}(i) = \dim_K(\langle P_{\leq i}\rangle/\langle I_{\leq i}\rangle)$ for $i \in \mathbb{Z}$ is called the **affine Hilbert function** of P/I.

For instance, the affine Hilbert function of $P = K[x]$ is given by $\mathrm{HF}^a_P(i) = \max\{0, i+1\}$ for all $i \in \mathbb{Z}$. The affine Hilbert function is not an invariant of an affine algebra. It depends on the choice of a presentation, as the following example shows.

Example 5.6.2. Consider the affine K-algebra $R = K[x]/(x^3)$. Using this presentation, we have $\mathrm{HF}^a_R(i) = \begin{cases} \min\{i+1, 3\} & \text{for } i \geq 0, \\ 0 & \text{otherwise.} \end{cases}$

But it is easy to see that R is isomorphic to $R' = K[x,y]/(xy, x^2 - y)$. In this case we calculate $\mathrm{HF}^a_{R'}(i) = \begin{cases} 3 & \text{for } i \geq 1, \\ \max\{0, i+1\} & \text{otherwise.} \end{cases}$ These two affine Hilbert functions differ, because they have a different value for $i = 1$.

The task of computing individual values of affine Hilbert functions can be reduced to the same task for ordinary Hilbert functions.

Proposition 5.6.3. (Basic Properties of Affine Hilbert Functions) *Let σ be a degree compatible term ordering on $\mathbb{T}^n$, and let $W = (1\ 1\ \cdots\ 1)$ be the matrix defining the standard grading on P.*

a) For every $i \in \mathbb{Z}$, we have $\mathrm{HF}^a_{P/I}(i) = \sum_{j=0}^{i} \mathrm{HF}_{P/\mathrm{LT}_\sigma(I)}(j)$. In particular, we have $\mathrm{HF}^a_{P/I}(i) = \mathrm{HF}^a_{P/\mathrm{LT}_\sigma(I)}(i)$ for all $i \in \mathbb{Z}$.

b) For every $i \in \mathbb{Z}$, we have $\mathrm{HF}^a_{P/I}(i) = \mathrm{HF}^a_{P/\mathrm{DF}_W(I)}(i)$.

c) Let x_0 be a homogenizing indeterminate, and let $\overline{P} = K[x_0, \ldots, x_n]$ be standard graded. Then we have $\mathrm{HF}^a_{P/I}(i) = \mathrm{HF}_{\overline{P}/I^{\mathrm{hom}}}(i)$ for all $i \in \mathbb{Z}$.

Proof. First we show a). By Macaulay's Basis Theorem 1.5.7, the residue classes of the terms in $B = \mathbb{T}^n \setminus \mathrm{LT}_\sigma\{I\}$ form a K-basis of P/I. We claim that, for every $i \in \mathbb{Z}$, the set $\overline{B}_{\leq i}$ of the residue classes of the terms in $B_{\leq i}$ form a K-basis of $\langle P_{\leq i}\rangle/\langle I_{\leq i}\rangle$.

To show that $\overline{B}_{\leq i}$ is a set of generators, we pick $v \in \langle P_{\leq i}\rangle/\langle I_{\leq i}\rangle$. So, v is the residue class of some polynomial $f \in P$ of the form $f = \sum_{t\in B} c_t\, t$ with $c_t \in K$ and $c_t = 0$ for all but finitely many terms t. Let f be a polynomial with minimal leading term with respect to σ whose residue class is v. Then we have $\deg(f) \leq i$ because if $\deg(f) > i$ and $g \in P_{\leq i}$ has residue class v, then we have $f - g \in I$ and $\mathrm{LT}_\sigma(f-g) = \mathrm{LT}_\sigma(f) \in \mathrm{LT}_\sigma\{I\} \cap B$ yields a contradiction. Hence v is contained in the span of $\overline{B}_{\leq i}$.

To show that the elements of $\overline{B}_{\leq i}$ are K-linearly independent, we assume that $c_1 t_1 + \cdots + c_s t_s \in \langle I_{\leq i}\rangle$ for some $c_1, \ldots, c_s \in K \setminus \{0\}$ and

$t_1, \ldots, t_s \in B_{\leq i}$. Then the relations $\mathrm{LT}_\sigma(c_1 t_1 + \cdots + c_s t_s) \in \{t_1, \ldots, t_s\} \subseteq B_{\leq i}$ and $\mathrm{LT}_\sigma(c_1 t_1 + \cdots + c_s t_s) \in \mathrm{LT}_\sigma(I)$ yield a contradiction.

Altogether, we have shown that $\mathrm{HF}^a_{P/I}(i) = \#B_{\leq i}$. Since Macaulay's Basis Theorem 1.5.7 shows that the residue classes of the terms in B are a K-basis of the ring $P/\mathrm{LT}_\sigma(I)$, and since that ring is graded, we know that the residue classes of the elements of B_j are a K-basis of $P_j/\mathrm{LT}_\sigma(I)_j$ for every $j \in \mathbb{Z}$. Therefore we have $\#B_{\leq i} = \sum_{j=0}^{i} \#B_j = \sum_{j=0}^{i} \dim_K(P_j/\mathrm{LT}_\sigma(I)_j) = \sum_{j=0}^{i} \mathrm{HF}_{P/\mathrm{LT}_\sigma(I)}(j)$ for every $i \in \mathbb{Z}$.

Next we prove b). Let $\{g_1, \ldots, g_s\}$ be a σ-Gröbner basis of I. Then we have $\mathrm{LT}_\sigma(\mathrm{DF}_W(g_i)) = \mathrm{LT}_\sigma(g_i)$ for $i = 1, \ldots, s$, and Proposition 4.2.15 yields

$$\begin{aligned} \mathrm{LT}_\sigma(\mathrm{DF}_W(I)) &= \big(\mathrm{LT}_\sigma(\mathrm{DF}_W(g_1)), \ldots, \mathrm{LT}_\sigma(\mathrm{DF}_W(g_s))\big) \\ &= (\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)) = \mathrm{LT}_\sigma(I) \end{aligned}$$

Hence the claim follows from a). To prove c), we may assume that $i \geq 1$. Let $\alpha : \overline{P}_i \longrightarrow P_{\leq i}$ be defined by $\alpha(F) = F^{\mathrm{deh}}$. Then α is K-linear by Proposition 4.3.2.g, surjective by Proposition 4.3.2.c, and injective by Proposition 4.3.2.h. Since it is clear that $\alpha(I_i^{\mathrm{hom}}) = I_{\leq i}$, the claim follows. □

Part c) of this proposition leads to the following algorithm for computing individual values of affine Hilbert functions.

Corollary 5.6.4. (Computation of Affine Hilbert Function Values) *Let I be a proper ideal in P which is generated by non-zero polynomials $f_1, \ldots, f_s$, and let $i \in \mathbb{Z}$. Consider the following instructions.*

1) *If $i < 0$, return zero and stop.*
2) *Choose a homogenizing indeterminate x_0, form $\overline{P} = K[x_0, \ldots, x_n]$, and compute $I^{\mathrm{hom}} = (f_1^{\mathrm{hom}}, \ldots, f_s^{\mathrm{hom}}) :_{\overline{P}} (x_0)^\infty$.*
3) *Compute $\mathrm{HF}_{\overline{P}/I^{\mathrm{hom}}}(i)$ using Corollary 5.1.19, return the result and stop.*

This is an algorithm which computes $\mathrm{HF}^a_{P/I}(i)$.

Let us apply this algorithm to a concrete case. The following example also shows why the assumption that σ is degree compatible cannot be dispensed with in part a) of the proposition.

Example 5.6.5. Let $P = \mathbb{Q}[x_1, x_2, x_3]$ and $I = (x_1x_2 - x_3,\ x_2x_3 - x_1,\ x_1x_3 - x_2)$. Then we can calculate $\mathrm{HF}^a_{P/I}(4)$ by computing

$$\begin{aligned} I^{\mathrm{hom}} &= (x_1x_2 - x_0x_3, x_2x_3 - x_0x_1, x_1x_3 - x_0x_2) :_{\overline{P}} (x_0)^\infty \\ &= (x_1x_2 - x_0x_3, x_2x_3 - x_0x_1, x_1x_3 - x_0x_2, x_1^2 - x_2^2, x_2^2 - x_3^2, x_3^3 - x_0^2x_3) \end{aligned}$$

and $\mathrm{HF}_{\overline{P}/I^{\mathrm{hom}}}(4) = 5$. Since all generators of I^{hom} have degree ≥ 2, we also see that $\mathrm{HF}^a_{P/I}(1) = 4$. If we choose the term ordering $\sigma = \mathtt{Lex}$, we have $\mathrm{LT}_\sigma(I) = (x_1, x_2^2, x_2x_3^2, x_3^3)$ and $\mathrm{HF}^a_{P/\mathrm{LT}_\sigma(I)}(1) = 3$. Therefore Proposition 5.6.3.a requires a degree compatible term ordering.

Of course, it is more enticing to compute all values of an affine Hilbert function at once. To achieve this goal, we introduce the affine version of Hilbert series.

Definition 5.6.6. The power series $\mathrm{HS}^a_{P/I}(z) = \sum_{i\geq 0} \mathrm{HF}^a_{P/I}(i)\, z^i \in \mathbb{Z}[[z]]$ is called the **affine Hilbert series** of P/I.

The following proposition provides us with two ways of calculating affine Hilbert series, one based on the computation of $\mathrm{LT}_\sigma(I)$, and one based on the computation of I^{hom}.

Proposition 5.6.7. *Let σ be a degree compatible term ordering on $\mathbb{T}^n$, let x_0 be a homogenizing indeterminate, and let $\overline{P} = K[x_0, \ldots, x_n]$.*

a) We have $\mathrm{HS}^a_{P/I}(z) = \frac{\mathrm{HS}_{P/\mathrm{LT}_\sigma(I)}(z)}{(1-z)} = \frac{\mathrm{HN}_{P/\mathrm{LT}_\sigma(I)}(z)}{(1-z)^{n+1}}$.

b) We have $\mathrm{HS}^a_{P/I}(z) = \mathrm{HS}_{\overline{P}/I^{\mathrm{hom}}}(z)$.

Proof. Using Proposition 5.6.3, we calculate

$$\begin{aligned} \mathrm{HS}^a_{P/I}(z) &= \sum_{i\geq 0} \big(\sum_{j=0}^{i} \mathrm{HF}_{P/\mathrm{LT}_\sigma(I)}(j) \big)\, z^i \\ &= \big(\sum_{i\geq 0} \mathrm{HF}_{P/\mathrm{LT}_\sigma(I)}(i)\, z^i \big) \cdot \big(\sum_{j\geq 0} z^j \big) = \tfrac{\mathrm{HS}_{P/\mathrm{LT}_\sigma(I)}(z)}{(1-z)} \end{aligned}$$

and $\mathrm{HS}^a_{P/I}(z) = \sum_{i\geq 0} \mathrm{HF}^a_{P/I}(i)\, z^i = \sum_{i\geq 0} \mathrm{HF}_{\overline{P}/I^{\mathrm{hom}}}(i)\, z^i = \mathrm{HS}_{\overline{P}/I^{\mathrm{hom}}}(z)$. □

For a homogeneous ideal, the affine Hilbert function and the Hilbert function of P/I are related as follows.

Proposition 5.6.8. *Let I be a proper homogeneous ideal in P.*

a) For all $i \in \mathbb{Z}$, we have $\mathrm{HF}^a_{P/I}(i) = \bigoplus_{j=0}^{i} \mathrm{HF}_{P/I}(j)$.

b) We have $\mathrm{HS}^a_{P/I}(z) = \frac{\mathrm{HS}_{P/I}(z)}{1-z}$.

Proof. Claim a) follows from Proposition 5.6.3.a and from the observation that Theorem 5.1.18 implies $\mathrm{HF}_{P/I}(i) = \mathrm{HF}_{P/\mathrm{LT}_\sigma(I)}(i)$ for all $i \in \mathbb{Z}$. To prove b), we use Theorem 4.3.22.a to see that $\overline{P}/(I^{\mathrm{hom}} + (x_0)) \cong P/I$. Since x_0 is a non-zerodivisor for $\overline{P}/I^{\mathrm{hom}}$ by Proposition 4.3.5.e, we have $\mathrm{HS}^a_{P/I}(z) = \mathrm{HS}_{\overline{P}/I^{\mathrm{hom}}}(z) = \frac{\mathrm{HS}_{P/I}(z)}{1-z}$ by Propositions 5.6.7.b and 5.2.16.b. □

Part b) of Proposition 5.6.7 and Theorem 5.2.20 imply that the affine Hilbert series of P/I is of the form $\mathrm{HS}^a_{P/I}(z) = \frac{\mathrm{HN}^a_{P/I}(z)}{(1-z)^{n+1}}$ with a polynomial $\mathrm{HN}^a_{P/I}(z) \in \mathbb{Z}[z]$ which is called the **affine Hilbert numerator** of P/I. We can simplify this fraction by cancelling $1-z$ as often as possible and obtain a representation $\mathrm{HS}^a_{P/I}(z) = \frac{\mathrm{hn}^a_{P/I}(z)}{(1-z)^{d+1}}$ with a polynomial $\mathrm{hn}^a_{P/I}(z) \in \mathbb{Z}[z]$

which satisfies $\mathrm{hn}^a_{P/I}(0) = 1$ and $\mathrm{hn}^a_{P/I}(1) \geq 1$ (see Proposition 5.4.2). The polynomial $\mathrm{hn}^a_{P/I}(z)$ is called the **simplified affine Hilbert numerator** of P/I. Moreover, by part b) of Proposition 5.6.8, we have $0 \leq d \leq n$.

In analogy with Section 5.4.A, we can now define the dimension and the multiplicity of an affine algebra.

Definition 5.6.9. Let I be a proper ideal in P, and let $\mathrm{HS}^a_{P/I}(z) = \frac{\mathrm{hn}^a_{P/I}(z)}{(1-z)^{d+1}}$ be the simplified Hilbert series of P/I.

a) The number $\dim(P/I) = d$ is called the **dimension** of P/I.
b) The number $\mathrm{mult}(P/I) = \mathrm{hn}^a_{P/I}(1)$ is called the **multiplicity** of P/I.

As its name suggests, the dimension of an affine algebra does not depend on the choice of a presentation. This will be shown in Subsection B. The multiplicity of an affine algebra may depend on the presentation as we shall see in Tutorial 76. By Proposition 5.6.8.b, the definitions of the dimension and the multiplicity of P/I agree with the corresponding definitions in Section 5.4 if I is a homogeneous ideal.

Since the affine Hilbert function of P/I equals the usual Hilbert function of $\overline{P}/I^{\mathrm{hom}}$, it is an integer function of polynomial type. The associated integer valued polynomial is, of course, uniquely determined and gets the following name.

Definition 5.6.10. Let I be a proper ideal in P.

a) The uniquely determined integer valued polynomial $\mathrm{HP}^a_{P/I}(t) \in \mathbb{Q}[t]$ such that $\mathrm{HP}^a_{P/I}(i) = \mathrm{HF}^a_{P/I}(i)$ for all $i \gg 0$ is called the **affine Hilbert polynomial** of P/I.
b) The regularity index of $\mathrm{HF}^a_{P/I}(t)$ is called the **affine regularity index** of P/I and is denoted by $\mathrm{ri}^a(P/I)$.

For a homogeneous ideal I, the Hilbert polynomial and the regularity index of P/I are related to their affine counterparts as follows.

Proposition 5.6.11. *Let I be a proper homogeneous ideal in P.*

a) We have $\mathrm{HP}_{P/I}(t) = \Delta\,\mathrm{HP}^a_{P/I}(t) = \mathrm{HP}^a_{P/I}(t) - \mathrm{HP}^a_{P/I}(t-1)$.
b) We have $\mathrm{ri}(P/I) = \mathrm{ri}^a(P/I) + 1$.
c) We have $\dim(P/I) = \deg \mathrm{HP}^a_{P/I}(t)$.
d) We have $\mathrm{mult}(P/I) = \dim(P/I)!\ \mathrm{LC}_{\mathtt{Deg}}(\mathrm{HP}^a_{P/I}(t))$.

Proof. First we show a). Proposition 5.6.8.a yields $\mathrm{HF}_{P/I}(i) = \Delta\,\mathrm{HF}^a_{P/I}(i)$ for all $i \in \mathbb{Z}$. Now it suffices to apply Corollary 5.1.11.a because $\mathrm{HF}^a_{P/I}$ is an integer function of polynomial type. In order to show b), we use the same argument and apply Corollary 5.1.11.b.

Next we prove c). If $\mathrm{HP}_{P/I}(t) = 0$, the polynomial $\mathrm{HP}^a_{P/I}(t)$ is a non-zero constant by a). Consequently, Theorem 5.4.15.b shows that we

have $\dim(P/I) = 0 = \deg(\mathrm{HP}^a_{P/I}(t))$. Otherwise, if $\mathrm{HP}_{P/I}(t) \neq 0$, Theorem 5.4.15.b and a) imply $\dim(P/I) = 1 + \deg(\mathrm{HP}_{P/I}(t)) = \deg(\mathrm{HP}^a_{P/I}(t))$.

Finally, we prove d). If we have $\mathrm{HP}_{P/I}(t) = 0$ then Theorem 5.4.15.c and a) yield $\mathrm{mult}(P/I) = \dim_K(P/I) = \mathrm{HP}^a_{P/I}(t)$, and the claim is true. Therefore we may now assume that $d = \deg(\mathrm{HP}^a_{P/I}(t)) \geq 1$. Then we write $\mathrm{HP}^a_{P/I}(t) = c_d t^d + c_{d-1}t^{d-1} + \cdots + c_0$ where $c_0, \ldots, c_d \in \mathbb{Q}$. Using a), we calculate

$$\begin{aligned} \mathrm{HP}_{P/I}(t) &= \mathrm{HP}^a_{P/I}(t) - \mathrm{HP}^a_{P/I}(t-1) \\ &= (c_d t^d + \cdots + c_0) - (c_d(t-1)^d + \cdots + c_0) \\ &= d\, c_d\, t^{d-1} + (\textit{terms of degree } \leq d-2) \end{aligned}$$

Therefore we get $d!\ \mathrm{LC}_{\mathtt{Deg}}(\mathrm{HP}^a_{P/I}(t)) = d!\, c_d = (d-1)!\ \mathrm{LC}_{\mathtt{Deg}}(\mathrm{HP}_{P/I}(t)) = \mathrm{mult}(P/I)$, as desired. □

For a non-homogeneous ideal I, we can compare the Hilbert polynomial, the regularity index, the dimension, and the multiplicity of the affine algebra P/I to the corresponding notions for $\overline{P}/I^{\mathrm{hom}}$.

Proposition 5.6.12. *Let I be a proper ideal in P, let x_0 be a homogenizing indeterminate, and let $\overline{P} = K[x_0, \ldots, x_n]$.*

a) We have $\mathrm{HP}^a_{P/I}(t) = \mathrm{HP}_{\overline{P}/I^{\mathrm{hom}}}(t)$.
b) We have $\mathrm{ri}^a(P/I) = \mathrm{ri}(\overline{P}/I^{\mathrm{hom}})$.
c) We have $\dim(P/I) = \dim(\overline{P}/I^{\mathrm{hom}}) - 1$.
d) We have $\mathrm{mult}(P/I) = \mathrm{mult}(\overline{P}/I^{\mathrm{hom}})$.

Proof. The first two claims follow from Proposition 5.6.3.c which says that the underlying Hilbert functions agree. Claims c) and d) follow from Proposition 5.6.7.b and Definitions 5.4.1 and 5.6.9. □

5.6.B Primary Decomposition in Noetherian Rings

Of the colors,
red, blue and yellow
are primary and irreducible.
(Alice Bailey and Djwhal Khul)

The goal of this subsection is to introduce some parts of the general theory of primary decomposition in Noetherian rings. Later we shall apply these results to prove that the definition of the dimension of an affine algebra via chains of prime ideals coincides with the definition via affine Hilbert polynomials. The computational aspects of this theory are treated in Tutorials 43 and 79. Recall that the rings we consider are always assumed to be commutative with identity element. A proper ideal I in a ring R is called a **prime ideal** if $rr' \in I$ implies $r \in I$ or $r' \in I$ for all $r, r' \in R$.

Definition 5.6.13. Let R be a ring. A prime ideal $\mathfrak{p}$ of R is called a **minimal prime** of R if there is no prime ideal $\mathfrak{q}$ such that $\mathfrak{q} \subset \mathfrak{p}$. We denote the set of all minimal primes of R by $\operatorname{Min}(R)$.

By Definition 2.4.4, a ring R is called **Noetherian** if every ascending chain of ideals becomes eventually stationary. Our next proposition shows that Noetherian rings have only finitely many minimal primes. In order to prove it, we need the following auxiliary result.

Lemma 5.6.14. *Let $I_1, \ldots, I_s$ be ideals in a ring R, and let $\mathfrak{p}$ be a prime ideal of R which contains $I_1 \cap \cdots \cap I_s$. Then $\mathfrak{p}$ contains one of the ideals I_i.*

Proof. For a contradiction, suppose that there exist elements $r_i \in I_i \setminus \mathfrak{p}$ for $i = 1, \ldots, s$. Then we have $r_1 \cdots r_s \in I_1 \cap \cdots \cap I_s \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal, it follows that one of the factors r_i is contained in $\mathfrak{p}$, in contradiction to the choice of r_i. □

Proposition 5.6.15. (Minimal Primes in Noetherian Rings)
Let R be a Noetherian ring.

a) Every radical ideal of R is the intersection of finitely many prime ideals of R.
b) The are only finitely many minimal primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of R. They satisfy $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s = \sqrt{(0)}$.
c) Every prime ideal of R contains one of the minimal primes.

Proof. In order to show a) we use the technique of **Noetherian recursion**. Suppose that claim a) is not true. Then the set of all radical ideals for which the claim does not hold contains a maximal element I with respect to inclusion because R is a Noetherian ring. Obviously, this ideal I is not a prime ideal. Thus there exist $a, b \in R$ such that $ab \in I$ and $a, b \notin I$. By the maximality of I, the ideals $J_1 = \sqrt{I + (a)}$ and $J_2 = \sqrt{I + (b)}$ are finite intersections of prime ideals. Hence it suffices to show $I = J_1 \cap J_2$ in order to arrive at a contradiction. Given $f \in J_1 \cap J_2$, there exist $m_1, m_2 \in \mathbb{N}$ and $g_1, g_2 \in I$ and $h_1, h_2 \in R$ such that $f^{m_1} = g_1 + ah_1$ and $f^{m_2} = g_2 + bh_2$. Hence we get $f^{m_1+m_2} = g_1g_2 + g_1bh_2 + g_2ah_1 + abh_1h_2 \in I$, and the fact that I is a radical ideal implies $f \in I$. As the other inclusion is obviously true, this proves $I = J_1 \cap J_2$.

For the proof of b), we use a) and write $\sqrt{(0)} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$ with prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of R for which we may assume that $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for distinct $i, j \in \{1, \ldots, s\}$. Since every minimal prime of R contains $\sqrt{(0)}$, the lemma shows that it is one of the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Conversely, each prime ideal of $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ is minimal, because otherwise it contains a strictly smaller prime ideal which has to contain one of the ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ by the lemma, in contradiction to the assumption that $\mathfrak{p}_i \supset \mathfrak{p}_j$ does not hold for $i \neq j$. Thus the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are exactly the minimal primes of R.

Claim c) follows from the lemma and the observation that every prime ideal of R contains $\sqrt{(0)}$. □

Our next definition and the subsequent propositions should look familiar to those of you who worked out the details of Tutorial 43.

Definition 5.6.16. Let R be a ring.

a) An ideal I of R is called **irreducible** if it cannot be written as the intersection of two ideals, both of which properly contain it.
b) An ideal I of R is called a **primary ideal** if $r\,r' \in I$ implies $r \in I$ or $r' \in \sqrt{I}$ for all $r, r' \in R$.

Clearly, part b) of this definition implies that the radical of a primary ideal I is a prime ideal $\mathfrak{p}$. In this situation we say that I is a **$\mathfrak{p}$-primary ideal** or that I is **primary for $\mathfrak{p}$**. The following proposition collects some basic properties of irreducible and primary ideals in Noetherian rings.

Proposition 5.6.17. *Let R be a Noetherian ring.*

a) If I is an irreducible ideal of R, it is a primary ideal.
b) Every proper ideal I of R is a finite intersection of irreducible ideals.
c) Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ be primary ideals of R, and let $r \in R$ be an element which is not contained in $\sqrt{q}_1 \cup \cdots \cup \sqrt{q}_s$. Then r is a non-zerodivisor for $R/(\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s)$.
d) Let $\mathfrak{p}$ be a prime ideal of R, and let $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ be $\mathfrak{p}$-primary ideals of R. Then $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ is a $\mathfrak{p}$-primary ideal of R.

Proof. First we prove a). Since I is irreducible, the ideal (0) is irreducible in the residue class ring R/I. We have to show that the ideal (0) is primary in this ring. By passing to R/I, we may assume that $I = (0)$. Let $r, r' \in R$ be elements with $r\,r' = 0$ and $r' \neq 0$. We need to show that there exists a number $i \in \mathbb{N}$ such that $r^i = 0$. If we can prove $(r^i) \cap (r') = (0)$ for some $i > 0$, we can conclude that $r^i = 0$ because (0) is irreducible. Since R is a Noetherian ring, the ascending chain of ideals $\mathrm{Ann}_R(r) \subseteq \mathrm{Ann}_R(r^2) \subseteq \cdots$ is eventually stationary, i.e. there exists a number $i \geq 0$ such that $\mathrm{Ann}_R(r^i) = \mathrm{Ann}_R(r^{i+1})$. Let $r'' \in (r^i) \cap (r')$. Then $r\,r' = 0$ and $r'' \in (r')$ imply $r\,r'' = 0$. Now we write $r'' = a\,r^i$ with $a \in R$ and use $a\,r^{i+1} = r''\,r = 0$ to obtain $a \in \mathrm{Ann}_R(r^{i+1}) = \mathrm{Ann}_R(r^i)$. Hence we get $r'' = a\,r^i = 0$, as desired.

Next we show b). We apply the technique of Noetherian recursion. Suppose that the claim is not true. The set of all ideals for which the claim does not hold contains a maximal element I with respect to inclusion because R is a Noetherian ring. Clearly, the ideal I is not irreducible. Therefore there exist two ideals I_1, I_2 which properly contain I and satisfy $I_1 \cap I_2 = I$. The maximality of I implies that both I_1 and I_2 are finite intersections of irreducible ideals. Hence also I is a finite intersection of irreducible ideals, a contradiction.

To prove c), we let $r' \in R$ be such that $r\,r' \in \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$. Since we have $r\,r' \in \mathfrak{q}_i$ and $r \notin \sqrt{\mathfrak{q}_i}$, it follows that $r' \in \mathfrak{q}_i$ for $i = 1, \ldots, s$. Hence the element r is a non-zerodivisor for $R/\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$.

Finally, we show d). Let $r, r' \in R$ be such that $r\,r' \in \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$, and assume that $r' \notin \sqrt{\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s} = \sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_s} = \mathfrak{p}$. Then we have $r\,r' \in \mathfrak{q}_i$ and $r' \notin \sqrt{\mathfrak{q}_i} = \mathfrak{p}$, and therefore $r \in \mathfrak{q}_i$ for $i = 1, \ldots, s$. This yields $r \in \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ and finishes the proof. □

The preceding proposition allows us to prove the existence of primary decompositions for ideals in Noetherian rings as follows.

Proposition 5.6.18. (Existence of Primary Decompositions)
Let R be a Noetherian ring. Every proper ideal I of R can be written as $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ with primary ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ of R such that the following conditions are satisfied.

1) For $i, j \in \{1, \ldots, s\}$ with $i \neq j$ we have $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$.
2) For $i = 1, \ldots, s$ we have $\bigcap_{j \neq i} \mathfrak{q}_j \nsubseteq \mathfrak{q}_i$.

Proof. Using parts a) and b) of Proposition 5.6.17, we obtain a decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ with primary ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ of R. Part d) of the same proposition allows us to combine those primary ideals which have the same radical. Thus we can achieve property 1). To achieve property 2), it suffices to drop superfluous ideals $\mathfrak{q}_i$. □

A representation $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ as in this proposition is called a **reduced primary decomposition** of I. The uniqueness of reduced primary decompositions will be discussed further in Tutorial 79 as will a way to compute them. There is one more result about prime ideals in Noetherian rings which will prove useful. It is sometimes known as the Prime Avoidance Lemma.

Proposition 5.6.19. (Prime Avoidance)
Let R be a Noetherian ring, let I be an ideal in R, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be prime ideals in R. If $I \nsubseteq \mathfrak{p}_i$ for $i = 1, \ldots, s$, then I is not contained in $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_s$.

Proof. Let us proceed by induction on s. For $s = 1$, the statement is obviously true. Now consider $s > 1$. For every $i \in \{1, \ldots, s\}$, the inductive hypothesis yields an element $r_i \in I \setminus \bigcup_{j \neq i} \mathfrak{p}_j$. If $r_i \notin \mathfrak{p}_i$ for some $i \in \{1, \ldots, s\}$, we are done. Otherwise we have $r_i \in (I \cap \mathfrak{p}_i) \setminus \bigcup_{j \neq i} \mathfrak{p}_j$ for $i = 1, \ldots, s$. Now we let $\tilde{r}_i = \prod_{j \neq i} r_j$ and we obtain $\tilde{r}_i \in (I \cap \bigcap_{j \neq i} \mathfrak{p}_j) \setminus \mathfrak{p}_i$ for $i = 1, \ldots, s$. Hence the element $r = \tilde{r}_1 + \cdots + \tilde{r}_s$ satisfies $r \in I \setminus \bigcup_{i=1}^{s} \mathfrak{p}_i$, as we wanted to show. □

In the last part of this subsection we adapt the preceding results to the graded case. The first contribution to this topic is a generalization of Proposition 1.7.12. There it was shown that, for a homogeneous ideal, the property of being prime can be checked using homogeneous elements only. Now it turns out that the same is true for primary ideals.

Proposition 5.6.20. *Let Γ be a monoid, let τ be a monoid ordering on Γ, let R be a Γ-graded ring, and let I be a homogeneous ideal in R. Then I is a primary ideal if and only if $r\,r' \in I$ implies $r \in I$ or $r' \in \sqrt{I}$ for homogeneous elements $r, r' \in R$.*

Proof. Let $r, r' \in R$ be such that $r\,r' \in I$ and $r \notin I$. We decompose r and r' into non-zero homogeneous components $r = r_{\gamma_1} + \cdots + r_{\gamma_r}$ and $r' = r'_{\delta_1} + \cdots + r'_{\delta_s}$ where $\gamma_1 >_\tau \cdots >_\tau \gamma_r$ and $\delta_1 >_\tau \cdots >_\tau \delta_s$. Clearly, we may assume that $r_{\gamma_1} \notin I$ since otherwise we could substitute r with $r - r_{\gamma_1}$ without affecting the assumptions $r\,r' \in I$ and $r \notin I$. It follows that $r_{\gamma_1} r'_{\delta_1} \in I$ because I is a homogeneous ideal. Hence the hypothesis yields $r'_{\delta_1} \in \sqrt{I}$. Choose $i \geq 0$ such that we have $(r'_{\delta_1})^i \in I$. Then it follows that $r\,(r' - r'_{\delta_1})^i \in I$. Arguing as before, we see that $r'_{\delta_2} \in \sqrt{I}$. Continuing in this way, we finally get $r' \in \sqrt{I}$, as we wanted. The converse implication follows immediately from the definition. □

The next step is a graded version of the primary decomposition of an ideal. Given an arbitrary ideal I, the homogeneous ideal generated by the homogeneous elements in I is called the homogeneous part of I. It was studied in Tutorial 50 and features prominently in the following proof.

Proposition 5.6.21. (Homogeneous Primary Decomposition) *Let Γ be a monoid possessing a monoid ordering τ, let R be a Γ-graded Noetherian ring, and let I be a proper homogeneous ideal of R. Then there exists a decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ with homogeneous primary ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ of R such that the following conditions are satisfied.*

1) For $i, j \in \{1, \ldots, s\}$ with $i \neq j$ we have $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$.
2) For $i = 1, \ldots, s$ we have $\bigcap_{j \neq i} \mathfrak{q}_j \nsubseteq \mathfrak{q}_i$.

Proof. Let $I \subset R$ be a proper homogeneous ideal. By Proposition 5.6.18, there exists a reduced primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ with primary ideals $\mathfrak{q}_i$ for $i = 1, \ldots, s$. For an ideal $J \subseteq R$, let J_Γ be the homogeneous part of J, i.e. the ideal generated by the homogeneous elements in J. The chain of inclusions $I = (\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s)_\Gamma \subseteq (\mathfrak{q}_1)_\Gamma \cap \cdots \cap (\mathfrak{q}_s)_\Gamma \subseteq \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s = I$ shows that we have $I = (\mathfrak{q}_1)_\Gamma \cap \cdots \cap (\mathfrak{q}_s)_\Gamma$. Next we prove that the ideals $(\mathfrak{q}_i)_\Gamma$ are primary ideals. By Proposition 5.6.20, it suffices to consider homogeneous elements $r, r' \in R$ such that $r\,r' \in (\mathfrak{q}_i)_\Gamma$ and $r \notin (\mathfrak{q}_i)_\Gamma$. Then $r \notin \mathfrak{q}_i$ implies $r' \in \sqrt{\mathfrak{q}_i}$, and therefore $r' \in \sqrt{(\mathfrak{q}_i)_\Gamma}$. Thus we have shown that $(\mathfrak{q}_1)_\Gamma, \ldots, (\mathfrak{q}_s)_\Gamma$ are primary ideals. Properties 1) and 2) can be achieved in the same way as in the proof of Proposition 5.6.18. □

Now we turn our attention to Prime Avoidance 5.6.19. To find a graded version of this result, we have to restrict the setting to standard graded algebras.

Proposition 5.6.22. (Homogeneous Prime Avoidance)
Let K be a field, let R be a standard graded K-algebra, let $I \subseteq R$ be a homogeneous ideal, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be homogeneous prime ideal of R such that $I \nsubseteq \mathfrak{p}_i$ for $i = 1, \ldots, s$, and let $d \in \mathbb{N}$. Then there exists a degree $\delta(d) \geq d$ such that $I_{\delta(d)} \nsubseteq (\mathfrak{p}_1)_{\delta(d)} \cup \cdots \cup (\mathfrak{p}_s)_{\delta(d)}$.

Proof. The method we use to prove this result is analogous to the method of proof for Proposition 5.6.19, except that we have to be careful to keep all elements homogeneous. Firstly, we observe that none of the ideals $\mathfrak{p}_i$ coincides with R_+ since the latter ideal contains all homogeneous ideals. Secondly, we treat the case $s = 1$. Let $r \in I$ and $r' \in R_+$ be homogeneous elements which are not contained in $\mathfrak{p}_1$. Choose $i \geq 1$ large enough so that $\delta(d) = \deg(r) + i \deg(r') \geq d$. Then we have $r\,(r')^i \in I_{\delta(d)} \setminus (\mathfrak{p}_1)_{\delta(d)}$.

Thirdly, we prove the case $s > 1$ by induction on s. By the inductive hypothesis, there exist natural numbers $\delta_1(d), \ldots, \delta_s(d)$ such that $\delta_i(d) \geq d$ and $I_{\delta_i(d)} \nsubseteq \bigcup_{j \neq i} (\mathfrak{p}_j)_{\delta_i(d)}$ for $i = 1, \ldots, s$. Therefore there exist homogeneous elements $r_i \in I_{\delta_i(d)}$ with $r_i \notin \bigcup_{j \neq i} (\mathfrak{p}_j)_{\delta_i(d)}$ for $i = 1, \ldots, s$. If we have $r_i \notin \mathfrak{p}_i$ for some $i \in \{1, \ldots, s\}$, we are done. Otherwise we have $r_i \in (I \cap \mathfrak{p}_i)_{\delta_i(d)} \setminus \bigcup_{j \neq i} (\mathfrak{p}_j)_{\delta_i(d)}$ for $i = 1, \ldots, s$. Now we define $d_i = \sum_{j \neq i} \delta_j(d)$ and $\tilde{r}_i = \prod_{j \neq i} r_j$, and we see that $\tilde{r}_i \in (I \cap \bigcap_{j \neq i} \mathfrak{p}_j)_{d_i} \setminus (\mathfrak{p}_i)_{d_i}$ for $i = 1, \ldots, s$. By raising the elements $\tilde{r}_i$ to appropriate powers, we may assume that $d_1 = \cdots = d_s$. We denote this number by $\delta(d)$. Then $r = \tilde{r}_1 + \cdots + \tilde{r}_s$ satisfies $r \in I_{\delta(d)} \setminus \bigcup_{i=1}^{s} (\mathfrak{p}_i)_{\delta(d)}$, and the claim follows. □

The following example shows that the proposition is in general not true for $\mathbb{Z}^m$-graded rings with $m \geq 2$.

Example 5.6.23. Let K be a field, and let $P = K[x, y]$ be graded by the identity matrix $\mathcal{I}_2 \in \mathrm{Mat}_2(\mathbb{Z})$. Then the homogeneous ideal $I = (x, y)$ of P is not contained in the prime ideals $\mathfrak{p}_1 = (x)$ and $\mathfrak{p}_2 = (y)$. Furthermore, we have $I_d = K \cdot x^{\alpha_1} y^{\alpha_2} = (x)_d \cup (y)_d$ for every $d = (\alpha_1, \alpha_2) \in \mathbb{N}^2$. In particular, we see that Homogeneous Prime Avoidance 5.6.22 does not hold.

Furthermore, the claim of the proposition does not hold for every degree $\delta(d) \geq d$, as our next example shows.

Example 5.6.24. Let $P = \mathbb{F}_2[x, y]$ be standard graded. Then the homogeneous ideal $I = (x, y)$ of P is not contained in the homogeneous prime ideals $\mathfrak{p}_1 = (x)$, $\mathfrak{p}_2 = (y)$, and $\mathfrak{p}_3 = (x + y)$. But we have $I_d = (x)_d \cup (y)_d \cup (x + y)_d$ for $d = 1$. Thus the claim of the proposition does not hold for every degree $\delta(d) \geq d$.

Finally, we use Homogeneous Prime Avoidance 5.6.22 to analyze homogeneous primary decompositions in greater detail. The following definition introduces a generalization of the notion of a non-zerodivisor which is particularly useful in the graded case.

Definition 5.6.25. Let K be a field, let R be a K-algebra, and let I be a proper ideal of R. An element $r \in R$ is called an **almost non-zerodivisor** for R/I if $\operatorname{Ann}_{R/I}(r+I)$ is a finite dimensional K-vector space.

The knowledge of a homogeneous primary decomposition enables us to find homogeneous almost non-zerodivisors as follows.

Proposition 5.6.26. *Let K be a field, let R be a standard graded K-algebra, let $I \subset R$ be a proper homogeneous ideal, let $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ be a reduced homogeneous primary decomposition of I, and let $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ for $i = 1, \ldots, s$.*

a) If $s = 1$ and $\mathfrak{p}_1 = R_+$ then R/I is a finite dimensional K-vector space. In particular, the residue class $r+I$ of every element $r \in R_+$ is nilpotent.

b) If $R_+ \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ then for every $d \in \mathbb{N}$ there exists a degree $\delta(d) \geq d$ and an element $r \in R_{\delta(d)}$ such that r is a non-zerodivisor for R/I.

c) If $s \geq 2$ and $R_+ \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$, we may assume without loss of generality that $\mathfrak{p}_1 = R_+$. Then for every $d \in \mathbb{N}$ there exists a degree $\delta(d) \geq d$ and an element $r \in R_{\delta(d)}$ such that r is an almost non-zerodivisor for R/I.

Proof. Claim a) follows from the observation that for every homogeneous element $r \in R$ of positive degree we have $r \in \mathfrak{p}_1 = \sqrt{I}$. Now we prove b). Let $d \in \mathbb{N}$. Using Proposition 5.6.22, we obtain a degree $\delta(d) \geq d$ and a homogeneous element $r \in (R_+)_{\delta(d)}$ such that $r \notin \bigcup_{i=1}^{s} (\mathfrak{p}_i)_{\delta(d)}$. By Proposition 5.6.17.c, the element r is a non-zerodivisor for R/I.

Finally we prove c). Let $d \in \mathbb{N}$. Using Proposition 5.6.22, we obtain a degree $\delta(d) \geq d$ and a homogeneous element $r \in (R_+)_{\delta(d)}$ such that $r \notin \bigcup_{i=2}^{s} (\mathfrak{p}_i)_{\delta(d)}$. Our goal is to show that r is an almost non-zerodivisor for R/I. The ideal $\operatorname{Ann}_{R/I}(r+I)$ is clearly homogeneous. To show that it is a finite-dimensional K-vector space, it suffices to prove that there exists a degree $i \geq 1$ such that every homogeneous element $r' \in R_j$ of degree $j \geq i$ with $(r'+I)(r+I) = 0$ satisfies $r' + I = 0$.

From the facts that R is a Noetherian ring and $\sqrt{q}_1 = R_+$ we conclude that there exists a number $i \geq 1$ such that $(R_+)^i \subseteq \mathfrak{q}_1$. In particular, this shows $(\mathfrak{q}_1)_j = R_j$ for all $j \geq i$. Therefore we see that $I_j = (\mathfrak{q}_1)_j \cap \cdots \cap (\mathfrak{q}_s)_j = (\mathfrak{q}_2)_j \cap \cdots \cap (\mathfrak{q}_s)_j$ for $j \geq i$. Hence the condition $r\,r' \in I$ implies that we have $r\,r' \in \mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_s$ for all $r' \in R_j$ with $j \geq i - \delta(d)$. Since we have $r \notin \bigcup_{i=2}^{s} (\mathfrak{p}_i)_{\delta(d)}$, Proposition 5.6.17.c tells us that r is a non-zerodivisor for $R/\mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_s$. Consequently, it follows that $r\,r' \in I$ implies $r' \in (\mathfrak{q}_2 \cap \cdots \cap \mathfrak{q}_s)_j = I_j$ for $j \geq i$. This is exactly what we wanted to prove. □

5.6.C The Krull Dimension of an Affine Algebra

Bear in mind that 400 years ago,
arithmetic was a difficult art!
So great an educator as Melanchthon
did not trust the average student
to penetrate into the secrets of fractions.
(Wolfgang Krull)

Using chains of prime ideals, we have the following concept of the dimension of a ring.

Definition 5.6.27. Let R be a ring. The **Krull dimension** of R is the supremum of the lengths d of chains $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_d$ of prime ideals in R. We denote it by $\operatorname{Kdim}(R)$ and write $\operatorname{Kdim}(R) = \infty$ if the supremum is not finite.

For some rings, their Krull dimension is easy to determine.

Example 5.6.28. For a field K we have $\operatorname{Kdim}(K) = 0$ since (0) is the only prime ideal of K.

Example 5.6.29. For a principal ideal domain R, we have $\operatorname{Kdim}(R) = 1$. In particular, we have $\operatorname{Kdim}(\mathbb{Z}) = 1$ and $\operatorname{Kdim}(K[x]) = 1$ for every field K. The prime ideals of R are the zero ideal and the principal ideals (f) where f is a non-zero prime element of R (see also Exercise 6).

Although it is possible for a Noetherian ring to have infinite Krull dimension, affine algebras have a finite Krull dimension. This is a consequence of the main theorem of this subsection which says that, for an affine algebra of the form P/I, we have $\operatorname{Kdim}(P/I) = \dim(P/I)$. The proof of this theorem consists of a number of steps. We begin at the beginning, i.e. with the zero-dimensional case. In the following, we let K be a field, we let $P = K[x_1, \ldots, x_n]$ be standard graded, and we let $I \subset P$ be a proper ideal.

Proposition 5.6.30. *For the affine K-algebra P/I, the following conditions are equivalent.*

a) $\dim_K(P/I) < \infty$
b) $\dim(P/I) = 0$
c) $\operatorname{Kdim}(P/I) = 0$

Proof. To show that a) implies b), we observe that the hypothesis implies that the chain of K-vector spaces

$$0 = \langle P_{\leq -1}\rangle/\langle I_{\leq -1}\rangle \subseteq \langle P_{\leq 0}\rangle/\langle I_{\leq 0}\rangle \subseteq \langle P_{\leq 1}\rangle/\langle I_{\leq 1}\rangle \subseteq \cdots$$

is eventually stationary. Therefore $\operatorname{HF}^a_{P/I}(i)$ is constant for $i \gg 0$, the polynomial $\operatorname{HP}^a_{P/I}(t)$ is constant, and $\dim(P/I) = \deg(\operatorname{HP}^a_{P/I}(t)) = 0$.

Next we prove that b) implies c). Let $\mathfrak{p}$ be a minimal prime of P/I. Since the K-vector space dimension of $\langle P_{\leq i}\rangle/\langle I_{\leq i}\rangle$ is constant for $i \gg 0$, both P/I and $(P/I)/\mathfrak{p}$ are finite dimensional K-vector spaces. It follows that the integral domain $(P/I)/\mathfrak{p}$ is a field, because the injective multiplication by a non-zero element is forced to be bijective. This means that there is no prime ideal in $(P/I)/\mathfrak{p}$ besides the zero ideal. Consequently, there is no prime ideal in P/I which contains $\mathfrak{p}$, as its residue class ideal would be a prime ideal in $(P/I)/\mathfrak{p}$. Altogether, we see that no two prime ideals of P/I are strictly contained in each other, i.e. that $\operatorname{Kdim}(P/I) = 0$.

Finally, we show that a) follows from c). By the hypothesis and Proposition 5.6.15.b, there are only finitely many prime ideals in P/I. These prime ideals are simultaneously minimal primes and maximal ideals of P/I. Thus their preimages $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ in P are exactly the maximal ideals of P containing I. By Hilbert's Nullstellensatz 2.6.6.b, we have $\dim_K(P/\mathfrak{m}_i) < \infty$ for $i = 1, \ldots, s$. Let $\overline{K}$ be the algebraic closure of K, and let $\overline{P} = \overline{K}[x_1, \ldots, x_n]$. Then the Finiteness Criterion 3.7.1 shows that there are only finitely many maximal ideals of $\overline{P}$ containing one of the ideals $\mathfrak{m}_i\,\overline{P}$. Let $\mathfrak{M}$ be a maximal ideal of $\overline{P}$ containing $I\,\overline{P}$. Then $\mathfrak{M} \cap P$ is a maximal ideal of P which contains I, i.e. it is one of the ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$. Hence $\mathfrak{M}$ contains one of the ideals $\mathfrak{m}_i\,\overline{P}$ for some $i \in \{1, \ldots, s\}$. Thus there are only finitely many maximal ideals of $\overline{P}$ containing $I\,\overline{P}$, and the Finiteness Criterion 3.7.1 yields the claim. □

The following consequence of this proposition will be used in the proof of our main theorem.

Corollary 5.6.31. *Let $I \subset P$ be a prime ideal such that $\dim(P/I) > 0$, and let $f \in P$ be an almost non-zerodivisor for P/I. Then we have $f \notin I$.*

Proof. The proposition and the hypothesis imply $\dim_K(P/I) = \infty$. Therefore we cannot have $f \in I$ since in this case $\operatorname{Ann}_{P/I}(f + I) = P/I$ would be an infinite dimensional K-vector space. □

The next step is to reduce the proof of $\dim(P/I) = \operatorname{Kdim}(P/I)$ to the case of an integral domain P/I.

Proposition 5.6.32. *Let* $\operatorname{Min}(P/I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$.

a) We have $\dim(P/I) = \dim(P/\sqrt{I}) = \dim((P/I)/(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s)) = \max\{\dim((P/I)/\mathfrak{p}_1), \ldots, \dim((P/I)/\mathfrak{p}_s)\}$.

b) We have $\operatorname{Kdim}(P/I) = \operatorname{Kdim}(P/\sqrt{I}) = \operatorname{Kdim}((P/I)/(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s)) = \max\{\operatorname{Kdim}((P/I)/\mathfrak{p}_1), \ldots, \operatorname{Kdim}((P/I)/\mathfrak{p}_s)\}$.

Proof. Let us begin by showing a). The first equality follows from Propositions 4.3.10.c, 5.4.8.c, and 5.6.12.c. More precisely, let x_0 be a homogenizing indeterminate, and let $\overline{P} = K[x_0, \ldots, x_n]$. Then we get $\dim(P/I) = \dim(\overline{P}/I^{\hom}) - 1 = \dim(\overline{P}/\sqrt{I^{\hom}}) - 1 = \dim(\overline{P}/(\sqrt{I})^{\hom}) - 1 = \dim(P/\sqrt{I})$. The second equality follows from parts a) and b) of Proposition 5.6.15.

The third equality is a consequence of Propositions 4.3.10.b, 5.4.9.b, and 5.6.12.c. More precisely, let $\mathfrak{P}_i$ be the preimage of $\mathfrak{p}_i$ in P for $i = 1, \ldots, s$. Then we get $\dim((P/I)/(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s)) = \dim(P/(\mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_s)) = \dim(\overline{P}/(\mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_s)^{\hom}) - 1 = \dim(\overline{P}/(\mathfrak{P}_1^{\hom} \cap \cdots \cap \mathfrak{P}_s^{\hom})) - 1 = \max\{\dim(\overline{P}/\mathfrak{P}_i^{\hom}) \mid i = 1, \ldots, s\} - 1 = \max\{\dim(P/\mathfrak{P}_i) \mid i = 1, \ldots, s\} = \max\{\dim((P/I)/\mathfrak{p}_i) \mid i = 1, \ldots, s\}$.

Now we prove b). The first two equalities follow from Proposition 5.6.15.b. Every minimal prime of P/I contains $\sqrt{(0)}$, i.e. the image of $\sqrt{I}$ in P/I. Therefore the prime ideals of P/I and $P/\sqrt{I}$ are in 1-1 correspondence. The third equality expresses the fact that every maximal chain of prime ideals $\mathfrak{q}_0 \subset \cdots \subset \mathfrak{q}_d$ in P/I starts with a minimal prime $\mathfrak{q}_0$. □

The central part of the proof of the main theorem is going to be an a induction on $\dim(P/I)$. Our next results provide us with inequalities on the various dimensions which make this induction possible. Given a non-zero polynomial $f \in P$ of degree d, we have for every $i \in \mathbb{N}$ an exact sequence of finite-dimensional K-vector spaces

$$(1) \qquad 0 \longrightarrow \mathrm{Ker}(\varepsilon_i) \longrightarrow P_{\leq i}/(I_{\leq i} + (f)_{\leq i}) \xrightarrow{\varepsilon_i} P_{\leq i}/(I + (f))_{\leq i} \longrightarrow 0$$

where ε_i is the canonical surjection, and an exact sequence of finite dimensional K-vector spaces

$$(2)\ 0 \to \mathrm{Ker}(\mu_i) \to P_{\leq i}/I_{\leq i} \xrightarrow{\mu_i} P_{\leq i+d}/I_{\leq i+d} \to P_{\leq i+d}/(I_{\leq i+d} + (f)_{\leq i+d}) \to 0$$

where μ_i is induced by multiplication by f.

Proposition 5.6.33. *Let $f \in P$ be a non-zero polynomial of degree d.*

a) For every $i \in \mathbb{N}$, we have a commutative diagram

$$\begin{array}{ccc} P_{\leq i}/I_{\leq i} & \xrightarrow{\mu_i} & P_{\leq i+d}/I_{\leq i+d} \\ \downarrow & & \downarrow \\ P_{\leq i+1}/I_{\leq i+1} & \xrightarrow{\mu_{i+1}} & P_{\leq i+d+1}/I_{\leq i+d+1} \end{array}$$

where the vertical maps are induced by the canonical inclusions and are injective. In particular, we have $\mathrm{Ker}(\mu_i) \subseteq \mathrm{Ker}(\mu_{i+1})$.

b) We have $\bigcup_{i \geq 0} \mathrm{Ker}(\mu_i) = \mathrm{Ann}_{P/I}(f + I)$.

c) If f is a non-zerodivisor for P/I then $\dim(P/(I+(f))) \leq \dim(P/I) - 1$.

Proof. Claim a) is clearly true, and b) follows from a). It remains to prove c). Sequence (1) yields $\mathrm{HF}^a_{P/(I+(f))}(i) \leq \dim_K(P_{\leq i}/(I_{\leq i} + (f)_{\leq i}))$, and by b) and sequence (2) we have $\dim_K(P_{\leq i}/(I_{\leq i} + (f)_{\leq i})) = \mathrm{HF}^a_{P/I}(i) - \mathrm{HF}^a_{P/I}(i-d)$. Consequently, we get $\mathrm{HP}^a_{P/(I+(f))}(i) \leq \mathrm{HP}^a_{P/I}(i) - \mathrm{HP}^a_{P/I}(i-d)$ for large enough i. Since $\deg(\mathrm{HP}^a_{P/I}(t) - \mathrm{HP}^a_{P/I}(t-d)) = \deg(\mathrm{HP}^a_{P/I}(t)) - 1$, the conclusion follows. □

The inequality in the last part of this proposition is an equality if we are given a homogeneous polynomial which is an almost non-zerodivisor for $P/\operatorname{DF}_W(I)$. This is the main result of our next proposition.

Proposition 5.6.34. *Let $W = (1\ 1\ \cdots\ 1) \in \operatorname{Mat}_{1,n}(\mathbb{Z})$, let $d \geq 1$, and let $f \in P_d$ be an almost non-zerodivisor for $P/\operatorname{DF}_W(I)$.*

a) The chain of K-vector spaces $\operatorname{Ker}(\mu_0) \subseteq \operatorname{Ker}(\mu_1) \subseteq \cdots$ is eventually stationary. In particular, the K-vector space $\bigcup_{i\geq 0} \operatorname{Ker}(\mu_i)$ is finite dimensional.

b) The polynomial f is an almost non-zerodivisor for P/I.

c) For large enough i, we have $\operatorname{Ker}(\varepsilon_i) = 0$.

d) If $\dim(P/I) > 0$ then we have $\dim(P/(I + (f))) = \dim(P/I) - 1$.

Proof. First we show a). The K-vector space $\operatorname{Ann}_{P/\operatorname{DF}_W(I)}(f + \operatorname{DF}_W(I))$ is finite dimensional by assumption. Let m be the maximal degree of one of its non-zero homogeneous components, or let $m = 0$ if this annihilator is zero. Let $i > m$, and let $g \in P$ be a non-zero polynomial of degree i such that $g + I_{\leq i} \in \operatorname{Ker}(\mu_i)$, i.e. such that $fg \in I_{\leq i+d}$. Then we have $\operatorname{DF}_W(g)\operatorname{DF}_W(f) = \operatorname{DF}_W(g)\, f \in \operatorname{DF}_W(I)$, and the definition of m implies $\operatorname{DF}_W(g) \in \operatorname{DF}_W(I)$. Thus there is a polynomial $h \in I_{\leq i}$ with $g - h \in P_{\leq i-1}$, and therefore $g + I_{\leq i} \in \operatorname{Ker}(\mu_{i-1})$. Since $i > m$ was arbitrary, we obtain $\operatorname{Ker}(\mu_i) = \operatorname{Ker}(\mu_m)$ for $i \geq m$. This proves a), and b) follows then from Proposition 5.6.33.b and the fact that $\operatorname{Ker}(\mu_m)$ is finite dimensional.

Next we prove c). Let m be defined as above, let $i \geq m$, and let $g \in P$ be a non-zero polynomial of degree i with $g + I_{\leq i} + (f)_{\leq i} \in \operatorname{Ker}(\varepsilon_i)$, i.e. with $g \in (I + (f))_{\leq i}$. Choose $h_1 \in I$, $h_2 \in P$ of minimal degree such that $g = h_1 - fh_2$. We have to show $\deg(h_1) \leq i$ and $\deg(fh_2) \leq i$. Suppose that $j = \deg(h_1) \geq i + 1$. Then $\deg(g) \leq i$ implies $\operatorname{DF}_W(h_1) - f \operatorname{DF}_W(h_2) = 0$, and therefore $f \operatorname{DF}_W(h_2) \in \operatorname{DF}_W(I)$. Since we have $j > m$, the definition of m yields $\operatorname{DF}_W(h_2) \in \operatorname{DF}_W(I)$. Hence there is an element $h_3 \in I$ for which $\operatorname{DF}_W(h_2) = \operatorname{DF}_W(h_3)$. So, the polynomial h_2 is of the form $h_2 = h_3 + h_4$ with $\deg(h_4) < \deg(h_2)$. Now the representation $g = (h_1 - fh_3) - fh_4$ satisfies $h_1 - f\,h_3 \in I_{\leq j-1}$ and $fh_4 \in (f)_{\leq j-1}$ and contradicts the minimality of $j = \deg(h_1)$.

Finally we show d). By c) and sequence (1), we have $\operatorname{HP}^a_{P/(I+(f))}(i) = \dim_K(P_{\leq i}/(I_{\leq i} + (f)_{\leq i})$ for large enough i. By a) and sequence (2), we have $\dim_K(P_{\leq i}/(I_{\leq i} + (f)_{\leq i}) = \operatorname{HP}^a_{P/I}(i) - \operatorname{HP}^a_{P/I}(i - d) + c$ for large enough i and $c = \dim_K(\bigcup_{i\geq 0} \operatorname{Ker}(\mu_i))$. Hence $\dim(P/I) = \deg(\operatorname{HP}^a_{P/I}) > 0$ implies $\deg(\operatorname{HP}^a_{P/(I+(f))}(t)) = \deg(\operatorname{HP}^a_{P/I}(t)) - 1$, and the proof is complete. □

The last ingredient we need for the proof of the main theorem is the analogous inequality for the Krull dimension of $P/(I + (f))$.

Lemma 5.6.35. *Let $f \in P$ be such that $f + I$ is not contained in a minimal prime of P/I. Then we have $\operatorname{Kdim}(P/(I + (f))) \leq \operatorname{Kdim}(P/I) - 1$.*

Proof. Let $\overline{\mathfrak{p}}_0$ be a minimal prime of $P/(I+(f))$ such that there is a maximal chain $\overline{\mathfrak{p}}_0 \subset \overline{\mathfrak{p}}_1 \subset \cdots \subset \overline{\mathfrak{p}}_d$ where $d = \operatorname{Kdim}(P/(I+(f)))$ and where $\overline{\mathfrak{p}}_i$ is a prime ideal of $P/(I+(f))$ for $i = 1, \ldots, d$. For $i = 0, \ldots, d$, let $\mathfrak{p}_i$ be the preimage of $\overline{\mathfrak{p}}_i$ in P/I. Thus we have a chain of prime ideals $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_d$ in R. The first prime ideal $\mathfrak{p}_0$ contains f. Hence it is not a minimal prime of P/I. By Proposition 5.6.15.c, it properly contains a minimal prime $\mathfrak{q}$ of P/I. Thus we have found a chain of prime ideals of length $d+1$ in P/I. This proves the claim. □

Theorem 5.6.36. (The Krull Dimension of an Affine Algebra) *Let I be an ideal in $P = K[x_1, \ldots, x_n]$. Then the affine algebra P/I satisfies*

$$\dim(P/I) = \operatorname{Kdim}(P/I)$$

In particular, the dimension of an affine algebra P/I is an invariant which does not depend the choice of the presentation.

Proof. First we show $\operatorname{Kdim}(P/I) \leq \dim(P/I)$ by induction on $\operatorname{Kdim}(P/I)$. The case $\operatorname{Kdim}(P/I) = 0$ is taken care of by Proposition 5.6.30. Now consider the case $d = \operatorname{Kdim}(P/I) > 0$. By Proposition 5.6.32, we may assume that I is a prime ideal. Let $(0) = \mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_d$ be a maximal chain of prime ideals in P/I. Every maximal chain of prime ideals in $(P/I)/\mathfrak{p}_1$ starts with the zero ideal. By taking preimages in P/I and prolongating the chain with $\mathfrak{p}_0$, we get a chain of prime ideals in P/I of length one greater. This shows that we have $\operatorname{Kdim}((P/I)/\mathfrak{p}_1) = \operatorname{Kdim}(P/I) - 1$. Thus the inductive hypothesis yields $\operatorname{Kdim}((P/I)/\mathfrak{p}_1) \leq \dim((P/I)/\mathfrak{p}_1)$. Let $f \in P \setminus I$ be a polynomial whose residue class is contained in $\mathfrak{p}_1 \setminus \{0\}$. Then f is a non-zerodivisor for P/I, and Propositions 5.6.12.c, 5.4.8.a, and 5.6.33.c imply $\dim((P/I)/\mathfrak{p}_1) \leq \dim(P/(I+(f))) \leq \dim(P/I) - 1$. Combining everything, we see that

$$\begin{aligned} \operatorname{Kdim}(P/I) - 1 &= \operatorname{Kdim}((P/I)/\mathfrak{p}_1) \leq \dim((P/I)/\mathfrak{p}_1) \\ &\leq \dim(P/(I+(f))) \leq \dim(P/I) - 1 \end{aligned}$$

Next we prove $\dim(P/I) \leq \operatorname{Kdim}(P/I)$ by induction on $\operatorname{Kdim}(P/I)$. The case $\operatorname{Kdim}(P/I) = 0$ follows again from Proposition 5.6.30. Now consider the case $\operatorname{Kdim}(P/I) > 0$. By the first part of the proof, this implies $\dim(P/I) > 0$. In view of Proposition 5.6.32, we may again assume that I is a prime ideal. Let $W = (1\ 1\ \cdots\ 1) \in \operatorname{Mat}_{1,n}(\mathbb{Z})$. By Proposition 5.6.3.b, we have $\dim(P/\operatorname{DF}_W(I)) = \dim(P/I) > 0$. We apply Proposition 5.6.26 to the ring P and the ideal $\operatorname{DF}_W(I)$. Since this ideal is not zero-dimensional, we get a homogeneous polynomial $f \in P$ which is an almost non-zerodivisor for $P/\operatorname{DF}_W(I)$. Then Proposition 5.6.34 implies that f is an almost non-zerodivisor for P/I and $\dim(P/(I+(f))) = \dim(P/I) - 1$. The inductive hypothesis yields $\dim(P/(I+(f)) \leq \operatorname{Kdim}(P/(I+(f)))$. Finally, we note that Corollary 5.6.31 shows $f \notin I$, and therefore Lemma 5.6.35 says that

we have the inequality $\operatorname{Kdim}(P/(I+(f))) \leq \operatorname{Kdim}(P/I) - 1$. Altogether, it follows that

$$\dim(P/I) - 1 = \dim(P/(I+(f))) \leq \operatorname{Kdim}(P/(I+(f))) \leq \operatorname{Kdim}(P/I) - 1$$

as we wanted to show. The additional claim follows from the observation that $\operatorname{Kdim}(P/I)$ is independent of the presentation since it refers only to chains of prime ideals in the ring P/I. □

Exercise 1. Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let $I \subseteq P$ be an ideal, and let $\overline{P} = K[x_0, \ldots, x_n]$ be standard graded. By Proposition 4.3.5.f, the element x_0 is a non-zerodivisor for $\overline{P}/I^{\text{hom}}$.

a) Show that $x_0 - 1$ is a non-zerodivisor for $\overline{P}/I^{\text{hom}}$.
b) Construct a short exact sequence of K-algebras

$$0 \longrightarrow \overline{P}/I^{\text{hom}} \xrightarrow{\mu} \overline{P}/I^{\text{hom}} \xrightarrow{\varepsilon} P/I \longrightarrow 0$$

where μ is induced by multiplication by $x_0 - 1$, and ε is induced by dehomogenization with respect to x_0.
c) Given $i \in \mathbb{Z}$, restrict the above sequence to the vector spaces generated by elements of degree $\leq i-1$ and $\leq i$, respectively. Show that this yields an exact sequence of finite dimensional K-vector spaces

$$0 \longrightarrow \langle \overline{P}_{\leq i-1} \rangle / \langle I^{\text{hom}}_{\leq i-1} \rangle \xrightarrow{\mu} \langle \overline{P}_{\leq i} \rangle / \langle I^{\text{hom}}_{\leq i} \rangle \xrightarrow{\varepsilon} \langle P_{\leq i} \rangle / \langle I_{\leq i} \rangle \longrightarrow 0$$

d) Using this sequence, prove the formula $\operatorname{HF}^a_{P/I}(i) = \operatorname{HF}_{\overline{P}/I^{\text{hom}}}(i)$ in an alternative way (see Proposition 5.6.3.c).

Exercise 2. Write CoCoA functions `AffineHS1`(...) and `AffineHS2`(...) which implement the two methods for computing affine Hilbert series suggested by the two parts of Proposition 5.6.7. Apply your functions to compute the affine Hilbert series of the algebras $\mathbb{Q}[x, y, z]/I_i$ for the following ideals I_i. Compare their results and their timings.

a) $I_1 = (x - 2z^4,\ y - 3z^5)$
b) $I_2 = (x^2 - y,\ xy - z,\ xz - y^2)$
c) $I_3 = (x^2 + y^3 + z^3 - 1,\ x^3 + y^4 + z^5 - 1)$

Exercise 3. Let K be a field, let $n \geq 2$, and let $P = K[x_1, \ldots, x_n]$. Show that $(x_1, \ldots, x_n)^2$ is an $(x_1, \ldots, x_n)$-primary ideal, but it is not irreducible.

Exercise 4. Let R be a Noetherian ring. Show that every prime ideal of R is irreducible, but the converse does not hold in general.

Exercise 5. Let R be a Noetherian ring. Show that every proper ideal of R is contained in a maximal ideal of R. Conclude that every maximal chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_d$ of prime ideals of R starts with a minimal prime $\mathfrak{p}_0$ and ends with a maximal ideal $\mathfrak{p}_d$.

Exercise 6. Let R be an integral domain.

a) Show that R has exactly one minimal prime, namely (0).
b) Prove that a non-zero principal ideal (f) of R is a prime ideal if and only if f is a prime element.
c) Assume that R is a principal ideal domain. Show that every inclusion $\mathfrak{p} \subseteq \mathfrak{q}$ of non-zero prime ideals in R is in fact an equality.

Exercise 7. Let R be a Noetherian ring and I an ideal in R. Show that $\sqrt{I}$ is the intersection of all prime ideals containing I. If you know **Zorn's Lemma**, you may try to prove this for an arbitrary ring R.

Exercise 8. Let R, S be rings, let I be an ideal in R, and let $\varphi : R \longrightarrow S$ be a ring homomorphism.

a) Show that, for every prime ideal $\mathfrak{p}$ of S, its preimage $\varphi^{-1}(\mathfrak{p})$ is a prime ideal of R.
b) Show that the prime ideals of R containing I are in 1-1 correspondence with the prime ideals of R/I.
c) Prove that the maximal ideals of R containing I are in 1-1 correspondence with the maximal ideals of R/I.
d) Conclude that $\mathrm{Kdim}(R) \geq \mathrm{Kdim}(R/I)$.

Exercise 9. Using the Chinese Remainder Theorem 3.7.4, show that the following conditions are equivalent for a reduced Noetherian ring R.

a) The ring R is the direct product of finitely many fields.
b) We have $\mathrm{Kdim}(R) = 0$.

Tutorial 76: The Multiplicity of an Affine Algebra

Research is what I'm doing
when I don't know what I'm doing.
(Wernher von Braun)

Using the affine Hilbert polynomial, we have defined the multiplicity of an affine algebra. In this tutorial we want to research this number further. Although we don't know yet what we'll be doing with this research, we shall look for connections between the multiplicities of different affine algebras, explicit formulas for the multiplicity of special rings, and efficient ways to compute them.

Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let $I \subset P$ be an ideal.

a) Show that the multiplicity of an affine algebra depends on the choice of a presentation. In other words, given another ring $P' = K[y_1, \ldots, y_m]$ and an ideal $I' \subset P'$, it is possible to have an isomorphism of K-algebras $P/I \cong P'/I'$ even though $\mathrm{mult}(P/I) \neq \mathrm{mult}(P'/I')$.
Hint: Consider $K[x, y, z]/(z - x^2)$.
b) Show that we have $\mathrm{mult}(P/I) = \dim_K(P/I) < \infty$ if $\dim(P/I) = 0$.
c) Deduce the formula $\mathrm{mult}(P/I) = \mathrm{mult}(P/\sqrt{I}) + \dim_K(\sqrt{I}/I)$ under the assumption that $\dim(P/I) = 0$, and exhibit an example with $\dim(P/I) > 0$ for which this formula does not hold.

d) Let $d = \dim(P/I)$, and let $I \subset P$ be a radical ideal. Write $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$ with distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of P. Prove the formula

$$\operatorname{mult}(P/I) = \sum_{\{i \mid \dim(P/\mathfrak{p}_i)=d\}} \operatorname{mult}(P/\mathfrak{p}_i)$$

Hint: Use the exact sequences of the proof of Proposition 5.4.9.

e) Assume that P is standard graded. Let $f \in P$ be a polynomial of degree $\delta \geq 1$ such that $\operatorname{DF}(f)$ is a non-zero divisor for $P/\operatorname{DF}(I)$. Show that we have $\operatorname{mult}(P/(I+(f))) = \delta \cdot \operatorname{mult}(P/I)$. (*Hint:* Use Proposition 5.6.12.d.)

f) Exhibit an example showing that in e) it is not sufficient to assume that f alone is a non-zero divisor for P/I.

g) Now assume that K is an infinite field and that $\dim(P/I) \geq 1$. Show that a generic linear polynomial $\ell \in P_{\leq 1}$ satisfies $\operatorname{mult}(P/(I + (\ell))) = \operatorname{mult}(P/I)$.

h) Write a CoCoA function `MultAffineAlg(...)` which takes an ideal I in $P = \mathbb{Q}[x_1, \ldots, x_n]$ and computes the multiplicity of P/I.
Hint: If $\dim(P/I) > 0$, reduce modulo a generically chosen linear polynomial.

i) Use your function `MultAffineAlg(...)` to compute the multiplicities of the following affine algebras.
   1) $\mathbb{Q}[x_1, x_2, x_3]/(x_1x_2,\ x_2x_3,\ x_1x_3)$
   2) $\mathbb{Q}[x_1, \ldots, x_5]/(x_1, \ldots, x_4)^3$
   3) $\mathbb{Q}[x_1, \ldots, x_5]/(x_1x_2^2,\ x_1x_3^2,\ x_1x_4^2,\ x_1x_5^2)$

Tutorial 77: Primary Decomposition of Monomial Ideals

Tell the truth and run.
(Yugoslav Proverb)

In Subsection B we encountered the primary decomposition of an ideal in a Noetherian ring. This raises the question of how to compute the primary decomposition of a polynomial ideal. A special case was treated in Tutorial 43 where we discussed the computation of the primary decomposition of a zero-dimensional polynomial ideal. In this tutorial we study another case where primary decompositions can be computed efficiently, namely the case of monomial ideals. Alas, the sword of Damocles is still hanging above us: although knowledge of the primary decomposition of a polynomial ideal is usually valuable, acquiring it is one of the most difficult tasks in Computational Commutative Algebra and is prone to overwhelm your computer. Having told this truth, we turn back to the monomial ideal case and delay facing the big task until the next section.

Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let $I \subset P$ be a monomial ideal. In the following, we present two methods for computing the primary decomposition of I. The first method is based on the observation that it

is easy to determine a decomposition of I into irreducible monomial ideals by splitting its minimal monomial generators into powers of indeterminates. Then the irreducible components corresponding to the same prime can be recombined by intersecting them. This approach is easy to formulate and implement, but it has the obvious disadvantage of creating a large number of components which then have to be intersected.

The second method uses Alexander duality. This duality is an involution on the set of radical monomial ideals which turns sums into intersections and vice versa. The prime components correspond to the minimal monomial generators of the Alexander dual. Hence we get an algorithm for computing the prime decomposition of a radical monomial ideal, and the general case can be reduced to it by the isolation of primary components explained in Tutorial 43.g.

a) Show that the ideal I is a prime ideal if and only if it is of the form $I = (x_{i_1}, \ldots, x_{i_s})$ with $1 \leq i_1 < \cdots < i_s \leq n$.
b) Let $t_1, t_2 \in \mathbb{T}^n$ be two coprime terms. Prove that $I = (I + (t_1)) \cap (I + (t_2))$.
c) Using b), show that if I is irreducible, it is of the form $I = (x_{i_1}^{\alpha_1}, \ldots, x_{i_s}^{\alpha_s})$ with $1 \leq i_1 < \cdots < i_s \leq n$ and $\alpha_1, \ldots, \alpha_s \in \mathbb{N}_+$.
Note: The converse implication is also true. This will be shown in Proposition 6.2.11.
d) Write a CoCoA function `MonIrredDecomp(...)` which takes a monomial ideal I and computes a decomposition of I into irreducible ideals.
Hint: Use b) and c).
e) Apply your function `MonIrredDecomp(...)` to compute a decomposition of the following monomial ideals into irreducible monomial ideals.
   1) $I_1 = (x_1 x_2^2 x_3^3,\ x_2 x_3^2 x_4^3,\ x_1 x_3^2 x_4^3) \subset \mathbb{Q}[x_1, x_2, x_3, x_4]$
   2) $I_2 = (x_1^3 x_2^3,\ x_2^3 x_3^3, \ldots, x_8^3 x_9^3) \subset \mathbb{Q}[x_1, \ldots, x_9]$
   3) $I_3 = (x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_9 \mid i = 1, \ldots, 9) \subset \mathbb{Q}[x_1, \ldots, x_9]$
f) Write a CoCoA function `MonPrimDecomp(...)` which finds the primary decomposition of a monomial ideal in the following way: first compute a decomposition into irreducible monomial ideals, and then combine the irreducible ideals having the same radical using the function `MonIntersection(...)` of Tutorial 8.
g) Apply your function `MonPrimDecomp(...)` to the ideals in e).

In the following we let $\mathfrak{R}$ be the set of all radical monomial ideals of P. The map $\varphi : \mathfrak{R} \longrightarrow \mathfrak{R}$ which sends $(x_1^{\alpha_{11}} \cdots x_n^{\alpha_{1n}}, \ldots, x_1^{\alpha_{s1}} \cdots x_n^{\alpha_{sn}})$ to $\cap_{i=1}^{s} (x_1^{\alpha_{i1}}, \ldots, x_n^{\alpha_{in}})$ is called **Alexander duality**.

h) Show that $\mathfrak{R}$ is closed under finite sums and intersections. Conclude that φ is well-defined.
i) Prove that we have $\varphi^2(I) = I$ for every $I \in \mathfrak{R}$. Deduce that φ is bijective.
j) Let $I_1, \ldots, I_r \in \mathfrak{R}$. Show that the map φ satisfies $\varphi(I_1 + \cdots + I_r) = \varphi(I_1) \cap \cdots \cap \varphi(I_r)$ and $\varphi(I_1 \cap \ldots \cap I_r) = \varphi(I_1) + \cdots + \varphi(I_r)$.

k) Let $\mathfrak{I}$ be the set of all monomial ideals in P, and let $\Phi : \mathfrak{I} \longrightarrow \mathfrak{I}$ be the map obtained by extending the definition of φ to all elements of $\mathfrak{I}$. Find examples which show that the map Φ does not share the properties in i) and j).

l) Write a CoCoA function `AlexDual(...)` which takes a monomial ideal I and computes $\Phi(I)$.

m) Apply your function `AlexDual(...)` to compute the Alexander duals of the following monomial ideals.

1) $J_1 = (x_1x_2x_3,\ x_2x_3x_4,\ x_1x_3x_4) \subset \mathbb{Q}[x_1, x_2, x_3, x_4]$
2) $J_2 = (x_1x_2,\ x_2x_3, \ldots, x_8x_9) \subset \mathbb{Q}[x_1, \ldots, x_9]$
3) $J_3 = (x_1x_2 \cdots x_{i-1}x_{i+1} \cdots x_9 \mid i = 1, \ldots, 9) \subset \mathbb{Q}[x_1, \ldots, x_9]$

n) A radical monomial ideal I with $\varphi(I) = I$ is called **self-dual**. Using your function `AlexDual(...)` or calculating by hand, prove that the monomial ideal

$$\begin{aligned} I \;=\; & (x_1x_2x_3,\ x_1x_2x_4,\ x_1x_3x_5,\ x_2x_4x_5,\ x_3x_4x_5, \\ & x_2x_3x_6,\ x_1x_4x_6,\ x_3x_4x_6,\ x_1x_5x_6,\ x_2x_5x_6) \end{aligned}$$

in $\mathbb{Q}[x_1, \ldots, x_6]$ is self-dual.

o) Using CoCoA, find all self-dual radical monomial ideals in $\mathbb{Q}[x_1, \ldots, x_6]$ which are minimally generated by ten terms of degree three.
Hint: Use the CoCoA function `Subsets(...)`.

p) Given $I \in \mathfrak{R}$ and $J = \varphi(I)$, prove that the largest degree of a minimal monomial generator of J is $n - \dim(P/I)$. Moreover, explain how one can get the associated primes of I from the minimal monomial generators of J.

q) Write CoCoA functions `AlexDim(...)` and `AlexPrimDecomp(...)` which compute the dimension and the primary decomposition of a radical monomial ideal using Alexander duality. Apply your functions to the ideals in m) and n).

5.7 Independent Sets of Indeterminates

Exercise 1. *What is* $(x-a)(x-b)\cdots(x-z)$ *?*
(Anonymous)

Sometimes it has to get very dark
before you see the light.
(Indian Proverb)

In the preceding section we proved that the dimension of an affine algebra, as defined via its affine Hilbert function, coincides with its Krull dimension, i.e. with a more geometric notion of dimension defined via chains of prime ideals. In this section we study another notion of dimension with a somewhat different geometric background: a d-dimensional affine variety should have a component which looks locally like a d-dimensional affine space. Thus there should be a projection onto a d-dimensional affine space which is locally an isomorphism. Algebraically, this idea corresponds to the combinatorial dimension of an affine algebra (see Subsection A) and to Noether Normalizations (see Tutorial 78). In fact, we shall see that to introduce dimension theory via maximal sets of independent indeterminates yields a surprisingly simple yet powerful approach.

But let us try do to things in chronological order — it is less confusing that way! Given an affine algebra P/I, where $P = K[x_1, \ldots, x_n]$ is a polynomial ring over a field K and I is a proper ideal in P, a set of indeterminates Y is said to be *independent* modulo I if the canonical map $K[Y] \longrightarrow P/I$ is injective. The maximal size of an independent set of indeterminates is called the *combinatorial dimension* of P/I. In the first subsection we prove that the combinatorial dimension of an affine algebra equals its dimension. Since we also provide algorithms for computing the combinatorial dimension, fresh light is shed on dimension theory, and we discover new paths leading deeper into its thicket.

In the second subsection we link independent sets of indeterminates to algebraically independent sets of elements and to *transcendence bases*. Despite their awe-inspiring name, you do not really need to resort to transcendental meditation to grasp the concept. Moreover, they provide the last link in our long chain comprising the different facets of dimension investigated so far. Finally, in the tutorials you will have the opportunity to construct special injective homomorphisms $K[Y] \longrightarrow P/I$ called Noether normalizations (see Tutorial 78) and to compute primary decompositions of ideals (see Tutorial 79). The latter is a natural continuation and generalization of Tutorial 43 where only zero-dimensional ideals are considered.

In the following we let K be a field, let $P = K[x_1, \ldots, x_n]$, and let I be a proper ideal in P. For every subset $Y \subseteq \{x_1, \ldots, x_n\}$, we denote the polynomial ring $K[x_i \mid x_i \in Y]$ by $K[Y]$ and the ideal $(x_i \mid x_i \in Y)$ by (Y).

5.7.A The Combinatorial Dimension of an Affine Algebra

Our immediate agenda is to examine the following concepts.

Definition 5.7.1. Let $Y \subseteq \{x_1, \ldots, x_n\}$ be a set of indeterminates.

a) The set Y is said to be **independent modulo** I or an **independent set of indeterminates modulo** I if $I \cap K[Y] = (0)$.
b) The set Y is called a **maximal independent set modulo** I if Y is independent modulo I and there is no set $Z \subseteq \{x_1, \ldots, x_n\}$ independent modulo I with $Y \subset Z$.
c) The largest number of elements of a maximal independent set of indeterminates modulo I is called the **combinatorial dimension** of P/I and is denoted by $\operatorname{cdim}(P/I)$.

Another way of phrasing the definition of an independent set Y modulo I is to say that the canonical K-algebra homomorphism $K[Y] \longrightarrow P/I$ has to be injective. The main goal of this subsection is to prove that the combinatorial dimension of P/I equals its dimension. The following example shows it is not true that all maximal independent sets of indeterminates modulo I have the same number of elements. But later we prove that this is true for a prime ideal I.

Example 5.7.2. Let $P = \mathbb{Q}[x, y, z]$ and $I = (x - xy,\ x - xz)$. Then we have $I \cap \mathbb{Q}[x] = (0)$. The set $\{x\}$ is a maximal independent set modulo I, since $I \cap \mathbb{Q}[x, y] = (x - xy)$ and $I \cap \mathbb{Q}[x, z] = (x - xz)$. Moreover, the equality $I \cap \mathbb{Q}[y, z] = (0)$ implies that also the set $\{y, z\}$ is a maximal independent sets modulo I.

In some cases the combinatorial dimension is easy to determine.

Example 5.7.3. Let $m \in \{0, \ldots, n-1\}$, let $Y \subset \{x_1, \ldots, x_n\}$ be a subset consisting of m indeterminates, and let $I = (Y)$. Then $\{x_1, \ldots, x_n\} \setminus Y$ is a maximal independent set modulo I which has the largest possible number of elements, and we have $\operatorname{cdim}(P/I) = n - m$. In particular, we get $\operatorname{cdim}(P) = n$.

Before studying combinatorial dimension further, we need to get a better understanding of independent sets of indeterminates. Theorem 3.4.5 on the computation of elimination modules allows us to characterize them as follows.

Remark 5.7.4. Let $Y \subseteq \{x_1, \ldots, x_n\}$ be a set of indeterminates. Then the following conditions are equivalent.

a) The set Y is independent modulo I.
b) For every elimination ordering σ for $\{x_1, \ldots, x_n\} \setminus Y$ and for every σ-Gröbner basis G of I, we have $G \cap K[Y] = \emptyset$.
c) There is an elimination ordering σ for $\{x_1, \ldots, x_n\} \setminus Y$ and a σ-Gröbner basis G of I such that $G \cap K[Y] = \emptyset$.

In particular, for a monomial ideal I, the set Y is independent modulo I if and only if no term in I is a product of indeterminates solely from Y.

Using these equivalences, we have an effective way to check whether a given set of indeterminates is independent modulo I. Thus we can compute the combinatorial dimension of an affine algebra as follows.

Proposition 5.7.5. *Let I be a proper ideal in P. Consider the following instructions.*

1) *Let $d = 0$ and $L_0 = \{\emptyset\}$.*
2) *Form the set L_{d+1} consisting of all sets $Y' \cup \{x_i\}$ with $Y' \in L_d$ and $i \in \{1, \ldots, n\}$ being larger than any of the indices of the indeterminates in Y'.*
3) *For each set $Y \in L_{d+1}$ check whether Y is independent modulo I. If not, delete Y from L_{d+1}.*
4) *If $L_{d+1} = \emptyset$, return (d, L_d) and stop. Otherwise, increase d by one and continue with step 2).*

This is an algorithm which computes $d = \operatorname{cdim}(P/I)$ and the set L_d of all maximal independent sets of indeterminates Y modulo I with $\#Y = d$.

Proof. Since finiteness is obvious, it suffices to prove correctness. After step 4) is finished, the set L_d contains only independent sets modulo I consisting of d elements. We claim that the returned set L_d contains all maximal independent sets modulo I of length $d = \operatorname{cdim}(P/I)$. Indeed, given any such set $Y = \{x_{i_1}, \ldots, x_{i_d}\}$, where $1 \leq i_1 < \cdots < i_d \leq n$, we can form a chain $\emptyset \subset \{x_{i_1}\} \subset \cdots \subset \{x_{i_1}, \ldots, x_{i_d}\}$ of independent sets modulo I such that each set in the chain is found and appended to L_{d+1} in one of the iterations of step 2).

Conversely, we claim that the returned set L_d contains only maximal independent sets Y modulo I. Let $Y \in L_d$, and let $x_m \in Y$ be the indeterminate having the largest index. Clearly, $L_{d+1} = \emptyset$ implies that Y cannot be extended to an independent set using an indeterminate x_i with $i > m$. Furthermore, a possible extension using another indeterminate would lead to another subset of L_d which could be extended by x_m, in contradiction to the fact that $L_{d+1} = \emptyset$. Thus the algorithm returns the correct result. □

Although this algorithm is correct, it is not efficient. In adverse cases it may require up to $2^n - 1$ Gröbner basis calculations to do its job. In Corollary 5.7.10 and Tutorial 78 we shall see more efficient ways to compute maximal sets of indeterminates modulo I.

In the meantime, we describe some properties of the combinatorial dimension. They will be of use later.

Proposition 5.7.6. (Properties of the Combinatorial Dimension) *Let $P = K[x_1, \ldots, x_n]$, let I be a proper ideal in P, and let Y be a subset of $\{x_1, \ldots, x_n\}$.*

a) We have $\operatorname{cdim}(P/I) = 0$ if and only if $\dim(P/I) = 0$.
b) If $J \subseteq I$ is another ideal of P and Y is independent modulo I then Y is independent modulo J. Consequently, we have $\operatorname{cdim}(P/J) \geq \operatorname{cdim}(P/I)$.
c) Let σ be a term ordering on $\mathbb{T}^n$. If the set Y is an independent set modulo $\operatorname{LT}_\sigma(I)$ then it is independent modulo I. Consequently, we have $\operatorname{cdim}(P/\operatorname{LT}_\sigma(I)) \leq \operatorname{cdim}(P/I)$.
d) Let $i \geq 1$. The set Y is independent modulo I if and only if it is independent modulo I^i. Thus we have $\operatorname{cdim}(P/I^i) = \operatorname{cdim}(P/I) = \operatorname{cdim}(P/\sqrt{I})$.
e) Let J be another proper ideal in P. The set Y is an independent set modulo $I \cap J$ if and only if it is independent modulo I or modulo J. Thus we have $\operatorname{cdim}(P/I \cap J) = \max\{\operatorname{cdim}(P/I), \operatorname{cdim}(P/J)\}$.

Proof. First we show a). By Proposition 5.6.30 and the Finiteness Criterion 3.7.1, the condition $\dim(P/I) = 0$ is equivalent to $I \cap K[x_i] \neq (0)$ for $i = 1, \ldots, n$, and this is precisely the definition of $\operatorname{cdim}(P/I) = 0$. To prove b), it suffices to note that $I \cap K[Y] = (0)$ implies $J \cap K[Y] = (0)$. Therefore, if Y is independent modulo I, it is also independent modulo J.

Next we show c). Suppose that Y is not independent modulo I. Hence there exists a non-zero polynomial $f \in I \cap K[Y]$. Then its leading term is a non-zero polynomial in $\operatorname{LT}_\sigma(I) \cap K[Y]$ and Y is not independent modulo $\operatorname{LT}_\sigma(I)$. For the proof of one implication in d), we can use $I^i \subseteq I$ and b). Conversely, assume that $I^i \cap K[Y] = (0)$ and $f \in I \cap K[Y]$. Then we have $f^i \in I^i \cap K[Y]$, and therefore $f^i = 0$. This implies $f = 0$, and consequently $I \cap K[Y] = (0)$. The second claim follows from the fact that there exists a number $i \geq 1$ such that $I^i \subseteq \sqrt{I}^{\,i} \subseteq I$.

Finally, we prove e). Clearly, $I \cap K[Y] = (0)$ implies $I \cap J \cap K[Y] = (0)$. Conversely, assume that $I \cap J \cap K[Y] = (0)$ and $I \cap K[Y] \neq (0)$. Let f be a non-zero polynomial in $I \cap K[Y]$. For every $g \in J \cap K[Y]$, we then find $fg \in I \cap J \cap K[Y] = (0)$, i.e. we have $fg = 0$. Thus we see that $g = 0$ and $J \cap K[Y] = (0)$. Therefore we have the inequality $\operatorname{cdim}(P/I \cap J) \leq \max\{\operatorname{cdim}(P/I), \operatorname{cdim}(P/J)\}$, and the other inequality follows from b). □

The converse of part c) of this proposition is not true in general, as the following example shows.

Example 5.7.7. Let $P = K[x, y]$, let $I = (x^2+y^2)$, and let $\sigma = \texttt{DegRevLex}$. Then $\{x\}$ is a maximal independent set modulo I, but it is not independent modulo $\operatorname{LT}_\sigma(I) = (x^2)$.

Our next proposition provides a nice description of the radical and the combinatorial dimension of a monomial ideal. In fact, it constitutes one of the reasons for calling $\operatorname{cdim}(P/I)$ the combinatorial dimension of I. Namely, the

combinatorial dimension of a monomial ideal is a number given by a simple combinatorial formula.

Proposition 5.7.8. (Combinatorial Dimension of Monomial Ideals) *Let I be a proper monomial ideal in P.*

a) We have $\sqrt{I} = \bigcap_{Y \subseteq \{x_1,\ldots,x_n\},\, \sqrt{I} \subseteq (Y)} (Y)$.

b) We have $\operatorname{cdim}(P/I) = n - \min\{\#Y \mid I \subseteq (Y) \subseteq \{x_1, \ldots, x_n\}\}$.

c) We have $\operatorname{cdim}(P/I) = \dim(P/I)$.

Proof. First we show a). It is clear that $\sqrt{I}$ is contained in the right-hand side. To prove the reverse inclusion, let $\{t_1, \ldots, t_s\}$ be the minimal monomial system of generators of $\sqrt{I}$. By Corollary 4.1.12, the set $\{t_1, \ldots, t_s\}$ consists of squarefree terms. For a contradiction, assume that some term $t \in \mathbb{T}^n$ is contained in the right-hand side, but not in $\sqrt{I}$. For every $i \in \{1, \ldots, s\}$, there exists an index $\nu_i \in \{1, \ldots, n\}$ such that x_{ν_i} divides t_i, but not t. Thus we have $t \notin (x_{\nu_1}, \ldots, x_{\nu_s})$ and $\sqrt{I} = (t_1, \ldots, t_s) \subseteq (x_{\nu_1}, \ldots, x_{\nu_s})$, in contradiction with our assumption.

In view of Proposition 5.7.6.d, it suffices to prove b) for a radical ideal I, since we have $I \subseteq (Y)$ if and only if $\sqrt{I} \subseteq (Y)$. In that case the claim follows from a), Example 5.7.3, and Proposition 5.7.6.e because

$$\begin{aligned} \operatorname{cdim}(P/I) &= \max\{\operatorname{cdim}(P/(Y)) \mid Y \subseteq \{x_1, \ldots, x_n\} \text{ and } I \subseteq (Y)\} \\ &= \max\{n - \#Y \mid Y \subseteq \{x_1, \ldots, x_n\} \text{ and } I \subseteq (Y)\} \\ &= n - \min\{\#Y \mid Y \subseteq \{x_1, \ldots, x_n\} \text{ and } I \subseteq (Y)\} \end{aligned}$$

yields the formula we were looking for.

Finally we show c). By Propositions 5.7.6.d and 5.4.8.c, it suffices to prove the claim for the radical monomial ideal $\sqrt{I}$. Using a) together with Propositions 5.4.9.b and 5.7.6.e, we see that we can even assume that I is generated by a subset of $\{x_1, \ldots, x_n\}$. Now the claim follows from Examples 5.4.3 and 5.7.3. □

Based on this proposition, we are ready to prove the equality of the dimension and the combinatorial dimension of an affine algebra in full generality.

Theorem 5.7.9. (Combinatorial Dimension of Affine Algebras) *Let $P = K[x_1, \ldots, x_n]$, and let I be a proper ideal in P. Then the affine algebra P/I satisfies* $\operatorname{cdim}(P/I) = \dim(P/I)$.

In particular, the combinatorial dimension of an affine algebra does not depend on the choice of presentation.

Proof. The inequality $\operatorname{cdim}(P/I) \geq \dim(P/I)$ follows by combining Propositions 5.7.6.c, 5.7.8.c, and 5.4.14.e. To prove the reverse inequality, we let $d = \dim(P/I)$. For a contradiction, we assume that there exists a set of indeterminates $Y \subseteq \{x_1, \ldots, x_n\}$ such that Y is independent modulo I and

$\#Y = d+1$. Then the injective K-algebra homomorphism $K[Y] \hookrightarrow P/I$ shows that we have $\mathrm{HF}^a_{P/I}(i) \geq \mathrm{HF}^a_{K[Y]}(i) = \binom{d+1+i}{d+1}$ for all $i \in \mathbb{Z}$. Therefore $\mathrm{HP}^a_{P/I}(t)$ is a polynomial of degree $\geq d+1$, in contradiction to the fact that $d = \dim(P/I) = \deg(\mathrm{HP}^a_{P/I}(t))$. □

This theorem allows us to compute dimensions and maximal independent sets of indeterminates in a more efficient manner.

Corollary 5.7.10. (Computation of the Combinatorial Dimension) *Let I be a proper ideal in P, and let σ be a degree compatible term ordering on $\mathbb{T}^n$.*

a) We have $\dim(P/\operatorname{LT}_\sigma(I)) = \dim(P/I)$.

b) Consider the following instructions.

1) Compute $\operatorname{LT}_\sigma(I)$ *using Buchberger's Algorithm.*

2) Compute the minimal monomial system of generators $\{t_1, \ldots, t_s\}$ *of* $\sqrt{\operatorname{LT}_\sigma(I)}$ *by taking the squarefree parts of the terms in a monomial set of generators of* $\operatorname{LT}_\sigma(I)$ *and by deleting those terms which are proper multiples of others.*

3) Apply the procedure `IndepSet`(Y,T) *to the sets* $Y = \{x_1, \ldots, x_n\}$ *and* $T = \{t_1, \ldots, t_s\}$. *Return its result and stop.*

Here `IndepSet`(Y,T) *is the recursive procedure defined by the following steps.*

I1) If $T = \emptyset$ *then return* Y *and stop.*

I2) For each $x_i \in Y$ *dividing* t_1, *let* $T_i = \{t \in T \mid x_i \text{ does not divide } t\}$. *Call the procedure* `IndepSet`$(Y \setminus \{x_i\}, T_i)$ *and denote its result by* L_i.

I3) Let L_j *be one of the sets* L_i *having the largest number of elements. Return* $L_j \cup \{x_i\}$ *and stop.*

This is an algorithm which computes a maximal independent set Y modulo I having the largest number of elements. In particular, it computes the combinatorial dimension $\operatorname{cdim}(P/I) = \#Y$.

Proof. To prove a), we introduce a homogenizing indeterminate x_0 and let $\overline{P} = K[x_0, x_1, \ldots, x_n]$. Now Lemma 4.3.16.c shows $\operatorname{LT}_{\overline{\sigma}}(I^{\mathrm{hom}}) = \operatorname{LT}_\sigma(I)\,\overline{P}$. Since we have $\overline{P}/\operatorname{LT}_\sigma(I)\,\overline{P} \cong (P/\operatorname{LT}_\sigma(I))[x_0]$, we see that x_0 is a non-zero divisor modulo $\operatorname{LT}_\sigma(I)\overline{P}$. By Proposition 5.4.6, we have $\dim(P/\operatorname{LT}_\sigma(I)) = \dim(\overline{P}/\operatorname{LT}_\sigma(I)\,\overline{P}) - 1 = \dim(\overline{P}/\operatorname{LT}_{\overline{\sigma}}(I^{\mathrm{hom}})) - 1$. Now Proposition 5.4.5.e yields $\dim(\overline{P}/\operatorname{LT}_{\overline{\sigma}}(I^{\mathrm{hom}})) = \dim(\overline{P}/I^{\mathrm{hom}})$. Hence the claim follows from Proposition 5.6.12.c.

To prove b), we note that a) and the theorem imply that it suffices to compute an independent set of indeterminates modulo $\operatorname{LT}_\sigma(I)$ which consists of $d = \dim(P/\operatorname{LT}_\sigma(I))$ elements. In the light of Proposition 5.7.8, it is clear that it suffices to do this for $\sqrt{\operatorname{LT}_\sigma(I)}$ instead. Hence we have to show that the recursive procedure `IndepSet`(Y,T) is an algorithm which computes a maximal independent set modulo $J = \sqrt{\operatorname{LT}_\sigma(I)}$ consisting of $\dim(P/J)$ elements.

First we observe that the recursive procedure is finite, because its recursive calls are applied to pairs (Y,T) where T has fewer elements. Thus we eventually arrive at $T=\emptyset$ and step I1) returns a result. Then we point out that step I1) returns the correct result if $J=(0)$, namely $Y=\{x_1,\ldots,x_n\}$. Next we note that

$$J=\bigcap_{x_i|t_1}(J+(x_i))=\bigcap_{x_i|t_1}(x_i,t_2,\ldots,t_s)=\bigcap_{x_i|t_1}((x_i)+(t_j\mid x_i\nmid t_j))$$

As a consequence of these equalities and Proposition 5.7.6.e, it suffices to compute a maximal independent set of indeterminates modulo each of the ideals $((x_i)+(t_j\mid x_i\nmid t_j))$ with $x_i\mid t_1$ and to take one having the largest number of elements. Such a set consists of x_i and a maximal independent set of indeterminates modulo $(t_j\mid x_i\nmid t_j)$ which has to be chosen from $Y\setminus\{x_i\}$. And this is exactly what is computed in steps I2) and I3). Hence the recursive procedure `IndepSet`(Y,T) is correct and we are done. □

Let us use part b) of this corollary to compute some combinatorial dimensions.

Example 5.7.11. Let K be a field and $P=K[x,y,z]$.

a) Let $I=(x^2+y^2+z^2)$. Using $\sigma=$ `DegLex`, we calculate $\mathrm{LT}_\sigma(I)=(x^2)$ and $\sqrt{\mathrm{LT}_\sigma(I)}=(x)$. Then we set $Y=\{x,y,z\}$ and $T=\{x\}$ in step 3). Now step I2) says that we have to compute `IndepSet`$(\{y,z\},\emptyset)$ recursively, and step I1) yields `IndepSet`$(\{y,z\},\emptyset)=\{y,z\}$. Hence step I3) returns `IndepSet`$(Y,T)=\{y,z\}$. Thus the output of the algorithm is that $\{y,z\}$ is a maximal independent set modulo I. Consequently, we have $\dim(P/I)=2$.

b) Let $I=(xy^2-x,\ y^2z-z)$. Using $\sigma=$ `DegRevLex`, we calculate $\mathrm{LT}_\sigma(I)=(xy^2,\ y^2z)$ and $\sqrt{\mathrm{LT}_\sigma(I)}=(xy,yz)$. Then we set $Y=\{x,y,z\}$ and $T=\{xy,yz\}$ in step 3). Now step I2) says that we have to compute $L_1=$ `IndepSet`$(\{y,z\},\{yz\})$ and $L_2=$ `IndepSet`$(\{x,z\},\emptyset)$ recursively. In the first case, step I2) requires further recursive calls for computing `IndepSet`$(\{z\},\emptyset)$ and `IndepSet`$(\{y\},\emptyset)$. Here the answers are $\{z\}$ and $\{y\}$, respectively, so that we can choose $L_1=\{z\}$ in step I3). In the second case, step I1) immediately returns $L_2=\{x,z\}$. Therefore we have to choose L_2 in step I3) now, and the algorithm returns `IndepSet`$(Y,T)=\{x,z\}$. Altogether, we find that $\{x,z\}$ is a maximal independent set modulo I and $\dim(P/I)=2$.

First secure an independent income,
then practice virtue.
(Greek Proverb)

5.7.B Transcendence Degrees

The Transcendental Field,
purified of all egological structure,
recovers its primary transparency.
(Jean-Paul Sartre)

The last topic of this section is yet another interpretation of the dimension of an affine K-algebra – namely as the maximal number of algebraically independent elements over K. The following definition introduces the necessary terminology. In particular, the notion of a transcendence basis of a field extension becomes transparent.

Definition 5.7.12. Let R be a K-algebra, and let $d \in \mathbb{N}_+$.

a) A set of elements $r_1, \ldots, r_d \in R$ is called **algebraically independent** over K if the only polynomial $f \in K[y_1, \ldots, y_d]$ with $f(r_1, \ldots, r_d) = 0$ is $f = 0$.
b) Let L/K be a field extension. A set of d elements $r_1, \ldots, r_d \in L$ is called a (finite) **transcendence basis** of L/K if $\{r_1, \ldots, r_d\}$ is algebraically independent over K and there exists no element $r_{d+1} \in L \setminus \{r_1, \ldots, r_d\}$ such that $\{r_1, \ldots, r_{d+1}\}$ is algebraically independent over K.

If a field extension L/K has a finite transcendence basis then all transcendence bases of L/K have the same number of elements. This result is analogous to the fact that two bases of a finitely generated K-vector space have the same number of elements. It can be proved as follows.

Proposition 5.7.13. *Let L/K be a field extension, let $d \in \mathbb{N}_+$, and let $r_1, \ldots, r_d \in L$ be d distinct elements.*

a) The set $\{r_1, \ldots, r_d\}$ is a transcendence basis of L/K if and only if $\{r_1, \ldots, r_d\}$ is algebraically independent over K and L is an algebraic field extension of $K(r_1, \ldots, r_d)$.
b) Let $\{r_1, \ldots, r_d\}$ be a transcendence basis of L/K. Then every transcendence basis of L/K consists of d elements.

Proof. To prove the implication "$\Rightarrow$" in a), we let $r_{d+1} \in L$. Since $\{r_1, \ldots, r_{d+1}\}$ is not algebraically independent, there exists a non-zero polynomial $f \in K[y_1, \ldots, y_{d+1}]$ such that $f(r_1, \ldots, r_{d+1}) = 0$. This polynomial has strictly positive degree with respect to y_{d+1}, because $\{r_1, \ldots, r_d\}$ is algebraically independent. Therefore we see that r_{d+1} is algebraic over the field $K(r_1, \ldots, r_d)$. Conversely, let $r_{d+1} \in L$. By hypothesis, this element is algebraic over $K(r_1, \ldots, r_d)$. Thus there is a non-zero polynomial $f \in K(r_1, \ldots, r_d)[y]$ such that $f(r_{d+1}) = 0$. By clearing denominators, we can find a non-zero polynomial $g \in K[y_1, \ldots, y_{d+1}]$ such that $g(r_1, \ldots, r_{d+1}) = 0$. Hence the set $\{r_1, \ldots, r_{d+1}\}$ is not algebraically independent.

Now we show b). Let $B = \{r_1, \ldots, r_d\}$ and $B' = \{r'_1, \ldots, r'_{d'}\}$ be two transcendence bases of L/K. Without loss of generality we may assume that $d' \geq d$. If $d = d'$, we are done. So, suppose that $d' > d$. If B is a subset of B', we immediately get a contradiction to the maximality of B. Otherwise, it suffices to show that we can exchange in B one element of $B \setminus B'$ by an element of B' and still have a transcendence basis. By repeating this process, we can then reach the case $B \subset B'$ eventually. Therefore we now assume that there exists an index $i \in \{1, \ldots, d\}$ such that $r_i \notin B'$.

We claim that there exists an index $j \in \{1, \ldots, d'\}$ such that $B \setminus \{r_i\} \cup \{r'_j\}$ is algebraically independent. If not, all elements $r'_1, \ldots, r'_{d'}$ are algebraic over $K(r_1, \ldots, r_{i-1}, r_{i+1}, \ldots, r_d)$ by a). Since B' is a transcendence basis, the element r_i is algebraic over $K(r'_1, \ldots, r'_{d'})$ by a) again. Hence the element r_i is algebraic over $K(r_1, \ldots, r_{i-1}, r_{i+1}, \ldots, r_d)$, in contradiction to the algebraic independence of B.

Finally, we have to show that $B \setminus \{r_i\} \cup \{r'_j\}$ is a maximal algebraically independent set. Suppose that $r \in L$ is a further element such that $B \setminus \{r_i\} \cup \{r'_j, r\}$ is algebraically independent. It suffices to prove that then one of the sets $B \cup \{r'_j\}$ or $B \cup \{r\}$ is algebraically independent in order to get a contradiction to the maximality of B. Suppose that both $B \cup \{r'_j\}$ and $B \cup \{r\}$ are algebraically dependent. Then r'_j is algebraic over $K(r_1, \ldots, r_d)$, and therefore over $K(r_1, \ldots, r_d, r)$. Moreover, the element r_i is algebraic over $K(r_1, \ldots, r_{i-1}, r_{i+1}, \ldots, r_d, r)$. Hence r'_j is algebraic over that field, in contradiction to the assumption that $B \setminus \{r_i\} \cup \{r'_j, r\}$ is algebraically independent. □

As a consequence of this proposition, we have a new invariant of field extensions.

Definition 5.7.14. Let L/K be a field extension for which there exists a finite transcendence basis $\{r_1, \ldots, r_d\}$. Then the number $\operatorname{trdeg}_K(L) = d$ is called the **transcendence degree** of L/K. If there is no finite transcendence basis, we set $\operatorname{trdeg}_K(L) = \infty$.

Now the dimension of an affine algebra can be characterized as follows.

Proposition 5.7.15. *Let I be a proper ideal in P.*

a) The number $d = \dim(P/I)$ equals the maximal number of algebraically independent elements $\{r_1, \ldots, r_d\}$ in P/I over K.

b) Let I be a prime ideal, and let $Q(P/I)$ be the field of fractions of P/I. Then $d = \dim(P/I)$ is the transcendence degree of $Q(P/I)$ over K, and every maximal independent set of indeterminates modulo I consists of d elements.

Proof. First we show a). By Theorem 5.7.9, there exists an independent set $Y \subseteq \{x_1, \ldots, x_n\}$ modulo I having d elements. Then the K-algebra homomorphism $K[Y] \hookrightarrow P/I$ is injective, and hence the image of the

elements of Y in P/I are algebraically independent over K. This proves that there are d algebraically independent elements in P/I. Now suppose that $r_1, \ldots, r_{d+1} \in P/I$ are algebraically independent elements over K. Let $y_1, \ldots, y_{d+1}$ be indeterminates. Then the K-algebra homomorphism $\varphi : K[y_1, \ldots, y_{d+1}] \longrightarrow P/I$ defined by $y_i \mapsto r_i$ for $i = 1, \ldots, d+1$ is injective. For $i = 1, \ldots, d+1$, let $f_i \in P$ be a representative of minimal degree of r_i, and let $N = \max\{\deg(f_1), \ldots, \deg(f_{d+1})\}$.

At this point we claim that $\varphi(\langle K[y_1, \ldots, y_{d+1}]_{\leq i}\rangle) \subseteq \langle P_{\leq Ni}\rangle / \langle I_{\leq Ni}\rangle$ for all $i \geq 0$. Indeed, let $g \in K[y_1, \ldots, y_{d+1}]$ be a polynomial of degree $\leq i$. Then we have $\varphi(g) = g(r_1, \ldots, r_{d+1}) = g(f_1, \ldots, f_{d+1}) + I$ and $\deg(g(f_1, \ldots, f_{d+1})) \leq N\,i$. This shows $\varphi(g) \in \langle P_{\leq Ni}\rangle / \langle I_{\leq Ni}\rangle$, as claimed. Using this claim, we conclude that $\mathrm{HF}^a_{P/I}(Ni) \geq \mathrm{HF}^a_{K[y_1,\ldots,y_{d+1}]}(i) = \binom{d+1+i}{d+1}$ for all $i \geq 0$. Thus $\mathrm{HP}^a_{P/I}(Nt)$ is a polynomial of degree $\geq d+1$, in contradiction to the fact that $d = \dim(P/I) = \deg \mathrm{HP}^a_{P/I}(t)$.

Now we prove b). In order to show the equality $d = \mathrm{trdeg}_K(Q(P/I))$, we let $Y \subseteq \{x_1, \ldots, x_n\}$ be a set of d indeterminates which are independent modulo I. We want to prove that the images of the elements of Y under the injective K-algebra homomorphism $K[Y] \hookrightarrow P/I \hookrightarrow Q(P/I)$ form a transcendence basis of $Q(P/I)$ over K. Without loss of generality, we may assume that $Y = \{x_1, \ldots, x_d\}$. For $i = 1, \ldots, n$, let $r_i \in Q(P/I)$ be the image of x_i in $Q(P/I)$. Clearly, the elements $r_1, \ldots, r_d$ are algebraically independent over K. For every $i \in \{d+1, \ldots, n\}$, there exists a non-zero polynomial $f_i \in I \cap K[x_1, \ldots, x_d, x_i]$ because Y is a maximal independent set of indeterminates modulo I. The polynomial f_i has a strictly positive degree with respect to the indeterminate x_i. In the field $Q(P/I)$ we obtain $f_i(r_1, \ldots, r_d, r_i) = 0$, i.e. the element r_i is algebraic over $K(r_1, \ldots, r_d)$. Therefore $Q(P/I)$ is an algebraic field extension of $K(r_1, \ldots, r_d)$ and $\{r_1, \ldots, r_d\}$ is a transcendence basis of $Q(P/I)$ over K.

The second claim in b) follows from the proof we have just given and the fact that all transcendence bases of $Q(P/I)$ over K have $\mathrm{trdeg}_K(Q(P/I))$ elements. □

Combining all characterizations of dimensions proved in the last two sections, we obtain the following corollary.

Corollary 5.7.16. *Let I be a proper ideal in P. Then we have*

$$\dim(P/I) = \mathrm{Kdim}(P/I) = \mathrm{cdim}(P/I)$$

and this number equals the maximal number of algebraically independent elements in P/I over K. Furthermore, if I is a prime ideal, this number is also equal to $\mathrm{trdeg}_K(Q(P/I))$.

This is the end of our long trip through the realm of dimension theory. However, if you are not satisfied yet, more work is waiting for you. Tutorial 78 discusses an important notion in commutative algebra and algebraic

geometry, that of Noether Normalization, while Tutorial 79 features a natural continuation of the work done in Tutorials 43 and 77.

Exercise 1. Look at the first quote!

Exercise 2. Let K be a field and $P = K[x_1, \ldots, x_n]$. Write two CoCoA functions `Cdim1(...)` and `Cdim2(...)` which implement the two methods for computing the combinatorial dimension of a proper ideal $I \subset P$ given by Proposition 5.7.5 and Corollary 5.7.10.b, respectively. Then apply your functions to the following cases and compare the timings.

a) $I_1 = (xy^2 - x,\ y^2z - z)$ in $P = \mathbb{Q}[x, y, z]$
b) $I_2 = (x^4y - 2x^2y + y,\ y^2 - y)$ in $P = \mathbb{Q}[x, y]$
c) $I_3 = (xy^2 - yz^2 - xy + z^2,\ x^2z - y^2z,\ x^3y - y^2z^2 - x^3 + yz^2,$
$y^3z - xz^3 - xyz + z^3)$ in $P = \mathbb{Q}[x, y, z]$

Exercise 3. Let L/K be a finitely generated field extension, i.e. let L be a field of the form $L = Q(R)$ where R is a finitely generated K-algebra and an integral domain.

a) Show that L/K is algebraic (i.e. every element of L is algebraic over K) if and only if $\dim_K(L) < \infty$.
b) Let M/L be a further finitely generated field extension. Show that M/K is algebraic if and only if M/L and L/K are algebraic.

Exercise 4. Let K be a field, let $n \geq 2$, let I be an ideal in $K[x_1, \ldots, x_n]$, and assume that $I \cap K[x_i] \neq (0)$ for $i = 1, 2$. Prove that $I \cap K[x_1 + x_2] \neq (0)$.

Exercise 5. Let K be a field, and let R be a standard graded K-algebra which is an integral domain.

a) Let $Q(R)_0 = \{\frac{f}{g} \mid f, g \in R \text{ homogeneous}, \deg(f) = \deg(g),\ g \neq 0\}$. Show that this is a field.
b) Find the transcendence degree of $Q(K[t^3, t^2u, tu^2, u^3])_0$ over K.

Exercise 6. Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let $1 \leq m < n$. For every $i \in \{1, \ldots, m\}$, let f_i be a polynomial of the form $f_i = x_i - g_i$ with $g_i \in K[x_{i+1}, \ldots, x_n]$. Furthermore, let $g \in K[x_{m+1}, \ldots, x_n]$ be an irreducible polynomial, and let $I = (f_1, \ldots, f_m, g)$.

a) Show that I is a prime ideal.
b) Prove that $\operatorname{trdeg}_K(Q(P/I)) = n - m - 1$.

Exercise 7. Let $A \subseteq B$ be an extension of affine algebras where B is a finitely generated A-module. Prove that $\dim(A) = \dim(B)$.
Hint: Represent B as a quotient of $A[y_1, \ldots, y_s]$ where $y_1, \ldots, y_s$ are new indeterminates which correspond to a set of generators of B as an A-module.

Tutorial 78: Noether Normalization

The Ark was built by amateurs;
the Titanic by professionals.
(Anonymous)

Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let $I \subset P$ be an ideal. A maximal independent set of indeterminates $Y \subseteq \{x_1, \ldots, x_n\}$ modulo I yields an injective ring homomorphism $K[Y] \hookrightarrow P/I$. In this tutorial, we are interested in the $K[Y]$-module structure of P/I defined via this ring homomorphism. In general, the $K[Y]$-module P/I is not finitely generated, and this may be the case for all maximal independent sets of indeterminates Y modulo I. As we shall see, it is possible to find algebraically independent elements $x'_1, \ldots, x'_d$ in P such that the canonical map $\varphi : K[x'_1, \ldots, x'_d] \hookrightarrow P/I$ is injective and turns P/I into a finitely generated $K[x'_1, \ldots, x'_d]$-module. Such an injective ring homomorphism φ is called a **Noether normalization** of P/I. In fact, if the field K is large enough, there exists a linear change of coordinates such that P/I has a Noether normalization in the new indeterminates.

Noether normalizations are ubiquitous and versatile tools in Computational Commutative Algebra. Geometrically, a Noether normalization corresponds to a projection map from $\mathcal{Z}(I)$ to a d-dimensional linear subspace of $\mathbb{A}^n$ whose image is again d-dimensional. Algebraically, it serves to describe the dimension of an affine algebra in yet another way, and computationally it can be useful in the calculation of the primary decomposition of I. Beginning as an amateur, you will emerge from this tutorial as a true professional in the art of constructing Noether normalizations.

a) Show that the ring $\mathbb{Q}[x_1, x_2]/(x_1 x_2)$ has no Noether normalization in the given coordinate system. Find a coordinate system in which it does.

Before we can go on, we need some bits of commutative ring theory. Given an injective ring homomorphism $\varphi : R \hookrightarrow S$, an element $f \in S$ is called **integral** over R if f is a zero of a monic univariate polynomial with coefficients in R. The map φ is called **integral** if every element of S is integral over R. If $\varphi : R \hookrightarrow S$ is a ring extension, i.e. if R is a subring of S and φ is the inclusion map, and if φ is integral, we also say that S is **integral over** R or that S/R is an **integral ring extension**. In the following all rings are assumed to be Noetherian. Let $A \hookrightarrow B \hookrightarrow C$ be injective ring homomorphisms.

b) Assume that B is a finitely generated A-module and C is a finitely generated B-module. Prove that C is a finitely generated A-module. Whence Lemma 2.6.3.a shows that C is a finitely generated A-algebra.

c) Given $b \in B$, prove that the following conditions are equivalent.
   1) The element b is integral over A.
   2) There exists a number $i \geq 0$ such that the subring $A[b]$ of B is generated by $\{1, b, b^2, \ldots, b^i\}$ as an A-module.

3) The subring $A[b]$ of B is a finitely generated A-module.
4) The subring $A[b]$ of B is contained in a subring of B which is a finitely generated A-module.

Hint: To prove 4)⇒1), let $S = As_1 + \cdots + As_\ell$ be a subring of B containing $A[b]$. For every $i \in \{1, \ldots, \ell\}$, write $b\,s_i$ as a linear combination of $s_1, \ldots, s_\ell$. Construct a matrix $\mathcal{M}$ with $\det(\mathcal{M}) \cdot S = 0$ and deduce that $\det(\mathcal{M}) = 0$.

d) Assume that B is integral over A, and C is integral over B. Prove that C is integral over A.

e) Show that $\tilde{A} = \{b \in B \mid b \text{ integral over } A\}$ is a ring. It is called the **integral closure** of A in B.

f) Assume that B is a field and that B is integral over A. Prove that A is a field, too. (*Hint:* For $a \in A \setminus \{0\}$, the element $\frac{1}{a} \in B$ is integral over A.)

g) Suppose that B is a finitely generated A-algebra. Show that B is integral over A if and only if B is a finitely generated A-module.

Next we study the consequences of these results in the following setting. Let K be a field, let $P = K[x_1, \ldots, x_n]$, let $Y \subseteq \{x_1, \ldots, x_n\}$, let $I \subset P$ be a non-zero ideal, and let $d = \dim(P/I)$. Recall that Y is independent modulo I if and only if the canonical map $\varphi : K[Y] \longrightarrow P/I$ is injective. By g), the map φ is integral if and only if P/I is finitely generated as a $K[Y]$-module.

h) Let $f \in P \setminus \{0\}$ and $\alpha \in \mathbb{N}_+$. Consider the polynomials $y_1 = x_1 - x_n^{\alpha}$, $y_2 = x_2 - x_n^{\alpha^2}, \ldots, y_{n-1} = x_{n-1} - x_n^{\alpha^{n-1}}$. Show that if α is large enough, the term of highest degree in the support of $f(y_1, \ldots, y_{n-1}, x_n)$ is a pure power of x_n.

i) Let $f \in P \setminus K$. Prove that there exist elements $y_1, \ldots, y_{n-1} \in P$ for which the canonical map $K[y_1, \ldots, y_{n-1}] \longrightarrow P/(f)$ is injective and integral.
Hint: Use h) to show that x_n is integral over $K[y_1, \ldots, y_{n-1}]$.

j) Let $f \in P \setminus \{0\}$, and assume that K is infinite. Show that, for a generic tuple $(a_1, \ldots, a_{n-1}) \in K^{n-1}$, the linear change of coordinates $y_1 = x_1 - a_1 x_n$, $y_2 = x_2 - a_2 x_n$, $\ldots$, $y_{n-1} = x_{n-1} - a_{n-1} x_n$, $y_n = x_n$ makes the map $K[y_1, \ldots, y_{n-1}] \longrightarrow P/(f)$ injective and integral.

k) **(Noether's Normalization Lemma)** Prove that there exist elements $y_1, \ldots, y_d \in P$ which are algebraically independent over K and have the property that the ring homomorphism $K[y_1, \ldots, y_d] \hookrightarrow P/I$ is injective and integral.
Hint: Use induction on $n - d$. If $n - d > 0$, let $f \in I \setminus \{0\}$, and let $y_1, \ldots, y_{n-1} \in P$ be chosen as in h). Then prove that the map $K[y_1, \ldots, y_{n-1}]/(I \cap K[y_1, \ldots, y_{n-1}]) \longrightarrow P/I$ is injective and integral. Now use Exercise 7 and the inductive hypothesis.

l) Assuming that K is infinite, show that there exists a linear change of coordinates given by $(y_1, \ldots, y_n) = (x_1, \ldots, x_n) \cdot \mathcal{A}$, where $\mathcal{A} \in \mathrm{Mat}_n(K)$ is a lower triangular matrix having units on the main diagonal, with the

property that $K[y_1, \ldots, y_d] \longhookrightarrow P/I$ is a Noether normalization. More generally, show that a generic lower triangular matrix will work.

m) (The Field Theoretic Version of Hilbert's Nullstellensatz 2.6.6 revisited) Let $\mathfrak{m}$ be a maximal ideal in P. Using Noether's Normalization Lemma, show that $P/\mathfrak{m}$ is a finitely generated K-vector space.

In the remaining part of this tutorial we want to examine algorithms for computing a Noether normalization of P/I. We start with a probabilistic algorithm whose probability of success is ... 1. In the following we let K be infinite, $I \subset P$ a non-zero ideal, and $d = \dim(P/I)$.

n) Choose a lower triangular matrix $\mathcal{A} \in \mathrm{Mat}_n(K)$ with random entries, and let $(y_1, \ldots, y_n) = (x_1, \ldots, x_n) \cdot \mathcal{A}$. Explain in what sense the map $K[y_1, \ldots, y_d] \longhookrightarrow P/I$ is a Noether normalization "with probability 1".

o) Now suppose that we do not know the dimension of P/I *a priori*, and we want to make sure that the matrix $\mathcal{A}$ above does indeed give rise to a Noether normalization. For this purpose, consider the following instructions.

1) Choose a lower triangular matrix $\mathcal{A} \in \mathrm{Mat}_n(K)$ with random entries, and let $(y_1, \ldots, y_n) = (x_1, \ldots, x_n) \cdot \mathcal{A}$.
2) Check whether the elements on the main diagonal of $\mathcal{A}$ are non-zero. If not, continue with step 1).
3) Compute $\mathcal{B} = \mathcal{A}^{-1}$ and the ideal $J = \varphi(I)$ where $\varphi : P \longrightarrow P$ is the change of coordinates such that $\varphi(x_i)$ is the i^{th} entry of the tuple $(x_1, \ldots, x_n) \cdot \mathcal{B}$.
4) Compute the reduced `Lex`-Gröbner basis G of J and $d = \dim(P/J)$.
5) If $G \cap K[y_1, \ldots, y_d] \neq \emptyset$, continue with step 1).
6) If there exists an index $i \in \{d+1, \ldots, n\}$ such that no element of G has a leading term which is a pure power of y_i, continue with step 1).
7) Return $\{y_1, \ldots, y_d\}$ and and stop.

Show that this is an algorithm which computes a set $\{y_1, \ldots, y_d\} \subset P_1$ such that $K[y_1, \ldots, y_d] \longhookrightarrow P/I$ is a Noether normalization.

p) Write a CoCoA function `RandomNN(...)` which uses the preceding algorithm to compute a Noether normalization of P/I. Apply this function to the following ideals in $\mathbb{Q}[x_1, x_2, x_3, x_4]$.

1) $I_1 = (x_1x_2 - x_3x_4)$
2) $I_2 = (x_1x_3 - x_2^2,\ x_1x_4 - x_2x_3,\ x_2x_4 - x_3^2)$
3) $I_3 = (x_1x_2x_3x_4 - 1)$

q) Using h), adapt the above algorithm to the case of a general base field K. Write a CoCoA function `GeneralNN(...)` which implements this general version and apply it to the examples in p).

Strictly speaking, the procedure in o) is not a deterministic algorithm because if you keep making bad choices for $\mathcal{A}$ in step 1), you could end up in an infinite loop. A procedure of this type is sometimes called a **randomized algorithm** or a **Las Vegas algorithm**. If this worries you, you can make

the choice of α in h) explicit and use an appropriate variant of q). However, there are only two possibilities that you really have to go back to step 1) from step 5) or 6). Either your random number generator has a serious flaw, or you are the unluckiest person on earth and your random choice hits a Zariski closed set in an affine space. Excluding these "impossible" events, you should never have to go back to step 1). At this point you should be quite satisfied: you have mastered the normalization process and become a veritable professional.

Tutorial 79: Primary Decompositions II

Decomposition is ...
... a primary part of all ecosystems.
... the undoing of every ideal composition.
... your state of mind after your hard disk dies.
(Anonymous)

The computation of primary decompositions is regarded as one of the primary tasks of Computational Commutative Algebra. It is also notorious for being one of the most difficult. In fact, it is so hard that the mere act of preparing this tutorial destroyed the hard disk of one of our computers. So, don't be surprised to find that you are in for quite a challenge!

The concept of primary decomposition first appeared in Volume 1. In Tutorial 43 we asked you to work out an algorithm for computing the primary decomposition of zero-dimensional polynomial ideals, albeit under the additional hypothesis that the base field is perfect. About 300 pages and four years later, we provided the existence of reduced primary decompositions in Noetherian rings in Section 5.6.B and studied their computation for monomial ideals in Tutorial 77.

So, what is left? Why do we bring up this topic once again? There are at least two major questions which still await an answer: to what extent is the reduced primary decomposition of a polynomial ideal uniquely determined, and how can we compute it in the general (non-zero-dimensional, non-monomial) case? Since the full treatment of these questions requires substantial effort, we have decided to structure this tutorial into handy sections, the first of which deals with the uniqueness question.

As for the computational problem, we introduce and study splitting elements in the second subsection. Using these elements, we can reduce the computation of the primary decomposition of one ideal to the computation of the primary decompositions of two ideals which will hopefully turn out to be simpler. Then we examine how we can reduce the computation to the zero-dimensional case by extending and contracting ideals suitably, and finally we get down to actual algorithms for computing the top-dimensional and the primary decompositions of arbitrary polynomial ideals.

Well, not quite arbitrary: for the zero-dimensional algorithm to work, we need a perfect base field. Unfortunately, our reduction to the zero-dimensional case introduces a base field of the form $K(y_1, \ldots, y_m)$ which is not perfect in positive characteristic. Although one can get around this problem using additional techniques, we prefer to keep this tutorial at a reasonable level of difficulty. Therefore we avoid further complicated twists in the algorithmic parts and assume that our base field K has characteristic zero. This has the obvious advantage that whatever extension of K we want to consider, it will always remain perfect.

1. Uniqueness of Reduced Primary Decompositions

The primal part of this primer on computing primary decompositions is primarily devoted to their uniqueness. It requires skillful application of some non-trivial commutative algebra techniques, for instance localization. If you deem it too formal, skip ahead to the second part.

Let R be a Noetherian ring, let I be a proper ideal in R having a reduced primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ with primary ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ of R, and let $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ for $i = 1, \ldots, s$. The ideals $\mathfrak{q}_i$ are called **primary components** of I, and the primes $\mathfrak{p}_i$ are called **prime components** of I. Recall that a prime ideal $\mathfrak{p} \subset R$ is called an **associated prime** of an R-module M if $\mathfrak{p} = \mathrm{Ann}_R(m)$ for some element $m \in M$ (see Tutorial 31). The set of all associated primes of M is denoted by $\mathrm{Ass}(M)$.

a) Prove the following rules for associated primes.
   1) $\mathrm{Ass}(R/\mathfrak{q}) = \{\mathfrak{p}\}$ if $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal
   2) $\mathrm{Ass}(U) \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(U) \cup \mathrm{Ass}(M/U)$ for submodules $U \subseteq M$
   3) $\mathrm{Ass}(M_S) = \{\mathfrak{p}R_S \mid \mathfrak{p} \in \mathrm{Ass}(M),\ \mathfrak{p} \cap S = \emptyset\}$ for multiplicatively closed subsets $S \subset R$

b) Show that the set of associated primes of R/I is $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Hence the set of prime components of I is uniquely determined.
   Hint: Consider the ideals $J_i = \bigcap_{j \neq i} \mathfrak{p}_i$ and argue by induction on s.

c) Let $\mathfrak{p}_i$ be a prime component of I. Prove that we can recover the associated primary component $\mathfrak{q}_i$ via the formula $\mathfrak{q}_i = I :_R (I :_R \mathfrak{p}_i^\infty)$. This process is called **isolation of primary components**.

d) Let $S \subset R$ be a multiplicatively closed subset. Prove that

$$IR_S = \bigcap_{\{i \mid \mathfrak{p}_i \cap S = \emptyset\}} \mathfrak{q}_i R_S$$

   is a reduced primary decomposition. (*Hint:* Show that $\mathfrak{p}_i \cap S \neq \emptyset$ implies $\mathfrak{q}_i R_S = R_S$.)

e) Let $\mathfrak{p}_i$ be a minimal element (with respect to inclusion) in the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Show that $\mathfrak{q}_i = IR_S \cap R$ for $S = R \setminus \mathfrak{p}_i$. In particular, the $\mathfrak{p}_i$-primary component of I is uniquely determined.

f) Let $\mathfrak{q}_i$ be an **embedded primary component** of I, i.e. let $\mathfrak{p}_i$ be an associated prime of R/I which is not minimal in $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Show by example that $\mathfrak{q}_i$ is in general not uniquely determined.
Hint: Consider $R = \mathbb{Q}[x_1, x_2]$ and $I = (x_1^2, x_1 x_2)$.

2. Splitting Elements

The idea behind the algorithms for computing primary decompositions is based on the notion of a splitting element. The primal motivation why we introduce this concept derives from the following elementary observations. Let R be a Noetherian ring, let $I \subseteq R$ be an ideal, and let $f \in R$.

g) Show that $I :_R (f) = I :_R (f^2)$ implies $I = (I :_R (f)) \cap (I + (f))$.
h) Let $\ell \geq 1$ be such that $I :_R (f)^\infty = I :_R (f)^\ell$. Prove that this implies $I = (I :_R (f^\ell)) \cap (I + (f^\ell))$.
i) Assume that both $I :_R (f)^\infty$ and $I + (f)$ properly contain I. Show that every prime component of I either contains $I :_R (f)^\infty$ or $I + (f)$, but not both. (*Hint:* Distinguish the cases $f \in \mathfrak{p}$ and $f \notin \mathfrak{p}$.)

Hence an element $f \in R \setminus \sqrt{I}$ for which the ideal $I :_R (f)^\infty$ properly contains I can be used to split the computation of the primary decomposition of I into two parts. This makes us interested in tracking down an element $f \in R \setminus \sqrt{I}$ which is a zero divisor for R/I. Such an element f is called a **splitting element** for I. Our hope is that if we can find a splitting element, the primary decompositions of $I :_R (f)$ and $I + (f)$ will be easier to compute. Before we start chasing after splitting elements, we need to prepare for the hunt.

3. Extension and Contraction of Ideals

The strategy for reducing the computation of primary decompositions to the zero-dimensional case comprises three phases: finding a maximal set of independent indeterminates Y, extending the given ideal to a zero-dimensional ideal in a polynomial ring over the field $K(Y)$, and contracting the primary components of that zero-dimensional ideal back to the original polynomial ring. The processes of extending and contracting ideals can be performed computationally as follows.

Let K be a field, and let $Y = \{y_1, \ldots, y_m\}$ and $Z = \{z_1, \ldots, z_k\}$ be algebraically independent sets of indeterminates over K.

j) Let J be an ideal in $K(Y)[Z]$, let σ be a term ordering on $\mathbb{T}(Z)$, let $\{f_1, \ldots, f_r\}$ be a σ-Gröbner basis of J which consists of elements of $K[Y, Z]$, and let $I = (f_1, \ldots, f_r) \subseteq K[Y, Z]$. Show that the contraction $J \cap K[Y, Z]$ can be computed using the formula

$$J \cap K[Y, Z] = I :_{K[Y,Z]} (h)^\infty$$

where $h = \operatorname{lcm}(\mathrm{LC}_\sigma(f_1), \ldots, \mathrm{LC}_\sigma(f_r)) \in K[Y]$.

k) Let $I \subseteq K[Y,Z]$ be an ideal, let $J = I\,K(Y)[Z]$ be its extension to $K(Y)[Z]$, let τ be an elimination ordering for Z on $\mathbb{T}(Y,Z)$, and let $G = \{g_1,\ldots,g_s\}$ be a τ-Gröbner basis of I. For $i = 1,\ldots,s$, we write $\mathrm{LT}_\tau(g_i) = t_i u_i$ with $t_i \in \mathbb{T}(Y)$ and $u_i \in \mathbb{T}(Z)$. Prove that $h = \mathrm{lcm}(t_1,\ldots,t_s)$ has the following properties.
   1) $h \notin I$
   2) $J \cap K[Y,Z] = I :_{K[Y,Z]} (h)^\infty$

4. Computing the Top-Dimensional Decomposition

Next we consider a polynomial ring $P = K[x_1,\ldots,x_n]$ over a field K, we let $I \subset P$ be an ideal, and we let $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ be a reduced primary decomposition of I. Using Corollary 5.7.10, we can compute a maximal independent set of indeterminates $Y \subseteq \{x_1,\ldots,x_n\}$ modulo I which consists of $\dim(P/I)$ elements. Without loss of generality we may renumber the ideals $\mathfrak{q}_1,\ldots,\mathfrak{q}_s$ so that there exists an index $r \in \{1,\ldots,s\}$ for which we have $\mathfrak{q}_i \cap K[Y] = (0)$ for $i = 1,\ldots,r$ and $\mathfrak{q}_i \cap K[Y] \neq (0)$ for $i = r+1,\ldots,s$. Finally, we let $Z = \{x_1,\ldots,x_n\} \setminus Y$.

l) Prove that the extension ideal $J = I\,K(Y)[Z]$ is zero-dimensional and $J = \mathfrak{q}_1 K(Y)[Z] \cap \cdots \cap \mathfrak{q}_r K(Y)[Z]$ is a reduced primary decomposition.

m) Let $I^{\mathrm{top}} = I\,K(Y)[Z] \cap P$. Prove that $I^{\mathrm{top}} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ is a reduced primary decomposition of I^{top}. Observe that we can compute I^{top} via the formula $I^{\mathrm{top}} = I :_P (h)^\infty$ as shown in k).

n) Show that we have $\dim(P/\mathfrak{q}_i) = \dim(P/I)$ for $i = 1,\ldots,r$ and $\dim(P/\mathfrak{q}_i) < \dim(P/I)$ for $i = r+1,\ldots,s$.
   Hint: Prove that if $\mathfrak{a}$ is an ideal for which $\sqrt{\mathfrak{a}}$ is prime then a set of elements is algebraically independent modulo $\sqrt{\mathfrak{a}}$ if and only if it is so modulo $\mathfrak{a}$. Then use Proposition 5.7.15.b.

The ideal I^{top} is called the **top-dimensional part** (or the **equidimensional part**) of the ideal I, and the reduced primary decomposition $I^{\mathrm{top}} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ is called the **top-dimensional decomposition** of I. By combining the above results with Tutorial 43, we can compute the top-dimensional decomposition of I. Assume that K has characteristic zero and that the ideal I is given by a set of generators.

o) Consider the procedure `TopDec(...)` defined by the following sequence of instructions.
   1) Using the algorithm of Corollary 5.7.10, compute a maximal set of independent indeterminates $Y \subseteq \{x_1,\ldots,x_n\}$ modulo I which consists of $\dim(P/I)$ elements.
   2) Using the function `PrimaryDec(...)` of Tutorial 43.r, compute a primary decomposition $J = \mathfrak{Q}_1 \cap \cdots \cap \mathfrak{Q}_r$ of the extension ideal $J = I\,K(Y)[Z]$.
   3) For $i = 1,\ldots,r$, compute $\mathfrak{q}_i = \mathfrak{Q}_i \cap P$ using j). Return the tuple $(\mathfrak{q}_1,\ldots,\mathfrak{q}_r)$.

Show that `TopDec(...)` is an algorithm which computes the top-dimensional decomposition of I. Write a CoCoA function which implements this algorithm and apply it to compute the top-dimensional decomposition of the following ideals.

1) $I_1 = (x_1^2,\, x_1x_2) \subset \mathbb{Q}[x_1, x_2]$
2) $I_2 = (x_1x_2,\, x_1x_3) \subset \mathbb{Q}[x_1, x_2, x_3]$
3) $I_3 = (x_1^4x_2 - 2x_1^2x_2 + x_2,\, x_2^2 - x_2) \subset \mathbb{Q}[x_1, x_2]$
4) $I_4 = (x_1x_4 - x_2x_3,\, x_5x_8 - x_6x_7,\, x_1x_6 - x_2x_5) \subseteq \mathbb{Q}[x_1, \ldots, x_8]$

5. Computing Primary Decompositions

What about the remaining primary components of I? How can we find them? We have arrived at the primary part of this tutorial and we need a prime idea. We already know how to compute the primary decomposition of $I^{\text{top}} = I :_P (h)^\infty$. Next we determine a number $\ell \geq 1$ for which $I :_P (h)^\infty = I :_P (h^\ell)$. So, we can use h^ℓ as a splitting element!

Let K be a field of characteristic zero, and let $I \subset P$ be an ideal given by a set of generators.

p) Consider the procedure `PD(...)` defined by the following sequence of instructions.
   1) Let $Q = \emptyset$ and $J = I$.
   2) Using the algorithm `TopDec(...)`, compute the top-dimensional decomposition of J. Adjoin the resulting tuple to Q.
   3) Let $h \in P$ be the polynomial computed by `TopDec(...)` for which $J^{\text{top}} = J :_P (h)^\infty$. Determine $\ell \geq 1$ such that $J :_P (h)^\infty = J :_P (h^\ell)$.
   4) If $J + (h^\ell) \neq (1)$, replace J by $J + (h^\ell)$ and continue with step 2).
   5) Let $Q = (\mathfrak{q}_1, \ldots, \mathfrak{q}_s)$. Remove from Q all redundant ideals, i.e. all ideals $\mathfrak{q}_i$ for which $\bigcap_{j \neq i} \mathfrak{q}_j \subseteq \mathfrak{q}_i$. Return the resulting list.

   Prove that `PD(...)` is an algorithm which computes a reduced primary decomposition of I.
   Hint: To show finiteness, prove that either $\dim(P/(J+(h^\ell))) < \dim(P/J)$ or the number of longest maximal independent sets of indeterminates modulo the ideal $J + (h^\ell)$ is strictly smaller than the corresponding number for J since Y is not independent modulo $J + (h^\ell)$.

q) Write a CoCoA function `PD(...)` which implements this algorithm. Apply your function `PD(...)` to compute the primary decompositions of the following ideals. (In some cases we have included the result to help you debug your code.)
   1) $I_1 = (x_1^2,\, x_1x_2) \subset \mathbb{Q}[x_1, x_2]$
      Result: $I_1 = \mathfrak{q}_1 \cap \mathfrak{q}_2$ with $\mathfrak{q}_1 = (x_1)$ and $\mathfrak{q}_2 = (x_1^2, x_2)$ (not unique!)
   2) $I_2 = (x_1x_2,\, x_1x_3) \subset \mathbb{Q}[x_1, x_2, x_3]$
      Result: $I_2 = \mathfrak{q}_1 \cap \mathfrak{q}_2$ with $\mathfrak{q}_1 = (x_1)$ and $\mathfrak{q}_2 = (x_2, x_3)$

3) $I_3 = (x_1^4x_2 - 2x_1^2x_2 + x_2,\, x_2^2 - x_2) \subset \mathbb{Q}[x_1, x_2]$
Result: $I_3 = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \mathfrak{q}_3$ with $\mathfrak{q}_1 = (x_2)$ and $\mathfrak{q}_2 = ((x_1+1)^2, x_2 - 1)$ and $\mathfrak{q}_3 = ((x_1 - 1)^2, x_2 - 1)$
4) $I_4 = (x_1x_4 - x_2x_3,\, x_5x_8 - x_6x_7,\, x_1x_6 - x_2x_5) \subseteq \mathbb{Q}[x_1, \ldots, x_8]$
Result: $I_4 = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \mathfrak{q}_3$ with $\mathfrak{q}_1 = (x_1,\, x_2,\, x_5x_8 - x_6x_7)$ and $\mathfrak{q}_2 = (x_5,\, x_6,\, x_1x_4 - x_2x_3)$ and $\mathfrak{q}_3 = I_4 + (x_4x_7 - x_3x_8,\, x_2x_7 - x_1x_8,\, x_4x_5 - x_3x_6)$
5) $I_5 = (x_2^4 - 2x_1x_2^2x_3 + x_1^2x_3^2,\, x_2^3x_3 - x_1x_2x_3^2 - x_1x_2^2x_4 + x_1^2x_3x_4,\, x_2^2x_3^2 - x_1x_3^3 - x_2^3x_4 + x_1x_2x_3x_4,\, x_2^2x_3^2 - 2x_1x_2x_3x_4 + x_1^2x_4^2,\, x_2x_3^3 - x_2^2x_3x_4 - x_1x_3^2x_4 + x_1x_2x_4^2,\, x_3^4 - 2x_2x_3^2x_4 + x_2^2x_4^2) \subset \mathbb{Q}[x_1, \ldots, x_4]$
6) $I_6 = (x_1x_2x_3 - x_1^2x_4,\, x_1x_2^2 - x_1^2x_3,\, x_3^2x_4 - x_2x_4^2,\, x_3^3 - x_1x_4^2,\, x_2x_3^2 - x_1x_3x_4,\, x_2x_3x_4 - x_1x_4^2,\, x_2^2x_4 - x_1x_3x_4,\, x_2^2x_3 - x_1x_2x_4,\, x_1x_3^2 - x_1x_2x_4,\, x_2^3 - x_1^2x_4) \subset \mathbb{Q}[x_1, \ldots, x_4]$
7) $I_7 = (x_3^4 - 2x_2x_3^2x_4 + x_2^2x_4^2,\, x_2x_3^3 - x_2^2x_3x_4 - x_1x_3^2x_4 + x_1x_2x_4^2,\, x_2^2x_3^2 - 2x_1x_2x_3x_4 + x_1^2x_4^2,\, x_1x_3^3 + x_2^3x_4 - 3x_1x_2x_3x_4 + x_1^2x_4^2,\, x_2^3x_3 - x_1x_2x_3^2 - x_1x_2^2x_4 + x_1^2x_3x_4,\, x_2^4 - 2x_1x_2^2x_3 + x_1^2x_3^2) \subset \mathbb{Q}[x_1, \ldots, x_4]$

5.8 General Hilbert Functions

An ignorant person
is one who doesn't know
what you have just found out.
(Will Rogers)

No matter how the final result may look to you, the story of this section (and several others in this book) is not nearly as straightforward as the presentation we finally achieved. When we told some colleagues about our intention to write something about multivariate Hilbert series, they patted us on our shoulders and made comments such as "Very Good! Did you know that I have been using them in my recent paper?" or "Oh yes, I usually teach those in my lecture course." However, it turned out to be difficult to get our hands on a published source for this material in the generality and style we envisaged. Searching the usual textbooks, we came up with a definition in [BH93] which in our notation reads as follows.

Let R be an arbitrary $\mathbb{Z}^m$-graded K-algebra and M a $\mathbb{Z}^m$-graded R-module, all of whose homogeneous components are finite-dimensional K-vector spaces. Then $\sum_{i=(i_1,\ldots,i_m)\in\mathbb{Z}^m} \dim_K(M_i)\, z_1^{i_1}\cdots z_m^{i_m}$ is called the Hilbert series of M.

O.K., at least we do have a definition to start with, don't we? Well, it would be good to know what kind of series we are using here. Maybe it is a multivariate Laurent series of the usual kind, i.e. an element of the localization $\mathbb{Z}[[z_1,\ldots,z_m]]_{z_1\cdots z_m}$. No, that can't be, since if we use $W = \left(\begin{smallmatrix}1 & 1\\ 0 & -1\end{smallmatrix}\right)$ on $P = K[x_1, x_2]$, then the homogeneous component of degree (d_1, d_2) of P is $K\, x_1^{d_1+d_2} x_2^{-d_2}$, and therefore the multivariate Hilbert series of P is $\mathrm{HS}_P(z_1, z_2) = \sum_{(d_1,d_2)\in\mathbb{Z}^2} z_1^{d_1+d_2} z_2^{-d_2}$ which has infinitely many terms with negative exponents.

Since this doesn't work, maybe we should consider $\mathrm{HS}_M(z_1,\ldots,z_m)$ as an element of the $\mathbb{Z}$-module $\mathbb{Z}[[z_1,\ldots,z_m,z_1^{-1},\ldots,z_m^{-1}]]$. Again we run into trouble, because Theorem 5.2.20 and Tutorial 68 clearly suggest that we should be able to multiply Hilbert series. But there is no way to make $\mathbb{Z}[[z_1,\ldots,z_m,z_1^{-1},\ldots,z_m^{-1}]]$ into a ring, because, for instance, the constant term of $(1+z_1+z_1^2+\cdots)\cdot(1+z_1^{-1}+z_1^{-2}+\cdots)$ is not defined. What is going on here?

Everybody is ignorant,
only on different subjects.
(Will Rogers)

At this point it started to dawn on us that we were much more ignorant on this subject than we had thought. Of course, an ignorant mathematician is one who doesn't know your latest result. But maybe the topic of multivariate Hilbert series really has been covered only scantily hitherto? Once again, the going is getting a bit tough. Therefore we rise to the challenge and get going!

The trouble we have just encountered is due to the fact that in the product formula $(\sum_{i\in\mathbb{Z}^m} a_i\mathbf{z}^i)\cdot(\sum_{j\in\mathbb{Z}^m} b_j\mathbf{z}^j) = \sum_{k\in\mathbb{Z}^m}(\sum_{i+j=k} a_ib_j)\,\mathbf{z}^k$, the sum over all (i,j) such that $i+j=k$ need not be finite. Miraculously, the positivity of the gradings we consider comes to our rescue once again. In order to have finite dimensional homogeneous components, we have to assume anyway that P is graded by a matrix of positive type. But then Proposition 4.1.21.a yields a monoid ordering σ on $\mathbb{Z}^m$ which is in fact a well-ordering on the monomodule generated by the degrees of the homogeneous elements of M. Thus the sets $\{i\in\mathbb{Z}^m \mid a_i\neq 0\}$ and $\{j\in\mathbb{Z}^m \mid b_j\neq 0\}$ are well-ordered by σ, and the summation of $\sum_{i+j=k} a_ib_j$ poses no problem anymore.

The detailed discussion of this question is the topic of Subsection A. Given a monoid ordering σ on $\mathbb{Z}^m$, we define the ring of σ-Laurent series as a suitable ring contained in $\mathbb{Z}[[\mathbf{z},\mathbf{z}^{-1}]]$. These rings are big enough to contain all Hilbert series we shall be interested in. In particular, the ring of `Lex`-Laurent series contains all Hilbert series of finitely generated graded modules over P for any positive grading. Thus we can proceed in Subsection B to define multigraded Hilbert functions and multivariate Hilbert series in the natural way. The basic properties of these objects are generalized from the standard graded to the multigraded case (see Proposition 5.8.9 and 5.8.13), and a simple formula for the multivariate Hilbert series of the polynomial ring is found (see Proposition 5.8.15).

In order to compute the multivariate Hilbert series of finitely generated graded modules polynomial rings graded by matrices of positive type, we generalize the results of Section 5.3 and provide an explicit algorithm (see Theorem 5.8.18). This algorithm also shows that multivariate Hilbert series have a shape similar to that described in Theorem 5.2.20 — they are given by the quotient of two multivariate polynomials (see Corollary 5.8.19).

In the last part of the section, we discuss the question of how multivariate Hilbert series transform when we change the grading. In particular, we obtain an easy description of how multivariate Hilbert series behave under refinement of the grading. Corollary 5.8.27 has many applications. Some of them are related to Rees rings, Hadamard series, and Segre products, and you can find out everything about them by solving Tutorials 81 and 82.

And what is the upshot of our little story? We believe that, in the future, what you have just found out will be considered to be well-known *folklore* of the subject, and only ignorant folks will have to rediscover it themselves. However, don't pity them! Doing it yourself is fun and well worth the effort.

The strangest thing about the future is that
then one will call our time the good old days.
(Ernest Hemingway)

5.8.A Rings of Multivariate Laurent Series

Create a warm, comfortable
and functional environment
with our stylish Laurent Series.
(Furniture Advertisement)

Judging from our introduction, multivariate Hilbert series may appear to be a nasty bunch. But by creating a functional environment using stylish rings of multivariate Laurent series, we shall now furnish you with everything you need to become comfortable in dealing with them.

In this subsection we let R be a ring. Recall that, for us, this always means a commutative ring with identity. In Definition 5.2.1.b we introduced the power series ring $R[[z_1, \ldots, z_m]]$ in m indeterminates over R. Every element $f \in R[[z_1, \ldots, z_m]]$ has a unique representation

$$f = \sum_{(i_1,\ldots,i_m)\in\mathbb{N}^m} a_{(i_1,\ldots,i_m)}\, z_1^{i_1} \cdots z_m^{i_m}$$

with $a_{(i_1,\ldots,i_m)} \in R$ for all $(i_1, \ldots, i_m) \in \mathbb{N}^m$. If we want to be brief, we shall write $f = \sum_{i\in\mathbb{N}^m} a_i\, \mathbf{z}^i$. Multiplication of power series is given by the formula

$$\Big(\sum_{i\in\mathbb{N}^m} a_i\, \mathbf{z}^i\Big) \cdot \Big(\sum_{j\in\mathbb{N}^m} b_j\, \mathbf{z}^j\Big) = \sum_{k\in\mathbb{N}^m} \Big(\sum_{i+j=k} a_i b_j\Big)\, \mathbf{z}^k$$

The following proposition follows easily by induction from Proposition 5.2.2.

Proposition 5.8.1. *Let* $f = \sum_{i\in\mathbb{N}^m} a_i\, \mathbf{z}^i$ *be an element of* $R[[z_1, \ldots, z_m]]$.

a) The element f *is a unit in* $R[[z_1, \ldots, z_m]]$ *if and only if* a_0 *is a unit in* R.

b) If R *is an integral domain then* $R[[z_1, \ldots, z_m]]$ *is also an integral domain.*

For the purpose of defining multivariate Hilbert series, the power series ring $R[[z_1, \ldots, z_m]]$ is not big enough. As we shall see, we need to allow negative exponents. Sometimes there will even be infinitely many terms having negative exponents. The following object is big enough to contain all the series we need.

Definition 5.8.2. The set $R^{\mathbb{Z}^m}$ is an R-module with respect to componentwise addition and scalar multiplication. We shall denote an element $(a_i)_{i\in\mathbb{Z}^m}$ by $\sum_{i\in\mathbb{Z}^m} a_i\, \mathbf{z}^i$ and the module by $R[[\mathbf{z}, \mathbf{z}^{-1}]]$. We call it the **module of extended power series**.

Unfortunately, the module of extended power series is not a ring with respect to the usual multiplication. For instance, the constant coefficient of the product $(1 + z_1 + z_1^2 + \cdots) \cdot (1 + z_1^{-1} + z_1^{-2} + \cdots)$ would be an infinite sum. But, as we have seen in the standard graded case, it is important to be able to multiply Hilbert series. Therefore we have to find a submodule of $R[[\mathbf{z}, \mathbf{z}^{-1}]]$ which is both small enough to be a ring and big enough to contain all the Hilbert series we need. The following definition gets us off the horns of this dilemma.

Definition 5.8.3. Let σ be a monoid ordering on $\mathbb{Z}^m$.

a) An extended power series $f = \sum_{i\in\mathbb{Z}^m} a_i\,\mathbf{z}^i$ is called a **σ-Laurent series** if there exists a subset $\Sigma \subseteq \mathbb{Z}^m$ such that $a_i = 0$ for all $i \notin \Sigma$ and such that the restriction of σ to Σ is a well-ordering.

b) The set of all σ-Laurent series is called the **σ-Laurent series ring** over R and will be denoted by $R[[\mathbf{z}, \mathbf{z}^{-1}]]_\sigma$.

Of course, now we have to prove that $R[[\mathbf{z}, \mathbf{z}^{-1}]]_\sigma$ really is a ring. The following lemma isolates the crucial point of the proof.

Lemma 5.8.4. *Let Σ be an infinite set, and let σ be a well-ordering on Σ. Then there exists an infinite strictly increasing sequence $i_1 <_\sigma i_2 <_\sigma \cdots$ of elements $i_1, i_2, \ldots$ in Σ.*

Proof. The sequence $i_1, i_2, \ldots$ is constructed inductively. By assumption, the set Σ has a minimal element i_1 with respect to σ. For every $j \geq 1$, the set $\Sigma \setminus \{i_1, \ldots, i_j\}$ is not empty, and therefore has a minimal element i_{j+1} with respect to σ. By construction, the sequence $i_1, i_2, \ldots$ is strictly increasing with respect to σ. □

Proposition 5.8.5. *Let σ be a monoid ordering on $\mathbb{Z}^m$. Then the set $R[[\mathbf{z}, \mathbf{z}^{-1}]]_\sigma$ of all σ-Laurent series is a ring with respect to componentwise addition and with respect to the multiplication given by the formula*

$$\Big(\sum_{i\in\mathbb{Z}^m} a_i\,\mathbf{z}^i\Big)\cdot\Big(\sum_{j\in\mathbb{Z}^m} b_j\,\mathbf{z}^j\Big) = \sum_{k\in\mathbb{Z}^m}\Big(\sum_{i+j=k} a_i b_j\Big)\,\mathbf{z}^k$$

Proof. Since the union of two subsets of $\mathbb{Z}^m$ which are well-ordered with respect to σ is again well-ordered, it is clear that the set $R[[\mathbf{z}, \mathbf{z}^{-1}]]_\sigma$ is an R-submodule of $R[[\mathbf{z}, \mathbf{z}^{-1}]]$. To show that the above formula yields a well-defined multiplication, it suffices to show that the sum $\sum_{i+j=k} a_i b_j$ is finite for each $k \in \mathbb{Z}^m$. Let Σ be the set of all $i \in \mathbb{Z}^m$ such that $a_i \neq 0$ or $b_i \neq 0$.

Suppose that the set $\{(i,j) \in \Sigma^2 \mid i + j = k\}$ is infinite. Then also the set $\Sigma' = \{i \in \Sigma \mid i + j = k \text{ for some } j \in \Sigma\}$ is infinite, and it is well-ordered with respect to σ. By the lemma, the set Σ' contains an infinite ascending sequence $i_1 <_\sigma i_2 <_\sigma \cdots$. Therefore, if we let $j_\ell = k - i_\ell$ for $\ell \geq 1$, we have an infinite strictly decreasing sequence $j_1 >_\sigma j_2 >_\sigma \cdots$ in Σ, in contradiction to the fact that σ is a well-ordering on Σ.

Finally, we note that the ring axioms can be easily verified for the given addition and multiplication. □

Let us examine the rings $R[[\mathbf{z}, \mathbf{z}^{-1}]]_\sigma$ for some term orderings σ.

Example 5.8.6. Let $m = 1$ and $\sigma = \mathtt{Deg}$. Then the ring $R[[z_1, z_1^{-1}]]_\sigma$ coincides with the usual Laurent series ring $R[[z_1]]_{z_1}$. In fact, for every $f = \sum_{i\in\mathbb{Z}} a_i z_1^i \in R[[z_1, z_1^{-1}]]_\sigma$, there exists an index $i_0 \in \mathbb{Z}$ such that $a_i = 0$ for $i < i_0$.

Example 5.8.7. Let $\sigma = \texttt{DegLex}$. Then the ring $R[[\mathbf{z}, \mathbf{z}^{-1}]]_\sigma$ consists of all extended power series $f = \sum_{i \in \mathbb{Z}^m} a_i \mathbf{z}^i$ for which there is an index $d \in \mathbb{Z}^m$ such that $a_i \neq 0$ implies $i \geq_{\texttt{DegLex}} d$. In particular, this means that every index $i = (i_1, \ldots, i_m)$ for which $a_i \neq 0$ has the property that $i_1 + \cdots + i_m$ is greater than or equal to the first component of d.

The ring $R[[\mathbf{z}, \mathbf{z}^{-1}]]_\sigma$ certainly contains all extended power series which have only finitely many terms with negative exponents, and it also contains some series having infinitely many terms with negative exponents such as $f = \sum_{i \geq 0} z_1^i z_2^{-i-1}$.

5.8.B Hilbert Functions in the General Case

Algebraic symbols are used
when you do not know
what you are talking about.
(Anonymous)

In this subsection we let K be a field and $P = K[x_1, \ldots, x_n]$ a polynomial ring over K which is graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type. Considering Proposition 4.1.19.b, it makes sense to generalize the definition of Hilbert functions as follows.

Definition 5.8.8. Let M be a finitely generated graded P-module. Then the map $\mathrm{HF}_M : \mathbb{Z}^m \longrightarrow \mathbb{Z}$ given by $(i_1, \ldots, i_m) \mapsto \dim_K(M_{(i_1,\ldots,i_m)})$ for all $(i_1, \ldots, i_m) \in \mathbb{Z}^m$ is called the **multigraded Hilbert function** of M. If we want to make the dependence on the grading explicit, we shall also denote it by $\mathrm{HF}_{M,W}$.

More generally, for a $\mathbb{Z}^m$-graded K-algebra R and a graded R-module M which has finite dimensional homogeneous components, we define the multigraded Hilbert function of M in the same way.

The term "multigraded" in this definition is intended to include the positively $\mathbb{Z}$-graded case, i.e. the case when $m = 1$ and W is a row of positive integers. Many properties of Hilbert functions generalize easily from the standard graded to the multigraded setting. The proof of the following proposition is obtained by imitating the proofs of Propositions 5.1.14, 5.1.16, Theorem 5.1.18, and Corollary 5.1.20.

Proposition 5.8.9. (Properties of Multigraded Hilbert Functions) *Let M be a finitely generated graded P-module.*

a) For every $d \in \mathbb{Z}^m$, the Hilbert function of the shifted module $M(d)$ is given by $\mathrm{HF}_{M(d)}(i) = \mathrm{HF}_M(d + i)$ for all $i \in \mathbb{Z}^m$.

b) Given finitely generated graded P-modules M', M'' and an exact sequence of graded P-modules

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

we have $\mathrm{HF}_M(i) = \mathrm{HF}_{M'}(i) + \mathrm{HF}_{M''}(i)$ for all $i \in \mathbb{Z}^m$.

c) Given finitely many finitely generated graded P-modules $M_1, \ldots, M_r$, we have $\mathrm{HF}_{M_1 \oplus \cdots \oplus M_r}(i) = \mathrm{HF}_{M_1}(i) + \cdots + \mathrm{HF}_{M_r}(i)$ for all $i \in \mathbb{Z}^m$.

d) Given $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, the graded free P-module $F = \bigoplus_{j=1}^r P(-\delta_j)$ has Hilbert function $\mathrm{HF}_F(i) = \sum_{j=1}^r \mathrm{HF}_P(i - \delta_j)$ for all $i \in \mathbb{Z}^m$.

e) Let $d \in \mathbb{Z}^m$. Given a polynomial $f \in P_d \setminus \{0\}$, we have

$$\mathrm{HF}_{M/fM}(i) = \mathrm{HF}_M(i) - \mathrm{HF}_{M/(0:_M(f))}(i - d)$$

for all $i \in \mathbb{Z}^m$. In particular, if f is a non-zerodivisor for M, we have $\mathrm{HF}_{M/fM}(i) = \mathrm{HF}_M(i) - \mathrm{HF}_M(i - d)$ for all $i \in \mathbb{Z}^m$.

f) Let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, let M be a graded submodule of $\bigoplus_{j=1}^r P(-\delta_j)$, and let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. Then we have $\mathrm{HF}_{\mathrm{LT}_\sigma(M)}(i) = \mathrm{HF}_M(i)$ for all $i \in \mathbb{Z}^m$.

g) Given a field extension $K \subseteq L$, we have $\mathrm{HF}_{M \otimes_K L}(i) = \mathrm{HF}_M(i)$ for all $i \in \mathbb{Z}^m$.

In order to actually use these rules for computing multigraded Hilbert functions, we still need to know the multigraded Hilbert function of the polynomial ring. Unfortunately, there is no simple formula as in the standard graded case (see Proposition 5.1.13).

Proposition 5.8.10. *Let $W = (w_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ and $(i_1, \ldots, i_m) \in \mathbb{Z}^m$. Then the value $\mathrm{HF}_P(i_1, \ldots, i_m)$ of the multigraded Hilbert function of P is the number of solutions $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ of the system of Diophantine equations*

$$\left\{ \begin{array}{rcl} w_{11}y_1 + \cdots + w_{1n}y_n & = & i_1 \\ w_{21}y_1 + \cdots + w_{2n}y_n & = & i_2 \\ \vdots & \vdots & \vdots \\ w_{m1}y_1 + \cdots + w_{mn}y_n & = & i_m \end{array} \right.$$

in the indeterminates $y_1, \ldots, y_n$.

Proof. To show this claim, we note that $\dim_K(P_{(i_1,\ldots,i_m)})$ is the number of terms $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ of multidegree $(i_1, \ldots, i_m)$. Using Definition 4.1.6, we see that $\deg_W(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}}$, and this equals $(i_1, \ldots, i_m)^{\mathrm{tr}}$ if and only if $(\alpha_1, \ldots, \alpha_m)$ solves the given system of equations. □

Admittedly, this description of HF_P is not very illuminating with respect to the overall structure of this function. To get a deeper insight, we revert again to the method of using generating functions. In other words, we use the values of a multigraded Hilbert function as the coefficients of a suitable extended power series.

Definition 5.8.11. Let M be a finitely generated graded P-module. The extended power series

$$\mathrm{HS}_M(z_1, \ldots, z_m) = \sum_{(i_1,\ldots,i_m) \in \mathbb{Z}^m} \mathrm{HF}_M(i_1, \ldots, i_m)\, z_1^{i_1} \cdots z_m^{i_m} \in \mathbb{Z}[[\mathbf{z}, \mathbf{z}^{-1}]]$$

is called the **multivariate Hilbert series** of M. We shall also denote it by $\mathrm{HS}_M(\mathbf{z})$, or by $\mathrm{HS}_{M,W}(\mathbf{z})$ if we want to stress the underlying grading.

More generally, for a $\mathbb{Z}^m$-graded K-algebra R and a graded R-module M which has finite dimensional homogeneous components, we define the multivariate Hilbert series of M by the same formula.

Again the term "multivariate" in this definition is intended to include the univariate case. Didn't we ask for a ring which contains those multivariate Hilbert series? As we saw in the first subsection, the $\mathbb{Z}$-module $\mathbb{Z}[[\mathbf{z}, \mathbf{z}^{-1}]]$ is not a ring. Fortunately, the assumption that the grading on P is of positive type comes to our rescue here.

Remark 5.8.12. Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type.

a) Let τ be one of the monoid orderings on $\mathbb{Z}^m$ of the type constructed in the proof of Proposition 4.1.21.a. In part b) of that proposition we saw that the restriction of τ to the set $\{d \in \mathbb{Z}^m \mid M_{W,d} \neq 0\}$ is a well-ordering for every finitely generated graded P-module M. Therefore we have $\mathrm{HS}_M(\mathbf{z}) \in \mathbb{Z}[[\mathbf{z}, \mathbf{z}^{-1}]]_\tau$, i.e. the Hilbert series we are interested in are all contained in the ring of τ-Laurent series over $\mathbb{Z}$.

b) Consider the set H of all Hilbert series of finitely generated graded P-modules. By Proposition 5.8.9.c, the sum of two such Hilbert series is again in H. It can be shown that also the product of two Hilbert series in H is again in H (see Tutorial 68 and Exercise 3). Therefore H is a subring of $\mathbb{Z}[[\mathbf{z}, \mathbf{z}^{-1}]]$.

c) Now suppose that P is positively graded by W. Then Corollary 4.2.5 shows that $\mathrm{HS}_M(\mathbf{z})$ is an element of the ring $\mathbb{Z}[[\mathbf{z}, \mathbf{z}^{-1}]]_{\mathtt{Lex}}$ for every finitely generated graded P-module M. Hence there exists one ring to rule them all: it contains all Hilbert series of all finitely generated graded modules for all positive gradings on P.

It is clear that the properties of multigraded Hilbert functions listed in Proposition 5.8.9 imply analogous properties of multivariate Hilbert series. For your convenience, we list them in the following proposition which follows immediately from Proposition 5.8.9 by comparing coefficients.

Proposition 5.8.13. (Properties of Multivariate Hilbert Series)
Let M be a finitely generated graded P-module.

a) For every $d = (d_1, \ldots, d_m) \in \mathbb{Z}^m$, the Hilbert series of $M(d)$ is given by $\mathrm{HS}_{M(d)}(z_1, \ldots, z_m) = z_1^{-d_1} \cdots z_m^{-d_m} \cdot \mathrm{HS}_M(z_1, \ldots, z_m)$.

b) Given finitely generated graded P-modules M', M'' and an exact sequence of graded P-modules

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

we have $\mathrm{HS}_M(\mathbf{z}) = \mathrm{HS}_{M'}(\mathbf{z}) + \mathrm{HS}_{M''}(\mathbf{z})$.

c) Given finitely many finitely generated graded P-modules $M_1, \ldots, M_r$, we have $\mathrm{HS}_{M_1 \oplus \cdots \oplus M_r}(\mathbf{z}) = \mathrm{HS}_{M_1}(\mathbf{z}) + \cdots + \mathrm{HS}_{M_r}(\mathbf{z})$.

d) Given a homogeneous polynomial $f \in P \setminus \{0\}$ of degree $d = (d_1, \ldots, d_m)$, we have

$$\mathrm{HS}_{M/fM}(\mathbf{z}) = \mathrm{HS}_M(\mathbf{z}) - z_1^{d_1} \cdots z_m^{d_m} \, \mathrm{HS}_{M/(0:_M(f))}(\mathbf{z})$$

In particular, we have $\mathrm{HS}_{M/fM}(\mathbf{z}) = (1 - z_1^{d_1} \cdots z_m^{d_m}) \, \mathrm{HS}_M(\mathbf{z})$ *if f is a non-zerodivisor for M.*

e) Let $\delta_1, \ldots, \delta_r \in \mathbb{Z}^m$, let M be a graded submodule of $\bigoplus_{j=1}^r P(-\delta_j)$, and let σ be a module term ordering on $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$. Then we have $\mathrm{HS}_{\mathrm{LT}_\sigma(M)}(\mathbf{z}) = \mathrm{HS}_M(\mathbf{z})$.

f) Given a field extension $K \subseteq L$, we have $\mathrm{HS}_{M \otimes_K L}(\mathbf{z}) = \mathrm{HS}_M(\mathbf{z})$.

Let us compute an actual multivariate Hilbert series.

Example 5.8.14. Let $P = K[x_1, x_2]$ be graded by $W = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. Then we have $P_{(i_1,i_2)} \neq 0$ if and only if $i_1 \geq 0$ and $i_2 \geq -i_1$. In these degrees we have $\dim_K(P_{(i_1,i_2)}) = 1$. Therefore we obtain

$$\mathrm{HS}_P(z_1, z_2) = \sum_{i_1 \geq 0} \sum_{i_2 \geq -i_1} z_1^{i_1} z_2^{i_2} = \Big(\sum_{i_1 \geq 0} z_1^{i_1} z_2^{-i_1} \Big) / (1 - z_2) = \tfrac{1}{(1 - z_1 z_2^{-1})(1 - z_2)}$$

This example suggests that there might be a simple formula for the Hilbert series of a multigraded polynomial ring. Our next theorem delivers a very satisfactory answer.

Theorem 5.8.15. (Multivariate Hilbert Series of Polynomial Rings) *Let $P = K[x_1, \ldots, x_n]$ be graded by a matrix $W = (w_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type. Then we have*

$$\mathrm{HS}_{P,W}(z_1, \ldots, z_m) = \frac{1}{\prod_{j=1}^n (1 - z_1^{w_{1j}} \cdots z_m^{w_{mj}})}$$

Proof. To prove this formula, we use induction on n. For $n = 1$, we have $\deg_W(x_1^i) = (iw_{11}, \ldots, iw_{m1})$. Therefore we obtain $\mathrm{HS}_P(z_1, \ldots, z_m) = \sum_{i \geq 0} z_1^{iw_{11}} \cdots z_m^{iw_{m1}} = 1/(1 - z_1^{w_{11}} \cdots z_m^{w_{m1}})$, i.e. the formula holds. Now consider the case $n > 1$ and let $d_n = \deg_W(x_n) = (w_{1n}, \ldots, w_{mn})$. Then Proposition 5.8.13.d yields $\mathrm{HS}_{P/(x_n)}(\mathbf{z}) = (1 - z_1^{w_{1n}} \cdots z_m^{w_{mn}}) \, \mathrm{HS}_P(\mathbf{z})$. Now we use the canonical isomorphism $P/(x_n) \cong K[x_1, \ldots, x_{n-1}]$ and the induction hypothesis to finish the proof. □

For instance, in the example above, this formula yields $\mathrm{HS}_P(z_1, z_2) = 1/((1 - z_1^0 z_2^1)(1 - z_1^1 z_2^{-1})) = 1/((1 - z_2)(1 - z_1 z_2^{-1}))$, in agreement with our direct computation. More generally, this theorem allows us to write down a formula for the multivariate Hilbert series of a finitely generated graded free P-module.

Corollary 5.8.16. *Given a graded free P-module $F = \bigoplus_{i=1}^{r} P(-\delta_i)$, where $\delta_i = (\delta_{i1}, \ldots, \delta_{im}) \in \mathbb{Z}^m$ for $i = 1, \ldots, r$, we have*

$$\mathrm{HS}_F(z_1, \ldots, z_m) = \sum_{i=1}^{r} \left(z_1^{\delta_{i1}} \cdots z_m^{\delta_{im}} / \prod_{j=1}^{n} (1 - z_1^{w_{1j}} \cdots z_m^{w_{mj}}) \right)$$

Proof. It suffices to combine the theorem and properties a) and c) of Proposition 5.8.13. □

Remark 5.8.17. Let $(i_1, \ldots, i_m) \in \mathbb{Z}^m$. Using Proposition 5.8.10 and Theorem 5.8.15, we see that the coefficient of $z_1^{i_1} \cdots z_m^{i_m}$ in the extended power series $1/\prod_{j=1}^{n}(1 - z_1^{w_{1j}} \cdots z_m^{w_{mj}})$ is the number of solutions $(a_1, \ldots, a_n) \in \mathbb{N}^n$ of the system of Diophantine equations

$$\left\{ \begin{array}{rcl} w_{11}a_1 + \cdots + w_{1n}a_n & = & i_1 \\ w_{21}a_1 + \cdots + w_{2n}a_n & = & i_2 \\ \vdots & \vdots & \vdots \\ w_{m1}a_1 + \cdots + w_{mn}a_n & = & i_m \end{array} \right.$$

For arbitrary finitely generated graded P-modules, we cannot expect to have an explicit formula for their multivariate Hilbert series such as the one in Corollary 5.8.16. But we can find an algorithm for computing this series by generalizing Proposition 5.3.1 and Theorem 5.3.2.

Theorem 5.8.18. (Computation of Multivariate Hilbert Series) *Let $P = K[x_1, \ldots, x_n]$ be graded by a matrix $W = (w_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type.*

a) Given a non-zero proper monomial ideal I in P, consider the procedure `MultMonHN`(I) *defined by the following sequence of instructions.*

1) Let $\{t_1, \ldots, t_s\}$ be the minimal monomial system of generators of I. If $s = 1$, let $(d_1, \ldots, d_m) = \deg_W(t_1) \in \mathbb{Z}^m$, return the polynomial $1 - z_1^{d_1} \cdots z_m^{d_m}$, and stop. Otherwise, let $J = (t_1, \ldots, t_{s-1})$.

2) Call the procedures `MultMonHN`(J) *and* `MultMonHN`$(J :_P (t_s))$, *and let $p_1(z_1, \ldots, z_m)$ and $p_2(z_1, \ldots, z_m)$ be the polynomials which they return.*

3) Let $(d_1, \ldots, d_m) = \deg_W(t_s)$. Return the polynomial $p_1(z_1, \ldots, z_m) - z_1^{d_1} \cdots z_m^{d_m}\, p_2(z_1, \ldots, z_m)$ and stop.

This is an algorithm which computes the polynomial $\mathrm{HN}_{P/I}(z_1, \ldots, z_m)$ in $\mathbb{Z}[z_1, \ldots, z_m]$ satisfying

$$\mathrm{HS}_{P/I}(z_1, \ldots, z_m) = \mathrm{HN}_{P/I}(z_1, \ldots, z_m) \,/\, \prod_{j=1}^{n} (1 - z_1^{w_{1j}} \cdots z_m^{w_{mj}})$$

b) Let $r \geq 1$, let $\delta_i = (\delta_{i1}, \ldots, \delta_{im}) \in \mathbb{Z}^m$ for $i = 1, \ldots, r$, let N be a graded submodule of $\bigoplus_{i=1}^{r} P(-\delta_i)$ such that $e_j \notin N$ for $j = 1, \ldots, r$, and let M be the graded P-module $M = \bigoplus_{i=1}^{r} P(-\delta_i)/N$. Consider the following sequence of instructions.

1) Compute the componentwise minimum $(\alpha_1, \ldots, \alpha_m)$ *of* $\delta_1, \ldots, \delta_r$.
2) Choose a module term ordering σ *on* $\mathbb{T}^n\langle e_1, \ldots, e_r\rangle$ *and compute* $\mathrm{LT}_\sigma(N)$ *using Buchberger's Algorithm.*
3) Let $\{t_1 e_{\gamma_1}, \ldots, t_s e_{\gamma_s}\}$ *be a system of generators of* $\mathrm{LT}_\sigma(N)$ *where* $t_1, \ldots, t_s \in \mathbb{T}^n$ *and* $\gamma_1, \ldots, \gamma_s \in \{1, \ldots, r\}$. *For* $i = 1, \ldots, r$, *let* $I_i \subseteq P$ *be the monomial ideal generated by* $\{t_j \mid 1 \leq j \leq s, \gamma_j = i\}$ *and compute* $\mathrm{HN}_{P/I_i}(z_1, \ldots, z_m)$ *by performing* `MultMonHN`(I_i).
4) Return the polynomial

$$\mathrm{HN}_M(z_1, \ldots, z_m) = \sum_{i=1}^{r} z_1^{\delta_{i1}-\alpha_1} \cdots z_m^{\delta_{im}-\alpha_m} \cdot \mathrm{HN}_{P/I_i}(z_1, \ldots, z_m)$$

and stop.

This is an algorithm which computes the polynomial $\mathrm{HN}_M(z_1, \ldots, z_m)$ *in* $\mathbb{Z}[z_1, \ldots, z_m]$ *satisfying*

$$\mathrm{HS}_M(z_1, \ldots, z_m) = z_1^{\alpha_1} \cdots z_m^{\alpha_m}\ \mathrm{HN}_M(z_1, \ldots, z_m) \,/\, \prod_{j=1}^{n} (1 - z_1^{w_{1j}} \cdots z_m^{w_{mj}})$$

Proof. First we show a). Finiteness follows exactly as in the proof of Theorem 5.3.2. To prove correctness we note that, for $s = 1$, the claim follows from Propositions 5.8.13.d and 5.8.15. For $s > 1$, we use induction on the recursion and Proposition 5.8.13.d again to conclude that $\mathrm{HS}_{P/I}(z_1, \ldots, z_m)$ has the desired shape.

The proof of b) proceeds exactly as the proof of Proposition 5.3.1, except that we have to replace the references to Proposition 5.2.15 by references to the corresponding parts of Proposition 5.8.13. □

This theorem shows that the multivariate Hilbert series of a finitely generated graded P-module has a shape which generalizes the shape described in Theorem 5.2.20.

Corollary 5.8.19. *For every finitely generated graded* P*-module* M, *the multivariate Hilbert series of* M *has the form*

$$\mathrm{HS}_{M,W}(z_1, \ldots, z_m) = \frac{z_1^{\alpha_1} \cdots z_m^{\alpha_m} \cdot \mathrm{HN}_M(z_1, \ldots, z_m)}{\prod_{j=1}^{n} (1 - z_1^{w_{1j}} \cdots z_m^{w_{mj}})}$$

where $(\alpha_1, \ldots, \alpha_m)$ *is the componentwise minimum of the degree sequence of* M, *and where* $\mathrm{HN}_M(z_1, \ldots, z_m)$ *is a polynomial in* $\mathbb{Z}[z_1, \ldots, z_m]$. *We call this polynomial the* **multivariate Hilbert numerator** *of* M.

Remark 5.8.20. The preceding theorem is the multivariate version of the Classical Hilbert Numerator Algorithm 5.3.2. Similarly, it is not difficult to generalize Theorem 5.3.7 to compute multivariate Hilbert numerators using strategies. All strategies discussed in Section 5.3 can be used in this case.

As usual, the best way to appreciate an algorithm is to apply it to some concrete cases.

Example 5.8.21. Let $P = \mathbb{Q}[x_1, x_2, x_3, x_4]$ be graded by $W = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 5 & 8 \end{smallmatrix}\right)$, and let $I = (x_1^2, x_2, x_3^3)$. We want to apply the algorithm of Theorem 5.8.18.a to compute the multivariate Hilbert series of P/I.

In the first step, we form $J = (x_1^2, x_2)$. In the second step, we compute the Hilbert numerators of P/J and of $P/(J :_P (x_3^3))$ recursively. In this case $J :_P (x_3^3) = (x_1^2, x_2)$ is equal to J. When we compute $\mathrm{HN}_{P/J}(z_1, z_2)$, we form $J' = (x_1^2)$ and $J'' = J :_P (x_2) = (x_1^2)$ and apply the algorithm recursively to them. Since $J' = J'' = (x_1^2)$ is a principal ideal, the algorithm yields $\mathrm{HN}_{P/J'}(z_1, z_2) = \mathrm{HN}_{P/J''}(z_1, z_2) = 1 - z_1^2$. Then we find $\mathrm{HN}_{P/J}(z_1, z_2) = \mathrm{HN}_{P/J'}(z_1, z_2) - z_1^2 \,\mathrm{HN}_{P/J''}(z_1, z_2) = (1 - z_1^2)^2$ in step 3). Thus the original algorithm computes $\mathrm{HN}_{P/I}(z_1, z_2) = \mathrm{HN}_{P/J}(z_1, z_2) - z_1^9 z_2^{15} \,\mathrm{HN}_{P/(J:_P(x_3^3))}(z_1, z_2) = (1 - z_1^2)^2(1 - z_1^9 z_2^{15})$. Altogether, we have

$$\mathrm{HS}_{P/I}(z_1, z_2) = \frac{(1-z_1^2)^2(1-z_1^9 z_2^{15})}{(1-z_1)(1-z_1^2)(1-z_1^3 z_2^5)(1-z_1^4 z_2^8)} = \frac{(1+z_1)(1+z_1^3 z_2^5+z_1^6 z_2^{10})}{1-z_1^4 z_2^8}$$

Example 5.8.22. Let $P = \mathbb{Q}[x_1, x_2, x_3]$ be graded by $W = \left(\begin{smallmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \end{smallmatrix}\right)$, and let $I = (x_1^3 x_2,\, x_2 x_3^2,\, x_2^2 x_3,\, x_3^4)$. We want to apply the algorithm of Theorem 5.8.18.a to compute the multivariate Hilbert series of P/I.

In the first steps, we form the ideals $J_1 = (x_1^3 x_2,\, x_2 x_3^2,\, x_2^2 x_3)$ and $J_2 = J_1 :_P (x_3^4) = (x_2)$ and apply the algorithm recursively to them. For J_2, it yields $\mathrm{HN}_{P/J_2}(z_1, z_2) = 1 - z_1$ in step 1). For J_1, we form $J_{11} = (x_1^3 x_2,\, x_2 x_3^2)$ and $J_{12} = J_1 :_P (x_2^2 x_3) = (x_1^3, x_3)$ and apply the algorithm recursively to these. Again the computation of $\mathrm{HN}_{P/J_{11}}(z_1, z_2)$ splits into $\mathrm{HN}_{P/(x_1^3 x_2)}(z_1, z_2) = 1 - z_1^4$ and $\mathrm{HN}_{P/(J_{11}:_P(x_2 x_3^2))}(z_1, z_2) = \mathrm{HN}_{P/(x_1^3)}(z_1, z_2) = 1 - z_1^3$. The result is $\mathrm{HN}_{P/J_{11}}(z_1, z_2) = (1 - z_1^4) - z_1^3 z_2^{-2}(1 - z_1^3)$. Similarly, the computation of $\mathrm{HN}_{P/J_{12}}(z_1, z_2)$ splits into $\mathrm{HN}_{P/(x_1^3)}(z_1, z_2) = 1 - z_1^3$ and $\mathrm{HN}_{P/(J_{12}:_P(x_3))}(z_1, z_2) = \mathrm{HN}_{P/(x_1^3)}(z_1, z_2) = 1 - z_1^3$. The result is $\mathrm{HN}_{P/J_{12}}(z_1, z_2) = (1 - z_1^3)(1 - z_1 z_2^{-1})$.

Coming back to the computation of $\mathrm{HN}_{P/J_1}(z_1, z_2)$, we now obtain $\mathrm{HN}_{P/J_1}(z_1, z_2) = \mathrm{HN}_{P/J_{11}}(z_1, z_2) - z_1^3 z_2^{-1} \,\mathrm{HN}_{P/J_{12}}(z_1, z_2) = 1 - z_1^4 + (1 - z_1^3) \cdot (z_1^4 z_2^{-2} - z_1^3 z_2^{-2} - z_1^3 z_2^{-1})$. Finally, the algorithm returns $\mathrm{HN}_{P/I}(z_1, z_2) = \mathrm{HN}_{P/J_1}(z_1, z_2) - z_1^4 z_2^{-4} \,\mathrm{HN}_{P/J_2}(z_1, z_2) = (1 - z_1)(1 - z_1 z_2^{-1})(-z_1^5 z_2^{-1} + z_1^3 z_2^{-3} + z_1^2 z_2^{-2} + z_1^3 + z_1^2 z_2^{-1} + z_1^2 + z_1 z_2^{-1} + z_1 + 1)$. Therefore the multivariate Hilbert series of P/I is

$$\mathrm{HS}_{P/I}(z_1, z_2) = \frac{-z_1^5 z_2^{-1} + z_1^3 z_2^{-3} + z_1^2 z_2^{-2} + z_1^3 + z_1^2 z_2^{-1} + z_1^2 + z_1 z_2^{-1} + z_1 + 1}{1 - z_1}$$

Example 5.8.23. Let $P = \mathbb{Q}[x_1, x_2, x_3]$ be graded by $W = \left(\begin{smallmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \end{smallmatrix}\right)$, and let M be the finitely generated graded P-module $M = (P(-\binom{3}{0}) \oplus P)/N$, where $N = \langle (x_1, x_1^3 x_2), (0, x_2 x_3^2), (0, x_2^2 x_3), (x_3^3, 0), (0, x_3^4) \rangle$. We want to apply

the algorithm of Theorem 5.8.18.b to compute the multivariate Hilbert series of M. Let us follow the steps of the algorithm.

1) We compute $(\alpha_1, \alpha_2) = (0, 0)$.
2) We choose $\sigma =$ `DegRevLexPos` and compute $\mathrm{LT}_\sigma(N) = \langle (x_1x_2x_3, 0), (x_1x_3^2, 0), (x_3^3, 0), (0, x_1^3x_2), (0, x_2^2x_3), (0, x_2x_3^2), (0, x_3^4)\rangle$.
3) We apply the procedure `MultMonHN(...)` to $I_1 = (x_1x_2x_3,\, x_1x_3^2,\, x_3^3)$ and $I_2 = (x_1^3x_2,\, x_2^2x_3,\, x_2x_3^2,\, x_3^4)$. It yields $\mathrm{HN}_{P/I_1}(z_1, z_2) = (1 - z_1z_2^{-1}) \cdot (-z_1^3z_2^{-2} - z_1^3z_2^{-1} + z_1^2z_2^{-2} + z_1z_2^{-1} + 1)$ and, for $\mathrm{HN}_{P/I_2}(z_1, z_2)$, the result computed in Example 5.8.22.
4) Return the result $\mathrm{HN}_M(z_1, z_2) = z_1^3\ \mathrm{HN}_{P/I_1}(z_1, z_2) + \mathrm{HN}_{P/I_2}(z_1, z_2) = (1 - z_1z_2^{-1})(-z_1^6z_2^{-2} + z_1^5z_2^{-2} - z_1^4z_2^{-3} - z_1^5z_2^{-1} + z_1^3z_2^{-3} + z_1^4z_2^{-1} - z_1^3z_2^{-2} - z_1^4 - z_1^3z_2^{-1} + z_1^2z_2^{-2} + z_1^3 + z_1z_2^{-1} + 1)$ and stop.

Thus the multivariate Hilbert series of M is $\mathrm{HS}_M(z_1, z_2) = \frac{\mathrm{HN}_M(z_1,z_2)}{(1-z_1)^2(1-z_1z_2^{-1})} = \frac{-z_1^6z_2^{-2}+z_1^5z_2^{-2}-z_1^4z_2^{-3}-z_1^5z_2^{-1}+z_1^3z_2^{-3}+z_1^4z_2^{-1}-z_1^3z_2^{-2}-z_1^4-z_1^3z_2^{-1}+z_1^2z_2^{-2}+z_1^3+z_1z_2^{-1}+1}{(1-z_1)^2}$.

5.8.C Change of Gradings

Instead of using magic,
refiners employ processing technology
to perform their unique brand of metamorphosis.
(Emanueal B. Noél)

In the final part of this section we study the relationship between multivariate Hilbert series of the same module arising from different metamorphoses, such as changes of gradings and refinements. We try to present the subject so that it should not appear to be a bag of magic tricks. Instead we use the processing technology developed in the preceding subsection. The basic question is the following: what happens to the Hilbert series when we change the grading? In particular, what happens when we use a coarser grading than our original one?

Given a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ which defines a grading on P and a matrix $A \in \mathrm{Mat}_{\ell,m}(\mathbb{Z})$ with $1 \le \ell \le m$, the $\mathbb{Z}$-linear map $\varphi : \mathbb{Z}^m \longrightarrow \mathbb{Z}^\ell$ whose defining matrix is A yields a homomorphism of graded rings

$$(\mathrm{id}_P, \varphi) :\ (P, \mathbb{Z}^m)\ \longrightarrow\ (P, \mathbb{Z}^\ell)$$

Given a graded module M over $(P, \mathbb{Z}^m)$, we can equip it with the structure of a graded $(P, \mathbb{Z}^\ell)$-module by defining

$$M_{A\cdot W,e} = \begin{cases} \bigoplus_{\{d\in\mathbb{Z}^m \mid A\cdot d = e\}} M_{W,d} & \text{if } e \in \mathrm{Im}(\varphi), \\ 0 & \text{otherwise.} \end{cases}$$

We shall say that the graded module $M = \bigoplus_{e\in\mathbb{Z}^\ell} M_{A\cdot W,e}$ is obtained from $M = \bigoplus_{d\in\mathbb{Z}^m} M_{W,d}$ by a **change of grading**.

Proposition 5.8.24. *Let $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ and $A = (a_{ij}) \in \mathrm{Mat}_{\ell,m}(\mathbb{Z})$ be two matrices such that the gradings on $P = K[x_1, \ldots, x_n]$ given by W and by $A \cdot W$ are both of positive type. Let M be a finitely generated P-module which is graded with respect to the grading given by W. Then the Hilbert series of M with respect to the grading given by $A \cdot W$ is*

$$\mathrm{HS}_{M,A\cdot W}(z_1, \ldots, z_\ell) = \mathrm{HS}_{M,W}(z_1^{a_{11}} \cdots z_\ell^{a_{\ell 1}}, \ldots, z_1^{a_{1m}} \cdots z_\ell^{a_{\ell m}})$$

Proof. The assumption that both W and $A \cdot W$ define gradings of positive type implies that $\mathrm{rk}(W) = m$ and $\mathrm{rk}(A \cdot W) = \ell$. Therefore the matrix A has maximal rank $\mathrm{rk}(A) = \ell$. By the definition of the grading, we have

$$\begin{aligned}
\mathrm{HS}_{M,A\cdot W}\ (\ z_1, \ldots, z_\ell) &= \sum_{e\in\mathbb{Z}^\ell} \sum_{\{d\in\mathbb{Z}^m \mid A\cdot d = e\}} \dim_K(M_{W,d})\, z_1^{e_1} \cdots z_\ell^{e_\ell} \\
&= \sum_{e\in\mathbb{Z}^\ell} \sum_{\{d\in\mathbb{Z}^m \mid A\cdot d = e\}} \dim_K(M_{W,d})\, z_1^{a_{11}d_1 + \cdots + a_{1m}d_m} \cdots z_\ell^{a_{\ell 1}d_1 + \cdots + a_{\ell m}d_m} \\
&= \sum_{e\in\mathbb{Z}^\ell} \sum_{\{d\in\mathbb{Z}^m \mid A\cdot d = e\}} \dim_K(M_{W,d})\, (z_1^{a_{11}} \cdots z_\ell^{a_{\ell 1}})^{d_1} \cdots (z_1^{a_{1m}} \cdots z_\ell^{a_{\ell m}})^{d_m} \\
&= \sum_{d\in\mathbb{Z}^m} \mathrm{HF}_{M,W}(d) (z_1^{a_{11}} \cdots z_\ell^{a_{\ell 1}})^{d_1} \cdots (z_1^{a_{1m}} \cdots z_\ell^{a_{\ell m}})^{d_m} \\
&= \mathrm{HS}_{M,W}(z_1^{a_{11}} \cdots z_\ell^{a_{\ell 1}}, \ldots, z_1^{a_{1m}} \cdots z_\ell^{a_{\ell m}})
\end{aligned}$$

as claimed. □

Example 5.8.25. Let $P = K[x_1, x_2, x_3]$ be graded by $W = \left(\begin{smallmatrix} -1 & 1 & 2 \\ 2 & 0 & 1 \end{smallmatrix}\right)$, and let $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Then we have $\mathrm{HS}_{P,W}(z_1, z_2) = 1/((1 - z_1^{-1}z_2^2)(1 - z_1)(1 - z_1^2 z_2))$ and $A \cdot W = \left(\begin{smallmatrix} 1 & 1 & 3 \\ 2 & 0 & 1 \end{smallmatrix}\right)$. The Hilbert series of P with respect to the grading given by $A \cdot W$ is $\mathrm{HS}_{P,A\cdot W}(z_1, z_2) = 1/((1 - z_1 z_2^2)(1 - z_1)(1 - z_1^3 z_2)) = \mathrm{HS}_{P,W}(z_1, z_1 z_2)$, in accordance with the proposition.

An important special case occurs when $A \cdot W$ is the submatrix of W which consists of the first ℓ rows of W. In this case we use the following terminology.

Definition 5.8.26. Let the polynomial ring $P = K[x_1, \ldots, x_n]$ be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $\ell \in \{1, \ldots, m\}$, and let $W = \left(\begin{smallmatrix} U \\ V \end{smallmatrix}\right)$, where $U \in \mathrm{Mat}_{\ell,n}(\mathbb{Z})$ and $V \in \mathrm{Mat}_{m-\ell,n}(\mathbb{Z})$. Then we say that the grading on P given by W **refines** the grading given by U, or that the the grading given by W is a **refinement** of the grading given by U.

To simplify the notation, we denote the concatenation of $d \in \mathbb{Z}^\ell$ and $e \in \mathbb{Z}^{m-\ell}$ by $(d, e) \in \mathbb{Z}^m$. We let $o = (0, \ldots, 0) \in \mathbb{Z}^\ell$. Then the K-vector space $P_{U,o} = \bigoplus_{e\in\mathbb{Z}^{m-\ell}} P_{(o,e)}$ is a graded K-algebra and for every $d \in \mathbb{Z}^\ell$, the K-vector space $M_{U,d} = \bigoplus_{e\in\mathbb{Z}^{m-\ell}} M_{(d,e)}$ is a graded $P_{U,o}$-module.

The following corollary allows us to pass from the multivariate Hilbert series of the module M with respect to the grading given by W to its multivariate Hilbert series with respect to the grading given by U.

Corollary 5.8.27. *Let $U \in \mathrm{Mat}_{\ell,n}(\mathbb{Z})$ be a matrix of positive type, let $V \in \mathrm{Mat}_{m-\ell,n}(\mathbb{Z})$, and let $W = \binom{U}{V} \in \mathrm{Mat}_{m,n}(\mathbb{Z})$.*

a) We have $\mathrm{HS}_{M,U}(z_1,\ldots,z_\ell) = \mathrm{HS}_{M,W}(z_1,\ldots,z_\ell,1,\ldots,1)$.

b) We have $P_{U,o} = K$ and for every $d \in \mathbb{Z}^\ell$, we have $\dim_K(M_{U,d}) = \sum_{e\in\mathbb{Z}^{m-\ell}} \dim_K(M_{(d,e)})$.

Proof. Claim a) follows from Proposition 5.8.24 by using the change of grading defined by $A = (\mathcal{I}_\ell \mid 0) \in \mathrm{Mat}_{\ell,m}(\mathbb{Z})$. Claim b) is obtained from a) by comparing coefficients. □

If the grading given by U is not of positive type, the vector space dimension of $P_{U,o}$ can be infinite. For instance, if we equip $P = \mathbb{Q}[x,y]$ with the grading given by $W = \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$ and use $U = (1\ 0)$, we have $P_{U,o} = K[y]$. In the corollary, we substitute $z_2 = 1$ in $\mathrm{HS}_{P,W}(z_1,z_2)$. But in our case this is not possible since $\mathrm{HS}_{P,W}(z_1,z_2) = \frac{1}{(1-z_1z_2)(1-z_2)}$. However, the ring $P_{U,o}$ is always a finitely generated K-algebra, as we shall see in Section 6.1.

Exercise 1. Find monoid orderings σ,τ on $\mathbb{Z}^m$ and an extended power series $f \in \mathbb{Z}[[\mathbf{z},\mathbf{z}^{-1}]]$ such that f is a σ-Laurent series but not a τ-Laurent series.

Exercise 2. Find the number of solutions in $\mathbb{N}^4$ of the following system of Diophantine equations.

$$\begin{cases} a_1 + 2a_2 + 3a_3 + 4a_4 = 15 \\ a_1 + 3a_2 + a_4 = 12 \end{cases}$$

Exercise 3. (*Note:* To do this exercise, you need tensor products of vector spaces. If necessary, you may want to solve the corresponding parts of Tutorial 68 first.)
Let K be a field, let the polynomial ring $P = K[x_1,\ldots,x_n]$ be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type, and let M, M' be finitely generated graded P-modules.

a) Show that there exists a finitely generated graded P-module $M \otimes_P M'$ such that $(M \otimes_P M')_d = \bigoplus_{i+j=d} M_i \otimes_K M'_j$ for all $d \in \mathbb{Z}^m$.

b) Conclude that the multivariate Hilbert series of $M \otimes_P M'$ is the product $\mathrm{HS}_M(\mathbf{z}) \cdot \mathrm{HS}_{M'}(\mathbf{z})$.

Exercise 4. Let K be a field, and let $P = K[x,y]$ be graded by the matrix $W = (1\ 2)$. Compute the Hilbert series of P and show that there are polynomials $p_1,p_2 \in \mathbb{Q}[t]$ such that $\mathrm{HF}_P(i) = \begin{cases} p_1(i) & \text{if } i \geq 0 \text{ is even,} \\ p_2(i) & \text{if } i \geq 1 \text{ is odd.} \end{cases}$

Exercise 5. Let K be a field, let $P = K[x_1,\ldots,x_n]$ be graded by a matrix $W = (w_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ of positive type, and let $f_1,\ldots,f_s$ be a homogeneous regular sequence in P. For $i = 1,\ldots,s$, let $(d_{i1},\ldots,d_{im}) = \deg_W(f_i) \in \mathbb{Z}^m$. Show that

$$\mathrm{HS}_{P/(f_1,\ldots,f_s)}(z_1,\ldots,z_m) = \frac{\prod_{i=1}^s (1 - z_1^{d_{i1}} \cdots z_m^{d_{im}})}{\prod_{j=1}^n (1 - z_1^{w_{1j}} \cdots z_m^{w_{mj}})}$$

Exercise 6. Let K be a field, and let $P = K[x_1, x_2, x_3]$ be graded by $W = \left(\begin{smallmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \end{smallmatrix}\right)$. Show that the ideal $I = (x_1x_2x_3,\ x_1x_3^2,\ x_3^3)$ has Hilbert numerator $\mathrm{HN}_{P/I}(z_1, z_2) = (1 - z_1z_2^{-1})(-z_1^3z_2^{-2} - z_1^3z_2^{-1} + z_1^2z_2^{-2} + z_1z_2^{-1} + 1)$.

Exercise 7. Let K be a field, let $P = K[x_1, x_2, x_3, x_4]$ be graded by the matrix $W = \left(\begin{smallmatrix} 1 & 1 & 2 & 2 \\ 3 & 3 & 1 & 1 \end{smallmatrix}\right)$, and let $f = x_1x_3 - x_2x_4$. Compute the multivariate Hilbert series of $P/(f)$ in the following two ways and compare the results:

a) Using Proposition 5.8.13.d.
b) Using the grading defined by $\left(\begin{smallmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{smallmatrix}\right)$ and Proposition 5.8.24.

Exercise 8. Let the polynomial ring $P = \mathbb{Q}[x_1, \ldots, x_5]$ be graded by $W = \left(\begin{smallmatrix} 1 & 1 & 1 & 2 & 2 \\ 3 & 1 & 0 & 1 & 0 \end{smallmatrix}\right)$, let $U = (1\ 1\ 1\ 2\ 2)$, and let $I \subseteq P$ be the ideal generated by $\{x_1x_3^8 - x_3^3x_4^3 - x_2x_4^2x_5^2,\ x_1x_4^2 - x_2^5,\ x_2^3x_4 + x_1x_2x_3^3 - x_1x_3^2x_4\}$. Using CoCoA, compute the Hilbert series $\mathrm{HS}_{P/I,W}(z_1, z_2)$ and $\mathrm{HS}_{P/I,U}(z_1)$. Verify the formula of Corollary 5.8.27.a.

Tutorial 80: Hilbert Driven Gröbner Basis Computations II

The best computer is a man,
and it's the only one
that can be mass-produced
by unskilled labor.
(Wernher Von Braun)

In Tutorial 69 we used the knowledge of the Hilbert series of a graded module to guide the computation of a homogeneous Gröbner basis. However, our results were limited to the standard graded setting. This tutorial takes off where part I ends. The first step is to generalize the Hilbert Driven Buchberger Algorithm to the case of an arbitrary positive $\mathbb{Z}$-grading. To perform this task, all you have to do is to turn your built-in computer on and rework the first items of Tutorial 69 thoughtfully.

When it comes to the general problem of computing Gröbner bases in a positively $\mathbb{Z}^m$-graded setting with $m > 1$, unskilled labour is not going to suffice anymore. If we were to recompute the Hilbert series every time we have finished the computations in a fixed multidegree, we would slow down our computer because we do way too much work. This is because the computations in two multidegrees whose first components agree cannot interfere with each other. In other words, if we find new Gröbner basis elements in one multidegree, the Hilbert function of the module the Gröbner basis elements generate does not change in the other multidegree. Hence we recompute the Hilbert series more selectively and get a nice and fast algorithm.

This leaves us with only one fly in the ointment: how do we know the Hilbert series of the module whose Gröbner basis we are after? Usually, we don't. But sometimes we may be able to apply our neural computer in a clever way. For these purposes it is an excellent device, and can be used for free.

Let K be a field, and let $P = K[x_1, \ldots, x_n]$ be $\mathbb{Z}$-graded by a positive matrix $W \in \mathrm{Mat}_{1,n}(\mathbb{Z})$.

a) Given a finitely generated graded P-module M with initial degree α, a number $j \in \mathbb{Z}$, and a graded submodule $N \subseteq M$ such that $N_i = M_i$ for $i < j$, prove that the following conditions are equivalent.
   1) $N_j \subset M_j$
   2) $\dim_K(M_j) - \dim_K(N_j) > 0$
   3) There exists a positive integer c_j such that $\mathrm{HN}_M(z) - \mathrm{HN}_N(z) = c_j z^{j-\alpha} + (\textit{terms of higher degree})$.

   Show that $c_j = \dim_K(M_j) - \dim_K(N_j)$ if these conditions are satisfied.

Let us now apply this observation to generalize the Hilbert Driven Buchberger Algorithm. Assume that we are computing a σ-Gröbner basis of a graded submodule M of $F = \bigoplus_{i=1}^{r} P(-\delta_i)$ using the Homogeneous Buchberger Algorithm 4.5.5, and also that we have just finished some degree d. Suppose additionally that we know the Hilbert numerator of M and that a computation of the Hilbert numerator of $N = \langle \mathrm{LT}_\sigma(\mathcal{G}) \rangle$ yields $\mathrm{HN}_M(z) - \mathrm{HN}_N(z) = c_j z^{j-\alpha} + (\textit{terms of higher degree})$ with $c_j > 0$.

c) Prove that $N_i = M_i$ for $i < j$, that $j > d$, and that there are neither reduced σ-Gröbner basis elements nor minimal homogeneous generators of M in degrees $d+1, \ldots, j-1$.

d) Show that $c_j \leq \#B_j + \#\mathcal{W}_j$ and that the reduced σ-Gröbner basis of M contains exactly c_j elements of degree j.

e) In the Homogeneous Buchberger Algorithm 4.5.5, replace steps 2), 3) and 6) by the following instructions.

   2') Let $N = \langle \mathrm{LT}_\sigma(\mathcal{G}) \rangle$. Compute the polynomial $\mathrm{HN}_M(z) - \mathrm{HN}_N(z)$. If it is zero, return $\mathcal{G}$ and stop. Otherwise, let $d \geq \alpha$ and $c_d > 0$ be such that $\mathrm{HN}_M(z) - \mathrm{HN}_N(z) = c_d z^{d-\alpha} + (\textit{terms of higher degree})$. Form the subset B_d of B, form the subtuple $\mathcal{W}_d$ of $\mathcal{W}$, and delete their entries from B and $\mathcal{W}$, respectively.

   3') If $B_d = \emptyset$ or if $\mathcal{G}$ contains c_d elements of degree d, continue with step 6'). Otherwise, choose a pair $(i, j) \in B_d$ and remove it from B_d.

   6') If $\mathcal{W}_d = \emptyset$ or if $\mathcal{G}$ contains c_d elements of degree d, continue with step 9). Otherwise, choose a vector $v \in \mathcal{W}_d$ and remove it from $\mathcal{W}_d$.

   Show that the resulting sequence of instructions defines an algorithm which computes a homogeneous σ-Gröbner basis of M. We call it the **Weighted Hilbert Driven Buchberger Algorithm**.

f) Implement the Weighted Hilbert Driven Buchberger Algorithm in a CoCoA function `WeightedHDBA(...)`. Apply this function to compute the `PosLex`-Gröbner bases of the following ideals or modules. In each case, use CoCoA first to compute the Hilbert series of M_i via its `DegRevLexPos`-Gröbner basis.

1) $M_1 = (x_1^2 - x_2^5, x_1^3 - x_3^4, x_1^4 - x_4^4) \subseteq \mathbb{Q}[x_1, x_2, x_3, x_4]$ graded by the matrix $W = (20\ 8\ 15\ 20)$
2) $M_2 = (x_1^6 - x_1x_3 + x_2^2,\ x_1^4x_2^2 - x_1^2x_2x_3 - x_3^2,\ x_1^{10} - x_3^2) \subseteq \mathbb{Q}[x_1, x_2, x_3]$ graded by the matrix $W = (1\ 3\ 5)$
3) $M_3 = \langle (0, x_2x_3, x_1^2x_3),\ (0, x_1x_3^2, x_1x_2^3 - x_1x_3^2),\ (x_2^5x_3^2, x_1x_3^5 - x_1x_4^3),\ (x_1x_2^2, x_2x_3, 0),\ (x_1^3x_2, 0, x_2x_3)\rangle \subseteq \mathbb{Q}[x_1, x_2, x_3]^3$ where $\mathbb{Q}[x_1, x_2, x_3]$ is graded by the matrix $W = (1\ 2\ 3\ 5)$

So far the generalization of the standard graded case has been straightforward. In the following we treat the truly multigraded setting, i.e. the setting where P is positively graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ for which $m > 1$. We could generalize the Weighted Hilbert Driven Buchberger Algorithm in the obvious way. But experience shows that the resulting algorithm performs poorly. How come? Roughly speaking, the reason is that a multigrading splits the module more than a simple grading, and different multidegrees can be totally independent of each other. This causes the following effect.

As above, we are assuming that we are computing a σ-Gröbner basis of a graded submodule M of $F = \bigoplus_{i=1}^r P(-\delta_i)$ using the Homogeneous Buchberger Algorithm 4.5.5, and that we have just finished looping through steps 3)–8) for some degree $d \in \mathbb{Z}^m$. Let $N = \langle \mathrm{LT}_\sigma(\mathcal{G})\rangle$ be the graded submodule of M generated by the elements of the Gröbner basis found up to this point.

g) Suppose that W is of the form $W = \binom{U}{V}$ with $V \in \mathrm{Mat}_{m-1,n}(\mathbb{Z})$ and with a positive matrix $U \in \mathrm{Mat}_{1,n}(\mathbb{Z})$. Moreover, suppose that there exist two distinct degrees $d_1 = \binom{\delta}{d_1'}$ and $d_2 = \binom{\delta}{d_2'}$ with $\delta \in \mathbb{Z}$ and $d_1', d_2' \in \mathbb{Z}^{m-1}$ for which $\mathrm{HF}_M(d_i) - \mathrm{HF}_N(d_i) > 0$ for $i = 1, 2$. Show that the submodule $N' = N + \langle M_{d_1}\rangle$ of M satisfies $\mathrm{HF}_{N'}(d_2) = \mathrm{HF}_N(d_2)$.

Therefore the process of *filling the gap* at d_1, i.e. looping through steps 3)–8) in degree d_1 until $\mathcal{G}$ contains the predicted number of elements of degree d_1, does not change the Hilbert function of $\langle\mathcal{G}\rangle$ in degree d_2. Similarly, filling the gap in degree d_2 is independent of filling the gap in degree d_1. So it would be a waste of time to recompute the Hilbert function of $\langle\mathcal{G}\rangle$ after the loop in degree d_1 has been completed. This observation suggests the following procedure.

h) Let W be of the form $W = \binom{U}{V}$ with a positive matrix $U \in \mathrm{Mat}_{1,n}(\mathbb{Z})$ and with $V \in \mathrm{Mat}_{m-1,n}(\mathbb{Z})$. In the Homogeneous Buchberger Algorithm 4.5.5, replace steps 1), 2), 3) and 6) by the following instructions.
   1') Let $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\delta = \min\{\deg_U(v_i) \mid i = 1, \ldots, s\}$, $\mathcal{G} = \emptyset$, and $s' = 0$.
   2') Let d be the smallest degree with respect to `Lex` of an element in B or in $\mathcal{W}$. If the first component of d equals δ then form the subset B_d of B, form the subtuple $\mathcal{W}_d$ of $\mathcal{W}$, and delete their entries from B and $\mathcal{W}$, respectively. Otherwise, let $N = \langle \mathrm{LT}_\sigma(\mathcal{G})\rangle$. Compute the polynomial $\mathrm{HN}_M(z) - \mathrm{HN}_N(z)$. If it is zero, return $\mathcal{G}$ and stop. If it

is non-zero, let $d \geq \alpha$ and $c_d > 0$ be such that $\mathrm{HN}_M(z) - \mathrm{HN}_N(z) = c_d z^{d-\alpha} + (\textit{terms of higher degree})$. Form the subset B_d of B, form the subtuple $\mathcal{W}_d$ of $\mathcal{W}$, and delete their entries from B and $\mathcal{W}$, respectively. Replace δ with the first component of d.

3') If $B_d = \emptyset$ or if $\mathcal{G}$ contains c_d elements of degree d, continue with step 6'). Otherwise, choose a pair $(i, j) \in B_d$ and remove it from B_d.

6') If $\mathcal{W}_d = \emptyset$ or if $\mathcal{G}$ contains c_d elements of degree d, continue with step 9). Otherwise, choose a vector $v \in \mathcal{W}_d$ and remove it from $\mathcal{W}_d$.

Show that the resulting sequence of instructions defines an algorithm which computes a homogeneous σ-Gröbner basis of M. We call it the **Multigraded Hilbert Driven Buchberger Algorithm**.

i) Implement the Multigraded Hilbert Driven Buchberger Algorithm in a CoCoA function `MultiHDBA(...)`.

j) Let the polynomial ring $\mathbb{Q}[x_1, \ldots, x_5]$ be graded by $W = \left(\begin{smallmatrix} 1 & 1 & 1 & 2 & 2 \\ 3 & 1 & 0 & 1 & 0 \end{smallmatrix}\right)$, and let $I_1 = (x_1x_3^8 - x_3^3x_4^3 - x_2x_4^2x_5^2,\ x_1x_4^2 - x_2^5,\ x_2^3x_4 + x_1x_2x_3^3 - x_1x_3^2x_4)$. Using CoCoA, compute a `DegRevLex`-Gröbner basis of I_1. Then determine the Hilbert numerator of I_1 and use it to drive the computation of a `Lex`-Gröbner basis of I_1 via `MultiHDBA(...)`.

k) Let $\mathbb{Q}[x_1, \ldots, x_6, y_1, \ldots, y_8]$ be graded by $W = \left(\begin{smallmatrix} 2&2&2&2&2&2&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&0&0&0 \end{smallmatrix}\right)$, and let $I_2 = (x_1 - y_1y_6 + y_2y_5,\ x_2 - y_1y_7 + y_3y_5,\ x_3 - y_1y_8 + y_4y_5,\ x_4 - y_2y_7 + y_3y_6,\ x_5 - y_2y_8 + y_4y_6,\ x_6 - y_3y_8 + y_4y_7)$. Using the lexicographic term ordering such that $x_1 >_{\mathtt{Lex}} \cdots >_{\mathtt{Lex}} x_6 >_{\mathtt{Lex}} y_1 >_{\mathtt{Lex}} \cdots >_{\mathtt{Lex}} y_8$, find the Hilbert numerator of I_2. Then pass it to your function `MultiHDBA(...)` to compute an `Elim(L)`-Gröbner basis of I_2 where $L = \{y_1, \ldots, y_8\}$.

Finally, you may object that the matrix W does not always have a positive first row. This objection is valid, but it is not difficult to clear this small hurdle.

l) Let $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ be a positive matrix. Write a CoCoA function which computes a non-singular matrix $A \in \mathrm{Mat}_m(\mathbb{Z})$ such that the first row of $A \cdot W$ consists of positive integers only.

m) Let P be graded by a positive matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let M be a graded submodule of a graded free P-module which is given by a homogenous set of generators. Explain how one can use l) and the Multigraded Hilbert Driven Buchberger Algorithm to compute a homogeneous Gröbner basis of M. (*Hint:* Use Proposition 4.1.14.)

The best ideas are common property.
(Seneca the Younger)

Tutorial 81: Rees Rings

There really are only two types
of people in the world,
those that don't do Math,
and those that take care of them.
(Anonymous)

Rees rings are important tools, both in commutative algebra and in algebraic geometry. A thorough explanation of their geometric meaning exceeds the scope of this book. For us, they are interesting examples for the theory of multigradings. In fact, you will be surprised to see how well-suited the results of this section are to defining a natural bigrading on a Rees ring and to computing the corresponding multivariate Hilbert series. One of the applications of this procedure is that we can take care of the people who *don't do Math*. A more common application is a clever way to compute the Hilbert series of the powers of an ideal.

Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let $\overline{P} = K[x_1, \ldots, x_n, t]$ where t is a new indeterminate. We equip $\overline{P}$ with the grading defined by the matrix $U = (0 \ \ldots \ 0 \ 1) \in \mathrm{Mat}_{1,n+1}(\mathbb{Z})$. Let I be an ideal in P which is generated by polynomials $f_1, \ldots, f_s$. The **Rees ring** of I is defined as the K-vector subspace $\mathcal{R}(I) = \bigoplus_{d \in \mathbb{N}} I^d \, t^d$ of $\overline{P}$.

a) Show that $\mathcal{R}(I)$ is a graded K-subalgebra of $\overline{P}$ with respect to the grading defined by U.
b) Prove that the polynomials $f_1 \, t, \ldots, f_s \, t$ generate the Rees ring $\mathcal{R}(I)$ as a P-algebra.
c) Conclude that we can choose further indeterminates $y_1, \ldots, y_s$ and define a surjective K-algebra homomorphism $\varphi : P[y_1, \ldots, y_s] \longrightarrow \mathcal{R}(I)$ such that $\varphi(y_i) = f_i \, t$ for $i = 1, \ldots, s$. Can you equip $P[y_1, \ldots, y_s]$ with a $\mathbb{Z}$-grading such that φ is a homomorphism of graded rings?
d) Write a CoCoA function `PresentRees(...)` which takes $f_1, \ldots, f_s$ and computes a system of generators of $\mathrm{Ker}(\varphi)$ which is homogeneous with respect to the grading defined in c).

For the remainder of this tutorial, we assume that P is standard graded, that I is a homogeneous ideal, and that $\{f_1, \ldots, f_s\}$ is a system of generators of I consisting of non-zero homogeneous polynomials. Moreover, we now equip $\overline{P}$ with the **bigrading** (i.e. with the $\mathbb{Z}^2$-grading) defined by the matrix $W = \binom{U}{V} \in \mathrm{Mat}_{2,n+1}(\mathbb{Z})$ where $U = (0 \ \ldots \ 0 \ 1)$ and $V = (1 \ \ldots \ 1 \ 0)$ are matrices in $\mathrm{Mat}_{1,n+1}(\mathbb{Z})$.

e) Prove that $\overline{P}$ is positively graded by W and that the multivariate Hilbert series of $\overline{P}$ with respect to this grading is $\mathrm{HS}_{\overline{P}}(z_1, z_2) = \frac{1}{(1-z_1)(1-z_2)^n}$.
f) Show that the Rees ring $\mathcal{R}(I)$ is a graded subring of $\overline{P}$ with respect to the grading given by W, and that its homogeneous component of bidegree $(d, e) \in \mathbb{Z}^2$ is $(I^d)_e \, t^d$.

g) Explain how one can equip $P[y_1, \ldots, y_s]$ with a $\mathbb{Z}^2$-grading such that φ is a homomorphism of bigraded rings. Then show that your function `PresentRees(...)` actually computes a bihomogeneous system of generators of $\mathrm{Ker}(\varphi)$.

h) For $i = 1, \ldots, s$, let $d_i = \deg(f_i)$. Prove that the multivariate Hilbert series of $\mathcal{R}(I)$ with respect to the grading given by W has the shape

$$\mathrm{HS}_{\mathcal{R}(I),W}(z_1, z_2) = \frac{\mathrm{HN}_{\mathcal{R}(I)}(z_1, z_2)}{(1-z_2)^n\,(1-z_1 z_2^{d_1})\cdots(1-z_1 z_2^{d_s})}$$

where $\mathrm{HN}_{\mathcal{R}(I)}(z_1, z_2) \in \mathbb{Z}[z_1, z_2]$. Write a CoCoA function `ReesHN(...)` which takes $f_1, \ldots, f_s$ and computes the multivariate Hilbert numerator $\mathrm{HN}_{\mathcal{R}(I)}(z_1, z_2)$ of the Rees ring.

i) Use your function `ReesHN(...)` to compute the multivariate Hilbert numerators of the Rees rings of the following homogeneous ideals.

1) $I_1 = (x_1^2,\, x_1x_2,\, x_1x_3,\, x_2^2,\, x_2x_3,\, x_3^2)$ in $\mathbb{Q}[x_1, x_2, x_3]$
2) $I_2 = (x_2^2 - x_1x_3,\, x_3^2 - x_2x_4,\, x_1x_4 - x_2x_3)$ in $\mathbb{Q}[x_1, x_2, x_3, x_4]$
3) The ideal I_3 in $\mathbb{Q}[x_1, \ldots, x_6]$ generated by the 3×3 minors of the matrix $\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_3 & x_4 & x_5 \\ x_3 & x_4 & x_5 & x_6 \end{pmatrix}$.

j) Now let $d \geq 1$. Construct an algorithm which computes the Hilbert series of I^d with respect to the standard grading.
Hint: In order to isolate the coefficient of z_1^d in $\mathrm{HS}_{\mathcal{R}(I),W}(z_1, z_2)$, you may replace $1/(1 - z_1 z_2^{d_j})$ by $1 + z_1 z_2^{d_j} + \cdots + z_1^d z_2^{d_j d}$ etc.

k) Based on this algorithm, write a CoCoA function `IdealPowerHN(...)` which takes $f_1, \ldots, f_s$ and d and computes the Hilbert numerator of P/I^d with respect to the standard grading.

l) Apply your function `IdealPowerHN(...)` to compute the Hilbert numerators of the following rings.

1) $\mathbb{Q}[x_1, x_2, x_3]/J_1^4$ where $J_1 = (x_1^2 - x_2x_3,\, x_2^2 - x_1x_3,\, x_3^2 - x_1x_2)$
2) $\mathbb{Q}[x_1, x_2, x_3, x_4]/J_2^3$ where $J_2 = (x_2x_4^2 - x_3^3,\, x_1x_4 - x_2x_3,\, x_1^2x_3 - x_2^3,\, x_1x_3^2 - x_2^2x_4)$
3) $\mathbb{Q}[x_1, x_2, x_3]/J_3^9$ where $J_3 = (x_1x_2,\, x_1x_3,\, x_2x_3)$

We cannot guarantee success,
but we can deserve it.
(George Washington)

Tutorial 82: Segre Products and Hadamard Series

Teacher: *"Now suppose the number of sheep is x ..."*
Student: *"Yes sir, but what happens if the number of sheep is not x ?"*
(Anonymous)

In algebraic geometry, the following construction has been studied intensively. Given a field K, the map

$$\begin{array}{rccc} \Phi: & \mathbb{P}^n_K \times \mathbb{P}^m_K & \longrightarrow & \mathbb{P}^{nm+n+m}_K \\ & ((a_0 : \ldots : a_n), (b_0 : \ldots : b_m)) & \longmapsto & (a_0b_0 : a_0b_1 : \ldots : a_nb_m) \end{array}$$

defines an embedding of projective varieties. If we restrict this map to the product of two subvarieties $V \subseteq \mathbb{P}^n_K$ and $W \subseteq \mathbb{P}^m_K$, the image $\Phi(V \times W)$ is a projective variety in $\mathbb{P}^{nm+n+m}_K$ which is called the **Segre product** of V and W. In this tutorial we examine the homogeneous coordinate rings of Segre products. We define them algebraically, compute a homogeneous presentation, and study their Hilbert series.

Suppose the Hilbert series of two standard graded K-algebras are given. Can we use this information to determine the Hilbert series of their Segre product more efficiently than blindly computing a Gröbner basis of its defining ideal? The key to answering this question affirmatively is the observation that the Hilbert series of a Segre product is the Hadamard product of the individual Hilbert series. On its own, this fact is not enough to construct an algorithm, but with a little extra effort we shall squeeze an effective procedure out of it.

But what happens if the Hilbert series of the two algebras are not given? Well, in general we have to resort to the homogenous presentation of their Segre product for finding the Hilbert series. But in one special case we can do much better: for the Hilbert series of the Segre product of two polynomial rings we shall derive a nice explicit formula in the last part of this tutorial.

Let K be a field, and let R be a bigraded (i.e. $\mathbb{Z}^2$-graded) K-algebra. Then the $\mathbb{Z}$-graded algebra $\mathrm{Diag}(R) = \bigoplus_{i\in\mathbb{Z}} R_{(i,i)}$ is called the **diagonal subalgebra** of R. Diagonal subalgebras of polynomial rings will be the topic of Exercise 5 in Section 6.1. Here we look at another particular case. Let $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$ be two sets of indeterminates. We equip the polynomial ring $R = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ with the grading given by the matrix

$$W = \begin{pmatrix} 1 & \ldots & 1 & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 1 & \ldots & 1 \end{pmatrix}$$

i.e. we let $\deg_W(x_i) = \binom{1}{0}$ and $\deg_W(y_j) = \binom{0}{1}$.

a) Show that we have $\mathrm{Diag}(R) = K[x_iy_j \mid 1 \le i \le n,\ 1 \le j \le m]$.
b) Using a), construct a natural surjective homomorphism of $\mathbb{Z}$-graded K-algebras $\varphi : K[z_{11}, \ldots, z_{nm}] \longrightarrow \mathrm{Diag}(R)$. Consequently, the diagonal subalgebra $\mathrm{Diag}(R)$ is a standard graded K-algebra.

c) Prove that the kernel of φ is the binomial ideal generated by all $z_{i_1 j_1} z_{i_2 j_2} - z_{i_3 j_3} z_{i_4 j_4}$ with $i_1 + i_2 = i_3 + i_4$ and $j_1 + j_2 = j_3 + j_4$.
Hint: The kernel of φ is homogeneous and satisfies $(\mathrm{Ker}(\varphi))_{\leq 1} = 0$. Reduce an arbitrary element of $\mathrm{Ker}(\varphi)$ suitably to the form $z_{11} f_1 + z_{1m} f_2 + z_{n1} f_3 + z_{nm} f_4$ and use induction.

Notice that the ring R can be viewed as the tensor product of the polynomial rings $P = K[x_1, \ldots, x_n]$ and $Q = K[y_1, \ldots, y_m]$ (see Tutorial 68). In the following we broaden our investigation and look at the diagonal algebra of the tensor product of two standard graded algebras.

Let $P = K[x_1, \ldots, x_n]$ and $Q = K[y_1, \ldots, y_m]$ be endowed with the standard grading, let $I \subset P$ and $J \subset Q$ be homogeneous ideals, and let $T = P/I \otimes_K Q/J$ be the tensor product of P/I and Q/J.

d) Define a $\mathbb{Z}^2$-grading on T such that there exists an isomorphism of $\mathbb{Z}^2$-graded algebras $T \cong R/(I \cdot R + J \cdot R)$.

The standard graded K-algebra $\mathrm{Diag}(P/I \otimes_K Q/J)$ is called the **Segre product** of P/I and Q/J and is denoted by $\mathrm{Seg}(P/I, Q/J)$. In particular, we have $\mathrm{Seg}(P, Q) = \mathrm{Diag}(R)$.

e) Let $d \in \mathbb{N}$ and $f \in P_d \setminus \{0\}$. Prove that we have $f \cdot \mathrm{Seg}(P, Q) = f \cdot R \cap \mathrm{Seg}(P, Q) = (f y_1^d, \ldots, f y_m^d)$.

f) Show that the homomorphism $\mathrm{Seg}(P, Q) \longrightarrow \mathrm{Seg}(P/I, Q/J)$ given by $f \otimes g \mapsto (f + I) \otimes (g + J)$ yields an isomorphism of $\mathbb{Z}$-graded K-algebras

$$\mathrm{Seg}(P, Q)/(I\,\mathrm{Seg}(P, Q) + J\,\mathrm{Seg}(P, Q)) \cong \mathrm{Seg}(P/I, Q/J)$$

g) Using e) and f), write a CoCoA function `SegIdeal(...)` which takes systems of generators of I and J and computes a system of generators of a homogeneous ideal $I_{\mathrm{Seg}} \subseteq K[z_{11}, \ldots, z_{nm}]$ such that $\mathrm{Seg}(P/I, Q/J) \cong K[z_{11}, \ldots, z_{nm}]/I_{\mathrm{Seg}}$.

h) Apply your function `SegIdeal(...)` to compute the defining ideal of the following Segre products.

1) $I_1 = (0) \subseteq \mathbb{Q}[x_1, x_2, x_3]$, $J_1 = (0) \subseteq \mathbb{Q}[y_1, y_2, y_3]$
2) $I_2 = (x_1^2, x_1 x_2, x_2^2) \subseteq \mathbb{Q}[x_1, x_2]$, $J_2 = (y_1^2, y_1 y_2, y_2^2) \subseteq \mathbb{Q}[y_1, y_2, y_3]$
3) $I_3 = (x_1 x_2, x_1 x_3) \subseteq \mathbb{Q}[x_1, x_2, x_3]$, $J_3 = (y_4^5) \subseteq \mathbb{Q}[y_1, \ldots, y_4]$

The homogeneous presentation $\mathrm{Seg}(P/I, Q/J) \cong K[z_{11}, \ldots, z_{nm}]/I_{\mathrm{Seg}}$ can be used to compute the Hilbert series of the Segre product of P/I and Q/J. However, given the Hilbert series of P/I and Q/J, it is desirable to determine the Hilbert series of the Segre product in a more direct manner. The first indication of how this could work is provided by the following formula.

i) Show that $\mathrm{Seg}(P/I, Q/J)_i \cong (P/I)_i \otimes_K (Q/J)_i$ for every $i \in \mathbb{N}$.

Let $f(z) = \sum_{i \in \mathbb{N}} a_i z^i$ and $g(z) = \sum_{j \in \mathbb{N}} b_j z^j$ be two univariate power series. Then the **Hadamard product** of f and g is the power series

$$\mathrm{Had}(f,g)(z) = \sum_{i\in\mathbb{N}} a_i b_i \, z^i$$

j) Prove the formula $\mathrm{HS}_{\mathrm{Seg}(P/I,Q/J)}(z) = \mathrm{Had}(\mathrm{HS}_{P/I}, \mathrm{HS}_{Q/J})(z)$.

This result is not yet sufficient to compute Hilbert series of Segre products because we still lack a finite description of the Hadamard product. A more detailed study is necessary.

Let $d = \dim(P/I)$ and $e = \dim(Q/J)$. Thus the Hilbert series of P/I and Q/J have the form $\mathrm{HS}_{P/I}(z) = \frac{\mathrm{hn}_{P/I}(z)}{(1-z)^d}$ and $\mathrm{HS}_{Q/J}(z) = \frac{\mathrm{hn}_{Q/J}(z)}{(1-z)^e}$, respectively, where $\mathrm{hn}_{P/I}(z), \mathrm{hn}_{Q/J}(z) \in \mathbb{Z}[z]$ are polynomials having constant coefficient one.

k) Show that the regularity index of $\mathrm{Had}(\mathrm{HS}_{P/I}, \mathrm{HS}_{Q/J})$ is less than or equal to $\max\{\mathrm{ri}(P/I), \mathrm{ri}(Q/J)\}$.

l) Using Hilbert polynomials, prove that the dimension of the Segre product is $\dim(\mathrm{Seg}(P/I, Q/J)) = \dim(P/I) + \dim(Q/J) - 1$

m) Show that the Hilbert series of the Segre product $S = \mathrm{Seg}(P/I, Q/J)$ is of the form $\mathrm{HS}_S(z) = \frac{\mathrm{hn}_S(z)}{(1-z)^{d+e-1}}$ with a polynomial $\mathrm{hn}_S(z) \in \mathbb{Z}[z]$ having $\deg(\mathrm{hn}_S(z)) \leq \max\{\mathrm{ri}(P/I), \mathrm{ri}(Q/J)\} + d + e - 2$ and $\mathrm{hn}_S(0) = 1$.

n) Given homogeneous systems of generators of I and J, consider the following sequence of instructions.

1) Using Theorem 5.4.15, compute $d = \dim(P/I)$ and $e = \dim(Q/J)$, as well as $r = \mathrm{ri}(P/I)$ and $s = \mathrm{ri}(Q/J)$.
2) Let $\ell = \max\{r, s\} + d + e - 2$. For $i = 0, \ldots, \ell$, compute the number $h_i = \mathrm{HF}_{P/I}(i) \cdot \mathrm{HF}_{Q/J}(i)$.
3) Let $H : \mathbb{Z} \longrightarrow \mathbb{Z}$ be defined by $H(i) = h_i$ for $0 \leq i \leq \ell$ and $H(i) = 0$ otherwise. Compute $c_j = \Delta^{d+e-1} H(j)$ for $j = 0, \ldots, \ell$. Return the polynomial $c_0 + c_1 z + \cdots + c_\ell z^\ell \in \mathbb{Z}$ and the number $d + e - 1$.

Prove that this is an algorithm which computes the simplified Hilbert numerator $\mathrm{hn}_S(z)$ and the dimension $\dim(S)$ of $S = \mathrm{Seg}(P/I, Q/J)$.

o) Write a CoCoA function `SegreHS(...)` which implements the algorithm of n). Apply this function to the examples in h).

In the last part of this tutorial we return to the case $I = J = (0)$, i.e. to the Segre product $\mathrm{Seg}(P, Q) = \mathrm{Diag}(R)$. Our goal is to find an explicit formula for the Hilbert series of this ring. Given a power series $f(z) = \sum_{i\in\mathbb{N}} a_i \, z^i \in \mathbb{Z}[[z]]$, we let $\Delta f(z) = a_0 + \sum_{i\geq 1}(a_i - a_{i-1}) \, z^i$.

p) Show that $\Delta\big(\mathrm{Had}(\mathrm{HS}_{P/I}, \mathrm{HS}_{Q/J})\big)(z) = \mathrm{Had}\big(\Delta(\mathrm{HS}_{P/I}), \mathrm{HS}_{Q/J}\big)(z) + \mathrm{Had}\big(\mathrm{HS}_{P/I}, \Delta(\mathrm{HS}_{Q/J})\big)(z) - \mathrm{Had}\big(\Delta(\mathrm{HS}_{P/I}), \Delta(\mathrm{HS}_{Q/J})\big)(z)$.
Hint: $a_i b_i - a_{i-1} b_{i-1} = (a_i - a_{i-1}) b_i + a_i (b_i - b_{i-1}) - (a_i - a_{i-1})(b_i - b_{i-1})$

q) Prove that $\binom{n}{i}\binom{m}{i} = \binom{n-1}{i}\binom{m}{i} + \binom{n}{i}\binom{m-1}{i} - \binom{n-1}{i}\binom{m-1}{i} + \binom{n-1}{i-1}\binom{m-1}{i-1}$ for $i \in \mathbb{N}$ and $m, n \in \mathbb{N}_+$.

r) Finally, prove the formula

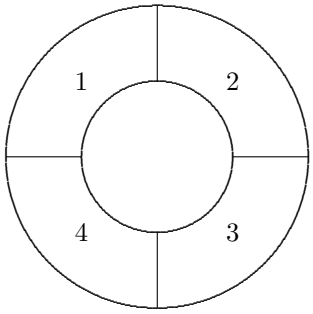
$$\mathrm{HS}_{\mathrm{Seg}(P,Q)}(z) = \frac{\sum_{j=0}^{\min\{n-1,m-1\}} \binom{n-1}{j}\binom{m-1}{j} z^j}{(1-z)^{n+m-1}}$$

Hint: Show $\Delta(\mathrm{HS}_{\mathrm{Seg}(P,Q)}) = \sum_{j=0}^{\min\{n-1,m-1\}} \binom{n-1}{j}\binom{m-1}{j} z^j/(1-z)^{n+m-2}$ using a double induction and the formulas proved in the preceding two items.

Tutorial 83: A Toy Example

Children today are tyrants.
They contradict their parents,
gobble their food,
and tyrannize their teachers.
(Socrates)

A popular children's toy consists of coloured 90 degree arcs which can be joined together to form *toy rings* and other shapes. Let us denote the available colours by $\{1, \ldots, n\}$.



If we have four colours available, we can create 55 toy rings which are pairwise different in the sense that no two of them can be transformed into each other by a movement in 3-dimensional space.

1) There are four unicoloured toy rings.
2) There are twelve toy rings having colour distribution $(3,1)$, i.e. consisting of three arcs of one colour and one arc of another colour.
3) There are six toy rings having colour distribution $(2,2)$ and adjacent arcs of the same colour.
4) There are six toy rings having colour distribution $(2,2)$ and opposite arcs of the same colour.
5) There are twelve toy rings having colour distribution $(2,1,1)$ and adjacent arcs of the same colour.
6) There are twelve toy rings having colour distribution $(2,1,1)$ and opposite arcs of the same colour.

7) There are three toy rings having colour distribution $(1,1,1,1)$. (Look at the colour opposite the segment of colour "1"!)

Let us increase the number of available colours.

a) Show that 120 different toy rings can be built using five colours, and for six colours there are 231 different toy rings.

This result motivates us to investigate the following philosophical question:

What is the deeper meaning of the number 231?

More seriously, we want to study the general problem of how one can count objects for which certain symmetries have to be taken into account. Of course, we could extend the above case-by-case argument to n available colours, but we are more interested in a general strategy. The deeper meaning of the number 231 should be that it is a value of a suitable multigraded Hilbert function.

Let us begin by classifying the symmetries of toy rings. We represent a toy ring by a quadruple (c_1, c_2, c_3, c_4) where $c_i \in \{1, \ldots, n\}$.

b) Show that the symmetry group G of toy rings is a subgroup of the permutation group S_4 which is isomorphic to the dihedral group D_4 of order eight. (For a definition of D_4, see Tutorial 40.) Write down these eight permutations.

Next we want to identify toy rings with terms in a suitable polynomial ring. We represent the possible values $1, \ldots, n$ of the colour c_i by the terms $x_i^{n-1}, x_i^{n-1}y_i, \ldots, y_i^{n-1}$ where the indeterminates x_i and y_i have degree one. In this way the n possible values of c_i are in 1–1 correspondence with the n terms of degree $n-1$ in $\mathbb{Q}[x_i, y_i]$. Then a toy ring $T = (c_1, c_2, c_3, c_4)$ is represented by the term

$$t_T = x_1^{n-c_1} y_1^{c_1-1} x_2^{n-c_2} y_2^{c_2-1} x_3^{n-c_3} y_3^{c_3-1} x_4^{n-c_4} y_4^{c_4-1} \in P = \mathbb{Q}[x_1, y_1, \ldots, x_4, y_4]$$

c) Equip the ring P with a $\mathbb{Z}^4$-grading such that toy rings correspond to terms of degree $(n{-}1,\ n{-}1,\ n{-}1,\ n{-}1)$. Then determine $\mathrm{HF}_P(i,i,i,i)$ for $i = 3, 4, 5$.

d) Prove that the number of terms of the form t_T is the $(n{-}1)^{\mathrm{st}}$ value of the Hilbert function of the **fourfold Segre product** $S = \bigoplus_{i \geq 0} P_{(i,i,i,i)} \subseteq P$.

e) Define 16 further indeterminates $Z = \{z_{ijk\ell} \mid i,j,k,\ell \in \{0,1\}\}$ and equip $R = \mathbb{Q}[Z]$ with the standard grading. Then show that the map $\varphi : R \longrightarrow S$ defined by $z_{ijk\ell} \mapsto x_1^i y_1^{1-i} \cdots x_4^\ell y_4^{1-\ell}$ is a surjective homomorphism of $\mathbb{Q}$-algebras.

f) Prove that the ideal $I = \mathrm{Ker}(\varphi)$ is generated by the set of all binomials $z_{i_1 j_1 k_1 \ell_1} z_{i_2 j_2 k_2 \ell_2} - z_{i_3 j_3 k_3 \ell_3} z_{i_4 j_4 k_4 \ell_4}$ for which $i_1 + i_2 = i_3 + i_4, \ldots, \ell_1 + \ell_2 = \ell_3 + \ell_4$.

g) Show that the Hilbert function of S satisfies $\mathrm{HF}_S(i) = (i{+}1)^4$ for $i \in \mathbb{N}$.

It remains to identify different terms in S which represent the same toy ring. The group G acts on S via the map

$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (\sigma, x_1^{\alpha_1} y_1^{\beta_1} \cdots x_4^{\alpha_4} y_4^{\beta_4}) & \longmapsto & x_{\sigma(1)}^{\alpha_1} y_{\sigma(1)}^{\beta_1} \cdots x_{\sigma(4)}^{\alpha_4} y_{\sigma(4)}^{\beta_4} \end{array}$$

Below we want to show that the function we are looking for is the Hilbert function of the **invariant ring** $S^G = \{f \in S \mid f^\sigma = f \text{ for all } \sigma \in G\}$, and that this Hilbert function can be computed using the presentation $S \cong R/I$.

h) Let $n \geq 1$. Prove that the action of G on S induces an action on the set of terms of degree n in S, and that the number of orbits of that operation equals $\dim_{\mathbb{Q}}(S^G)_n$. Explain why this implies that the number of toy rings for n available colours is given by $\mathrm{HF}_{S^G}(n)$.

i) Let the group G act on R via $(z_{i_1 i_2 i_3 i_4})^\sigma = z_{i_{\sigma(1)} i_{\sigma(2)} i_{\sigma(3)} i_{\sigma(4)}}$ for $\sigma \in G$. Prove that for every $n \geq 1$, the vector space I_n is invariant under this action and that we have $(S^G)_n \cong (R^G)_n/(I_n \cap R^G)$.

j) Find the orbits of the action of G on the set of indeterminates in R. Deduce that there are six toy rings for two available colours.

In principle, we could try to use Tutorial 40 to compute a set of algebra generators of R^G. However, in this particular case, the algorithm given there is too inefficient. In Tutorial 98 we will discuss a more powerful approach. For the time being, let us assume that we have somehow found a set of homogeneous polynomials $f_1, \ldots, f_m \in R$ such that $R^G = \mathbb{Q}[f_1, \ldots, f_m]$. We form the polynomial ring $Q = \mathbb{Q}[y_1, \ldots, y_m]$ and equip it with the $\mathbb{Z}$-grading given by $\deg(y_i) = \deg(f_i)$ for $i = 1, \ldots, m$.

k) How can one find a homogeneous ideal $J \subseteq Q$ such that there exists an isomorphism of graded $\mathbb{Q}$-algebras $Q/J \cong S^G$? Given $f_1, \ldots, f_m$, explain how one can compute J, and hence HF_{S^G}.

l) Using the method described at the beginning of this tutorial, show that we have $\mathrm{HF}_{S^G}(i) = \frac{1}{8}\, i^4 + \frac{3}{4}\, i^3 + \frac{15}{8}\, i^2 + \frac{9}{4}\, i + 1$ for every $i \in \mathbb{N}$.

So, what is the deeper meaning of the number 231? Although the true answer to this question may never be known, our toy example suggests that we should consider 231 as the value of the formula

$$\tfrac{1}{8}\, 5^4 + \tfrac{3}{4}\, 5^3 + \tfrac{15}{8}\, 5^2 + \tfrac{9}{4}\, 5 + 1$$

One Ring to rule them all,
One Ring to find them,
One Ring to bring them all
and in the darkness bind them.
(J.R.R. Tolkien)

6. Further Applications

The simplest form of mathematics is music.
(Socrates)

Here we are at the finale. Like the last movement of a symphony, the pace of our exposition increases and many themes and variations follow each other in rapid succession. Consequently, Italian imagination slightly prevails over German rigour. The sections do not always follow the well trodden path, a few exercises are like small research projects, and some tutorials take on the character of sections. Hand in hand with this more liberal style of presentation goes a steady crescendo of quotes and jokes which play the incidental music for the final fireworks.

To find out what exactly is going on here, we rejoin the three friends we met in the introduction of the previous chapter. Their stroll through the Italian *parco* has led them to a beautiful villa.

G: Look how nicely the park blends with this villa. What a magical view!
A: Speaking of magic, did you see the magic square in the book we were talking about? It is called the Jupiter magic square and is contained in an engraving by Albrecht Dürer dating all they way back to 1514. It has so many symmetries and special properties that the medieval alchemists attributed to it healing powers.
C: And what is its connection to Computational Commutative Algebra?
A: That's quite clear to me: such squares can be counted using multigraded Hilbert functions. But why is this in the sixth chapter?
C: Aren't there zillions of magic squares? Can the value of this Hilbert function really be computed?
A: Aha, now I see. The authors use toric ideals and Hilbert bases to compute the number of magic squares. These are pretty sophisticated theories where algebra blends with combinatorics.
G: Are there also some elementary applications?
A: Yes, for instance you can use Hilbert bases to find the solutions of the equation $3x - 5y + 4z = 0$ which consist of triples of natural numbers.
C: Listen! I hear someone playing a familiar tune over there.
G: Indeed! There is going to be a concert in this park and the orchestra has started practising.

A: Speaking of which, in Section 6.2 the authors also play an old tune: they use homogenizations and degree forms for liftings of ideals.
C: Liftings? Are they heavy?
A: Well, they are usually rather difficult to lift properly. At least for monomial ideals good liftings can be constructed using distractions.
G: So, besides gin there are also other distractions in mathematics. I wonder why people tend to believe that mathematics is a dull subject.
A: Why don't we stop here and listen to the rehearsal? The tunes they are playing remind me of the good old days when there were no computers in mathematics and nobody asked for non-trivial examples or actual applications.
C: What about these finite sets of points in Section 6.3? Are there non-trivial examples and actual applications? Probably these Gröbner basis techniques become wholly impractical as soon as you apply them to a large point set coming from a real application.
A: Fortunately there is the Buchberger-Möller algorithm which reduces the task of finding the vanishing ideal of a finite set of points to a manageable linear algebra problem. With it you can deal with point sets such as those coming from statistics.
G: Personally, I don't trust any statistics I didn't massage myself. Anyway, when you do actual examples on a computer, don't you get a lot of rounding errors? Do you trust these computations?
A: Indeed, this seems to be a problem with Gröbner bases: they are ill-behaved when you apply them to approximate inputs. This problem of numerical instability is tackled in Section 6.4 where the authors use border bases instead of Gröbner bases.
C: Does that mean that everything you told us about Gröbner bases and their computation was useless? Or is there no way to compute border bases?
A: No, no! Although border bases can be computed and have many characterizations mimicking the characterizations of Gröbner bases in the first volume of this book, they seem to work best for zero-dimensional ideals.
G: The pace of this rehearsal is really picking up. The orchestra has just finished an Argentinian tango, and now they are playing Brazilian samba and bossa nova at the same time. From this mixture it is not easy to filter out the leitmotif of their performance.
A: Did you know that one can also filter polynomial rings and modules?
C: What do you mean?
A: Well, the authors show in Section 6.5 that filtrations on polynomial rings allow them to generalize both the theory of Gröbner bases and Macaulay bases. Moreover, using adic filtrations, they present many classical commutative algebra results, and they define and compute tangent cones.
G: Tangent cones at singular points of varieties? Are we back to geometry?
A: Exactly.

G: Can I use Computational Commutative Algebra to study singularities in detail?
A: Yes, you can, and Tutorial 95 is a good place to start.
C: Didn't you say that Gröbner basis theory applies to polynomial ideals and modules? Don't you need to do computations in local rings for studying singularities?
A: That is correct. You need Mora's Algorithm. Hence you will also have to do Tutorial 93.
C: Wow! That sounds like a lot of work. Is there also something in this book that I can just enjoy without having to work it out myself?
A: Of course, there's plenty. There are stories about the good old days, Brazilian dreams, and of course SAGBI bases.
G: What? SAGBI? Strongly Advertising Gröbner Based Ideas?
A: Almost. It means Subalgebra Analog to Gröbner Bases for Ideals. It was invented for the purpose of handling subalgebras of polynomial rings computationally, just as Gröbner bases do with ideals. But, being a gardener, you know that not every sweet root gives birth to sweet grass. Sometimes SAGBI bases are not finite.
C: Therefore there cannot exist an algorithm to compute them. So, why did you claim that SAGBI bases are useful for computations?
A: Because there is an enumerative procedure to compute them. If the SAGBI basis is finite, the procedure finds it after finitely many steps. However, the procedure is not easy: for instance, you need toric ideals as a computational tools. But once you have a finite SAGBI basis of a subalgebra, it is like possessing the key to its hidden secrets.
G: You guys are getting carried away. You don't even notice the music anymore. And what about the beautiful geometry of this garden?

With much fanfare the orchestra begins playing the coda of the piece they are rehearsing.

A: You are right. This flourish of trumpets is the proper introduction to the last section of this book. The authors allegedly teach you how to prove geometric theorems automatically.
C: Automatically? Do you mean using a computer? You must be joking. You mathematicians would be out of a job!
A: Yes and no. Theorems in Euclidean geometry can be translated to statements about polynomials belonging to ideals. And you already know how to decide ideal membership. But theorem proving turns out to be semi-automatic at best: you need to find a good polynomial model of your theorem, must be careful not to overlook degenerate cases, and have to reinterpret the computer results geometrically.
G: This situation resembles modern gardening where machines help humans a lot, but they do not replace him. But to call this artificial intelligence really stretches my imagination.

A: Indeed, Section 6.7 poses more philosophical questions than it answers. But there are many wonderful examples, and you are invited to implement and try out your own Automatic Prover.
G: This path has led us nicely across the entire park. It is the thread of Ariadne through this labyrinth of trees, bushes and flower beds.
A: Just as the idea of generalizing Gröbner bases guided us through this final chapter.
C: Are you saying that this ends the project the authors had in mind when they started it many years ago?

The three friends have rejoined the path along the seashore. The orchestra has stopped practising, the sounds of the park are dying away, the wind subsides, and the rays of the setting sun create a pale reflection on the smooth sea. No more jokes, no more metaphors, and they return along the path to the little harbour of the village.

The gardening season
officially begins on January 1st,
and ends on December 31.
(Marie Huston)

6.1 Toric Ideals and Hilbert Bases

In order to make an apple pie from scratch,
you must first create the universe.
(Carl Sagan)

In the beginning the Universe was created.
This made a lot of people angry
and was widely regarded as a bad move.
(Douglas Adams)

To start this chapter in the appropriate way, we go back to one of the roots of mathematics. In linear algebra students learn how to solve linear equations with integer coefficients over the field of rational numbers. Solving them over the integers is still not that difficult, but suppose we are interested in the solutions consisting of tuples of natural numbers. For example, how can we describe the set of non-negative integer solutions of the equation $3z_1 - 5z_2 + 4z_3 = 0$?

One way to answer this question is to create, from scratch, a whole new universe: toric ideals and Hilbert bases. We encountered toric ideals briefly in Tutorials 36 and 38, but Hilbert bases are a new instance of the phenomenon of "Hilbert inflation" discussed in the introduction of Section 5.4. Fortunately, they increase the Hilbert inflation rate only by a negligible amount.

How does one go about creating a universe? In spite of the danger of making a lot of people angry, we begin the first subsection with the introduction of some terminology. Given a matrix of integers $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, the toric ideal $I(\mathcal{A})$ is defined to be the kernel of the K-algebra homomorphism $\varphi : P \longrightarrow L$ given by $x_i \mapsto y_1^{a_{1i}} \cdots y_m^{a_{mi}}$ where $P = K[x_1, \ldots, x_n]$ is a polynomial ring over a field K and $L = K[y_1, \ldots, y_m, y_1^{-1}, \ldots, y_m^{-1}]$ is a Laurent polynomial ring. This toric ideal contains a wealth of information about the set of integer solutions $\mathcal{L}(\mathcal{A}) \subseteq \mathbb{Z}^n$ of the system of Diophantine equations $\mathcal{A} \cdot (z_1, \ldots, z_n)^{\mathrm{tr}} = 0$. A case in point is Proposition 6.1.4 where we show that the elements of $\mathcal{L}(\mathcal{A})$ are in 1–1 correspondence with the *pure* binomials in $I(\mathcal{A})$, i.e. with the polynomials of the form $t - t'$ where $t, t' \in \mathbb{T}^n$ are coprime terms.

Hence it becomes imperative to find good ways of computing the toric ideal associated to an integer matrix. Here we can rework and expand the ideas in Tutorial 38. In particular, we shall show that a system of generators of $\mathcal{L}(\mathcal{A})$ gives rise to a lattice ideal from which we can compute $I(\mathcal{A})$ via saturation (see Theorem 6.1.9). But doesn't all this theory lead us away from our true goal? Didn't we claim that finding $\mathcal{L}(\mathcal{A})$ is not so difficult and that we are really interested in the monoid $\mathcal{L}_+(\mathcal{A}) = \mathcal{L}(\mathcal{A}) \cap \mathbb{N}^n$? And what kind of description of $\mathcal{L}_+(\mathcal{A})$ are we looking for?

Those are the questions. To answer them requires even more creations (i.e. definitions) which we will do in the second subsection. If we partially order the monoid $\mathcal{L}_+(\mathcal{A})$ partially by setting $(v_1, \ldots, v_n) \succ (w_1, \ldots, w_n)$ if $v_i \geq w_i$ for $i = 1, \ldots, n$, the set of minimal elements with respect to $\succ$ is called the

Hilbert basis of $\mathcal{L}_+(\mathcal{A})$. The main results are that the Hilbert basis of $\mathcal{L}_+(\mathcal{A})$ is finite, generates $\mathcal{L}_+(\mathcal{A})$ as a monoid, and can be computed using Gröbner bases (see Proposition 6.1.12 and Theorem 6.1.17). This computation uses a most versatile tool: the Lawrence lifting of a matrix. Unlike Lawrence of Arabia, who spent most of his time in wild desert lands, our Lawrence liftings are fountains of lush applications and operate in an orderly world of matrices where columns and rows keep their assigned positions.

To celebrate the beauty and power of Hilbert bases, we end the section with a number of examples introduced by a homemade couplet. Not only do we present the full solution of the equation $3z_1 - 5z_2 + 4z_3 = 0$, but we also treat inhomogeneous Diophantine equations and systems of Diophantine equations. After that, if you thirst for even more, there are exercises containing applications to straight line subalgebras (see Exercise 5), margins of integer matrices (see Exercise 6), and integer programming (see Exercise 7). Finally, for the truly insatiable, we have tutorials on the magic of magic squares (see Tutorial 84), dangerous gaps in monoids (see Tutorial 85), and the search for the positive type of a matrix (see Tutorial 86).

Although it may be widely regarded as a bad move, we now stop joking and begin collecting the ingredients for our apple pie.

6.1.A Toric Ideals

The pure and simple truth
is rarely pure and never simple.
(Oscar Wilde)

Let K be a field and $P = K[x_1, \ldots, x_n]$ a polynomial ring over K. Given further indeterminates $y_1, \ldots, y_m$, we let $L = K[y_1, \ldots, y_m, y_1^{-1}, \ldots, y_m^{-1}]$ be the Laurent polynomial ring in the indeterminates $y_1, \ldots, y_m$ over K. An element of the form $y_1^{i_1} y_2^{i_2} \cdots y_m^{i_m} \in L$ with $i_1, \ldots, i_m \in \mathbb{Z}$ is called an **extended term**. The monoid of all extended terms is denoted by $\mathbb{E}^m$ (see Tutorial 36).

Definition 6.1.1. Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let $t_i = y_1^{a_{1i}} y_2^{a_{2i}} \cdots y_m^{a_{mi}}$ for $i = 1, \ldots, n$. We define a K-algebra homomorphism $\varphi : P \longrightarrow L$ by $\varphi(x_i) = t_i$ for $i = 1, \ldots, n$. Then the ideal $I(\mathcal{A}) = \mathrm{Ker}(\varphi)$ in P is called the **toric ideal** associated to the matrix $\mathcal{A}$, or to the tuple of terms $(t_1, \ldots, t_n)$.

Below we shall show that this definition agrees with the definition in Tutorial 38 if $\mathcal{A} \in \mathrm{Mat}_{m,n}(\mathbb{N})$. Notice that every toric ideal is a prime ideal because it is the kernel of a homomorphism to an integral domain. The next proposition implies that toric ideals are special kinds of binomial ideals. Recall that a **binomial** in P is a polynomial of the form $at + a't'$ with coefficients $a, a' \in K \setminus \{0\}$ and distinct terms $t, t' \in \mathbb{T}^n$. A **binomial ideal** is an ideal generated by binomials. The following types of binomials will turn out to be useful.

Definition 6.1.2. Let $S \subseteq P$ be a set of polynomials.

a) A binomial in P is called **unitary** if it is of the form $t - t'$ with $t, t' \in \mathbb{T}^n$. The set of all unitary binomials in S will be denoted by $\mathrm{UB}(S)$.
b) A binomial in P is called **pure** if it is of the form $t - t'$ with coprime terms $t, t' \in \mathbb{T}^n$. The set of all pure binomials in S will be denoted by $\mathrm{PB}(S)$.

For an extended term $t \in \mathbb{E}^m$, there exists a unique minimal number $\tau(t) \in \mathbb{N}$ such that $t \cdot (y_1 \cdots y_m)^{\tau(t)} \in K[y_1, \ldots, y_m]$. Now we are ready to explain one way of computing toric ideals. We warn you right away that this is not a very efficient method.

Proposition 6.1.3. (Basic Properties of Toric Ideals)
Let $t_1, \ldots, t_n \in \mathbb{E}^m$, let $I \subseteq P$ be the toric ideal associated to $(t_1, \ldots, t_n)$, and let $J \subseteq K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ be the binomial ideal generated by $\{\pi^{\tau(t_1)}(x_1 - t_1), \ldots, \pi^{\tau(t_n)}(x_n - t_n)\}$ where $\pi = y_1 \cdots y_m$.

a) We have $I = (J : \pi^\infty) \cap K[x_1, \ldots, x_n]$.
b) Let z be a new indeterminate, and let G be a Gröbner basis of the ideal $J + (\pi z - 1)$ with respect to an elimination ordering for $\{y_1, \ldots, y_m, z\}$. Then the toric ideal I is generated by $G \cap K[x_1, \ldots, x_n]$.
c) The toric ideal I is generated by pure binomials.

Proof. To prove a), we note that $L = K[y_1, \ldots, y_m, y_1^{-1}, \ldots, y_m^{-1}]$ is isomorphic to the localization $K[y_1, \ldots, y_m]_\pi$. Given a further indeterminate z, Proposition 3.5.6 tells us that L is isomorphic to $K[y_1, \ldots, y_m, z]/(\pi z - 1)$. Then we look at the diagram of K-algebra homomorphisms

$$\begin{array}{ccc} P = K[x_1, \ldots, x_n] & \xrightarrow{\varphi} & K[y_1, \ldots, y_m]_\pi \\ \downarrow \alpha & & \uparrow \psi \\ K[x_1, \ldots, x_n, y_1, \ldots, y_m] & \xrightarrow{\beta} & K[x_1, \ldots, x_n, y_1, \ldots, y_m]_\pi \end{array}$$

where φ is the map defined in 6.1.1, where α and β are the canonical injective homomorphisms, and where the homomorphism of K-algebras ψ is defined by $\psi(y_i) = y_i$ for $i = 1, \ldots, m$ and $\psi(x_i) = t_i$ for $i = 1, \ldots, n$. Since this diagram is commutative, we have $I = \mathrm{Ker}(\varphi) = \alpha^{-1}(\beta^{-1}(\mathrm{Ker}(\psi)))$. Hence it suffices to prove that $J : \pi^\infty = \beta^{-1}(\mathrm{Ker}(\psi))$.

Let $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]_\pi$. The ideal JQ coincides with the ideal generated by $\{x_1 - t_1, x_2 - t_2, \ldots, x_n - t_n\}$. Notice that Q is isomorphic to $R[x_1, \ldots, x_n]$ for $R = K[y_1, \ldots, y_m]_\pi$. Therefore Proposition 3.6.1.a yields $JQ = \mathrm{Ker}\,(\psi)$. Hence we have $\beta^{-1}(\mathrm{Ker}(\psi)) = \beta^{-1}(JQ) = J : \pi^\infty$ by Proposition 3.5.11.b.

To prove b), we consider the sequence of K-algebra homomorphisms

$$P \xrightarrow{\alpha} K[x_1, \ldots, x_n, y_1, \ldots, y_m] \xrightarrow{\gamma} K[x_1, \ldots, x_n, y_1, \ldots, y_m, z]$$

where α and γ are the canonical injective homomorphisms. Let $\widetilde{J}$ be the ideal generated by J and by $\pi z - 1$ in the ring $K[x_1, \ldots, x_n, y_1, \ldots, y_m, z]$. Using Theorem 3.5.13.a, we see that $\gamma^{-1}(\widetilde{J}) = J : \pi^\infty$. We may identify P with its image $\gamma(\alpha(P))$ and use a) to conclude that $I = \alpha^{-1}(J : \pi^\infty) = \alpha^{-1}(\gamma^{-1}(\widetilde{J})) = \widetilde{J} \cap P$. Now the claim follows from Theorem 3.4.5.

To prove c), we observe that $\widetilde{J}$ is generated by unitary binomials. Hence G consists of unitary binomials. The fact that those binomials satisfy $\gcd(t_1, t_2) = 1$ follows from the observation that I is a prime ideal. □

The algorithm for computing toric ideals implied by part b) of this proposition does not depend on the base field K. Therefore, in practise, a computationally inexpensive field such as $\mathbb{Z}/(2)$ can be used. However, as we said before, the actual computation of toric ideals can benefit from many other optimizations (see for instance Tutorial 38). Next we explain the main ideas behind more efficient implementations of this computation.

For this purpose we use a number of further abbreviations. Given an integer $a \in \mathbb{Z}$, we let $a^+ = \max\{a, 0\}$ and $a^- = \max\{-a, 0\}$. Thus we have $a = a^+ - a^-$. For a tuple of integers $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$, we let $a^+ = (a_1^+, \ldots, a_n^+)$ and $a^- = (a_1^-, \ldots, a_n^-)$. Hence we get $a = a^+ - a^-$ again. Moreover, we shall use the convention that $\mathbf{x}^a$ denotes the extended term $x_1^{a_1} \cdots x_n^{a_n}$. Finally, in analogy to Tutorial 38, the kernel of the $\mathbb{Z}$-linear map $\mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ defined by $\mathcal{A}$ will be denoted by $\mathcal{L}(\mathcal{A})$.

Proposition 6.1.4. *Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ be given.*

a) For the map $\varrho' : \mathbb{Z}^n \longrightarrow P$ defined by $\varrho'(u) = \mathbf{x}^{u^+} - \mathbf{x}^{u^-}$, we have $\varrho'(\mathcal{L}(\mathcal{A})) \subseteq \mathrm{PB}(I(\mathcal{A}))$. In particular, the restriction of the map ϱ' yields a map $\varrho : \mathcal{L}(\mathcal{A}) \longrightarrow \mathrm{PB}(I(\mathcal{A}))$.

b) For the map $\vartheta' : \mathrm{UB}(P) \longrightarrow \mathbb{Z}^n$ defined by $\vartheta'(\mathbf{x}^\alpha - \mathbf{x}^\beta) = \alpha - \beta$, we have $\vartheta'(\mathrm{PB}(I(\mathcal{A}))) \subseteq \mathcal{L}(\mathcal{A})$. In particular, the restriction of the map ϑ' yields a map $\vartheta : \mathrm{PB}(I(\mathcal{A})) \longrightarrow \mathcal{L}(\mathcal{A})$.

c) The maps ϱ and ϑ are inverse to each other.

d) The toric ideal $I(\mathcal{A})$ is generated by $\{\varrho(v) \mid v \in \mathcal{L}(\mathcal{A})\}$.

Proof. First we prove a). For $u = (u_1, \ldots, u_n) \in \mathcal{L}(\mathcal{A})$, we have

$$\begin{cases} a_{11}u_1^+ + a_{12}u_2^+ + \cdots + a_{1n}u_n^+ &= a_{11}u_1^- + a_{12}u_2^- + \cdots + a_{1n}u_n^- \\ a_{21}u_1^+ + a_{22}u_2^+ + \cdots + a_{2n}u_n^+ &= a_{21}u_1^- + a_{22}u_2^- + \cdots + a_{2n}u_n^- \\ \vdots & \vdots \\ a_{m1}u_1^+ + a_{m2}u_2^+ + \cdots + a_{mn}u_n^+ &= a_{m1}u_1^- + a_{m2}u_2^- + \cdots + a_{mn}u_n^- \end{cases}$$

Using the terms $t_i = y_1^{a_{1i}} \cdots y_m^{a_{mi}}$ for $i = 1, \ldots, n$, we obtain $t_1^{u_1^+} \cdots t_n^{u_n^+} = t_1^{u_1^-} \cdots t_n^{u_n^-}$. Hence we see that $x_1^{u_1^+} \cdots x_n^{u_n^+} - x_1^{u_1^-} \cdots x_n^{u_n^-} \in I(\mathcal{A})$. This binomial is clearly pure.

To show b), we observe that $x_1^{\alpha_1}\cdots x_n^{\alpha_n} - x_1^{\beta_1}\cdots x_n^{\beta_n} \in \mathrm{PB}(I(\mathcal{A}))$ implies $t_1^{\alpha_1}\cdots t_n^{\alpha_n} = t_1^{\beta_1}\cdots t_n^{\beta_n}$ for the extended terms $t_1,\ldots,t_n$ defined above. Therefore we see that

$$\left\{\begin{array}{ccc} a_{11}\alpha_1 + a_{12}\alpha_2 + \cdots + a_{1n}\alpha_n & = & a_{11}\beta_1 + a_{12}\beta_2 + \cdots + a_{1n}\beta_n \\ a_{21}\alpha_1 + a_{22}\alpha_2 + \cdots + a_{2n}\alpha_n & = & a_{21}\beta_1 + a_{22}\beta_2 + \cdots + a_{2n}\beta_n \\ \vdots & \vdots & \vdots \\ a_{m1}\alpha_1 + a_{m2}\alpha_2 + \cdots + a_{mn}\alpha_n & = & a_{m1}\beta_1 + a_{m2}\beta_2 + \cdots + a_{mn}\beta_n \end{array}\right.$$

Thus we conclude that $(\alpha_1-\beta_1,\ldots,\alpha_n-\beta_n) \in \mathcal{L}(\mathcal{A})$.

Next we prove c). By definition, we have $\vartheta \circ \varrho = \mathrm{id}_{\mathcal{L}(\mathcal{A})}$. On the other hand, let $b = x_1^{\alpha_1}\cdots x_n^{\alpha_n} - x_1^{\beta_1}\cdots x_n^{\beta_n} \in \mathrm{PB}(I(\mathcal{A}))$. Then we have $\vartheta(b) = (\alpha_1-\beta_1,\ldots,\alpha_n-\beta_n)$, and the fact that b is a pure binomial implies $((\alpha_1-\beta_1)^+,\ldots,(\alpha_n-\beta_n)^+) - ((\alpha_1-\beta_1)^-,\ldots,(\alpha_n-\beta_n)^-) = (\alpha_1,\ldots,\alpha_n) - (\beta_1,\ldots,\beta_n)$. Consequently, we get $\varrho\circ\vartheta = \mathrm{id}_{\mathrm{PB}(I(\mathcal{A}))}$.

Finally we note that d) follows from c) and Proposition 6.1.3.c. □

This proposition provides us with a first idea for creating a good algorithm for computing $I(\mathcal{A})$ from scratch. Since there are well-known efficient algorithms for computing a set of generators of $\mathcal{L}(\mathcal{A})$, we know many elements of $I(\mathcal{A})$. How big a part of $I(\mathcal{A})$ can we obtain from a system of generators of $\mathcal{L}(\mathcal{A})$? To study this question more closely, we introduce a name for such ideals.

Definition 6.1.5. Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $\mathcal{L}(\mathcal{A})$ be the kernel of the $\mathbb{Z}$-linear map $\mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ defined by $\mathcal{A}$, and let $V = \{v_1,\ldots,v_r\}$ be a set of vectors in $\mathcal{L}(\mathcal{A})$. Then the ideal $I_V = (\varrho(v_1),\ldots,\varrho(v_r)) \subseteq P$ is called the **lattice ideal** associated to V.

By definition, the lattice ideal I_V is contained in the toric ideal $I(\mathcal{A})$ of $\mathcal{A}$. The following example shows that this may be a proper inclusion even when V generates the $\mathbb{Z}$-module $\mathcal{L}(\mathcal{A})$ and that adding a "superfluous" generator to V may enlarge I_V properly.

Example 6.1.6. The toric ideal associated to the matrix $\mathcal{A} = \left(\begin{smallmatrix} 4&0&0&1&1 \\ 1&0&4&0&2 \\ 0&5&1&4&2 \end{smallmatrix}\right)$ is

$$\begin{array}{rcl} I(\mathcal{A}) & = & (x_3x_4^2 - x_2x_5^2,\ x_1^2x_2^6 - x_4^7x_5,\ x_1^2x_2^3x_3^3 - x_4x_5^7, \\ & & x_1^2x_2^2x_3^4x_4 - x_5^9,\ x_1^2x_2^4x_3^2 - x_4^3x_5^5,\ x_1^2x_2^5x_3 - x_4^5x_5^3) \end{array}$$

and this is a minimal system of generators. It is easy to check that the set $V = \{(2,6,0,-7,-1),\ (0,1,-1,-2,2)\}$ is a $\mathbb{Z}$-basis of $\mathcal{L}(\mathcal{A})$. Obviously, the ideal I_V is properly contained in $I(\mathcal{A})$.

Now consider the set $V' = V \cup \{(2,3,3,-1,-7)\}$ where $(2,3,3,-1,-7) = (2,6,0,-7,-1) - 3(0,1,-1,-2,2)$. This ideal $I_{V'} = (x_1^2x_2^6 - x_4^7x_5,\ x_2x_5^2 - x_3x_4^2,\ x_1^2x_2^3x_3^3 - x_4x_5^7)$ properly contains $I_V = (x_1^2x_2^6 - x_4^7x_5,\ x_2x_5^2 - x_3x_4^2)$.

The following proposition provides a partial converse to this example: if the addition of a vector to V does not enlarge I_V then this vector was already contained in the span of the previous elements of V.

Proposition 6.1.7. *Let $\mathcal{A} \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let $V = \{v_1, \ldots, v_r\}$ be a set of vectors in $\mathcal{L}(\mathcal{A})$, and let $v \in \mathbb{Z}^n$. If we have $t\,\varrho'(v) \in I_V$ for some $t \in \mathbb{T}^n$, then there exist $c_1, \ldots, c_r \in \mathbb{Z}$ with $v = c_1 v_1 + \cdots + c_r v_r$. In particular, we see that $v \in \mathcal{L}(\mathcal{A})$.*

Proof. When we compute a Gröbner basis of I_V, forming S-polynomials and performing reduction steps preserves the property that the polynomials under consideration are unitary binomials. Therefore the resulting Gröbner basis consists of unitary binomials. Moreover, when we use Explicit Membership 3.1.9 to express $t\,\varrho'(v)$ in terms of the generators $\varrho(v_1), \ldots, \varrho(v_r)$, both the division of $t\,\varrho'(v)$ by the Gröbner basis and the expression of the Gröbner basis in terms of the generators use only operations involving integer coefficients. Hence, if we let $V_\pm = V \cup \{-v_1, \ldots, -v_r\}$, if we use $\varrho'(-v_i) = -\varrho'(v_i)$, and if we allow repetition of summands, we get a representation

$$t\,\varrho'(v) = t\,\mathbf{x}^{v^+} - t\,\mathbf{x}^{v^-} = \sum_{i=1}^{s} \mathbf{x}^{c_i}(\mathbf{x}^{u_i^+} - \mathbf{x}^{u_i^-})$$

with $c_i \in \mathbb{N}^n$ and $u_1, \ldots, u_s \in V_\pm$. To finish the proof we show that this representation implies $v = u_1 + \cdots + u_s$. Let $c = \log(t) \in \mathbb{N}^n$. We proceed by induction on s. For $s = 1$, the equation $t\,\mathbf{x}^{v^+} - t\,\mathbf{x}^{v^-} = \mathbf{x}^{c_1}(\mathbf{x}^{u_1^+} - \mathbf{x}^{u_1^-})$ implies $c + v^+ = c_1 + u_1^+$ and $c + v^- = c_1 + u_1^-$, and therefore $v = v^+ - v^- = u_1^+ - u_1^- = u \in V_\pm$.

Now consider the case $s > 1$. Since the term $t\,\mathbf{x}^{v^+}$ has to be equal to one of the terms $\mathbf{x}^{c_i}\mathbf{x}^{u_i^+}$, we may renumber $u_1, \ldots, u_s$ so that we have $t\,\mathbf{x}^{v^+} = \mathbf{x}^{c_1}\mathbf{x}^{u_1^+}$. Then the equality $c + v^+ = c_1 + u_1^+$ yields $v - u_1 = v^+ - v^- - u_1^+ + u_1^- = c_1 + u_1^- - c - v^-$. Let $\tilde{c} \in \mathbb{N}^n$ be the componentwise minimum of $c_1 + u_1^-$ and $c + v^-$, and let $\tilde{t} = \mathbf{x}^{\tilde{c}}$. In this way the vector $\tilde{v} = v - u_1$ satisfies $\tilde{c} + \tilde{v}^+ = c_1 + u_1^+$ and $\tilde{c} + \tilde{v}^- = c + v^-$. By applying the inductive hypothesis to the representation

$$\tilde{t}\,\varrho'(\tilde{v}) = \mathbf{x}^{c_1 + u_1^+} - \mathbf{x}^{c + v^-} = \sum_{i=2}^{s} \mathbf{x}^{c_i}(\mathbf{x}^{u_i^+} - \mathbf{x}^{u_i^-})$$

we obtain $\tilde{v} = v - u_1 = u_2 + \cdots + u_s$, i.e. the claim. □

The creation of the algorithm needs one more ingredient.

Proposition 6.1.8. *Let $V = \{v_1, \ldots, v_r\} \subset \mathbb{Z}^n$, let $c_1, \ldots, c_r \in \mathbb{Z}$, and let $v = c_1 v_1 + \cdots + c_r v_r$. Then there exist a term $t \in \mathbb{T}^n$ and polynomials $f_1, \ldots, f_r \in P$ such that*

$$t\,(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) = \sum_{i=1}^{r} f_i\,(\mathbf{x}^{v_i^+} - \mathbf{x}^{v_i^-})$$

Moreover, we have $f_i = \sum_{j=1}^{c_i} t_{ij}$ *if* $c_i > 0$ *and* $f_i = -\sum_{j=1}^{-c_i} t_{ij}$ *if* $c_i < 0$, *where the summands* t_{ij} *are pairwise distinct terms.*

Proof. First we prove the following claim. Let $w_1, \ldots, w_s \in \mathbb{Z}^n$, and let $v = w_1 + \cdots + w_s$. Then there exist terms $t, t_1, \ldots, t_s$ such that

$$t\,(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) = \sum_{i=1}^{s} t_i\,(\mathbf{x}^{w_i^+} - \mathbf{x}^{w_i^-})$$

We use induction on s. The case $s = 1$ is obviously true. For $s = 2$, the equality $v = w_1 + w_2$ yields $v^+ + w_1^- + w_2^- = v^- + w_1^+ + w_2^+$, and hence

$$\begin{aligned}\mathbf{x}^{w_1^-}\mathbf{x}^{w_2^-}(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) &= \mathbf{x}^{w_1^+}\mathbf{x}^{w_2^+}\mathbf{x}^{v^-} - \mathbf{x}^{w_1^-}\mathbf{x}^{w_2^-}\mathbf{x}^{v^-} \\ &= \mathbf{x}^{v^-}\mathbf{x}^{w_2^+}(\mathbf{x}^{w_1^+} - \mathbf{x}^{w_1^-}) + \mathbf{x}^{v^-}\mathbf{x}^{w_1^-}(\mathbf{x}^{w_2^+} - \mathbf{x}^{w_2^-})\end{aligned}$$

Now consider the case $s > 2$ and let $w = w_2 + \cdots + w_s$. By induction, there exist terms $t', t'_1, t'_2, t'', t''_2, \ldots, t''_s$ such that $t'(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) = t'_1(\mathbf{x}^{w_1^+} - \mathbf{x}^{w_1^-}) + t'_2(\mathbf{x}^{w^+} - \mathbf{x}^{w^-})$ and $t''(\mathbf{x}^{w^+} - \mathbf{x}^{w^-}) = \sum_{i=2}^{s} t''_i(\mathbf{x}^{w_i^+} - \mathbf{x}^{w_i^-})$. By multiplying the first equation by t'' and the second by t'_2, we get $t't''(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) = t'_1 t''(\mathbf{x}^{w_1^+} - \mathbf{x}^{w_1^-}) + \sum_{i=2}^{s} t'_2 t''_i(\mathbf{x}^{w_i^+} - \mathbf{x}^{w_i^-})$, as desired.

Next we apply this claim to the case $w_i = c_i v_i$. It yields terms $t, t_1, \ldots, t_s$ such that $t(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) = \sum_{i=1}^{s} t_i(\mathbf{x}^{c_i v_i^+} - \mathbf{x}^{c_i v_i^-})$. If $c_i > 0$, we can factorize as follows: $\mathbf{x}^{c_i v_i^+} - \mathbf{x}^{c_i v_i^-} = (\mathbf{x}^{v_i^+} - \mathbf{x}^{v_i^-}) \cdot \sum_{j=1}^{c_i} \mathbf{x}^{(j-1)v_i^+}\mathbf{x}^{(c_i-j)v_i^-}$. Similarly, if $c_i < 0$, we have a factorization $\mathbf{x}^{c_i v_i^+} - \mathbf{x}^{c_i v_i^-} = -(\mathbf{x}^{-c_i v_i^-} - \mathbf{x}^{-c_i v_i^+}) = -(\mathbf{x}^{v_i^+} - \mathbf{x}^{v_i^-}) \cdot \sum_{j=1}^{-c_i} \mathbf{x}^{(j-1)v_i^+}\mathbf{x}^{(-c_i-j)v_i^-}$. Altogether, we obtain a representation $t\,(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) = \sum_{i=1}^{s} f_i\,(\mathbf{x}^{v_i^+} - \mathbf{x}^{v_i^-})$ with $f_i = \sum_{j=1}^{c_i} t_i\,\mathbf{x}^{(j-1)v_i^+}\mathbf{x}^{(c_i-j)v_i^-}$ for $c_i > 0$ and with $f_i = \sum_{j=1}^{-c_i} t_i\,\mathbf{x}^{(j-1)v_i^+}\mathbf{x}^{(-c_i-j)v_i^-}$ for $c_i < 0$. □

Finally we can start the creation in earnest. The following theorem explains the difference between a toric ideal and its lattice ideals. It is widely regarded as a very good move towards an efficient algorithm for computing toric ideals.

Theorem 6.1.9. (Toric Ideals Via Saturation)
Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, *let* $\mathcal{L}(\mathcal{A})$ *be the kernel of the* $\mathbb{Z}$*-linear map* $\mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ *defined by* $\mathcal{A}$, *and let* $V = \{v_1, \ldots, v_r\} \subseteq \mathcal{L}(\mathcal{A})$. *Furthermore, let* $\pi = x_1 x_2 \cdots x_n$. *Then the following conditions are equivalent.*

a) We have $I(\mathcal{A}) = I_V :_P \pi^\infty$.
b) In the localization P_π *we have* $I(\mathcal{A})_\pi = (I_V)_\pi$.
c) The set V *generates the* $\mathbb{Z}$*-module* $\mathcal{L}(\mathcal{A})$.

Proof. The implication "a)⇒b)" follows from the fact that π is a unit in P_π. To prove "b)⇒a)" we recall that $I_V :_P \pi^\infty = I_V P_\pi \cap P$ by Proposition 3.5.11.b. Moreover, since $I(\mathcal{A})$ is a prime ideal and π is obviously

not one of its elements, we have $I(\mathcal{A}) = I(\mathcal{A}) :_P \pi^\infty = I(\mathcal{A})\, P_\pi \cap P$. By combining these equalities with b), we obtain the claim.

Next we show that a) implies c). For a vector $v \in \mathcal{L}(\mathcal{A})$, Proposition 6.1.4 shows $\varrho(v) \in I(\mathcal{A}) = I_V :_P \pi^\infty$. Therefore there exists a number $i \geq 1$ such that $\pi^i \varrho(v) \in I_V$. By Proposition 6.1.7, it follows that v is contained in the $\mathbb{Z}$-module generated by V. Hence V generates all of $\mathcal{L}(\mathcal{A})$.

Finally we prove that c) implies a). Given $f \in P$ with $\pi^i f \in I_V$ for some $i \geq 1$, the facts that $\pi^i f$ is contained in the prime ideal $I(\mathcal{A})$ and $\pi \notin I(\mathcal{A})$ imply $f \in I(\mathcal{A})$. Thus we have shown the inclusion $I_V :_P \pi^\infty \subseteq I(\mathcal{A})$. To prove the converse inclusion, we recall that Proposition 6.1.3.c says that $I(\mathcal{A})$ is generated by pure binomials. So, let $b \in I(\mathcal{A})$ be a pure binomial, and let $v = \vartheta(b) \in \mathcal{L}(\mathcal{A})$ be the unique vector with $b = \varrho(v)$. By assumption, there exist $c_1, \ldots, c_r \in \mathbb{Z}$ such that $v = c_1 v_1 + \cdots + c_r v_r$. Now Proposition 6.1.8 implies that there is a term $t \in \mathbb{T}^n$ such that $t\varrho(v) \in (\varrho(v_1), \ldots, \varrho(v_r)) = I_V$. Consequently, we have $\pi^i b = \pi^i \varrho(v) \in I_V$ for large enough i, and the proof is complete. □

Based on this theorem, we can formulate a first version of an efficient algorithm for computing toric ideals.

Corollary 6.1.10. *Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. Consider the following sequence of instructions.*

1) *Compute a system of generators $V = \{v_1, \ldots, v_r\}$ of $\mathcal{L}(\mathcal{A})$.*
2) *For $i = 1, \ldots, r$, write $v_i = v_i^+ - v_i^-$ and let $\varrho(v_i) = \mathbf{x}^{v_i^+} - \mathbf{x}^{v_i^-} \in P$. Form the lattice ideal $I_V = (\varrho(v_1), \ldots, \varrho(v_r))$ and compute the saturation $I = I_V :_P (x_1 \cdots x_n)^\infty$.*
3) *Return the ideal I and stop.*

This is an algorithm which computes the toric ideal $I(\mathcal{A})$ associated to $\mathcal{A}$.

There are many ways to perform step 1) of this algorithm. A common method is to compute the **Hermite normal form** of $\mathcal{A}$ and to read the solutions off the corresponding unimodular transformation matrix (see [Co93]). Clearly, this algorithm admits numerous optimizations. For instance, to compute the saturation in step 2) we can use the optimizations suggested by Tutorial 37.g,i and Tutorial 38.k.

6.1.B Hilbert Bases

Having created the universe of toric ideals and their computation, we return to our original intent: to make an apple pie from scratch. The dough of this pie is called its Hilbert basis. Although it requires some more work to really produce Hilbert bases, we can at least get started by defining them.

As before, we let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. We consider the homogeneous system of linear Diophantine equations $\mathcal{A}\,\mathbf{z} = 0$ and denote by $\mathcal{L}(\mathcal{A})$ the

subgroup of $\mathbb{Z}^n$ consisting of its solutions. Then we let $\mathcal{L}_+(\mathcal{A}) = \mathcal{L}(\mathcal{A}) \cap \mathbb{N}^n$ be the set of its componentwise non-negative solutions. Clearly, the set $\mathcal{L}_+(\mathcal{A})$ is a submonoid of $\mathbb{N}^n$.

Next we consider the following partial ordering $\succ$ on $\mathcal{L}_+(\mathcal{A})$. Given two vectors $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n) \in \mathcal{L}_+(\mathcal{A})$, we let $u \succ v$ if $u_i \geq v_i$ for $i = 1, \ldots, n$ and if this inequality is strict for some $i \in \{1, \ldots, n\}$. By Theorem 1.4.19, the ordering `Lex` is a term ordering on $\mathbb{N}^n$. Therefore its restriction to $\mathcal{L}_+(\mathcal{A})$ is a well-ordering. Obviously, $u \succ v$ implies $u >_{\texttt{Lex}} v$. Therefore there exist minimal elements in $\mathcal{L}_+(\mathcal{A}) \setminus \{0\}$ with respect to $\succ$.

Definition 6.1.11. The set of all minimal elements of $\mathcal{L}_+(\mathcal{A}) \setminus \{0\}$ with respect to the partial ordering $\succ$ is called the **Hilbert basis** of $\mathcal{L}_+(\mathcal{A})$.

As we have seen, the Hilbert basis of $\mathcal{L}_+(\mathcal{A})$ always exists. Below we shall show that it is finite and effectively computable. But first we want to prove that it has the desired property of generating the monoid $\mathcal{L}_+(\mathcal{A})$.

Proposition 6.1.12. *Let $\mathcal{A} \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let H be the Hilbert basis of $\mathcal{L}_+(\mathcal{A})$. Then every element of $\mathcal{L}_+(\mathcal{A})$ can be written as a linear combination of elements of H with coefficients in $\mathbb{N}$.*

Proof. Let $S \subseteq \mathcal{L}_+(\mathcal{A})$ be the set of all vectors which can be written as a linear combination of elements of H with coefficients in $\mathbb{N}$. For a contradiction, assume that $\mathcal{L}_+(\mathcal{A}) \setminus S \neq \emptyset$. We have already noted that `Lex` is a well-ordering on $\mathcal{L}_+(\mathcal{A})$. Hence there exists a minimal element $u \in \mathcal{L}_+(\mathcal{A}) \setminus S \neq \emptyset$ with respect to `Lex`. Clearly, we have $u \notin H$. Thus there exists a vector $v \in H$ such that $u \succ v$. Now we use that fact that $u - v \in \mathcal{L}_+(\mathcal{A})$ to conclude that $u \succ u - v$. This shows $u >_{\texttt{Lex}} u - v$, and therefore $u - v \in S$. But this implies $u \in S$, a contradiction. □

Slowly but surely our apple pie is taking shape, but one ingredient is still missing.

Definition 6.1.13. Let $\mathcal{A} \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. Then the matrix $\overline{\mathcal{A}} = \begin{pmatrix} \mathcal{A} & 0 \\ \mathcal{I}_n & \mathcal{I}_n \end{pmatrix}$ where $\mathcal{I}_n$ is the identity matrix of size n, is called the **Lawrence lifting** of $\mathcal{A}$.

In the following we want to show that the toric ideals of $\mathcal{A}$ and $\overline{\mathcal{A}}$ are closely related. The first connection between $\mathcal{A}$ and $\overline{\mathcal{A}}$ is that the map $\lambda : \mathcal{L}(\mathcal{A}) \longrightarrow \mathcal{L}(\overline{\mathcal{A}})$ defined by $\lambda(u) = (u, -u)$ is clearly bijective. But much more is true. However, before going into the details, we reinterpret $I(\overline{\mathcal{A}})$ as follows.

Remark 6.1.14. Recall that the toric ideal $I(\overline{\mathcal{A}})$ is contained in a polynomial ring $\overline{P} = K[x_1, \ldots, x_n, \xi_1, \ldots, \xi_n]$ having $2n$ indeterminates. It is the kernel of the K-algebra homomorphism

$$\bar{\varphi} : \overline{P} \longrightarrow \overline{L} = K[y_1, \ldots, y_m, w_1, \ldots, w_n, y_1^{-1}, \ldots, y_m^{-1}, w_1^{-1}, \ldots, w_n^{-1}]$$

defined by $x_i \mapsto t_i w_i$ and $\xi_j \mapsto w_j$ for $i, j \in \{1, \ldots, n\}$. Here the extended terms t_i are defined by $t_i = y_1^{a_{1i}} \cdots y_m^{a_{mi}}$ as in Definition 6.1.1.

To compute $I(\overline{\mathcal{A}})$, we can simplify the situation by looking at the commutative diagram

$$\begin{array}{ccc} \overline{P} = K[x_1, \ldots, x_n, \xi_1, \ldots, \xi_n] & \xrightarrow{\bar{\varphi}} & \overline{L} \\ \big\downarrow \varPhi & & \big\| \\ K[x_1, \ldots, x_n, w_1, \ldots, w_n] & \xrightarrow{\psi} & \overline{L} \end{array}$$

where $\varPhi$ is the K-algebra homomorphism given by $\varPhi(x_i) = x_i$ and $\varPhi(\xi_i) = w_i$ for $i = 1, \ldots, n$, and where ψ satisfies $\psi(x_i) = t_i w_i$ and $\psi(w_i) = w_i$ for $i = 1, \ldots, n$. Since $\varPhi$ is an isomorphism, we can identify the kernel of $\bar{\varphi}$ with the kernel of ψ using this isomorphism.

In this way, we shall from now on identify the toric ideal $I(\overline{\mathcal{A}})$ with its image under the isomorphism $\varPhi$. In other words, we shall consider $I(\overline{\mathcal{A}})$ as the ideal $\mathrm{Ker}(\psi)$ in $K[x_1, \ldots, x_n, w_1, \ldots, w_n]$.

Using this remark, we can now give an in-depth description of $I(\overline{\mathcal{A}})$.

Proposition 6.1.15. *Let $\mathcal{A} \in \mathrm{Mat}_{m,n}(K)$, let $\overline{\mathcal{A}}$ be the Lawrence lifting of $\mathcal{A}$, and let $Q = K[x_1, \ldots, x_n, w_1, \ldots, w_n]$.*

a) The toric ideal $I(\overline{\mathcal{A}}) \subseteq Q$ has a system of generators consisting of binomials of the form $x_1^{\alpha_1} \cdots x_n^{\alpha_n} w_1^{\beta_1} \cdots w_n^{\beta_n} - x_1^{\beta_1} \cdots x_n^{\beta_n} w_1^{\alpha_1} \cdots w_n^{\alpha_n}$ where $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbb{N}$.

b) There is a bijection between $\mathrm{PB}(I(\mathcal{A}))$ and $\mathrm{PB}(I(\overline{\mathcal{A}}))$ which maps a binomial $\mathbf{x}^\alpha - \mathbf{x}^\beta$ to $\mathbf{x}^\alpha \mathbf{w}^\beta - \mathbf{x}^\beta \mathbf{w}^\alpha$.

c) There is a bijection between $\mathcal{L}_+(\mathcal{A})$ and the elements in $\mathrm{PB}(I(\overline{\mathcal{A}}))$ of the form $\mathbf{x}^\alpha - \mathbf{w}^\alpha$ with $\alpha \in \mathbb{N}^n$.

Proof. First we prove a). As in Proposition 6.1.3, let $\pi = y_1 \cdots y_m$ and $J = (\pi^{\tau(t_1)}(x_1 - w_1 t_1), \ldots, \pi^{\tau(t_n)}(x_n - w_n t_n))$. In order to compute the toric ideal $I(\overline{\mathcal{A}}) \subseteq Q$ we have to eliminate $\{y_1, \ldots, y_m, z\}$ from the ideal generated by J and $\pi z - 1$ in the ring $\overline{Q} = K[x_1, \ldots, x_n, w_1, \ldots, w_n, y_1, \ldots, y_m, z]$. We equip $\overline{Q}$ with the $\mathbb{Z}^n$-grading defined by $(\mathcal{I}_n \mid \mathcal{I}_n \mid 0) \in \mathrm{Mat}_{n,2n+m+1}(\mathbb{Z})$ and observe that the ideal $J + (\pi z - 1)$ is homogeneous with respect to this grading. Hence also $I(\overline{\mathcal{A}})$ is homogeneous with respect to this grading. By Proposition 6.1.3.c, the toric ideal is generated by pure binomials. Thus the claim follows from the observation that pure binomials which are homogeneous with respect to the defined grading have the desired shape.

To prove b), we look at the sequence

$$\mathrm{PB}(I(\mathcal{A})) \xrightarrow{\vartheta} \mathcal{L}(\mathcal{A}) \xrightarrow{\lambda} \mathcal{L}(\overline{\mathcal{A}}) \xrightarrow{\varrho} \mathrm{PB}(I(\overline{\mathcal{A}}))$$

Here the map ϑ is defined by $\vartheta(\mathbf{x}^\alpha - \mathbf{x}^\beta) = \alpha - \beta$ for $\mathbf{x}^\alpha - \mathbf{x}^\beta \in \mathrm{PB}(I(\mathcal{A}))$, the map λ is given by $\lambda(u) = (u, -u)$, and the map ϱ satisfies $\varrho((u,v)) = \mathbf{x}^{u^+}\mathbf{w}^{v^+} - \mathbf{x}^{u^-}\mathbf{w}^{v^-}$ for $u, v \in \mathbb{Z}^n$. We have already noted that λ is a bijection. By Proposition 6.1.4.b, the maps ϑ and ϱ are bijective, too. Therefore the composition $\eta = \varrho \circ \lambda \circ \vartheta$ is a bijective map $\eta : \mathrm{PB}(I(\mathcal{A})) \longrightarrow \mathrm{PB}(I(\overline{\mathcal{A}}))$ which satisfies

$$\eta(\mathbf{x}^\alpha - \mathbf{x}^\beta) = (\varrho \circ \lambda)(\alpha - \beta) = \varrho((\alpha - \beta, \beta - \alpha)) = \mathbf{x}^\alpha \mathbf{w}^\beta - \mathbf{x}^\beta \mathbf{w}^\alpha$$

for all $\mathbf{x}^\alpha - \mathbf{x}^\beta \in \mathrm{PB}(I(\mathcal{A}))$.

Finally, we show c). Given $u \in \mathcal{L}_+(\mathcal{A})$, the corresponding element of $\mathrm{PB}(I(\mathcal{A}))$ is $\mathbf{x}^u - 1$, and the corresponding element of $\mathrm{PB}(I(\overline{\mathcal{A}}))$ is $\mathbf{x}^u - \mathbf{w}^u$. Thus the claim follows from b). □

The last part of this proposition yields a bijection between the minimal elements of $\mathcal{L}_+(\mathcal{A}) \setminus \{0\}$ with respect to $\succ$ and the elements $\mathbf{x}^u - \mathbf{w}^u$ in $\mathrm{PB}(I(\overline{\mathcal{A}}))$ with the property that there is no other element $\mathbf{x}^v - \mathbf{w}^v$ in $\mathrm{PB}(I(\overline{\mathcal{A}}))$ for which $u \succ v$. Let us call these elements the **primitive separated binomials** in $\mathrm{PB}(I(\overline{\mathcal{A}}))$.

Corollary 6.1.16. *Let $\mathcal{A} \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. Then there exists a bijection between the Hilbert basis of $\mathcal{L}_+(\mathcal{A})$ and the set of primitive separated binomials in $\mathrm{PB}(I(\overline{\mathcal{A}}))$.*

Proof. This follows from the observation that the two concepts of minimality correspond to each other via the bijection proved in part c) of the proposition. □

Now we put everything into the oven, let it bake for a while and out comes a beautiful theorem.

Theorem 6.1.17. (Finiteness and Computation of Hilbert Bases) *Let $\mathcal{A} \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let G be a reduced Gröbner basis of $I(\overline{\mathcal{A}})$. Then the set $H = \{\alpha \in \mathbb{N}^n \mid \mathbf{x}^\alpha - \mathbf{w}^\alpha \in G\}$ is finite, and it is the Hilbert basis of the monoid $\mathcal{L}_+(\mathcal{A})$.*

Proof. By Proposition 6.1.15, every reduced Gröbner basis G of $I(\overline{\mathcal{A}})$ consists of pure binomials of the form $\mathbf{x}^\alpha \mathbf{w}^\beta - \mathbf{x}^\beta \mathbf{w}^\alpha$ with $\alpha, \beta \in \mathbb{N}^n$. By Corollary 6.1.16, it suffices to show that the primitive separated binomials $\mathbf{x}^\alpha - \mathbf{w}^\alpha$ in $\mathrm{PB}(I(\overline{\mathcal{A}}))$ are precisely the elements of the form $\mathbf{x}^\alpha - \mathbf{w}^\alpha$ in G.

Let $\mathbf{x}^\alpha - \mathbf{w}^\alpha$ be a primitive separated binomial in $\mathrm{PB}(I(\overline{\mathcal{A}}))$. Its leading term is either $\mathbf{x}^\alpha$ or $\mathbf{w}^\alpha$. Suppose the leading term is $\mathbf{x}^\alpha$. Since there exists an element of G whose leading term divides $\mathbf{x}^\alpha$, there is an element of the form $\mathbf{x}^{\alpha'} - \mathbf{w}^{\alpha'}$ with $\alpha \succ \alpha'$ in G. By the definition of a primitive separated binomial, we get $\alpha = \alpha'$ and $\mathbf{x}^\alpha - \mathbf{w}^\alpha \in G$. If the leading term of $\mathbf{x}^\alpha - \mathbf{w}^\alpha$ is $\mathbf{w}^\alpha$, the same argument works.

Conversely, every element of the form $\mathbf{x}^\alpha - \mathbf{w}^\alpha$ in G is a primitive separated binomial because an element $\mathbf{x}^{\alpha'} - \mathbf{w}^{\alpha'}$ with $\alpha \succ \alpha'$ would have a leading term which properly divides one of the terms in the support of $\mathbf{x}^\alpha - \mathbf{w}^\alpha$. □

A first application of this theorem is the result announced at the end of Section 5.8.

Corollary 6.1.18. *Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. Then the K-vector space $P_{W,0}$ is a finitely generated K-algebra.*

Proof. A K-basis of $P_{W,0}$ is given by the set of terms $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ such that $W \cdot (\alpha_1, \ldots, \alpha_n)^{\mathrm{tr}} = 0$. Therefore the Hilbert basis of $\mathcal{L}_+(W)$ generates $P_{W,0}$ as a K-algebra. This Hilbert basis is finite by the theorem. □

Our style being ample, this section ends
with pompous examples and boastful comments.
(Martin Kreuzer, not painted on any sundial — yet)

In the last two sections we furnished you with toric ideals, Hilbert bases, exotic algebraic symbols, and a sophisticated tool for treating refined gradings. Now we find it most fitting to wind up this section with some examples demonstrating not only the power, but also the flexibility of these instruments. To put it bluntly, we use all this heavy artillery to shoot down a few innocent looking Diophantine equations. Although you could solve most of them by hand calculation or other methods, we hope that these examples will help you to grasp the method and apply it to more complicated situations, for instance in the exercises and tutorials. Let us begin with the equation mentioned in the introduction of this section.

Example 6.1.19. Consider the Diophantine equation $3z_1 - 5z_2 + 4z_3 = 0$. To find all triples $(a_1, a_2, a_3) \in \mathbb{N}^3$ which satisfy this equation, we can proceed as follows. Let $\mathcal{A} = (3\ -5\ 4)$. We use CoCoA to compute the reduced `DegRevLex`-Gröbner basis of the toric ideal of the Lawrence lifting of $\mathcal{A}$. The result is $\{x_2x_3^2w_1 - x_1w_2w_3^2,\ x_3w_1^3w_2 - x_1^3x_2w_3,\ x_1^2x_2^2x_3 - w_1^2w_2^2w_3,\ x_3^3w_1^4 - x_1^4w_3^3,\ x_1^5x_2^3 - w_1^5w_2^3,\ x_2^4x_3^5 - w_2^4w_3^5,\ x_1x_2^3x_3^3 - w_1w_2^3w_3^3\}$. Thus the set of primitive separated binomials in $\mathrm{PB}(I(\overline{\mathcal{A}}))$ is

$$\{x_1^2x_2^2x_3 - w_1^2w_2^2w_3,\ x_1^5x_2^3 - w_1^5w_2^3,\ x_2^4x_3^5 - w_2^4w_3^5,\ x_1x_2^3x_3^3 - w_1w_2^3w_3^3\}$$

Therefore the Hilbert basis of $\mathcal{L}_+(\mathcal{A})$ is $\{(2,2,1),\ (5,3,0),\ (0,4,5),\ (1,3,3)\}$. In other words, the non-negative solutions of the equation $3z_1 - 5z_2 + 4z_3 = 0$ are precisely the triples

$$(a_1, a_2, a_3) = n_1(2,2,1) + n_2(5,3,0) + n_3(0,4,5) + n_4(1,3,3)$$

with $n_1, n_2, n_3, n_4 \in \mathbb{N}$. This Hilbert basis can also be used to determine the subring $P_{\mathcal{A},0}$ where $P = K[x_1, x_2, x_3]$ is equipped with the $\mathbb{Z}$-grading given by $\mathcal{A}$. Corollary 6.1.18 yields $P_{\mathcal{A},0} = K[x_1^2x_2^2x_3,\ x_1^5x_2^3,\ x_2^4x_3^5,\ x_1x_2^3x_3^3]$.

Inhomogeneous Diophantine equations can be solved using a similar technique, but require an extra trick.

Example 6.1.20. Consider the Diophantine equation $2z_1 + 5z_2 + 3z_3 = 11$. We want to find its non-negative integer solutions. They are the non-negative integer solutions of the homogeneous equation $2z_1 + 5z_2 + 3z_3 - 11z_4 = 0$ having fourth coordinate one. Let $\mathcal{A} = (2\ 5\ 3\ -11)$. We use CoCoA to compute the reduced `DegRevLex`-Gröbner basis of the toric ideal of the Lawrence lifting of $\mathcal{A}$ and obtain the following primitive separated binomials:

$\{x_2x_3^2x_4 - w_2w_3^2w_4,\ x_1x_3^3x_4 - w_1w_3^3w_4,\ x_1^3x_2x_4 - w_1^3w_2w_4,\ x_1^4x_3x_4 - w_1^4w_3w_4,$
$x_1x_2^4x_4^2 - w_1w_2^4w_4^2,\ x_1^2x_2^3x_3x_4^2 - w_1^2w_2^3w_3w_4^2,\ x_2^6x_3x_4^3 - w_2^6w_3w_4^3,\ x_1^{11}x_4^2 - w_1^{11}w_4^2,$
$x_3^{11}x_4^3 - w_3^{11}w_4^3,\ x_2^{11}x_4^5 - w_2^{11}w_4^5\}$

So, the Hilbert basis of $\mathcal{L}_+(\mathcal{A})$ is $\{(0,1,2,1),\ (1,0,3,1),\ (3,1,0,1),\ (4,0,1,1),$ $(1,4,0,2),\ (2,3,1,2),\ (0,6,1,3),\ (11,0,0,2),\ (0,0,11,3),\ (0,11,0,5)\}$. Since we are only interested in solutions whose last coordinate is one, it is clear that the only solutions are $(0,1,2)$, $(1,0,3)$, $(3,1,0)$, and $(4,0,1)$.

The situation in this example was particularly favourable because no Hilbert basis vector has last coordinate zero and the number of solutions is finite. Our next example is more intricate.

Example 6.1.21. Consider the system of Diophantine equations

$$\begin{cases} z_1 + 4z_2 + z_3 - 2z_4 &= 5 \\ 2z_1 - z_2 + z_3 - 3z_4 &= 0 \end{cases}$$

To find its non-negative integer solutions, we determine the non-negative integer solutions of the associated homogeneous system

$$\begin{cases} z_1 + 4z_2 + z_3 - 2z_4 - 5z_5 &= 0 \\ 2z_1 - z_2 + z_3 - 3z_4 &= 0 \end{cases}$$

which have last coordinate one. Let $\mathcal{A} = \begin{pmatrix} 1 & 4 & 1 & -2 & -5 \\ 2 & -1 & 1 & -3 & 0 \end{pmatrix}$. We use CoCoA to compute the reduced `DegRevLex`-Gröbner basis of the toric ideal of the Lawrence lifting of $\mathcal{A}$ and obtain the following Hilbert basis of $\mathcal{L}_+(\mathcal{A})$:

$$\{(0,1,1,0,1),\ (1,0,1,1,0),\ (0,0,15,5,1),\ (5,10,0,0,9),\ (6,9,0,1,8),$$
$$(7,8,0,2,7),\ (8,7,0,3,6),\ (9,6,0,4,5),\ (10,5,0,5,4),\ (11,4,0,6,3),$$
$$(12,3,0,7,2),\ (13,2,0,8,1),\ (14,1,0,9,0)\}$$

Since we are interested in elements of $\mathcal{L}_+(\mathcal{A})$ whose last coordinate is one, the relevant solutions are those whose last coordinate is zero or one. Let $Z = \{n_1(1,0,1,1) + n_2(14,1,0,9) \mid n_1, n_2 \in \mathbb{N}\}$. Then we have three families of solutions, namely $(0,1,1,0) + Z$, $(0,0,15,5) + Z$, and $(13,2,0,8) + Z$. They were surely not easy to guess at first sight!

Our last example is a first step towards practical applications of this theory (see also Exercise 6). Furthermore, it shows how the methods introduced in the last two sections combine to provide us with a powerful toolbox. We can use multigraded Hilbert series to count solutions of systems of linear Diophantine equations and Hilbert bases to describe those solutions explicitly.

Example 6.1.22. Let us find out how many matrices in $\mathrm{Mat}_2(\mathbb{N})$ have both row sums equal to two. We can do this in four ways!

For the first method, we apply the theory developed in Section 5.8. We label each position in the matrix by an indeterminate. Then we notice that the matrices $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$ with $a_{11} + a_{12} = a_{21} + a_{22} = 2$ are in 1–1 correspondence with the power products $x_1^{a_{11}} x_2^{a_{12}} x_3^{a_{21}} x_4^{a_{22}}$ in $P = \mathbb{Q}[x_1, x_2, x_3, x_4]$ which have degree $\binom{2}{2}$ with respect to the grading given by $\left(\begin{smallmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{smallmatrix}\right)$. By Proposition 5.8.15, the bivariate Hilbert series of P with respect to this grading is

$$\mathrm{HS}_P(z_1, z_2) = \tfrac{1}{(1-z_1)^2(1-z_2)^2}$$

Therefore the answer is simply the coefficient of $z_1^2 z_2^2$ in the expansion of this series. By expanding the product $(1 + z_1 + z_1^2 + \cdots)^2 (1 + z_2 + z_2^2 + \cdots)^2$, we see that the answer is nine.

Alternatively, we can proceed in the following way. First we solve the homogeneous Diophantine equation $z_1 + z_2 = z_3 + z_4$ as in the previous examples. Using $\mathcal{A} = (1\ 1\ -1\ -1)$, the Hilbert basis of $\mathcal{L}_+(\mathcal{A})$ turns out to be $\{(1,0,1,0),\ (1,0,0,1),\ (0,1,0,1),\ (0,1,1,0)\}$. The corresponding matrices

$$\left(\begin{smallmatrix} 1 & 0 \\ 1 & 0 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$$

have row sums one. We are looking for all their $\mathbb{N}$-linear combinations with row sums equal to two. For this purpose, we use the above correspondence and represent them as power products $t_1 = x_1 x_3$, $t_2 = x_1 x_4$, $t_3 = x_2 x_4$, and $t_4 = x_2 x_3$ in P. Since their row sums are one, we need to determine the power products of degree two in the terms t_i. To compute the value of the Hilbert function of the ring $Q = \mathbb{Q}[t_1, t_2, t_3, t_4]$ in degree two, we use the surjective $\mathbb{Q}$-algebra homomorphism $\varphi : \mathbb{Q}[y_1, y_2, y_3, y_4] \longrightarrow Q$ defined by $y_i \mapsto t_i$. Its kernel I is the toric ideal of (t_1, t_2, t_3, t_4) and turns out to be $I = (y_1 y_3 - y_2 y_4)$. Therefore we get

$$\mathrm{HS}_Q(z) = \mathrm{HS}_{\mathbb{Q}[y_1,y_2,y_3,y_4]/I}(z) = \tfrac{1+z}{(1-z)^3} = 1 + 4z + 9z^2 + \cdots$$

and hence the desired number is $\mathrm{HF}_Q(2) = 9$. Using this method, we can even list the nine solution matrices. They correspond to the images under φ of the nine terms of degree two in $\mathbb{Q}[y_1, y_2, y_3, y_4]$ whose residue classes form a $\mathbb{Q}$-basis of $\mathbb{Q}[y_1, y_2, y_3, y_4]/I$. We find the following nine matrices:

$$\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 1 & 1 \\ 2 & 0 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 1 & 1 \\ 0 & 2 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 2 & 0 \\ 1 & 1 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 2 & 0 \\ 2 & 0 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 0 & 2 \\ 1 & 1 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 0 & 2 \\ 2 & 0 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 0 & 2 \\ 0 & 2 \end{smallmatrix}\right)$$

The third method is to solve the system of inhomogeneous Diophantine equations

$$\begin{cases} z_1 + z_2 &= 2 \\ z_3 + z_4 &= 2 \end{cases}$$

using the technique explained in the preceding example. The Hilbert basis of the associated homogeneous system is

$$\{(1,1,0,2,1),\ (0,2,1,1,1),\ (1,1,2,0,1),\ (1,1,1,1,1),\ (2,0,1,1,1),\\ (2,0,0,2,1),\ (0,2,0,2,1),\ (2,0,2,0,1),\ (0,2,2,0,1)\}$$

It yields the same nine solution matrices. Finally, we present the fourth method: hand calculation! Unfortunately, this method does not work in more complicated examples.

Exercise 1. Let K be a field, and let $P = K[x,y,z]$ be graded by $W = (2\ -5\ 1)$. Find a presentation of $P_{W,0}$ as an affine K-algebra.

Exercise 2. For every $i \geq 1$, find a Diophantine equation

$$a_{i1}z_1 + a_{i2}z_2 + a_{i3}z_3 = 0$$

such that the Hilbert basis of $\mathcal{L}_+((a_{i1}\ a_{i2}\ a_{i3}))$ has at least i elements.

Exercise 3. Consider the equation $2z_1 + 3z_2 + 5z_3 = 23$.

a) Using a suitable grading on a polynomial ring with three indeterminates, compute the number of non-negative solutions of this equation.
b) Find the solutions by exhaustive search.
c) Compute the Hilbert basis of $\mathcal{L}_+(\mathcal{A})$ where $\mathcal{A} = (2\ \ 3\ \ 5\ \ -23)$. Use it to determine the solutions of the above equation.

Exercise 4. Using the first three methods of Example 6.1.22, find the number of matrices in $\mathrm{Mat}_2(\mathbb{N})$ with first row sum 10 and second row sum 14. (*Hint:* For the second method, consider the Diophantine equation $14z_1 + 14z_2 = 10z_3 + 10z_4$.)

Exercise 5. (Diagonal Subalgebras of Polynomial Rings)
In this exercise we explore the concept of a diagonal subalgebra further (see Tutorial 82). First we recall its definition in the case of a graded polynomial ring. Let K be a field, and let $P = K[x_1, \ldots, x_n]$ be graded by $W \in \mathrm{Mat}_{2,n}(\mathbb{Z})$ of rank two. The K-subalgebra $\mathrm{Diag}(P) = \bigoplus_{i \in \mathbb{N}} P_{(i,i)}$ of P is called the **diagonal subalgebra** of P.

a) Show that the set Γ of all terms in $\mathrm{Diag}(P)$ is a monoid and that the Hilbert basis of $\log(\Gamma)$ corresponds to a system of K-algebra generators of $\mathrm{Diag}(P)$.
b) Write a CoCoA function `DiagGens(...)` which takes W and computes a system of K-algebra generators of $\mathrm{Diag}(\ldots)$. (*Hint:* Use the built-in command `HilbertBasis(...)`.)
c) Apply your function `DiagGens(...)` to the gradings given by the following matrices.

1) $W_1 = \binom{4\ 1\ 8}{1\ 5\ 3}$
2) $W_2 = \binom{1\ 1\ 1\ 0}{0\ 0\ 0\ 3}$
3) $W_3 = \binom{1\ 4\ 1\ 0\ 0}{0\ 0\ 0\ 2\ 5}$

d) Let $d \geq 2$ and $W = \binom{1\ 1\ \cdots\ 1\ 0}{0\ 0\ \cdots\ 0\ d}$. Prove that the diagonal subalgebra of P is generated by the terms in $\{tx_n \mid t \in \mathbb{T}(x_1, \ldots, x_{n-1})_d\}$. Interpret this result in terms of Veronese subrings (see Tutorial 66).

e) Finally, we generalize diagonal subalgebras of P as follows. Let $(r, s) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Show that $\mathrm{Slsa}_{(r,s)}(P) = \bigoplus_{i \in \mathbb{Z}} P_{(ir,is)}$ is a finitely generated K-subalgebra of P. It is called a **straight line subalgebra** of P.

f) Write a CoCoA function `Slsa(...)` which takes (r, s) and W and computes a set of K-algebra generators of the straight line subalgebra $\mathrm{Slsa}_{(r,s)}(P)$.

Exercise 6. (Margins of Matrices)
Given a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{N})$, we define the **row margins** of W to be the sums of the entries in each row, and the **column margins** of W to be the sums of the entries in each column. In statistics, matrices together with their row and column margins are called **contingency tables**. Our goal in this exercise is to enumerate contingency tables with given margins. Clearly, the margins have to be non-negative integers. We may assume that the margins are positive because otherwise the corresponding row or column of W is zero. Let $(r_1, \ldots, r_m) \in (\mathbb{N}_+)^m$ and $(c_1, \ldots, c_n) \in (\mathbb{N}_+)^n$.

a) Consider the following sequence of instructions.

1) Compute the Hilbert basis $\{v_1, \ldots, v_s\} \subset \mathbb{N}^{mn}$ of $\mathcal{L}_+(\mathcal{A})$ where $\mathcal{A} \in \mathrm{Mat}_{m+n-1,mn}(\mathbb{Z})$ is the coefficient matrix of the following linear system of equations:

$$\begin{aligned}
r_2z_{11} + \cdots + r_2z_{1n} - r_1z_{21} - \cdots - r_1z_{2n} &= 0\\
r_3z_{11} + \cdots + r_3z_{1n} - r_1z_{31} - \cdots - r_1z_{3n} &= 0\\
&\vdots\\
r_mz_{11} + \cdots + r_mz_{1n} - r_1z_{m1} - \cdots - r_1z_{mn} &= 0\\
c_1z_{11} + \cdots + c_1z_{1n} - r_1z_{11} - \cdots - r_1z_{m1} &= 0\\
c_2z_{11} + \cdots + c_2z_{1n} - r_1z_{12} - \cdots - r_1z_{m2} &= 0\\
&\vdots\\
c_nz_{11} + \cdots + c_nz_{1n} - r_1z_{1n} - \cdots - r_1z_{mn} &= 0
\end{aligned}$$

2) For $i = 1, \ldots, s$, write $v_i = (w_{jk}^{(i)})$ and form the term $t_i = \prod_{j,k} z_{jk}^{w_{jk}^{(i)}}$ in $\mathbb{Q}[z_{11}, \ldots, z_{mn}]$. Compute the kernel of the $\mathbb{Q}$-algebra homomorphism $\varphi : \mathbb{Q}[y_1, \ldots, y_s] \longrightarrow \mathbb{Q}[z_{11}, \ldots, z_{mn}]$ given by $y_i \mapsto t_i$.

3) Equip the ring $\mathbb{Q}[y_1, \ldots, y_s]$ with the $\mathbb{Z}$-grading defined by setting $\deg(y_i) = w_{11}^{(i)} + \cdots + w_{1n}^{(i)}$ for $i = 1, \ldots, s$. Compute the value of the Hilbert function of $\mathbb{Q}[y_1, \ldots, y_s]/\operatorname{Ker}(\varphi)$ in degree r_1 and return it.

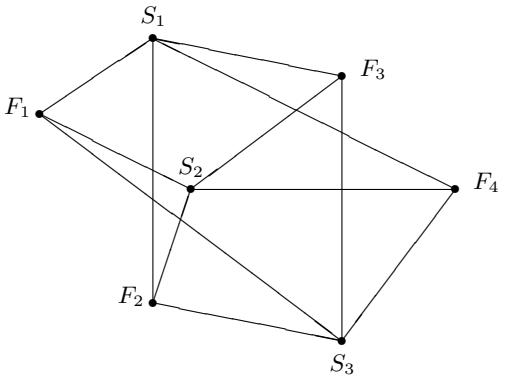
Prove that this is an algorithm which computes the number of contingency tables with row margins $(r_1, \ldots, r_m)$ and column margins $(c_1, \ldots, c_n)$.

b) Implement the above algorithm in a CoCoA function `Contingency(...)` which takes $(r_1, \ldots, r_m)$ and $(c_1, \ldots, c_n)$ and computes the number of contingency tables having these row and column margins.

c) Apply your function `Contingency(...)` to the following tuples of row and column margins. In each case, list all possible contingency tables.

1) $(6, 14)$, $(10, 10)$ (*Hint:* There are seven matrices.)
2) $(1, 1, 2)$, $(1, 1, 1, 1)$ (*Hint:* There are 12 matrices.)
3) $(5, 3, 5, 2)$, $(6, 4, 5)$ (*Hint:* There are 660 matrices.)

Exercise 7. (Transportation Plans)
Four factories F_1, F_2, F_3, F_4 produce, respectively, supplies of $120, 204, 92$, and 55 indivisible units of the same good. Three shops S_1, S_2, S_3 have respective demands of $183, 190$, and 98 units. There is a cost c_{ij} associated with transporting one unit from factory F_i to shop S_j. Let a_{ij} be the number of units of goods to be shipped from factory F_i to shop S_j. The tuple $(a_{11}, a_{12}, \ldots, a_{43}) \in \mathbb{N}^{12}$ is called a **transportation plan**.



a) Determine the linear system of equations satisfied by a transportation plan. In other words, find a matrix $\mathcal{A} \in \mathrm{Mat}_{7,12}(\mathbb{Z})$ such that the transportation plans are the solutions in $\mathbb{N}^{12}$ of the system of linear equations

$$\mathcal{A} \cdot (z_{11}, z_{12}, \ldots, z_{43})^{\mathrm{tr}} = (120, 204, 92, 55, 183, 190, 98)$$

b) Assume that the the cost function is given by the table

$$\begin{array}{c} \\ F_1 \\ F_2 \\ F_3 \\ F_4 \end{array} \begin{array}{c} \begin{array}{ccc} S_1 & S_2 & S_3 \end{array} \\ \begin{pmatrix} 1 & 1 & 3 \\ 2 & 1 & 1 \\ 1 & 1 & 2 \\ 3 & 2 & 1 \end{pmatrix} \end{array}$$

Show that $(120, 0, 0, 14, 190, 0, 0, 0, 92, 49, 0, 6)$ is a solution and its cost is 675.

c) Using the toric ideal associated to $\mathcal{A}$ and the cost function in b), prove that a solution of minimal cost is $(120, 0, 0, 0, 161, 43, 63, 29, 0, 0, 0, 55)$ and that its cost is 471.

Tutorial 84: Magic Squares

Genoa [...] first seduces you,
puts you under its spell,
and then only little by little
allows you to see its magic.
(Phyllis Macchioni)

About 2200 B.C. the Chinese constructed a magic square by decorating the back of a divine tortoise. Medieval alchemists believed that magic squares held the key to converting base metals into gold. What is so magic about magic squares? Why have these simple mathematical constructions drawn so much attention ever since ancient times? In this tutorial you will be prompted to explore some hidden secrets of magic squares, although we cannot promise that they will enable you to convert base metals into gold.

First of all, what is a magic square? Is it one of the squares of the magic city of Genova? Or is it a square matrix with non-negative integer entries such that the rows, the columns, and the two diagonals add up to the same natural number? In 1514, the German painter and engraver Albrecht Dürer made his most famous engraving, *Melencolia*. It contains the following *Jupiter magic square*

$$\begin{array}{|cccc|}\hline 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 12 \\ 4 & 15 & 14 & 1 \\ \hline \end{array}$$

Each row, column and diagonal of this square adds up to 34. In fact, this square is even more special because also the four entries of every 2×2 submatrix centered on one of the two diagonals add up to 34, the sum of two symmetric entries with respect to the center is always 17, and each number $1, 2, \ldots, 16$ occurs exactly once. Furthermore, the bottom row contains the engraving's date, 1514. In view of all these special properties, it is easy to see why some Renaissance astrologers believed that the charm of this magic square could cure *Melencolia*, a depressed state of mind which destroys an artist's enthusiasm for his work.

Thus we now introduce the following definition. A matrix $M \in \mathrm{Mat}_r(\mathbb{N})$ is called a **magic square** if its rows, columns, and its two diagonals all add up to the same number. This number is then called its **magic sum**. For instance, the Jupiter magic square has magic sum 34. Let $\mathrm{MQ}(r)$ be the set of magic squares of size $r \times r$. For every $s \in \mathbb{N}$, the set of elements of $\mathrm{MQ}(r)$ whose magic sum is s will be denoted by $\mathrm{MQ}(r, s)$. For instance, the only element of $\mathrm{MQ}(2, 2)$ is $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. In the following we let K be a field. (Observe that it does not matter which field we choose, so for actual computations we may opt for $K = \mathbb{Z}/(2)$.)

a) Using Example 6.1.22 as a guide, find a matrix W which defines a grading on $K[x_{11}, x_{12}, x_{21}, x_{22}]$ such that $\#\mathrm{MQ}(2, s)$ is a suitable coefficient in

the expansion of the Hilbert series of P with respect to the grading defined by W.

b) Using a), compute $\#\mathrm{MQ}(2,3)$, $\#\mathrm{MQ}(2,4)$ and $\#\mathrm{MQ}(2,5)$.

c) More generally, let $r \in \mathbb{N}_+$, and let $P = K[x_{11}, x_{12}, \ldots, x_{rr}]$ be a polynomial ring in r^2 indeterminates over K. Determine a matrix $W \in \mathrm{Mat}_{2r+2,r^2}(\mathbb{N})$ such that the coefficient of $z_1^s z_2^s \cdots z_{2r+2}^s$ in the expansion of the Hilbert Series $\mathrm{HS}_{P,W}(z_1, \ldots, z_{2r+2})$ is $\#\mathrm{MQ}(r,s)$.

d) Let us identify a magic square in $\mathrm{MQ}(r)$ with a term in P in the same way as in Example 6.1.22. Show that the elements in $\mathrm{MQ}(r)$ are in one-to-one correspondence with the non-negative solutions of a homogeneous system of linear Diophantine equations $\mathcal{A}\,\mathbf{z} = 0$ where the matrix $\mathcal{A}$ has entries in $\{-1, 0, 1\}$.

e) Let $\{v_1, \ldots, v_\ell\}$ be the Hilbert basis of $\mathcal{L}_+(\mathcal{A})$, and let $Q = K[t_1, \ldots, t_\ell]$ be the K-subalgebra of P generated by $t_i = \mathbf{x}^{v_i}$ for $i = 1, \ldots, \ell$. Show that $\#\mathrm{MQ}(r,s) = \mathrm{HF}_Q(s)$ for every $s \geq 0$.

f) Prove that $\#\mathrm{MQ}(2,s) = 1$ if s is even and $\#\mathrm{MQ}(2,s) = 0$ if s is odd.

g) Show that the Hilbert basis of $\mathrm{MQ}(3)$ is

$$\left\{ \begin{pmatrix} 1&1&1\\1&1&1\\1&1&1 \end{pmatrix}, \begin{pmatrix} 1&2&0\\0&1&2\\2&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&2\\2&1&0\\0&2&1 \end{pmatrix}, \begin{pmatrix} 2&0&1\\0&1&2\\1&2&0 \end{pmatrix}, \begin{pmatrix} 0&2&1\\2&1&0\\1&0&2 \end{pmatrix} \right\}$$

Deduce that the magic sum of every magic square of size 3×3 is a multiple of three.

h) Compute the Hilbert basis of $\mathrm{MQ}(4)$. Verify that it contains 20 squares, eight of which have magic sum one, and 12 of which have magic sum two.

i) Now get some inspiration from Example 6.1.22 and use the powerful function `Toric(...)` of CoCoA to show that $\#\mathrm{MQ}(4,34) = 163,890,864$.

The number of magic squares having the same magic number as the Jupiter magic square is almost 164 million! Now, is the Jupiter magic square really so special? In the remaining part of this tutorial we examine this question in detail.

j) The Jupiter magic square has the additional property that the four entries of each 2×2 submatrix centered on one of the diagonals sum to its magic number. Such magic squares are called **supermagic squares**. Prove that this property leads to 12 further linear equations. Compute the corresponding Hilbert basis and show that there are 12,186,468 supermagic squares in $\mathrm{MQ}(4,34)$.

k) The Jupiter magic square has also the following property: the sum of two entries which are symmetric with respect to the central point of the square is always 17. Such magic squares are called **associated magic squares**. Prove that every associated magic square of size 4×4 is supermagic, and that there are 35,208 associated supermagic squares in $\mathrm{MQ}(4,34)$.

l) Furthermore, the Jupiter magic square is a **traditional magic square**, i.e. it contains each of the numbers $1, 2, \ldots, 16$ exactly once. By exploit-

ing the presentation of the ring Q you used above, construct all associated supermagic squares of size 4×4. Show that 384 of them are traditional.

m) Finally, there is one last property of the Jupiter magic square that we have not yet used. Its two central lower positions contain the numbers 15 and 14 to commemorate the engraving's year of origin. By inspecting the 384 squares above, prove that there exist four squares having all the properties of the Jupiter magic square, and that they differ only by interchanging the first and last columns respectively the second and third rows. So, all in all, the Jupiter magic square is indeed rather unique!

n) But Albrecht Dürer could have done even better. Show that two of the four squares in m) have the additional property that their columns are increasing or decreasing sequences of numbers. This leaves us with one final assignment: find a nice property of one of these two squares which makes it unique, and thus maximizes its magic powers!

Tutorial 85: Computing the Gaps

This is the ingenuity gap,
the critical gap between our need
for ideas to solve complex problems
and our actual supply of those ideas.
(Thomas Homer-Dixon)

The purpose of this tutorial is to help you fill a small portion of your ingenuity gap. To begin with, we try to fill some critical gaps in your postage stamp collection. For the sake of argument, let us assume that you have a large supply of 30 cent and 50 cent stamps available, but no other values. You can easily pay for letters costing 0, 30, 50, 60, 80, 90, and 100 cents, since $60 = 30 + 30$, $80 = 30 + 50$, $90 = 30 + 30 + 30$, and $100 = 50 + 50$. Overcoming your ingenuity gap, you notice that you can also pay for letters costing $N \cdot 10$ cents where N is any integer greater than 10. For instance, you can add a suitable multiple of 30 to one of the numbers in $\{80, 90, 100\}$. On the other hand, no matter how ingenious you are, you cannot pay exactly for letters whose postage is not a multiple of ten, nor for those whose postage is 10, 20, 40, or 70 cents.

Do multivariate Hilbert series and toric ideals have any bearing on this postage stamp problem? Of course! Otherwise, would we be asking this rhetorical question? But instead of telling you what we know, instead of simplifying the intricate, let us generalize the problem. Assuming that you are collecting the stamps of several countries, which mixed frankings are you unable to realize given a finite number of combinations of denominations? In other words, given finitely many tuples $b_1, \ldots, b_r \in \mathbb{N}^n$, which elements of $\mathbb{N}^n$ are not contained in the submonoid generated by $\{b_1, \ldots, b_r\}$? These are the gaps. We seek their computation. You can find them with pure binomials, for in Computational Commutative Algebra there is no *ignorabimus*.

Let $r \in \mathbb{N}_+$, let $b_1, \ldots, b_r \in \mathbb{N}$, and let $B = (b_1, \ldots, b_r)$ be the submonoid of $\mathbb{N}$ generated by $\{b_1, \ldots, b_r\}$. We denote the set $\mathbb{N} \setminus B$ by $\mathrm{Gaps}(B)$ or $\mathrm{Gaps}(b_1, \ldots, b_r)$ and call its elements the **gaps** of B.

a) Let $b_1, b_2 \in \mathbb{N}_+$ be coprime numbers. Prove that $\mathrm{Gaps}(b_1, b_2)$ is finite. *Hint:* There exist $a_1, a_2 \in \mathbb{N}_+$ with $a_1 b_1 - a_2 b_2 = 1$. Add multiples $c(a_1 b_1 - a_2 b_2)$ with $0 < c < b_1$ to a big element of B.

b) Prove that $\mathrm{Gaps}(b_1, \ldots, b_r)$ is finite if and only if $\gcd(b_1, \ldots, b_r) = 1$. *Hint:* Use a) and induction on r.

c) Let K be a field, let $K[x]$ be standard graded, and let S be the K-subalgebra of $K[x]$ generated by $\{x^{b_1}, \ldots, x^{b_r}\}$. Show that one can compute HS_S by presenting S as $K[y_1, \ldots, y_r]/I$ where $K[y_1, \ldots, y_r]$ is graded by $W = (b_1\ b_2\ \cdots\ b_r)$ and I is a suitable toric ideal.

d) Write a CoCoA function `GapsHS(...)` which implements this method and apply it to compute the Hilbert series of $K[x^{b_1}, \ldots, x^{b_r}]$ for the following tuples $(b_1, \ldots, b_r)$.

   1) $(4, 7)$
   2) $(30, 50)$
   3) $(6, 10, 15)$

e) Using b) and d), write a CoCoA function `Gaps(...)` which takes the tuple $(b_1, \ldots, b_r)$, checks whether $\mathrm{Gaps}(b_1, \ldots, b_r)$ is finite or not, and returns accordingly, the set of gaps or the message `"Infinitely many gaps!"`. Apply your function to the examples in d).

f) Let $b_1, b_2 \in \mathbb{N}_+$ be coprime numbers. Prove that Hilbert series of the ring $S = K[x^{b_1}, x^{b_2}]$ is $\mathrm{HS}_S(z) = \frac{1 - z^{b_1 b_2}}{(1 - z^{b_1})(1 - z^{b_2})}$.

g) In the setting of f), give another proof of a) by showing that $\frac{1}{1-z} - \mathrm{HS}_S(z)$ is a polynomial. (*Hint:* Note that the residue class of b_2 generates the group $\mathbb{Z}/b_1\mathbb{Z}$.)

h) Let $b_1, b_2 \in \mathbb{N}_+$ be coprime numbers. Show that the largest element in $\mathrm{Gaps}(b_1, b_2)$ is $b_1 b_2 - b_1 - b_2$.

In the second part of this tutorial we generalize the above setting and find gaps of submonoids of $\mathbb{N}^n$. Let $r, n \in \mathbb{N}_+$, let $b_1, \ldots, b_r \in \mathbb{N}^n$, and let B be the submonoid of $\mathbb{N}^n$ generated by $\{b_1, \ldots, b_r\}$. As above, we denote the set $\mathbb{N}^n \setminus B$ by $\mathrm{Gaps}(B)$ or $\mathrm{Gaps}(b_1, \ldots, b_r)$ and call its elements the **gaps** of B.

Let K be a field and $P = K[x_1, \ldots, x_n]$. For $a = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, we denote the term $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ by $\mathbf{x}^a$. Furthermore, let S be the monomial K-subalgebra of P generated by $\mathbf{x}^{b_1}, \ldots, \mathbf{x}^{b_r}$, i.e. let $S = K[\mathbf{x}^{b_1}, \ldots, \mathbf{x}^{b_r}]$.

i) Show that S is a $\mathbb{Z}^n$-graded subalgebra of P with respect to the grading given by $\mathcal{I}_n \in \mathrm{Mat}_n(\mathbb{Z})$. Prove that one can compute the multivariate Hilbert series of S as follows.

   1) Represent S as a residue class algebra $K[y_1, \ldots, y_r]/I$ where I is a suitable toric ideal.

2) Equip the ring $K[y_1, \ldots, y_r]$ with the $\mathbb{Z}^n$-grading given by the matrix $W = (b_1 \ \cdots \ b_r) \in \mathrm{Mat}_{n,r}(\mathbb{Z})$ and show that I is homogeneous with respect to this grading.

j) Write a CoCoA function `GenGapsHS(...)` which takes $\{b_1, \ldots, b_r\}$ and computes the multivariate Hilbert series of $S = K[\mathbf{x}^{b_1}, \ldots, \mathbf{x}^{b_r}]$.

k) Apply your function `GenGapsHS(...)` to the following sets $\{b_1, \ldots, b_r\}$.
1) $\{6, 10, 15\} \subset \mathbb{N}$
2) $\{(2,0), (1,1), (0,2), (3,0), (1,2), (0,3)\} \subset \mathbb{N}^2$
3) $\{(2,0,0), (0,2,0), (0,0,2), (1,1,1), (5,0,0), (0,5,0), (0,0,5)\} \subset \mathbb{N}^3$

l) Explain how one can use the multivariate Hilbert series of S to decide whether $\mathrm{Gaps}(B)$ is finite or not. Write a CoCoA function `GenGaps(...)` which takes the tuple $(b_1, \ldots, b_r)$, checks whether $\mathrm{Gaps}(b_1, \ldots, b_r)$ is finite or not, and returns accordingly, the set of gaps or the message `"Infinitely many gaps!"`. Apply your function to the examples in k).

Always remember to check carefully whether your proof has a !

Tutorial 86: Matrices of Positive Type

You have to put your money where your mouth is.
(Wall Street Adage)

Only when the last tree is cut,
only when the last river is polluted,
only when the last fish is caught,
will they realise that you can't eat money.
(Native American Adage)

In Chapter 4 we put our money where our mouth is. We made a wishlist of good properties a nice grading should have: finitely generated graded modules should have finite dimensional homogeneous components, there should be a well-behaved minimal number of homogeneous generators, and there should be a term ordering on the monoid of degrees of non-zero polynomials. Then we showed that gradings of positive type have all these wonderful properties, and from there on we stopped worrying about gradings which don't. For instance, the entire treatment of multigraded Hilbert functions in Section 5.8 was based on the assumption that the polynomial ring is graded by a matrix of positive type. Therefore it is getting time for a confession: you can't eat this money, at least not yet. This is to say, given a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, we have not seen a method for detecting whether or not it is of positive type.

For instance, suppose we want to check if the matrix $W = \left(\begin{smallmatrix} -1 & 5 & -5 \\ -2 & 13 & -12 \end{smallmatrix}\right)$ is of positive type. So, we want to determine whether there exist $z_1, z_2 \in \mathbb{Z}$ with the property that $-z_1 - 2z_2$, $5z_1 + 13z_2$, and $-5z_1 - 12z_2$ are all positive integers. Fiddling with some plausible pairs (z_1, z_2) quickly shows that the grading given by W is actually a refinement of the standard grading. However, lacking this happenstance, how should we go about this in a systematic

way? One way to view the problem is to observe that we want to check if the system

$$\begin{cases} -z_1 - 2\,z_2 - z_3 &= 0 \\ 5z_1 + 13z_2 - z_4 &= 0 \\ -5z_1 - 12z_2 - z_5 &= 0 \end{cases}$$

has solutions in $\mathbb{Z}^2 \times \mathbb{N}^3$. This suggests that we should endeavour to generalize some of the theory in this section to the case where we require that only certain components of a solution are non-negative. After performing this task in the first part of the tutorial, the desired algorithm for checking whether a matrix is of positive type will follow easily.

Being of positive type ourselves, we hope that you will reap rich rewards from working through this tutorial, that not too many trees had to be cut for its production, and that the earth will not have to give way to an interplanetary bypass anytime soon.

To get going, let us introduce some terminology. Given an integer matrix $\mathcal{A} \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ and a set $N \subseteq \{1, \ldots, n\}$, we let

$$\mathcal{L}_N(\mathcal{A}) = \{(\alpha_1, \ldots, \alpha_n) \in \mathcal{L}(\mathcal{A}) \mid \alpha_i \geq 0 \text{ for all } i \in N\}$$

Observe that $\mathcal{L}_N(\mathcal{A})$ is a monoid and $\mathcal{L}_+(\mathcal{A}) = \mathcal{L}_N(\mathcal{A})$ for $N = \{1, \ldots, n\}$. By $\mathrm{PB}_N(I(\mathcal{A}))$, we denote the set all of pure binomials $\mathbf{x}^\alpha - \mathbf{x}^\beta$ for which no pair $(i,j) \in N^2$ satisfies both $x_i \mid \mathbf{x}^\alpha$ and $x_j \mid \mathbf{x}^\beta$. Analogously, let $\mathrm{PB}_N(I(\overline{\mathcal{A}}))$ be the set of all **N-separated binomials**, i.e. the set of all binomials $\mathbf{x}^\alpha \mathbf{w}^\beta - \mathbf{x}^\beta \mathbf{w}^\alpha$ for which no pair $(i,j) \in N^2$ satisfies both $x_i \mid \mathbf{x}^\alpha$ and $x_j \mid \mathbf{x}^\beta$.

a) Show that the map $\lambda : \mathcal{L}(\mathcal{A}) \longrightarrow \mathcal{L}(\overline{\mathcal{A}})$ defined by $\lambda(u) = (u, -u)$ induces a bijection between $\mathcal{L}_N(\mathcal{A})$ and $\mathcal{L}_N(\overline{\mathcal{A}})$.

b) Prove that the bijection between $\mathrm{PB}(I(\mathcal{A}))$ and $\mathrm{PB}(I(\overline{\mathcal{A}}))$ defined in Proposition 6.1.15.c identifies $\mathrm{PB}_N(I(\mathcal{A}))$ and $\mathrm{PB}_N(I(\overline{\mathcal{A}}))$.

c) Generalize Proposition 6.1.15.c by showing that there is a bijection between $\mathcal{L}_N(\mathcal{A})$ and the set of N-separated binomials in $\mathrm{PB}(I(\overline{\mathcal{A}}))$.

d) Generalize Corollary 6.1.16 by proving that there exists a bijection between the Hilbert basis of the monoid $\mathcal{L}_N(\mathcal{A})$ and the set of primitive N-separated binomials in $\mathrm{PB}(I(\overline{\mathcal{A}}))$.

e) Let G be a reduced Gröbner basis of $I(\overline{\mathcal{A}})$, and let H be the set of all N-separated binomials in G. Generalize Theorem 6.1.17 by showing that H is finite and is indeed the Hilbert basis of the monoid $\mathcal{L}_N(\mathcal{A})$.

f) Write a CoCoA function `HBpartial(...)` which takes the set N and the matrix $\mathcal{A}$ and computes the Hilbert basis of the monoid $\mathcal{L}_N(\mathcal{A})$.

g) Apply your function `HBpartial(...)` to compute the Hilbert basis of $\mathcal{L}_N(\mathcal{A})$ for the following examples.

1) $N_1 = \{1\}$, $\mathcal{A}_1 = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 5 & 12 \\ 1 & -5 & -13 \end{pmatrix}$

2) $N_2 = \{1, 2\}$, $\mathcal{A}_2 = \begin{pmatrix} -1 & 0 & 2 & 3 \\ -1 & 1 & 5 & -3 \\ 0 & -1 & -4 & 7 \end{pmatrix}$

3) $N_3 = \{1, 4\}$, $\mathcal{A}_3 = \begin{pmatrix} 1 & 1 & 0 & -1 \\ 1 & 0 & 1 & -2 \\ 0 & 1 & 1 & -4 \end{pmatrix}$

h) Now implement a CoCoA function `IsPosType`(...) which takes the matrix $\mathcal{A}$, checks whether it is of positive type, and returns the message `"Matrix not of positive type!"` or a tuple $(c_1, \ldots, c_m) \in \mathbb{Z}^m$ such that $c_1a_1 + \cdots + c_ma_m$ has positive entries only. Here $a_1, \ldots, a_m$ are the rows of $\mathcal{A}$. (*Hint:* Use the method of the example in the introduction of this tutorial and the function `HBpartial`(...).)

i) Apply your function `IsPosType`(...) to the following matrices.

1) $\begin{pmatrix} -1 & 5 & -5 \\ -2 & 13 & -12 \end{pmatrix}$

2) $\begin{pmatrix} -1 & 5 & 5 \\ -3 & 13 & 12 \end{pmatrix}$

3) $\begin{pmatrix} -1 & 5 & -5 & 1 \\ -1 & 13 & -12 & 1 \\ 2 & -1 & 1 & -3 \end{pmatrix}$

4) $\begin{pmatrix} -1 & 3 & -5 & 1 \\ 3 & -6 & -4 & 17 \\ -2 & -1 & 12 & -3 \end{pmatrix}$

6.2 Liftings of Ideals and Distractions

The four branches of arithmetic —
ambition, distraction, uglification and derision.
(Lewis Carroll)

In this section we address the problem of defining and computing *liftings* of ideals. Now, what is this supposed to mean? Are they heavy? Are they too awkward for one person to handle? Should you ask a co-worker for help? Do you need mechanical help? Maybe. Although we worked together intensely to provide you with light reading, it is a heavy task to find liftings of ideals with good properties. Here a lifting of a homogeneous ideal I in the polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K is a homogeneous ideal J in $\overline{P} = K[x_0, \ldots, x_n]$ such that I is obtained by setting $x_0 \mapsto 0$ in J and x_0 is a non-zero divisor for $\overline{P}/J$. For instance, homogenizations are liftings of degree form ideals (see Corollary 6.2.5).

The main reason why we are interested in lifting ideals will become evident in the next section where we lift zero-dimensional monomial ideals to vanishing ideals of projective point sets (see Theorem 6.3.31). For this purpose we are not only looking for some lifting of given monomial ideal, but a very nice one, namely a lifting which is a radical ideal. To find such nice liftings, we employ the second branch of arithmetic: *distractions*. The distraction of a term $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with respect to a tuple π of sequences of elements of K is the polynomial

$$D_\pi(t) = \prod_{i=1}^{\alpha_1} (x_1 - c_{1i}) \cdot \prod_{i=1}^{\alpha_2} (x_2 - c_{2i}) \cdot \cdots \prod_{i=1}^{\alpha_n} (x_n - c_{ni})$$

and the distraction of a monomial ideal is obtained by distracting its minimal monomial system of generators. Distraction is a rather well-behaved operation on monomial vector subspaces of P (see Proposition 6.2.10). Our main result, Theorem 6.2.12, says that the homogenization of the distraction of a monomial ideal is a lifting and a radical ideal. By applying this theorem you will be able to lift monomial ideals without any effort. To help you master this branch of arithmetic a.s.a.p., we now stop distracting you and start explaining liftings.

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be positively graded by a matrix $W \in \mathrm{Mat}_{1,n}(\mathbb{Z})$, and let $\overline{P} = K[x_0, \ldots, x_n]$ be graded by $\overline{W} = (1 \mid W)$. In Section 4.3 we considered the dehomogenization $F(1, x_1, \ldots, x_n)$ of a polynomial $F \in \overline{P}$. Here we study the K-algebra homomorphism $\overline{P} \longrightarrow P$ defined by $x_0 \mapsto 0$ and $x_i \mapsto x_i$ for $i = 1, \ldots, n$. Given a polynomial $F \in \overline{P}$, we let $F^{\inf} = F(0, x_1, \ldots, x_n)$, and for an ideal $J \subseteq \overline{P}$, we let $J^{\inf} = (F^{\inf} \mid F \in J)$. The following remark explains the choice of this notation.

Remark 6.2.1. Suppose that P and $\overline{P}$ are standard graded. In Tutorial 52 we saw that there exists an injective map $\imath_0 : \mathbb{A}^n \longrightarrow \mathbb{P}^n$ defined by $\imath_0(p_1, \ldots, p_n) = (1 : p_1 : \ldots : p_n)$.

a) A homogeneous ideal J in $\overline{P}$ defines a projective zero-set $V = \mathcal{Z}^+(J)$ in $\mathbb{P}^n$.
b) Its dehomogenization $J^{\mathrm{deh}} \subseteq P$ defines the affine part $V \cap \imath_0(\mathbb{A}^n)$ of V (see Tutorial 52.c).
c) The homogeneous ideal $J^{\mathrm{inf}} \subseteq P$ defines $V \cap H^{\mathrm{inf}} = V \cap \mathcal{Z}^+(x_0)$, the set of points at infinity of V (see Tutorial 52.h).

Our next lemma collects some easy results. You should compare its part b) with Theorem 4.3.22.a which contains a complementary statement.

Lemma 6.2.2. *Let f be a polynomial and I an ideal in P, and let J be a homogeneous ideal in $\overline{P}$.*

a) We have $(f^{\mathrm{hom}})^{\mathrm{inf}} = \mathrm{DF}_W(f)$.
b) We have $(I^{\mathrm{hom}})^{\mathrm{inf}} = \mathrm{DF}_W(I)$.
c) The ideal J^{inf} is homogeneous.

Proof. To prove a), we may assume that $f \neq 0$. Note that f can be decomposed into homogeneous components $f = f_1 + \cdots + f_s$ where $f_i \in P$ is a homogeneous polynomial and $\deg_W(f_1) > \cdots > \deg_W(f_s)$. By definition, we have $\mathrm{DF}_W(f) = f_1$. For $i = 2, \ldots, s$, let $\alpha_i = \deg_W(f_1) - \deg_W(f_i) > 0$. Now the claim follows from $f^{\mathrm{hom}} = f_1 + x_0^{\alpha_2} f_2 + \cdots x_0^{\alpha_s} f_s$.

Claim b) is a consequence of a) and the fact that the map which sends F to F^{inf} is a homomorphism. For the same reason, if $F_1, \ldots, F_r$ are homogeneous polynomials in $\overline{P}$ which generate J then $J^{\mathrm{inf}} = ({F_1}^{\mathrm{inf}}, \ldots, {F_r}^{\mathrm{inf}})$. Hence c) follows from the observation that the polynomials ${F_i}^{\mathrm{inf}}$ are homogeneous. □

Given an ideal $I \subseteq P$, Proposition 4.3.5.f says that x_0 is a non-zerodivisor for $\overline{P}/I^{\mathrm{hom}}$. In fact, homogenizations are characterized by this property, as the following proposition shows.

Proposition 6.2.3. *For a proper homogeneous ideal $J \subseteq \overline{P}$, the following conditions are equivalent.*

a) The indeterminate x_0 is a non-zerodivisor for $\overline{P}/J$.
b) We have $J = (J^{\mathrm{deh}})^{\mathrm{hom}}$.
c) We have $J^{\mathrm{inf}} = \mathrm{DF}_W(J^{\mathrm{deh}})$.

Proof. To prove that a) implies b), we apply the characterization of the homogenization given in Corollary 4.3.7. Since x_0 is a non-zerodivisor for $\overline{P}/J$, we have $J :_{\overline{P}} (x_0)^\infty = J$. As J is homogeneous, we get $J = (J^{\mathrm{deh}})^{\mathrm{hom}}$.

The fact that b) implies c) is an immediate consequence of Lemma 6.2.2.b. Thus it remains to prove that c) implies a). Suppose that there exists a non-zero homogeneous polynomial $\widetilde{F} \in \overline{P} \setminus J$ such that $x_0 \widetilde{F} \in J$. We choose such a polynomial $\widetilde{F}$ of minimal degree. We write $\widetilde{F} = x_0^{t-1} F$, where $F \in \overline{P}$ is a homogeneous polynomial which is not divisible by x_0, and where $t \geq 1$.

By assumption, there exists a homogeneous polynomial $G \in J$ such that $\mathrm{DF}_W(F^{\mathrm{deh}}) = G^{\mathrm{inf}}$. Since $G^{\mathrm{inf}} \neq 0$, the polynomial G is not divisible by x_0, and therefore $G = (G^{\mathrm{deh}})^{\mathrm{hom}}$. Now Lemma 6.2.2.a yields $\mathrm{DF}_W(F^{\mathrm{deh}}) = G^{\mathrm{inf}} = ((G^{\mathrm{deh}})^{\mathrm{hom}})^{\mathrm{inf}} = \mathrm{DF}_W(G^{\mathrm{deh}})$. Hence there is a homogeneous polynomial $G' \in \overline{P}$ such that $F - G = x_0 G'$. Here we have $G' \notin J$ because $F \notin G$. Since $G \in J$, we have $x_0^t(F - G) \in J$. Therefore we get $\deg_{\overline{W}}(G') < \deg_{\overline{W}}(F)$ and $x_0^{t+1} G' = x_0^t(F - G) \in J$ and $G' \notin J$, in contradiction to the minimality of $\deg_{\overline{W}}(\widetilde{F})$. □

For ideals which satisfy the equivalent conditions of this proposition, we introduce the following name.

Definition 6.2.4. Let $I \subset P$ be a homogeneous ideal. A homogeneous ideal J in $\overline{P}$ is called a **lifting** of I with respect to x_0 or an **x_0-lifting** of I if the following conditions are satisfied:

a) The indeterminate x_0 is a non-zero divisor for $\overline{P}/J$.
b) We have $I = J^{\mathrm{inf}}$.

In the following we shall find some ideals in P which have a lifting in $\overline{P}$. We start by considering the easiest cases.

Corollary 6.2.5. *Let I be a proper ideal in P.*

a) The ideal I^{hom} is an x_0-lifting of $\mathrm{DF}_W(I)$.
b) If I is homogeneous, the extension $I\,\overline{P}$ is an x_0-lifting of I.

Proof. To prove a), we observe that by Proposition 4.3.5.f, the indeterminate x_0 is a non-zero divisor for $\overline{P}/I^{\mathrm{hom}}$, and Lemma 6.2.2.b yields $(I^{\mathrm{hom}})^{\mathrm{inf}} = \mathrm{DF}_W(I)$. Claim b) follows from a), since if I is homogeneous, then $I = \mathrm{DF}_W(I)$ and $I^{\mathrm{hom}} = I\,\overline{P}$. □

Our next result gives us more insight into the structure of liftings. Later it will allow us to lift special ideals and prove useful properties.

Proposition 6.2.6. (Characterization of Liftings)
Let $I \subset P$ be a homogeneous ideal, and let $\{f_1, \ldots, f_s\}$ be a set of homogeneous generators of I. For a homogeneous ideal $J \subseteq \overline{P}$, the following conditions are equivalent.

a) The ideal J is an x_0-lifting of I.
b) There are polynomials $p_1, \ldots, p_s \in P$ of degree $\deg_W(p_i) < \deg_W(f_i)$ for $i = 1, \ldots, s$ such that the polynomials $g_i = f_i + p_i$ form a Macaulay basis of J^{deh} and additionally we have $J = (g_1^{\mathrm{hom}}, \ldots, g_s^{\mathrm{hom}})$.

Proof. First we prove that a) implies b). By Proposition 6.2.3, we have $J = (J^{\mathrm{deh}})^{\mathrm{hom}}$ and $I = \mathrm{DF}_W(J^{\mathrm{deh}})$. Thus $f_1, \ldots, f_s \in \mathrm{DF}_W(J^{\mathrm{deh}})$, and so there exist polynomials $g_1, \ldots, g_s \in J^{\mathrm{deh}}$ for which $f_i = \mathrm{DF}_W(g_i)$ for $i = 1, \ldots, s$. In particular, every polynomial g_i is of the form $g_i = f_i + p_i$

where each $p_i \in P$ has degree $\deg_W(p_i) < \deg_W(f_i)$. Now $\mathrm{DF}_W(J^{\mathrm{deh}}) = (f_1, \ldots, f_s) = (\mathrm{DF}_W(g_1), \ldots, \mathrm{DF}_W(g_s))$, and thus $\{g_1, \ldots, g_s\}$ is a Macaulay basis of J^{deh}. Theorem 4.3.19 yields the remaining claim $J = (J^{\mathrm{deh}})^{\mathrm{hom}} = (g_1^{\mathrm{hom}}, \ldots, g_s^{\mathrm{hom}})$.

To prove the converse implication, we note that $J = (g_1^{\mathrm{hom}}, \ldots, g_s^{\mathrm{hom}})$ implies $J^{\mathrm{deh}} = (g_1, \ldots, g_s)$. Since the set $\{g_1, \ldots, g_s\}$ is a Macaulay basis of J^{deh}, Theorem 4.3.19 yields $(J^{\mathrm{deh}})^{\mathrm{hom}} = (g_1^{\mathrm{hom}}, \ldots, g_s^{\mathrm{hom}}) = J$. Consequently, by Corollary 6.2.5.a, the ideal J is a lifting of $\mathrm{DF}_W(J^{\mathrm{deh}}) = (\mathrm{DF}_W(g_1), \ldots, \mathrm{DF}_W(g_s)) = (f_1, \ldots, f_s) = I$. □

The main class of ideals we want to lift in this section are monomial ideals. The ideals we shall lift to are called distractions. In order to explain the geometry underlying this algebraic concept, we need a lemma which provides useful rules for computing with ideals.

Lemma 6.2.7. *Let R be a ring, and let I_1, I_2, I_3, I_4 be ideals in R.*

a) We have the **distributive laws**

$$I_1(I_2 + I_3) = I_1I_2 + I_1I_3 \quad \textit{and} \quad (I_1 \cap I_2)I_3 \subseteq I_1I_3 \cap I_2I_3$$

b) If $I_1 \supseteq I_2$ or $I_1 \supseteq I_3$, we have the **modular law**

$$I_1 \cap (I_2 + I_3) = (I_1 \cap I_2) + (I_1 \cap I_3)$$

c) If $I_1 + I_2 = R$ then $I_1I_2I_3 + I_4 = (I_1I_3 + I_4) \cap (I_2I_3 + I_4)$.

Proof. In the first distributive law, the inclusion "$\subseteq$" holds since $I_1(I_2+I_3)$ is generated by elements of the form $f_1(f_2 + f_3) = f_1f_2 + f_1f_3$ with $f_i \in I_i$. The converse inclusion is clear. The second distributive law follows from $(I_1 \cap I_2)I_3 \subseteq I_1I_3$ and $(I_1 \cap I_2)I_3 \subseteq I_2I_3$. In the modular law, the inclusion "$\supseteq$" is obviously true. To prove the converse inclusion, we let $f \in I_1 \cap (I_2+I_3)$ and write $f = g + h$ with $g \in I_2$ and $h \in I_3$. Without loss of generality, assume that $I_1 \supseteq I_2$. Then we have $g \in I_1$, and therefore $h = f - g \in I_1$. This shows $f = g + h \in (I_1 \cap I_2) + (I_1 \cap I_3)$.

Next we show c). The inclusion "$\subseteq$" is clearly true. Using the hypothesis and a), we calculate

$$\begin{aligned}
(I_1I_3 + \quad I_4 \quad) \cap (I_2I_3 + I_4) &= [(I_1I_3 + I_4) \cap (I_2I_3 + I_4)]\,(I_1 + I_2) \\
&= [(I_1I_3 + I_4) \cap (I_2I_3 + I_4)]\,I_1 + [(I_1I_3 + I_4) \cap (I_2I_3 + I_4)]\,I_2 \\
&\subseteq [(I_1^2I_3 + I_1I_4) \cap (I_1I_2I_3 + I_1I_4)] + [(I_1I_2I_3 + I_2I_4) \cap (I_2^2I_3 + I_2I_4)] \\
&\subseteq I_1I_2I_3 + I_1I_4 + I_2I_4 = I_1I_2I_3 + (I_1 + I_2)\,I_4 \\
&= I_1I_2I_3 + I_4
\end{aligned}$$

and the proof is complete. □

Now we are ready to prove a fact which implies that ideals generated by certain products of linear forms are vanishing ideals of very special sets of points. This aspect will be studied further in the next section. Here we shall use these special ideals to lift monomial ideals to radical ideals.

Proposition 6.2.8. *Let $s \geq 1$, let $1 \leq i_1 < \cdots < i_s \leq n$, and for each $j \in \{1, \ldots, s\}$ let $f_j \in P$ be a squarefree polynomial which has the form $f_j = (x_{i_j} - c_{i_j 1}) \cdots (x_{i_j} - c_{i_j d_j})$ with $d_j \geq 1$ and $c_{i_j k} \in K$ for $k = 1, \ldots, d_j$. Then the ideal $I = (f_1, \ldots, f_s)$ satisfies*

$$I = \bigcap_{\substack{j_1=1,\ldots,d_1 \\ \vdots \\ j_s=1,\ldots,d_s}} (x_{i_1} - c_{i_1 j_1}, \ldots, x_{i_s} - c_{i_1 j_s})$$

Proof. For every ideal which is generated by squarefree polynomials of the given form, we let $\Delta(I) = d_1 + \cdots + d_s$. We argue by induction on $\Delta(I)$. For $\Delta(I) = 1$ the claim is clearly true because in this case I is generated by one linear polynomial. Likewise, if all the polynomials f_j are linear, there is nothing to prove.

Now consider the case $\Delta(I) > 1$. Without loss of generality we may assume that the polynomial f_1 has at least two factors. Thus we can write it in the form $f_1 = (x_{i_1} - c_{i_1 1})(x_{i_1} - c_{i_1 2})\tilde{f}_1$ with $\tilde{f}_1 \in P$. Then we have a decomposition $I = I_1 I_2 (\tilde{f}_1) + (f_2, \ldots, f_s)$ with $I_1 = (x_{i_1} - c_{i_1 1})$ and $I_2 = (x_{i_1} - c_{i_1 2})$. Since f_1 is squarefree, we see that $I_1 + I_2 = P$. Therefore we can apply Lemma 6.2.7.c and get

$$I = [((x_{i_1} - c_{i_1 1})\tilde{f}_1) + (f_2, \ldots, f_s)] \cap [((x_{i_1} - c_{i_1 2})\tilde{f}_1) + (f_2, \ldots, f_s)]$$

The ideals $J_1 = ((x_{i_1} - c_{i_1 1})\tilde{f}_1) + (f_2, \ldots, f_s)$ and $J_2 = ((x_{i_1} - c_{i_1 2})\tilde{f}_1) + (f_2, \ldots, f_s)$ satisfy $\Delta(J_1) < \Delta(I)$ and $\Delta(J_2) < \Delta(I)$. Now an application of the inductive hypothesis yields the claim. □

In the following, we let K be an infinite field. We choose n sequences $\pi_1, \ldots, \pi_n$ of elements of K in such a way that each sequence consists of pairwise distinct elements. Thus we let $\pi_i = (c_{i1}, c_{i2}, \ldots)$ with $c_{ij} \in K$ and $c_{ij} \neq c_{ik}$ for $j \neq k$.

Definition 6.2.9. Let $\pi = (\pi_1, \ldots, \pi_n)$.

a) For every term $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathbb{T}^n$, the polynomial

$$D_\pi(t) = \prod_{i=1}^{\alpha_1} (x_1 - c_{1i}) \cdot \prod_{i=1}^{\alpha_2} (x_2 - c_{2i}) \cdots \prod_{i=1}^{\alpha_n} (x_n - c_{ni})$$

is called the **distraction** of t with respect to π.

b) Let I be a monomial ideal in P, and let $\{t_1, \ldots, t_s\}$ be the unique minimal monomial system of generators of I. Then we say that the ideal $D_\pi(I) = (D_\pi(t_1), \ldots, D_\pi(t_s))$ is the **distraction** of I with respect to π.

c) The K-linear map $D_\pi : P \longrightarrow P$ defined by $t \mapsto D_\pi(t)$ for $t \in \mathbb{T}^n$ is called the the **π-distraction**.

In order to define the distraction $D_\pi(I)$, it suffices to specify the first $\max\{\deg_{x_i}(t_j) \mid j \in \{1,\dots,s\}\}$ elements of the sequence π_i. In particular, we do not have to assume that K is infinite.

Given two vector subspaces of P, we use the notation $V\,W$ to denote the vector subspace of P generated by $\{vw \mid v \in V, w \in W\}$. If $V = \langle v\rangle$, we simply write vW instead of $\langle v\rangle W$. Moreover, a monomial vector subspace of P is defined to be a vector subspace generated by terms. In the next proposition we forget for a moment the grading on P given by W and write $P_{\leq s}$ for the K-vector space of polynomials of standard degree less than or equal to s.

Proposition 6.2.10. *Let $\pi = (\pi_1,\dots,\pi_n)$, let D_π be the π-distraction, and let $V, V_1,\dots,V_r$ be monomial vector subspaces of P.*

a) For every $s \geq 1$, we have $D_\pi(V\,P_{\leq s}) = D_\pi(V)\,P_{\leq s}$.
b) For every $s \geq 1$, the π-distraction D_π induces an isomorphism of vector spaces $D_\pi : P_{\leq s} \longrightarrow P_{\leq s}$. In particular, the map D_π is bijective.
c) We have $\bigcap_{i=1}^r D_\pi(V_i) = D_\pi(\bigcap_{i=1}^r V_i)$.

Proof. First we show a) by induction on s. To prove the formula for $s = 1$, it suffices to show that we have $D_\pi(t\,P_{\leq 1}) = D_\pi(t)\,P_{\leq 1}$ for every $t \in \mathbb{T}^n$. Let $t = x_1^{\alpha_1}\cdots x_n^{\alpha_n} \in \mathbb{T}^n$. Since $\{1, x_1,\dots,x_n\}$ is a K-basis of $P_{\leq 1}$, we have $D_\pi(t\,P_{\leq 1}) = \langle D_\pi(t), D_\pi(x_1 t),\dots,D_\pi(x_n t)\rangle$. The latter vector space is equal to $\langle D_\pi(t), (x_1 - c_{1\,\alpha_1+1})D_\pi(t),\dots,(x_n - c_{n\,\alpha_n+1})D_\pi(t)\rangle$ and this is equal to $D_\pi(t)\,P_{\leq 1}$ since also $\{1, x_1 - c_{1\,\alpha_1+1},\dots,x_n - c_{n\,\alpha_n+1}\}$ is a K-basis of $P_{\leq 1}$. For $s > 1$, we use $P_{\leq 1}\,P_{\leq s} = P_{\leq s+1}$ and the inductive hypothesis to get $D_\pi(V\,P_{\leq s}) = D_\pi(V\,P_{\leq s-1}\,P_{\leq 1}) = D_\pi(V\,P_{\leq s-1})\,P_{\leq 1} = D_\pi(V)\,P_{\leq s-1}\,P_{\leq 1} = D_\pi(V)\,P_{\leq s}$.

By taking $V = K$ in a), we get that D_π induces a surjective K-linear map from $P_{\leq s}$ onto itself. This implies b), and c) is an immediate consequence of b). □

Before we proceed to the main theorem of this section, we insert the characterization of irreducible monomial ideals we promised in Tutorial 77.

Proposition 6.2.11. *A monomial ideal I in P is irreducible if and only if it is of the form $I = (x_{i_1}^{d_1},\dots,x_{i_s}^{d_s})$ with $1 \leq i_1 < \cdots < i_s \leq n$ and $d_1,\dots,d_s \in \mathbb{N}$.*

Proof. First we assume that I is irreducible. Let $t_1,\dots t_s \in \mathbb{T}^n$ be a system of generators of I. If one of the terms, say t_1, factors non-trivially into $t_1 = t_1' t_1''$ with coprime terms $t_1', t_1'' \in \mathbb{T}^n$, we have a decomposition $I = (t_1', t_2,\dots,t_s) \cap (t_1'', t_2,\dots,t_s)$ which contradicts the irreducibility of I. Hence I is necessarily of the stated form.

Conversely, suppose that I is of the form $I = (x_{i_1}^{d_1}, \ldots, x_{i_s}^{d_s})$ with $1 \leq i_1 < \cdots < i_s \leq n$ and $d_1, \ldots, d_s \in \mathbb{N}$. For a contradiction, assume that we have $I = J_1 \cap J_2$ with ideals J_1, J_2 which contain I properly. We choose $f \in J_1 \setminus I$ and $g \in J_2 \setminus I$. By multiplying f and g by suitable terms, we find elements $\tilde{f} \in J_1 \setminus I$ and $\tilde{g} \in J_2 \setminus I$ such that $(x_{i_1}, \ldots, x_{i_s})\tilde{f} \in I$ and $(x_{i_1}, \ldots, x_{i_s})\tilde{g} \in I$. Let $t = x_{i_1}^{d_1-1} \cdots x_{i_s}^{d_s-1}$. Since $I :_P (x_{i_1}, \ldots, x_{i_s}) = (t)$, the term t divides both $\tilde{f}$ and $\tilde{g}$, i.e. there exist $f', g' \in P$ for which $\tilde{f} = tf'$ and $\tilde{g} = tg'$. Using Proposition 5.6.20, it is easy to see that I is a primary ideal. Then $tf'g' \in (I + (\tilde{f})) \cap (I + (\tilde{g})) \subseteq J_1 \cap J_2 = I$ shows that we have $f'g' \in \sqrt{I} = (x_{i_1}, \ldots, x_{i_s})$. Hence we conclude that $f' \in (x_{i_1}, \ldots, x_{i_s})$ or $g' \in (x_{i_1}, \ldots, x_{i_s})$, and therefore $\tilde{f} \in I$ or $\tilde{g} \in I$, a contradiction. □

The following theorem says that distractions allow us to lift monomial ideals to radical ideals. It is remarkable that, besides monomial ideals, very few ideals are known to have liftings which are radical ideals.

Theorem 6.2.12. (Liftings of Monomial Ideals)
Let $\pi = (\pi_1, \ldots, \pi_n)$, let $I \subset P$ be a monomial ideal, and let $\{t_1, \ldots, t_s\}$ be its minimal monomial system of generators.

a) The distraction $D_\pi(I)$ is an intersection of finitely many ideals which are generated by linear polynomials.
b) The distraction $D_\pi(I)$ is a radical ideal.
c) For every term ordering σ on $\mathbb{T}^n$, the set $\{D_\pi(t_1), \ldots, D_\pi(t_s)\}$ is the reduced σ-Gröbner basis of $D_\pi(I)$.
d) We have $D_\pi(I)^{\text{hom}} = (D_\pi(t_1)^{\text{hom}}, \ldots, D_\pi(t_s)^{\text{hom}})$ in $\overline{P}$. This ideal is an x_0-lifting of I and a radical ideal.

Proof. First we show a). By Proposition 5.6.17.a, every ideal is a finite intersection of irreducible ideals. Therefore Proposition 6.2.10.c allows us to assume that I is irreducible, and hence of the shape described in Proposition 6.2.11. Then the ideal $D_\pi(I)$ satisfies the conditions of Proposition 6.2.8 and this proposition yields the claim. For the proof of b) we use a) and the fact that ideals generated by linear polynomials are prime ideals.

Next we prove c). For $s = 1$, the claim is obviously true. Now consider the case $s > 1$. The rules for computing with leading terms 1.5.3 imply $\mathrm{LT}_\sigma(D_\pi(t_i)) = t_i$ for $i = 1, \ldots, s$. By Theorem 2.3.7, the syzygy module of the tuple $\mathcal{T} = (t_1, \ldots, t_s) = (\mathrm{LT}_\sigma(D_\pi(t_1)), \ldots, \mathrm{LT}_\sigma(D_\pi(t_s))$ is generated by the fundamental syzygies $\{\sigma_{\mu\nu} \mid 1 \leq \mu < \nu \leq s\}$.

Let $1 \leq \mu < \nu \leq s$. We write $t_\mu = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $t_\nu = x_1^{\beta_1} \cdots x_n^{\beta_n}$. Then we set $\gamma_i = \max\{\alpha_i, \beta_i\}$ for $i = 1, \ldots, n$. The fundamental syzygy of t_μ and t_ν is

$$\sigma_{\mu\nu} = x_1^{\gamma_1 - \alpha_1} \cdots x_n^{\gamma_n - \alpha_n} e_\mu - x_1^{\gamma_1 - \beta_1} \cdots x_n^{\gamma_n - \beta_n} e_\nu \in P^s$$

For $i = 1, \ldots, n$, we define $f_i = (x_i - c_{i\,\alpha_i+1}) \cdots (x_i - c_{i\,\beta_i})$ if $\alpha_i < \beta_i$ and $f_i = 1$ if $\alpha_i \geq \beta_i$. Moreover, let $f_i' = (x_i - c_{i\,\beta_i+1}) \cdots (x_i - c_{i\,\alpha_i})$

if $\alpha_i > \beta_i$ and $f_i' = 1$ if $\alpha_i \leq \beta_i$. Then it is easy to check that $s_{\mu\nu} = f_1 \cdots f_n\, e_\mu - f_1' \cdots f_n'\, e_\nu \in P^s$ is a syzygy of $(D_\pi(t_1), \ldots, D_\pi(t_s))$, and that the σ-leading form of this syzygy in the sense of Definition 2.3.4 is $\mathrm{LF}_{\sigma,\mathcal{T}}(s_{\mu\nu}) = \sigma_{\mu\nu}$. Therefore Condition D_2) of Theorem 2.4.1 is satisfied and $\{D_\pi(t_1), \ldots, D_\pi(t_s)\}$ is a σ-Gröbner basis of $D_\pi(I)$.

Moreover, this Gröbner basis is actually the reduced σ-Gröbner basis of $D_\pi(I)$: it is monic, its leading terms $\{t_1, \ldots, t_s\}$ are the minimal monomial system of generators of $\mathrm{LT}_\sigma(D_\pi(I)) = I$, and the terms in the support of $D_\pi(t_i) - t_i$ cannot be reduced further, because they are proper divisors of t_i.

Finally, we prove d). Since all terms in the support of $D_\pi(t_i)$ are divisors of t_i, and since P is positively $\mathbb{Z}$-graded by W, we have $\mathrm{DF}_W(D_\pi(t_i)) = t_i$ for $i = 1, \ldots, s$. By choosing a term ordering σ which is compatible with $\deg_W$ and applying Proposition 4.2.15, we see that $\{D_\pi(t_1), \ldots, D_\pi(t_s)\}$ is a Macaulay basis of $D_\pi(I)$ and that $\mathrm{DF}_W(D_\pi(I)) = I$. Hence Theorem 4.3.19 yields $D_\pi(I)^{\mathrm{hom}} = (D_\pi(t_1)^{\mathrm{hom}}, \ldots, D_\pi(t_s)^{\mathrm{hom}})$. Then Lemma 6.2.2 shows $(D_\pi(I)^{\mathrm{hom}})^{\mathrm{inf}} = \mathrm{DF}_W(D_\pi(I)) = I$. By Proposition 4.3.5.f, the indeterminate x_0 is a non-zero divisor for $\overline{P}/D_\pi(I)^{\mathrm{hom}}$. Altogether, it follows that the ideal $D_\pi(I)^{\mathrm{hom}} = (D_\pi(t_1)^{\mathrm{hom}}, \ldots, D_\pi(t_s)^{\mathrm{hom}})$ is an x_0-lifting of I. The fact that it is a radical ideal is a consequence of Proposition 4.3.10.c, because $D_\pi(I)$ is a radical ideal by b), and this property is preserved under homogenization. □

The following example illustrates the theorem by showing how to lift a specific monomial ideal.

Example 6.2.13. Let $P = \mathbb{Q}[x_1, x_2, x_3, x_4]$ be standard graded, and let $I = (t_1, t_2, t_3)$ be the monomial ideal in P which is minimally generated by $t_1 = x_1^3 x_2$, $t_2 = x_1 x_2 x_3^2$, and $t_3 = x_1^2 x_4^4$. Now we choose sequences $\pi_1 = (2, 3, 4, \ldots)$, $\pi_2 = (5, \ldots)$, $\pi_3 = (6, 4, \ldots)$, and $\pi_4 = (0, 1, 2, 3, \ldots)$ where it does not matter which values we choose for the dots because they are not used. Then we let $\pi = (\pi_1, \pi_2, \pi_3, \pi_4)$ and compute

$$\begin{aligned}
D_\pi(t_1)^{\mathrm{hom}} &= (x_1 - 2x_0)(x_1 - 3x_0)(x_1 - 4x_0)(x_2 - 5x_0) \\
D_\pi(t_2)^{\mathrm{hom}} &= (x_1 - 2x_0)(x_2 - 5x_0)(x_3 - 6x_0)(x_3 - 4x_0) \\
D_\pi(t_3)^{\mathrm{hom}} &= (x_1 - 2x_0)(x_1 - 3x_0)\, x_4\, (x_4 - x_0)(x_4 - 2x_0)(x_4 - 3x_0)
\end{aligned}$$

Now part d) of the theorem says that $(D_\pi(t_1)^{\mathrm{hom}}, D_\pi(t_2)^{\mathrm{hom}}, D_\pi(t_3)^{\mathrm{hom}})$ is an x_0-lifting of I and a radical ideal.

If you are looking for further distractions, we invite you to indulge in some gin (see Exercise 6) or Super Great Spaghetti (see Tutorial 87).

For centuries, people thought the moon was made of green cheese.
Then the astronauts found that the moon is really a big hard rock.
That's what happens to cheese when you leave it out.
(Age 6, from "Deep Thoughts from Young Minds")

Exercise 1. Let K be a field, let $P = K[x_1, \ldots, x_n]$, let σ be a term ordering on $\mathbb{T}^n$, and let I be an ideal in P.

a) Prove that if $\mathrm{LT}_\sigma(I)$ is a radical ideal then I is radical, too.
b) Show that the converse to part a) is not true in general.
c) Using a), give an alternative proof of the last claim in Theorem 6.2.12.d.

Exercise 2. Let K be a field, let $P = K[x, y, z]$, and let I be the ideal $(x^2y^2, x^2z, x^3, y^3, z^4)$. Write I as an intersection of irreducible monomial ideals.

Exercise 3. In the setting of Theorem 6.2.12, prove that every subset of $\{D_\pi(t_1), \ldots, D_\pi(t_s)\}$ is the reduced σ-Gröbner basis of the ideal it generates.

Exercise 4. Let K be a field, and let $P = K[x_1, \ldots, x_n]$.

a) Let σ be a term ordering on $\mathbb{T}^n$. Characterize all pairs $(f, g) \in P^2$ for which $\{f, g\}$ is a σ-Gröbner basis of the ideal (f, g).
b) Characterize all pairs $(f, g) \in P^2$ for which $\{f, g\}$ is a σ-Gröbner basis of the ideal (f, g) for every term ordering σ.

Exercise 5. Let K be an infinite field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let $I \subseteq P$ be a monomial ideal, and let $\overline{P} = K[x_0, \ldots, x_n]$ be standard graded. We choose sequences $\pi_1, \ldots, \pi_n$ of pairwise distinct elements of K and set $\pi = (\pi_1, \ldots, \pi_n)$. Prove that the ideal $J = D_\pi(I)^{\mathrm{hom}} \subseteq \overline{P}$ satisfies $\Delta \mathrm{HF}_{\overline{P}/J}(i) = \mathrm{HF}_{P/I}(t)$ for all $i \in \mathbb{Z}$.

Exercise 6. (Gin, Strongly Stable Ideals, and Distractions)
Would you like to have more distractions? How about another sip of gin? Let K be a an infinite field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let $I \subseteq P$ be a homogeneous ideal, and let σ be a term ordering on $\mathbb{T}^n$. Given further indeterminates y_{ij}, let $L = K(y_{ij})$, let $\mathcal{Y} = (y_{ij}) \in \mathrm{Mat}_n(L)$, and let $\Psi_\mathcal{Y} : L[x_1, \ldots, x_n] \longrightarrow L[x_1, \ldots, x_n]$ be the homogeneous linear change of coordinates defined by $\mathcal{Y}$. Recall that the ideal $\mathrm{gin}_\sigma(I) = \mathrm{LT}_\sigma(\Psi_\mathcal{Y}(I))$ is called the **generic initial ideal** of I with respect to σ (see Tutorial 75).

a) Show that there exist two matrices $\mathcal{L}$,$\mathcal{U} \in \mathrm{Mat}_n(L)$ such that $\mathcal{L}$ is lower triangular, $\mathcal{U}$ is upper triangular, and we have $\mathcal{Y} = \mathcal{U}\mathcal{L}$.
b) Prove that we have $\mathrm{gin}_\sigma(I) = \mathrm{LT}_\sigma(\Psi_\mathcal{L}\Psi_\mathcal{U}(I))$.
c) For a strongly stable ideal $I \subseteq P$ (as defined in Tutorial 75), show that $\Psi_\mathcal{U}(I) = I$.
d) Show that we have $\mathrm{LT}_\sigma(\Psi_\mathcal{L}(I)) = \mathrm{LT}_\sigma(I)$ for every ideal $I \subseteq P$.
e) Combine everything to show that a strongly stable ideal $I \subseteq P$ satisfies $\mathrm{gin}_\sigma(I) = I$.

Now we consider the monomial ideal $I = (x_1^5, x_1^4x_2, x_1^4x_3, x_1^3x_2^2, x_1^2x_2^3)$ in $P = \mathbb{Q}[x_1, x_2, x_3]$. For every $i \in \{1, 2, 3\}$, let $\pi_i = (0, 1, 2, \ldots)$, and let $\pi = (\pi_1, \pi_2, \pi_3)$. Then consider the homogeneous ideal $J = D_\pi(I)^{\mathrm{hom}}$ in $\overline{P} = \mathbb{Q}[x_0, x_1, x_2, x_3]$.

f) Show that we have $\mathrm{gin}_\sigma(J/x_0J) = I$.
g) Let $\ell \in \overline{P}$ be a linear form with randomly chosen coefficients. Using CoCoA, check that we have $\mathrm{gin}_{\mathtt{DegRevLex}}(J/\ell J) = I$.
h) Let σ be the term ordering $\mathtt{Ord}(V)$ on the monoid $\mathbb{T}(x_0, x_1, x_2, x_3)$, where $V = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$, and let $\ell \in \overline{P}$ be a linear form with randomly chosen coefficients. Using CoCoA, check that we have $\mathrm{gin}_\sigma(J/\ell J) \neq I$.

Tutorial 87: SuperG Bases

Super Great Spaghetti.
This is definitely not gourmet.
It's just really good.
(Shirley Corriher)

Are you getting tired of Gröbner bases? What about *superG bases*? This is definitely not a piece of extravaganza. It's just really cool. From Theorem 6.2.12.c we get a remarkable property of a set $\{D_\pi(t_1), \ldots, D_\pi(t_s)\}$ of distractions of terms: *every subset is a Gröbner basis.* Is this a mere curiosity or are there other sets of polynomials with this property?

Some examples spring to mind immediately. For instance, a set of terms has this property. Moreover, given a term ordering σ, every set of polynomials with pairwise coprime leading terms is a σ-Gröbner basis, and the same is true for every subset. So it is natural to look for less obvious sets of polynomials with this remarkable property. They are called superG bases and constitute the topic of this tutorial. For instance, we shall see that the set of distractions of the minimal monomial generators of a monomial ideal is a superG basis. Our goal is to find characterizations of superG bases which allow us to classify them.

Before leaping into action, we have to sound a cautionary note: although everything here is elementary Gröbner basis theory, some arguments are rather tricky and involved. If you get stuck hopelessly, you can have a peek at the paper [CR90] from which the material for this tutorial has been extracted. That said, let the feast commence!

Let K be a field, let $P = K[x_1, \ldots, x_n]$ and let σ be a term ordering on $\mathbb{T}^n$. A set of non-zero polynomials $\{f_1, \ldots, f_r\}$ is called a **superG basis** with respect to σ or a **σ-superG basis** if every subset of $\{f_1, \ldots, f_r\}$ is a σ-Gröbner basis of the ideal it generates. A set comprising one non-zero polynomial is obviously a σ-superG basis. The first interesting question is therefore when two non-zero polynomials form a σ-superG basis. We start our investigation by answering this question.

a) For $f_1, f_2 \in P \setminus \{0\}$, prove that the following conditions are equivalent.
   1) The set $\{f_1, f_2\}$ is a σ-superG basis.
   2) The set $\{f_1, f_2\}$ is a σ-Gröbner basis of the ideal (f_1, f_2).
   3) We have $\gcd(\mathrm{LT}_\sigma(f_1), \mathrm{LT}_\sigma(f_2)) = \mathrm{LT}_\sigma(\gcd(f_1, f_2))$.

   Hint: Consider the lifting of the fundamental syzygy σ_{12}.

In the following we want to generalize this characterization. For this purpose we introduce additional notation. Let $r \geq 1$, let $f_1, \ldots, f_r \in P \setminus \{0\}$, and let $S = \{i_1, \ldots, i_s\} \subseteq \{1, \ldots, r\}$. Then we denote the polynomial $\gcd(f_{i_1}, \ldots, f_{i_s})$ by $\gcd_S(f_1, \ldots, f_r)$. If S is a proper subset of $\{1, \ldots, r\}$, we let S^+ be the set of all subsets of $\{1, \ldots, r\}$ containing S and having $\#S + 1$ elements. This allows us to define

$$\mathrm{lcm}_S^+(f_1,\ldots,f_r) = \begin{cases} 1 & \text{if } S = \{1,\ldots,r\} \\ \mathrm{lcm}(\gcd_T(f_1,\ldots,f_r) \mid T \in S^+) & \text{if } S \subset \{1,\ldots,r\}. \end{cases}$$

Finally, we let $\mathrm{fac}_S(f_1,\ldots,f_r) = \frac{\gcd_S(f_1,\ldots,f_r)}{\mathrm{lcm}_S^+(f_1,\ldots,f_r)}$. These constructions have a number of super great properties.

b) Show that the following conditions are equivalent.
   1) The set $\{f_1,\ldots,f_r\}$ is a σ-superG basis.
   2) For $1 \le i < j \le r$, we have $\gcd(\mathrm{LT}_\sigma(f_i), \mathrm{LT}_\sigma(f_j)) = \mathrm{LT}_\sigma(\gcd(f_i,f_j))$.
   3) For every $S \subseteq \{1,\ldots,r\}$, we have $\gcd_S(\mathrm{LT}_\sigma(f_1),\ldots,\mathrm{LT}_\sigma(f_r)) = \mathrm{LT}_\sigma(\gcd_S(f_1,\ldots,f_r))$.

   Hint: Use a) and induction on r. For "2)⇒3)", prove that it suffices to show that $\gcd(f_1,\ldots,f_r) = 1$ implies $t = \gcd(\mathrm{LT}_\sigma(f_1),\ldots,\mathrm{LT}_\sigma(f_r)) = 1$. Then use the inductive hypothesis and 2) to get $t^2 \mid \mathrm{LT}_\sigma(f_i)$.

c) Let K be infinite, let $\pi = (\pi_1,\ldots,\pi_n)$ be a tuple of sequences of pairwise distinct elements of K, let $I \subset P$ be a proper monomial ideal, and let $\{t_1,\ldots,t_s\}$ be the minimal monomial system of generators of I. Using b), prove that $\{D_\pi(t_1),\ldots,D_\pi(t_s)\}$ is a σ-superG basis for every term ordering σ on $\mathbb{T}^n$.

d) Write a CoCoA function `CheckSuperG(...)` which takes a list of non-zero polynomials, checks whether they form a superG basis with respect to the current term ordering, and returns the corresponding Boolean value. Using distractions and other examples, demonstrate the correctness of your function.

In the next part of this tutorial we want to derive a second characterization of superG bases. It will enable us to construct all σ-superG bases having a given tuple of leading terms.

e) Prove that $\mathrm{fac}_S(f_1,\ldots,f_r) \in P$ for every $S \subseteq \{1,\ldots,r\}$.

f) Let $S_1, S_2 \subset \{1,\ldots,r\}$ be such that $S_1 \not\subset S_2$ and $S_2 \not\subset S_1$. Show that $\mathrm{fac}_{S_1}(f_1,\ldots,f_r)$ and $\mathrm{fac}_{S_2}(f_1,\ldots,f_r)$ are coprime.
   Hint: For a common divisor g, prove that g divides $\gcd_{S_1\cup S_2}(f_1,\ldots,f_r)$ and g^2 divides $\gcd_{S_i}(f_1,\ldots,f_r)$.

g) For $S \subseteq \{1,\ldots,r\}$, show that $\mathrm{lcm}_S^+(f_1,\ldots,f_r) = \prod_{T\supset S} \mathrm{fac}_T(f_1,\ldots,f_r)$.
   Hint: Use descending induction on $\#S$. For $S \subset \{1,\ldots,r\}$, prove that $\mathrm{lcm}_S^+(f_1,\ldots,f_r) = \mathrm{lcm}(\prod_{U\supseteq T} \mathrm{fac}_U(f_1,\ldots,f_r) \mid T \in S^+)$ and use f).

h) Using g), prove that $f_i = \prod_{S\supseteq\{i\}} \mathrm{fac}_S(f_1,\ldots,f_r)$ for every $i \in \{1,\ldots,r\}$.

i) Based on the results of the preceding parts, we can now prove another characterization of superG bases. Show that the following conditions are equivalent.
   1) The set $\{f_1,\ldots,f_r\}$ is a σ-superG basis.
   2) For every $S \subseteq \{1,\ldots,r\}$, we have

$$\mathrm{LT}_\sigma(\mathrm{fac}_S(f_1,\ldots,f_r)) = \mathrm{fac}_S(\mathrm{LT}_\sigma(f_1),\ldots,\mathrm{LT}_\sigma(f_r))$$

3) For every $S \subset \{1, 2, \ldots, r\}$ there exists a polynomial $f_S \in P$ such that $\mathrm{LT}_\sigma(f_S) = \mathrm{fac}_S(\mathrm{LT}_\sigma(f_1), \ldots, \mathrm{LT}_\sigma(f_r))$ and $f_i = \prod_{S \supseteq \{i\}} f_S$.

Hint: To show that 1) implies 2), use downward induction on $\#S$ and prove the formula $\mathrm{LT}_\sigma(\mathrm{lcm}_S^+(f_1, \ldots, f_r)) = \mathrm{lcm}_S^+(\mathrm{LT}_\sigma(f_1), \ldots, \mathrm{LT}_\sigma(f_r))$. To show that 3) implies 1), prove $f_i = \prod_{S \supseteq \{i,j\}} f_S \cdot g_i$ with the help of h) and deduce that $\gcd(f_i, f_j) = \prod_{S \supseteq \{i,j\}} f_S$ for $1 \leq i < j \leq r$.

j) Let $\{f_1, \ldots, f_r\}$ be a σ-superG basis. Show that the polynomials f_S in condition 3) of part i) are given by $f_S = \mathrm{fac}_S(f_1, \ldots, f_r)$ for every $S \subset \{1, \ldots, r\}$. (*Hint:* Use descending induction on $\#S$ and g).)

The characterization of superG bases contained in i) makes it possible to classify all possible σ-superG bases having given leading terms. To explain the method, we use the following example.

k) Let $P = K[x, y, z]$ and $\sigma =$ `DegRevLex`. Describe all superG bases $\{f_1, f_2, f_3\}$ with $\mathrm{LT}_\sigma(f)_1 = x^2y$, $\mathrm{LT}_\sigma(f_2) = xz^3$, and $\mathrm{LT}_\sigma(f_3) = xy^2z$. To be able to use condition 3) of i), prove the following equations:

1) $\mathrm{fac}_{\{1,2,3\}}(\mathrm{LT}_\sigma(f_1), \mathrm{LT}_\sigma(f_2), \mathrm{LT}_\sigma(f_3)) = x$
2) $\mathrm{fac}_{\{1,2\}}(\mathrm{LT}_\sigma(f_1), \mathrm{LT}_\sigma(f_2), \mathrm{LT}_\sigma(f_3)) = 1$
3) $\mathrm{fac}_{\{1,3\}}(\mathrm{LT}_\sigma(f_1), \mathrm{LT}_\sigma(f_2), \mathrm{LT}_\sigma(f_3)) = y$
4) $\mathrm{fac}_{\{2,3\}}(\mathrm{LT}_\sigma(f_1), \mathrm{LT}_\sigma(f_2), \mathrm{LT}_\sigma(f_3)) = z$
5) $\mathrm{fac}_{\{1\}}(\mathrm{LT}_\sigma(f_1), \mathrm{LT}_\sigma(f_2), \mathrm{LT}_\sigma(f_3)) = x$
6) $\mathrm{fac}_{\{2\}}(\mathrm{LT}_\sigma(f_1), \mathrm{LT}_\sigma(f_2), \mathrm{LT}_\sigma(f_3)) = z^2$
7) $\mathrm{fac}_{\{3\}}(\mathrm{LT}_\sigma(f_1), \mathrm{LT}_\sigma(f_2), \mathrm{LT}_\sigma(f_3)) = y$

l) In $\mathbb{Q}[x, y, z]$ consider the polynomials $f_1 = (x+12345)(y+35)(x+125)$, $f_2 = (z^2+x+y)(z-1)(x+125)$, and $f_3 = (y+35)(y+6)(z-1)(x+125)$. Show that $\{f_1, f_2, f_3\}$ is a `DegRevLex`-superG basis.

m) Construct an algorithm which takes a term ordering σ on $\mathbb{T}^n$ and a tuple of terms $(t_1, \ldots, t_r)$ and returns a description of *all* σ-superG bases $\{f_1, \ldots, f_r\}$ with $\mathrm{LT}_\sigma(f_i) = t_i$ for $i = 1, \ldots, r$.
Hint: The result should be a set of elements of a larger polynomial ring which contains additional indeterminates representing the coefficients which can be chosen arbitrarily.

6.3 Finite Sets of Points

The more we learn the more primitive
our previous understanding appears,
and the more challenging
the problems become.
(Halton C. Arp)

In the 1970s and early 1980s, algebraic geometry was essentially synonymous with Grothendieck's scheme theory. Most geometers were busily developing new cohomology theories and proving vanishing theorems in them; some had never seen the equations of a non-trivial example for their theories. In this atmosphere the few hardy folks who dared to give talks about such down-to-earth topics as finite sets of points in affine or projective spaces were confronted with disinterest or even ridicule. Now, about a quarter of a century later, the tide has turned completely: finite sets of points are an active and well-respected branch of algebraic geometry. How did this change come about?

When one starts to reduce deep problems in algebraic geometry to their essential parts, it frequently turns out that at their core lies a question which has been studied for a long time, and sometimes this question is related to finite sets of points. For instance, already in the eighteenth century G. Cramer and L. Euler discussed (in their correspondence) a phenomenon which is nowadays called the *Cayley-Bacharach property* and which is dealt with in Tutorial 88. Later, in 1843, A. Cayley formulated a theorem which was a vast generalization of what Cramer and Euler had stumbled upon. But unfortunately the claim was false and the proof invalid. This was not corrected until 1886, when I. Bacharach used M. Noether's "$A\Phi + B\Psi$"-theorem to give a correct statement and a true proof. Many decades later it turned out that the Cayley-Bacharach property is connected to the "Gorenstein property" of the homogeneous coordinate ring of a projective point set, and today a generalization of this property is central to an important conjecture by D. Eisenbud, M. Green and J. Harris.

What does all of this have to do with Computational Commutative Algebra? We think that finite sets of points provide excellent examples for the ways in which computer algebra methods can be applied. They show up in many branches of mathematics besides algebraic geometry, for instance in interpolation, coding theory, and statistics. Efficient algorithms help us to compute with larger and larger point sets, to check results and conjectures, and to discover new ones. In this sense the purpose of the current section is to introduce you to some modern methods for working on a classical subject and to show you how Computational Commutative Algebra provides a unifying approach to different areas of mathematics.

The first subsection begins at the beginning. Given a field K and a finite set of points $\mathbb{X}$ in K^n, geometric properties of $\mathbb{X}$ are intrinsically related to algebraic properties of its affine coordinate ring $P/\mathcal{I}(\mathbb{X})$ where

$P = K[x_1, \ldots, x_n]$. For instance, it is a simple observation that the number of points in $\mathbb{X}$ equals the vector space dimension of $P/\mathcal{I}(\mathbb{X})$. Not quite as simple is the observation that there exist hypersurfaces passing through all points of $\mathbb{X}$ bar any one of the points. The polynomials defining these hypersurfaces are called the *separators* of $\mathbb{X}$. They can be used to solve the interpolation problem for $\mathbb{X}$ (see Proposition 6.3.6 and Exercise 1). Next we have a look at affine point sets $\mathbb{X}$ of the form $\mathbb{X} = M_1 \times \cdots \times M_n$ with finite subsets $M_i \subseteq K$ (see Proposition 6.3.8) because they are useful in statistics where they are known as *full designs* (see Tutorial 92).

Algorithmically, the main task is to compute the vanishing ideal of an affine point set from the coordinates of the points. In principle this task can be solved using the Gröbner basis methods explained in the previous chapters. In fact, we have $\mathcal{I}(\mathbb{X}) = \mathcal{I}(p_1) \cap \cdots \cap \mathcal{I}(p_s)$ for $\mathbb{X} = \{p_1, \ldots, p_s\}$. However, for larger examples this method is not efficient. A much better approach is the Buchberger-Möller Algorithm 6.3.10 which performs the task using linear algebra. Moreover, the Buchberger-Möller Algorithm can be modified to produce the separators as a by-product.

In geometry, it is frequently advisable to embed affine varieties in projective spaces in order to gain global invariants such as Hilbert functions and graded Betti numbers. Hence we do the same for affine point sets in the second subsection. Given a projective point set $\mathbb{X} \subseteq \mathbb{P}^n_K$, its homogeneous coordinate ring $R = \overline{P}/\mathcal{I}^+(\mathbb{X})$, where $\overline{P} = K[x_0, \ldots, x_n]$, contains a lot of information about the geometry of $\mathbb{X}$. It is a standard graded, 1-dimensional K-algebra whose multiplicity is the number of points in $\mathbb{X}$ (see Proposition 6.3.21). After possibly enlarging the base field K and performing a homogeneous linear change of coordinates, we may assume that x_0 is a non-zero divisor for R. Geometrically, this means that no point of $\mathbb{X}$ lies on the hyperplane at infinity. Algebraically, it can be expressed by saying that R is a Cohen-Macaulay ring. The Hilbert function and the regularity index of R are further data encoding certain aspects of the geometry of $\mathbb{X}$ (see Proposition 6.3.23 and Tutorial 88).

Thus it is important to be able to compute the homogeneous vanishing ideal of a projective point set from given coordinate tuples of the individual points. One way to do this would be to pass to the situation when there is no point of $\mathbb{X}$ on the hyperplane at infinity, compute the vanishing ideal of the corresponding affine point set using the Buchberger-Möller Algorithm, and homogenize the result. But for several reasons it is more useful to adapt the Buchberger-Möller technique directly to the projective setting by performing the computation degree-by-degree (see Theorem 6.3.24).

Finally, we use the theory developed in Section 5.5 to classify the possible Hilbert functions of projective point sets in the third subsection, and we invite you to study the graded Betti numbers of generic sets of points in Tutorial 89. Besides the applications of the theory of finite sets of points to interpolation and to statistics mentioned already, we present an application

to coding theory in Tutorial 90. It is clear that this section contains only the first steps of a long journey. But if you follow it attentively, you will be ready to start exploring some challenging problems of current interest on your own.

6.3.A Affine Point Sets

After having established
Lemmas A, B, and C,
we get a D. Lemma.
(Michael Möller)

Let K be a field, let $n \geq 1$, and let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over K. Recall that, given a field extension $K \subseteq L$ and a subset $S \subseteq L^n$, we defined the vanishing ideal $\mathcal{I}(S) \subseteq P$ of S by

$$\mathcal{I}(S) = \{f \in P \mid f(c_1, \ldots, c_n) = 0 \text{ for all } (c_1, \ldots, c_n) \in S\}$$

In this subsection we want to examine the following special case of this definition.

Definition 6.3.1. Let K be a field and $P = K[x_1, \ldots, x_n]$.

a) An element $p = (c_1, \ldots, c_n)$ of K^n is also called a **K-rational point**. The numbers $c_1, \ldots, c_n \in K$ are called the **coordinates** of p.
b) A finite set $\mathbb{X} = \{p_1, \ldots, p_s\}$ of distinct K-rational points $p_1, \ldots, p_s \in K^n$ is called an **affine point set**.
c) The vanishing ideal $\mathcal{I}(\mathbb{X}) \subseteq P$ of an affine point set $\mathbb{X} \subseteq K^n$ is called an **ideal of points**.
d) The K-algebra $P/\mathcal{I}(\mathbb{X})$ is called the **(affine) coordinate ring** of $\mathbb{X}$.

The simplest case of an affine point set is a single K-rational point.

Example 6.3.2. Let $p = (c_1, \ldots, c_n) \in K^n$ be a K-rational point and $\mathbb{X} = \{p\}$. By Proposition 3.6.1.a, the vanishing ideal of $\mathbb{X}$ is given by the ideal $\mathcal{I}(\mathbb{X}) = (x_1 - c_1, \ldots, x_n - c_n) \subseteq P$.

In the following, we let $p_i = (c_{i1}, \ldots, c_{in}) \in K^n$ with $c_{ij} \in K$ for $i = 1, \ldots, s$ and $j = 1, \ldots, n$, and we let $\mathbb{X}$ be the affine point set $\mathbb{X} = \{p_1, \ldots, p_s\}$. In the next proposition we collect some basic properties of the vanishing ideal of $\mathbb{X}$.

Proposition 6.3.3. (Basic Properties of Ideals of Points)
Let $\mathbb{X} = \{p_1, \ldots, p_s\}$ be an affine point set as above.

a) We have $\mathcal{I}(\mathbb{X}) = \mathcal{I}(p_1) \cap \cdots \cap \mathcal{I}(p_s)$.
b) The map $\varphi : P/\mathcal{I}(\mathbb{X}) \longrightarrow K^s$ defined by $\varphi(f + \mathcal{I}(\mathbb{X})) = (f(p_1), \ldots, f(p_s))$ is an isomorphism of K-algebras. In particular, the ideal $\mathcal{I}(\mathbb{X})$ is zero-dimensional.

c) *For any term ordering* σ *on* $\mathbb{T}^n$, *the set* $\mathbb{T}^n \setminus \mathrm{LT}_\sigma\{I(\mathbb{X})\}$ *consists of precisely* s *terms.*

Proof. To prove a), it is sufficient to note that a polynomial f is in $\mathcal{I}(\mathbb{X})$ if and only if it vanishes at every point p_i with $1 \leq i \leq s$. The proof of b) follows by combining a), the Chinese Remainder Theorem 3.7.4, and the isomorphisms $P/\mathcal{I}(p_i) \cong K$ given by $f + \mathcal{I}(p_i) \mapsto f(p_i)$. Finally, claim c) follows from b) and Macaulay's Basis Theorem 1.5.7. □

Clearly, the formula $\mathcal{I}(\mathbb{X}) = \mathcal{I}(p_1) \cap \cdots \cap \mathcal{I}(p_s)$ can be used together with the algorithms of Section 3.2.A to compute a system of generators of $\mathcal{I}(\mathbb{X})$ if the coordinates of $p_1, \ldots, p_s$ are given. However, this method is not efficient for large sets of points (i.e. when $s \gg 0$) because the necessary Gröbner basis computations become very demanding. A much more efficient method will be discussed below. Not every zero-dimensional ideal in P is an ideal of points, as our next example shows.

Example 6.3.4. Let I be the ideal generated by $f = x^2 + 1$ in $P = \mathbb{Q}[x]$. Then I is zero-dimensional, but there is no affine point set $\mathbb{X} \subseteq \mathbb{Q}$ such that $I = \mathcal{I}(\mathbb{X})$. The reason is that the polynomial $f \in I$ does not vanish at any point of $\mathbb{Q}$.

Given an affine point set $\mathbb{X}$, the polynomials in $\mathcal{I}(\mathbb{X})$ are not the only interesting ones. If we want to perform polynomial interpolation, we also need to know the following polynomials.

Definition 6.3.5. Let $\mathbb{X} = \{p_1, \ldots, p_s\} \subseteq K^n$ be an affine point set, and let $\mathcal{X}$ be the tuple $(p_1, \ldots, p_s)$.

a) Let $i \in \{1, \ldots, s\}$. A polynomial $f \in P$ is called a **separator** of p_i from $\mathbb{X} \setminus p_i$ if $f(p_i) = 1$ and $f(p_j) = 0$ for $j \neq i$.
b) Let $a_1, \ldots, a_s \in K$. A polynomial $f \in P$ is called an **interpolator** for the tuple $(a_1, \ldots, a_s)$ at $\mathcal{X}$ if $f(p_i) = a_i$ for $i = 1, \ldots, s$.

It is clear that separators and interpolators are not unique. Two separators of p_i and two interpolators for a tuple $(a_1, \ldots, a_s) \in K^s$ differ by an element of $\mathcal{I}(\mathbb{X})$. What is not so clear at this point is whether separators and interpolators always exist. Our next proposition gives an affirmative answer.

Proposition 6.3.6. *Let* $\mathbb{X} = \{p_1, \ldots, p_s\} \subseteq K^n$ *be an affine point set, and let* $\mathcal{X}$ *be the tuple* $(p_1, \ldots, p_s)$.

a) *For every* $i \in \{1, \ldots, s\}$, *there exists a separator of* p_i *from* $\mathbb{X} \setminus p_i$.
b) *For every* $(a_1, \ldots, a_s) \in K^s$, *there exists an interpolator for* $(a_1, \ldots, a_s)$ *at* $\mathcal{X}$.
c) *Let* $\mathbb{Y}$ *be an affine point set contained in* $\mathbb{X}$. *For every* $p_i \in \mathbb{X}$, *let* $f_i \in P$ *be a separator of* p_i *from* $\mathbb{X} \setminus p_i$, *and let* $f_{\mathbb{X}\setminus\mathbb{Y}} = \sum_{p_i \in \mathbb{X}\setminus\mathbb{Y}} f_i$. *Then we have* $\mathcal{I}(\mathbb{Y}) = \mathcal{I}(\mathbb{X}) + (f_{\mathbb{X}\setminus\mathbb{Y}})$.

Proof. Parts a) and b) follow from Proposition 6.3.3.b by taking suitable preimages under the map φ. To prove c), it suffices to show the inclusion "$\subseteq$", because the reverse inclusion is obviously true. Let $f \in \mathcal{I}(\mathbb{Y})$. Since we have $(1 - f_{\mathbb{X}\setminus\mathbb{Y}})(p_i) = 0$ for all i such that $p_i \in \mathbb{X} \setminus \mathbb{Y}$, we see that $f(1 - f_{\mathbb{X}\setminus\mathbb{Y}}) \in \mathcal{I}(\mathbb{X})$, and therefore $f \in \mathcal{I}(\mathbb{X}) + (f_{\mathbb{X}\setminus\mathbb{Y}})$. □

An efficient method for computing separators will be presented below. If we know the separators $f_1, \ldots, f_s$ of $p_1, \ldots, p_s$, respectively, we can produce an interpolator f for $(a_1, \ldots, a_s) \in K^s$ by setting $f = \sum_{i=1}^{s} a_i f_i$.

Our next topic is the connection between affine point sets and distractions. The following definition originated in statistics (see Tutorial 92).

Definition 6.3.7. Let $M_1, \ldots, M_n$ be finite subsets of K. Then the affine point set $\mathbb{X} = M_1 \times \cdots \times M_n \subseteq K^n$ is called the **full design** on $(M_1, \ldots, M_n)$.

The vanishing ideal of a full design is a special case of a distraction, as our next proposition shows.

Proposition 6.3.8. *For $i = 1, \ldots, n$, let $r_i \geq 1$, and let $M_i = \{a_{i1}, \ldots, a_{ir_i}\}$ be a subset of the field K consisting of r_i distinct elements. Furthermore, let $\mathbb{X} = M_1 \times \cdots \times M_n$ be the full design on $(M_1, \ldots, M_n)$.*

a) The vanishing ideal of $\mathbb{X}$ is given by $\mathcal{I}(\mathbb{X}) = (f_1, \ldots, f_n)$ where we let $f_i = \prod_{j=1}^{r_i}(x_j - a_{ij})$ for $i = 1, \ldots, n$.

b) Let $\pi = (\pi_1, \ldots, \pi_n)$ where π_i is a sequence of distinct elements of the field K starting with $\pi_i = (a_{i1}, a_{i2}, \ldots, a_{ir_i}, \ldots)$. Then we have

$$\mathcal{I}(\mathbb{X}) = (D_\pi(x_1^{r_1}), \ldots, D_\pi(x_n^{r_n}))$$

In particular, the set $\mathbb{X}$ is the set of zeros of a distraction.

c) For every term ordering σ, the set $\{f_1, \ldots, f_n\}$ is the reduced σ-Gröbner basis of $\mathcal{I}(\mathbb{X})$.

d) For every affine point set $\mathbb{Y}$, there is a unique minimal full design containing $\mathbb{Y}$.

Proof. Claim a) follows from Theorem 6.2.8 and Proposition 6.3.3.a. Claim b) follows from the definition of the distraction $D_\pi(x_i^{r_i})$. Claim c) follows from b) and Theorem 6.2.12.c. It remains to prove d). For $i = 1, \ldots, n$, we let M_i be the set of i^{th} coordinates of the points of $\mathbb{Y}$. Then the full design $\mathbb{X} = M_1 \times \cdots \times M_n$ contains $\mathbb{Y}$. Clearly, every full design containing $\mathbb{Y}$ has to contain $\mathbb{X}$. Hence $\mathbb{X}$ is the unique minimal full design containing $\mathbb{Y}$. □

Corollary 6.3.9. *The vanishing ideal of an affine point set in K^n has a system of generators consisting of $n + 1$ polynomials.*

Proof. Let $\mathbb{Y}$ be an affine point set, and let $\mathbb{X}$ be the unique minimal full design containing $\mathbb{X}$. By part a) of the proposition, the ideal $\mathcal{I}(\mathbb{X})$ is generated by n polynomials. Now the claim follows from Propositon 6.3.6.c. □

In our quest to study affine point sets, one task is still ahead of us: we need a more efficient way to compute their vanishing ideals than the one which follows from Proposition 6.3.3.a. Our next theorem can be used to show that this task can be solved in a number of steps which depends polynomially on n and s. If you try out an implementation of this algorithm (for instance the one in CoCoA), you will see immediately how much faster it is than computing the intersections in Proposition 6.3.3.a.

Before presenting this algorithm, we note that we represent evaluation vectors as rows of a matrix instead of putting them into the columns. The reason is that we want to simplify the matrix by using row reductions. Let us explain briefly what this means. The most important aspect is that an ordering must be imposed on the columns of the matrix: the most natural is left-to-right, and by permuting the columns we may assume that this is indeed the chosen ordering. In a matrix $\mathcal{M}$ we say that a row whose first non-zero element occurs in column c is a **reducer** for column c; a zero row is not a reducer for any column. In the algorithm below, the matrix $\mathcal{M}$ is constructed so that every row is a reducer, and no column has more than one associated reducer. A row vector may then be reduced against $\mathcal{M}$ by repeatedly subtracting suitable multiples of the reducers in $\mathcal{M}$ to eliminate the first non-zero element in the vector. The process ends when the vector becomes zero or when there is no reducer in $\mathcal{M}$ for the column in which the first non-zero entry lies.

Theorem 6.3.10. (The Buchberger-Möller Algorithm)
Let σ be a term ordering on $\mathbb{T}^n$, and let $\mathbb{X} = \{p_1, \ldots, p_s\}$ be an affine point set in K^n whose points $p_i = (c_{i1}, \ldots, c_{in})$ are given via their coordinates $c_{ij} \in K$. Consider the following sequence of instructions.

1) *Let $\mathcal{G} = \emptyset$, $O = \emptyset$, $\mathcal{S} = \emptyset$, $L = \{1\}$, and let $\mathcal{M} = (m_{ij}) \in \mathrm{Mat}_{0,s}(K)$ be a matrix having s columns and initially zero rows.*
2) *If $L = \emptyset$, return the pair $(\mathcal{G}, O)$ and stop. Otherwise, choose the term $t = \min_\sigma(L)$ and delete it from L.*
3) *Compute the evaluation vector $(t(p_1), \ldots, t(p_s)) \in K^s$ and reduce it against the rows of $\mathcal{M}$ to obtain*

$$(v_1, \ldots, v_s) = (t(p_1), \ldots, t(p_s)) - \sum_i a_i \, (m_{i1}, \ldots, m_{is})$$

with $a_i \in K$.
4) *If $(v_1, \ldots, v_s) = (0, \ldots, 0)$ then append the polynomial $t - \sum_i a_i s_i$ to $\mathcal{G}$ where s_i is the i^{th} element in $\mathcal{S}$. Remove from L all multiples of t. Then continue with step 2).*
5) *Otherwise $(v_1, \ldots, v_s) \neq (0, \ldots, 0)$, so append $(v_1, \ldots, v_s)$ as a new row to $\mathcal{M}$ and $t - \sum_i a_i s_i$ as a new element to $\mathcal{S}$. Add t to O, and add to L those elements of $\{x_1 t, \ldots, x_n t\}$ which are neither multiples of an element of L nor of $\mathrm{LT}_\sigma(\mathcal{G})$. Continue with step 2).*

This is an algorithm which returns a pair $(\mathcal{G}, O)$ *such that* $\mathcal{G}$ *is the reduced* σ*-Gröbner basis of* $\mathcal{I}(\mathbb{X})$ *and* $O = \mathbb{T}^n \setminus \mathrm{LT}_\sigma\{\mathcal{I}(\mathbb{X})\}$.

Proof. First we exhibit termination. In each iteration either step 4) is performed or step 5). By its construction, the matrix $\mathcal{M}$ always has linearly independent rows. Hence step 5), which adjoins a row to $\mathcal{M}$, can be performed at most s times. Since the set L is enlarged only in step 5) and each iteration removes one element of L, we arrive at $L = \emptyset$ after finitely many iterations.

To prove correctness, we let $\mathcal{G}'$ be the reduced σ-Gröbner basis of $\mathcal{I}(\mathbb{X})$ and $O' = \mathbb{T}^n \setminus \mathrm{LT}_\sigma\{\mathcal{I}(\mathbb{X})\}$. Then we simultaneously prove the following three claims by induction on the number of iterations of the algorithm: after steps 2)–5) have been performed for some term t, the tuple $\mathcal{G}$ consists of the elements g in $\mathcal{G}'$ such that $\mathrm{LT}_\sigma(g) \leq_\sigma t$, we have $O = \{t' \in O' \mid t' \leq_\sigma t\}$, and if there exists a term $t' \in \mathbb{T}^n \setminus \mathrm{LT}_\sigma\{\mathcal{I}(\mathbb{X})\}$ with $t' >_\sigma t$ then $\min_\sigma(L)$ is the smallest such term.

This is clearly true after zero iterations, i.e. after step 1) has been executed. Now let us follow the steps of one iteration. If step 4) is performed, i.e. if $(v_1, \ldots, v_s) = (0, \ldots, 0)$, then the polynomial $t - \sum_i a_i s_i$ is contained in $\mathcal{I}(\mathbb{X})$ because we see inductively that the i^{th} row of $\mathcal{M}$ is the evaluation vector of s_i. Moreover, by construction of $\mathcal{S}$, the terms in the support of s_i are all smaller than t with respect to σ and contained in O. Thus $t = \mathrm{LT}_\sigma(t - \sum_i a_i s_i)$ is of the form $t = t' \,\mathrm{LT}_\sigma(g)$ for some $t' \in \mathbb{T}^n$ and an element g of $\mathcal{G}'$. By step 5), no element of $\mathrm{LT}_\sigma(\mathcal{G})$ divides t. Therefore the inductive hypothesis implies $t' = 1$. Hence $t - \sum_i a_i s_i$ is an element of $\mathcal{G}'$ and $\mathcal{G}$ is still correct after this iteration.

Next, we suppose that $(v_1, \ldots, v_s) \neq (0, \ldots, 0)$. In order to show $t \in O'$, we argue by contradiction and assume $t = t' \,\mathrm{LT}_\sigma(g)$ for some $t' \in \mathbb{T}^n$ and g in $\mathcal{G}'$. Again, the definition of L implies $t' = 1$. Thus g is of the form $g = t - \sum_j b_j t_j$ with $b_j \in K$ and $t_j \in O'$. The inductive hypothesis yields $t_j \in O$. Hence the fact that the evaluation vector of g is zero implies that $(t(p_1), \ldots, t(p_s))$ is a linear combination of the rows of $\mathcal{M}$, a contradiction. Consequently, we have $t \in O'$, and the set O is still correct after this iteration.

Finally, we show the third claim. If $\{t' \in \mathbb{T}^n \setminus \mathrm{LT}_\sigma\{\mathcal{I}(\mathbb{X})\} \mid t' >_\sigma t\}$ is not empty, its smallest term $\tilde{t}$ with respect to σ is clearly contained in $L \cup \{x_1 t, \ldots, x_n t\}$. Moreover, the term $\tilde{t}$ is not a multiple of a term in $\mathrm{LT}_\sigma(\mathcal{G})$ because those terms are contained in $\mathrm{LT}_\sigma(\mathcal{I}(\mathbb{X}))$ by the inductive hypothesis. Altogether, it follows that $\tilde{t} = \min_\sigma(L)$, as we wanted to show.

At the end of the algorithm, i.e. when $L = \emptyset$, we therefore have $\mathcal{G} = \mathcal{G}'$ and $O = O'$ and correctness is proved. □

A small alteration of this algorithm allows us to compute the separators of $\mathbb{X}$ as well.

Corollary 6.3.11. *In the setting of the theorem, replace step 2) by the following instruction.*

2') If $L = \emptyset$ then row reduce $\mathcal{M}$ to a diagonal matrix and mimic these row operations on the elements of $\mathcal{S}$ (considered as a column vector). Next replace $\mathcal{S}$ by $\mathcal{M}^{-1}\mathcal{S}$, return the triple $(\mathcal{G}, O, \mathcal{S})$, and stop. If $L \neq \emptyset$, choose the term $t = \min_\sigma(L)$ and delete it from L.

The resulting sequence of instructions defines again an algorithm. It returns a triple $(\mathcal{G}, O, \mathcal{S})$ such that $\mathcal{G}$ is the reduced σ-Gröbner basis of $\mathcal{I}(\mathbb{X})$, such that $O = \mathbb{T}^n \setminus \mathrm{LT}_\sigma\{\mathcal{I}(\mathbb{X})\}$, and the tuple $\mathcal{S}$ contains the separators of p_i from $\mathbb{X} \setminus p_i$ for $i = 1, \ldots, s$.

Proof. Throughout the course of the algorithm, the rows of the matrix $\mathcal{M}$ are the evaluation vectors $(s_i(p_1), \ldots, s_i(p_s))$ of the polynomials in $\mathcal{S}$. At the end of the algorithm, i.e. when $L = \emptyset$, the set O contains s terms. Hence step 5) shows that at this point $\mathcal{M}$ is an upper triangular matrix of size $s \times s$. When we diagonalize $\mathcal{M}$ and mimic the necessary row operations on $\mathcal{S}$, we get a tuple $\mathcal{S}$ whose elements satisfy $s_i(p_j) = 0$ for $i \neq j$ and $m_{ii} = s_i(p_i) \neq 0$. Consequently, the elements of $\mathcal{M}^{-1}\mathcal{S}$ are the separators of p_i from $\mathbb{X} \setminus p_i$ for $i = 1, \ldots, s$. □

Although it is already very efficient, the Buchberger-Möller algorithm can be improved further. Let us point out some possibilities.

Remark 6.3.12. Assume that we are in the setting of the theorem.

a) In step 2), the term t is either 1 or of the form $t = x_i t'$ for some term $t' \in O$. In the latter case we can compute the evaluation vector $(t(p_1), \ldots, t(p_s))$ in step 3) more efficiently by storing the evaluation vector of t' and multiplying it componentwise by $(x_i(p_1), \ldots, x_i(p_s)) = (c_{1i}, \ldots, c_{si})$.
b) If the base field K is the field of rational numbers, the entries of $\mathcal{M}$ grow quickly when we increase the number of points. In this case we can speed up the algorithm by computing the Gröbner basis $\mathcal{G}$ of $\mathcal{I}(\mathbb{X})$ modulo several primes and recombining the results with the help of the Chinese Remainder Theorem 3.7.4. The details of this *modular version* of the Buchberger-Möller algorithm are contained in [Ab00].

For small affine point sets, we can use the Buchberger-Möller algorithm to calculate the vanishing ideal by hand.

Example 6.3.13. Let $\mathbb{X}$ be the affine point set in $\mathbb{A}^2_{\mathbb{Q}}$ consisting of the five points $p_1 = (0,0)$, $p_2 = (0,-1)$, $p_3 = (1,0)$, $p_4 = (1,1)$, and $p_5 = (-1,1)$, and let $\sigma = \texttt{DegLex}$. We compute $\mathcal{I}(\mathbb{X})$ and follow the steps of the algorithm.

1) Let $\mathcal{G} = \emptyset$, $O = \emptyset$, $\mathcal{S} = \emptyset$, and $L = \{1\}$.
2) Choose $t = 1$ and let $L = \emptyset$.
3) Compute $(t(p_1), \ldots, t(p_5)) = (1,1,1,1,1) = (v_1, \ldots, v_5)$.

5) Let $\mathcal{M} = (1\ 1\ 1\ 1\ 1)$, $\mathcal{S} = (1)$, $O = \{1\}$, and $L = \{y, x\}$.
2) Choose $t = y$ and let $L = \{x\}$.
3) Compute $(t(p_1), \ldots, t(p_5)) = (0, -1, 0, 1, 1) = (v_1, \ldots, v_5)$.
5) Let $\mathcal{M} = \left(\begin{smallmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & -1 & 0 & 1 & 1 \end{smallmatrix}\right)$, $\mathcal{S} = (1, y)$, $O = \{1, y\}$, and $L = \{x, y^2\}$.
2) Choose $t = x$ and let $L = \{y^2\}$.
3) Compute $(t(p_1), \ldots, t(p_5)) = (0, 0, 1, 1, -1) = (v_1, \ldots, v_5)$.
5) Let $\mathcal{M} = \left(\begin{smallmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & -1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & -1 \end{smallmatrix}\right)$, $\mathcal{S} = (1, y, x)$, $O = \{1, y, x\}$, and $L = \{y^2, xy, x^2\}$.
2) Choose $t = y^2$ and let $L = \{xy, x^2\}$.
3) Compute $(t(p_1), \ldots, t(p_5)) = (0, 1, 0, 1, 1)$ and reduce it against the rows of $\mathcal{M}$ to obtain $(v_1, \ldots, v_5) = (0, 1, 0, 1, 1) + (0, -1, 0, 1, 1) = (0, 0, 0, 2, 2)$.
5) Let $\mathcal{M} = \left(\begin{smallmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & -1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 2 & 2 \end{smallmatrix}\right)$, $\mathcal{S} = (1, y, x, y^2 + y)$, $O = \{1, y, x, y^2\}$, and $L = \{xy, x^2, y^3\}$.
2) Choose $t = xy$ and let $L = \{x^2, y^3\}$.
3) Compute $(t(p_1), \ldots, t(p_5)) = (0, 0, 0, 1, -1)$ and reduce it against the rows of $\mathcal{M}$ to obtain $(v_1, \ldots, v_5) = (0, 0, 0, 0, 2)$.
5) Let $\mathcal{M} = \left(\begin{smallmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & -1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 2 \end{smallmatrix}\right)$, $\mathcal{S} = (1,\ y,\ x,\ y^2 + y, xy - \frac{1}{2}y^2 - \frac{1}{2}y)$, $O = \{1, y, x, y^2, xy\}$, and $L = \{x^2, y^3, xy^2\}$.
2) Choose $t = x^2$ and let $L = \{y^3, xy^2\}$.
3) Compute $(t(p_1), \ldots, t(p_5)) = (0, 0, 1, 1, 1)$ and $(v_1, \ldots, v_5) = (0, \ldots, 0)$.
4) Let $\mathcal{G} = (x^2 + xy - \frac{1}{2}y^2 - x - \frac{1}{2}y)$ and $L = \{y^3, xy^2\}$.
2) Choose $t = y^3$ and let $L = \{xy^2\}$.
3) Compute $(t(p_1), \ldots, t(p_5)) = (0, -1, 0, 1, 1)$ and $(v_1, \ldots, v_5) = (0, \ldots, 0)$.
4) Let $\mathcal{G} = (x^2 + xy - \frac{1}{2}y^2 - x - \frac{1}{2}y,\ y^3 - y)$ and $L = \{xy^2\}$.
2) Choose $t = xy^2$ and let $L = \emptyset$.
3) Compute $(t(p_1), \ldots, t(p_5)) = (0, 0, 0, 1, -1)$ and $(v_1, \ldots, v_5) = (0, \ldots, 0)$.
4) Let $\mathcal{G} = (x^2 + xy - \frac{1}{2}y^2 - x - \frac{1}{2}y,\ y^3 - y,\ xy^2 - xy)$ and $L = \emptyset$.
2) Return $(\mathcal{G}, O)$ and stop.

The result of this computation is that $\mathcal{G} = (x^2 + xy - \frac{1}{2}y^2 - x - \frac{1}{2}y,\ y^3 - y,\ xy^2 - xy)$ is the reduced σ-Gröbner basis of $\mathcal{I}(\mathbb{X})$ and $O = \{1, x, y, xy, y^2\}$ represents a $\mathbb{Q}$-basis of $\mathbb{Q}[x, y]/\mathcal{I}(\mathbb{X})$.

6.3.B Projective Point Sets

The shortest distance between two points
is under construction.
(Noelie Altile)

In Tutorial 35 we introduced projective spaces, and in Tutorials 46 and 52 we studied some of their properties. Since the topics of this subsection are projective point sets, their homogeneous vanishing ideals and their Hilbert functions, we shall recall some of the main definitions. Let K be a field, and

let $P = K[x_1, \ldots, x_n]$ and $\overline{P} = K[x_0, \ldots, x_n]$ be standard graded polynomial rings over K.

Definition 6.3.14. For $n \geq 0$, we define an equivalence relation $\sim$ on $K^{n+1} \setminus \{0\}$ by letting $(c_0, \ldots, c_n) \sim (c'_0, \ldots, c'_n)$ if and only if there exists an element $\lambda \in K$ such that $(c'_0, \ldots, c'_n) = (\lambda c_0, \ldots, \lambda c_n)$.

a) The set of equivalence classes $\mathbb{P}^n_K = (K^{n+1} \setminus \{0\})/\sim$ with respect to $\sim$ is called the **n-dimensional projective space** over K.
b) The equivalence class p of a tuple $(c_0, \ldots, c_n) \in K^{n+1} \setminus \{0\}$ is called a **(projective) point** in $\mathbb{P}^n_K$. We denote it by $p = (c_0 : c_1 : \ldots : c_n)$.
c) A finite set of distinct points $\mathbb{X} = \{p_1, \ldots, p_s\} \subseteq \mathbb{P}^n_K$ is called a **projective point set**.
d) Given a projective point set $\mathbb{X} = \{p_1, \ldots, p_s\} \subseteq \mathbb{P}^n_K$, the homogeneous ideal

$$\mathcal{I}^+(\mathbb{X}) = (f \in \overline{P} \mid f \text{ homogeneous}, f(p_1) = \cdots = f(p_s) = 0) \subseteq \overline{P}$$

is called the **homogeneous vanishing ideal** of $\mathbb{X}$, and the graded K-algebra $\overline{P}/\mathcal{I}^+(\mathbb{X})$ is called the **homogeneous coordinate ring** of $\mathbb{X}$.

Notice that the homogeneous vanishing ideal of a projective point set is well-defined, because if $p = (c_0 : \ldots : c_n) = (\lambda c_0 : \ldots : \lambda c_n)$ are two coordinate tuples representing the same projective point, then $f(c_0, \ldots, c_n) = 0$ implies $f(\lambda c_0, \ldots, \lambda c_n) = \lambda^d f(c_0, \ldots, c_n) = 0$ for every $f \in \overline{P}_d$. Moreover, it is a radical ideal, since $f^i(c_0, \ldots, c_n) = 0$ for some $i \geq 1$ implies $f(c_0, \ldots, c_n) = 0$. Clearly, we have $\mathcal{I}^+(\mathbb{X}) = \bigcap_{i=1}^s \mathcal{I}^+(\{p_i\})$. Our next remark collects some relations between affine and projective point sets which are special cases of the material discussed in Tutorial 52.

Remark 6.3.15. Let $\mathbb{X} \subseteq \mathbb{P}^n_K$ be a projective point set.

a) For every $i \in \{0, \ldots, n\}$, there exists an injective map $\imath_i : \mathbb{A}^n_K \longrightarrow \mathbb{P}^n_K$ given by $(c_1, \ldots, c_n) \mapsto (c_1 : \cdots : c_i : 1 : c_{i+1} : \cdots : c_n)$. The images of $\imath_0, \ldots, \imath_n$ cover $\mathbb{P}^n_K$.
b) The set $\mathbb{X} \cap \imath_0(\mathbb{A}^n_K)$ is called the **affine part** of $\mathbb{X}$. We shall identify it with its preimage $\mathbb{X}^a = \imath_0^{-1}(\mathbb{X} \cap \imath_0(\mathbb{A}^n_K))$ in $\mathbb{A}^n_K$. Clearly, the set $\mathbb{X}^a$ is an affine point set.
c) The set $H^{\inf} = \mathcal{Z}^+(x_0) = \{(c_0 : \cdots : c_n) \in \mathbb{P}^n_K \mid c_0 = 0\}$ is called the **hyperplane at infinity** of $\mathbb{P}^n_K$. The n-dimensional projective space is the disjoint union of its affine part $\imath_0(\mathbb{A}^n_K)$ and the hyperplane at infinity. The map $H^{\inf} \longrightarrow \mathbb{P}^{n-1}_K$ given by $(0 : c_1 : \ldots : c_n) \mapsto (c_1 : \ldots : c_n)$ is well-defined and bijective.
d) The projective point set $\mathbb{X}^{\inf} = \mathbb{X} \cap H^{\inf}$ is called the set of **points at infinity** of $\mathbb{X}$. The set $\mathbb{X}$ is the disjoint union of its affine part and its set of points at infinity.

The following proposition explains the relations between the vanishing ideals of a projective point set, its affine part, and its set of points at infinity. We recall from Section 6.2 that if J is an ideal in $\overline{P}$, then $J^{\inf} = (F(0, x_1, \ldots, x_n) \mid F \in J)$.

Proposition 6.3.16. *Let $\mathbb{X} \subseteq \mathbb{P}^n_K$ be a projective point set.*

a) The vanishing ideal of the affine part of $\mathbb{X}$ is $\mathcal{I}(\mathbb{X}^a) = \mathcal{I}^+(\mathbb{X})^{\deh}$.
b) If $\mathbb{X}$ is contained in the affine part of $\mathbb{P}^n_K$ then $\mathcal{I}^+(\mathbb{X}) = \mathcal{I}(\mathbb{X}^a)^{\hom}$.
c) The vanishing ideal of the set of points at infinity of $\mathbb{X}$ is given by $\mathcal{I}^+(\mathbb{X}^{\inf}) = \sqrt{\mathcal{I}^+(\mathbb{X}) + (x_0)}$.
d) If we identify $H^{\inf}$ with $\mathbb{P}^{n-1}_K$, the homogeneous vanishing ideal of $\mathbb{X}^{\inf}$ in $\mathbb{P}^{n-1}_K$ is $\sqrt{(\mathcal{I}^+(\mathbb{X}))^{\inf}}$.

Proof. First we show the inclusion "$\subseteq$" in a). Given $f \in \mathcal{I}(\mathbb{X}^a)$, the homogeneous polynomial $x_0\, f^{\hom} \in \overline{P}$ vanishes at all points of $\mathbb{X}$. Hence we have $f = (x_0\, f^{\hom})^{\deh} \in \mathcal{I}^+(\mathbb{X})^{\deh}$. Conversely, let $F \in \mathcal{I}^+(\mathbb{X})$. We choose an arbitrary point $p = (1 : c_1 : \ldots : c_n) \in \mathbb{X}$. Then we have $F^{\deh}(c_1, \ldots, c_n) = F(1, c_1, \ldots, c_n) = 0$, and therefore $F^{\deh} \in \mathcal{I}(\mathbb{X}^a)$. This proves a).

The inclusion "$\subseteq$" in b) follows from a), since $\mathcal{I}(\mathbb{X}^a)^{\hom} = (\mathcal{I}^+(\mathbb{X})^{\deh})^{\hom}$ contains $\mathcal{I}^+(\mathbb{X})$. To prove the converse inclusion, let $f \in \mathcal{I}(\mathbb{X}^a)$ and $p = (1 : c_1 : \ldots : c_n) \in \mathbb{X} = \mathbb{X} \cap \imath_0(\mathbb{A}^n_K)$. Then $f(c_1, \ldots, c_n) = 0$ implies $f^{\hom}(1, c_1, \ldots, c_n) = 0$. Hence we obtain $f^{\hom} \in \mathcal{I}^+(\mathbb{X})$.

Next we prove c). Given a homogeneous polynomial $F \in \mathcal{I}^+(\mathbb{X}^{\inf})$, we may assume that no term in the support of F is divisible by x_0. Then we have $F = F^{\deh}$, and for large enough i there exists a polynomial $f \in P$ of degree $\deg(f) < \deg((F^{\deh})^i)$ such that $f(p) = (F^{\deh})^i(p)$ for all $p \in \mathbb{X}^a$. Hence we get $F^i - x_0^{i\deg(F)-\deg(f)} f^{\hom} \in \mathcal{I}^+(\mathbb{X})$, and thus $F \in \sqrt{\mathcal{I}^+(\mathbb{X}) + (x_0)}$. To prove the converse inclusion, we observe that $\mathcal{I}^+(\mathbb{X}) + (x_0) \subseteq \mathcal{I}^+(\mathbb{X}^{\inf})$ and that the ideal $\mathcal{I}^+(\mathbb{X}^{\inf})$ is radical.

Finally, we show d). Given a homogeneous polynomial $F \in P$ satisfying $F(p) = 0$ for all $p \in \mathbb{X}^{\inf}$, we have $F \in \sqrt{\mathcal{I}^+(\mathbb{X}) + (x_0)}$ by c). Thus there exists a number $i \geq 1$ and a homogeneous polynomial $G \in \overline{P}$ such that $F^i + x_0 G \in \mathcal{I}^+(\mathbb{X})$. By substituting $x_0 \mapsto 0$ in this relation we see that $F^i \in (\mathcal{I}^+(\mathbb{X}))^{\inf}$. Conversely, a homogeneous polynomial $F \in P$ such that $F^i \in (\mathcal{I}^+(\mathbb{X}))^{\inf}$ for some $i \geq 1$ satisfies $F^i(p) = 0$ for all $p \in \mathbb{X}$. In particular, this implies $F(p) = 0$ for all $p \in \mathbb{X}^{\inf}$. □

Parts c) and d) of this proposition are not true if we do not pass to the respective radical ideals, as the following example shows.

Example 6.3.17. Let $\mathbb{X} \subseteq \mathbb{P}^2_{\mathbb{Q}}$ be the projective point set consisting of the points $p_1 = (0 : 1 : 1)$, $p_2 = (1 : 1 : 0)$, $p_3 = (1 : 0 : 1)$, and $p_4 = (1 : 1 : 1)$. Then we have $\mathcal{I}^+(\mathbb{X}) = ((x_0 - x_1 + x_2)(x_0 - x_2),\, (x_0 - x_1 - x_2)(x_1 - x_2))$ and $\mathcal{I}^+(\mathbb{X}) + (x_0) = (x_0,\, x_1^2 - x_2^2,\, x_1 x_2 - x_2^2)$. Thus the linear polynomial $x_1 - x_2$ is contained in $\mathcal{I}^+(\mathbb{X}^{\inf}) = (x_0, x_1 - x_2)$, but not in $\mathcal{I}^+(\mathbb{X}) + (x_0)$.

Furthermore, if we identify $H^{\inf}$ with $\mathbb{P}^1_{\mathbb{Q}}$, the polynomial $x_1 - x_2$ is contained in the vanishing ideal of $\mathbb{X}^{\inf} \subseteq \mathbb{P}^1_{\mathbb{Q}}$, but not in $\mathcal{I}^+(\mathbb{X})^{\inf} = (x_1^2 - x_2^2, x_1x_2 - x_2^2)$.

The preceding proposition has several useful applications. For instance, it allows us to compute the homogeneous vanishing ideal of a projective point set contained in the affine part of $\mathbb{P}^n_K$ as follows.

Corollary 6.3.18. *Let $\mathbb{X} = \{p_1, \ldots, p_s\} \subseteq \mathbb{P}^n_K$ be a projective point set which is contained in $\imath_0(\mathbb{A}^n_K)$, let $p_i = (1 : c_{i1} : \ldots : c_{in})$ for $i = 1, \ldots, s$, and let σ be a degree compatible term ordering on $\mathbb{T}^n$. Consider the following instructions.*

1) *For $i = 1, \ldots, s$, let $p'_i = (c_{i1}, \ldots, c_{in}) \in \mathbb{A}^n_K$. Compute the reduced σ-Gröbner basis $G = \{g_1, \ldots, g_r\}$ of $\mathbb{X}^a = \{p'_1, \ldots, p'_s\}$ using the Buchberger-Möller Algorithm 6.3.10.*
2) *For $i = 1, \ldots, r$, compute the homogenization $g_i^{\hom}$ of g_i with respect to x_0.*
3) *Return $G^{\hom} = \{g_1^{\hom}, \ldots, g_r^{\hom}\}$ and stop.*

This is an algorithm which computes the reduced $\overline{\sigma}$-Gröbner basis of $\mathcal{I}^+(\mathbb{X})$, where $\overline{\sigma}$ is the extension of σ (see Definition 4.3.13).

Proof. The Buchberger-Möller algorithm returns the reduced σ-Gröbner basis G of $\mathcal{I}(\mathbb{X}^a)$. By Proposition 4.3.21, the set $G^{\hom}$ is a $\overline{\sigma}$ Gröbner basis of $\mathcal{I}(\mathbb{X}^a)^{\hom}$. In fact, it is the reduced $\overline{\sigma}$-Gröbner basis because we have $\mathrm{LT}_{\overline{\sigma}}(g_i^{\hom}) = \mathrm{LT}_{\sigma}(g_i)$ for $i = 1, \ldots, r$. Now part b) of the proposition yields the claim. □

Although it is easy to implement and reasonably efficient, the algorithm described in Corollary 6.3.18 has two drawbacks: it computes the reduced Gröbner basis of $\mathcal{I}^+(\mathbb{X})$ only with respect to very special term orderings on $\mathbb{T}(x_0, \ldots, x_n)$, and it requires that $\mathbb{X}$ is contained in the affine part of $\mathbb{P}^n_K$. The homogeneous vanishing ideal of a single projective point is easy to determine, as our next corollary shows.

Corollary 6.3.19. *Let $p = (c_0 : \ldots : c_n) \in \mathbb{P}^n_K$ be a projective point. Then its homogeneous vanishing ideal is $\mathcal{I}^+(\{p\}) = (c_ix_j - c_jx_i \mid 0 \leq i < j \leq n)$.*

Proof. Since one of the coordinates of p has to be non-zero, we may assume without loss of generality that $c_0 \neq 0$. Then we have $p = (1 : \frac{c_1}{c_0} : \ldots : \frac{c_n}{c_0})$, and the preceding corollary yields $\mathcal{I}^+(\{p\}) = (x_1 - \frac{c_1}{c_0}x_0, \ldots, x_n - \frac{c_n}{c_0}x_0) = (c_0x_i - c_ix_0 \mid 1 \leq i \leq n)$. Since we have $c_ix_j - c_jx_i = \frac{c_i}{c_0}(c_0x_j - c_jx_0) - \frac{c_j}{c_0}(c_0x_i - c_ix_0)$ for $1 \leq i < j \leq n$, the claim follows. □

Based on this corollary and the formula $\mathcal{I}^+(\mathbb{X}) = \bigcap_{i=1}^s \mathcal{I}^+(\{p_i\})$, we can develop a second method for computing the homogeneous vanishing ideal of a projective point set $\mathbb{X} = \{p_1, \ldots, p_s\} \subseteq \mathbb{P}^n_K$. It is more general than the

first one because it does not require that the point set is contained in the affine part of $\mathbb{P}^n_K$. However, as in the affine case, this method is in general quite inefficient.

A much better algorithm is described below. It is based on a thorough study of the algebraic properties of the homogeneous coordinate ring of $\mathbb{X}$. We need the following auxiliary result.

Lemma 6.3.20. *Assume that the field K has infinitely many elements. Given finitely many points $p_1, \ldots, p_s \in K^{n+1}$, there exists a linear form $\ell \in \overline{P}_1$ such that $\ell(p_i) \neq 0$ for $i = 1, \ldots, s$.*

Proof. For $i = 1, \ldots, s$, let $p_i = (c_{i0}, \ldots, c_{in})$ with $c_{ij} \in K$. A linear form $\ell = a_0x_0 + \cdots a_nx_n \in \overline{P}_1$ vanishes at the point p_i if and only if $(a_0, \ldots, a_n)$ is a zero of $c_{i0}x_0 + \cdots + c_{in}x_n$. Hence we are looking for a point $(a_0, \ldots, a_n)$ in K^{n+1} such that the polynomial $f = \prod_{i=1}^{s}(c_{i0}x_0 + \cdots + c_{in}x_n)$ does not vanish at this point. By Proposition 5.5.21.a, such a point exists. □

Proposition 6.3.21. (Coordinate Rings of Projective Point Sets) *Let $R = \overline{P}/\mathcal{I}^+(\mathbb{X})$ be the homogeneous coordinate ring of a projective point set $\mathbb{X} = \{p_1, \ldots, p_s\} \subseteq \mathbb{P}^n_K$, and for $i = 1, \ldots, s$ let $\mathfrak{p}_i$ denote the image of $\mathcal{I}^+(\{p_i\})$ in R.*

a) The ring R is a 1-dimensional standard graded K-algebra.
b) We have $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s = (0)$ and $\operatorname{Min}(R) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$.
c) The canonical R-linear map $\Phi : R \longrightarrow R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_s$ given by $r \mapsto (r + \mathfrak{p}_1, \ldots, r + \mathfrak{p}_s)$ is injective.
d) For $i = 1, \ldots, s$, there exists a homogeneous isomorphism of K-algebras $R/\mathfrak{p}_i \cong K[x_0]$.
e) Let $\ell \in \overline{P}_1$. Then we have $\mathbb{X} \cap \mathcal{Z}^+(\ell) = \emptyset$ if and only if ℓ is a non-zero divisor for R.
f) We have $\operatorname{mult}(R) = s$.

Proof. First we show a). It is clear that $R = \overline{P}/\mathcal{I}^+(\mathbb{X})$ is a standard graded K-algebra. By Proposition 5.4.5.f, the dimension of R does not change under a base field extension. Therefore we may assume that K has infinitely many elements. Then the lemma yields a linear form $\ell \in \overline{P}_1$ such that $\ell(p_i) \neq 0$ for $i = 1, \ldots, s$. After performing a linear change of coordinates, we may assume that $\ell = x_0$. Thus we have $\mathbb{X} \cap H^{\inf} = \emptyset$ and $\mathbb{X} = \imath_0(\mathbb{X}^a)$, and Proposition 6.3.16.a shows $\mathcal{I}(\mathbb{X}^a) = \mathcal{I}^+(\mathbb{X})^{\deh}$. Therefore the ring $S = R/(x_0 - 1) \cong P/\mathcal{I}^+(\mathbb{X})^{\deh}$ is the affine coordinate ring of $\mathbb{X}^a$. Since $\mathcal{I}(\mathbb{X}^a)$ is a zero-dimensional ideal, we have $\dim(S) = 0$. Now Proposition 5.6.12.c implies $\dim(R) = \dim(\overline{P}/\mathcal{I}(\mathbb{X}^a)^{\hom}) = \dim(P/\mathcal{I}(\mathbb{X}^a)) + 1 = 1$.

Now we prove b). The claim $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s = (0)$ follows from the fact that $\mathcal{I}^+(\mathbb{X}) = \mathcal{I}^+(\{p_1\}) \cap \cdots \cap \mathcal{I}^+(\{p_s\})$. To show the inclusion "$\subseteq$" in the second claim, we assume that there exists a minimal prime $\mathfrak{q} \in \operatorname{Min}(R) \setminus \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ of R. For every $i \in \{1, \ldots, s\}$, choose an element $f_i \in \mathfrak{p}_i \setminus \mathfrak{q}$. Then we have $f_1 \cdots f_s \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s = (0)$, and hence $f_1 \cdots f_s \in \mathfrak{q}$, in contradiction to

$f_i \notin \mathfrak{q}$ for $i = 1, \ldots, s$. The converse inclusion follows immediately from Lemma 5.6.14 because every prime ideal of R contains $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s = (0)$.

Since c) is a consequence of b), we prove d) next. Let $\ell \in \overline{P}_1$ be a linear form such that $\ell(p_i) \neq 0$. After a linear change of coordinates, we may assume that $\ell = x_0$. Then we have $p_i = (1 : c_1 : \ldots : c_n)$ with $c_1, \ldots, c_n \in K$, and Corollary 6.3.19 yields

$$R/\mathfrak{p}_i \cong \overline{P}/\mathcal{I}^+(\{p_i\}) = \overline{P}/(x_1 - c_1x_0, \ldots, x_n - c_nx_0) \cong K[x_0]$$

For the proof of the implication "$\Rightarrow$" in e), it suffices to note that ℓ is not contained in $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_s$ and to apply Proposition 5.6.17.c. Conversely, suppose that $\ell \in \mathfrak{p}_i$. Then Proposition 5.6.32.a implies $\dim(R/(\ell)) = 1$, whereas Proposition 5.6.34.c yields $\dim(R/(\ell)) = 0$, a contradiction.

Finally we show f). By Proposition 5.4.5.f, we may assume that K is infinite. Using the lemma and a suitable linear change of coordinates, we see that it suffices to treat the case when $\mathbb{X}$ is contained in the affine part of $\mathbb{P}^n_K$. Hence we have $R = \overline{P}/\mathcal{I}(\mathbb{X}^a)^{\hom}$, and using Proposition 5.6.12.d, we obtain $\operatorname{mult}(R) = \operatorname{mult}(P/\mathcal{I}(\mathbb{X}^a))$. Now an application of Proposition 6.3.3.b finishes the proof, because $\operatorname{mult}(P/\mathcal{I}(\mathbb{X}^a)) = \dim_K(P/\mathcal{I}(\mathbb{X}^a)) = s$. □

These algebraic properties of the homogeneous coordinate ring of a projective point set imply that its Hilbert function has certain nice properties. First we introduce another name for this Hilbert function.

Definition 6.3.22. Let $\mathbb{X} \subseteq \mathbb{P}^n_K$ be a projective point set with homogeneous coordinate ring $R = \overline{P}/\mathcal{I}^+(\mathbb{X})$. Then the Hilbert function $\mathrm{HF}_R : \mathbb{Z} \longrightarrow \mathbb{Z}$ of R is also called the **Hilbert function** of $\mathbb{X}$ and denoted by $\mathrm{HF}_{\mathbb{X}}$.

Its first difference function $\Delta \mathrm{HF}_{\mathbb{X}} : \mathbb{Z} \longrightarrow \mathbb{Z}$ is called the **Castelnuovo function** of $\mathbb{X}$.

Proposition 6.3.23. *Let $\mathbb{X} = \{p_1, \ldots, p_s\} \subseteq \mathbb{P}^n_K$ be a projective point set.*

a) For $i < 0$, we have $\mathrm{HF}_{\mathbb{X}}(i) = 0$, and we have $\mathrm{HF}_{\mathbb{X}}(0) = 1$.
b) Let $r_{\mathbb{X}} = \mathrm{ri}(\mathrm{HF}_{\mathbb{X}})$. Then we have $\mathrm{HF}_{\mathbb{X}}(i) = s$ for all $i \geq r_{\mathbb{X}}$.
c) We have $\mathrm{HF}_{\mathbb{X}}(0) < \mathrm{HF}_{\mathbb{X}}(1) < \cdots < \mathrm{HF}_{\mathbb{X}}(r_{\mathbb{X}})$.

Proof. Let R be the homogeneous coordinate ring of $\mathbb{X}$. Claim a) is true because R is a standard graded K-algebra. By the definition of $\mathrm{ri}(\mathrm{HF}_{\mathbb{X}})$, we have $\mathrm{HF}_{\mathbb{X}}(i) = \mathrm{HP}_R(i)$ for all $i \geq r_{\mathbb{X}}$. Hence b) follows from $\dim(R) = 1$ and Theorem 5.4.15.b. It remains to prove c). By Corollary 5.1.20, we may assume that K is infinite. Thus we can use Lemma 6.3.20.b and a linear change of coordinate to get $\mathbb{X} \subseteq \imath_0(\mathbb{A}^n_K)$. Now Proposition 6.3.21.e shows that x_0 is a non-zero divisor for R. Consequently, the ring $\overline{R} = R/(x_0)$ is a zero dimensional standard graded K-algebra. In particular, we have $\overline{R}_{i+1} = x_1\overline{R}_i + \cdots + x_n\overline{R}_i$ for $i \geq 1$. Therefore, if $\overline{R}_i = 0$ for some $i \geq 1$, then we have $\overline{R}_j = 0$ for all $j \geq i$. This means that $\overline{R}_i \neq 0$ for $0 \leq i < \mathrm{ri}(\mathrm{HF}_{\overline{R}})$ and $\mathrm{HF}_R(i) = \mathrm{HF}_R(i-1) + \mathrm{HF}_{\overline{R}}(i) > \mathrm{HF}_R(i-1)$ for $1 \leq i \leq \mathrm{ri}(\mathrm{HF}_R) = \mathrm{ri}(\mathrm{HF}_{\overline{R}}) - 1$. □

Based on this knowledge of the shape of the Hilbert function of $\mathbb{X}$, we can now develop an efficient procedure for computing the homogeneous vanishing ideal of $\mathbb{X}$ which combines the linear algebra approach underlying the Buchberger-Möller Algorithm 6.3.10 with the ideas behind the Hilbert-driven strategies explained in Tutorial 69.

Theorem 6.3.24. (Projective Buchberger-Möller Algorithm) *Let $\mathbb{X} = \{p_1, \ldots, p_s\} \subseteq \mathbb{P}^n_K$ be a projective point set, where each point p_i is given by a fixed coordinate tuple $p_i = (c_{i0} : \cdots : c_{in})$, and let σ be a term ordering on $\mathbb{T}^{n+1}$. Consider the following sequence of instructions.*

1) *Let $G = \emptyset$, $\mathcal{S} = \emptyset$, $L = \{1\}$, $d = 0$, and let $\mathcal{M} = (m_{ij})$ be a matrix over K with s columns and initially zero rows.*
2) *Compute the Hilbert series of $S = \overline{P}/(\mathrm{LT}_\sigma(g) \mid g \in G)$ and check whether $\mathrm{HF}_S(i) = s$ for all $i \geq d$. If this is true, return G and stop. Otherwise, increase d by one, let $\mathcal{S} = \emptyset$, let $\mathcal{M} = (m_{ij})$ be a matrix over K with s columns and zero rows, and let L be the set of all terms in $\mathbb{T}^{n+1}_d$ which are not multiples of an element $\mathrm{LT}_\sigma(g)$ with $g \in G$.*
3) *If $L = \emptyset$, continue with step 2). Otherwise, choose $t = \min_\sigma(L)$ and remove it from L.*
4) *For $i = 1, \ldots, s$, compute $t(p_i) = t(c_{i0}, \ldots, c_{in})$. Reduce the vector $(t(p_1), \ldots, t(p_s))$ against the rows of $\mathcal{M}$ to obtain*

$$(v_1, \ldots, v_s) = (t(p_1), \ldots, t(p_s)) - \sum_i a_i \, (m_{i1}, \ldots, m_{is})$$

with $a_i \in K$.
5) *If $(v_1, \ldots, v_s) = (0, \ldots, 0)$ then append the polynomial $t - \sum_i a_i s_i$ to G, where s_i is the i^{th} element of the list $\mathcal{S}$. Continue with step 3).*
6) *If $(v_1, \ldots, v_s) \neq (0, \ldots, 0)$ then add $(v_1, \ldots, v_s)$ as a new row to $\mathcal{M}$ and $t - \sum_i a_i s_i$ as a new element to $\mathcal{S}$. Continue with step 3).*

This is an algorithm which returns the reduced σ-Gröbner basis of $\mathcal{I}^+(\mathbb{X})$.

Proof. To simplify the notation, we let $\mathrm{LT}_\sigma(G) = (\mathrm{LT}_\sigma(g) \mid g \in G)$ and $I = \mathcal{I}^+(\mathbb{X})$. First we show finiteness of the algorithm. From the construction we see that each time step 2) is entered, the number of rows of $\mathcal{M}$ is exactly $\mathrm{HF}_{\overline{P}/I}(d)$: all terms of degree d outside $\mathrm{LT}_\sigma(G)$ are examined for being a leading term of an element of I, and a list of representatives of a K-basis of $(\overline{P}/I)_d$ is constructed in $\mathcal{S}$. By Proposition 6.3.23, we eventually reach $\mathrm{HF}_{\overline{P}/I}(d) = s$. Moreover, when d surpasses the largest degree of a minimal generator of $\mathrm{LT}_\sigma(I)$, the condition in step 2) is satisfied and the algorithm stops.

Now we prove correctness. By construction, the list G contains only elements of I. Hence we always have the inclusion $\mathrm{LT}_\sigma(G) \subseteq \mathrm{LT}_\sigma(I)$ and the relations $\mathrm{HF}_{\overline{P}/\mathrm{LT}_\sigma(G)}(d) \geq \mathrm{HF}_{\overline{P}/\mathrm{LT}_\sigma(I)}(d) = \mathrm{HF}_{\mathbb{X}}(d)$. When the criterion of step 2) is satisfied, we necessarily have $\mathrm{LT}_\sigma(G) = \mathrm{LT}_\sigma(I)$ because if there was a minimal generator t of $\mathrm{LT}_\sigma(I)$ in degree $i > d$, we would

have $\mathrm{HF}_{\overline{P}/(\mathrm{LT}_\sigma(G)+(t))}(i) < \mathrm{HF}_{\overline{P}/\mathrm{LT}_\sigma(G)}(i) = s = \mathrm{HF}_{\overline{P}/I}(i)$, a contradiction. Therefore the set G is a σ-Gröbner basis of I when the algorithm stops. By construction, this is the reduced σ-Gröbner basis of I. □

Let us add some remarks about possible variations and optimizations of this algorithm.

Remark 6.3.25. Assume that we are in the setting of the theorem.

a) The computation of the reduced Gröbner basis in the algorithm of the theorem proceeds degree by degree. If we stop the computation after some degree d is finished, the set G is a d-truncated σ-Gröbner basis of $\mathcal{I}^+(\mathbb{X})$.
b) The first part of step 2) is a **stopping criterion**, i.e. a criterion which tells us whether we have already found all elements of the reduced Gröbner basis of $\mathcal{I}^+(\mathbb{X})$. Other stopping criteria can be used instead, e.g. the one given in [Ab00], Theorem 3.10.
c) Variants of this algorithm can be constructed which also compute separators. For projective point sets, every point has separators in several degrees. The minimal degrees of the separators are useful invariants of $\mathbb{X}$. This aspect is explored more thoroughly in Tutorial 88.

Let us conclude the discussion of the projective Buchberger-Möller algorithm by computing one example by hand.

Example 6.3.26. Let $\mathbb{X} = \{p_1, \ldots, p_7\} = \mathbb{P}^2_K$, where $K = \mathbb{F}_2$, and where $p_1 = (1:0:0)$, $p_2 = (1:0:1)$, $p_3 = (1:1:0)$, $p_4 = (1:1:1)$, $p_5 = (0:0:1)$, $p_6 = (0:1:0)$, and $p_7 = (0:1:1)$. We want to compute the reduced `Lex`-Gröbner basis of the homogeneous vanishing ideal $\mathcal{I}^+(\mathbb{X})$. Here are the steps of the projective Buchberger-Möller algorithm.

1) Let $G = \emptyset$, $\mathcal{S} = \emptyset$, $d = 0$, and $\mathcal{M} \in \mathrm{Mat}_{0,7}(\mathbb{F}_2)$.
2) The Hilbert function of $S = \overline{P}$ satisfies $\mathrm{HF}_S(d) = 1$. Hence we let $d = 1$, $\mathcal{S} = \emptyset$, $\mathcal{M} \in \mathrm{Mat}_{0,7}(\mathbb{F}_2)$, and $L = \{x_0, x_1, x_2\}$.
3) Choose $t = x_2$ and let $L = \{x_0, x_1\}$.
4) Compute $(t(p_1), \ldots, t(p_7)) = (0,1,0,1,1,0,1) = (v_1, \ldots, v_7)$.
6) Let $\mathcal{M} = (0\,1\,0\,1\,1\,0\,1)$ and $\mathcal{S} = (x_2)$.
3) Choose $t = x_1$ and let $L = \{x_0\}$.
4) Compute $(t(p_1), \ldots, t(p_7)) = (0,0,1,1,0,1,1) = (v_1, \ldots, v_7)$.
6) Let $\mathcal{M} = \left(\begin{smallmatrix} 0&1&0&1&1&0&1 \\ 0&0&1&1&0&1&1 \end{smallmatrix}\right)$ and $\mathcal{S} = (x_2, x_1)$.
3) Choose $t = x_0$ and let $L = \emptyset$.
4) Compute $(t(p_1), \ldots, t(p_7)) = (1,1,1,1,0,0,0) = (v_1, \ldots, v_7)$.
6) Let $\mathcal{M} = \left(\begin{smallmatrix} 0&1&0&1&1&0&1 \\ 0&0&1&1&0&1&1 \\ 1&1&1&1&0&0&0 \end{smallmatrix}\right)$ and $\mathcal{S} = (x_2, x_1, x_0)$.
2) The Hilbert function of $S = \overline{P}$ satisfies $\mathrm{HF}_S(d) = 3$. Hence we let $d = 2$, $\mathcal{S} = \emptyset$, $\mathcal{M} \in \mathrm{Mat}_{0,7}(\mathbb{F}_2)$, and $L = \{x_0^2, x_0x_1, x_0x_2, x_1^2, x_1x_2, x_2^2\}$.

Now we continue to cycle through the loop in steps 3)–6). No Gröbner basis elements are discovered, and after six loops we arrive at step 2) again.

2) The Hilbert function of $S = \overline{P}$ satisfies $\mathrm{HF}_S(d) = 6$. Hence we let $d = 3$, $\mathcal{S} = \emptyset$, $\mathcal{M} \in \mathrm{Mat}_{0,7}(\mathbb{F}_2)$, and $L = \{x_0^3, x_0^2x_1, x_0^2x_2, x_0x_1^2, x_0x_1x_2, x_0x_2^2, x_1^3, x_1^2x_2, x_1x_2^2, x_2^3\}$.
3) Choose $t = x_2^3$ and let $L = \{x_0^3, x_0^2x_1, x_0^2x_2, x_0x_1^2, x_0x_1x_2, x_0x_2^2, x_1^3, x_1^2x_2, x_1x_2^2\}$.
4) Compute $(t(p_1), \ldots, t(p_7)) = (0,1,0,1,1,0,1) = (v_1, \ldots, v_7)$.
6) Let $\mathcal{M} = (0\ 1\ 0\ 1\ 1\ 0\ 1)$ and $\mathcal{S} = (x_2^3)$.
3) Choose $t = x_1x_2^2$ and let $L = \{x_0^3, x_0^2x_1, x_0^2x_2, x_0x_1^2, x_0x_1x_2, x_0x_2^2, x_1^3, x_1^2x_2\}$.
4) Compute $(t(p_1), \ldots, t(p_7)) = (0,0,0,1,0,0,1) = (v_1, \ldots, v_7)$.
6) Let $\mathcal{M} = \left(\begin{smallmatrix} 0&1&0&1&1&0&1 \\ 0&0&0&1&0&0&1 \end{smallmatrix}\right)$ and $\mathcal{S} = (x_2^3, x_1x_2^2)$.
3) Choose $t = x_1^2x_2$ and let $L = \{x_0^3, x_0^2x_1, x_0^2x_2, x_0x_1^2, x_0x_1x_2, x_0x_2^2, x_1^3\}$.
4) Compute $(t(p_1), \ldots, t(p_7)) = (0,0,0,1,0,0,1)$ and reduce it against the rows of $\mathcal{M}$ to obtain $(v_1, \ldots, v_7) = (0, \ldots, 0)$.
5) Let $G = \{x_1^2x_2 + x_1x_2^2\}$.
3) Choose $t = x_1^3$ and let $L = \{x_0^3, x_0^2x_1, x_0^2x_2, x_0x_1^2, x_0x_1x_2, x_0x_2^2\}$.
4) Compute $(t(p_1), \ldots, t(p_7)) = (0,0,1,1,0,1,1) = (v_1, \ldots, v_7)$
6) Let $\mathcal{M} = \left(\begin{smallmatrix} 0&1&0&1&1&0&1 \\ 0&0&0&1&0&0&1 \\ 0&0&1&1&0&1&1 \end{smallmatrix}\right)$ and $\mathcal{S} = (x_2^3, x_1x_2^2, x_1^3)$.
3) Choose $t = x_0x_2^2$ and let $L = \{x_0^3, x_0^2x_1, x_0^2x_2, x_0x_1^2, x_0x_1x_2\}$.
4) Compute $(t(p_1), \ldots, t(p_7)) = (0,1,0,1,0,0,0)$ and reduce it against the rows of $\mathcal{M}$ to obtain $(v_1, \ldots, v_7) = (0,0,0,0,1,0,1)$.
6) Let $\mathcal{M} = \left(\begin{smallmatrix} 0&1&0&1&1&0&1 \\ 0&0&0&1&0&0&1 \\ 0&0&1&1&0&1&1 \\ 0&0&0&0&1&0&1 \end{smallmatrix}\right)$ and $\mathcal{S} = (x_2^3, x_1x_2^2, x_1^3, x_0x_2^2 + x_2^3)$.
3) Choose $t = x_0x_1x_2$ and let $L = \{x_0^3, x_0^2x_1, x_0^2x_2, x_0x_1^2\}$.
4) Compute $(t(p_1), \ldots, t(p_7)) = (0,0,0,1,0,0,0)$ and reduce it against the rows of $\mathcal{M}$ to obtain $(v_1, \ldots, v_7) = (0,0,0,0,0,0,1)$.
6) Let $\mathcal{M} = \left(\begin{smallmatrix} 0&1&0&1&1&0&1 \\ 0&0&0&1&0&0&1 \\ 0&0&1&1&0&1&1 \\ 0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&1 \end{smallmatrix}\right)$ and $\mathcal{S} = (x_2^3, x_1x_2^2, x_1^3, x_0x_2^2+x_2^3, x_0x_1x_2+x_1x_2^2)$.
3) Choose $t = x_0x_1^2$ and let $L = \{x_0^3, x_0^2x_1, x_0^2x_2\}$.
4) Compute $(t(p_1), \ldots, t(p_7)) = (0,0,1,1,0,0,0)$ and reduce it against the rows of $\mathcal{M}$ to obtain $(v_1, \ldots, v_7) = (0,0,0,0,0,1,1)$.
6) Let $\mathcal{M} = \left(\begin{smallmatrix} 0&1&0&1&1&0&1 \\ 0&0&0&1&0&0&1 \\ 0&0&1&1&0&1&1 \\ 0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&1 \\ 0&0&0&0&0&1&1 \end{smallmatrix}\right)$ and $\mathcal{S} = (x_2^3,\ x_1x_2^2,\ x_1^3,\ x_0x_2^2+x_2^3,\ x_0x_1x_2+x_1x_2^2,\ x_0x_1^2 + x_1^2x_2)$.
3) Choose $t = x_0^2x_2$ and let $L = \{x_0^3, x_0^2x_1\}$.
4) Compute $(t(p_1), \ldots, t(p_7)) = (0,1,0,1,0,0,0)$ and reduce it against the rows of $\mathcal{M}$ to obtain $(v_1, \ldots, v_7) = (0, \ldots, 0)$.
5) Let $\mathcal{G} = \{x_1^2x_2 + x_1x_2^2,\ x_0^2x_2 + x_0x_2^2\}$.
3) Choose $t = x_0^2x_1$ and let $L = \{x_0^3\}$.
4) Compute $(t(p_1), \ldots, t(p_7)) = (0,0,1,1,0,0,0)$ and reduce it against the rows of $\mathcal{M}$ to obtain $(v_1, \ldots, v_7) = (0, \ldots, 0)$.
5) Let $\mathcal{G} = \{x_1^2x_2 + x_1x_2^2,\ x_0^2x_2 + x_0x_2^2,\ x_0^2x_1 + x_0x_1^2\}$.
3) Choose $t = x_0^3$ and let $L = \emptyset$.
4) Compute $(t(p_1), \ldots, t(p_7)) = (1,1,1,1,0,0,0) = (v_1, \ldots, v_7)$.

6) Let $\mathcal{M} = \begin{pmatrix} 0&1&0&1&1&0&1 \\ 0&0&0&1&0&0&1 \\ 0&0&1&1&0&1&1 \\ 0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&1 \\ 0&0&0&0&0&1&1 \\ 1&1&1&1&0&0&0 \end{pmatrix}$ and $\mathcal{S} = (x_2^3,\, x_1x_2^2,\, x_1^3,\, x_0x_2^2+x_2^3,\, x_0x_1x_2+x_1x_2^2,\, x_0x_1^2+x_1^2x_2,\, x_0^3)$.
2) Compute $\mathrm{LT}_{\mathtt{Lex}}(G) = (x_0^2x_1, x_0^2x_2, x_1^2x_2)$ and $\mathrm{HF}_{\overline{P}/(x_0^2x_1, x_0^2x_2, x_1^2x_2)}(i) = 7$ for $i \geq 3$. Return G and stop.

Altogether, we find that the reduced `Lex`-Gröbner basis of $\mathcal{I}^+(\mathbb{X})$ is the set $G = \{x_0^2x_1 + x_0x_1^2,\, x_0^2x_2 + x_0x_2^2,\, x_1^2x_2 + x_1x_2^2\}$.

6.3.C Hilbert Functions of Points

Guiding a group of mathematicians
is like herding cats.
(Anthony V. Geramita)

In this subsection we want to guide you through a complete classification of all possible Hilbert functions of projective point sets. In Proposition 6.3.23, we have seen some of their basic properties. Their growth is restricted by the bounds we proved in Section 5.5.C. Let $\mathbb{X} = \{p_1 \ldots, p_s\} \subseteq \mathbb{P}_K^n$ be a projective point set and $\mathrm{HF}_{\mathbb{X}} : \mathbb{Z} \longrightarrow \mathbb{Z}$ its Hilbert function.

Remark 6.3.27. For all $i \geq 1$, we have $\mathrm{HF}_{\mathbb{X}}(i+1) \leq (\mathrm{HF}_{\mathbb{X}}(i)_{[i]})_+^+$ and $\Delta\,\mathrm{HF}_{\mathbb{X}}(i+1) \leq (\Delta\,\mathrm{HF}_{\mathbb{X}}(i)_{[i]})_+^+$. This follows from Corollary 5.5.28, because $\mathrm{HF}_{\mathbb{X}}$ is the Hilbert function of $R = \overline{P}/\mathcal{I}^+(\mathbb{X})$ and $\Delta\,\mathrm{HF}_{\mathbb{X}}$ is the Hilbert function of $\overline{R}/(x_0)$ if x_0 is a non-zero divisor for R. The last condition can be satisfied since Hilbert functions do not change under base field extensions, and if K is infinite then we have $\mathbb{X} \subseteq \imath_0(\mathbb{A}_K^n)$ after a suitable linear change of coordinates.

Thus it is natural to introduce the following notion.

Definition 6.3.28. A function $H : \mathbb{Z} \longrightarrow \mathbb{Z}$ is called an **O-sequence** if it has the following properties.

a) For $i < 0$, we have $H(i) = 0$, and $H(0) = 1$.
b) There exists a number $r \in \mathbb{N}$ such that $H(i) = 0$ for $i \geq r$ and $H(i) \neq 0$ for $0 \leq i < r$.
c) For $i = 1, \ldots, r-1$, we have $H(i+1) \leq (H(i)_{[i]})_+^+$.

Proposition 6.3.23 and Remark 6.3.27 yield the following result.

Corollary 6.3.29. *The Castelnuovo function $\Delta H_{\mathbb{X}}$ of a projective point set $\mathbb{X}$ is an O-sequence.*

Next we ask whether every O-sequence is the Castelnuovo function of a suitable projective point set. The first step in this direction is provided by the following proposition.

Proposition 6.3.30. *For an integer function $H : \mathbb{Z} \longrightarrow \mathbb{Z}$, the following conditions are equivalent.*

a) The function H is an O-sequence.
b) There exists a `Lex`*-segment ideal $I \subseteq P$ such that $\dim(P/I) = 0$ and $H = \mathrm{HF}_{P/I}$.*

Proof. First we show that a) implies b). By Theorem 5.5.32, there exists a unique `Lex`-segment ideal $I \subseteq P$ such that $H = \mathrm{HF}_{P/I}$. Since we have $H(i) = 0$ for $i \geq r$, the K-vector space P/I is finite-dimensional. Therefore P/I is a zero-dimensional ring. Conversely, Theorem 5.5.32 yields conditions a) and c) of Definition 6.3.28. Moreover, since $\dim(P/I) = 0$ we conclude that there exists a number $r \geq 1$ such that $(P/I)_{r-1} \neq 0$ and $(P/I)_i = 0$ for $i \geq r$. Now the fact that P/I is a standard graded algebra implies $(P/I)_i \neq 0$ for $0 \leq i < r$. □

At this point we are ready to characterize Hilbert functions of projective point sets over an infinite base field K.

Theorem 6.3.31. (Hilbert Functions of Projective Point Sets) *Let K be a field with infinitely many elements, and let $H : \mathbb{Z} \longrightarrow \mathbb{Z}$ be an integer function. Then the following conditions are equivalent.*

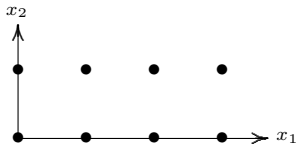
a) There exists a projective point set $\mathbb{X} \subseteq \mathbb{P}^n_K$ such that $H = \mathrm{HF}_{\mathbb{X}}$.
b) The function $\Delta H : \mathbb{Z} \longrightarrow \mathbb{Z}$ is an O-sequence.

Proof. Corollary 6.3.29 shows that a) implies b). To prove the converse implication, we apply Proposition 6.3.30 and get a `Lex`-segment ideal $I \subseteq P$ such that $\dim(P/I) = 0$ and $\mathrm{HF}_{P/I} = \Delta H$. We choose sequences $\pi_1, \ldots, \pi_n$ of pairwise distinct elements of K and let $\pi = (\pi_1, \ldots, \pi_n)$. By Theorem 6.2.12.d, the ideal $J = D_\pi(I)^{\mathrm{hom}}$ is an x_0-lifting of I and a radical ideal. Here x_0 is a non-zero divisor for $\overline{P}/J$ and $\overline{P}/(J + (x_0)) \cong P/I$. Hence we have $\Delta H = \mathrm{HF}_{P/I} = \Delta \mathrm{HF}_{\overline{P}/J}$. Together with $H(i) = \mathrm{HF}_{\overline{P}/J}(i) = 0$ for $i < 0$ and $H(0) = \mathrm{HF}_{\overline{P}/J}(0) = 1$, this shows that $H = \mathrm{HF}_{\overline{P}/J}$. Therefore it remains to prove that there exists a projective point set $\mathbb{X} \subseteq \mathbb{P}^n_K$ such that $J = \mathcal{I}^+(\mathbb{X})$.

By Theorem 6.2.8, the ideal $D_\pi(I)$ is an intersection of finitely many vanishing ideals of affine points, i.e. of ideals of the form $(x_1 - c_{i1}, \ldots, x_n - c_{in})$ with $c_{ij} \in K$. Hence we can use the rule given in Proposition 4.3.10.b to deduce that J is the intersection of finitely many ideals of the form $(x_1 - c_{i1}x_0, \ldots, x_n - c_{in}x_0)$. Since these ideals are the homogeneous vanishing ideals of the points $(1 : c_{i1} : \cdots : c_{in}) \in \mathbb{P}^n_K$, the claim follows. □

It is clear that the implication "b)⇒a)" of the theorem continues to hold if K is finite, but has sufficiently many elements. The following example shows how one can use the proof of the theorem to construct the corresponding projective point set.

Example 6.3.32. Let $K = \mathbb{F}_5$ and $H : \mathbb{Z} \longrightarrow \mathbb{Z}$ be the O-sequence such that $H(1) = H(2) = H(3) = 2$, $H(4) = 1$, and $H(i) = 0$ for $i \geq 5$. The corresponding Lex-segment ideal in $K[x_1, x_2]$ is (x_1^4, x_2^2). We choose the sequences $\pi_1 = (0, 1, 2, 3)$ and $\pi_2 = (0, 1)$ and let $J = D_\pi((x_1^4, x_2^2))^{\text{hom}} = (x_2(x_2 - x_0), x_1(x_1 - x_0)(x_1 - 2x_0)(x_1 - 3x_0))$. Then J is the homogeneous vanishing ideal of the projective point set $\mathbb{X} = \{(1 : 0 : 0), (1 : 1 : 0), (1 : 2 : 0), (1 : 3 : 0), (1 : 0 : 1), (1 : 1 : 1), (1 : 2 : 1), (1 : 3 : 1)\}$ in $\mathbb{P}_K^2$. The Castelnuovo function of $\mathbb{X}$ is H.



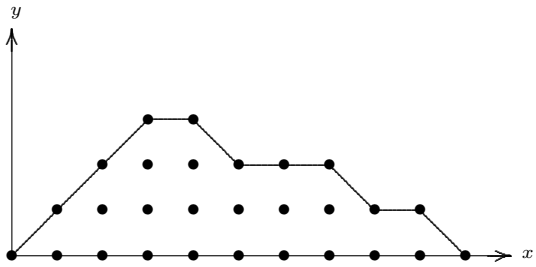
If K has too few elements, the theorem is not true anymore, as our next example demonstrates.

Example 6.3.33. Let $K = \mathbb{F}_2$ and $H : \mathbb{Z} \longrightarrow \mathbb{Z}$ be the O-sequence such that $H(1) = 2$, $H(2) = H(3) = H(4) = 1$, and $H(i) = 0$ for $i \geq 5$. The 2-dimensional projective space over K is a set $\mathbb{X}$ which consists of seven points. Its Hilbert function is $\mathrm{HF}_{\mathbb{X}} : 1\ 3\ 6\ 7\ 7\ \cdots$ (see Example 6.3.26). We are looking for a subset $\mathbb{Y}$ consisting of six of those points such that $\mathrm{HF}_{\mathbb{Y}} : 1\ 3\ 4\ 5\ 6\ 6\ \cdots$ which does not appear to be unreasonable at first sight.

As in Remark 6.3.27, we may perform a base field extension and a linear change of coordinates such that x_0 becomes a non-zero divisor for the homogeneous coordinate ring $R = \overline{P}/\mathcal{I}^+(\mathbb{X})$ of $\mathbb{X}$. Then the Hilbert function of $R/(x_0)$ is $\mathrm{HF}_{R/(x_0)} = \Delta\,\mathrm{HF}_{\mathbb{X}} : 1\ 2\ 3\ 1$. Since the line $\mathcal{Z}^+(x_0)$ also misses the points of $\mathbb{Y}$, the polynomial x_0 is a non-zero divisor for the homogeneous coordinate ring S of $\mathbb{Y}$ and we have $\mathrm{HF}_{S/(x_0)} = \Delta\,\mathrm{HF}_{\mathbb{Y}} : 1\ 2\ 1\ 1\ 1$. Now $S/(x_0)$ is supposed to be a residue class ring of $R/(x_0)$, but this is impossible since $(R/(x_0))_4 = 0$ and $(S/(x_0))_4 \neq 0$.

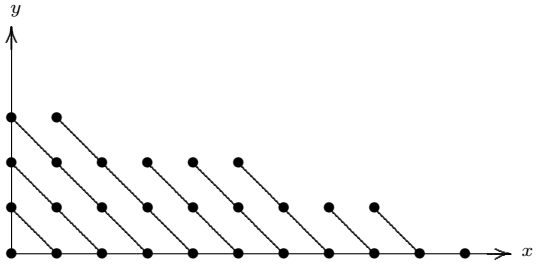
Finally, we mention a particularly simple and impressive method for constructing a point set in $\mathbb{P}_K^2$ with a given Hilbert function if the characteristic of K is zero.

Corollary 6.3.34. *Let K be a field of characteristic zero and $H : \mathbb{Z} \longrightarrow \mathbb{Z}$ be an O-sequence with $H(1) \leq 2$. Consider the points in $\mathbb{N}^2$ lying "on and under" the graph of H in the following sense:*



Then the corresponding projective point set $\mathbb{X}$ *in the affine part of* $\mathbb{P}^2_K$ *has Castelnuovo function* H*.*

Proof. Let $\pi_1 = \pi_2 = (0, 1, 2, \ldots)$, let $\pi = (\pi_1, \pi_2)$, and let $I \subseteq K[x_1, x_2]$ be the `Lex`-segment ideal corresponding to H. By Proposition 6.2.8, the ideal $J = D_\pi(I)^{\mathrm{hom}}$ is the homogeneous vanishing ideal of the projective point set of the form



where the number of points on the diagonal line through $(i, 0)$ is $H(i)$. Now it suffices to apply the linear change of coordinates given by $x_0 \mapsto x_0$, $x_1 \mapsto x_1 + x_2$, and $x_2 \mapsto x_2$ to obtain the desired projective point set. □

Exercise 1. (Lagrange Interpolation)
Let K be a field, let $p_1, \ldots, p_s \in K$ be pairwise distinct elements, let $\mathbb{X} = \{p_1, \ldots, p_s\} \subseteq \mathbb{A}^1_K$, and let $q_1, \ldots, q_s \in K$.

a) For $i = 1, \ldots, s$, show that $f_i = \prod_{j \neq i} \frac{x - p_j}{p_i - p_j} \in K[x]$ is a separator of p_i from $\mathbb{X} \setminus p_i$.
b) Prove that $q_1 f_1 + \cdots + q_s f_s \in K[x]$ is an interpolator for $(q_1, \ldots, q_s)$ with respect to $(p_1, \ldots, p_s)$.

Exercise 2. Let $\mathbb{X} = \{(0,0,0), (1,0,0), (0,1,0), (0,0,1)\} \subseteq \mathbb{A}^3_{\mathbb{Q}}$. Compute the reduced `DegRevLex`-Gröbner basis of $\mathcal{I}(\mathbb{X})$ by applying the Buchberger-Möller algorithm.

Exercise 3. Find all polynomials $f \in \mathbb{Q}[x, y]$ which attain the following values: $f(2,3) = 1$, $f(5,2) = 3$, $f(-1,1) = 0$, $f(2,-5) = -1$, and $f(-2,-2) = 10$.

Exercise 4. Let K be a field of characteristic zero, let $I \subseteq K[x_1, \ldots, x_n]$ be a zero-dimensional monomial ideal, and let σ be a term ordering on $\mathbb{T}^n$. We identify the terms in $\mathcal{O}_\sigma(I) = \mathbb{T}^n \setminus \mathrm{LT}_\sigma\{I\} = \{t_1, \ldots, t_s\}$ with the points $p_i = \log(t_i) \in \mathbb{A}_K^n$, and we let $\pi_i = (0, 1, 2, \ldots)$ for $i = 1, \ldots, n$. Prove that the vanishing ideal of the affine point set $\mathbb{X} = \{p_1, \ldots, p_s\}$ in $\mathbb{A}_K^n$ is $\mathcal{I}(\mathbb{X}) = (D_\pi(t_1), \ldots, D_\pi(t_s))$, where $\pi = (\pi_1, \ldots, \pi_n)$.

Exercise 5. Let $\mathbb{X} \subset \mathbb{P}^2_\mathbb{Q}$ be a projective point set whose homogeneous vanishing ideal is of the form $\mathcal{I}^+(\mathbb{X}) = (F, G)$ with homogeneous polynomials $F, G \in \mathbb{Q}[x_0, x_1, x_2]$. Show that the following conditions are equivalent.

a) The Castelnuovo function of $\mathbb{X}$ has the shape $\Delta\,\mathrm{HF}_\mathbb{X} : 1\ 1\ \cdots 1\ 0\ 0 \cdots$.
b) We have $\min\{\deg(F), \deg(G)\} = 1$.

Exercise 6. Let K be a field, let $\overline{P} = K[x_0, \ldots, x_n]$ be standard graded, and let $\mathbb{X} \subset \mathbb{P}^n_K$ be a projective point set with the property that $\Delta\,\mathrm{HF}_\mathbb{X}(r_\mathbb{X} - 1) = \Delta\,\mathrm{HF}_\mathbb{X}(r_\mathbb{X}) = 1$. Prove that $\mathbb{X}$ contains $r_\mathbb{X} + 1$ points on a line.

Exercise 7. Show that the algorithm in Theorem 6.3.24 is not correct if we replace the first part of step 2) by the following instruction:
Compute the Hilbert series of $S = \overline{P}/(\mathrm{LT}_\sigma(g) \mid g \in G)$ *and check whether* $\mathrm{HF}_S(d) = s$.

Exercise 8. Classify the possible Castelnuovo functions of five points in $\mathbb{P}^2_\mathbb{Q}$.

Tutorial 88: The Cayley-Bacharach Property

"Mullah Nasrudin, can I borrow your clothes-line?"
"Sorry, I am using it to dry flour."
"How on earth can you dry flour on a clothes-line?"
"It is less difficult than you think
when you do not want to lend it."

"Mullah Nasrudin, can I borrow your donkey?"
"Sorry, but it is not home today."
"EEH-AAH!"
"Why are you lying? Your donkey is home!"
"Do you believe me or the donkey?"

In this tutorial we want to acquire some experience in handling projective point sets. Rather than borrowing the built-in CoCoA command for computing their homogeneous vanishing ideals, we believe it is more honest and instructive for you to implement the Projective Buchberger-Möller Algorithm 6.3.24 on your own. You know, *you can observe a lot by just watching.* Knowing many examples is a powerful alternative source of experience. And don't try to compute vanishing ideals of large point sets using syzygies: it will take forever. "Good judgement comes from experience", said Mullah Nasrudin, "and experience comes from bad judgement."

By expending a little extra effort, we can even ferret out the separators of the point set. These are homogeneous polynomials which vanish at all of the points except one. Separators are not unique: given a projective point set $\mathbb{X}$ and a point $p \in \mathbb{X}$, there is a minimal degree of a separator of p from $\mathbb{X} \setminus \{p\}$. It is called the degree of the point in $\mathbb{X}$ and denoted by $\deg_{\mathbb{X}}(p)$. For every $d \geq \deg_{\mathbb{X}}(p)$, there is a 1-dimensional space of separators of p from $\mathbb{X} \setminus \{p\}$ in degree d. The sequence of the degrees of the points in $\mathbb{X}$ contains information about $\mathbb{X}$ and is called its conductor sequence. What secrets can we tease out of the conductor sequence of a projective point set? "I can't tell you the secret of the universe", said Mullah Nasrudin, "because then it would not be a secret anymore."

A particularly interesting situation occurs when all points of the set $\mathbb{X}$ have the maximal possible degree, namely the regularity index of the Hilbert function of $\mathbb{X}$. This property is called the Cayley-Bacharach property of $\mathbb{X}$. It has been studied in various guises for more than two centuries. For instance, you will show that a set of points in the projective plane which is the complete intersection of two plane curves enjoys this property. What is the Cayley-Bacharach property good for? Does it have any practical applications? "The moon is more useful than then sun", said Mullah Nasrudin, "because in the night we have more need of light."

Let K be a field, let $(c_{i0}, c_{i1}, \ldots, c_{in}) \in K^{n+1} \setminus \{0\}$ for $i = 1, \ldots, s$, and let $\mathbb{X} \subseteq \mathbb{P}^n_K$ be the projective point set $\mathbb{X} = \{p_1, \ldots, p_s\}$ given by $p_i = (c_{i0} : \ldots : c_{in})$ for $i = 1, \ldots, s$. We assume that $\mathbb{X}$ consists of s distinct points. Moreover, we equip the polynomial ring $\overline{P} = K[x_0, \ldots, x_n]$ with the standard grading, and we choose a term ordering σ in $\mathbb{T}^{n+1}$.

a) Write a CoCoA function `ProjBuMo(...)` which implements the Projective Buchberger-Möller Algorithm 6.3.24. It should take the matrix with rows $p_1, \ldots, p_s$ as its input and return the reduced σ-Gröbner basis of $\mathcal{I}^+(\mathbb{X})$. *Hint:* First you may want to write a subroutine which reduces a vector against the rows of a matrix in the sense explained before Theorem 6.3.10.

b) Apply your function `ProjBuMo(...)` to compute the homogeneous vanishing ideals of the following projective point sets.
   1) $\mathbb{X}_1 = \{(1{:}0{:}0), (0{:}1{:}0), (0{:}0{:}1)\} \subseteq \mathbb{P}^2_{\mathbb{Q}}$
   2) $\mathbb{X}_2$, the set of K-rational points in $\mathbb{P}^2_K$ where $K = \mathbb{Z}/(3)$
   3) $\mathbb{X}_3 = \{(1{:}1{:}1), (1{:}1{:}-1), (-1{:}1{:}-1), (-1{:}1{:}1), (1{:}4{:}1), (1{:}4{:}-1), (-1{:}4{:}-1), (-1{:}4{:}1)\} \subseteq \mathbb{P}^2_K$ where $K = \mathbb{Z}/(13)$

c) Formulate and prove the projective analog of Corollary 6.3.11. Expand your function `BuMo(...)` to include the new step 2') which returns also a list of homogeneous separators of $\mathbb{X}$. Call the new function `ExtBuMo(...)`.

d) Using your function `ExtBuMo(...)`, compute lists of homogeneous separators for the projective point sets in b).

e) Use `ExtBuMo(...)` to solve the following *separation problem*: find the equation of a hypersurface containing a given subset $\mathbb{Y}$ of $\mathbb{X}$ but which does

not pass through any point of $\mathbb{X} \setminus \mathbb{Y}$. Write a CoCoA function `CutOut(...)` which takes $\mathbb{Y} \subseteq \mathbb{X}$ and computes the equation of a hypersurface $H \subseteq \mathbb{P}^n$ which cuts out $\mathbb{Y}$, i.e. for which we have $\mathbb{Y} = \mathbb{X} \cap H$.

In the following we let $R = \overline{P}/\mathcal{I}^+(\mathbb{X})$ be the homogeneous coordinate ring of $\mathbb{X}$, we denote its Hilbert function by $\mathrm{HF}_{\mathbb{X}} = \mathrm{HF}_R$, and we let $r_{\mathbb{X}} = \mathrm{ri}_{\mathrm{HF}_{\mathbb{X}}}$.

f) Show that the map $\varepsilon : R_{r_{\mathbb{X}}} \longrightarrow K^s$ which is defined by sending $f + \mathcal{I}^+(\mathbb{X})$ to $(f(c_{10}, \ldots, c_{1n}), \ldots, f(c_{s0}, \ldots, c_{sn}))$ is an isomorphism of K-vector spaces.

g) Using f), show that for every $i \in \{1, \ldots, s\}$, there exists a homogeneous separator of p_i from $\mathbb{X} \setminus \{p_i\}$ of degree $r_{\mathbb{X}}$.

h) Let $1 \leq i \leq s$ and $\mathbb{Y} = \mathbb{X} \setminus \{p_i\}$. Prove that there is a degree $d \in \mathbb{N}$, called the **degree of p_i in $\mathbb{X}$** and denoted by $\deg_{\mathbb{X}}(p_i)$, such that

$$\mathrm{HF}_{\mathbb{Y}}(j) = \begin{cases} \mathrm{HF}_{\mathbb{X}}(j) & \text{for } j < d, \\ \mathrm{HF}_{\mathbb{X}}(j) - 1 & \text{for } j \geq d. \end{cases}$$

Furthermore, observe that we have $\deg_{\mathbb{X}}(p_k) \leq r_{\mathbb{X}}$ for $k = 1, \ldots, s$.

i) Show that, for any number $1 \leq t \leq s$, there exists a subset $\mathbb{Y} \subseteq \mathbb{X}$ consisting of t points such that the Hilbert function of $\mathbb{Y}$ satisfies $\mathrm{HF}_{\mathbb{Y}}(i) = \min\{t, \mathrm{HF}_{\mathbb{X}}(i)\}$ for every $i \in \mathbb{Z}$.

j) Explain how you can modify your program `ExtBuMo(...)` to compute a list of homogeneous separators of minimal degrees of $\mathbb{X}$. The tuple $(\deg_{\mathbb{X}}(p_1), \ldots, \deg_{\mathbb{X}}(p_s))$ is called the **conductor sequence** of $\mathbb{X}$. Write a CoCoA function `ConductorSeq(...)` which takes the matrix with rows $p_1, \ldots, p_s$ as input and computes the conductor sequence of $\mathbb{X}$.
Hint: Every time a degree is finished, diagonalize the matrix $\mathcal{M}$ as much as possible, mimic the necessary row operations on $\mathcal{S}$, and put the degrees of new separators you find into their position in the output tuple.

k) Using your function `ConductorSeq(...)`, compute the conductor sequences of the projective points sets in b) and of the following examples.
   1) $\mathbb{X}_4 = \mathcal{Z}^+_{\mathbb{Q}}(x_1(x_1 - x_0)(x_1 - 2x_0), x_2(x_2 - x_0)(x_2 - 2x_0)) \setminus \{(1{:}1{:}1)\} \subseteq \mathbb{P}^2_{\mathbb{Q}}$
   2) $\mathbb{X}_5 \subseteq \mathbb{P}^2_{\mathbb{Q}}$ given by the picture in Corollary 6.3.34
   3) $\mathbb{X}_6 = \{(1{:}0{:}0), (1{:}2{:}2), (1{:}3{:}3), (1{:}4{:}4), (1{:}1{:}0), (1{:}0{:}1)\} \subseteq \mathbb{P}^2_{\mathbb{Q}}$

The set $\mathbb{X}$ is said to have the **Cayley-Bacharach property**, or to be a **Cayley-Bacharach scheme**, if $\deg_{\mathbb{X}}(p_i) = r_{\mathbb{X}}$ for $i = 1, \ldots, s$. In the last part of this tutorial we look for examples of Cayley-Bacharach schemes.

l) Write a CoCoA function `IsCayleyBacharach(...)` which takes the matrix with rows $p_1, \ldots, p_s$ as input and checks whether $\mathbb{X}$ has the Cayley-Bacharach property. Find out which of the sets $\mathbb{X}_1, \ldots, \mathbb{X}_6$ have the Cayley-Bacharach property.

m) Assume that $\mathbb{X} \subseteq \mathbb{P}^2_K$ is a complete intersection of two hypersurfaces, i.e. assume that there are homogeneous polynomials $F, G \in K[x_0, x_1, x_2]$ of degree $a = \deg(F)$ and $b = \deg(G)$ such that $\mathcal{I}^+(\mathbb{X}) = (F, G)$. Show that $\mathbb{X}$ has the Cayley-Bacharach property by proving the following facts.

1) We may assume that x_0 is a non-zero divisor for R.
2) Let $\overline{R} = R/(x_0)$, and let $H \in K[x_0, x_1, x_2]$ be a homogeneous separator of a point p_i from $\mathbb{X} \setminus \{p_i\}$. Show that the residue class of $h = H(0, x_1, x_2)$ is an element of the **socle** of $\overline{R}$, i.e. that it is annihilated by the homogeneous maximal ideal $\overline{R}_+$.
Hint: Multiply H by lines passing through p_i.
3) Consider the presentation $\overline{R} \cong K[x_1, x_2]/(f, g)$ with $f = F(0, x_1, x_2)$ and $g = G(0, x_1, x_2)$. Prove that the socle of $\overline{R}$ is $\overline{R}_{a+b-2}$.
Hint: Write $x_1 h = c_{11} f + c_{12} g$ and $x_2 h = c_{21} f + c_{22} g$. Then use $\mathrm{Syz}(f, g) = \langle (-g, f) \rangle$ and show $\deg(h) \geq a + b - 2$.

Can you generalize this result to complete intersections in $\mathbb{P}^n_K$?

n) Write a CoCoA function `IsOSequence(...)` which takes a list of nonnegative integers, checks if it is an O-sequence, and returns the corresponding Boolean value.
o) Find all possible Hilbert functions of a projective point set $\mathbb{X} \subseteq \mathbb{P}^2_{\mathbb{Q}}$ consisting of ten points. Write a CoCoA function `AllHF(...)` to do this for any number of points in $\mathbb{P}^2_{\mathbb{Q}}$ and verify your result in some cases. How far can you compute `AllHF(...)`?
p) Find all Hilbert functions among the ones constructed in n) which have the property that any projective point set $\mathbb{X}$ with this Hilbert function is a Cayley-Bacharach scheme.

Tutorial 89: Generic Sets of Points

He knows nothing;
and he thinks he knows everything.
That points clearly to a political career.
(George Bernard Shaw)

Not wanting to embark on a political career yet, we admit that there are numerous problems concerning finite sets of points about which we know very little. One of the first and most natural questions is what the Hilbert function, degree sequence, and graded Betti numbers are for the vanishing ideal (or the homogeneous coordinate ring) of a "generically chosen" projective point set. Whereas the generic Hilbert function is not difficult to determine, there are (as of this writing) only partial results about the generic values of the degree sequence and the graded Betti numbers. In this tutorial we deduce some basic facts about these numbers. Moreover, we explore the Ideal Generation Conjecture and the Minimal Resolution Conjecture using CoCoA.

Let K be an infinite field, let $\overline{P} = K[x_0, \ldots, x_n]$ be a standard graded polynomial ring over K, let $s \geq 1$, let $\mathbb{X} = \{p_1, \ldots, p_s\} \subseteq \mathbb{P}^n_K$ be a projective point set, let $\mathcal{I}^+(\mathbb{X}) \subseteq \overline{P}$ be the homogeneous vanishing ideal of $\mathbb{X}$, and let $R = \overline{P}/\mathcal{I}^+(\mathbb{X})$ be the homogeneous coordinate ring of $\mathbb{X}$. Assume that $\mathcal{P}$ is a property of projective point sets consisting of s distinct points. In analogy

with Definition 5.5.19.c, we say that $\mathcal{P}$ holds for a **generic set of s points** if there exists a non-empty Zariski open subset U of $(K^{n+1})^s$ such that property $\mathcal{P}$ holds for every projective point set $\mathbb{X} = \{p_1, \ldots, p_s\}$ whose points $p_i = (p_{i0} : \ldots : p_{in})$ satisfy

$$((p_{10}, \ldots, p_{1n}), \ldots, (p_{s0}, \ldots, p_{sn})) \in U$$

We say that $\mathbb{X}$ has **generic Hilbert function** (or that $\mathbb{X}$ is **in generic position**) if $\mathrm{HF}_{\mathbb{X}}(i) = \min\{s, \binom{i+n}{n}\}$ for all $i \geq 0$.

a) Show that a generic set of s points has generic Hilbert function and the property that no three points are **collinear** (i.e. no three points are contained in a line).
b) Let $K = \mathbb{Q}$. Write a CoCoA function `GenPoints(...)` which takes s and computes an $s \times (n+1)$-matrix over $\mathbb{Q}$ whose rows represent the points of a projective point set $\mathbb{X}$ which has generic Hilbert function and no three points of which are collinear.

In the following we assume that $\mathbb{X}$ has generic Hilbert function. Let α be the least degree of a non-zero element in $\mathcal{I}^+(\mathbb{X})$. The **Ideal Generation Conjecture (IGC)** predicts the number of the minimal homogeneous generators of $\mathcal{I}^+(\mathbb{X})$ and their degrees for a generic set of s points. In the next part of this tutorial we derive an explicit version of this conjecture and prove it in some cases.

c) Let d be the unique integer such that $\binom{d+n}{n} \leq s < \binom{d+1+n}{n}$. Show that $d = \alpha - 1$.
d) Prove that there exists an element $\ell \in R_1$ for which $S = R/(\ell)$ has Hilbert function $\mathrm{HF}_S(i) = \Delta \mathrm{HF}_{\mathbb{X}}(i)$ for all $i \in \mathbb{Z}$. Conclude that $S_i = 0$ for all $i \geq \alpha + 1$.
e) Show that, after a suitable linear change of coordinates, the ring S has a presentation $S \cong K[y_1, \ldots, y_n]/J$ where $K[y_1, \ldots, y_n]$ is a standard graded polynomial ring and J is a homogeneous ideal which has the same number of minimal homogeneous generators as $\mathcal{I}^+(\mathbb{X})$ in each degree.
f) Prove that J has minimal homogeneous generators in degrees α and $\alpha + 1$ only, and that is has exactly $\binom{\alpha+n}{n} - s$ minimal homogeneous generators in degree α.
g) Let $\Phi : S_1 \times J_\alpha \longrightarrow S_{\alpha+1}$ be the multiplication map. Show the inequality $\mathrm{rk}(\Phi) \leq \min\{\binom{\alpha+1+n}{n}, n\binom{\alpha+n}{n} - ns\}$. Deduce that the ideal J has at least $\beta = \binom{\alpha+1+n}{n} - \min\{\binom{\alpha+1+n}{n}, n\binom{\alpha+n}{n} - ns\}$ minimal homogeneous generators in degree $\alpha + 1$.

The upshot of this discussion is that the ideal $\mathcal{I}^+(\mathbb{X})$ has exactly $\binom{\alpha+n}{n} - s$ minimal homogeneous generators in degree α, at least β minimal homogeneous generators in degree $\alpha + 1$, and no other minimal homogeneous generators. The Ideal Generation Conjecture says that the number of minimal homogeneous generators in degree $\alpha + 1$ should be exactly β for generic sets of points.

h) Write a CoCoA program `IGC_Points(...)` which constructs, for any given s, a set of s points in $\mathbb{P}^n_{\mathbb{Q}}$ satisfying IGC. Apply this program to as many pairs (s, n) as possible.

i) Let $\alpha \geq 2$ and $1 \leq r \leq \alpha$. Prove that there exist terms $t_1, \ldots, t_r \in \mathbb{T}^2_\alpha$ such that the multiplication map

$$\Phi : K[x_1, x_2]_1 \times (Kt_1 \oplus \cdots \oplus Kt_r) \longrightarrow K[x_1, x_2]_{\alpha+1}$$

satisfies $\mathrm{rk}(\Phi) = \min\{2r, \alpha + 2\}$.

j) Using i) and Theorem 6.2.12, prove that for every $s \geq 1$ there exists a projective point set $\mathbb{X} = \{p_1, \ldots, p_s\} \subset \mathbb{P}^2_K$ which has generic Hilbert function and satisfies IGC.

It can be shown that there exists a Zariski open subset of $(K^{n+1})^s$ which corresponds to projective point sets having generic Hilbert function and satisfying IGC. If this open set is non-empty, a generic set of s points satisfies IGC. In the remaining parts of this tutorial we want to generalize IGC. Recall that the degrees $d_{11} \leq d_{12} \leq \cdots \leq d_{1r_1}$ of the minimal homogeneous generators of the ideal $\mathcal{I}^+(\mathbb{X})$ form its degree sequence, and that its minimal graded free resolution has the shape

$$0 \to \bigoplus_{i=1}^{r_n} \overline{P}(-d_{ni}) \longrightarrow \cdots \longrightarrow \bigoplus_{i=1}^{r_2} \overline{P}(-d_{2i}) \longrightarrow \bigoplus_{i=1}^{r_1} \overline{P}(-d_{1i}) \longrightarrow \mathcal{I}^+(\mathbb{X}) \to 0$$

with sequences of integers $d_{j1} \leq d_{j1} \leq \cdots \leq d_{jr_j}$ (see Section 4.8). The **Minimal Resolution Conjecture (MRC)** predicts the values of these degree sequences for generic sets of points. In the following we examine an explicit version of this conjecture and use CoCoA to prove or disprove it in special cases.

To simplify the discussion, we let K be a field having infinitely many elements, and we assume that we have performed a linear change of coordinates such that the projective point set $\mathbb{X} = \{p_1, \ldots, p_s\} \subset \mathbb{P}^n_K$ satisfies $\mathbb{X} \cap \mathcal{Z}^+(x_0) = \emptyset$.

k) Prove that we have $d_{11} < d_{21} < \cdots < d_{n1}$.

l) *(This part requires some knowledge of homological algebra, in particular of Tutorial 33.)* For $i = 1, \ldots, n$, let $F_i^{\check{}}$ be the graded free module $F_i^{\check{}} = \bigoplus_{j=1}^{r_j} \overline{P}(d_{ij})$. Show that the dual sequence

$$0 \longrightarrow \overline{P} \longrightarrow F_1^{\check{}} \longrightarrow \cdots \longrightarrow F_n^{\check{}} \longrightarrow \mathrm{Ext}^n_{\overline{P}}(R, \overline{P}) \longrightarrow 0$$

is the minimal graded free resolution of the Ext-module $\mathrm{Ext}^n_{\overline{P}}(R, \overline{P})$. Deduce that we have $d_{nr_n} > d_{n-1r_{n-1}} > \cdots > d_{1r_1}$.

Hint: To show that $\mathrm{depth}_{\mathcal{I}^+(\mathbb{X})}(\overline{P}) = n$, embed $\mathbb{X}$ in a full design.

m) Write CoCoA functions `Alpha(...)`, `Ri(...)`, and `MGFRdegs(...)` which take the ideal $\mathcal{I}^+(\mathbb{X})$ and compute the numbers α, $\mathrm{ri}(\mathrm{HF}_{\mathbb{X}})$, and the list of lists of numbers

$$((d_{11}, \ldots, d_{1r_1}), \ldots, (d_{n1}, \ldots, d_{nr_n}))$$

n) Suppose that the projective point set $\mathbb{X}$ has generic Hilbert function. Using d) and Tutorial 64.a, show that $d_{nr_n} \in \{\alpha+n-1,\, \alpha+n\}$.
Hint: Prove that $\mathrm{ri}(\mathrm{HF}_{\mathbb{X}}) = d_{nr_n} - n$.

o) By combining m) and n), prove that the minimal graded free resolution of $\mathcal{I}^+(\mathbb{X})$ has the shape

$$0 \longrightarrow \overline{P}(-\alpha-n+1)^{a_n} \oplus \overline{P}(-\alpha-n)^{b_n} \longrightarrow \cdots \longrightarrow \overline{P}(-\alpha)^{a_1} \oplus \overline{P}(-\alpha-1)^{b_1} \longrightarrow \mathcal{I}^+(\mathbb{X}) \longrightarrow 0$$

if $\mathbb{X}$ has generic Hilbert function. Here the numbers a_i, b_i are non-negative integers.

p) Show that $\mathrm{ri}(\mathrm{HF}_{\mathbb{X}}) = \alpha - 1$ if and only if the number of points of $\mathbb{X}$ is a binomial coefficient of the form $s = \binom{\alpha-1+n}{n}$. Prove that in this case we have $b_1 = \cdots = b_n = 0$ and we can calculate the numbers a_i recursively just knowing the Hilbert function of $\mathbb{X}$.

q) Use p) to find the resolution of $s = \binom{2+n}{n}$ points in $\mathbb{P}^n$ which don't lie on a quadric hypersurface for $n = 2, 3, 4, \ldots$. What do you conjecture the resolution should be for all n? Use CoCoA to check your conjecture for as many n as possible!

r) Prove that if, for a generic set of points $\mathbb{X}$, the first syzygy module of $\mathcal{I}^+(\mathbb{X})$ begins in degree $\alpha+2$ (rather than degree $\alpha+1$), then all the remaining syzygy modules are generated in the highest degree possible. Conclude that $a_2 = \cdots a_n = 0$ and find formulas for the numbers $a_1, b_1, b_2, \ldots, b_n$.

It is time to provide the explicit statement of the Minimal Resolution Conjecture. Let $m = \frac{\alpha}{s}\binom{\alpha+n}{n} - \alpha$, and assume that s is different from $\binom{\alpha-1+n}{n}$. Then the Minimal Resolution Conjecture says that a generic set of s points satisfies $a_{m+1} = b_{m-1} = 0$.

s) *(This part involves some tricky calculations with binomial coefficients.)* Let $\mathbb{X}$ be a set of points with $\mathrm{ri}(\mathrm{HF}_{\mathbb{X}}) = \alpha$, and let $\delta = s - \binom{\alpha-1+n}{n}$. Show that $a_1 = \binom{\alpha+n}{n} - s$, $b_n = \delta$, and $a_i - b_{i-1} = \binom{\alpha-1+n}{\alpha-1+i}\binom{\alpha-2+i}{\alpha-1} - \delta\binom{n}{i-1}$ for $i = 2, \ldots, n$.

t) Implement a CoCoA function `ExBetti(...)` which computes the matrix $\binom{a_1 \cdots a_n}{b_1 \cdots b_n}$ expected by MRC for a generic set of s points.

u) Use CoCoA to verify MRC for small numbers of points in $\mathbb{P}^2_{\mathbb{Q}}$, $\mathbb{P}^3_{\mathbb{Q}}$ and $\mathbb{P}^4_{\mathbb{Q}}$. How far can you go?

v) Compute the minimal graded free resolutions of the homogeneous vanishing ideals of several randomly chosen sets of 11 points in $\mathbb{P}^6_{\mathbb{Q}}$ and check that they do not satisfy MRC. Can you do the same for 12 points in $\mathbb{P}^7_{\mathbb{Q}}$ and 13 points in $\mathbb{P}^8_{\mathbb{Q}}$? Can you find further exceptions to MRC?

Good resolutions are simply checks
that men draw on a bank
where they have no account.
(Oscar Wilde)

Tutorial 90: Error-Correcting Codes

The fact that our econometric models at the Fed,
the best in the world,
have been wrong for 14 straight quarters,
does not mean that they will not be right
in the 15^{th} quarter.
(Alan Greenspan)

The goal of coding theory is to transfer information efficiently and safely across a "noisy" channel, i.e. a channel which modifies some of the transmitted data. Examples of such information transfers are satellite transmissions and data storage on compact disks or other media. To achieve this goal, we first equip the message with a certain amount of redundant information. Then we transfer the resulting *code word*. The *received word* may contain errors. The number of positions in which it differs from the word we sent out is called its *Hamming distance* from that code word. Although these Hamming metric models may not be the best in the world, they will reconstruct the original message in many cases. Of course, even if this reconstruction has been right for 14 straight message words, this does not mean that it will be right for the 15^{th} word. Schematically, the basic setup looks as follows.

$$\textit{message} \longrightarrow \boxed{\text{encoder}} \overset{\substack{code\\word}}{\longrightarrow} \boxed{\text{channel}} \overset{\substack{received\\word}}{\longrightarrow} \boxed{\text{decoder}} \longrightarrow \textit{reconstruction}$$

Now we have to fill this abstract scheme with concrete contents. The first step is to divide the message into suitable units, called *words*, and to represent those words mathematically. For an alphabet, we use the elements of a finite field K. Then a word of length k is a tuple in K^k. The encoder performs an injective map $\varepsilon : K^k \longrightarrow K^n$ where n is the length of the code words. Accordingly, the decoder is a map $\delta : K^n \longrightarrow K^k$ such that $\delta \circ \varepsilon$ is the identity. The set $C = \varepsilon(K^k)$ is called the **code** and its elements are the **code words**.

Let $m \in K^k$ be the message word, let $c = \varepsilon(m) \in K^n$ be the code word sent out, and let $e \in K^n$ be the error introduced by the noisy channel. Thus the received word is $c + e$. If there exists a map δ with the property that $\delta(c + e) = m$ for all e having at most t non-zero entries, we say that the code C is **t-error correcting**. Naturally, we would like to correct as many errors as possible. The overhead we have introduced is the **redundancy** $n-k$ of the code. Thus a more precise formulation of our goal is that we want to find codes which correct many errors and have a small redundancy. So, let us see how many errors we can correct. Even if we will not always be right, we may take heart from the fact that economists have successfully predicted ten of the last three recessions.

To search for concrete "good" codes, we specialize further and consider linear encoders. Let p be a prime number, let $e > 0$, let $q = p^e$, and let

$K = \mathbb{F}_q$ be the field with q elements. A **linear code** C over K is a K-subvector space of K^n. The number n is called the **length** of C, and the number $k = \dim_K(C)$ is called the **dimension** of C.

Given a two tuples $v, w \in K^n$, we define their **Hamming distance** $\eta(v, w)$ as the number of non-zero entries of $v - w$. Then the **minimal distance** of C is $d = \min\{\eta(v, w) \mid v, w \in C,\ v \neq w\}$. Sometimes we combine the three basic numbers and say that C is an **[n,k,d]-code**.

a) Show that η has the following properties of a **metric** on K^n.
   1) We have $\eta(v, w) \geq 0$ for all $v, w \in K^n$ and $\eta(v, w) = 0$ if and only if $v = w$.
   2) The map η is symmetric, i.e. we have $\eta(v, w) = \eta(w, v)$ for all tuples $v, w \in K^n$.
   3) The map η satisfies the **triangle inequality**. This means that we have $\eta(u, w) \leq \eta(u, v) + \eta(v, w)$ for all tuples $u, v, w \in K^n$.

b) Prove that the minimal distance of a linear code C is the minimum of the numbers $\#\{i \mid c_i \neq 0\}$ where $(c_1, \ldots, c_n)$ ranges over the set of all non-zero code words.

c) Show that C is t-error correcting if $d \geq 2t + 1$.

d) Prove the **Singleton bound** $d \leq n - k + 1$. This implies that the error-correcting capability of a linear code is bounded by its redundancy.
   Hint: Delete the last $d - 1$ components of each code word and count the words of the resulting code.

One way of specifying a linear code is by giving a matrix $\mathcal{G} \in \mathrm{Mat}_{k,n}(K)$ whose rows form a K-basis of C. The matrix $\mathcal{G}$ is called a **generator matrix** of C.

g) Determine the minimum distance of the linear codes over $K = \mathbb{F}_2$ given by the following generator matrices.
   1) $\mathcal{G}_1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ ([4,2] cyclic code)
   2) $\mathcal{G}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ ([7,4] Hamming code)
   3) $\mathcal{G}_3 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ v_1 & v_2 & \cdots & v_{32} \end{pmatrix}$ where $\{v_1, \ldots, v_{32}\} = K^5$
   ([5,1] binary Reed-Muller code)

h) Write a CoCoA function `MinDist(...)` which takes the generator matrix of a linear code and computes its minimal distance. Use this function to check your results for the codes in g).

How can we find linear codes coming close to or attaining the Singleton bound? The following construction utilizes projective point sets. So, let $\mathbb{X}=\{p_1, \ldots, p_s\} \subseteq \mathbb{P}^n_K$ be a projective point set, let $R = K[x_0, \ldots, x_n]/\mathcal{I}^+(\mathbb{X})$ be its homogeneous coordinate ring, and let $1 \leq j < \mathrm{ri}(\mathrm{HF}_{\mathbb{X}})$. For every $i \in \{1, \ldots, s\}$, we write $p_i = (p_{i0} : \ldots : p_{in})$ with elements $p_{ik} \in K$. Then the image of the K-linear map $\varrho_j : R_j \longrightarrow K^s$ defined by the rule

$\varrho_j(f) = (f(p_{10}, \ldots, p_{1n}), \ldots, f(p_{s0}, \ldots, p_{sn}))$ is called the j^{th} **generalized Reed-Muller code** associated to $\mathbb{X}$ and is denoted by $C_j(\mathbb{X})$.

i) In the above setting, prove that $C_j(\mathbb{X})$ is a linear code of length s and dimension $k = \mathrm{HF}_{\mathbb{X}}(j)$.

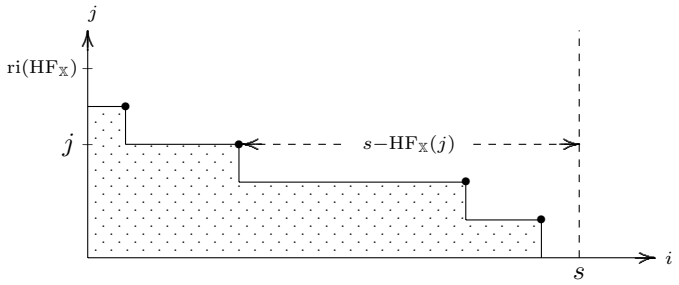
j) Determine which of the linear codes defined by the generator matrices in g) are generalized Reed-Muller codes.

Our next task is to compute the minimal distance of generalized Reed-Muller codes. For every $i \in \{1, \ldots, s-1\}$, we say that the projective point set $\mathbb{X}$ is **(i,j)-uniform** if every subset $\mathbb{Y} \subseteq \mathbb{X}$ consisting of $s - i$ points satisfies $\mathrm{HF}_{\mathbb{Y}}(j) = \mathrm{HF}_{\mathbb{X}}(j)$.

k) Show that $\mathbb{X}$ has the Cayley-Bacharach property if and only if $\mathbb{X}$ is $(1, \mathrm{ri}(\mathrm{HF}_{\mathbb{X}}) - 1)$-uniform.

l) Suppose that $\mathbb{X}$ is (i, j)-uniform. Prove that $\mathbb{X}$ is $(i-1, j)$-uniform and $(i, j-1)$-uniform.

m) Show that we have $i \leq s - \mathrm{HF}_{\mathbb{X}}(j)$ if $\mathbb{X}$ is (i, j)-uniform. Hence there exists an **region of uniformity** of $\mathbb{X}$ which looks as follows.



n) Prove that the minimal distance of $C_j(\mathbb{X})$ is

$$d = 1 + \max\{i \in \{1, \ldots, s-1\} \mid \mathbb{X} \text{ is } (i, j)\text{-uniform}\}$$

Hint: Show that $d \geq i + 1$ if and only if every $f \in R_j \setminus \{0\}$ vanishes at $\leq s - i - 1$ points of $\mathbb{X}$, and this is equivalent to $\mathbb{X}$ being (i, j)-uniform.

So, to find good codes we have to find projective point sets with high uniformity. Given a generator matrix, the encoder of a linear code is obviously easy to implement and very efficient. But what about the decoder? As it turns out, decoding linear codes is in general not that easy. In the last part of this tutorial we study the most common method, called **syndrome decoding**, which admits numerous optimizations.

Let $\mathcal{G} \in \mathrm{Mat}_{k,n}(K)$ be a generator matrix for a linear $[n, k, d]$-code C. A matrix $\mathcal{H} \in \mathrm{Mat}_{n-k,n}(K)$ is called a **parity check matrix** for C if it has rank $n - k$ and satisfies $\mathcal{G}\,\mathcal{H}^{\mathrm{tr}} = 0$.

o) Show that the code $C^{\perp} \subseteq K^n$ with generator matrix $\mathcal{H}$ consists of all tuples $(c_1, \ldots, c) \in K^n$ which satisfy $c_1 d_1 + \cdots + c_n d_n = 0$ for all $(d_1, \ldots, d_n) \in C$. The code $C^{\perp}$ is called the **dual code** of C.

p) Find the parity check matrices of the codes in g).
q) Suppose that $\mathcal{G}$ is **systematic**, i.e. that it has the form $\mathcal{G} = (\mathcal{I}_k \mid \mathcal{G}')$ with a matrix $\mathcal{G}' \in \mathrm{Mat}_{k,n-k}(K)$. Find a parity check matrix of C.

Let $\mathcal{H}$ be a parity check matrix for C, let $c \in C$ be a code word which has been sent, and let $v = c+e \in K^n$ be the received word. Then the element $v\,\mathcal{H}^{\mathrm{tr}}$ is called the **syndrome** of v. Given a fixed syndrome s, the set of all tuples $v \in K^n$ with that syndrome $s = v\,\mathcal{H}^{\mathrm{tr}}$ is called the **coset** of s. A tuple $\ell \in K^n$ with syndrome s and minimal Hamming distance $\eta(\ell, 0)$ is called a **coset leader** of s.

r) Show that the syndrome of a received word depends only on the error vector, and not on the code word which has been sent.
s) Assuming that $d \geq 2t+1$, prove that any coset containing a tuple $v \in K^n$ with $\eta(v, 0) \leq t$ has a unique coset leader. Give an example in which the coset leader is not unique.
t) Write a CoCoA function `CosetLeaders(...)` which takes $\mathcal{G}$ and computes the list of all pairs (s, ℓ) where ℓ is a coset leader of a syndrome s.
u) Let L be the list computed by the function `CosetLeaders(...)`, let $\mathcal{G}^*$ be a left inverse of $\mathcal{G}^{\mathrm{tr}}$, and let $v \in K^n$ be a received word. Consider the **Syndrome Decoding Algorithm** defined by the following instructions.
   1) Compute $s = v\,\mathcal{H}^{\mathrm{tr}}$ and use the list L to find all coset leaders of s.
   2) If there is more than one coset leader, return `"Reconstruction not unique"` and stop.
   3) Let ℓ be the unique coset leader, and let $c = v - \ell$. Return the tuple $m = \mathcal{G}^*\, c \in K^k$.

   Prove that if $d \geq 2t + 1$ and no more than t errors occurred in the transmission of a code word $c = \varepsilon(m)$, then the Syndrome Decoding Algorithm correctly reconstructs m.
v) Write a CoCoA function `SynDecode(...)` which implements the Syndrome Decoding Algorithm. Apply this function to the codes C_i defined by the matrices $\mathcal{G}_i$ in g) and the following words.
   1) C_1 and $v_1 = (0, 0, 0, 1)$
   2) C_2 and $v_2 = (1, 1, 0, 1, 1, 0, 1)$
   3) C_3 and $v_3 = (0, 1, 0, 1, 0, 1, \ldots, 0, 1)$

6.4 Border Bases

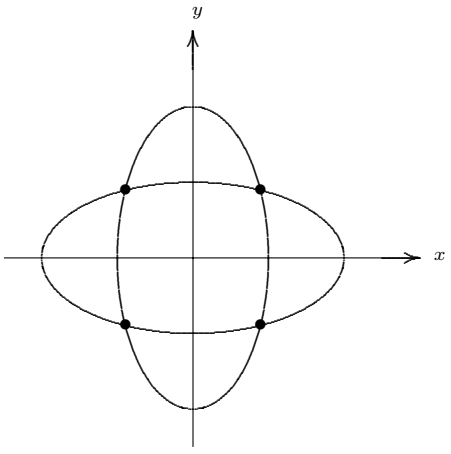
Given a choice between two theories,
take the one which is funnier.
(Anonymous)

After smoothly traversing together more than 700 pages of Gröbner basis territory, we are about to hit some obstacles. We have to confess that Gröbner bases are not the wholly sacred generating systems of an ideal we may have led you to believe. (The more sins you confess, the more books you will sell!) The following two examples highlight a couple of serious glitches.

Example 6.4.1. Consider the polynomial system

$$\begin{array}{rcrcl} f_1 & = & \frac{1}{4}\,x^2 + y^2 - 1 & = & 0 \\ f_2 & = & x^2 + \frac{1}{4}\,y^2 - 1 & = & 0 \end{array}$$

The intersection of $\mathcal{Z}(f_1)$ and $\mathcal{Z}(f_2)$ in $\mathbb{A}^2(\mathbb{C})$ consists of the four points $\mathbb{X} = \{(\pm\sqrt{4/5},\, \pm\sqrt{4/5})\}$.

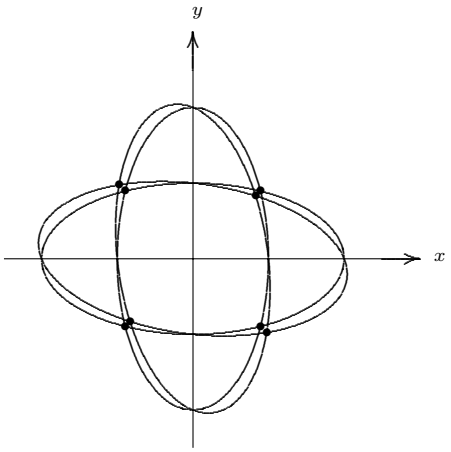


Using Gröbner basis theory, we describe this situation as follows. The set $\{x^2-\frac{4}{5},\, y^2-\frac{4}{5}\}$ is the reduced Gröbner basis of the ideal $I = (f_1, f_2) \subseteq \mathbb{C}[x, y]$ with respect to σ = `DegRevLex`. Therefore we have $\mathrm{LT}_\sigma(I) = (x^2,\, y^2)$, and the residue classes of the terms in $\mathbb{T}^2 \setminus \mathrm{LT}_\sigma\{I\} = \{1,\, x,\, y,\, xy\}$ form a $\mathbb{C}$-vector space basis of $\mathbb{C}[x, y]/I$.

Now consider the slightly perturbed polynomial system

$$\begin{array}{rcrcl} \tilde{f}_1 & = & \frac{1}{4}\,x^2 + y^2 + \varepsilon\,xy - 1 & = & 0 \\ \tilde{f}_2 & = & x^2 + \frac{1}{4}\,y^2 + \varepsilon\,xy - 1 & = & 0 \end{array}$$

where ε is a small number. The intersection of $\mathcal{Z}(\tilde{f}_1)$ and $\mathcal{Z}(\tilde{f}_2)$ consists of four perturbed points $\widetilde{\mathbb{X}}$ close to those in $\mathbb{X}$.



This time the ideal $\tilde{I} = (\tilde{f}_1, \tilde{f}_2)$ has the reduced σ-Gröbner basis

$$\{x^2 - y^2,\ xy + \tfrac{5}{4\varepsilon}\, y^2 - \tfrac{1}{\varepsilon},\ y^3 - \tfrac{16\varepsilon}{16\varepsilon^2 - 25}\, x + \tfrac{20}{16\varepsilon^2 - 25}\, y\}$$

Moreover, we have $\mathrm{LT}_\sigma(\tilde{I}) = (x^2,\ xy,\ y^3)$ and $\mathbb{T}^2 \setminus \mathrm{LT}_\sigma\{\tilde{I}\} = \{1,\ x,\ y,\ y^2\}$.

A *small* change in the coefficients of f_1 and f_2 has led to a *big* change in the Gröbner basis of (f_1, f_2) and in the associated vector space basis of $\mathbb{C}[x, y]/(f_1, f_2)$, although the zeros of the system have not changed much. Numerical analysts call this kind of unstable behaviour a *representation singularity.*

Example 6.4.2. Consider the ideal $I = (x^2 + xy + y^2,\ x^3,\ x^2y,\ xy^2,\ y^3)$ in $\mathbb{Q}[x, y]$. This ideal is symmetric with respect to swapping x and y. Since the leading term of $x^2 + xy + y^2$ is either x^2 or y^2, the ideal I has two possible leading term ideals, namely the ideals $J_1 = (x^2,\ xy^2,\ y^3)$ and $J_2 = (x^3,\ x^2y,\ y^2)$. Neither is symmetric. Thus they do not give rise to symmetric vector space bases of $\mathbb{Q}[x, y]/I$. However, the set of terms $\mathcal{O} = \{1,\ x,\ y,\ x^2,\ y^2\}$ is symmetric and represents a vector space basis of $\mathbb{Q}[x, y]/I$.

In other words, Gröbner bases *break* the symmetry! It is more natural to compute in $\mathbb{Q}[x, y]/I$ using a symmetric basis. Therefore we would like to find another system of generators of I which has properties similar to a Gröbner basis, but corresponds to the symmetric vector space basis $\mathcal{O}$ of $\mathbb{Q}[x, y]/I$ given above.

What can we do about this? We can introduce a new theory! In this section we describe the theory of border bases of zero-dimensional polynomial ideals. Its *raison d'être* is to address the above shortcomings of Gröbner bases. Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let $I \subseteq P$ be a zero-dimensional ideal. The basic idea of border basis theory is to describe a zero-dimensional

ring P/I by an order ideal of monomials $\mathcal{O}$ whose residue classes form a K-basis of P/I and by the multiplication table of this basis.

The advantages of using an order ideal rather than an arbitrary set of terms are manifold. For instance, we can define the *border* $\partial\mathcal{O}$ of $\mathcal{O}$ by $\partial\mathcal{O} = \bigcup_{i=1}^{n} x_i\mathcal{O}\backslash\mathcal{O}$. To describe the multiplicative structure of P/I, it suffices to know how products $x_i\,t \in \partial\mathcal{O}$ with $t \in \mathcal{O}$ can be decomposed in the form $x_i\,t \in \langle\mathcal{O}\rangle_K + I$. Moreover, by defining $\overline{\partial\mathcal{O}} = \mathcal{O}\cup\partial\mathcal{O}$ and $\partial^2\mathcal{O} = \partial(\overline{\partial\mathcal{O}})$ and repeating this procedure, we can introduce higher borders. Then the *index* of a term t with respect to $\mathcal{O}$ is the uniquely defined number such that $t \in \partial^i\mathcal{O}$. Although it is not quite as well behaved as the degree, it enables us to introduce the border form of a polynomial.

Having laid the foundations, we can build border basis theory according to the blueprint in Chapters 1 and 2. Let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal and $\partial\mathcal{O} = \{b_1, \ldots, b_\nu\}$ its border. A *border prebasis* consists of polynomials of the form $g_j = b_j - \sum_{i=1}^{\mu} \alpha_{ij}t_i$ with $\alpha_{ij} \in K$ and can be used for *border division* (see Proposition 6.4.11). It is a *border basis* if and only if the residue classes of $\{t_1, \ldots, t_\mu\}$ form a K-basis of P/I. If $\mathcal{O}$ represents a vector space basis of P/I, then an $\mathcal{O}$-border basis of I exists, is uniquely determined (see Proposition 6.4.17), and generates the ideal (see Proposition 6.4.15). Furthermore, it is then possible to define and compute normal forms with respect to $\mathcal{O}$.

In the second subsection we show that border bases can be characterized by special generation, generation of border form ideals, and confluence of the associated rewrite relations much as Gröbner bases are. They are also characterized by the fact that their associated formal multiplication matrices commute (see Theorem 6.4.30) and have their own "Buchberger criterion" (see Proposition 6.4.34). Finally, they allow us to overcome the shortcomings of Gröbner bases mentioned above (see Examples 6.4.22 and 6.4.14) and can be computed using the Border Basis Algorithm 6.4.36.

So, which theory is it going to be? Gröbner bases or border bases? We leave this choice to your personal sense of humour.

6.4.A Existence and Uniqueness of Border Bases

Let K be a field, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let $\mathbb{T}^n$ be the monoid of terms in P. The following kind of subset of $\mathbb{T}^n$ will be central to this section.

Definition 6.4.3. Let $\mathcal{O}$ be a non-empty subset of $\mathbb{T}^n$.

a) The **closure** of $\mathcal{O}$ is the set $\overline{\mathcal{O}}$ of all terms in $\mathbb{T}^n$ which divide one of the terms of $\mathcal{O}$.
b) The set $\mathcal{O}$ is called an **order ideal** if $\overline{\mathcal{O}} = \mathcal{O}$, i.e. $\mathcal{O}$ is closed under forming divisors.

Order ideals have many names in the literature. A collection of alternatives is contained in Subsection 0.5 of the introduction. We chose this name because it indicates that order ideals are the analogs of ideals in the theory of partially ordered sets. The complement of an order ideal is a monoideal of terms and vice versa. Given an order ideal, we construct further order ideals as follows.

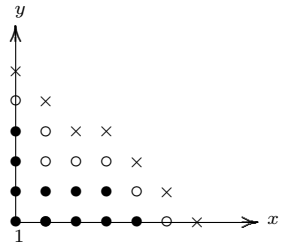
Definition 6.4.4. Let $\mathcal{O} \subseteq \mathbb{T}^n$ be an order ideal.

a) The **border** of $\mathcal{O}$ is the set $\partial\mathcal{O} = \mathbb{T}_1^n \cdot \mathcal{O} \setminus \mathcal{O} = (x_1\mathcal{O} \cup \ldots \cup x_n\mathcal{O}) \setminus \mathcal{O}$. The **first border closure** of $\mathcal{O}$ is the set $\overline{\partial\mathcal{O}} = \mathcal{O} \cup \partial\mathcal{O}$.

b) For every $k \geq 1$, we inductively define the $(k+1)^{\text{st}}$ **border** of $\mathcal{O}$ by $\partial^{k+1}\mathcal{O} = \partial(\overline{\partial^k\mathcal{O}})$ and the $(k+1)^{\text{st}}$ **border closure** of $\mathcal{O}$ by the rule $\overline{\partial^{k+1}\mathcal{O}} = \overline{\partial^k\mathcal{O}} \cup \partial^{k+1}\mathcal{O}$. For convenience, we let $\partial^0\mathcal{O} = \overline{\partial^0\mathcal{O}} = \mathcal{O}$.

The k^{th} border closure of an order ideal is an order ideal for every $k \geq 0$.

Example 6.4.5. Let $\mathcal{O} = \{1, x, y, x^2, xy, y^2, x^3, x^2y, y^3, x^4, x^3y\} \subset \mathbb{T}^2$. Then the set $\mathcal{O}$ is an order ideal. We visualize $\mathcal{O}$ and its first two borders as follows.



Let us collect some properties of borders and border closures.

Proposition 6.4.6. (Basic Properties of Borders)
Let $\mathcal{O} \subseteq \mathbb{T}^n$ be an order ideal.

a) For every $k \geq 0$, we have a disjoint union $\overline{\partial^k\mathcal{O}} = \bigcup_{i=0}^{k} \partial^i\mathcal{O}$. Consequently, we have a disjoint union $\mathbb{T}^n = \bigcup_{i=0}^{\infty} \partial^i\mathcal{O}$.

b) For every $k \geq 1$, we have $\partial^k\mathcal{O} = \mathbb{T}_k^n \cdot \mathcal{O} \setminus \mathbb{T}_{<k}^n \cdot \mathcal{O}$.

c) A term $t \in \mathbb{T}^n$ is divisible by a term in $\partial\mathcal{O}$ if and only if $t \in \mathbb{T}^n \setminus \mathcal{O}$.

Proof. First we show a). The definition of $\overline{\partial\mathcal{O}}$ yields $\overline{\partial\mathcal{O}} = \mathcal{O} \cup \mathbb{T}_1^n \cdot \mathcal{O}$. Inductively, it follows that $\overline{\partial^{k+1}\mathcal{O}} = \overline{\partial^k\mathcal{O}} \cup \mathbb{T}_1^n \cdot \overline{\partial^k\mathcal{O}} = \overline{\partial^k\mathcal{O}} \cup \mathbb{T}_{k+1}^n\mathcal{O}$. The second part of a) follows from the observation that every term is in $\overline{\partial^k\mathcal{O}}$ for some $k \geq 0$, and claim b) is a consequence of $\partial^{k+1}\mathcal{O} = \overline{\partial^{k+1}\mathcal{O}} \setminus \overline{\partial^k\mathcal{O}}$. Finally, claim c) holds because b) implies that $t \in \partial^k\mathcal{O}$ for some $k \geq 1$ is equivalent to the existence of a factorization $t = t't''$ with $\deg(t') = k - 1$ and $t'' \in \partial\mathcal{O}$. □

The disjoint union in part a) of this proposition allows us to measure the "distance" of a term from an order ideal as follows.

Definition 6.4.7. Let $\mathcal{O} \subseteq \mathbb{T}^n$ be an order ideal.

a) For every $t \in \mathbb{T}^n$, the unique number $k \in \mathbb{N}$ such that $t \in \partial^k \mathcal{O}$ is called the **index** of t with respect to $\mathcal{O}$ and is denoted by $\mathrm{ind}_{\mathcal{O}}(t)$.
b) For a polynomial $f \in P \setminus \{0\}$, we define the **index** of f with respect to $\mathcal{O}$ (or the $\mathcal{O}$**-index** of f) by $\mathrm{ind}_{\mathcal{O}}(f) = \max\{\mathrm{ind}_{\mathcal{O}}(t) \mid t \in \mathrm{Supp}(f)\}$.

Let us point out some useful properties of the index.

Proposition 6.4.8. *Let $\mathcal{O} \subseteq \mathbb{T}^n$ be an order ideal.*

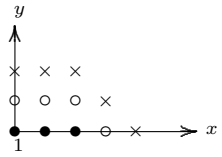
a) For a term $t \in \mathbb{T}^n$, the number $k = \mathrm{ind}_{\mathcal{O}}(t)$ is the smallest natural number such that $t = t't''$ with $t' \in \mathbb{T}^n_k$ and $t'' \in \mathcal{O}$.
b) Given two terms $t, t' \in \mathbb{T}^n$, we have $\mathrm{ind}_{\mathcal{O}}(t\,t') \leq \deg(t) + \mathrm{ind}_{\mathcal{O}}(t')$.
c) For non-zero polynomials $f, g \in P$ such that $f + g \neq 0$, we have the inequality $\mathrm{ind}_{\mathcal{O}}(f+g) \leq \max\{\mathrm{ind}_{\mathcal{O}}(f), \mathrm{ind}_{\mathcal{O}}(g)\}$.
d) For non-zero polynomials $f, g \in P$, we have the inequality

$$\mathrm{ind}_{\mathcal{O}}(f\,g) \leq \min\{\deg(f) + \mathrm{ind}_{\mathcal{O}}(g),\ \deg(g) + \mathrm{ind}_{\mathcal{O}}(f)\}$$

Proof. Claim a) follows from Proposition 6.4.6.b, and b) follows from a). Claim c) is a consequence of the inclusion $\mathrm{Supp}(f+g) \subseteq \mathrm{Supp}(f) \cup \mathrm{Supp}(g)$. Finally, claim d) follows from b) and $\mathrm{Supp}(fg) \subseteq \{t'\,t'' \mid t' \in \mathrm{Supp}(f),\ t'' \in \mathrm{Supp}(g)\}$. □

Unfortunately, using the $\mathcal{O}$-index to order terms has a serious drawback: this ordering is incompatible with multiplication, i.e. $\mathrm{ind}_{\mathcal{O}}(t) \leq \mathrm{ind}_{\mathcal{O}}(t')$ does not, in general, imply $\mathrm{ind}_{\mathcal{O}}(t\,t'') \leq \mathrm{ind}_{\mathcal{O}}(t'\,t'')$. Our next example is a case in point.

Example 6.4.9. Let $\mathcal{O} = \{1, x, x^2\} \subseteq \mathbb{T}^2$. Then $\mathcal{O}$ is an order ideal with border $\partial\mathcal{O} = \{y, xy, x^2y, x^3\}$. The following diagram illustrates the situation.



Multiplying the terms on both sides of $\mathrm{ind}_{\mathcal{O}}(x^2) < \mathrm{ind}_{\mathcal{O}}(y)$ by x^2, we get $\mathrm{ind}_{\mathcal{O}}(x^2 \cdot x^2) > \mathrm{ind}_{\mathcal{O}}(x^2 \cdot y)$. Similarly, multiplying the terms on both sides of $\mathrm{ind}_{\mathcal{O}}(y) = \mathrm{ind}_{\mathcal{O}}(x^2y)$ by x, we get $\mathrm{ind}_{\mathcal{O}}(x \cdot y) < \mathrm{ind}_{\mathcal{O}}(x \cdot x^2y)$.

From now on we let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be a finite order ideal in $\mathbb{T}^n$, and we let $\partial\mathcal{O} = \{b_1, \ldots, b_\nu\}$ be its border. We shall use the residue classes of the terms in $\mathcal{O}$ as a K-basis of the residue class ring of P modulo some zero-dimensional ideal. For the zero-dimensional ideal, we shall look for a system of generators which has the following shape.

Definition 6.4.10. A set of polynomials $G = \{g_1, \ldots, g_\nu\}$ is called an **$\mathcal{O}$-border prebasis** if the polynomials have the form $g_j = b_j - \sum_{i=1}^{\mu} \alpha_{ij} t_i$ with $\alpha_{ij} \in K$ for $1 \leq i \leq \mu$ and $1 \leq j \leq \nu$.

Border prebases are already sufficient to perform polynomial division with remainder. The following algorithm provides a fundamental tool in working with border prebases.

Proposition 6.4.11. (The Border Division Algorithm)
Let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal in $\mathbb{T}^n$, let $\partial\mathcal{O} = \{b_1, \ldots, b_\nu\}$ be its border, and let $\{g_1, \ldots, g_\nu\}$ be an $\mathcal{O}$-border prebasis. Given a polynomial $f \in P$, consider the following sequence of instructions.

1) Let $f_1 = \cdots = f_\nu = 0$, $c_1 = \cdots = c_\mu = 0$, and $h = f$.
2) If $h = 0$, return $(f_1, \ldots, f_\nu, c_1, \ldots, c_\mu)$ and stop.
3) If $\mathrm{ind}_{\mathcal{O}}(h) = 0$ then write $h = c_1 t_1 + \cdots + c_\mu t_\mu$ with $c_1, \ldots, c_\mu \in K$. Return $(f_1, \ldots, f_\nu, c_1, \ldots, c_\mu)$ and stop.
4) If $\mathrm{ind}_{\mathcal{O}}(h) > 0$ then let $h = a_1 h_1 + \cdots + a_s h_s$ with $a_1, \ldots, a_s \in K \setminus \{0\}$ and $h_1, \ldots, h_s \in \mathbb{T}^n$ such that $\mathrm{ind}_{\mathcal{O}}(h_1) = \mathrm{ind}_{\mathcal{O}}(h)$. Determine the smallest index $i \in \{1, \ldots, \nu\}$ for which h_1 factors as $h_1 = t' b_i$ with a term $t' \in \mathbb{T}^n$ of degree $\mathrm{ind}_{\mathcal{O}}(h) - 1$. Subtract $a_1 t' g_i$ from h, add $a_1 t'$ to f_i, and continue with step 2).

This is an algorithm which returns a tuple $(f_1, \ldots, f_\nu, c_1, \ldots, c_\mu) \in P^\nu \times K^\mu$ such that

$$f = f_1 g_1 + \cdots + f_\nu g_\nu + c_1 t_1 + \cdots + c_\mu t_\mu$$

and $\deg(f_i) \leq \mathrm{ind}_{\mathcal{O}}(f) - 1$ for all $i \in \{1, \ldots, \nu\}$ with $f_i g_i \neq 0$. This representation does not depend on the choice of the term h_1 in step 4).

Proof. First we show that the instructions can be executed. In step 3) the fact that $\mathrm{ind}_{\mathcal{O}}(h) = 0$ implies $\mathrm{Supp}(h) \subseteq \mathcal{O}$. In step 4) we write h as a linear combination of terms and note that at least one of them, say h_1, has to have index $k = \mathrm{ind}_{\mathcal{O}}(h) > 0$. By Proposition 6.4.8.a, there is a factorization $h_1 = \tilde{t}\, t_i$ with $\tilde{t} \in \mathbb{T}^n_k$ and $t_i \in \mathcal{O}$, and there is no such factorization with a term $\tilde{t}$ of smaller degree. Since $k > 0$, we can write $\tilde{t} = t' x_j$ for some $t' \in \mathbb{T}^n$ and $j \in \{1, \ldots, n\}$. Then we have $\deg(t') = k - 1$, and the fact that $\tilde{t}$ has the smallest possible degree implies $x_j\, t_i \in \partial\mathcal{O}$. Thus we see that $h_1 = t'\,(x_j\, t_i) = t'\, b_k$ for some $b_k \in \partial\mathcal{O}$.

Next we prove termination. We show that step 4) is performed only finitely many times. Let us investigate the subtraction $h - a_1 t' g_i$ in step 4). By definition, there is a representation $g_i = b_i - \sum_{k=1}^{\mu} \alpha_{ki} t_k$ such that $\alpha_{ki} \in K$ for $k = 1, \ldots, \mu$. Hence the subtraction becomes

$$h - a_1 t' g_i = a_1 h_1 + \ldots + a_s h_s - a_1 t' b_i + a_1 t' \sum_{k=1}^{\mu} \alpha_{ki} t_k$$

Now, since we have $a_1 h_1 = a_1 t' b_i$, a term of index $\mathrm{ind}_{\mathcal{O}}(h)$ is removed from h and replaced by terms of the form $t'\, t_\ell \in \overline{\partial^{k-1}\mathcal{O}}$ which have strictly smaller

index. The algorithm terminates after finitely many steps because there are only finitely many terms of index smaller or equal to that of a given term.

Finally, we prove correctness. To this end, we show that the equation

$$f = h + f_1 g_1 + \cdots + f_\nu g_\nu + c_1 t_1 + \cdots + c_\mu t_\mu$$

is an invariant of the algorithm. It is satisfied at the end of step 1). A polynomial f_i is changed only in step 4). There the subtraction $h - a_1 t' g_i$ is compensated by the addition $(f_i + a_1 t')g_i$. The constants $c_1, \ldots, c_\mu$ are changed only in step 3) in which h is replaced by $c_1 t_1 + \ldots + c_\mu t_\mu$. When the algorithm stops, we have $h = 0$. This proves the stated representation of f.

The additional claim that this representation does not depend on the choice of h_1 in step 4) follows from the observation that h_1 is replaced by terms of strictly smaller index. Thus the different executions of step 4) corresponding to the reduction of several terms of a given index in h do not interfere with one another. Hence the final result, after all those terms have been rewritten, is independent of the order in which they are handled. □

Notice that the representation computed by the Border Division Algorithm is *optimal* in the sense that for every $t \in \mathrm{Supp}(f_i)$ we have $\mathrm{ind}_{\mathcal{O}}(tb_i) = \deg(t) + 1$ and $\mathrm{ind}_{\mathcal{O}}(t(g_i - b_i)) \leq \deg(t)$. Let us try out the Border Division Algorithm in a concrete example.

Example 6.4.12. Let $\mathcal{O} = \{t_1, t_2, t_3\} \subseteq \mathbb{T}^2$ be the order ideal given by $t_1 = 1$, $t_2 = x$, and $t_3 = y$. The border of $\mathcal{O}$ is $\partial\mathcal{O} = \{b_1, b_2, b_3\}$ with $b_1 = x^2$, $b_2 = xy$, and $b_3 = y^2$. The polynomials $g_1 = x^2 + x + 1$, $g_2 = xy + y$, and $g_3 = y^2 + x + 1$ constitute an $\mathcal{O}$-border prebasis. We want to divide the polynomial $f = x^3y^2 - xy^2 + x^2 + 2$ by this $\mathcal{O}$-border prebasis.

For easy reference, the next three borders are $\partial^2\mathcal{O} = \{x^3, x^2y, xy^2, y^3\}$, $\partial^3\mathcal{O} = \{x^4, x^3y, x^2y^2, xy^3, y^4\}$, and $\partial^4\mathcal{O} = \{x^5, x^4y, x^3y^2, x^2y^3, xy^4, y^5\}$. We apply the Border Division Algorithm and follow its steps.

1) Let $f_1 = f_2 = f_3 = 0$, $c_1 = c_2 = c_3 = 0$, and $h = x^3y^2 - xy^2 + x^2 + 2$. The $\mathcal{O}$-indices of the terms in $\mathrm{Supp}(h)$ are 4,2,1 and 0, respectively, so h has index 4.
4) We have $x^3y^2 = xy^2 \cdot b_1$ with $\deg xy^2 = \mathrm{ind}(h) - 1$. Thus we let $f_1 = xy^2$ and $h = x^3y^2 - xy^2 + x^2 + 2 - xy^2(x^2 + x + 1)$. The terms in the support of $h = -x^2y^2 - 2xy^2 + x^2 + 2$ have $\mathcal{O}$-indices 3,2,1 and 0, respectively.
4) We have $x^2y^2 = y^2 \cdot b_1$ with $\deg y^2 = \mathrm{ind}(h) - 1$. Add $-y^2$ to f_1 to obtain $f_1 = xy^2 - y^2$, and let $h = -x^2y^2 - 2xy^2 + x^2 + 2 + y^2(x^2 + x + 1)$. The terms in the support of $h = -xy^2 + x^2 + y^2 + 2$ have $\mathcal{O}$-indices 2,1,1 and 0, respectively.
4) We have $xy^2 = y \cdot b_2$ with $\deg y = \mathrm{ind}(h) - 1$. Let $f_2 = -y$, and let $h = -xy^2 + x^2 + y^2 + 2 + y(xy + y)$. The terms in the support of the polynomial $h = x^2 + 2y^2 + 2$ have $\mathcal{O}$-indices 1,1 and 0, respectively.
4) We have $x^2 = 1 \cdot b_1$ with $\deg 1 = \mathrm{ind}(h) - 1$. Add 1 to f_1 to obtain $f_1 = xy^2 - y^2 + 1$, and let $h = x^2 + 2y^2 + 2 - 1(x^2 + x + 1)$. The terms in the support of $h = 2y^2 - x + 1$ have $\mathcal{O}$-indices 1,0 and 0, respectively.

4) We have $y^2 = 1 \cdot b_3$ with $\deg 1 = \operatorname{ind}(h) - 1$. Add 2 to f_3 to obtain $f_3 = 2$, and let $h = 2y^2 - x + 1 - 2(y^2 + x + 1)$. The terms in the support of $h = -3x - 1$ have $\mathcal{O}$-indices 0 and 0. Thus we have $\operatorname{ind}_{\mathcal{O}}(h) = 0$.
3) We have $h = -1 \cdot t_1 - 3 \cdot t_2 + 0 \cdot t_3$. The algorithm returns the tuple $(xy^2 - y^2 + 1, -y, 2, 1, -3, 0)$ and stops.

Altogether, we have computed the representation

$$f = (xy^2 - y^2 + 1)g_1 - y\,g_2 + 2\,g_3 - 1\,t_1 - 3\,t_2 + 0\,t_3$$

If we perform the algorithm with respect to the tuple $(g'_1, g'_2, g'_3) = (g_3, g_2, g_1)$, it computes the representation

$$\begin{aligned} f &= (x^3 + x)g'_1 - 1\,g'_2 + (x^2 + 2)\,g'_3 + 1\,t_1 - 3\,t_2 - 1\,t_3 \\ &= (x^2 + 2)g_1 - 1\,g_2 + (x^3 + x)\,g_3 + 0\,t_1 + 1\,t_2 - 1\,t_3 \end{aligned}$$

This shows that the order of the polynomials in the $\mathcal{O}$-border prebasis does affect the outcome of the Border Division Algorithm.

Just as we did with the Division Algorithm in Section 1.6, we use the result of the Border Division Algorithm to define the **normal $\mathcal{O}$-remainder** $\operatorname{NR}_{\mathcal{O},\mathcal{G}}(f) = c_1 t_1 + \cdots + c_\mu t_\mu$ of a polynomial f with respect to the tuple $\mathcal{G} = (g_1, \ldots, g_\nu)$. In the above example we have $\operatorname{NR}_{\mathcal{O},\mathcal{G}}(f) = -3x - 1$ and $\operatorname{NR}_{\mathcal{O},\mathcal{G}'}(f) = x - y$.

The elements f and $\operatorname{NR}_{\mathcal{O},\mathcal{G}}(f)$ represent the same residue class in the ring $P/(g_1, \ldots, g_\nu)$. In particular, the residue classes of the elements of $\mathcal{O}$ generate the K-vector space $P/(g_1, \ldots, g_\nu)$. It follows from the above example that this system of generators is not necessarily a basis. In fact, we have $4x - y + 1 = \operatorname{NR}_{\mathcal{O},\mathcal{G}'}(f) - \operatorname{NR}_{\mathcal{O},\mathcal{G}}(f) \in (g_1, \ldots, g_\nu)$. So, it is natural to introduce the following notion.

Definition 6.4.13. Let $G = \{g_1, \ldots, g_\nu\}$ be an $\mathcal{O}$-border prebasis, let $\mathcal{G}$ be the tuple $(g_1, \ldots, g_\nu)$, and let $I \subseteq P$ be an ideal containing G. The set G or the tuple $\mathcal{G}$ is called an **$\mathcal{O}$-border basis** of I if one of the following equivalent conditions is satisfied.

a) The residue classes $\overline{\mathcal{O}} = \{\bar{t}_1, \ldots, \bar{t}_\mu\}$ form a K-vector space basis of P/I.
b) We have $I \cap \langle \mathcal{O} \rangle_K = \{0\}$.
c) We have $P = I \oplus \langle \mathcal{O} \rangle_K$.

Border bases provide us with enough flexibility to be able to keep the symmetry in Example 6.4.2.

Example 6.4.14. Let $P = \mathbb{Q}[x, y]$ and $I = (x^2 + xy + y^2,\ x^3,\ x^2y,\ xy^2,\ y^3)$. The set $\mathcal{O} = \{1, x, y, x^2, y^2\}$ is an order ideal consisting of $\dim_K(P/I) = 5$ terms. Since we have $\partial\mathcal{O} = \{x^3, x^2y, xy, xy^2, y^3\}$, the polynomials $g_1 = x^3$, $g_2 = x^2y$, $g_3 = xy + x^2 + y^2$, $g_4 = xy^2$, and $g_5 = y^3$ form an $\mathcal{O}$-border prebasis of I. Moreover, the conditions of the definition are satisfied because I is homogeneous and condition c) can be checked degree-by-degree. Thus the set $G = \{g_1, \ldots, g_5\}$ is an $\mathcal{O}$-border basis of I.

Now we show that the definition implicitly contains the fact that an $\mathcal{O}$-border basis of I actually generates I.

Proposition 6.4.15. *Let G be an $\mathcal{O}$-border basis of an ideal $I \subseteq P$. Then the ideal I is generated by G.*

Proof. By definition, we have $(g_1, \ldots, g_\nu) \subseteq I$. To prove the converse inclusion, let $f \in I$. Using the Border Division Algorithm 6.4.11, the polynomial f can be expanded as $f = f_1 g_1 + \ldots + f_\nu g_\nu + c_1 t_1 + \ldots + c_\mu t_\mu$, where $f_1, \ldots, f_\nu \in P$ and $c_1, \ldots, c_\mu \in K$. This implies the equality of residue classes $0 = \bar{f} = c_1 \bar{t}_1 + \ldots + c_\mu \bar{t}_\mu$ in P/I. By assumption, the residue classes $\bar{t}_1, \ldots, \bar{t}_\mu$ are K-linearly independent. Hence $c_1 = \ldots = c_\mu = 0$, and the expansion of f turns out to be $f = f_1 g_1 + \ldots + f_\nu g_\nu$. □

Having defined a new mathematical object, we look for its existence and possibly its uniqueness. A necessary condition for the existence of an $\mathcal{O}$-border basis of I is clearly given by $\#\mathcal{O} = \dim_K(P/I)$. However, our next example shows that this condition is not sufficient.

Example 6.4.16. Let $P = \mathbb{Q}[x, y]$, and let I be the vanishing ideal of the set of five points $\mathbb{X} = \{(0,0), (0,-1), (1,0), (1,1), (-1,1)\}$ in $\mathbb{A}^2_{\mathbb{Q}}$. Then we have $\dim_K(P/I) = 5$. In $\mathbb{T}^2$ the following order ideals contain five elements:

$$\mathcal{O}_1 = \{1, x, x^2, x^3, x^4\},\ \mathcal{O}_2 = \{1, x, x^2, x^3, y\},\ \mathcal{O}_3 = \{1, x, x^2, y, y^2\}$$
$$\mathcal{O}_4 = \{1, x, x^2, y, xy\},\ \mathcal{O}_5 = \{1, x, y, y^2, y^3\},\ \mathcal{O}_6 = \{1, y, y^2, y^3, y^4\}$$
$$\mathcal{O}_7 = \{1, x, y, xy, y^2\}$$

Not all of these are suitable for border bases of I. For example, the residue classes of the elements of $\mathcal{O}_1$ cannot form a K-vector space basis of P/I, since $x^3 - x \in I$. Similarly, the residue classes of the elements of $\mathcal{O}_6$ cannot form a K-vector space basis of P/I, since $y^3 - y \in I$.

Proposition 6.4.17. (Existence and Uniqueness of Border Bases) *Let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal, let $I \subseteq P$ be a zero-dimensional ideal, and assume that the residue classes of the elements of $\mathcal{O}$ form a K-vector space basis of P/I.*

a) There exists a unique $\mathcal{O}$-border basis of I.
b) Let G be an $\mathcal{O}$-border prebasis whose elements are in I. Then G is the $\mathcal{O}$-border basis of I.
c) Let k be the field of definition of I. Then the $\mathcal{O}$-border basis of I is contained in $k[x_1, \ldots, x_n]$.

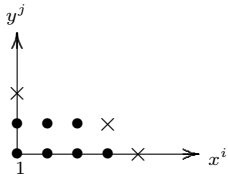
Proof. First we prove a). Let $\partial\mathcal{O} = \{b_1, \ldots, b_\nu\}$. For every $i \in \{1, \ldots, \nu\}$, the hypothesis implies that the residue class of b_i in P/I is linearly dependent on the residue classes of the elements of $\mathcal{O}$. Therefore I contains a polynomial of the form $g_i = b_i - \sum_{j=1}^{\mu} \alpha_{ij} t_j$ with $\alpha_{ij} \in K$. Then $G = \{g_1, \ldots, g_\nu\}$ is an

$\mathcal{O}$-border prebasis, and hence an $\mathcal{O}$-border basis of I by Definition 6.4.13. Let $G' = \{g'_1, \ldots, g'_\nu\}$ be another $\mathcal{O}$-border basis of I. Suppose there exists an index $i \in \{1, \ldots, \nu\}$ such that $g'_i = b_i - \sum_{j=1}^{\mu} \alpha'_{ij} t_j$ with $\alpha'_{ij} \neq \alpha_{ij}$ for some index $j \in \{1, \ldots, \mu\}$, then $g_i - g'_i$ is a non-zero polynomial in I with support in $\mathcal{O}$. This contradicts the hypothesis and proves a).

Next we show b). By Definition 6.4.13, it suffices to observe that the set G is an $\mathcal{O}$-border basis of I and to apply a). Finally, we prove claim c). Let $P' = k[x_1, \ldots, x_n]$ and $I' = I \cap P'$. Given a term ordering σ, the ideals I and I' have the same reduced σ-Gröbner basis by Lemma 2.4.16. Hence we have $\mathbb{T}^n \setminus \mathrm{LT}_\sigma\{I\} = \mathbb{T}^n \setminus \mathrm{LT}_\sigma\{I'\}$, and therefore $\dim_k(P'/I') = \dim_K(P/I)$. The elements of $\mathcal{O}$ are contained in P', and they are linearly independent modulo I'. Therefore their residue classes form a k-vector space basis of P'/I'. Let G' be the $\mathcal{O}$-border basis of I'. Then G' is an $\mathcal{O}$-border prebasis whose elements are contained in I. Thus the claim follows from b). □

Does a given zero-dimensional ideal possess a border basis at all? Using part a) of the proposition, we can rephrase this question as follows: Given a zero-dimensional ideal I, are there order ideals such that the residue classes of their elements form a K-vector space basis of P/I? The answer is yes, which we are going to show with the help of Gröbner bases.

Given an order ideal $\mathcal{O} \subset \mathbb{T}^n$, its complement $\mathbb{T}^n \setminus \mathcal{O}$ is the set of terms of a monomial ideal. Recall that every monomial ideal has a unique minimal set of generators (see Proposition 1.3.11). The elements of the minimal set of generators of the monomial ideal corresponding to $\mathbb{T}^n \setminus \mathcal{O}$ are called the **corners** of $\mathcal{O}$. A picture illustrates the appropriateness of this name.



Our next proposition helps us clarify the relationship between Gröbner bases and border bases of a zero-dimensional polynomial ideal.

Proposition 6.4.18. *Let σ be a term ordering on $\mathbb{T}^n$, and let $\mathcal{O}_\sigma(I)$ be the order ideal $\mathbb{T}^n \setminus \mathrm{LT}_\sigma\{I\}$. Then there exists a unique $\mathcal{O}_\sigma(I)$-border basis G of I, and the reduced σ-Gröbner basis of I is the subset of G corresponding to the corners of $\mathcal{O}_\sigma(I)$.*

Proof. By Macaulay's Basis Theorem 1.5.7, the residue classes of the elements in $\mathcal{O}_\sigma(I)$ form a K-vector space basis of P/I. Thus Proposition 6.4.17.a implies the existence and uniqueness of the $\mathcal{O}_\sigma(I)$-border basis of I.

To prove the second claim, we let $b \in \mathbb{T}^n \setminus \mathcal{O}_\sigma(I)$ be a corner of $\mathcal{O}_\sigma(I)$. The element of the reduced σ-Gröbner basis of I with leading term b has the form $b - \mathrm{NF}_{\sigma,I}(b)$, where $\mathrm{NF}_{\sigma,I}(b)$ is contained in the span of $\mathcal{O}_\sigma(I)$. Since the $\mathcal{O}_\sigma(I)$-border basis of I is unique, this Gröbner basis element coincides with the border basis element corresponding to b. □

To summarize the discussion, the ideal I does not necessarily have an $\mathcal{O}$-border basis for every order ideal $\mathcal{O}$ consisting of $\dim_K(P/I)$ terms, but there is always an $\mathcal{O}$-border basis for $\mathcal{O} = \mathbb{T}^n \setminus \mathrm{LT}_\sigma\{I\}$ where σ is some term ordering. However, Examples 6.4.2 and 6.4.14 show that not every border basis of I arises from a term ordering. In this sense, the theory of border bases of zero-dimensional ideals generalizes the theory of their Gröbner bases.

The following proposition shows that, when we divide by a border basis, the normal remainder does not depend on the order of the elements.

Proposition 6.4.19. *Let $\mathcal{G} = (g_1, \ldots, g_\nu)$ be the $\mathcal{O}$-border basis of an ideal $I \subseteq P$, let $\pi : \{1, \ldots, \nu\} \longrightarrow \{1, \ldots, \nu\}$ be a permutation, and let $\mathcal{G}' = (g_{\pi(1)}, \ldots, g_{\pi(\nu)})$ be the corresponding permutation of the tuple $\mathcal{G}$. Then we have $\mathrm{NR}_{\mathcal{O},\mathcal{G}}(f) = \mathrm{NR}_{\mathcal{O},\mathcal{G}'}(f)$ for every polynomial $f \in P$.*

Proof. The Border Division Algorithm applied to $\mathcal{G}$ and $\mathcal{G}'$, respectively, yields representations

$$f = f_1 g_1 + \cdots + f_\nu g_\nu + \mathrm{NR}_{\mathcal{O},\mathcal{G}}(f) = f'_1 g_{\pi(1)} + \cdots + f'_\nu g_{\pi(\nu)} + \mathrm{NR}_{\mathcal{O},\mathcal{G}'}(f)$$

where $f_i, f'_j \in P$. Therefore we have $\mathrm{NR}_{\mathcal{O},\mathcal{G}}(f) - \mathrm{NR}_{\mathcal{O},\mathcal{G}'}(f) \in \langle \mathcal{O} \rangle_K \cap I$. The hypothesis that I has an $\mathcal{O}$-border basis implies $\langle \mathcal{O} \rangle_K \cap I = \{0\}$. Hence the claim follows. □

This result allows us to generalize the concept of a normal form to border basis theory.

Definition 6.4.20. Let $G = \{g_1, \ldots, g_\nu\}$ be the $\mathcal{O}$-border basis of I. The **normal form** of a polynomial $f \in P$ with respect to $\mathcal{O}$ is the polynomial $\mathrm{NF}_{\mathcal{O},I}(f) = \mathrm{NR}_{\mathcal{O},\mathcal{G}}(f)$.

The normal form $\mathrm{NF}_{\mathcal{O},I}(f)$ of $f \in P$ can be calculated by dividing f by the $\mathcal{O}$-border basis of I. It is zero if and only if $f \in I$. Further basic properties of normal forms are collected in the following proposition.

Proposition 6.4.21. (Basic Properties of Normal Forms)
Let $\mathcal{O}$ be an order ideal, let $I \subseteq P$ be an ideal which has an $\mathcal{O}$-border basis, let $a_1, a_2 \in K$, and let $f, f_1, f_2 \in P$.

a) If there exists a term ordering σ such that $\mathcal{O} = \mathcal{O}_\sigma(I)$, we have $\mathrm{NF}_{\mathcal{O},I}(f) = \mathrm{NF}_{\sigma,I}(f)$.
b) We have $\mathrm{NF}_{\mathcal{O},I}(a_1 f_1 + a_2 f_2) = a_1 \mathrm{NF}_{\mathcal{O},I}(f_1) + a_2 \mathrm{NF}_{\mathcal{O},I}(f_2)$.
c) We have $\mathrm{NF}_{\mathcal{O},I}(\mathrm{NF}_{\mathcal{O},I}(f)) = \mathrm{NF}_{\mathcal{O},I}(f)$.

d) We have $\mathrm{NF}_{\mathcal{O},I}(f_1\, f_2) = \mathrm{NF}_{\mathcal{O},I}\big(\mathrm{NF}_{\mathcal{O},I}(f_1)\ \mathrm{NF}_{\mathcal{O},I}(f_2)\big)$.

Proof. Claim a) follows because both $\mathrm{NF}_{\mathcal{O},I}(f)$ and $\mathrm{NF}_{\sigma,I}(f)$ are equal to the uniquely determined polynomial in $f + I$ whose support is contained in $\mathcal{O}$. Claims b), c), and d) follow from the same uniqueness. □

Before we continue to examine border bases theory in greater detail, let us come back to one of the starting questions of this section: are border bases numerically stable? Let us reconsider Example 6.4.1.

Example 6.4.22. Let $P = \mathbb{Q}[x,y]$, let $I = (\frac{1}{4}\,x^2 + y^2 - 1,\ x^2 + \frac{1}{4}\,y^2 - 1)$, and let $\tilde{I} = (\frac{1}{4}\,x^2 + y^2 + \varepsilon\,xy - 1,\ x^2 + \frac{1}{4}\,y^2 + \varepsilon\,xy - 1)$ with a small number ε. Then both I and $\tilde{I}$ have a border basis with respect to $\mathcal{O} = \{1, x, y, xy\}$. The border of $\mathcal{O}$ is $\partial\mathcal{O} = \{x^2, x^2y, xy^2, y^2\}$. The $\mathcal{O}$-border basis of I is

$$\{x^2 - \tfrac{4}{5},\ x^2y - \tfrac{4}{5}y,\ xy^2 - \tfrac{4}{5}x,\ y^2 - \tfrac{4}{5}\}$$

The $\mathcal{O}$-border basis of $\tilde{I}$ is

$$\begin{aligned}&\{x^2 + \tfrac{4}{5}\,\varepsilon xy - \tfrac{4}{5},\ x^2y - \tfrac{16\varepsilon}{16\varepsilon^2-25}\,x + \tfrac{20}{16\varepsilon^2-25}\,y,\\ &xy^2 + \tfrac{20}{16\varepsilon^2-25}\,x - \tfrac{16\varepsilon}{16\varepsilon^2-25}\,y,\ y^2 + \tfrac{4}{5}\,\varepsilon xy - \tfrac{4}{5}\}\end{aligned}$$

When we vary the coefficients of xy in the two generators from zero to ε, we see that one border bases changes continuously into the other (see also Exercise 2). Thus the border basis behaves numerically stable under small perturbations of the coefficient of xy.

In addition, this example is another instance of the phenomenon that Gröbner bases do not preserve the symmetry of the given system of equations, whereas some border bases do.

6.4.B Characterizations of Border Bases

In this subsection we develop the analogy between border bases and Gröbner bases further. More precisely, we characterize border bases in several ways which mimic the characterizations of Gröbner bases in Chapter 2. But we shall also encounter a characterization of border bases for which no Gröbner basis analog exists. We continue to use the notation and hypotheses introduced above. In particular, let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal in $\mathbb{T}^n$, let $\partial\mathcal{O} = \{b_1, \ldots, b_\nu\}$ be its border, let $G = \{g_1, \ldots, g_\nu\}$ be an $\mathcal{O}$-border prebasis, let $\mathcal{G}$ be the tuple $(g_1, \ldots, g_\nu)$, and let $I \subseteq P$ be the zero-dimensional ideal generated by G.

The following result is the border basis version of Proposition 2.1.1.

Proposition 6.4.23. (Border Bases and Special Generation)
In the above setting, the set G is an $\mathcal{O}$-border basis of I if and only if the following equivalent conditions are satisfied.

A_1. *For every* $f \in I \setminus \{0\}$, *there exist polynomials* $f_1, \ldots, f_\nu \in P$ *such that* $f = f_1 g_1 + \cdots + f_\nu g_\nu$ *and* $\deg(f_i) \leq \operatorname{ind}_\mathcal{O}(f) - 1$ *whenever* $f_i \neq 0$.

A_2. *For every* $f \in I \setminus \{0\}$, *there exist polynomials* $f_1, \ldots, f_\nu \in P$ *such that* $f = f_1 g_1 + \cdots + f_\nu g_\nu$ *and* $\max\{\deg(f_i) \mid i \in \{1, \ldots, \nu\}, f_i \neq 0\} = \operatorname{ind}_\mathcal{O}(f) - 1$.

Proof. First we show that A_1 holds if G is an $\mathcal{O}$-border basis. The Border Division Algorithm provides us with a representation $f = f_1 g_1 + \cdots + f_\nu g_\nu + c_1 t_1 + \cdots + c_\mu t_\mu$ with $f_1, \ldots, f_\nu \in P$ and $c_1, \ldots, c_\mu \in K$ such that we have $\deg(f_i) \leq \operatorname{ind}_\mathcal{O}(f) - 1$ for $i = 1, \ldots, \nu$. Then we have $c_1 t_1 + \cdots + c_\mu t_\mu \in I$, and the hypothesis implies $c_1 = \cdots = c_\mu = 0$.

Next we prove that A_1 implies A_2. If $\deg(f_i) < \operatorname{ind}_\mathcal{O}(f) - 1$ then Proposition 6.4.8.b yields $\operatorname{ind}_\mathcal{O}(f_i g_i) \leq \deg(f_i) + \operatorname{ind}_\mathcal{O}(g_i) = \deg(f_i) + 1 < \operatorname{ind}_\mathcal{O}(f)$. By Proposition 6.4.8.c, there has to be at least one number $i \in \{1, \ldots, \nu\}$ such that $\deg(f_i) = \operatorname{ind}_\mathcal{O}(f) - 1$.

Finally, assume that A_2 holds and that there are $c_1, \ldots, c_\mu \in K$ with $c_1 t_1 + \cdots + c_\mu t_\mu \in I$. By applying A_2 to the polynomial $f = c_1 t_1 + \cdots + c_\mu t_\mu$ in I, we get a representation $f = f_1 g_1 + \cdots + f_\nu g_\nu$ with $f_1, \ldots, f_\nu \in P$ such that $\max\{\deg(f_i) \mid i \in \{1, \ldots, \nu\}, f_i \neq 0\} = \operatorname{ind}_\mathcal{O}(f) - 1 = -1$. Hence $f_1 = \cdots = f_\nu = 0$, and therefore $c_1 = \cdots = c_\mu = 0$. Consequently, the set G is an $\mathcal{O}$-border basis. □

In Proposition 2.1.2, Gröbner bases were characterized as sets of polynomials whose leading terms generate the leading term ideal. In the theory of border bases, leading terms have to be replaced by border forms which are defined as follows.

Definition 6.4.24. Given $f \in P$, we write $f = a_1 u_1 + \cdots + a_s u_s$ with coefficients $a_1, \ldots, a_s \in K \setminus \{0\}$ and terms $u_1, \ldots, u_s \in \mathbb{T}^n$ satisfying $\operatorname{ind}_\mathcal{O}(u_1) \geq \cdots \geq \operatorname{ind}_\mathcal{O}(u_s)$.

a) The polynomial $\mathrm{BF}_\mathcal{O}(f) = \sum_{\{i \mid \operatorname{ind}_\mathcal{O}(u_i) = \operatorname{ind}_\mathcal{O}(f)\}} a_i u_i \in P$ is called the **border form** of f with respect to $\mathcal{O}$. For $f = 0$, we let $\mathrm{BF}_\mathcal{O}(f) = 0$.

b) Given an ideal $I \subseteq P$, the ideal $\mathrm{BF}_\mathcal{O}(I) = (\mathrm{BF}_\mathcal{O}(f) \mid f \in I)$ is called the **border form ideal** of I with respect to $\mathcal{O}$.

For example, the elements of the $\mathcal{O}$-border prebasis G have the border form $\mathrm{BF}_\mathcal{O}(g_i) = b_i$. Now we characterize border bases by their border form ideal.

Proposition 6.4.25. (Border Bases and Border Form Ideals)
In the above setting, the set G *is an* $\mathcal{O}$*-border basis of* I *if and only if one of the following equivalent conditions is satisfied.*

B_1. *For every* $f \in I$, *the support of* $\mathrm{BF}_\mathcal{O}(f)$ *is contained in* $\mathbb{T}^n \setminus \mathcal{O}$.

B_2. *We have* $\mathrm{BF}_\mathcal{O}(I) = (\mathrm{BF}_\mathcal{O}(g_1), \ldots, \mathrm{BF}_\mathcal{O}(g_\nu)) = (b_1, \ldots, b_\nu)$.

Proof. First we show that a border basis satisfies condition B_1. Suppose that the border form of a polynomial $f \in I \setminus \{0\}$ contains a term of $\mathcal{O}$ in its support. Then all terms in the support of f are contained in $\mathcal{O}$, i.e. $f = c_1 t_1 + \cdots + c_\mu t_\mu$ for suitable $c_1, \ldots, c_\mu \in K$. Now the hypothesis implies $c_1 = \cdots = c_\mu = 0$, in contradiction to $f \neq 0$.

Next we prove that B_1 implies B_2. Since $g_i \in I$, we have $b_i \in \mathrm{BF}_\mathcal{O}(I)$ for $i = 1, \ldots, \nu$. To prove the reverse inclusion, let $f \in I \setminus \{0\}$. By B_1 and Proposition 6.4.6.c, every term in the support of $\mathrm{BF}_\mathcal{O}(f)$ is divisible by a term in $\partial\mathcal{O}$. Hence the border form of f is contained in $(b_1, \ldots, b_\nu)$.

Finally, we show that B_2 implies that G is a border basis. Let $c_1, \ldots, c_\mu$ be elements in K with $f = c_1 t_1 + \cdots + c_\mu t_\mu \in I$. Then all terms in the support of f have index zero, and thus $f = \mathrm{BF}_\mathcal{O}(f)$. By B_2 and Proposition 6.4.6.c, it follows that $c_1 = \cdots = c_\mu = 0$. □

To characterize border bases in analogy with conditions C_1) – C_4) of Proposition 2.2.5, we define the rewrite relation associated to G. Let $f \in P$ be a polynomial, let $t \in \mathrm{Supp}(f)$ be a multiple of a border term $t = t' b_i$, and let $c \in K$ be the coefficient of t in f. Then $h = f - c t' g_i$ does not contain the term t anymore. We say that f **reduces to** h **in one step** using g_i and write $f \xrightarrow{g_i} h$. The reflexive, transitive closure of the relations $\xrightarrow{g_i}$, $i \in \{1, \ldots, \nu\}$, is called the **rewrite relation** associated to G and is denoted by $\xrightarrow{G}$. The equivalence relation generated by $\xrightarrow{G}$ is denoted by $\xleftrightarrow{G}$. In stark contrast to Gröbner basis theory, rewrite relations associated to border prebases are, in general, not Noetherian. This is demonstrated by the following example.

Example 6.4.26. Let $P = \mathbb{Q}[x, y]$ and $\mathcal{O} = \{1, x, y, x^2, y^2\}$. Then $\mathcal{O}$ is an order ideal with border $\partial\mathcal{O} = \{xy, x^3, x^2y, xy^2, y^3\}$. Consider the $\mathcal{O}$-border prebasis $G = \{g_1, \ldots, g_5\}$, where $g_1 = xy - x^2 - y^2$, $g_2 = x^3$, $g_3 = x^2y$, $g_4 = xy^2$, and $g_5 = y^3$. The chain of reductions

$$x^2y \xrightarrow{g_1} x^3 + xy^2 \xrightarrow{g_2} xy^2 \xrightarrow{g_1} x^2y + y^3 \xrightarrow{g_5} x^2y$$

can be repeated indefinitely, and hence $\xrightarrow{G}$ is not Noetherian.

This lack of Noetherianity has adverse consequences for the properties of the rewrite relation $\xrightarrow{G}$. For instance, Proposition 2.2.2.a does not hold true anymore. Fortunately, the equivalence relation $\xleftrightarrow{G}$ still captures equivalence modulo I.

Remark 6.4.27. Let $\xleftrightarrow{G}$ be the rewrite equivalence relation associated to an $\mathcal{O}$-border prebasis $G = \{g_1, \ldots, g_\nu\}$, and let $f_1, f_2, f_3, f_4 \in P$.

a) If $f_1 \xleftrightarrow{G} f_2$ and $f_3 \xleftrightarrow{G} f_4$ then $f_1 + f_3 \xleftrightarrow{G} f_2 + f_4$.
b) If $f_1 \xleftrightarrow{G} f_2$ then $f_1 f_3 \xleftrightarrow{G} f_2 f_3$.
c) We have $f_1 \xleftrightarrow{G} f_2$ if and only if $f_1 - f_2 \in (g_1, \ldots, g_\nu)$.

These properties can be proved in exactly the same way as the corresponding properties in Proposition 2.2.2.

The definition of a confluent rewrite relation $\xrightarrow{G}$ and an irreducible polynomial $f \in P$ with respect to $\xrightarrow{G}$ are the same as in Section 2.2. For example, any polynomial f with support in $\mathcal{O}$ is irreducible with respect to $\xrightarrow{G}$; by Proposition 6.4.6.c, it contains no term that can be reduced. In particular, the normal remainder $\mathrm{NR}_{\mathcal{O},\mathcal{G}}(f)$ computed by the Border Division Algorithm is irreducible with respect to $\xrightarrow{G}$.

Proposition 6.4.28. (Border Bases and Rewrite Relations)
In the above setting, the set G is an $\mathcal{O}$-border basis of I if and only if the following equivalent conditions are satisfied.

C_1. *For $f \in P$, we have $f \xrightarrow{G} 0$ if and only if $f \in I$.*
C_2. *If $f \in I$ is irreducible with respect to $\xrightarrow{G}$, we have $f = 0$.*
C_3. *For every $f \in P$, there exists an element $h \in P$ such that $f \xrightarrow{G} h$ and h is irreducible with respect to $\xrightarrow{G}$. The element h is uniquely determined.*
C_4. *The rewrite relation $\xrightarrow{G}$ is confluent.*

Proof. First we show that a border basis has property C_1. If a polynomial $f \in P$ satisfies $f \xrightarrow{G} 0$, it is enough to collect the subtractions performed by the individual reduction steps on the right-hand side to obtain $f \in (g_1, \ldots, g_\nu)$. Conversely, let $f \in I$. We apply the Border Division Algorithm to f. It performs reduction steps using elements of G to compute the normal remainder $\mathrm{NR}_{\mathcal{O},\mathcal{G}}(f) \in \langle \mathcal{O} \rangle_K$. Since $f \in I$, we also have $\mathrm{NR}_{\mathcal{O},\mathcal{G}}(f) \in I$. The hypothesis that G is a border basis yields $\mathrm{NR}_{\mathcal{O},\mathcal{G}}(f) \in I \cap \langle \mathcal{O} \rangle_K = 0$, i.e. we have $f \xrightarrow{G} 0$.

To prove that C_1 implies C_2, note that C_1 shows $f \xrightarrow{G} 0$ for $f \in I$. Thus a polynomial $f \in I$ which is irreducible with respect to $\xrightarrow{G}$ has to be zero. Next we prove that C_2 implies C_3. Let $f \in P$. The Border Division Algorithm performs a reduction $f \xrightarrow{G} \mathrm{NR}_{\mathcal{O},\mathcal{G}}(f)$, i.e. there exists a reduction to a polynomial which is irreducible with respect to $\xrightarrow{G}$. Suppose that $f \xrightarrow{G} h$ and h is irreducible with respect to $\xrightarrow{G}$. Then $h - \mathrm{NR}_{\mathcal{O},\mathcal{G}}(f) \in I$ and the support of this difference is contained in $\mathcal{O}$. Thus it is irreducible with respect to $\xrightarrow{G}$ and C_2 yields $h = \mathrm{NR}_{\mathcal{O},\mathcal{G}}(f)$. Altogether, the normal remainder of f has the properties required by C_3.

Now we show that C_3 implies C_4. Let $f_1 \xrightarrow{G} f_2$ and $f_1 \xrightarrow{G} f_3$ be two reductions. The Border Division Algorithm yields $f_1 \xrightarrow{G} \mathrm{NR}_{\mathcal{O},\mathcal{G}}(f_2)$ and $f_1 \xrightarrow{G} \mathrm{NR}_{\mathcal{O},\mathcal{G}}(f_3)$. Since normal remainders are irreducible with respect to $\xrightarrow{G}$, condition C_3 implies $\mathrm{NR}_{\mathcal{O},\mathcal{G}}(f_2) = \mathrm{NR}_{\mathcal{O},\mathcal{G}}(f_3)$. Therefore there are reductions $f_2 \xrightarrow{G} f_4$ and $f_3 \xrightarrow{G} f_4$ with $f_4 = \mathrm{NR}_{\mathcal{O},\mathcal{G}}(f_2) = \mathrm{NR}_{\mathcal{O},\mathcal{G}}(f_3)$.

Finally, to show that G is a border basis if it satisfies C_4, we can use Proposition 6.4.27.c and proceed as in the proof of $C_4) \Rightarrow C_1)$ in Proposition 2.2.5. □

Next we turn to a characterization of border bases which has no Gröbner basis analog. Since the residue classes of the elements of $\mathcal{O}$ generate P/I as a K-vector space, we can describe the ring structure of this vector space by describing the effect of multiplying these generators by an indeterminate as follows.

Definition 6.4.29. Let $G = \{g_1, \ldots, g_\nu\}$ be an $\mathcal{O}$-border prebasis, i.e. let $g_j = b_j - \sum_{i=1}^{\mu} \alpha_{ij} t_i$ with $\alpha_{ij} \in K$ for $i = 1, \ldots, \mu$ and $j = 1, \ldots, \nu$. Given $r \in \{1, \ldots, n\}$, we define the r^{th} **formal multiplication matrix** $\mathcal{X}_r = (\xi_{k\ell}^{(r)})$ of G by

$$\xi_{k\ell}^{(r)} = \begin{cases} \delta_{ki}, & \text{if } x_r\, t_\ell = t_i \\ \alpha_{kj}, & \text{if } x_r\, t_\ell = b_j \end{cases}$$

Here we let $\delta_{ki} = 1$ if $k = i$ and $\delta_{ki} = 0$ otherwise.

The formal multiplication matrices encode the following procedure. We multiply an element of $\langle \mathcal{O} \rangle_K$ by the indeterminate x_r. Whenever $x_r\, t_i = b_j$ is contained in the border, we reduce by the corresponding border polynomial g_j so that the result stays in $\langle \mathcal{O} \rangle_K$. Elements $v = c_1\, t_1 + \ldots + c_\mu\, t_\mu \in \langle \mathcal{O} \rangle_K$ are encoded as column vectors $(c_1, \ldots, c_\mu)^{\text{tr}} \in K^\mu$. Hence $x_r\, v$ corresponds to $\mathcal{X}_r\, (c_1, \ldots, c_\mu)^{\text{tr}}$. Observe that all matrix components $\xi_{k\ell}^{(r)}$ are determined by the polynomials $g_1, \ldots, g_\nu$.

The following theorem characterizes border bases by the property that their formal multiplication matrices commute.

Theorem 6.4.30. (Border Bases and Commuting Matrices)
Let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal, let $G = \{g_1, \ldots, g_\nu\}$ be an $\mathcal{O}$-border prebasis, and let $I = (g_1, \ldots, g_\nu)$. Then the following conditions are equivalent.

a) The set G is an $\mathcal{O}$-border basis of I.
b) The formal multiplication matrices of G are pairwise commuting.

In that case the formal multiplication matrices represent the multiplication endomorphisms of P/I with respect to the basis $\{\bar{t}_1, \ldots, \bar{t}_\mu\}$.

Proof. Let $\mathcal{X}_1, \ldots, \mathcal{X}_n$ be the formal multiplication matrices corresponding to the given $\mathcal{O}$-border prebasis $G = \{g_1, \ldots, g_\nu\}$.

First we prove that a) implies b). Since G is an $\mathcal{O}$-border basis, the set $\{\bar{t}_1, \ldots, \bar{t}_\mu\}$ is a K-vector space basis of P/I, and each matrix $\mathcal{X}_r$ defines a K-linear map $\varphi_r : P/I \longrightarrow P/I$. We want to show that φ_r is the endomorphism corresponding to multiplication by x_r. Consider the expansions

$$\begin{aligned}\varphi_r(\bar{t}_1) &= \xi_{11}^{(r)}\bar{t}_1 + \cdots + \xi_{\mu 1}^{(r)}\bar{t}_\mu \\ &\vdots \\ \varphi_r(\bar{t}_\mu) &= \xi_{1\mu}^{(r)}\bar{t}_1 + \cdots + \xi_{\mu\mu}^{(r)}\bar{t}_\mu\end{aligned}$$

In these expansions only two cases occur. The product $x_r\, t_\ell$ either equals some term t_i in the order ideal $\mathcal{O}$ or some border term $b_j \in \partial\mathcal{O}$. In the former case we have $\varphi_r(\bar{t}_\ell) = \bar{t}_i = x_r\bar{t}_\ell$, and in the latter case we have $\varphi_r(\bar{t}_\ell) = \alpha_{1j}\bar{t}_1 + \cdots + \alpha_{\mu j}\bar{t}_\mu = \bar{b}_j = x_r\bar{t}_\ell$. From this it follows that the map $\varphi_r : P/I \longrightarrow P/I$ is multiplication by x_r for $r = 1, \ldots, n$. Therefore we have $\mathcal{X}_r\mathcal{X}_s = \mathcal{X}_s\mathcal{X}_r$ for $r, s \in \{1, \ldots, n\}$, i.e. the matrices $\mathcal{X}_1, \ldots, \mathcal{X}_n$ are pairwise commuting.

It remains to show that b) implies a). Without loss of generality, let $t_1 = 1$. The matrices $\mathcal{X}_1, \ldots, \mathcal{X}_n$ define a P-module structure on $\langle\mathcal{O}\rangle_K$ via

$$f \cdot (c_1t_1 + \ldots + c_\mu t_\mu) = (t_1, \ldots, t_\mu) f(\mathcal{X}_1, \ldots, \mathcal{X}_n)(c_1, \ldots, c_\mu)^{\mathrm{tr}}$$

where we set $f(\mathcal{X}_1, \ldots, \mathcal{X}_n) = f\,\mathcal{I}_\mu$ for $f \in K$.

First we show that this P-module is cyclic with generator t_1. To do so, we use induction on degree to show that $t_i \cdot t_1 = t_i$ for $i = 1, \ldots, \mu$. Let e_i denote the matrix of size $\mu \times 1$ whose i^{th} entry is 1 and whose other entries are 0. The induction starts with $t_1 = (t_1, \ldots, t_\mu)\mathcal{I}_\mu \cdot e_1$. For the induction step, let $t_i = x_j\, t_k$. Then we have

$$\begin{aligned}t_i \cdot t_1 &= (t_1, \ldots, t_\mu)t_i(\mathcal{X}_1, \ldots, \mathcal{X}_n)e_1 = (t_1, \ldots, t_\mu)\mathcal{X}_j\, t_k(\mathcal{X}_1, \ldots, \mathcal{X}_n)e_1 \\ &= (t_1, \ldots, t_\mu)\mathcal{X}_j e_k = (t_1, \ldots, t_\mu)e_i = t_i\end{aligned}$$

Thus we obtain a surjective P-linear map $\tilde{\Theta} : P \longrightarrow \langle\mathcal{O}\rangle_K$ which satisfies $f \mapsto f \cdot t_1$ and an induced isomorphism of P-modules $\Theta : P/J \longrightarrow \langle\mathcal{O}\rangle_K$ with $J = \operatorname{Ker}\tilde{\Theta}$. In particular, the residue classes $t_1 + J, \ldots, t_\mu + J$ are K-linearly independent.

Next we show that $I \subseteq J$. Let $b_j = x_k\, t_\ell$. Then we have

$$\begin{aligned}g_j(\mathcal{X}_1, \ldots, \mathcal{X}_n)e_1 &= b_j(\mathcal{X}_1, \ldots, \mathcal{X}_n)e_1 - \sum_{i=1}^{\mu}\alpha_{ij}t_i(\mathcal{X}_1, \ldots, \mathcal{X}_n)e_1 \\ &= \mathcal{X}_k\, t_\ell(\mathcal{X}_1, \ldots, \mathcal{X}_n)e_1 - \sum_{i=1}^{\mu}\alpha_{ij}e_i = \mathcal{X}_k\, e_\ell - \sum_{i=1}^{\mu}\alpha_{ij}e_i \\ &= \sum_{i=1}^{\mu}\alpha_{ij}e_i - \sum_{i=1}^{\mu}\alpha_{ij}e_i = 0\end{aligned}$$

Therefore we obtain $g_j \in \ker\tilde{\Theta}$ for $j = 1, \ldots, \nu$ and thus $I \subseteq J$, as desired.

Hence there is a natural surjective ring homomorphism $\Psi : P/I \to P/J$. Since the set $\{t_1 + I, \ldots t_\mu + I\}$ generates the K-vector space P/I, and since the set $\{t_1 + J, \ldots, t_\mu + J\}$ is K-linearly independent, both sets must be bases and $I = J$. This shows that G is an $\mathcal{O}$-border basis of I. □

The following example shows that the formal multiplication matrices corresponding to an $\mathcal{O}$-border prebasis are not always commuting.

Example 6.4.31. Let $P = \mathbb{Q}[x, y]$ and $\mathcal{O} = \{1, x, y, x^2, y^2\}$. Then the border of $\mathcal{O}$ is $\partial\mathcal{O} = \{xy, x^3, y^3, x^2y, xy^2\}$. Consider the set of polynomials $G = \{g_1, g_2, g_3, g_4, g_5\}$ with $g_1 = xy - x^2 - y^2$, $g_2 = x^3 - x^2$, $g_3 = y^3 - y^2$, $g_4 = x^2y - x^2$, and $g_5 = xy^2 - y^2$. It is an $\mathcal{O}$-border prebasis of the ideal $I = (g_1, \ldots, g_5)$. Its multiplication matrices

$$\mathcal{X} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathcal{Y} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

do not commute, because

$$\mathcal{X} \cdot \mathcal{Y} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix} \quad \neq \quad \mathcal{Y} \cdot \mathcal{X} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

By the theorem, the set G is not an $\mathcal{O}$-border basis of I.

Based on the preceding theorem, we can now prove an analog of Buchberger's Criterion 2.5.3. The first step is to analyze the commutativity conditions in Theorem 6.4.30 and translate them back into equations for the coefficients of $g_1, \ldots, g_\nu$.

Proposition 6.4.32. *For $j = 1, \ldots, \nu$, we write $g_j = b_j - \sum_{i=1}^{\mu} \alpha_{ij} t_i$ with $\alpha_{ij} \in K$. Given $r \in \{1, \ldots, n\}$, we define a map*

$$\begin{array}{rccl} \varrho\colon & \{1, \ldots, \mu\} & \longrightarrow & \mathbb{N} \\ & i & \longmapsto & \begin{cases} j & \text{if } x_r t_i = t_j \in \mathcal{O}, \\ k & \text{if } x_r t_i = b_k \in \partial\mathcal{O}. \end{cases} \end{array}$$

Then the $\mathcal{O}$-border prebasis G of I is an $\mathcal{O}$-border basis of I if and only if the following equations are satisfied for $p = 1, \ldots, \mu$ and $1 \leq r < s \leq n$:

$$(1) \quad \sum_{\{m \mid x_r t_m \in \mathcal{O}\}} \delta_{p\varrho(m)} \alpha_{mk} + \sum_{\{m \mid x_r t_m \in \partial\mathcal{O}\}} \alpha_{p\varrho(m)} \alpha_{mk} = \alpha_{p\ell} \qquad \text{if } x_r t_i = t_j,\ x_s t_i = b_k,\ x_r b_k = b_\ell$$

$$(2) \quad \sum_{\{m \mid x_r t_m \in \mathcal{O}\}} \delta_{p\varrho(m)} \alpha_{mk} + \sum_{\{m \mid x_r t_m \in \partial\mathcal{O}\}} \alpha_{p\varrho(m)} \alpha_{mk} = \sum_{\{m \mid x_s t_m \in \mathcal{O}\}} \delta_{p\varrho(m)} \alpha_{mk} + \sum_{\{m \mid x_r t_m \in \partial\mathcal{O}\}} \alpha_{p\varrho(m)} \alpha_{mk} \qquad \text{if } x_r t_i = b_j,\ x_s t_i = b_k$$

Proof. By Theorem 6.4.30, the set G is an $\mathcal{O}$-border basis if and only if $\mathcal{X}_r\mathcal{X}_s e_i = \mathcal{X}_s\mathcal{X}_r e_i$ for $i = 1, \ldots, \mu$. Translating this back into the language of $\langle\mathcal{O}\rangle_K$, the resulting condition depends on the position of t_i relative to the border of $\mathcal{O}$. We distinguish four cases.

t_k	t_ℓ
t_i	t_j

First case: $x_r\, x_s\, t_i \in \mathcal{O}$

Since $\mathcal{O}$ is an order ideal, we have $t_j = x_r t_i \in \mathcal{O}$ and $t_k = x_s t_i \in \mathcal{O}$. Thus we have $\mathcal{X}_r\mathcal{X}_s e_i = \mathcal{X}_r e_k = e_\ell = \mathcal{X}_s e_j = \mathcal{X}_s\mathcal{X}_r e_i$, i.e. the commutativity condition holds by the definition of the formal multiplication matrices.

t_k	b_ℓ
t_i	t_j

Second case: $x_r\, x_s\, t_i \in \partial\mathcal{O}$ and $x_r\, t_i,\ x_s\, t_i \in \mathcal{O}$

Say, $x_r\, t_i = t_j$, $x_s\, t_i = t_k$, and $x_r\, x_s\, t_i = b_\ell$. Then we have

$$\mathcal{X}_r\, \mathcal{X}_s\, e_i = \mathcal{X}_r\, e_k = (\alpha_{1\ell}, \ldots, \alpha_{\mu\ell})^{\mathrm{tr}} = \mathcal{X}_s\, e_j = \mathcal{X}_s\, \mathcal{X}_r\, e_i$$

Again, commutativity follows immediately from the definition of the formal multiplication matrices.

b_k	b_ℓ
t_i	t_j

Third case: $x_r\, t_i \in \mathcal{O}$ and $x_s\, t_i \in \partial\mathcal{O}$

Since $\overline{\partial\mathcal{O}}$ and $\mathcal{O}$ are order ideals, this case implies $x_r\, x_s\, t_i \in \partial\mathcal{O}$. Say $x_r\, t_i = t_j$, $x_s\, t_i = b_k$, and $x_r\, x_s\, t_i = b_\ell$. The commutativity condition becomes $\mathcal{X}_r\, (\alpha_{1k}, \ldots, \alpha_{\mu k})^{\mathrm{tr}} = (\alpha_{1\ell}, \ldots, \alpha_{\mu\ell})^{\mathrm{tr}}$, i.e. $\sum_{m=1}^{\mu} \xi_{pm}^{(r)} \alpha_{mk} = \alpha_{p\ell}$ for $p = 1, \ldots, \mu$. According to the definition of the formal multiplication matrices, these conditions are equivalent to equations (1) for $p = 1, \ldots, \mu$.

b_k	$*$
t_i	b_j

Fourth case: $x_t\, t_i \in \partial\mathcal{O}$ and $x_s\, t_i \in \partial\mathcal{O}$

Say $x_r\, t_i = b_j$ and $x_s\, t_i = b_k$. The commutativity condition becomes $\mathcal{X}_r(\alpha_{1k}, \ldots, \alpha_{\mu k})^{\mathrm{tr}} = \mathcal{X}_s(\alpha_{1j}, \ldots, \alpha_{\mu j})^{\mathrm{tr}}$, i.e. $\sum_{m=1}^{\mu} \xi_{pm}^{(r)} \alpha_{mk} = \sum_{m=1}^{\mu} \xi_{pm}^{(s)} \alpha_{mj}$ for $p = 1, \ldots, \mu$. These conditions are equivalent to equations (2) for $p = 1, \ldots, \mu$.

This covers all cases. Altogether, we have shown that $\mathcal{X}_r\mathcal{X}_s = \mathcal{X}_s\mathcal{X}_r$ for $1 \le r < s \le n$ is equivalent to the set of equations (1), (2). □

Next we want to interpret the equations (1), (2) in terms of the rewrite relation associated to G. The following definition is motivated by the third and fourth cases above.

Definition 6.4.33. Let $b_i, b_j \in \partial\mathcal{O}$ be two distinct border terms.

a) The border terms b_i and b_j are called **next-door neighbours** if we have $b_i = x_k\, b_j$ for some $k \in \{1, \ldots, n\}$.
b) The border terms b_i and b_j are called **across-the-street neighbours** if $x_k\, b_i = x_\ell\, b_j$ for some $k, \ell \in \{1, \ldots, n\}$.
c) The border terms b_i and b_j are called **neighbours** if they are next-door neighbours or across-the-street neighbours.

At this point we are ready to prove the border basis analog of Buchberger's Criterion 2.5.3. The **S-polynomial** of two distinct elements $g_i, g_j \in G$ is defined by

$$\mathrm{S}(g_i, g_j) = (\mathrm{lcm}(b_i, b_j)/b_i)\, g_i - (\mathrm{lcm}(b_i, b_j)/b_j)\, g_j.$$

Proposition 6.4.34. (Buchberger's Criterion for Border Bases) *In the above setting, the $\mathcal{O}$-border prebasis G is an $\mathcal{O}$-border basis of I if and only if one of the following equivalent conditions is satisfied.*

D_1. *For all $1 \leq i < j \leq \nu$, the S-polynomial $\mathrm{S}(g_i, g_j)$ reduces to zero via $\xrightarrow{G}$.*
D_2. *For all neighbours b_i and b_j, the S-polynomial $\mathrm{S}(g_i, g_j)$ reduces to zero via $\xrightarrow{G}$.*

Proof. Condition D_1 holds if G is a border basis, since $\mathrm{S}(g_i, g_j) \in I$ and G satisfies Condition C_1. Since D_1 trivially implies D_2, it remains to prove that G is a border basis if D_2 holds.

Given next-door neighbours $b_\ell = x_r b_k$, we calculate

$$\begin{aligned}
g_\ell - x_r\, g_k &= (b_\ell - \sum_{m=1}^{\mu} \alpha_{m\ell} t_m) - x_r(b_k - \sum_{m=1}^{\mu} \alpha_{mk} t_m) \\
&= -\sum_{m=1}^{\mu} \alpha_{m\ell} t_m + \sum_{m=1}^{\mu} \alpha_{mk}(x_r\, t_m) \\
&= -\sum_{m=1}^{\mu} \alpha_{m\ell} t_m + \sum_{\{m \mid x_r t_m \in \mathcal{O}\}} \alpha_{mk} t_{\varrho(m)} + \sum_{\{m \mid x_r t_m \in \partial\mathcal{O}\}} \alpha_{mk} b_{\varrho(m)} \\
&= -\sum_{m=1}^{\mu} \alpha_{m\ell} t_m + \sum_{\{m \mid x_r t_m \in \mathcal{O}\}} \alpha_{mk} t_{\varrho(m)} + \sum_{\{m \mid x_r t_m \in \partial\mathcal{O}\}} \alpha_{mk} g_{\varrho(m)} \\
&\quad + \sum_{\{m \mid x_r t_m \in \partial\mathcal{O}\}} \big(\alpha_{mk} \sum_{p=1}^{\mu} \alpha_{p,\varrho(m)} t_p\big)
\end{aligned}$$

Since $(g_1, \ldots, g_\nu) \subseteq I$, the coefficient of each t_p has to vanish in the sum

$$-\sum_{m=1}^{\mu} \alpha_{m\ell} t_m + \sum_{\{m \mid x_r t_m \in \mathcal{O}\}} \alpha_{mk} t_{\varrho(m)} + \sum_{\{m \mid x_r t_m \in \partial\mathcal{O}\}} \big(\alpha_{mk} \sum_{p=1}^{\mu} \alpha_{p,\varrho(m)} t_p\big)$$

This vanishing condition yields exactly equations (1) in Proposition 6.4.32.

Given across-the-street neighbours $x_r b_k = x_s b_j$, we calculate

$$\begin{aligned}
x_r\, g_k - x_s\, g_j &= x_r(b_k - \sum_{m=1}^{\mu} \alpha_{mk} t_m) - x_s(b_j - \sum_{m=1}^{\mu} \alpha_{mj} t_m) \\
&= -\sum_{m=1}^{\mu} \alpha_{mk}(x_r\, t_m) + \sum_{m=1}^{\mu} \alpha_{mj}(x_s\, t_m) \\
&= -\sum_{\{m \mid x_r t_m \in \mathcal{O}\}} \alpha_{mk} t_{\varrho(m)} - \sum_{\{m \mid x_r t_m \in \partial\mathcal{O}\}} \alpha_{mk} b_{\varrho(m)}
\end{aligned}$$

$$
\begin{aligned}
& + \sum_{\{m \mid x_s t_m \in \mathcal{O}\}} \alpha_{mj} t_{\varrho(m)} + \sum_{\{m \mid x_s t_m \in \partial\mathcal{O}\}} \alpha_{mj} b_{\varrho(m)} \\
= \; & - \sum_{\{m \mid x_r t_m \in \mathcal{O}\}} \alpha_{mk} t_{\varrho(m)} - \sum_{\{m \mid x_r t_m \in \partial\mathcal{O}\}} \alpha_{mk} g_{\varrho(m)} \\
& - \sum_{\{m \mid x_r t_m \in \partial\mathcal{O}\}} \alpha_{mk} \sum_{p=1}^{\mu} \alpha_{p\varrho(m)} t_p \\
& + \sum_{\{m \mid x_s t_m \in \mathcal{O}\}} \alpha_{mj} t_{\varrho(m)} + \sum_{\{m \mid x_s t_m \in \partial\mathcal{O}\}} \alpha_{mj} g_{\varrho(m)} \\
& + \sum_{\{m \mid x_s t_m \in \partial\mathcal{O}\}} \alpha_{mj} \sum_{p=1}^{\mu} \alpha_{p\varrho(m)} t_p
\end{aligned}
$$

Again the coefficient of each t_p has to vanish, and this yields exactly the equations (2) in Proposition 6.4.32. Altogether, we see that $g_\ell - x_r\, g_k \xrightarrow{G} 0$ or $x_r\, g_k - x_s\, g_j \xrightarrow{G} 0$, respectively, implies the commutativity of the formal multiplication matrices, and therefore that G is an $\mathcal{O}$-border basis. □

Let us end this section with a concrete algorithm for computing border bases. For a description of what we mean by transforming a matrix into row echelon form, see the discussion before Theorem 6.3.10.

Lemma 6.4.35. *Let $d \in \mathbb{N}$, let $\mathcal{L} = \mathbb{T}^n_{\leq d}$, let V be a K-vector subspace of $\langle \mathcal{L} \rangle_K$ such that $(V + x_1 V + \cdots + x_n V) \cap \langle \mathcal{L} \rangle_K = V$, let $\{v_1, \ldots, v_r\}$ be a K-basis of V, and let σ be a degree compatible term ordering. Consider the following sequence of instructions.*

1) *Write $\mathcal{L} = \{\ell_1, \ldots, \ell_s\}$ such that $\ell_1 >_\sigma \ell_2 >_\sigma \cdots >_\sigma \ell_s$.*
2) *For $i = 1, \ldots, r$, write $v_i = a_{i1}\ell_1 + \cdots + a_{is}\ell_s$ with $a_{ij} \in K$. Form the matrix $\mathcal{V} = (a_{ij}) \in \mathrm{Mat}_{r,s}(K)$.*
3) *Using row operations, transform $\mathcal{V}$ into row echelon form. Call the result $\mathcal{W}$.*
4) *Let $\mathcal{O}$ be the set of terms in $\mathcal{L}$ corresponding to the pivot-free columns of $\mathcal{W}$, i.e. the columns of $\mathcal{W}$ in which no row of $\mathcal{W}$ has its first non-zero entry. Return $\mathcal{O}$ and stop.*

This is an algorithm which computes an order ideal $\mathcal{O} \subseteq \mathcal{L}$ such that the residue classes of the terms in $\mathcal{O}$ form a K-vector space basis of $\langle \mathcal{L} \rangle_K / V$.

Proof. The procedure is obviously finite. Thus we prove correctness. The terms in $\mathcal{O}$ are linearly independent modulo V because a non-trivial element in $\langle \mathcal{O} \rangle_K \cap V$ would correspond to a row of $\mathcal{W}$ whose first non-zero position is in a column corresponding to a term of $\mathcal{O}$.

To prove that $\mathcal{O}$ is an order ideal, it suffices to show that $\ell_i \in \mathcal{L} \setminus \mathcal{O}$ and $t\,\ell_i \in \mathcal{L}$ imply $t\,\ell_i \in \mathcal{L} \setminus \mathcal{O}$ for all $t \in \mathbb{T}^n$. Given a term $\ell_i \in \mathcal{L} \setminus \mathcal{O}$, there exists a vector $v \in V$ which corresponds to the row of $\mathcal{W}$ whose first non-zero entry is in position i. Thus we have $\ell_i = \mathrm{LT}_\sigma(v)$. Now let $\ell_j = t\,\ell_i \in \mathcal{L}$ for some $t \in \mathbb{T}^n$. Then we see that $\ell_j = \mathrm{LT}_\sigma(t\,v)$. Since σ is degree compatible, it

follows that all elements of $\mathrm{Supp}(t\,v)$ are in $\mathcal{L}$. Hence the term ℓ_j corresponds to a column of the matrix $\mathcal{W}$ in which one of its rows has its first non-zero entry. Thus we have $t\,\ell_i \in \mathcal{L} \setminus \mathcal{O}$, and the proof is complete. □

Theorem 6.4.36. (The Border Basis Algorithm)
Let $I \subseteq P$ be a zero-dimensional ideal generated by a set of non-zero polynomials $\{f_1, \ldots, f_s\}$, and let σ be a degree compatible term ordering. Consider the following sequence of instructions.

1) *Let $V_0 \subseteq P$ be the K-vector subspace generated by $\{f_1, \ldots, f_s\}$.*
2) *Let $d = \max\{\deg(t) \mid t \in \mathrm{Supp}(f_1) \cup \cdots \cup \mathrm{Supp}(f_s)\}$ and $\mathcal{L} = \mathbb{T}^n_{\leq d}$.*
3) *For $i = 0, 1, 2, \ldots$ compute $V_{i+1} = (V_i + x_1\,V_i + \cdots + x_n\,V_i) \cap \langle\mathcal{L}\rangle_K$ until $V_{i+1} = V_i$.*
4) *Using the lemma, compute an order ideal $\mathcal{O} \subseteq \mathcal{L}$ such that the residue classes of the terms in $\mathcal{O}$ form a K-vector space basis of $\langle\mathcal{L}\rangle_K / V_i$.*
5) *Check whether $\partial\mathcal{O} \subseteq \mathcal{L}$. If this is not the case, increase d by one, replace $\mathcal{L}$ by $\mathbb{T}^n_{\leq d}$, replace V_0 by V_i, and continue with step 3).*
6) *Let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ and $\partial\mathcal{O} = \{b_1, \ldots, b_\nu\}$. For $j = 1, \ldots, \nu$, use linear algebra to compute the representation $\bar{b}_j = \sum_{i=1}^{\mu} \alpha_{ij}\bar{t}_i$ of $\bar{b}_j \in \langle\mathcal{L}\rangle_K / V_i$ in terms of the basis $\{\bar{t}_1, \ldots, \bar{t}_\mu\}$ and let $g_j = b_j - \sum_{i=1}^{\mu} \alpha_{ij} t_i$. Then let $G = \{g_1, \ldots, g_\nu\}$, return the pair $(\mathcal{O}, G)$, and stop.*

This is an algorithm which returns a pair $(\mathcal{O}, G)$ where $\mathcal{O}$ is an order ideal and G is the $\mathcal{O}$-border basis of I.

Proof. First we prove finiteness. Since $V_i \subseteq V_{i+1}$ for $i \geq 0$ and since $\dim_K(\langle\mathcal{L}\rangle_K) < \infty$, the sequence $V_0 \subseteq V_1 \subseteq \cdots$ is eventually stationary. Thus step 3) involves only a finite amount of computation. To show that the loop in steps 3) – 5) is finite, we have to prove that we eventually have $\partial\mathcal{O} \subseteq \mathcal{L}$. Let σ be a degree compatible term ordering on $\mathbb{T}^n$, and let $H = \{h_1, \ldots, h_{s'}\}$ be the reduced σ-Gröbner basis of I. For $j = 1, \ldots, s'$, there is a representation $h_j = p_{j1}f_1 + \cdots + p_{js}f_s$ with $p_{jk} \in P$. Let $d = \max\{\deg(p_{jk}f_k) \mid j \in \{1, \ldots, s'\}, k \in \{1, \ldots, s\}\}$. By construction, we have $H \subseteq V_i$ after step 3) has been performed for $\mathcal{L} = \mathbb{T}^n_{\leq d}$. Now we apply the algorithm of the lemma. It follows that none of the leading terms $\mathrm{LT}_\sigma(h_j)$ is contained in $\mathcal{O}$. Thus we have $\mathcal{O} \subseteq \mathbb{T}^n \setminus \mathrm{LT}_\sigma\{I\}$ and $\#\mathcal{O} \leq \dim_K(P/I)$. Therefore it suffices to repeat the loop until d is larger than this dimension in order to force $\partial\mathcal{O} \subseteq \mathcal{L}$.

Next we prove correctness. When the loop in steps 3) – 5) finishes, we have $\partial\mathcal{O} \subseteq \mathcal{L}$. Hence step 6) can be performed and yields $G \subseteq V_i \subseteq I$. By construction, the set G is an $\mathcal{O}$-border prebasis. Given two neighbours $b_j, b_k \in \partial\mathcal{O}$, the corresponding S-polynomial $\mathrm{S}(g_j, g_k)$ has its support in $\overline{\partial\mathcal{O}} \subseteq \mathcal{L}$. Hence we can find $c_1, \ldots, c_\nu \in K$ such that $\mathrm{S}(g_j, g_k) - \sum_{\ell=1}^{\nu} c_\ell g_\ell$ has its support in $\mathcal{O}$. Since this polynomial is contained in V_i and $\mathcal{O}$ represents a K-vector space basis of $\langle\mathcal{L}\rangle_K / V_i$, it follows that $\mathrm{S}(g_j, g_k) - \sum_{\ell=1}^{\nu} c_\ell g_\ell = 0$. Consequently, the S-polynomial $\mathrm{S}(g_j, g_k)$ reduces to zero using $\xrightarrow{G}$, and Buch-

berger's Criterion for Border Bases 6.4.34 proves that G is an $\mathcal{O}$-border basis of the ideal $(g_1, \ldots, g_\nu)$.

Finally, we show $(g_1, \ldots, g_\nu) = I$. The inclusion "$\subseteq$" was already observed above. For $j = 1, \ldots, s$, we have $f_j \in V_0 \subseteq V_i \subseteq \langle \mathcal{L} \rangle_K$. Every term in $\mathcal{L} \setminus \mathcal{O}$ is a multiple of one of the terms $b_1, \ldots, b_\nu$. Therefore we can use $\xrightarrow{G}$ to reduce f_j to an element in $\langle \mathcal{O} \rangle_K$. But that element is also contained in V_i, and hence it is zero. In other words, we have $f_j \in (g_1, \ldots, g_\nu)$, and the proof is complete. □

Let us add some remarks about possible optimizations of this algorithm.

Remark 6.4.37. Assume that we are in the setting of the theorem.

a) Every time step 4) calls the algorithm of the lemma, we can reuse the result of the previous call: the list of terms corresponding to the columns of $\mathcal{V}$ has been enlarged, and the elements of the previous basis $\{v_1, \ldots, v_r\}$ are contained in the current vector space V_i.
b) Since I is a zero-dimensional ideal, there exists for each $j \in \{1, \ldots, n\}$ a non-zero polynomial of minimal degree in $I \cap K[x_j]$. When the algorithm of the lemma discovers a row of $\mathcal{W}$ corresponding to such a polynomial, we can exclude all proper multiples of its leading term from the further sets $\mathcal{L}$. The reason is that there has to be an element of the border basis whose border term divides that leading term.
c) In the algorithm of the lemma, it is not necessary to order the terms in $\mathcal{L}$ with respect to a degree compatible term ordering. We may choose a different ordering, but in that case it is not sure that the resulting set of terms $\mathcal{O}$ is an order ideal.

To wrap up this section we apply the algorithm of the theorem to the ideal in Example 6.4.16.

Example 6.4.38. Let $P = \mathbb{Q}[x, y]$, let $\sigma = \texttt{DegLex}$, and let $I = (f_1, f_2, f_3)$, where $f_1 = x^2 + xy - \frac{1}{2}y^2 - x - \frac{1}{2}y$, $f_2 = y^3 - y$, and $f_3 = xy^2 - xy$. We follow the steps of the Border Basis Algorithm 6.4.36.

1) Let $V_0 = \langle f_1, f_2, f_3 \rangle_K$.
2) Let $d = 3$ and $\mathcal{L} = \{x^3, x^2y, xy^2, y^3, x^2, xy, y^2, x, y, 1\}$.
3) Compute $V_1 = \langle f_1, f_2, f_3, yf_1, xf_1 \rangle$ and $V_2 = V_1$.
4) Form the matrix

$$\mathcal{V} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & -\frac{1}{2} & -1 & -\frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & -\frac{1}{2} & 0 & -1 & -\frac{1}{2} & 0 & 0 & 0 \\ 1 & 1 & -\frac{1}{2} & 0 & -1 & -\frac{1}{2} & 0 & 0 & 0 & 0 \end{pmatrix}$$

Since $\mathcal{V}$ is already in row echelon form, we let $\mathcal{O} = \{xy, y^2, x, y, 1\}$ be the terms corresponding to the last five columns.

5) We have $\partial\mathcal{O} \subseteq \mathcal{L}$.
6) Since $\partial\mathcal{O} = \{x^2, x^2y, xy^2, y^3\}$, we compute $g_1 = x^2 + xy - \frac{1}{2}y^2 - x - \frac{1}{2}y$, $g_2 = x^2y - \frac{1}{2}y^2 - \frac{1}{2}y$, $g_3 = xy^2 - xy$, and $g_4 = y^3 - y$. Return the pair $(\mathcal{O}, G)$, where $G = \{g_1, g_2, g_3, g_4\}$ and stop.

Altogether, we have computed the order ideal $\mathcal{O} = \{1, x, y, x^2, y^2\}$ and the $\mathcal{O}$-border basis $G = \{f_1, yf_1 - f_3 + \frac{1}{2}f_2, f_3, f_2\}$ of I.

Observe that we could have chosen the coefficient of xy as the pivot element in the first row of $\mathcal{V}$. Then the algorithm would have returned the order ideal $\mathcal{O}' = \{1, x, y, x^2, y^2\}$ and the $\mathcal{O}'$-border basis $G' = \{x^3 - x, x^2y - \frac{1}{2}y^2 - \frac{1}{2}y, xy + x^2 - \frac{1}{2}y^2 - x - \frac{1}{2}y, xy^2 + x^2 - \frac{1}{2}y^2 - x - \frac{1}{2}y, y^3 - y\}$. The order ideal $\mathcal{O}'$ is not of the form $\mathbb{T}^2 \setminus \mathrm{LT}_\sigma\{I\}$ for any term ordering σ.

Exercise 1. Let $a, b \in \mathbb{N}_+$, and let I be the monoideal in $\mathbb{T}^2$ generated by $\{x^a, y^b\}$. For every $k \geq 0$, describe the k^{th} border of $\mathcal{O} = \mathbb{T}^2 \setminus I$.

Exercise 2. Let $P = \mathbb{Q}[x, y]$, let $a, b \in \mathbb{Q}$, and let $I \subseteq P$ be the ideal generated by $f_1 = \frac{1}{2}x^2 + y^2 + axy - 1$ and $f_2 = x^2 + \frac{1}{2}y^2 + bxy - 1$. Compute the border basis of I with respect to $\mathcal{O} = \{1, x, y, xy\}$ and show that it varies continuously with the parameters a, b.

Exercise 3. Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let $A \subseteq P$. We say that A is **invariant** under the action of the symmetric group (or that A is **symmetric**) if $f(x_1, \ldots, x_n) \in A$ implies $f(x_{\pi(1)}, \ldots, x_{\pi(n)}) \in A$ for every permutation π of $\{1, \ldots, n\}$.
Now let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal in $\mathbb{T}^n$, and let $I \subseteq P$ be a zero-dimensional ideal. Assume that the residue classes of the elements of $\mathcal{O}$ form a K-vector space basis of P/I and that both $\mathcal{O}$ and I are symmetric.

a) Prove that the $\mathcal{O}$-border basis of I is also symmetric.
b) Compare this result with Examples 6.4.2 and 6.4.14.

Exercise 4. Let A be the set of all ideals I in $P = \mathbb{Q}[x, y]$ having the property that the residue classes of the elements in $\{1, x\}$ form a basis of P/I as a K-vector space. Prove that A can be parametrized by $\mathbb{Q}^4$.

Exercise 5. Let K be a field, let $P = K[x_1, \ldots, x_n]$, let $\mathcal{O}$ be an order ideal in $\mathbb{T}^n$, and let $c_1, \ldots, c_s$ be the corners of $\mathbb{T}^n \setminus \mathcal{O}$. Moreover, let I be a zero-dimensional ideal in P which has an $\mathcal{O}$-border basis, and let $g_1, \ldots, g_s$ be the elements in this border basis corresponding to $c_1, \ldots, c_s$. Finally, let $J = (g_1, \ldots, g_s)$, and assume that there exists a term ordering σ such that $\mathrm{LT}_\sigma(g_i) = c_i$ for $i = 1, \ldots, s$. Prove the following claims.

a) $\dim_K(P/J) = \dim_K(P/I)$
b) $\mathcal{O} = \mathcal{O}_\sigma(I)$
c) The set $\{g_1, \ldots, g_s\}$ is the reduced σ-Gröbner basis of I.

Exercise 6. Let $P = \mathbb{Q}[x, y]$. Apply the Border Basis Algorithm 6.4.36 to the ideal $I = (x^2 - xy + y^2, x^3 - x^2y, x^2y - xy^2, xy^2 - y^3, x^3 + y^3)$. Is it possible to modify it so that it computes the $\mathcal{O}$-border basis of I with respect to $\mathcal{O} = \{1, x, y, x^2, y^2\}$?

Tutorial 91: Module Structures on Vector Spaces

If you try to fail, and succeed,
which have you done?
(George Carlin)

Both, of course!
(John Abbott)

Suppose we are given a finite dimensional vector space over a field K and we want to turn it into a $K[x_1, \ldots, x_n]$-module. How can we succeed? How could we fail? Is the result going to be a cyclic $K[x_1, \ldots, x_n]$-module or not? How can we check this computationally? Our goal in this tutorial is to guide you to the answers to these questions. Whether we succeed or fail is still up in the air — and even if you don't find the solutions, we hope that you'll at least admire the problems.

Let K be a field, let V be a K-vector space, and let $P = K[x_1, \ldots, x_n]$. If V carries a P-module structure, multiplication by an indeterminate gives an endomorphism of V. For $i = 1, \ldots, n$, the P-linear map $\Phi_i : V \longrightarrow V$ defined by $v \mapsto x_i\, v$ is called the i^{th} **multiplication endomorphism** of V.

a) Let V be a P-module, i.e. assume that V carries a P-module structure. Show that the multiplication endomorphisms of V are pairwise commuting elements of the endomorphism ring $\mathrm{End}_K(V)$, but that this ring is not commutative if $\dim_K(V) \geq 2$.

b) Let $I \subseteq P$ be an ideal. Using the canonical homomorphism $P \twoheadrightarrow P/I$, define a P-module structure on P/I, and show that this P-module is cyclic.

Thus a P-module structure on V gives rise to a set of n pairwise commuting endomorphisms. Now let us find out whether the converse is also true. Let $\Phi_1, \ldots, \Phi_n \in \mathrm{End}_K(V)$ be pairwise commuting.

c) Show that there is a natural way of equipping V with a P-module structure such that Φ_i is the i^{th} multiplication endomorphism of V, namely the structure defined by

$$P \times V \longrightarrow V \qquad \text{such that} \qquad (f, v) \mapsto f(\Phi_1, \ldots, \Phi_n)(v)$$

d) Prove that the map $\eta_\Phi : P \longrightarrow \mathrm{End}_K(V)$ defined by $f \mapsto f(\Phi_1, \ldots, \Phi_n)$ is a ring homomorphism.

e) Show that every ring homomorphism $\eta : P \longrightarrow \mathrm{End}_K(V)$ induces a P-module structure on V via the rule $f \cdot v = \eta(f)(v)$.

Of particular interest are P-module structures on V for which V is a cyclic P-module. We want to show that such structures are essentially of the type given in b). For this we need to consider the **annihilator** of V, i.e. the ideal $\mathrm{Ann}_P(V) = \{f \in P \mid f \cdot V = 0\}$.

f) Let V be equipped with a P-module structure corresponding to a ring homomorphism $\eta : P \longrightarrow \mathrm{End}_K(V)$. Prove that $\mathrm{Ann}_P(V) = \ker(\eta)$.

g) Let V be a cyclic P-module. Show that there exist an ideal $I \subseteq P$ and a P-linear isomorphism $\Theta : P/I \longrightarrow V$ such that the multiplication endomorphisms of V are given by the formula $\Phi_i = \Theta \circ \varphi_i \circ \Theta^{-1}$ where $\varphi_i : P/I \longrightarrow P/I$ is the endomorphism corresponding to multiplication by x_i for $i = 1, \ldots, n$. Moreover, prove that I is zero-dimensional if V is a finite dimensional vector space.
Hint: Let $w \in V$ be a generator of the P-module V. Consider the kernel I of the P-linear map $\tilde{\Theta} : P \longrightarrow V$ given by $1 \mapsto w$.

h) Let V be a P-module, and let $w \in V$. Show that $\mathrm{Ann}_P(V) \subseteq \mathrm{Ann}_P(w)$. Furthermore, prove that $\mathrm{Ann}_P(w) = \mathrm{Ann}_P(V)$ if V is a cyclic P-module with generator w.

i) Let V be a P-module, and let $w \in V$. Show that there exists a P-linear map $\Psi_w : P/\mathrm{Ann}_P(V) \longrightarrow V$ defined by $f + \mathrm{Ann}_P(V) \mapsto f \cdot w$. Prove that the map Ψ_w is an isomorphism of P-modules if and only if w generates V as a P-module.
Hint: To prove that Ψ_w is injective if w generates V, consider $f \in P$ such that $f + \mathrm{Ann}_P(V) \in \ker(\Psi_w)$ and show $f(\Phi_1, \ldots, \Phi_n) = 0$.

In the remaining parts of this tutorial we let V be a finite-dimensional K-vector space of dimension μ. We fix a K-basis $\mathcal{V} = (v_1, \ldots, v_\mu)$ of V. Thus every endomorphism of V can be represented by a matrix of size $\mu \times \mu$ over K. In particular, when V is a P-module, then $\mathcal{M}_1, \ldots, \mathcal{M}_n$ denote the matrices corresponding to the multiplication endomorphisms $\Phi_1, \ldots, \Phi_n$.

Using the following variant of the Buchberger-Möller algorithm, we can calculate $\mathrm{Ann}_P(V)$ as the kernel of the composite map

$$\eta : P \longrightarrow \mathrm{End}_K(V) \cong \mathrm{Mat}_\mu(K)$$

where η is the map defined in e). Moreover, the algorithm provides a vector space basis of $P/\mathrm{Ann}_P(V)$. To facilitate the formulation of this algorithm, we use the following convention. Given a matrix $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_\mu(K)$, we order its entries by letting $a_{ij} \prec a_{k\ell}$ if $i < k$, or if $i = k$ and $j < \ell$. In this way we "flatten" the matrix to a vector in K^{μ^2}. Then we can reduce $\mathcal{A}$ against a list of matrices by using the usual Gaußian reduction procedure.

j) **(The Buchberger-Möller Algorithm for Matrices)**
Let σ be a term ordering on $\mathbb{T}^n$, and let $\mathcal{M}_1, \ldots, \mathcal{M}_n \in \mathrm{Mat}_\mu(K)$ be pairwise commuting. Consider the following sequence of instructions.

M1. Let $G = \emptyset$, $\mathcal{O} = \emptyset$, $S = \emptyset$, $N = \emptyset$, and $L = \{1\}$.

M2. If $L = \emptyset$, return the pair $(G, \mathcal{O})$ and stop. Otherwise let $t = \min_\sigma(L)$ and delete it from L.

M3. Compute $t(\mathcal{M}_1, \ldots, \mathcal{M}_n)$ and reduce it against $N = (\mathcal{N}_1, \ldots, \mathcal{N}_k)$ to obtain

$$\mathcal{R} = t(\mathcal{M}_1, \ldots, \mathcal{M}_n) - \sum_{i=1}^{k} c_i \mathcal{N}_i \qquad \text{with} \quad c_i \in K$$

M4. If $\mathcal{R} = 0$, append the polynomial $t - \sum_i c_i s_i$ to G, where s_i denotes the i^{th} element of S. Remove from L all multiples of t. Continue with step M2.

M5. Otherwise, we have $\mathcal{R} \neq 0$. Append $\mathcal{R}$ to N and $t - \sum_i c_i s_i$ to S. Append the term t to $\mathcal{O}$, and append to L those elements of $\{x_1 t, \ldots, x_n t\}$ which are neither multiples of a term in L nor in $\mathrm{LT}_\sigma(G)$. Continue with step M2.

Prove that this is an algorithm which returns the reduced σ-Gröbner basis G of $\mathrm{Ann}_P(V)$ and a list of terms $\mathcal{O}$ whose residue classes form a K-vector space basis of $P/\mathrm{Ann}_P(V)$.

Hint: You can proceed as follows:

1) To prove termination, use Corollary 1.3.6.
2) Let $I = \mathrm{Ann}_P(V)$, and let H be the reduced σ-Gröbner basis of I. To show correctness, prove by induction that after a term t has been treated by the algorithm, the following holds: the list G contains all elements of H whose leading terms are less than or equal to t, and the list $\mathcal{O}$ contains all elements of $\mathbb{T}^n \setminus \mathrm{LT}_\sigma(I)$ which are less than or equal to t.
3) Show that the polynomial $t - \sum_{i=1}^k c_i s_i$ resulting from step M3 of the next iteration has leading term t.
4) Prove that the polynomial $g = t - \sum_{i=1}^k c_i s_i$ is an element of H if $\mathcal{R} = 0$ in step M4.
5) Finally, show that the term t is not contained in $\mathrm{LT}_\sigma(I)$ if $\mathcal{R} \neq 0$ in step M5.

k) Apply the Buchberger-Möller Algorithm for Matrices to the following example. Let $V = \mathbb{Q}^3$, let $\mathcal{V} = (e_1, e_2, e_3)$ be its canonical basis, and let V be equipped the the $\mathbb{Q}[x, y]$-module structure defined by

$$\mathcal{M}_1 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad \mathcal{M}_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Compute the reduced `DegLex`-Gröbner basis of $\mathrm{Ann}_P(V)$ and a K-basis of $P/\mathrm{Ann}_P(V)$.

l) Write a CoCoA function `BuMoMat(...)` which implements the algorithm of j). Apply your function to the example in k) and compare its result to yours.

Now we are ready for the main algorithm of this tutorial: we can check effectively whether a P-module structure given by commuting matrices defines a cyclic module.

m) **(Cyclicity Test)**
Let V be a finite dimensional K-vector space with basis $\mathcal{V} = (v_1, \ldots, v_\mu)$, and let $\Phi_1, \ldots, \Phi_n$ be pairwise commuting endomorphisms of V given by their respective matrices $\mathcal{M}_1, \ldots, \mathcal{M}_n$. We equip V with the P-module

structure defined by $\Phi_1, \ldots, \Phi_n$. Consider the following sequence of instructions.

C1. Using the Buchberger-Möller Algorithm for Matrices, compute a tuple of terms $\mathcal{O} = (t_1, \ldots, t_m)$ whose residue classes form a K-basis of $P/\operatorname{Ann}_P(V)$.
C2. If $m \neq \mu$ then return `"V is not cyclic"` and stop.
C3. Let $z_1, \ldots, z_\mu$ be new indeterminates and $\mathcal{A} \in \operatorname{Mat}_\mu(K[z_1, \ldots, z_\mu])$ the matrix whose columns are $t_i(\mathcal{M}_1, \ldots, \mathcal{M}_n) \cdot (z_1, \ldots, z_\mu)^{\mathrm{tr}}$ for $i = 1, \ldots, \mu$. Compute the determinant $d = \det(\mathcal{A}) \in K[z_1, \ldots, z_\mu]$.
C4. Check if there exists a tuple $(c_1, \ldots, c_\mu) \in K^\mu$ for which the polynomial value $d(c_1, \ldots, c_\mu)$ is non-zero. In this case return `"V is cyclic"` and $w = c_1 v_1 + \cdots + c_\mu v_\mu$. Then stop.
C5. Return `"V is not cyclic"` and stop.

Prove that this is an algorithm which checks whether V is cyclic and, in the affirmative case, computes a generator.
Hint: Use i). Examine the images of the basis elements $\{\bar{t}_1, \ldots, \bar{t}_\mu\}$ for linear independence.

n) Apply the Cyclicity Test to the example in k). Show that V is cyclic and find a generator.

o) Let $V = \mathbb{Q}^3$, let $\mathcal{V} = (e_1, e_2, e_3)$ be its canonical basis, and equip V with the $\mathbb{Q}[x, y]$-module structure defined by the commuting matrices

$$\mathcal{M}_1 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \mathcal{M}_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Apply the Cyclicity Test and show that V is not cyclic although the dimensions of V and of $P/\operatorname{Ann}_P(V)$ coincide.

p) Write a CoCoA function `CyclTest(...)` which takes a list of n commuting matrices and checks whether they define a cyclic P-module. Apply your function to the examples in k) and o).
Hint: If the field K is infinite, the check in step C4 can be simplified to checking $d \neq 0$. For a finite field K, we can, in principle, check all tuples in K^μ.

We end this tutorial by considering the special case $n = 1$. Let $\mathcal{M}$ be a matrix representing an endomorphism $\Phi \in \operatorname{End}_K(V)$, and let V be equipped with the $K[x]$-module structure defined by $(f, v) \mapsto f(\Phi)(v)$. When is V a cyclic P-module? Let us interpret the meaning of the steps of our cyclicity test in this case.

q) Show that the Buchberger-Möller Algorithm for Matrices yields a monic polynomial $f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0$, which is the **minimal polynomial** of $\mathcal{M}$ (and of Φ), and the tuple $\mathcal{O} = (1, x, x^2, \ldots, x^{d-1})$.

r) Prove that the algorithm stops at step C2 only if the minimal polynomial and the characteristic polynomial of $\mathcal{M}$ differ.

s) Suppose we reach step C3. Show that then $\det(\mathcal{M})$ necessarily is non-zero and V is a cyclic P-module. In conclusion, steps C3, C4, C5 are redundant in the univariate case. This corresponds to the well-known fact that V is a cyclic $K[x]$-module if and only if the minimal polynomial and the characteristic polynomial of Φ coincide.

Tutorial 92: Design of Experiments

Probability and statistics will come to be viewed
as the natural tools in mathematical
as well as scientific modelling.
The intellectual world will come to view
logic as a beautiful elegant idealization,
but to view statistics as the standard way
in which we reason and think.
(David Mumford)

If statistics is really going to be the standard way in which we reason and think, it cannot hurt to stray for a while into the world of scientific modelling. We invite you to follow us on an excursion into a part of statistics called *design of experiments*. To motivate the terminology introduced later, let us start with an actual statistical problem.

A number of similar chemical plants had been successfully operating for several years in different locations. In a newly constructed plant the filtration cycle took almost twice as long as in the older plants. Seven possible causes of the difficulty were considered by the experts.

1. The water for the new plant was different in mineral content.
2. The raw material was not identical in all respects to that used in the older plants.
3. The temperature of filtration in the new plant was slightly lower than in the older plants.
4. A new recycle device was absent in the older plants.
5. The rate of addition of caustic soda was higher in the new plant.
6. A new type of filter cloth was being used in the new plant.
7. The holdup time was lower than in the older plants.

These causes lead to seven variables $x_1, \ldots, x_7$. Each of them can assume only two values, namely *old* and *new* which we denote by 0 and 1, respectively. All possible combinations of these values form the full design $D = \{0,1\}^7 \subseteq \mathbb{A}^7(\mathbb{Q})$ (see Definition 6.3.7). Its vanishing ideal is $\mathcal{I}(D) = (x_1^2 - x_1, x_2^2 - x_2, \ldots, x_7^2 - x_7)$ in the polynomial ring $\mathbb{Q}[x_1, \ldots, x_7]$.

Our task is to identify an unknown function $\bar{f} : D \longrightarrow K$, namely the length of a filtration cycle. This function is called the **model**, since it is a mathematical model of the quantity which has to be computed or optimized. In order to fully identify it, we would have to perform $128 = 2^7$ cycles. This

is impracticable since it would require too much time and money. On the other hand, suppose for a moment that we had conducted all experiments and the result was $\bar{f} = a + b\,x_1 + c\,x_2$ for some $a, b, c \in \mathbb{Q}$. At this point it becomes clear that we have wasted many resources. Had we known in advance that $\bar{f}$ is given by a polynomial having only three unknown coefficients, we could have identified them by performing only *three* suitable experiments! Namely, if we determine three values of the polynomial $a + b\,x_1 + c\,x_2$ and the associated matrix of coefficients is invertible, we can easily find a, b, c by solving a system of three linear equations in these three unknowns.

However, *a priori* one does not know that the answer has the shape indicated above. In practice, one has to make some guesses, perform well-chosen experiments, and possibly modify the guesses until the process yields the desired answer. In the case of the chemical plant, it turned out that only x_1 and x_5 were relevant for identifying the model.

Motivated by this example, we introduce the statistical jargon which is commonly used in the design of experiments. Let K be a field. For $i = 1, \ldots, n$, let $\ell_i \geq 1$ and $D_i = \{a_{i1}, a_{i2}, \ldots, a_{i\ell_i}\} \subseteq K$. Then we say that the **full design** $D = D_1 \times \cdots \times D_n \subseteq \mathbb{A}^n(K)$ has **levels** $(\ell_1, \ldots \ell_n)$.

The polynomials $f_i = (x_i - a_{i1}) \cdots (x_i - a_{i\ell_i})$ with $i = 1, \ldots, n$ generate the vanishing ideal $\mathcal{I}(D) \subseteq P$ of D. They are called the **canonical polynomials** of D. For any term ordering σ on $\mathbb{T}^n$, the canonical polynomials are the reduced σ-Gröbner basis of $\mathcal{I}(D)$ (see Proposition 6.3.8). Thus the order ideal

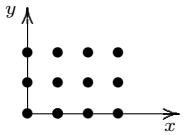
$$\mathcal{O}_D = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid 0 \leq \alpha_i < \ell_i \text{ for } i = 1, \ldots, n\}$$

is canonically associated to D and represents a K-basis of $P/\mathcal{I}(D)$.

Our main task is to identify an unknown function $\bar{f} : D \longrightarrow K$ called the **model**. Since it is defined on a finite set, it can in principle be determined by performing all experiments corresponding to the points in D and measuring the value of $\bar{f}$ each time. A subset F of a full design D is called a **fraction**. We want to choose a fraction $F \subseteq D$ that allows us to identify the model if we have some extra knowledge about the form of $\bar{f}$. In particular, we need to describe the order ideals whose residue classes form a K-basis of $P/\mathcal{I}(F)$. Statisticians express this property by saying that such order ideals are **identified by** F.

To get better acquainted with these definitions, it is best to reason and think statistically and solve a few easy problems.

a) Show that every model $\bar{f} : D \longrightarrow K$ is a polynomial function, i.e. that there exists a polynomial $f \in P$ such that $\bar{f}(p) = f(p)$ for all $p \in D$.
b) Consider the full design $D = \{0, 1, 2, 3\} \times \{0, 1, 2\}$



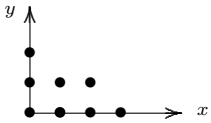
in $\mathbb{A}^2(\mathbb{Q})$. Determine the canonical polynomials and the order ideal $\mathcal{O}_D$.

c) Let $F = \{p_1, \ldots, p_\mu\} \subseteq D$ be a fraction and $\mathcal{O} = \{t_1, \ldots, t_\nu\} \subseteq \mathcal{O}_D$ an order ideal. Prove that the following conditions are equivalent.
   1) The order ideal $\mathcal{O}$ is identified by the fraction F.
   2) The vanishing ideal $\mathcal{I}(F)$ has an $\mathcal{O}$-border basis.
   3) We have $\mu = \nu$ and $\det(t_i(p_j)) \neq 0$.

In the last condition there is one point which needs additional explanation. How can we choose the fraction F such that the matrix of coefficients is invertible? In other words, given a full design D and an order ideal $\mathcal{O} \subseteq \mathcal{O}_D$, which fractions $F \subseteq D$ have the property that the residue classes of the elements of $\mathcal{O}$ are a K-basis of $P/\mathcal{I}(F)$? We call this the **inverse problem**. Below we develop an algorithm which solves the inverse problem, but before doing so we need some preparations.

Using **distracted fractions**, one can show that there always exists at least one solution of the inverse problem. Let us look at an example to illustrate the method.

d) Let D be the full design $D = \{0, 1, 2, 3\} \times \{0, 1, 2\}$ contained in $\mathbb{A}^2(\mathbb{Q})$, and let $\mathcal{O} = \{1, x, y, x^2, xy, y^2, x^3, x^2y\} \subset \mathcal{O}_D$. The order ideal $\mathcal{O}$ can be visualized as follows.



Use the **distracted fraction**, i.e. the fraction whose points are the points marked by bullets in the above sketch, to identify $\mathcal{O}$. For an arbitrary term ordering σ, find the reduced σ-Gröbner basis of $\mathcal{I}(F)$ and prove that $\mathcal{O} = \mathbb{T}^n \setminus \mathrm{LT}_\sigma\{\mathcal{I}(F)\}$.

e) Let D be a full design, let $\{f_1, \ldots, f_n\}$ be its canonical polynomials, let $\overline{K}$ be the algebraic closure of K, and let I be a proper ideal of $\overline{K}[x_1, \ldots, x_n]$ such that $\mathcal{I}(D) \subseteq I$. Show that the ideal I has the following properties.
   1) The ideal I is a radical ideal. It is the vanishing ideal of a fraction of D.
   2) The ideal I is generated by elements of P, and $I \cap P$ is a radical ideal.
   3) The polynomials of every border basis of I are elements of P.

   Hint: To prove 1), let $F = \mathcal{Z}(I)$ and show $I = \mathcal{I}(F)$.

Now we are ready to state the main result of this tutorial. Our goal is to solve the inverse problem. The idea is to proceed as follows. We are given a full design D and an order ideal $\mathcal{O}$. By Proposition 6.4.17, there is a 1-1 correspondence between ideals I for which the residue classes of the terms in $\mathcal{O}$ are a K-basis of P/I and border bases whose elements are "marked" by the

terms in $\partial\mathcal{O}$. Except for the border basis elements which are canonical polynomials of D, we can write them down using indeterminate coefficients and require that the corresponding formal multiplication matrices are pairwise commuting. For I to be the vanishing ideal of a fraction contained in D, we have to make sure that I contains I_D. To this end, we require that the normal $\mathcal{O}$-remainders of the canonical polynomials of D are zero. By combining these requirements, we come to the following result.

f) **(Computing All Fractions)**
Let D be a full design with levels $(\ell_1, \ldots, \ell_n)$, and let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal contained in $\mathcal{O}_D$ with $t_1 = 1$. Consider the following definitions.

1) Let $C = \{f_1, \ldots, f_n\}$ be the set of canonical polynomials of D, where f_i is marked by $x_i^{\ell_i}$, i.e. $\mathrm{LT}_\sigma(f_i) = x_i^{\ell_i}$ for any term ordering σ.
2) Decompose $\partial\mathcal{O}$ into two subsets $\partial\mathcal{O}_1 = \{x_1^{\ell_1}, \ldots, x_n^{\ell_n}\} \cap \partial\mathcal{O}$ and $\partial\mathcal{O}_2 = \partial\mathcal{O} \setminus \partial\mathcal{O}_1$.
3) Let C_1 be the subset of C marked by elements of $\partial\mathcal{O}_1$, and let $C_2 = C \setminus C_1$.
4) Let $\eta = \#(\partial\mathcal{O}_2)$. For $i = 1, \ldots, \eta$ and $j = 1, \ldots, \mu$, introduce new indeterminates z_{ij}.
5) For every $b_k \in \partial\mathcal{O}_2$, let $g_k = b_k - \sum_{j=1}^{\mu} z_{kj} t_j \in K(z_{ij})[x_1, \ldots, x_n]$.
6) Let $G = \{g_1, \ldots, g_\eta\}$ and $H = G \cup C_1$. Let $\mathcal{M}_1, \ldots, \mathcal{M}_n$ be the formal multiplication matrices associated to the $\mathcal{O}$-border prebasis H.
7) Let $\mathcal{I}(\mathcal{O})$ be the ideal in $K[z_{ij}]$ generated by the entries of the matrices $\mathcal{M}_i\mathcal{M}_j - \mathcal{M}_j\mathcal{M}_i$ for $1 \le i < j \le n$, and by the entries of the column matrices $f(\mathcal{M}_1, \ldots, \mathcal{M}_n) \cdot e_1$ for all $f \in C_2$ where $e_1 = (1, 0, \ldots, 0)^{\mathrm{tr}}$.

Then show that $\mathcal{I}(\mathcal{O})$ is a zero-dimensional ideal in $K[z_{ij}]$ whose zeros are in 1-1 correspondence with the solutions of the inverse problem, i.e. with fractions $F \subseteq D$ such that $\mathcal{O}$ represents a K-basis of $P/\mathcal{I}(F)$.
Extended hint: To show that every $p = (p_{ij}) \in \mathcal{Z}_K(\mathcal{I}(\mathcal{O}))$ yields a fraction F which identifies $\mathcal{O}$, prove the following claims:

1) Let $\overline{}$ denote the substitution homomorphism $z_{ij} \mapsto p_{ij}$. Then we have $f(\overline{\mathcal{M}}_1, \ldots, \overline{\mathcal{M}}_n) \cdot e_1 = 0$ for every $f \in C_2$.
2) The set $\overline{H} = \overline{G} \cup C_1$ is the $\mathcal{O}$-border basis of the ideal $\overline{I}$ generated by it.
3) We have $f \in \overline{I}$ for all $f \in C_2$.
4) The ideal $\overline{I}$ is the vanishing ideal of a fraction of D.

Conversely, let $F \subseteq D$ be a fraction which identifies $\mathcal{O}$. Find a corresponding zero of $\mathcal{I}(\mathcal{O})$ as follows:

1) Let B be the $\mathcal{O}$-border basis of $\mathcal{I}(F)$, write $B = B_1 \cup B_2$, and show $B_1 = C_1$.

2) Write the polynomials in B_2 in the form $\bar{g}_k = b_k - \sum_{j=1}^{\mu} \alpha_{kj} t_j$ where $b_k \in \partial\mathcal{O}_2$ and $\alpha_{kj} \in K$. Let $p = (\alpha_{ij}) \in K^{\mu\eta}$.
3) Prove $f(\overline{\mathcal{M}}_1, \ldots, \overline{\mathcal{M}}_n) \cdot e_1 = \mathrm{NF}_{\mathcal{O},\mathcal{I}(F)}(f)$.
4) Show that p is a zero of $\mathcal{I}(\mathcal{O})$.

g) Let D be the full design $D = \{-1, 0, 1\} \times \{-1, 1\}$ with levels $(3, 2)$ contained in $\mathbb{A}^2(\mathbb{Q})$. Solve the inverse problem for the order ideal $\mathcal{O} = \{1, x, y\}$ by following the steps of f). In particular, show that $\mathcal{I}(\mathcal{O}) = (z_{12}z_{21} - z_{11}z_{22} - z_{21}z_{23} + z_{13},\ z_{21}z_{22} + z_{23},\ z_{22}z_{23} + z_{21},\ z_{22}^2 - 1,\ z_{13}z_{22} - z_{12}z_{23} + z_{23}^2 - z_{11},\ z_{22}z_{23} + z_{21},\ z_{11}z_{12} + z_{13}z_{21},\ z_{12}^2 + z_{13}z_{22} + z_{11} - 1,\ z_{12}z_{13} + z_{13}z_{23})$. Using CoCoA, check that $\mathcal{I}(O)$ is a zero-dimensional, radical ideal of multiplicity 18. This means that among the $20 = \binom{6}{3}$ triples of points of D, there are 18 triples which solve the inverse problem. Show that the two missing fractions are $\{(0, 0), (0, 1), (0, -1)\}$ and $\{(1, 0), (1, 1), (1, -1)\}$.

h) Let D be the full design $D = \{-1, 0, 1\} \times \{-1, 0, 1\}$ with levels $(3, 3)$ contained in $\mathbb{A}^2(\mathbb{Q})$. Solve the inverse problem for the order ideal $\mathcal{O} = \{1, x, y, x^2, y^2\}$ by following the steps of f). In particular, show that $\mathcal{I}(\mathcal{O})$ is the ideal generated by the following 20 polynomials:

$$
\begin{array}{cc}
z_{21}z_{23} + z_{25}z_{31} - z_{11} & z_{21}z_{22} + z_{11}z_{24} - z_{31} \\
z_{13}z_{21} + z_{15}z_{31} - z_{21} & z_{21}z_{32} + z_{11}z_{34} - z_{21} \\
z_{22}z_{23} + z_{25}z_{32} - z_{12} + z_{21} + z_{24} & z_{22}^2 + z_{12}z_{24} - z_{32} \\
z_{13}z_{22} + z_{15}z_{32} + z_{11} + z_{14} - z_{22} & z_{22}z_{32} + z_{12}z_{34} - z_{22} \\
z_{23}^2 + z_{25}z_{33} - z_{13} & z_{22}z_{23} + z_{13}z_{24} + z_{21} + z_{25} - z_{33} \\
z_{13}z_{23} + z_{15}z_{33} - z_{23} & z_{23}z_{32} + z_{13}z_{34} - z_{23} + z_{31} + z_{35} \\
z_{23}z_{24} + z_{25}z_{34} - z_{14} + z_{22} & z_{14}z_{24} + z_{22}z_{24} - z_{34} \\
z_{13}z_{24} + z_{15}z_{34} + z_{12} - z_{24} & z_{24}z_{32} + z_{14}z_{34} - z_{24} \\
z_{23}z_{25} + z_{25}z_{35} - z_{15} & z_{15}z_{24} + z_{22}z_{25} + z_{23} - z_{35} \\
z_{13}z_{25} + z_{15}z_{35} - z_{25} & z_{25}z_{32} + z_{15}z_{34} - z_{25} + z_{33}
\end{array}
$$

Using CoCoA, check that $\mathcal{I}(\mathcal{O})$ is a zero-dimensional, radical ideal of multiplicity 81. This means that among the $126 = \binom{9}{5}$ five-tuples of points in D there are 81 five-tuples which solve the inverse problem.

i) Show that one of the zeros of the ideal $\mathcal{I}(\mathcal{O})$ in h) is the point $p \in \mathbb{Q}^{15}$ whose coordinates are

$$
\begin{array}{lllll}
z_{11} = 0 & z_{12} = 0 & z_{13} = -\frac{1}{2} & z_{14} = 0 & z_{15} = -\frac{1}{2} \\
z_{21} = 0 & z_{22} = -1 & z_{23} = -\frac{1}{2} & z_{24} = 1 & z_{25} = -\frac{1}{2} \\
z_{31} = 0 & z_{32} = -1 & z_{33} = -\frac{1}{2} & z_{34} = 1 & z_{35} = -\frac{1}{2}
\end{array}
$$

Find the corresponding $\mathcal{O}$-border basis and the fraction defined by this basis. (It is our old friend from Example 6.4.16!)

j) In view of our discussion in this section, it is natural to ask how many of the 81 fractions F found in h) have the property that $\mathcal{O}$ is not of the form $\mathbb{T}^n \setminus \mathrm{LT}_\sigma\{\mathcal{I}(F)\}$ for any term ordering σ. One can prove that 36 of those 81 fractions are of that type. Try to find as many of these as possible

(See also Exercise 5). This is a surprisingly high number which shows that border bases provide sometimes a much more flexible environment for working with zero-dimensional ideals than Gröbner bases do.

6.5 Filtrations

Lua,[...] *Moon,[...]*
Desmetaforizada *Without the metaphors*
Desmitificada,[...] *Without the mythology,[...]*
Gosto de ti assim: *I like you as you are:*
Coisa em si, *Object that you are,*
- Satélite. *- A satellite.*
(Manuel Bandeira, Brazilian poet)

Sometimes you are in a melancholic mood and you think back to the good old days when a friend of yours was declaiming sagacious Brazilian poems by Manuel Bandeira. Quite naturally, the flow of your memories carries you to a romantic night under the full moon on a Brazilian beach. You realize that, despite your efforts to think of it as a mere satellite hovering over a stretch of sand, a touch of magic emanates from this scenery. Suddenly a mixture of *samba* and *forrò* fills your mind. An old *bossa nova* overlaps the rhythm of a traditional *frevo*, and the combination is both mesmerizing and addictive.

As you try to filter the tunes and thoughts, the shrill ring of your telephone pulls you back to reality. Now the necessary filtrations are of a totally different nature. So, what are we talking about here? After discussing briefly which kind of filtrations we are *not* looking at, we define a filtration Φ on an algebra R over a field K as a family of K-vector subspaces $\Phi = \{F_\gamma R \mid \gamma \in \mathbb{Z}^m\}$ of R which obeys a few natural rules (see Definition 6.5.1). We show that this definition generalizes several settings considered in earlier chapters, e.g. those for the theories of Macaulay bases and Gröbner bases (see Examples 6.5.3 and 6.5.4). If we require the filtration to be reasonably well-behaved, i.e. to be orderly and separated, we can introduce leading forms with respect to Φ as elements of a ring called the associated graded ring. Here an important difference with the earlier theories surfaces. So far we have never noticed the associated graded ring of $K[x_1, \ldots, x_n]$ because it was always isomorphic to $K[x_1, \ldots, x_n]$ (see Proposition 6.5.8). Using leading forms, we can then define leading form ideals and Φ-standard bases, the generalization of Macaulay and Gröbner bases.

After studying the basic properties of these constructions, we apply them in the second subsection to a very different kind of filtration. Given an ideal I of R, the I-adic filtration Φ is defined by the powers of I, i.e. by the family $\Phi = \{I^{-\gamma} \mid \gamma \in \mathbb{Z}\}$. (The minus sign serves to make this an ascending filtration. For $\gamma \geq 0$, we define $I^{-\gamma} = R$.) We show that for these filtrations the properties of being orderly and separated coincide. The proof of this result uses some beautiful pieces of commutative algebra: the Artin-Rees Lemma (see Theorem 6.5.20) and Krull's Intersection Theorem (see Theorem 6.5.21).

Then we come to the central computational result of this section. Based on Lazard's Method (see Theorem 6.5.25), we explain an algorithm for computing tangent cones at the origin. Geometrically, tangent cones generalize

the notion of a tangent line to a curve at a smooth point. But don't worry, for us they are algebraic objects which can be computed. In fact, their computation corresponds to finding the leading form ideal of an ideal with respect to the $(x_1, \ldots, x_n)$-adic filtration on $K[x_1, \ldots, x_n]$ (see Corollary 6.5.26).

Here the section stops, but the real fun is just about to begin. We have prepared for you three major tutorials. The first tutorial deals with Mora's Algorithm for computing standard bases (see Tutorial 93), the second shows you how to define and compute Hilbert functions of filtered rings (see Tutorial 94), and the third gives you a glimpse of the vast ocean of theory concerning singular points on algebraic varieties (see Tutorial 95). And we are not referring to that singular little point on the horizon: a small boat sailing slowly into the Brazilian twilight.

O barquinho vai, a tardinha cai ...

6.5.1 General Filtrations

The poly-ring panel filter is perfect
for a number of filtration applications.
(Air Filtration Product Advertisement)

In the last tutorial we encountered filtrations in a chemical plant. So, what is a filtration? A dictionary suggests the following definition.

> **Filtration:** *the physical or mechanical process of separating insoluble particulate matter from a fluid, such as air or liquid, by passing the fluid through a filter medium that will not allow the particulates to pass through it.*

However, we want to filter polynomial rings, not fluids. In that case, even the well advertised poly-ring panel filter is not perfect. Clearly, we need a different kind of device. Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let R be a K-algebra.

Definition 6.5.1. Let $m \geq 1$, let σ be a monoid ordering on $\mathbb{Z}^m$, and for every $\gamma \in \mathbb{Z}^m$ let $F_\gamma R$ denote a K-vector subspace of R. The family $\Phi = \{F_\gamma R \mid \gamma \in \mathbb{Z}^m\}$ is said to be a $(\mathbb{Z}^m, \sigma)$**-filtration** on R if the following conditions are satisfied:

a) $F_\gamma R \subseteq F_{\gamma'} R$ for all $\gamma, \gamma' \in \mathbb{Z}^m$ with $\gamma \leq_\sigma \gamma'$
b) $\bigcup_{\gamma \in \mathbb{Z}^m} F_\gamma R = R$
c) $(F_\gamma R) \cdot (F_{\gamma'} R) \subseteq F_{\gamma+\gamma'} R$ for all $\gamma, \gamma' \in \mathbb{Z}^m$
d) $1 \in F_0 R$ and $1 \notin F_\gamma R$ if $\gamma <_\sigma 0$

When the indexing set $\mathbb{Z}^m$ and the ordering σ are clear, the family Φ is simply called a **filtration** on R.

You may not have noticed, but we have already encountered a number of filtrations on the polynomial ring P, although we have never identified them explicitly as such. The simplest example is the filtration induced by the degree of a polynomial. This filtration was used implicitly in Section 5.6.

Example 6.5.2. Let σ be the monoid ordering $<$ on $\mathbb{Z}$, and let P be standard graded. For $\gamma \in \mathbb{Z}$, let $F_\gamma P = \{f \in P \setminus \{0\} \mid \deg(f) \leq \gamma\} \cup \{0\}$. Then the family $\Phi = \{F_\gamma P \mid \gamma \in \mathbb{Z}\}$ is a $(\mathbb{Z}, \sigma)$-filtration on P. It is called the **standard degree filtration** on P.

More generally, if P is graded by a matrix and the degrees are ordered by `Lex` as in Section 4.2, there exists a filtration associated to this grading.

Example 6.5.3. Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. For every $\gamma \in \mathbb{Z}^m$, let $F_\gamma P = \{f \in P \setminus \{0\} \mid \deg_W(f) \leq_{\mathtt{Lex}} \gamma\} \cup \{0\}$. Then it is easy to check that $\Phi = \{F_\gamma P \mid \gamma \in \mathbb{Z}^m\}$ is a $(\mathbb{Z}^m, \mathtt{Lex})$-filtration on P. It is called the **$\deg_W$-filtration** on P.

Later we shall see that Macaulay bases are related to filtrations. In fact, Gröbner bases, too, are related to filtrations. The basic link is given by the following example.

Example 6.5.4. Let σ be a term ordering on $\mathbb{T}^n$. Using the isomorphism of monoids $\log : \mathbb{T}^n \longrightarrow \mathbb{N}^n$, we can view σ as a monoid ordering on $\mathbb{N}^n$, and using Proposition 1.4.14, we can extend σ uniquely to a monoid ordering on $\mathbb{Z}^n$ which we denote by σ again. For every $\gamma \in \mathbb{Z}^n$, we define the vector space $F_\gamma P = \{f \in P \setminus \{0\} \mid \log(\mathrm{LT}_\sigma(f)) \leq_\sigma \gamma\} \cup \{0\}$. Then it is easy to see that $\Phi = \{F_\gamma P \mid \gamma \in \mathbb{Z}^n\}$ is a $(\mathbb{Z}^n, \sigma)$-filtration on P. It is called the **σ-Gröbner filtration** on P.

Both $\deg_W$-filtrations and Gröbner filtrations are special cases of the following more general construction. If P is graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ and we use a term ordering σ to compare the degrees, we can define a $(\mathbb{Z}^m, \sigma)$-filtration on P by letting $F_\gamma P = \{f \in P \setminus \{0\} \mid \deg_W(f) \leq_\sigma \gamma\} \cup \{0\}$ for all $\gamma \in \mathbb{Z}^n$. Before studying filtrations any further, we have to generalize them to modules, of course.

Definition 6.5.5. Let M be an R-module, let $m \geq 1$, let σ be a monoid ordering on $\mathbb{Z}^m$, and let Φ be a $(\mathbb{Z}^m, \sigma)$-filtration on R. Furthermore, for every $\gamma \in \mathbb{Z}^m$ let $F_\gamma M$ be a K-vector subspace of M.

The family $\Psi = \{F_\gamma M \mid \gamma \in \mathbb{Z}^m\}$ is called a **$(\mathbb{Z}^m, \sigma)$-filtration** on M which is compatible with Φ if the following conditions are satisfied:

a) $F_\gamma M \subseteq F_{\gamma'} M$ for all $\gamma, \gamma' \in \mathbb{Z}^m$ with $\gamma \leq_\sigma \gamma'$
b) $\bigcup_{\gamma \in \mathbb{Z}^m} F_\gamma M = M$
c) $(F_\gamma R) \cdot (F_{\gamma'} M) \subseteq F_{\gamma+\gamma'} M$ for all $\gamma, \gamma' \in \mathbb{Z}^m$

We simply say that Ψ is a **filtration** on M if it is clear which ordering σ and which filtration Φ on R we are considering.

If the polynomial ring P is graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ and M is a graded P-module, there exists a natural $\deg_W$-filtration on M compatible with the $\deg_W$-filtration on P, namely the filtration given by the vector spaces $F_\gamma M = \{v \in M \setminus \{0\} \mid \deg_W(v) \leq_{\mathtt{Lex}} \gamma\} \cup \{0\}$ for $\gamma \in \mathbb{Z}^m$.

Aside from the fact that it is easy to find examples, one fundamental question remains unanswered: Why do we want to filter polynomial rings and modules? This brings us to the *Leitmotiv* of this section. Filtrations are a hidden thread connecting several topics we have discussed, for instance Gröbner bases and Macaulay bases. But they are not only an abstract generalization, they also enable us to treat standard bases and tangent cones in the second subsection. For this purpose we need some additional bits of the general theory.

In the following we want to produce a graded ring from a filtered one and a graded module over that graded ring from a filtered module. Let R be a K-algebra, let $m \geq 1$, and let σ be a monoid ordering on $\mathbb{Z}^m$. Moreover, let $\Phi = \{F_\gamma R \mid \gamma \in \mathbb{Z}^m\}$ be a $(\mathbb{Z}^m, \sigma)$-filtration on R, let M be an R-module, and let M be equipped with a $(\mathbb{Z}^m, \sigma)$-filtration $\Psi = \{F_\gamma M \mid \gamma \in \mathbb{Z}^m\}$ which is compatible with Φ. For any $\gamma \in \mathbb{Z}^m$, we denote the K-vector space $\bigcup_{\gamma' <_\sigma \gamma} F_{\gamma'} M$ by $F_{<_\sigma \gamma} M$.

Remark 6.5.6. Let $\gamma, \gamma' \in \mathbb{Z}^m$. To define a product

$$(F_\gamma R / F_{<_\sigma \gamma} R) \times (F_{\gamma'} R / F_{<_\sigma \gamma'} R) \longrightarrow F_{\gamma+\gamma'} R / F_{<_\sigma \gamma+\gamma'} R$$

we let $\overline{a}_1$ and $\overline{a}_2$ be the residue classes of two elements $a_1 \in F_\gamma R$ and $a_2 \in F_{\gamma'} R$. Then we set $\overline{a}_1 \cdot \overline{a}_2 = \overline{a_1\, a_2}$. This yields a well-defined element in $F_{\gamma+\gamma'} R / F_{<_\sigma \gamma+\gamma'} R$ because we have $a_1\, a_2 \in F_{\gamma+\gamma'} R$ by Definition 6.5.1.c and for $a_3 \in F_{<_\sigma \gamma} R$ and $a_4 \in F_{<_\sigma \gamma'} R$ we have

$$\overline{(a_1 + a_3)\,(a_2 + a_4)} = \overline{a_1\, a_2} + \overline{a_1 a_4 + a_2 a_3 + a_3 a_4} = \overline{a_1\, a_2}$$

It is straightforward to check that the K-vector space $\bigoplus_{\gamma \in \mathbb{Z}^m} F_\gamma R / F_{<_\sigma \gamma} R$ becomes a $\mathbb{Z}^m$-graded K-algebra if we equip it with this multiplication.

Likewise, we can equip the K-vector space $\bigoplus_{\gamma \in \mathbb{Z}^m} F_\gamma M / F_{<_\sigma \gamma} M$ with the well-defined scalar multiplication induced by

$$(F_\gamma R / F_{<_\sigma \gamma} R) \times (F_{\gamma'} M / F_{<_\sigma \gamma'} M) \longrightarrow F_{\gamma+\gamma'} M / F_{<_\sigma \gamma+\gamma'} M$$

Definition 6.5.7. The $\mathbb{Z}^m$-graded K-algebra $\mathrm{gr}_\Phi(R) = \bigoplus_{\gamma \in \mathbb{Z}^m} F_\gamma R / F_{<_\sigma \gamma} R$ is called the **associated graded ring** of R with respect to the filtration Φ. The K-vector space $\mathrm{gr}_\Psi(M) = \bigoplus_{\gamma \in \mathbb{Z}^m} F_\gamma M / F_{<_\sigma \gamma} M$, equipped with the scalar multiplication defined above, is a $\mathbb{Z}^m$-graded $\mathrm{gr}_\Phi(R)$-module. It is called the **associated graded module** of M with respect to Ψ.

Sometimes associated graded rings and associated graded modules are easy to describe.

Proposition 6.5.8. *Let $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let P be equipped with the grading given by W and the $\deg_W$-filtration Φ. Moreover, let M be a graded P-module, and let Ψ be the $\deg_W$-filtration on M.*

Let $\lambda : P \longrightarrow \mathrm{gr}_\Phi(P)$ be the map of $\mathbb{Z}^m$-graded rings defined as follows. Given $\gamma \in \mathbb{Z}^m$ and a homogeneous polynomial $f \in P_\gamma$, let $\lambda(f)$ be the residue class of f in $\mathrm{gr}_\Phi(P)_\gamma = F_\gamma P / F_{<_{\mathrm{Lex}}\gamma} P$. Extend this definition to P by sending a polynomial to the sum of the images of its homogeneous components.

a) The map λ is an isomorphism of $\mathbb{Z}^m$-graded K-algebras.
b) If we view $\mathrm{gr}_\Psi(M)$ as a P-module via λ, there is an isomorphism of graded P-modules $\mu : M \longrightarrow \mathrm{gr}_\Psi(M)$
c) Given a term ordering σ and the σ-Gröbner filtration Φ' on P, we have a natural isomorphism of $\mathbb{Z}^n$-graded K-algebras $P \longrightarrow \mathrm{gr}_{\Phi'}(P)$ which maps a term t to its residue class in $\mathrm{gr}_{\Phi'}(P)_{\log(t)}$.

Proof. For each $\gamma \in \mathbb{Z}^m$, the restriction of the map λ to P_γ is the composition of the inclusion $P_\gamma \hookrightarrow F_\gamma P$ with the canonical surjective map $F_\gamma P \twoheadrightarrow F_\gamma P / F_{<_{\mathrm{Lex}}\gamma} P$. It is injective because we have $P_\gamma \cap F_{<_{\mathrm{Lex}}\gamma} P = \{0\}$. It is surjective because the residue class of a polynomial in $F_\gamma P$ is the residue class of its homogeneous component of degree γ. Thus the map λ is bijective. By the construction of the multiplication in $\mathrm{gr}_\Phi(P)$, it is an isomorphism of graded K-algebras. This proves claim a). Claims b) and c) follow in the same way. □

Our next proposition clarifies the behaviour of filtrations and associated graded modules under the processes of forming submodules and residue class modules.

Proposition 6.5.9. *Let N be an R-submodule of M.*

a) For every $\gamma \in \mathbb{Z}^m$, we define the K-vector subspace $F_\gamma N = (F_\gamma M) \cap N$. Then the family $\widetilde{\Psi} = \{F_\gamma N \mid \gamma \in \mathbb{Z}^m\}$ is a $(\mathbb{Z}^m, \sigma)$-filtration on N. It is called the **induced filtration** *on N.*
b) The canonical K-linear maps $F_\gamma N / F_{<_\sigma \gamma} N \longrightarrow F_\gamma M / F_{<_\sigma \gamma} M$ give rise to a homogeneous injective $\mathrm{gr}_\Phi(R)$-linear map $\alpha : \mathrm{gr}_{\widetilde{\Psi}}(N) \longrightarrow \mathrm{gr}_\Psi(M)$.
c) For every $\gamma \in \mathbb{Z}^m$, we let $F_\gamma(M/N) = (F_\gamma M)/(F_\gamma N)$. Then the family $\overline{\Psi} = \{F_\gamma(M/N) \mid \gamma \in \mathbb{Z}^m\}$ is a $(\mathbb{Z}^m, \sigma)$-filtration on M/N.
d) The canonical maps $F_\gamma M / F_{<_\sigma \gamma} M \longrightarrow F_\gamma(M/N)/F_{<_\sigma \gamma}(M/N)$ yield a homogeneous surjective $\mathrm{gr}_\Phi(R)$-linear map $\beta : \mathrm{gr}_\Psi(M) \longrightarrow \mathrm{gr}_{\overline{\Psi}}(M/N)$.
e) The sequence

$$0 \longrightarrow \mathrm{gr}_{\widetilde{\Psi}}(N) \xrightarrow{\alpha} \mathrm{gr}_\Psi(M) \xrightarrow{\beta} \mathrm{gr}_{\overline{\Psi}}(M/N) \longrightarrow 0$$

is an exact sequence of $\mathbb{Z}^m$-graded $\mathrm{gr}_\Phi(R)$-modules.

Proof. Since a) amounts only to a simple check of definitions, we start by proving claim b). The only non-trivial claim is that the map α is injective. Given an element $v \in F_\gamma N$ which satisfies $\alpha(v + F_{<_\sigma \gamma} N) = 0$, we have

$v \in (F_{<_\sigma \gamma} M) \cap (F_\gamma N) = (F_{<_\sigma \gamma} M) \cap N$, and this vector space equals $F_{<_\sigma \gamma} N$ because we have

$$(F_{<_\sigma \gamma} M) \cap N = \Big(\bigcup_{\gamma' <_\sigma \gamma} F_{\gamma'} M \Big) \cap N = \bigcup_{\gamma' <_\sigma \gamma} F_{\gamma'} N = F_{<_\sigma \gamma} N$$

Claims c) and d) follow immediately from the definitions. Hence it remains to prove the exactness of the sequence in e). The only non-trivial part is that the elements of $\mathrm{Ker}(\beta)$ are contained in the image of α. Let $v \in F_\gamma M$ be an element for which we have $\bar{v} = v + F_{<_\sigma \gamma} M \in \mathrm{Ker}(\beta)$. Thus the residue class of v in $F_\gamma M / F_\gamma N$ is contained in some vector space $F_\delta M / F_\delta N$ with $\delta <_\sigma \gamma$. Using the isomorphism of K-vector spaces $F_\delta M / F_\delta N \cong (F_\delta M + N)/N$, we see that $v \in (F_\delta M) + N$. We choose $w \in F_\delta M$ and $u \in N$ such that $v = w + u$. Now the claim follows from $u = v - w \in N \cap F_\gamma M = F_\gamma N$ and $\alpha(\bar{u}) = \bar{v} - \bar{w} = \bar{v}$. □

Since the passage from a filtered ring to its associated graded ring is a useful technique in commutative algebra, we introduce the following benign properties of filtrations which will aid us in mastering this technique.

Definition 6.5.10. Let M be a filtered R-module as above.

a) The filtration Ψ is called **orderly** if for every element $v \in M \setminus \{0\}$ there exists an element $\gamma \in \mathbb{Z}^m$ such that v is contained in $F_\gamma M$ but not in $F_{<_\sigma \gamma} M$. In this case γ is called the **order** of v with respect to Ψ and is denoted by $\mathrm{ord}_\Psi(v)$.
b) The filtration Ψ is called **separated** if we have $\bigcap_{\gamma \in \mathbb{Z}^m} F_\gamma M = \{0\}$.
c) Let Ψ be orderly, and let $v \in M \setminus \{0\}$ be an element of order γ. Then the residue class of v in $\mathrm{gr}_\Psi(M)_\gamma = F_\gamma M / F_{<_\sigma \gamma} M$ is called the **leading form** of v with respect to Ψ and is denoted by $\mathrm{LF}_\Psi(v)$. For $v = 0$, we set $\mathrm{LF}_\Psi(v) = 0$.

If Ψ is orderly, every non-zero element of M has a unique order with respect to Ψ and a well-defined leading form. Furthermore, an orderly filtration is separated because every non-zero element of M is contained in exactly one set $F_\gamma M \setminus F_{<_\sigma \gamma} M$. There do exist filtrations which are not separated (and therefore not orderly). For instance, the $(\mathbb{Z}, <)$-filtration Φ on $\mathbb{Q}[x]$ defined by $F_\gamma \mathbb{Q}[x] = \mathbb{Q}[x]$ for $\gamma \geq 0$ and $F_\gamma \mathbb{Q}[x] = (x)$ for $\gamma < 0$ is obviously not separated. Moreover, there are separated filtrations which are not orderly (see Exercise 1). Finally, we note that the leading form $\mathrm{LF}_\Psi(v)$ of a non-zero element $v \in M$ is a homogeneous element of $\mathrm{gr}_\Psi(M)$ of degree $\mathrm{ord}_\Psi(v)$.

Let us examine $\deg_W$-filtrations and Gröbner filtrations with respect to these properties.

Example 6.5.11. Let $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let the polynomial ring P be equipped with its $\deg_W$-filtration Φ, and let a graded P-module M be equipped with its $\deg_W$-filtration Ψ. Then the filtrations Φ and Ψ are orderly. For every $v \in M \setminus \{0\}$, we have $\mathrm{ord}_\Psi(v) = \deg_W(v)$. Furthermore, if

we let $\gamma = \mathrm{ord}_\Psi(v)$, the isomorphism $F_\gamma M / F_{<_{\mathrm{Lex}}\gamma} M \cong M_\gamma$ identifies $\mathrm{LF}_\Psi(v)$ with $\mathrm{DF}_W(v)$.

Example 6.5.12. Let σ be a term ordering on $\mathbb{T}^n$. Then the σ-Gröbner filtration Φ on P is orderly. For a non-zero polynomial $f \in P$, we have $\mathrm{ord}_\Phi(f) = \log(\mathrm{LT}_\sigma(f))$. Furthermore, if we let $\gamma = (\gamma_1, \ldots, \gamma_n) = \mathrm{ord}_\Phi(f)$ and $t = x_1^{\gamma_1} \cdots x_n^{\gamma_n}$, the isomorphism $F_\gamma P / F_{<_\sigma \gamma} P \cong K \cdot t$ identifies $\mathrm{LF}_\Phi(f)$ with $\mathrm{LM}_\sigma(f)$.

Having introduced the leading form of an element with respect to a filtration, we now proceed to define leading form modules.

Definition 6.5.13. Let N be an R-submodule of M, and let both Φ and Ψ be orderly.

a) The graded $\mathrm{gr}_\Phi(R)$-submodule $\mathrm{LF}_\Psi(N) = \langle \mathrm{LF}_\Psi(v) \mid v \in N \rangle$ of $\mathrm{gr}_\Psi(M)$ is called the **leading form module** of N with respect to the filtration Ψ.
b) A set of elements $\{v_1, \ldots, v_s\} \subseteq N$ is called a **Ψ-standard basis** of N if we have $\mathrm{LF}_\Psi(N) = \langle \mathrm{LF}_\Psi(v_1), \ldots, \mathrm{LF}_\Psi(v_s) \rangle$. If it is clear which filtration we are considering, we simply say that $\{v_1, \ldots, v_s\}$ is a **standard basis** of N.

Remark 6.5.14. Several special cases of standard bases have been studied before.

a) Let $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, let the polynomial ring P be equipped with the $\deg_W$-filtration Φ, and let $I \subseteq P$ be an ideal. Then we have $\mathrm{LF}_\Phi(I) = \mathrm{DF}_W(I)$, and a Φ-standard basis of I is simply a Macaulay basis of I with respect to the grading given by W.
b) Let σ be a term ordering on $\mathbb{T}^n$, let P be equipped with the σ-Gröbner filtration Φ, and let $I \subseteq P$ be an ideal. Then we have $\mathrm{LF}_\Phi(I) = \mathrm{LT}_\sigma(I)$, and a Φ-standard basis of I is nothing but a σ-Gröbner basis of I.

In contrast to Macaulay bases and Gröbner bases, a standard basis of an ideal need not generate it, as our next example shows.

Example 6.5.15. Let $P = K[x, y]$ be graded by $W = (-1\ -1)$, let Φ be the $\deg_W$-filtration on P, and let $I = (x - x^2, xy)$. Since we have $I \subseteq (x)$ and $\mathrm{LF}_\Phi(x - x^2) = x$, we see that $\mathrm{LF}_\Phi(I) = (x)$. Hence $\{x - x^2\}$ is a Φ-standard basis of I, but clearly not a set of generators.

Using leading form modules, we reformulate part e) of Proposition 6.5.9 as follows.

Corollary 6.5.16. *Let N be a submodule of M, and assume that both filtrations Φ and Ψ are orderly. Then there exists a homogeneous isomorphism of $\mathrm{gr}_\Phi(R)$-modules $\bar{\beta} : \mathrm{gr}_\Psi(M)/\mathrm{LF}_\Psi(N) \cong \mathrm{gr}_{\overline{\Psi}}(M/N)$.*

Proof. It suffices to note that the image of the map α in the proposition is exactly $\mathrm{LF}_\Psi(N)$. □

For σ-Gröbner filtrations and $\deg_W$-filtrations, we have seen in Sections 2.5 and 4.2 how we can compute standard bases. In the next subsection we meet a new kind of filtration which leads to interesting new standard bases.

6.5.B Adic Filtrations and Tangent Cones

In the following we let R be a finitely generated K-algebra and $I \subseteq R$ an ideal.

Definition 6.5.17. Let σ be the monoid ordering $<$ on $\mathbb{Z}$. For every $\gamma \in \mathbb{Z}$, let $F_\gamma R = I^{-\gamma}$ where we use the convention that $I^\delta = R$ for $\delta \leq 0$. Then the family $\Phi = \{F_\gamma R \mid \gamma \in \mathbb{Z}\}$ is clearly a $(\mathbb{Z}, \sigma)$-filtration on R. It is called the **adic filtration** with respect to I or the **I-adic filtration** on R.

In the case of an I-adic filtration Φ, we shall write LF_I instead of LF_Φ and $\mathrm{gr}_I(R)$ instead of $\mathrm{gr}_\Phi(R)$. For adic filtrations, the associated graded ring satisfies $\mathrm{gr}_I(R)_{-\gamma} \cong I^\gamma / I^{\gamma+1}$ for every $\gamma \geq 0$ and $\mathrm{gr}_I(R)_{-\gamma} = 0$ for $\gamma < 0$. The following example introduces a useful adic filtration. For a generalization, see Proposition 6.5.24.

Example 6.5.18. Let $P = K[x_1, \ldots, x_n]$ be graded by $W = (-1 \cdots -1)$, let $\mathfrak{m} = (x_1, \ldots, x_n)$, and let $I \subseteq \mathfrak{m}$ be an ideal of P.

a) For $\gamma > 0$, we have $P_\gamma = \mathrm{gr}_\mathfrak{m}(P)_\gamma = 0$. For $\gamma \leq 0$, the elements of P_γ are the homogeneous polynomials of standard degree $-\gamma$. Hence we have $P_\gamma \subseteq \mathfrak{m}^{-\gamma}$. The map φ_γ which is the composition of this inclusion with the canonical map $\mathfrak{m}^{-\gamma} \twoheadrightarrow \mathfrak{m}^{-\gamma}/\mathfrak{m}^{-\gamma-1}$ is bijective since we have $\mathfrak{m}^{-\gamma} = \bigoplus_{i=\gamma}^{\infty} P_i$ for all $\gamma \leq 0$. From this it follows easily that the map $\varphi = \bigoplus_{\gamma \in \mathbb{Z}} \varphi_\gamma : P \longrightarrow \mathrm{gr}_\mathfrak{m}(P)$ is an isomorphism of $\mathbb{Z}$-graded K-algebras.

b) The $\mathfrak{m}$-adic filtration Φ on P is orderly and we have $\mathrm{ord}_\Phi(f) = \deg_W(f)$ for every $f \in P \setminus \{0\}$. If we identify the leading form of a non-zero polynomial f with its preimage under the isomorphism φ, it corresponds to the homogeneous component of f of *lowest degree* with respect to the standard grading.

c) If we identify $\mathrm{LF}_\mathfrak{m}(I)$ with its preimage under the isomorphism φ, we get an isomorphism of $\mathbb{Z}$-graded K-algebras $\mathrm{gr}_{\mathfrak{m}/I}(P/I) \cong P/\mathrm{LF}_\mathfrak{m}(I)$ (see Corollary 6.5.16).

Next we study the question of whether adic filtrations are orderly. The following remark points out that, for these special filtrations, it is sufficient to ask whether they are separated.

Remark 6.5.19. Assume that the I-adic filtration Φ on R is separated. For every element $a \in R \setminus \{0\}$ there exists a number $i \geq 0$ such that $a \in I^i \setminus I^{i+1}$. Hence the filtration Φ is orderly. Consequently, the properties of being orderly and of being separated are equivalent for I-adic filtrations.

The following theorem is the basic tool for answering our question. In its proof we use the Rees ring $\mathcal{R}(I)$ of I which was also the topic of Tutorial 81. This ring is the $\mathbb{Z}$-graded R-algebra $\mathcal{R}(I) = \bigoplus_{d\in\mathbb{Z}} \mathcal{R}(I)_d$ with $\mathcal{R}(I)_d = I^d$ for all $d \in \mathbb{Z}$.

Theorem 6.5.20. (The Artin-Rees Lemma)
Let R be a finitely generated K-algebra, and let I and J be ideals in R. Then there exists a number $c \in \mathbb{N}$ such that we have $I^d \cap J = I^{d-c}(I^c \cap J)$ for every $d \geq c$.

Proof. By Hilbert's Basis Theorem 2.4.6, the ring R is Noetherian. Hence there exists a finite system of generators $\{a_1, \ldots, a_m\}$ of I. We define an R-algebra homomorphism $\varepsilon : R[x_1, \ldots, x_m] \longrightarrow \mathcal{R}(I)$ by $\varepsilon(x_i) = a_i \in \mathcal{R}(I)_1$ for $i = 1, \ldots, m$. The map ε is clearly surjective. In particular, it follows from Hilbert's Basis Theorem 2.4.6 that $\mathcal{R}(I)$ is a Noetherian ring, too.

If we equip $R[x_1, \ldots, x_m]$ with the standard grading, the map ε is also homogeneous. Now we observe that $\bigoplus_{d\in\mathbb{N}}(I^d \cap J)$ is a homogeneous ideal of $\mathcal{R}(I)$. Let $f_1, \ldots, f_s \in R[x_1, \ldots, x_m]$ be homogeneous polynomials which generate the ideal $\widetilde{J} = \varepsilon^{-1}(\bigoplus_{d\in\mathbb{N}}(I^d \cap J))$. Let c be the maximum of the degrees of $f_1, \ldots, f_s$. Since we have $\widetilde{J}_c = \sum_{i=1}^{s} R[x_1, \ldots, x_m]_{c-\deg(f_i)}\, f_i$, it follows that the ideal $\bigoplus_{d\geq c} \widetilde{J}_d$ has a system of generators $\{g_1, \ldots, g_t\}$ consisting of homogeneous polynomials of degree c. Let $q \in I^d \cap J$ with $d \geq c$. Then there exists a homogeneous polynomial $p \in R[x_1, \ldots, x_m]_d$ whose image is $\varepsilon(p) = q$. Using Corollary 1.7.11, we find a representation $p = \sum_{i=1}^{t} h_i g_i$ with homogeneous polynomials $h_i \in R[x_1, \ldots, x_m]$ of degree $\deg(h_i) = d - c \geq 0$. Consequently, we obtain $q = \sum_{i=1}^{t} \varepsilon(h_i)\varepsilon(g_i) \in I^{d-c}(I^c \cap J)$. Since the other inclusion is obvious, the proof is complete. □

The Artin-Rees Lemma implies the following important property of the intersection ideal $\bigcap_{\gamma\in\mathbb{N}} I^\gamma$.

Theorem 6.5.21. (Krull's Intersection Theorem)
Let R be a finitely generated K-algebra, let I be an ideal in R, and let $J = \bigcap_{\gamma\in\mathbb{N}} I^\gamma$.

a) We have $J = I\,J$.
b) There exists an element $a \in I$ such that $(1 - a)J = 0$.
c) The ideal J consists of all elements $b \in R$ satisfying $(1 - a)b = 0$ for some element $a \in I$.
d) If R is an integral domain and $I \subset R$, the I-adic filtration on R is orderly.

Proof. First we prove a). The inclusion $I\,J \subseteq J$ is obviously true. We use the Artin-Rees Lemma to find a number $c \in \mathbb{N}$ such that $J = I^d \cap J = I^{d-c}(I^c \cap J)$ for every $d \in \mathbb{N}$. In particular, for $d = c + 1$ we get $J \subseteq I\,J$.

Next we prove b). Let $\{b_1, \ldots, b_s\}$ be a system of generators of J. By a), there exist elements $a_{ij} \in I$ such that $b_i = \sum_{j=1}^{s} a_{ij} b_j$ for $i = 1, \ldots, s$. Thus

the matrix $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_s(R)$ satisfies $(\mathcal{I}_s - \mathcal{A}) \cdot (b_1, \ldots, b_s)^{\mathrm{tr}} = 0$. By multiplying this equation on the left by the adjoint matrix of $(\mathcal{I}_s - \mathcal{A})$, we get $\det(\mathcal{I}_s - \mathcal{A})\, b_i = 0$ for $i = 1, \ldots, s$. When we expand this determinant, we see that it is of the form $1 - a$ with $a \in I$. Hence we have $(1-a)b_i = 0$ for $i = 1, \ldots, s$, and the claim is proved.

Since b) implies one inclusion in c), we now prove the other inclusion. Let $b \in R$ be such that $(1-a)b = 0$ for some $a \in I$. Then $b = ab = a^2b = \cdots$ implies $b \in \bigcap_{i \geq 1} I^i = J$, as we wanted to show. Finally, we note that claim d) follows immediately from c). □

Krull's Intersection Theorem can be used in two ways: we can construct adic filtrations which are not orderly, and we can prove that certain adic filtrations are orderly. Let us demonstrate this by a couple of examples.

Example 6.5.22. Let $R = K[x, y]/(x - xy)$, and let $I \subseteq R$ be the principal ideal generated by the residue class $\bar{y}$ of y. Then we have $(1 - \bar{y})\, \bar{x} = 0$, and Krull's Intersection Theorem yields $\bar{x} \in \bigcap_{\gamma \geq 0} I^\gamma$. Since we have $\bar{x} \neq 0$, the I-adic filtration on R is not separated, and therefore not orderly.

Example 6.5.23. Let Γ be a monoid on which there exists a term ordering τ, let R be a finitely generated, Γ-graded K-algebra, and let $I \subset R$ be a homogeneous ideal. Then we have $I \subseteq R_+ = \bigoplus_{\gamma >_\tau 0} R_\gamma$ and the ideal $J = \bigcap_{i \geq 0} I^i$ satisfies $J = I\, J \subseteq (R_+)\, J$ by Krull's Intersection Theorem. Now the Graded Version of Nakayama's Lemma 1.7.15 yields $J = 0$. Hence the I-adic filtration on R is separated, and therefore orderly.

In the remainder of this section let K be a field, let $P = K[x_1, \ldots, x_n]$, let $y_1, \ldots, y_m$ be further indeterminates, let $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$, and let $\mathfrak{n}$ be the ideal generated by $\{x_1, \ldots, x_n\}$ in Q. We generalize and extend Example 6.5.18 as follows.

Proposition 6.5.24. *Let Q be graded by $W = (-1 \ \ -1 \cdots -1 \ \ 0 \cdots 0)$ where $W \in \mathrm{Mat}_{1,n+m}(\mathbb{Z})$ contains n entries -1 and m entries zero.*

a) The $\mathfrak{n}$-adic filtration on Q is identical to the $\deg_W$-filtration.
b) For each $\gamma \in \mathbb{Z}$, let $\varphi_\gamma : Q_\gamma \longrightarrow (\mathrm{gr}_\mathfrak{n}(Q))_\gamma = \mathfrak{n}^{-\gamma}/\mathfrak{n}^{-\gamma-1}$ be the composition of the inclusion $Q_\gamma \subset \mathfrak{n}^{-\gamma}$ with the canonical surjective map $\mathfrak{n}^{-\gamma} \twoheadrightarrow \mathfrak{n}^{-\gamma}/\mathfrak{n}^{-\gamma-1}$. Then the map $\varphi = \bigoplus_{\gamma \in \mathbb{Z}} \varphi_\gamma : Q \longrightarrow \mathrm{gr}_\mathfrak{n}(Q)$ is an isomorphism of $\mathbb{Z}$-graded K-algebras.
c) The $\mathfrak{n}$-adic filtration on Q is orderly.
d) For every $f \in Q \setminus \{0\}$, we have $\varphi(\mathrm{DF}_W(f)) = \mathrm{LF}_\mathfrak{n}(f)$.
e) For every ideal $J \subseteq Q$, we have $\varphi(\mathrm{DF}_W(J)) = \mathrm{LF}_\mathfrak{n}(J)$.

Proof. To prove a), we note that $\mathfrak{n}^\gamma$ is a monomial ideal for every $\gamma \geq 1$. Therefore we have $f \in \mathfrak{n}^\gamma$ if and only if all terms $t \in \mathrm{Supp}(f)$ satisfy $t \in \mathfrak{n}^\gamma$, and this is equivalent to $\deg_W(t) \leq -\gamma$ for all $t \in \mathrm{Supp}(f)$. Hence we see that both filtrations satisfy $F_\gamma Q = \{f \in Q \setminus \{0\} \mid \deg_W(f) \leq -\gamma\} \cup \{0\}$

for every $\gamma \in \mathbb{Z}$. The other claims follow from a) and the corresponding results for $\deg_W$-filtrations in the first subsection (see Proposition 6.5.8 and Example 6.5.11). □

Given an ideal $J \subseteq Q$, we would like to compute a standard basis of J with respect to the $\mathfrak{n}$-adic filtration. Using the isomorphism φ of part b) of the proposition, we identify Q and $\mathrm{gr}_{\mathfrak{n}}(Q)$. This means that we are looking for a Macaulay basis with respect to the grading given by the matrix $W = (-1\ -1 \cdots -1\ 0 \cdots 0)$. Unfortunately, we cannot use the method of Corollary 4.2.16 because it requires the grading to be non-negative. Our next theorem does the trick.

Theorem 6.5.25. (Lazard's Method)
Let $J \subseteq Q$ be an ideal, and let $\{f_1, \ldots, f_s\} \subseteq Q \setminus \{0\}$ be a system of generators of J. Choose a homogenizing indeterminate x_0 and equip the polynomial ring $\overline{Q} = K[x_0, \ldots, x_n, y_1, \ldots, y_m]$ with the grading defined by $\deg(x_i) = 1$ for $i = 0, \ldots, n$ and $\deg(y_j) = 0$ for $j = 1, \ldots, m$. Furthermore, let σ be an elimination ordering for x_0 on the monoid of terms of $\overline{Q}$, and let $\{G_1, \ldots, G_t\}$ be a homogeneous σ-Gröbner basis of the ideal $(f_1^{\mathrm{hom}}, \ldots, f_s^{\mathrm{hom}})$ in $\overline{Q}$. Then we have $\mathrm{LF}_{\mathfrak{n}}(J) = (\mathrm{LF}_{\mathfrak{n}}(G_1^{\mathrm{deh}}), \ldots, \mathrm{LF}_{\mathfrak{n}}(G_t^{\mathrm{deh}}))$.

Proof. Let $\overline{J} = (f_1^{\mathrm{hom}}, \ldots, f_s^{\mathrm{hom}}) \subseteq \overline{Q}$. The inclusion "$\supseteq$" is a consequence of the observation that $G_i^{\mathrm{deh}} \in \overline{J}^{\mathrm{deh}} = ((f_1^{\mathrm{hom}})^{\mathrm{deh}}, \ldots, (f_s^{\mathrm{hom}})^{\mathrm{deh}}) = J$ for $i = 1, \ldots, t$. To prove the inclusion "$\subseteq$", let $f \in J \setminus \{0\}$. By Corollary 4.3.8, there exists a number $\ell \geq 0$ such that $x_0^\ell f^{\mathrm{hom}} \in \overline{J}$. Therefore $\mathrm{LT}_\sigma(x_0^\ell f^{\mathrm{hom}})$ is a multiple of $\mathrm{LT}_\sigma(G_i)$ for some index $i \in \{1, \ldots, t\}$.

Now let $f = f_1 + \cdots + f_r$ be the decomposition of f into homogeneous components with respect to the grading given by $\deg(x_i) = 1$ for $i = 1, \ldots, n$ and $\deg(y_j) = 0$ for $j = 1, \ldots, m$. Here f_k is homogeneous of degree $d_k \geq 0$ and we may assume that $d_1 < \cdots < d_r$. It follows that we have $f^{\mathrm{hom}} = x_0^{d_r - d_1} f_1 + \cdots + x_0^{d_r - d_{r-1}} f_{r-1} + f_r$ and $\mathrm{LT}_\sigma(f^{\mathrm{hom}}) = x_0^{d_r - d_1}\ \mathrm{LT}_\sigma(f_1)$ because σ is an elimination ordering for x_0. Moreover, the fact that the $\mathfrak{n}$-adic filtration is the $\deg_W$-filtration on Q implies $\mathrm{LF}_{\mathfrak{n}}(f) = f_1$.

In a similar way, using Proposition 4.3.2.h we know that $G_i = x_0^\alpha (G_i^{\mathrm{deh}})^{\mathrm{hom}}$ for some $\alpha \geq 0$, and so conclude that $\mathrm{LT}_\sigma(G_i) = x_0^\beta\ \mathrm{LT}_\sigma(\mathrm{LF}_{\mathfrak{n}}(G_i^{\mathrm{deh}}))$ for some $\beta \geq 0$. Altogether, it follows that the term $x_0^{\ell + d_r - d_1}\ \mathrm{LT}_\sigma(\mathrm{LF}_{\mathfrak{n}}(f))$ is a multiple of $x_0^\beta\, \mathrm{LT}_\sigma(\mathrm{LF}_{\mathfrak{n}}(G_i^{\mathrm{deh}}))$. Let us denote the restriction of σ to the terms of Q by σ'. Then we know that $\mathrm{LT}_{\sigma'}(\mathrm{LF}_{\mathfrak{n}}(f))$ is a multiple of $\mathrm{LT}_{\sigma'}(\mathrm{LF}_{\mathfrak{n}}(G_i^{\mathrm{deh}}))$ for some $i \in \{1, \ldots, t\}$. Since $f \in J \setminus \{0\}$ was arbitrary, this shows that $\{\mathrm{LF}_{\mathfrak{n}}(G_1^{\mathrm{deh}}), \ldots, \mathrm{LF}_{\mathfrak{n}}(G_t^{\mathrm{deh}})\}$ is a σ'-Gröbner basis of $\mathrm{LF}_{\mathfrak{n}}(J)$. In particular, it is a system of generators. □

The case $m = 0$ deserves a special mention. In this case we have $\mathfrak{n} = \mathfrak{m} = (x_1, \ldots, x_n)$. Given an ideal $J \subseteq P$, the zero set of $\mathrm{LF}_{\mathfrak{m}}(J)$ is also called the **tangent cone** of J at the origin. So, using this geometric terminology, the problem is how to effectively compute polynomials which

define the tangent cone of J at the origin. The theorem immediately yields the following algorithm.

Corollary 6.5.26. (The Tangent Cone Algorithm)
Let $P = K[x_1, \ldots, x_n]$ be standard graded, let $\mathfrak{m} = (x_1, \ldots, x_n)$, and let $J \subseteq \mathfrak{m}$ be an ideal which is generated by a set of non-zero polynomials $\{f_1, \ldots, f_s\}$. Consider the following sequence of instructions.

1) *Let $\overline{P} = K[x_0, \ldots, x_n]$ be standard graded, and let $\overline{J}$ be the ideal $(f_1^{\text{hom}}, \ldots, f_s^{\text{hom}})$ in $\overline{P}$.*
2) *Let σ be an elimination ordering for x_0 on $\mathbb{T}(x_0, \ldots, x_n)$. Compute a homogeneous σ-Gröbner basis $\{G_1, \ldots, G_t\}$ of $\overline{J}$.*
3) *Return the ideal $(\mathrm{LF}_{\mathfrak{m}}(G_1^{\text{deh}}), \ldots, \mathrm{LF}_{\mathfrak{m}}(G_t^{\text{deh}}))$.*

This is an algorithm which computes the ideal $\mathrm{LF}_{\mathfrak{m}}(J)$ defining the tangent cone of J at the origin.

Notice that Corollary 6.5.16 also provides us with a description of the associated graded ring of P/J in this setting. Specifically, we have

$$\mathrm{gr}_{\mathfrak{m}/J}(P/J) \cong K[x_1, \ldots, x_n]/(\mathrm{LF}_{\mathfrak{m}}(G_1^{\text{deh}}), \ldots, \mathrm{LF}_{\mathfrak{m}}(G_t^{\text{deh}}))$$

Let us compute a tangent cone using this algorithm.

Example 6.5.27. Let the ring $P = \mathbb{Q}[x_1, x_2, x_3, x_4]$ be standard graded, let $\mathfrak{m} = (x_1, x_2, x_3, x_4)$, and let $J = (x_1x_2 - x_3^2,\ x_2^2 - x_4^5)$. We follow the steps of the Tangent Cone Algorithm.

1) Equip the ring $\overline{P} = \mathbb{Q}[x_0, \ldots, x_4]$ with the standard grading, and let $\overline{J} = (x_1x_2 - x_3^2,\ x_0^3x_2^2 - x_4^5)$.
2) Let $\sigma = \mathtt{Ord}(V)$ be the elimination ordering for x_0 defined by the matrix

$$V = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 \end{pmatrix}$$

   We compute the reduced σ-Gröbner basis of J. We obtain the result $\{x_1x_2 - x_3^2,\ x_0^3x_2^2 - x_4^5,\ x_0^3x_2x_3^2 - x_1x_4^5,\ x_0^3x_4^4 - x_1^2x_4^5\}$.
3) Return the ideal $(x_1x_2 - x_3^2,\ x_2^2,\ x_2x_3^2,\ x_3^4)$ and stop.

Altogether, we have computed $\mathrm{LF}_{\mathfrak{m}}(J) = (x_1x_2 - x_3^2,\ x_2^2,\ x_2x_3^2,\ x_3^4)$.

The tangent cone at the origin contains information about the geometric nature of the origin as a point on $\mathcal{Z}(J)$ (see Tutorial 95).

Exercise 1. Let K be a field, let $P = K[x, y]$, and let Φ be the filtration $\Phi = \{F_{(a,b)}P \mid (a, b) \in \mathbb{Z}^2\}$ where

$$F_{(a,b)}P = \begin{cases} \{f \in P \mid \deg_x(f) \leq a\} & \text{if either } a > 0 \text{ or } a = 0 \text{ and } b \geq 0, \\ 0 & \text{if either } a < 0 \text{ or } a = 0 \text{ and } b < 0. \end{cases}$$

a) Show that Φ is a $(\mathbb{Z}^2, \texttt{Lex})$-filtration on P.
b) Show that Φ is separated but not orderly.

Exercise 2. Let K be a field, let R be a finitely generated K-algebra, and let R be equipped with an orderly filtration Φ.

a) Prove that for all $f, g \in R$ we have either $\mathrm{LF}_\Phi(f)\,\mathrm{LF}_\Phi(g) = \mathrm{LF}_\Phi(fg)$ or $\mathrm{LF}_\Phi(f)\,\mathrm{LF}_\Phi(g) = 0$.
b) Show that if $\mathrm{gr}_\Phi(R)$ is an integral domain then also R is an integral domain.
c) Find an example where R is an integral domain, but $\mathrm{gr}_\Phi(R)$ is not.

Exercise 3. Let K be a field, let $P = K[x_1, \ldots x_n]$, let $\mathfrak{m}$ be the ideal $(x_1, \ldots, x_n)$, let $f \in \mathfrak{m}$, and let $I = (f)$. Show that there exists a natural isomorphism $\mathrm{gr}_{\mathfrak{m}/I}(P/I) \cong P/(\mathrm{LF}_\mathfrak{m}(f))$.

Exercise 4. With the same assumptions as in Definition 6.5.17, let M be a P-module. We define a $(\mathbb{Z}, \sigma)$-filtration on M by setting $F_\gamma M = I^{-\gamma}M$ for $\gamma \in \mathbb{Z}$ and call it the **I-adic filtration** on M.

a) Show that $\mathrm{gr}_I(M)$ is a $\mathbb{Z}$-graded $\mathrm{gr}_I(P)$-module in a natural way.
b) Let $J \subseteq P$ be an ideal. Give an example where the I-adic filtration on the P-module J and the filtration induced on J by the I-adic filtration on P are different.
c) Show that if $J = (f)$ and f is a non-zerodivisor for P/I^d for every $d > 0$ then the two filtrations in b) coincide.
d) Let $P = \mathbb{Q}[x_1, \ldots, x_9]$, and let $I \subseteq P$ be the ideal generated by the 2×2-minors of the matrix $\mathcal{M} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix}$. Using CoCoA, show that x_1 is a non-zerodivisor for P/I and that $x_1 \det(\mathcal{M}) \in I^2$. Deduce that in part c) it is not sufficient to assume that f is a non-zerodivisor for P/I.

Exercise 5. Let $R = K[[x_1, \ldots, x_n]]$ be the power series ring in n indeterminates over a field K, and let $\mathfrak{m} = (x_1, \ldots, x_n)$. Prove that $\mathrm{gr}_\mathfrak{m}(R) \cong K[x_1, \ldots, x_n]$.

Exercise 6. Let K be a field, let $P = K[x_1, \ldots, x_4]$ be standard graded, and let $J \subseteq P$ be the ideal generated by $f_1 = x_1^2x_2 + x_1^4x_4 + x_3^6$ and $f_2 = x_1x_2^2$. Compute the ideal defining the tangent cone of J at the origin.

Tutorial 93: Mora's Algorithm

How much can we generalize Gaußian reduction
in order to compute Gröbner bases?
(Teo Mora)

What happens if we want to solve the ideal membership problem in a localization of the polynomial ring? For instance, let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K, let $S \subset P$ be the multiplicatively closed subset $1 + (x_1, \ldots, x_n) = \{1 + f \mid f \in (x_1, \ldots, x_n)\}$, and let $p_1, \ldots, p_s \in P$ be non-zero polynomials which generate an ideal $I_S = p_1 P_S + \cdots + p_s P_S$ in the localization P_S. Notice that this localization is canonically isomorphic to the localization of P at the maximal ideal $(x_1, \ldots, x_n)$. To check whether a given polynomial $q \in P$ satisfies $\frac{q}{1} \in I_S$, we have to find out whether there exist elements $u \in S$ and $a_1, \ldots, a_s \in P$ which satisfy the equation $uq = a_1 p_1 + \cdots + a_s p_s$ with $u \in S$. Since there is no obvious *a priori* bound on the degree of u, it is not clear how we could try to generalize Gaußian reduction (or its generalization, the Buchberger algorithm) to solve this problem. Fortunately, we can call into play an algorithm invented by Teo Mora which converts the world of localized rings to the Gröbner basis theology.

In the following we let K be a field, we let $P = K[x_1, \ldots, x_n]$ be standard graded, we let $S = 1 + (x_1, \ldots, x_n)$, and we let σ be a monoid ordering on $\mathbb{T}^n$. We assume that σ is **degree-anticompatible**, i.e. that it is of the form $\sigma = \mathtt{Ord}(W)$ with a non-singular matrix $W \in \mathrm{Mat}_n(\mathbb{Z})$ whose first row is $(-1 \cdots -1)$. Moreover, we let Φ be the $\deg_W$-filtration on P. Our main goal in this tutorial is to develop an algorithm for computing Φ-standard bases in this setting.

a) Generalize Example 6.5.4 to monoid orderings σ and show that Φ is the σ-Gröbner filtration in this more general sense. Moreover, for a non-zero polynomial $f \in P$, prove that $\mathrm{LF}_\Phi(f) = \mathrm{LM}_\sigma(f)$. Conclude that we have $\mathrm{LF}_\Phi(I) = \mathrm{LT}_\sigma(I)$ for every ideal $I \subseteq P$.

Now let us see how Φ-standard bases can be used to solve the ideal membership problem in P_S. A map which assigns to each polynomial $f \in P$ and each tuple of polynomials $\mathcal{G} = (g_1, \ldots, g_s) \in P^s$ a polynomial $\mathrm{WR}_{\sigma,\mathcal{G}}(f)$ is called a **weak remainder** if it has the following properties.

1) $\mathrm{WR}_{\sigma,\mathcal{G}}(0) = 0$
2) If $\mathrm{WR}_{\sigma,\mathcal{G}}(f) \neq 0$ then $\mathrm{LT}_\sigma(\mathrm{WR}_{\sigma,\mathcal{G}}(f)) \notin (\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s))$.
3) There exist polynomials $u \in S$ and $a_1, \ldots, a_s \in P$ satisfying the equation $uf = a_1 g_1 + \cdots + a_s g_s + \mathrm{WR}_{\sigma,\mathcal{G}}(f)$ and $\mathrm{LT}_\sigma(a_i g_i) \leq_\sigma \mathrm{LT}_\sigma(f)$ for all i with $a_i g_i \neq 0$.

Below we shall show that a weak remainder map exists and that it can be computed effectively. Let $I \subseteq P$ be an ideal, and let $\mathcal{G} = (g_1, \ldots, g_s)$ be a Φ-standard basis of I.

b) Prove that a polynomial $f \in P$ satisfies $\frac{f}{1} \in IP_S$ if and only if $\mathrm{WR}_{\sigma,\mathcal{G}}(f) = 0$. Hence the knowledge of a standard basis enables us to check ideal membership in P_S effectively.

c) Let $P = \mathbb{Q}[x_1, x_2]$, and let $I \subseteq P$ be the ideal generated by $f_1 = x_1^7 x_2^{10}$, $f_2 = x_1^8 - x_1^7 x_2^2$, and $f_3 = x_2^{10} - x_1^2 x_2^9$. Show that $\mathcal{G} = (f_2, f_3)$ is a Φ-standard basis of I, that $f_1 \notin (f_2, f_3)$, and that $\mathrm{WR}_{\sigma,\mathcal{G}}(f_1) = 0$. Hence the statement of b) does not hold in the ring P.

d) Let $J \subseteq P$ be an ideal such that $JP_S \subseteq IP_S$ and $\mathrm{LT}_\sigma(J) = \mathrm{LT}_\sigma(I)$. Prove that this implies $JP_S = IP_S$ and $IP_S = g_1 P_S + \cdots + g_s P_S$. In other words, a Φ-standard basis generates the localized ideal.

e) Using the example in c) show that we may have $(g_1, \ldots, g_s) \subset I$ in d). Thus a Φ-standard basis of an ideal in P is not necessarily a system of generators.

Next we need an algorithm for computing weak remainders. To prove the correctness of the algorithm, it will be convenient to describe a homogeneous version first. For this purpose we introduce further notation and hypotheses. Given a non-zero polynomial $f \in P$, we write its decomposition into homogeneous components in the form $f = f_1 + \cdots + f_r$ where f_i is homogeneous of some degree d_i and $d_1 < \cdots < d_r$. Then the number $\mathrm{ec}(f) = d_r - d_1$ is called the **écart** of f. (This is a French term whose English meaning is something like "range".) Now we let x_0 be a new indeterminate, we equip $\overline{P} = K[x_0, \ldots, x_n]$ with the standard grading, and we let the term ordering $\overline{\sigma}$ on $\mathbb{T}^{n+1}$ be the extension of σ by $(1\ 1\ \cdots\ 1)$ (see Definition 4.3.13). Observe that $\overline{\sigma}$ is an elimination ordering for x_0.

f) Prove that every $f \in P \setminus \{0\}$ satisfies $\mathrm{LT}_{\overline{\sigma}}(f^{\mathrm{hom}}) = x_0^{\mathrm{ec}(f)}\, \mathrm{LT}_\sigma(f)$.

g) Let $F, G_1, \ldots, G_s \in \overline{P}$ be non-zero homogeneous polynomials. Consider the following sequence of instructions.

H1) Let $H = F$ and $L = \{G_1, \ldots, G_s\}$.

H2) Let $L' = \{G \in L \mid \mathrm{LT}_{\overline{\sigma}}(G) \text{ divides } x_0^\alpha\, \mathrm{LT}_{\overline{\sigma}}(H) \text{ for some } \alpha \in \mathbb{N}\}$. For each $G \in L'$, let α_G be the minimal number $\alpha \in \mathbb{N}$ for which $\mathrm{LT}_{\overline{\sigma}}(G)$ divides $x_0^\alpha\, \mathrm{LT}_{\overline{\sigma}}(H)$. If $L' = \emptyset$ return H and stop.

H3) Otherwise, choose $G \in L'$ with minimal α_G. If $\alpha_G > 0$ then append H to L.

H4) Replace H by $(\widetilde{H}^{\mathrm{deh}})^{\mathrm{hom}}$, where $\widetilde{H} = x_0^{\alpha_G} H - \frac{x_0^{\alpha_G}\, \mathrm{LM}_{\overline{\sigma}}(H)}{\mathrm{LM}_{\overline{\sigma}}(G)} G$.

H5) If $H = 0$, return H and stop. Otherwise, continue with step H2).

Prove that this is an algorithm which computes a homogeneous polynomial $H \in \overline{P}$ such that there exist further homogeneous polynomials $U, A_1, \ldots, A_s \in \overline{P}$ having the following properties:

g1) $U F = A_1 G_1 + \cdots + A_s G_s + H$.

g2) $\mathrm{LT}_{\overline{\sigma}}(U) = x_0^\alpha$ for some $\alpha \in \mathbb{N}$

g3) The polynomials $UF, A_1 G_1, \ldots, A_s G_s, H$ are all homogeneous of the same degree.

g4) No leading term $\mathrm{LT}_{\overline{\sigma}}(G_i)$ divides $x_0^\beta\, \mathrm{LT}_{\overline{\sigma}}(H)$ for any $\beta \in \mathbb{N}$.

Hint: For finiteness, argue as in the proof of the usual Division Algorithm 1.6.4. To prove correctness, proceed by induction on the iterations of the algorithm. Start with $U = 1$ and $A_i = 0$. For the element G chosen in step 2), distinguish the cases $G \in \{G_1, \ldots, G_s\}$ and $G = H_i$, the value of H after the i^{th} iteration. In both cases update U and the A_i so that equation g1) remains true.

h) **(The Weak Remainder Algorithm)**
Let $f \in P$ and $\mathcal{G} = (g_1, \ldots, g_s) \in P^s$. Consider the following sequence of instructions.

W1) Let $h = f$ and $L = \{g_1, \ldots, g_s\}$.
W2) Let $L' = \{g \in L \mid \mathrm{LM}_\sigma(g) \text{ divides } \mathrm{LM}_\sigma(h)\}$. If $L' = \emptyset$, return h and stop.
W3) Otherwise, choose $g \in L'$ with minimal $\mathrm{ec}(g)$. If $\mathrm{ec}(g) > \mathrm{ec}(h)$ then append h to L.
W4) Replace h by $h - \frac{\mathrm{LM}_\sigma(h)}{\mathrm{LM}_\sigma(g)}\, g$.
W5) If $h = 0$, return h and stop. Otherwise, continue with step W2).

Prove that this sequence defines an algorithm which computes a weak remainder $h = \mathrm{WR}_{\sigma,\mathcal{G}}(f)$. (*Hint:* Dehomogenize the algorithm in g).)

i) Apply the Weak Remainder Algorithm to the following examples where $P = \mathbb{Q}[x_1, x_2, x_3]$ is equipped with the term ordering $\sigma = \texttt{Ord}\begin{pmatrix} -1 & -1 & -1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$.

1) $f = x_1^2 + x_2^3 + x_3^3 + x_1^4 + x_2^5$, $\mathcal{G} = (x_1, x_2)$
2) $f = x_1^2 + x_2^2 + x_3^3$, $\mathcal{G} = (x_1 - x_1x_2, x_2^2 + x_1^3, x_3^3 - x_1^4)$
3) $f = x_1 + x_1^2 + x_1^3 + x_1^4$, $\mathcal{G} = (x_1 + x_1^2 + x_1^3)$

j) Write a CoCoA function `WeakRem(...)` which takes a polynomial $f \in P$ and a tuple $\mathcal{G} = (g_1, \ldots, g_s) \in P^s$ and computes the weak remainder $\mathrm{WR}_{\sigma,\mathcal{G}}(f)$ with respect to the term ordering σ given by the negative of the matrix defining the current term ordering. Apply your function to the examples in i) and compare its results to your hand calculations.

The last part of this tutorial contains the actual algorithm for computing Φ-standard bases. Some of the proofs here are more demanding than usual — you will be asked to rework part of the material in Volume 1. Of course, you may also choose to believe the results and try your hand at their implementation instead. For polynomials $f_1, f_2 \in P$, let $\mathrm{S}(f_1, f_2)$ denote the S-polynomial of f_1 and f_2.

k) Prove the analog of Buchberger's Criterion 2.5.3 in the present setting. Let $I \subseteq P$ be an ideal, and let $\mathcal{G} = (g_1, \ldots, g_s)$ be a tuple of polynomials in I whose images in P_S generate the ideal IP_S. Prove that the following conditions are equivalent.

1) $\mathcal{G}$ is a Φ-standard basis of I.
2) For all $i, j \in \{1, \ldots, s\}$, an application of the algorithm in g) to $\mathrm{S}(g_i^{\mathrm{hom}}, g_j^{\mathrm{hom}})$ and $(g_1^{\mathrm{hom}}, \ldots, g_s^{\mathrm{hom}})$ yields $H = 0$.
3) For all $i, j \in \{1, \ldots, s\}$, we have $\mathrm{WR}_{\sigma,\mathcal{G}}(\mathrm{S}(g_i, g_j)) = 0$.

Hint: To prove that 2) implies 1), start from g1) with $F = \mathrm{S}(G_i, G_j)$ and construct a lifting s_{ij} of σ_{ij} as in the proof of Proposition 2.5.2. Then consider equation g1) for $F = f^{\mathrm{hom}}$ with $f \in I \setminus \{0\}$ and show that $\mathrm{LT}_{\overline{\sigma}}(A_i G_i) \neq \mathrm{LT}_{\overline{\sigma}}(A_j G_j)$ whenever $i \neq j$.

l) **(Mora's Algorithm)**
Let $I \subseteq P$ be an ideal, and let $\{f_1, \ldots, f_s\} \subseteq I$ be a set of polynomials whose images in P_S generate the ideal IP_S. Consider the following sequence of instructions.

M1) Let $s' = s$, let $B = \{(i,j) \mid 1 \leq i < j \leq s\}$, and let $\mathcal{G} = (g_1, \ldots, g_s)$ with $g_i = f_i$ for $i = 1, \ldots, s$.
M2) If $B = \emptyset$, return the result $\mathcal{G}$ and stop. Otherwise, choose a pair $(i,j) \in B$ and delete it from B.
M3) Compute $S_{ij} = \mathrm{S}(g_i, g_j)$ and $S'_{ij} = \mathrm{WR}_{\sigma,\mathcal{G}}(S_{ij})$. If the result is $S'_{ij} = 0$, continue with step M2).
M4) Increase s' by one. Append $g_{s'} = S'_{ij}$ to $\mathcal{G}$ and the set of pairs $\{(i, s') \mid 1 \leq i < s'\}$ to B. Then continue with step M2).

Prove that this is an algorithm which computes a Φ-standard basis $\mathcal{G}$ of I. (*Hint:* Imitate the proof of Buchberger's Algorithm and use the above analog of Buchberger's Criterion.)

m) Apply Mora's Algorithm to compute the Φ-standard bases for the following ideals in $P = \mathbb{Q}[x_1, x_2]$ with respect to the $\deg_W$-filtration Φ defined by $W = \left(\begin{smallmatrix} -1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$.

1) $f_1 = x_1^3 x_2^3,\ f_2 = x_1^4 - x_2^5$
2) $f_1 = x_1 - x_2^4,\ f_2 = x_2^2 - x_1^3$
3) $f_1 = x_1^4 - x_1^3 x_2^2,\ f_2 = x_2^4 - x_1^2 x_2^3$
4) $f_1 = x_1^8 - x_1^7 x_2^2,\ f_2 = x_2^{10} - x_1^2 x_2^9$

n) Write a CoCoA function `SBasis(...)` which takes a list of polynomials and computes a Φ-standard basis of the ideal they generate. Assume that Φ is the $\deg_W$-filtration given by the negative of the matrix defining the current term ordering.

o) Apply your function `SBasis(...)` to compute Φ-standard bases of the examples in m) and of the following examples, where Φ is given by the matrix $W = \left(\begin{smallmatrix} -1 & -1 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right)$.

1) $f_1 = x_1^2 + x_2^2 + x_3^2,\ f_2 = x_1 x_2 + x_2^3 + x_3^3,\ f_3 = x_1^5 + x_1 x_2^6 + x_3^7$
2) $f_1 = x_2 + x_3 - x_1^2 - x_2^2,\ f_2 = x_3 - x_1^2 - x_2^2,\ f_3 = x_1^2 - x_2 x_3$
3) $f_1 = x_1 - x_2^2 x_3,\ f_2 = x_3 - x_2^3,\ f_3 = x_1^2 + x_1^3 - x_2 x_3^3 - x_3^5$

p) Play some games of mor(r)a!

The scientific theory I like best
is that the rings of Saturn are composed
entirely of lost airline luggage.
(Mark Russell)

Tutorial 94: Hilbert Functions of Primary Ideals

Husband: *"I saw you making faces at me all the time, but you notice I not only bid this grand slam but I made it. What can you say about that?"*
Wife: *"If you had played it right you would have lost it."*
(Benjamin Graham)

Is it possible to introduce and compute Hilbert functions and Hilbert series for filtered rings? For instance, can we do it for an affine algebra $R = K[x_1, \ldots, x_n]/I$ with respect to its $(\bar{x}_1, \ldots, \bar{x}_n)$-adic filtration? In this tutorial we bid a grand slam: we propose to solve this problem not only for the ideal $(\bar{x}_1, \ldots, \bar{x}_n)$, but for any ideal $\overline{\mathfrak{q}}$ primary to it. The idea behind the definition is straightforward enough: the vector space dimension of each $R/\overline{\mathfrak{q}}^i$ is finite and can be combined to form a $\overline{\mathfrak{q}}$-adic Hilbert function $\mathrm{HF}_{R,\overline{\mathfrak{q}}}$.

But it is far less obvious how one could possibly compute this function, or rather its associated Hilbert series. The first steps are to notice that to find this function is equivalent to finding the Hilbert function of the associated graded ring, and that the associated graded ring is generated as an algebra by the residue classes of a system of generators of I. The next step is more tricky. We produce a presentation of the associated graded ring as a residue class ring of a larger polynomial ring where the generators of the ideal become residue classes of indeterminates. Then it appears as if we had played it right but lost it: the natural grading on this larger polynomial ring is not of positive type and does not allow the computation of Hilbert series.

At this point we have to play our final trump card. By passing to another associated graded ring with respect to a different filtration, we get a homogeneous presentation with respect to a positive bigrading. The corresponding multigraded Hilbert series can be computed and yields the desired Hilbert series via a change of grading. We've done it! Now stop making faces and get going!

Let K be a field, let $P = K[x_1, \ldots, x_n]$, let $I \subseteq P$ be an ideal, and let $R = P/I$. Moreover, we let $\mathfrak{m} = (x_1, \ldots, x_n) \subseteq P$, we assume that there exists an $\mathfrak{m}$-primary ideal $\mathfrak{q} \subseteq P$ containing I, and we denote the residue class ideals of $\mathfrak{m}$ and $\mathfrak{q}$ in R by $\overline{\mathfrak{m}}$ and $\overline{\mathfrak{q}}$, respectively. In this setting, our goals are to define and compute a Hilbert function which measures the growth of the $\overline{\mathfrak{q}}$-adic filtration of R.

a) For an ideal $\mathfrak{a} \subseteq \mathfrak{m} \subseteq P$, show that $\mathfrak{a}$ is $\mathfrak{m}$-primary if and only if one of the following equivalent conditions holds.
   1) We have $\sqrt{\mathfrak{a}} = \mathfrak{m}$.
   2) There exists a number $i \geq 1$ such that $\mathfrak{m}^i \subseteq \mathfrak{a} \subseteq \mathfrak{m}$.
   3) We have $\dim_K(P/\mathfrak{a}) < \infty$.

b) Using a), write a CoCoA function `IsPrimary(...)` which checks whether a given ideal $\mathfrak{a}$ of P yields an $\overline{\mathfrak{m}}$-primary ideal $\overline{\mathfrak{a}}$ of R.

c) Apply your function `IsPrimary(...)` to show that the ideal $\overline{\mathfrak{a}}$ is an $\overline{\mathfrak{m}}$-primary ideal in the following examples. We use $P = \mathbb{Q}[x, y, z]$.
   1) $I = (0)$ and $\mathfrak{a} = (x, y, z)^2$
   2) $I = (x^2y - z^7)$ and $\mathfrak{a} = (x^2 - y^3,\ y^4, z^5)$
   3) $I = (xy,\ xz,\ yz)$ and $\mathfrak{a} = (x,\ y^2,\ yz,\ z^2)$
   4) $I = (x^2y^3 - x^3yz + xz^3 - y^2z^2,\ xz^2 - y^2z)$ and $\mathfrak{a} = (x^3,\ xz,\ y^2,\ z^3)$

d) Prove that $\dim_K(R/\overline{\mathfrak{q}}^i)$ is finite for every $i \geq 1$.

Based on this result we let the **$\overline{\mathfrak{q}}$-adic Hilbert function** of R be the map

$$\mathrm{HF}_{R,\overline{\mathfrak{q}}} : \mathbb{Z} \longrightarrow \mathbb{N} \quad \text{given by} \quad i \longmapsto \dim_K(R/\overline{\mathfrak{q}}^{\,i+1})$$

where we set $\overline{\mathfrak{q}}^i = R$ for $i \leq 0$. Furthermore, the associated Hilbert series

$$\mathrm{HS}_{R,\overline{\mathfrak{q}}}(z) = \sum_{i \geq 0} \dim_K(R/\overline{\mathfrak{q}}^{\,i+1})\, z^i = \sum_{i \geq 0} \mathrm{HF}_{R,\overline{\mathfrak{q}}}(i)\, z^i$$

is called the **$\overline{\mathfrak{q}}$-adic Hilbert series** of R. Next we want to find an effective way to compute $\overline{\mathfrak{q}}$-adic Hilbert series. Let Φ be the $\overline{\mathfrak{q}}$-adic filtration of R, let $\{f_1, \ldots, f_m\} \subset P$ be a system of generators of $\mathfrak{q}$, and let $\{g_1, \ldots, g_s\} \subset P$ be a system of generators of I. The idea underlying our algorithm is based on the following observations.

e) Show that we have $\mathrm{HS}_{R,\overline{\mathfrak{q}}}(z) = \frac{1}{1-z}\ \mathrm{HS}_{\mathrm{gr}_{\overline{\mathfrak{q}}}(R)}(z^{-1})$.

f) Prove that the residue classes $\{\bar{f}_1, \ldots, \bar{f}_m\}$ form a system of $R/\overline{\mathfrak{q}}$-algebra generators of the associated graded ring $\mathrm{gr}_{\overline{\mathfrak{q}}}(R)$. Here $\bar{f}_i$ denotes the residue class of f_i in $\overline{\mathfrak{q}}/\overline{\mathfrak{q}}^2$.

g) Let $y_1, \ldots, y_m$ be further indeterminates, let $Q = P[y_1, \ldots, y_m]$, and let $J = (y_1 - f_1, \ldots, y_m - f_m)$ be the diagonal ideal in Q. Construct an isomorphism of K-algebras $\varphi : R \longrightarrow Q/J$ having the property that the image of $\overline{\mathfrak{q}}$ is the ideal $\tilde{\mathfrak{q}} \subseteq Q/J$ generated by the set of residue classes $\{y_1 + J, \ldots, y_m + J\}$.

h) Show that the isomorphism φ induces an isomorphism of K-algebras $\overline{\varphi} : \mathrm{gr}_{\overline{\mathfrak{q}}}(R) \longrightarrow \mathrm{gr}_{\tilde{\mathfrak{q}}}(Q/J)$ which maps $\bar{f}_i$ to $\bar{y}_i$, the image of y_i in $\tilde{\mathfrak{q}}/\tilde{\mathfrak{q}}^2$.

i) Now use Corollary 6.5.16 and Proposition 6.5.24 to get an isomorphism of $\mathbb{Z}$-graded K-algebras $\psi : \mathrm{gr}_{\overline{\mathfrak{q}}}(R) \longrightarrow Q/\widetilde{J}$ where Q is graded by $\deg(x_i) = 0$ and $\deg(y_j) = -1$, and where $\widetilde{J}$ is a homogeneous ideal of Q with respect to this grading. Describe explicitly how $\widetilde{J}$ is obtained from the generators of I and $\mathfrak{q}$.

Unfortunately, the above grading on Q is of non-negative type but not of positive type. Therefore the homogeneous components of Q are not finite dimensional and we cannot yet use e) and i) to compute the $\overline{\mathfrak{q}}$-adic Hilbert series of R. However, now the results of Section 5.8.C come to our rescue.

j) Let $\overline{\mathfrak{n}}$ be the residue class ideal of $(x_1, \ldots, x_n)Q$ in $Q/\widetilde{J}$, and let Ψ be the $\overline{\mathfrak{n}}$-adic filtration on $Q/\widetilde{J}$. In the same way as above, construct an isomorphism of $\mathbb{Z}$-graded K-algebras $\imath : \mathrm{gr}_{\overline{\mathfrak{n}}}(Q/\widetilde{J}) \longrightarrow Q/\widehat{J}$ where Q

is graded by $\deg(x_i) = -1$ and $\deg(y_j) = 0$, and where $\widehat{J} \subseteq Q$ is a homogeneous ideal with respect to this grading. Describe explicitly how the elements of $\widehat{J}$ are obtained from the elements of $\widetilde{J}$.

k) Show that $\widehat{J}$ is in fact a homogeneous ideal with respect to the bigrading on Q given by $W = \binom{0 \cdots 0\ 1 \cdots 1}{1 \cdots 1\ 0 \cdots 0}$. Since this grading is positive, we can compute the multigraded Hilbert series $\mathrm{HS}_{Q/\widehat{J},W}(z_1, z_2)$.

l) Prove that we have $\mathrm{HS}_{\mathrm{gr}_{\overline{\mathfrak{q}}}(R)}(z) = \mathrm{HS}_{Q/\widehat{J},W}(z^{-1}, 1)$ and deduce the formula $\mathrm{HS}_{R,\overline{\mathfrak{q}}}(z) = \frac{1}{1-z}\,\mathrm{HS}_{Q/\widehat{J},W}(z, 1)$.

m) By way of some examples, examine what happens to $\mathrm{HS}_{Q/\widehat{J},W}(z, 1)$ when $\mathfrak{q}$ contains I, but is not $\mathfrak{m}$-primary.

n) Implement a CoCoA function `PrimaryHS(...)` which takes I and $\mathfrak{q}$ and computes the $\overline{\mathfrak{q}}$-adic Hilbert series $\mathrm{HS}_{R,\overline{\mathfrak{q}}}(z)$ of R.

o) Apply your function `PrimaryHS(...)` to the examples in c).

Tutorial 95: Singularities

Mathematics is like chequers
in being suitable for the young,
not too difficult, amusing,
and without peril to the state.
(Plato)

This is the third and final tutorial of this section. We have seen that adic filtrations and standard bases open up the world of localized rings to effective computation, and that this world has its own species of Hilbert functions and Hilbert series. What is the geometric meaning of all this? Although the details are beyond the scope of this book, we can imagine the elements of a ring of the form $R = K[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}/I$ as "germs" of functions near the origin o. This means that we identify two functions if they are equal on a neighbourhood of o. Thus the ring R captures some aspects of the geometry of the variety $V = \mathcal{Z}(I)$ near the origin. In particular, we shall see that this ring R contains the information specifying whether o is a regular or a singular point of V, and in the latter case that computations in R allow us to say something about the nature of the singularity.

Singularity theory may or may not be without peril to the state. However, it is surely a difficult topic. If this tutorial should turn out to be arduous and not too amusing for you, we suggest that you skip some of the most onerous proofs and concentrate on the examples and the programs to get a feeling for the chequered and varied world of singularities.

Let K be a field, let $\overline{K}$ be an algebraic closure of K, let $P = K[x_1, \ldots, x_n]$ be standard graded, and let $I \subset P$ be a radical ideal for which we have $I \subseteq (x_1, \ldots, x_n)$. Geometrically speaking, this means that $V = \mathcal{Z}(I) \subseteq \mathbb{A}^n_{\overline{K}}$

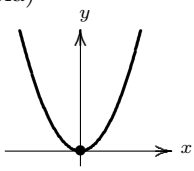
is an affine variety which contains the point $o = (0, \ldots, 0)$ and that I is the vanishing ideal of V in P (see Section 2.6). The affine K-algebra $R = P/I$ is called the **affine coordinate ring** of V. Let $\mathfrak{m} \subset R$ be the maximal ideal generated by the residue classes of $x_1, \ldots, x_n$. (Observe that this notation differs from the one chosen in the section. To simplify the presentation, we decided to use $\mathfrak{m}$ instead of $\overline{\mathfrak{m}}$.) The localization R_S of R at the multiplicative set $S = R \setminus \mathfrak{m}$ is also denoted by $R_{\mathfrak{m}}$ and is called the **local ring** of V at o.

a) Prove that the ring $R_{\mathfrak{m}}$ contains exactly one maximal ideal, namely the ideal $\mathfrak{m}R_{\mathfrak{m}}$.
b) Show that the map $J \mapsto JR_{\mathfrak{m}}$ defines a 1–1 correspondence between the ideals $J \subseteq R$ with $J \cap S = \emptyset$ and the ideals in $R_{\mathfrak{m}}$. Moreover, show that this correspondence induces a bijection between the set of prime ideals $\mathfrak{p} \subset R$ with $\mathfrak{p} \cap S = \emptyset$ and the set of prime ideals of $R_{\mathfrak{m}}$.
c) Prove the inequalities $\operatorname{Kdim}(R_{\mathfrak{m}}) \leq \dim(R) \leq \mu(\mathfrak{m})$. Here $\mu(\mathfrak{m})$ denotes the minimal number of generators of $\mathfrak{m}$. Furthermore, prove that $\operatorname{Kdim}(R_{\mathfrak{m}}) \leq \mu(\mathfrak{m}R_{\mathfrak{m}}) = \dim_K(\mathfrak{m}/\mathfrak{m}^2)$. (*Hint:* Use b) and Proposition 5.4.6.)

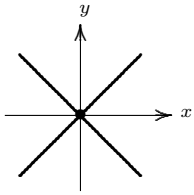
The number $\mu(\mathfrak{m}R_{\mathfrak{m}})$ is called the **embedding dimension** of $R_{\mathfrak{m}}$ and is denoted by $\operatorname{edim}(R_{\mathfrak{m}})$. The ring $R_{\mathfrak{m}}$ is called a **regular local ring** if we have $\operatorname{Kdim}(R_{\mathfrak{m}}) = \operatorname{edim}(R_{\mathfrak{m}})$, otherwise it is called a **singular local ring**. Geometers express these properties as follows. The point o is called a **regular point** of the variety V if $R_{\mathfrak{m}}$ is a regular local ring. Otherwise, the point o is called a **singular point** or a **singularity** of V. To get some insight into the geometric meaning of these notions, we examine a number of examples.

d) Let $P = \mathbb{Q}[x, y]$. For the plane curves given by the following equations, determine whether $o = (0, 0)$ is a singular point. Moreover, compute their tangent cones at the origin.

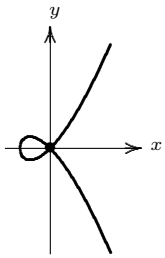
1) $C_1 = \mathcal{Z}(y - x^2)$ (parabola)



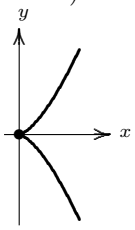
2) $C_2 = \mathcal{Z}(x^2 - y^2)$ (two crossing lines) Here o is called a **node**.



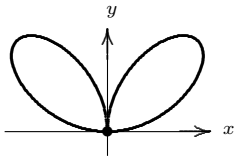
3) $C_3 = \mathcal{Z}(x^2 - y^2 + x^3)$ (elliptic curve having a node at p)



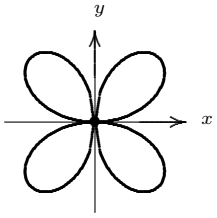
4) $C_4 = \mathcal{Z}(y^2 - x^3)$ (cuspidal cubic) Here p is called a **cusp**.



5) $C_5 = \mathcal{Z}(3xy - x^3 - y^3)$ (folium of Descartes)



6) $C_6 = \mathcal{Z}(4x^2y^2 - (x^2 + y^2)^3)$ (four-leafed rose)



Our next goal is to find an algorithm which enables us to check whether o is a singularity or not. The key result is called the **Jacobian criterion**. Let $\{f_1, \ldots, f_s\}$ be a set of non-zero polynomials which generate I. Then the **Jacobian matrix** of the tuple $\mathcal{F} = (f_1, \ldots, f_s)$ is defined to be the matrix $\mathrm{Jac}(\mathcal{F}) = \left(\frac{\partial f_i}{\partial x_j}\right) \in \mathrm{Mat}_{s,n}(P)$. Since the Jacobian matrix uses partial derivatives, it is convenient to assume $\mathrm{char}(K) = 0$ for the remainder of this tutorial.

e) Show that we have $\mathrm{edim}(R_{\mathfrak{m}}) = n - \mathrm{rk}\left(\mathrm{Jac}(\mathcal{F})(0, \ldots, 0)\right)$. Conclude that $R_{\mathfrak{m}}$ is a regular local ring if and only if the rank of the matrix $\mathrm{Jac}(\mathcal{F})(0, \ldots, 0) \in \mathrm{Mat}_{s,n}(K)$ is $n - \dim(R_{\mathfrak{m}})$.
Hint: Compare the dimensions of $\mathfrak{m}/\mathfrak{m}^2$ and $(x_1, \ldots, x_n)/(x_1, \ldots, x_n)^2$.

f) (This part is quite difficult. Attempt to solve it only on a day when you feel very brave.) Show that the $\mathfrak{m}$-adic Hilbert series $\mathrm{HS}_{R,\mathfrak{m}}(z)$ of R

defined in the preceding tutorial has the shape $\mathrm{HS}_{R,\mathfrak{m}}(z) = \frac{p(z)}{(1-z)^d}$ for some polynomial $p(z) \in \mathbb{Q}[z]$ with $p(1) \neq 0$ and with $d = \mathrm{Kdim}(R_{\mathfrak{m}})$.
Hint: Imitate the proof of Theorem 5.6.36. Prove that the number d does not change when you replace $\mathfrak{m}$ by an $\mathfrak{m}$-primary ideal and that it goes down by one when you replace R by $R/(a)$ for some non-zero divisor a of R.

g) Using e) and f), construct an algorithm for checking whether o is a regular point of V or a singularity. Implement this algorithm in a CoCoA function `IsSingular(...)`. Apply your function to the examples in d) and to the following varieties in $\mathbb{A}^3_{\mathbb{Q}}$ defined over $P = \mathbb{Q}[x, y, z]$. (If possible, sketch them!)

1) $V_1 = \mathcal{Z}(x^2 + y^2 - z^2)$ (circular cone)
2) $V_2 = \mathcal{Z}(xy,\, xz)$ (a line and a plane)
3) $V_3 = \mathcal{Z}(x^2 - y^2)$ (two planes)
4) $V_4 = \mathcal{Z}(x - y^2 - z^2)$ (paraboloid)
5) $V_5 = \mathcal{Z}(x - y^2, x - z^3)$ (twisted cubic curve)
6) $V_6 = \mathcal{Z}(x^2 - yz^2)$
7) $V_7 = \mathcal{Z}(x^2 + y^3 - yz^2)$
8) $V_8 = \mathcal{Z}(xyz + x^4 + y^4 + z^4)$
9) $V_9 = \mathcal{Z}(x^2 + y^4z^2 - 2y^3z^3 + y^2z^4 + y^7 + z^7)$

Now that we know how to decide whether o is a singularity of V or not, we can ask the same question for other points of V. Here we say that a point $p \in V$ is a singularity of V (resp. a regular point of V) if the point o is a singularity (resp. a regular point) of the affine variety obtained by performing a linear change of coordinates which maps p to o. The set of all singular points of V is denoted by $\mathrm{Sing}(V)$ and is called the **singular locus** of V.

h) Show that the notion of a singularity of V is well-defined, i.e. that it does not depend on the linear change of coordinates we choose.

i) Let $p = (p_1, \ldots, p_n) \in V$, let $\overline{P} = \overline{K}[x_1, \ldots, x_n]$, let $\mathfrak{p}$ be the ideal $(x_1 - p_1, \ldots, x_n - p_n)$ in $\overline{P}$, and let $\overline{P}_{\mathfrak{p}}$ be the localization of $\overline{P}$ at the multiplicative set $\overline{P} \setminus \mathfrak{p}$. Prove that we have

$$\mathrm{rk}\left(\mathrm{Jac}(\mathcal{F})(p_1, \ldots, p_n)\right) \leq n - \dim(\overline{P}_{\mathfrak{p}}/(f_1, \ldots, f_s)\overline{P}_{\mathfrak{p}})$$

and that p is a singularity of V if and only if we have a strict inequality here.

j) Suppose that V is **equi-dimensional** of dimension $d = \dim(V)$, i.e. that we have $\dim(P/\mathfrak{q}) = d$ for every minimal prime $\mathfrak{q}$ of I. Show that we have $\mathrm{Sing}(V) = \mathcal{Z}(I + J)$ where J is the ideal generated by the minors of size $(n-d) \times (n-d)$ of the Jacobian matrix $\mathrm{Jac}(\mathcal{F})$.

k) Write a CoCoA function `Sing(...)` which takes I, checks whether the affine variety $V = \mathcal{Z}(I)$ is equidimensional, and computes the ideal defining the singular locus of V in that case.
Hint: Use the built-in CoCoA function `EquiIsoDec(...)`.

Having found the singularities of an equidimensional variety V, we are interested in studying their properties. Does $\mathrm{Sing}(V)$ consist only of a few isolated points? Are they singular because they are contained in several irreducible components of V? How does V "look" locally in the vicinity of a singular point? Can we distinguish different types of singularities? These are difficult questions. In what follows we try to answer them partially in a special case.

Let V be a hypersurface, i.e. assume that $V = \mathcal{Z}(f)$ is defined by a single polynomial $f \in P$, let $p = (p_1, \ldots, p_n) \in \overline{K}^n$, and let $\mathfrak{p}$ be the corresponding maximal ideal $\mathfrak{p} = (x_1 - p_1, \ldots, x_n - p_n) \subseteq \overline{P}$. We introduce the following notions.

1) The point p is called an **isolated critical point** of f if the ideal $(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})\overline{P}_{\mathfrak{p}}$ is $\mathfrak{p}\overline{P}_{\mathfrak{p}}$-primary.
2) The point p is called an **isolated singularity** of V if $(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})\overline{P}_{\mathfrak{p}}$ is a $\mathfrak{p}\overline{P}_{\mathfrak{p}}$-primary ideal.
3) The number $\mathrm{Mil}_p(V) = \dim_K(\overline{P}_{\mathfrak{p}}/(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})\overline{P}_{\mathfrak{p}}) \in \mathbb{N} \cup \{\infty\}$ is called the **Milnor number** of V at p.
4) The number $\mathrm{Tju}_p(V) = \dim_K(\overline{P}_{\mathfrak{p}}/(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})\overline{P}_{\mathfrak{p}}) \in \mathbb{N} \cup \{\infty\}$ is called the **Tjurina number** of V at p.

The Milnor number and the Tjurina number allow us a first insight into the nature of a singularity. In the following we assume that we have moved the point p to the origin $o = (0, \ldots, 0)$.

l) Show that $\mathrm{Mil}_o(V) < \infty$ if and only if o is an isolated critical point of f.
m) Prove that $\mathrm{Tju}_o(V) < \infty$ if and only if o is an isolated singularity of V.
n) Show that $\mathrm{Mil}_o(V) > 0$ if and only if o is a **critical point** of f, i.e. if and only if $o \in \mathcal{Z}((\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}))$.
o) Prove that $\mathrm{Tju}_o(V) > 0$ if and only if $o \in \mathrm{Sing}(V)$.
p) Show that C_2 – C_6, V_1, V_7 – V_9 are precisely the varieties among the examples in d) and g) which have an isolated singularity at o.
q) Write CoCoA functions `Milnor(...)` and `Tjurina(...)` which compute the Milnor number and the Tjurina number of V at o, respectively. Apply your functions to the isolated singularities found in p).

Assume that o is an isolated singularity of V. Then o is called a **node** if the **Hessian matrix** $\mathrm{Hess}(\mathcal{F}) = \left(\frac{\partial^2 f}{\partial x_i \partial x_j}\right) \in \mathrm{Mat}_n(P)$ is non-singular at o, i.e. if we have $\det(\mathrm{Hess}(\mathcal{F})(0, \ldots, 0)) \neq 0$.

r) Show that o is a node of V if and only if $\mathrm{Mil}_o(V) = 1$, and that this is also equivalent to $\mathrm{Tju}_o(V) = 1$.
s) Write a CoCoA function `IsNode(...)` which checks whether o is a node of $V = \mathcal{Z}(I)$. Determine the nodes among the isolated singularities found in p).

6.6 SAGBI Bases

Boo Barkee revealed his love for mathematics
when he licked a draft of the paper about SAGBI.
(From "**S**ubalgebra **A**nalog to **G**röbner **B**ases for **I**deals")

Two mathematicians were walking in a forest. They were discussing the question whether it is possible to generalize Gröbner bases to subalgebras. Suddenly they realized that they had forgotten the sheets of scrap paper on which they had scribbled some new results. They decided to turn around and head home where they had left the dog Boo. And when they arrived, they were astonished to see that Boo had revealed his love for mathematics. He had been playing with the sheets, licking them, and spreading them all around the house. The revelation motivated further development of the theory and they invented the acronym "**S**ubalgebra **A**nalogs to **G**röbner **B**ases for **I**deals". This happened in the good old days. Boo has now passed away, but what has become of SAGBI bases since then? How should we integrate a theory for subalgebras with theories for ideals and modules?

We learn from history that we do not learn from history.

Trying to learn from Chapter 2, we want to define a subalgebra analog to Gröbner bases. A careful reading of the previous section suggests how we can go about this: given a subalgebra S of a polynomial ring $P = K[x_1, \ldots, x_n]$ over a field K and a term ordering σ on $\mathbb{T}^n$, the σ-Gröbner filtration on P induces a filtration Ψ on S. A subset $G \subseteq S \setminus \{0\}$ is called a σ-SAGBI basis of S if the leading terms $\{\mathrm{LT}_\sigma(g) \mid g \in G\}$ generate the K-algebra $\mathrm{gr}_\Psi(S)$. Although this approach is the correct one, we have to be extremely cautious because subalgebras of P need not be finitely generated. For instance the subalgebra S of $P = K[x, y]$ defined by $S = K[x, xy, xy^2, xy^3, \ldots]$ is not finitely generated. After we identify $\mathrm{gr}_\Psi(S)$ with the K-subalgebra $K[\mathrm{LT}_\sigma(f) \mid f \in S \setminus \{0\}]$ of S, we discover that some K-subalgebras $S \subseteq P$ have no finite SAGBI basis whatsoever (see Examples 6.6.7 and 6.6.8). Fortunately, SAGBI bases do share some of the good properties of Gröbner bases. They generate the subalgebra (see Proposition 6.6.3) and they satisfy the SAGBI analogs of Conditions B) in Section 2.1 (see Corollary 6.6.5.c). In several special cases, we prove that finite SAGBI bases exist, e.g. for subalgebras of $K[x]$ (see Proposition 6.6.9), for systems of generators having algebraically independent leading terms (see Proposition 6.6.11), and for subalgebras containing elements f_i with $\mathrm{LT}_\sigma(f_i) \in K[x_i]$ for $i = 1, \ldots, n$ (see Proposition 6.6.13).

Those who fail to learn from history are doomed to repeat it.

So, how far does the analogy between Gröbner bases and SAGBI bases extend? Are we doomed to repeat everything we did in Chapter 2? In the second subsection we dig deeper and deeper into this topic and try to recreate Theorem 2.4.1 in the SAGBI world. The SAGBI basis analogs of Conditions A)

in Section 2.1 and Conditions C) in Section 2.2 are straightforward to introduce (see Propositions 6.6.14 and 6.6.18). The most difficult aspect is the characterization of Gröbner bases by the lifting of syzygies. In SAGBI basis theory, the module of syzygies has to be replaced by the ideal of algebraic relations. Then everything works as expected. We construct the fundamental SAGBI diagram (see Proposition 6.6.22) and formulate the SAGBI equivalents of Conditions D) in Section 2.3 (see Proposition 6.6.23). Finally, our historical excursion reaches port in Theorem 6.6.25 which says that all these Conditions A), B), C), and D) characterize SAGBI bases.

Everytime history repeats itself the price goes up.

Having worked our way through such a formidable chunk of theory, we naturally want to compute SAGBI bases. The third subsection is devoted to this task. As before we want to redo the construction of Buchberger's Algorithm in Section 2.5 but before we even start we have to face the reality that prices have gone up much more than the official estimate predicted. There is no hope to find an algorithm because, as we saw, not every K-subalgebra of P has a finite SAGBI basis. Hence the best we can hope for is an *enumerating procedure*. This is a procedure which looks, smells, and tastes like an algorithm but it comes without the guarantee of finiteness. Using T-polynomials, the SAGBI analogs of S-polynomals, we derive the SAGBI Basis Criterion 6.6.28, the SAGBI analog of the Buchberger's Criterion 2.5.3. Then we introduce the SAGBI Basis Procedure, the SAGBI analog of Buchberger's Algorithm 2.5.5. This procedure entails further "sagbities", the SAGBI analogs of subtleties, because one cannot add new SAGBI basis elements one at a time. Rather, it is essential that the irreducible reductions of all T-polynomials are appended simultaneously, as the Tricky Example 6.6.30 shows.

The only thing we learn from history is that we learn nothing.

Is this really true? We hope not. Instead, we would like you to study reduced and truncated SAGBI bases in Tutorial 96, and we would like to entice you to employ subalgebras of polynomial rings for gluing points (see Exercise 8) and for computing invariants using a Hilbert-driven strategy (see Tutorial 98).

Although the details are beyond the scope of this book, let us point out that SAGBI bases have a geometric interpretation, too. Suppose there exists a finite σ-SAGBI basis $G = \{g_1, \ldots, g_s\}$ of S. The K-algebra homomorphism $K[y_1, \ldots, y_s] \longrightarrow S$ defined by $y_i \mapsto g_i$ corresponds to a "parametrized" affine variety. Similarly, the map $K[y_1, \ldots, y_s] \longrightarrow S$ defined by $y_i \mapsto \mathrm{LT}_\sigma(g_i)$ corresponds to a "toric" variety. In the language of algebraic geometry one can express this situation by saying that a SAGBI basis gives rise to a "deformation" of an arbitrary parametrized variety into a toric variety. This is the SAGBI analog of the flat family we discussed in Section 4.3.B. Once again history repeats itself but on a different level and with some new twists.

6.6.A Definition and Basic Properties of SAGBI Bases

In the following we let K be a field, $P = K[x_1, \ldots, x_n]$ a polynomial ring over K, and $S \subseteq P$ a finitely generated K-subalgebra. Thus there are polynomials $f_1, \ldots, f_s \in P$ such that $S = K[f_1, \ldots, f_s]$. In other words, the ring S is the image of the K-algebra homomorphism $\varphi : K[y_1, \ldots, y_s] \longrightarrow P$ defined by $\varphi(y_i) = f_i$. Given a filtration on P, we can introduce an induced filtration on S in the same way as we did for ideals (see Proposition 6.5.9).

Proposition 6.6.1. *Let $m \geq 1$, let σ be a monoid ordering on $\mathbb{Z}^m$, and let $\Phi = \{F_\gamma P \mid \gamma \in \mathbb{Z}^m\}$ be a $(\mathbb{Z}^m, \sigma)$-filtration on P.*

a) For every $\gamma \in \mathbb{Z}^m$, let $F_\gamma S = (F_\gamma P) \cap S$. The family $\Psi = \{F_\gamma S \mid \gamma \in \mathbb{Z}^m\}$ is a $(\mathbb{Z}^m, \sigma)$-filtration on S. It is called the **induced filtration** *on S.*

b) The canonical K-linear maps $F_\gamma S / F_{<_\sigma \gamma} S \longrightarrow F_\gamma P / F_{<_\sigma \gamma} P$ give rise to a homogeneous injective K-algebra homomorphism $\imath : \mathrm{gr}_\Psi(S) \hookrightarrow \mathrm{gr}_\Phi(P)$.

c) If Φ is an orderly filtration then Ψ is also orderly, and the map $\imath$ satisfies $\imath(\mathrm{LF}_\Psi(f)) = \mathrm{LF}_\Phi(f)$ for all $f \in S \setminus \{0\}$. Consequently, the image of $\imath$ is the K-subalgebra $K[\mathrm{LF}_\Phi(f) \mid f \in S \setminus \{0\}]$ of $\mathrm{gr}_\Phi(P)$.

Proof. Claim a) is clearly true. The proof of b) is analogous to the proof of Proposition 6.5.9.b. Claim c) follows immediately from b). □

The most interesting situation arises when Φ is a Gröbner filtration. Recall that in this case we have an isomorphism $\mathrm{gr}_\Phi(P) \xrightarrow{\sim} P$ (see Proposition 6.5.8.c). Using the composition $\mathrm{gr}_\Psi(S) \hookrightarrow \mathrm{gr}_\Phi(P) \xrightarrow{\sim} P$, we can identify $\mathrm{LF}_\Psi(f)$ with $\mathrm{LM}_\sigma(f)$ for every $f \in S \setminus \{0\}$. This identification will be used throughout the section without further mention.

In the following we let σ be a term ordering on $\mathbb{T}^n$, we let Φ be the σ-Gröbner filtration on P, and we let Ψ be the induced filtration on S. Note that the above identification implies $\mathrm{gr}_\Psi(S) = K[\mathrm{LT}_\sigma(f) \mid f \in S \setminus \{0\}]$. In particular, this associated graded ring is an integral domain because it is a K-subalgebra of P. To simplify the notation, we write $K[T]$ instead of $K[f \mid f \in T]$ when T is a subset of P. Likewise, for $T \subseteq P \setminus \{0\}$, we let $\mathrm{LT}_\sigma(T) = \{\mathrm{LT}_\sigma(f) \mid f \in T\}$.

Definition 6.6.2. A set $G \subseteq S \setminus \{0\}$ is called a **σ-SAGBI basis** of S if we have $\mathrm{gr}_\Psi(S) = K[\mathrm{LT}_\sigma(G)]$.

Clearly, this notion is the subalgebra analog to the notion of a standard basis. Since standard bases for Gröbner filtrations are Gröbner bases, we recover the meaning of the acronym "SAGBI" once again: **S**ubalgebra **A**nalog to **G**röbner **B**ases for **I**deals. It is obvious that every K-subalgebra has a SAGBI basis, because the set $S \setminus \{0\}$ is a σ-SAGBI basis of S for every term ordering σ. However, this set is not really an exciting SAGBI basis since it is not finite. A standard basis of an ideal need not generate it (see Example 6.5.15), but SAGBI bases do not share this bad behaviour, as the following result shows.

Proposition 6.6.3. *Every σ-SAGBI basis of S is a system of K-algebra generators of S.*

Proof. Let $G \subseteq S \setminus \{0\}$ be a σ-SAGBI basis of S. For a contradiction, assume that $K[G] \subset S$. Let $f \in S \setminus K[G]$ be an element whose leading term is minimal with respect to σ. Since $\mathrm{LT}_\sigma(f) \in K[\mathrm{LT}_\sigma(G)]$, there exist elements $g_1, \ldots, g_\ell \in G$, and exponents $a_1, \ldots, a_\ell \in \mathbb{N}_+$ such that $\mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(g_1)^{a_1} \cdots \mathrm{LT}_\sigma(g_\ell)^{a_\ell}$. Hence the leading term of the polynomial $h = f - \mathrm{LC}_\sigma(f)\,\mathrm{LC}_\sigma(g_1^{a_1} \ldots g_\ell^{a_\ell})^{-1} g_1^{a_1} \cdots g_\ell^{a_\ell}$ satisfies the inequality $\mathrm{LT}_\sigma(h) <_\sigma \mathrm{LT}_\sigma(f)$. Thus we get $h \in K[G]$, contradicting $f \notin K[G]$. □

The ring $\mathrm{gr}_\Psi(S)$ is a **monomial subalgebra** of P, i.e. a subalgebra for which there exists a set of K-algebra generators consisting of terms. For every $m \geq 1$ and every $\mathbb{Z}^m$-grading on P given by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, a monomial subalgebra is a graded subalgebra of P with respect to this grading. Moreover, monomial subalgebras have the following properties.

Proposition 6.6.4. *Let $S \subseteq P$ be a monomial subalgebra, and let G be a set of terms which generates the K-algebra S.*

a) Every term in the support of a polynomial in S is a power product of terms in G. In particular, the term itself is contained in S.
b) Among all sets of terms which generate the K-algebra S there is a unique minimal element with respect to inclusion. We call it the **minimal monomial system of algebra generators** *of S.*
c) If S is a finitely generated K-algebra, its minimal monomial system of algebra generators is finite.

Proof. First we show a). Every $f \in S$ is of the form $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha g_1^{\alpha_1} \cdots g_s^{\alpha_s}$ with $c_\alpha \in K$ and $g_1, \ldots, g_s \in G$. Thus we see that every term in the support of f is a power product of $g_1, \ldots, g_s$.

To prove b), it suffices to show that two irredundant monomial systems of algebra generators T_1 and T_2 of S are equal. For a contradiction, suppose that $T_1 \neq T_2$. Since T_1 and T_2 are irredundant, we find $t_1 = \min_\sigma(T_1 \setminus T_2)$ and $t_2 = \min_\sigma(T_2 \setminus T_1)$. Without loss of generality we may assume $t_1 <_\sigma t_2$. Since t_1 is a power product of terms in T_2 and smaller with respect to σ than any element in $T_2 \setminus T_1$, it has to be a power product of elements in $T_2 \cap T_1$. This contradicts the hypothesis that T_1 is irredundant.

Finally we show c). By a), the terms in the support of the polynomials of a finite set of K-algebra generators of S are a finite monomial system of K-algebra generators of S. By b), this set contains the minimal monomial system of K-algebra generators of S. □

When we apply this proposition to the monomial subalgebra $\mathrm{gr}_\Psi(S)$ of P, we obtain the following result.

Corollary 6.6.5. *Let S be a K-subalgebra of P.*

a) Every term in $\mathrm{gr}_\Psi(S)$ is a leading term of an element of S.
b) The ring $\mathrm{gr}_\Psi(S)$ has a unique minimal monomial system of algebra generators consisting of leading terms $\mathrm{LT}_\sigma(f)$ where $f \in S \setminus \{0\}$. In particular, there exists a finite σ-SAGBI basis of S if and only if this minimal monomial system of algebra generators is finite.
c) For a set $G \subseteq P \setminus \{0\}$ with $S = K[G]$, the following conditions are equivalent.

B_1) We have $\mathrm{gr}_\Psi(S) = K[\mathrm{LT}_\sigma(G)]$, i.e. G is a σ-SAGBI basis of S.
B_2) The monoid $\{\mathrm{LT}_\sigma(f) \mid f \in S \setminus \{0\}\}$ is generated by the set of leading terms $\{\mathrm{LT}_\sigma(f) \mid f \in G\}$.

Proof. The first claim follows from the proposition and the observation that a power product of leading terms is a leading term. Claims b) and c) follow immediately from the proposition. □

When the polynomial ring P is graded by a matrix, subalgebras generated by homogeneous polynomials are also graded and Hilbert functions can be defined for them as follows.

Proposition 6.6.6. *Let P be graded by a matrix $W \in \mathrm{Mat}_{m,n}(\mathbb{Z})$, and let $S \subseteq P$ be a K-subalgebra generated by a set of non-zero homogeneous polynomials.*

a) For every $d \in \mathbb{Z}^m$ let $S_d = P_d \cap S$. Then we have $S = \bigoplus_{d \in \mathbb{Z}^m} S_d$ and this decomposition turns S into a $\mathbb{Z}^m$-graded K-subalgebra of P.
b) If W is of positive type, we have $\mathrm{HF}_S(d) = \mathrm{HF}_{\mathrm{gr}_\Psi(S)}(d)$ for all $d \in \mathbb{Z}^m$.
c) Suppose that $S = K[f_1, \ldots, f_s]$ with homogeneous non-zero polynomials $f_1, \ldots, f_s \in P$, and let $d_i = \deg_W(f_i)$ for $i = 1, \ldots, s$. Let $y_1, \ldots, y_s$ be further indeterminates, and let $K[y_1, \ldots, y_s]$ be equipped with the $\mathbb{Z}^m$-grading given by $U = (d_1 \cdots d_s)$. Then the surjective K-algebra homomorphism $\varepsilon : K[y_1, \ldots, y_s] \longrightarrow S$ defined by $\varepsilon(y_i) = f_i$ for $i = 1, \ldots, s$ is homogeneous. It induces an isomorphism of graded K-algebras $\bar{\varepsilon} : K[y_1, \ldots, y_s]/J \longrightarrow S$ where J is a homogeneous ideal.

Proof. To prove a), it suffices to show the claim $S = \sum_{d \in \mathbb{Z}^m} (P_d \cap S)$. Notice that this sum is direct, since it is so in P. Let $F \subseteq P \setminus \{0\}$ be a homogeneous system of generators of the K-algebra S, and let $f \in S$. Then there exist elements $f_1, \ldots, f_s \in F$ and a polynomial $g \in K[y_1, \ldots, y_s]$ such that $f = g(f_1, \ldots, f_s)$. We write $g = c_1 t_1 + \cdots + c_r t_r$ with coefficients $c_1, \ldots, c_r \in K \setminus \{0\}$ and terms $t_1, \ldots, t_r \in \mathbb{T}(y_1, \ldots, y_s)$. Then we have $f = c_1 t_1(f_1, \ldots, f_s) + \cdots + c_s t_s(f_1, \ldots, f_s)$ and the fact that the polynomials $t_i(f_1, \ldots, f_s)$ are homogeneous yields the claim.

Now we show b). First we claim that every term $t \in \mathrm{gr}_\Psi(S)$ is the leading term of a polynomial in S. Namely, given a term $t \in \mathrm{gr}_\Psi(S)$, there exist $g_1, \ldots, g_\ell \in S$ and $a_1, \ldots, a_\ell \in \mathbb{N}_+$ such that $t = (\mathrm{LT}_\sigma(g_1))^{a_1} \cdots (\mathrm{LT}_\sigma(g_\ell))^{a_\ell}$,

and this yields $t = \mathrm{LT}_\sigma(g_1^{a_1} \cdots g_s^{a_s})$. Next we consider a degree $d \in \mathbb{Z}^m$. We note that S_d is the K-vector space generated by all homogeneous polynomials of degree d which are contained in S. It is a finite dimensional K-vector space because it is a subspace of P_d and P_d is finite dimensional since W is of positive type. Using linear reductions, we may assume that there is a K-basis of S_d consisting of polynomials with pairwise distinct leading terms with respect to σ. These leading terms are the only possible leading terms of elements of S_d. By our initial claim, the leading terms of the polynomials in S_d generate $\mathrm{gr}_\Psi(S)_d$. This completes the proof of b).

Finally, to show c), it suffices to remark that ε is homogeneous because $\deg_U(y_i) = d_i = \deg_W(f_i)$ for $i = 1, \ldots, s$. □

We have already seen that infinite SAGBI-bases always exist. But what about finite SAGBI-bases? In the following examples we exhibit subalgebras of P which have no finite SAGBI basis at all.

Example 6.6.7. Let $P = K[x_1, x_2]$ be standard graded, and let $S \subseteq P$ be the K-subalgebra $S = K[f_1, f_2, f_3]$ where $f_1 = x_1 + x_2$, $f_2 = x_1x_2$, and $f_3 = x_1x_2^2$. We want to show that S has no finite σ-SAGBI basis, no matter which term ordering σ we use. The proof consists of several steps.

1) Since we have $x_1^2x_2 = (x_1 + x_2)x_1x_2 - x_1x_2^2 = f_1f_2 - f_3 \in S$, we can represent S as $S = K[x_1 + x_2, x_1x_2, x_1^2x_2, x_1x_2^2]$. In particular, we see that S is invariant under the interchange of x_1 and x_2.
2) Using Proposition 6.6.6.c, we construct an isomorphism of graded K-algebras $\bar{\varepsilon} : K[y_1, y_2, y_3]/J \longrightarrow S$ which satisfies $\bar{\varepsilon}(y_i + J) = f_i$. Here $K[y_1, y_2, y_3]$ is graded by the matrix $W = (1\ 2\ 3)$ and J is a homogeneous ideal with respect to this grading. We compute the ideal J by implicitization (see Corollary 3.6.3) and get $J = y_2^3 - y_1y_2y_3 + y_3^2$. Since this is a principal ideal generated by a homogeneous polynomial of degree 6, the Hilbert series of S is

$$\begin{aligned} \mathrm{HS}_S(z) &= \tfrac{1-z^6}{(1-z)(1-z^2)(1-z^3)} = \tfrac{1-z+z^2}{(1-z)^2} = (1 - z + z^2)(1 + 2z + 3z^2 + \cdots) \\ &= 1 + z + 2z^2 + 3z^3 + \cdots \end{aligned}$$

by Proposition 5.8.9.d and Theorem 5.8.10. In particular, we see that $\mathrm{HF}_S(i) = \mathrm{HF}_P(i) - 1$ for all $i > 1$.
3) We want to show that every σ-SAGBI basis of S is infinite. By 1), we may assume that $x_1 >_\sigma x_2$. We claim that we have $x_1^a x_2^b \in \mathrm{gr}_\Psi(S)$ for all $a > 0$ and $b \geq 0$ but $x_2^b \notin \mathrm{gr}_\Phi(S)$ for $b > 0$.
To prove this claim, we note that since $x_1 = \mathrm{LT}_\sigma(f_1) \in \mathrm{gr}_\Psi(S)$ it suffices to treat the case $a = 1$. Now we use induction on b. Clearly, the claim holds for $b \in \{0, 1, 2\}$ because we have $x_1x_2 = \mathrm{LT}_\sigma(f_2) \in \mathrm{gr}_\Psi(S)$ and $x_1x_2^2 = \mathrm{LT}_\sigma(f_3) \in \mathrm{gr}_\Psi(S)$. For $b \geq 3$, the claim follows by induction using the formula $x_1x_2^b = f_1\, x_1x_2^{b-1} - f_2\, x_1x_2^{b-2}$.

4) By combining the results of steps 2) and 3), it follows for every $d \geq 1$ that $(\mathrm{gr}_\Psi(S))_d = K\, x_1^d \oplus \cdots \oplus K\, x_1 x_2^{d-1}$. From this we deduce that we have $\mathrm{gr}_\Psi(S) = K[x_1, x_1x_2, x_1x_2^2, \ldots]$. This ring is not a finitely generated K-algebra because $x_1x_2^d \notin K[x_1, x_1x_2, \ldots, x_1x_2^{d-1}]$ for every $d \geq 1$ since $\deg_{x_1}(x_1x_2^d) = 1$. Consequently, the K-algebra S has no finite σ-SAGBI basis, as we wanted to show.

Our next example is similar, but slightly more involved. It will be used later to study our algorithm for computing SAGBI bases (see Example 6.6.30).

Example 6.6.8. Let $P = \mathbb{Q}[x_1, x_2]$ be standard graded, and let $S \subseteq P$ be the $\mathbb{Q}$-subalgebra $S = \mathbb{Q}[f_1, f_2, f_3]$ where $f_1 = x_1 - x_2$, $f_2 = x_1x_2 - x_2^2$, and $f_3 = x_1x_2^2$. We want to show that S has no finite σ-SAGBI basis, no matter which term ordering σ we use. Again the proof consists of several steps.

1) Using Proposition 6.6.6.c, we construct an isomorphism of graded K-algebras $\bar{\varepsilon} : K[y_1, y_2, y_3]/J \longrightarrow S$ where $K[y_1, y_2, y_3]$ is graded by the matrix $W = (1\ 2\ 3)$ and J is a homogeneous ideal with respect to this grading. We compute the ideal J by implicitization and obtain $J = (y_1^2y_2^2 - y_2^3 - y_1^3y_3)$. Therefore the Hilbert series of S is
$$\mathrm{HS}_S(z) = \tfrac{1-z^6}{(1-z)(1-z^2)(1-z^3)} = 1 + z + 2z^2 + 3z^3 + \cdots$$
and we get $\mathrm{HF}_S(i) = \mathrm{HF}_P(i) - 1$ for all $i > 1$.
2) Next we choose a term ordering σ on $\mathbb{T}^2$ for which $x_1 >_\sigma x_2$. To show that $x_1^a x_2^b \in \mathrm{gr}_\Psi(S)$ for $a > 0$ and $b \geq 0$ it suffices to deal with the case $a = 1$ because $x_1 = \mathrm{LT}_\sigma(f_1) \in \mathrm{gr}_\Psi(S)$. The proof that $x_1x_2^b \in \mathrm{gr}_\Psi(S)$ for $b \geq 0$ is divided into two steps.
3) For $0 \leq b \leq 4$ we have $x_1 = \mathrm{LT}_\sigma(f_1)$, $x_1x_2 = \mathrm{LT}_\sigma(f_2)$, $x_1x_2^2 = \mathrm{LT}_\sigma(f_3)$, and we can check that
$$\begin{aligned} x_1x_2^3 &= \mathrm{LT}_\sigma(f_4) \quad \text{for} \quad f_4 = x_1x_2^3 - x_2^4 = f_1f_3 - f_2^2 \in S \\ x_1x_2^4 &= \mathrm{LT}_\sigma(f_5) \quad \text{for} \quad f_5 = x_1x_2^4 - x_2^5 = f_2f_3 - f_1f_4 \in S \end{aligned}$$
4) Now we use induction in steps of three. The base cases $b = 2$, $b = 3$, and $b = 4$ were treated in step 3). For $b \geq 5$, we claim that
$$\begin{aligned} f_{b+1} &= x_1x_2^{3c-1} - \tfrac{c-1}{c}x_2^{3c} = -\tfrac{c-1}{c}\,(f_2f_{3c-2} - f_3f_{3c-3}) && \text{if } b{+}1 = 3c \\ f_{b+1} &= x_1x_2^{3c} - x_2^{3c+1} = -(f_2f_{3c-1} - f_3f_{3c-2}) && \text{if } b{+}1 = 3c{+}1 \\ f_{b+1} &= x_1x_2^{3c+1} - x_2^{3c+2} = -\tfrac{c}{c-1}\,(f_2f_{3c} - f_3f_{3c-1}) && \text{if } b{+}1 = 3c{+}2 \end{aligned}$$
There are three possibilities. If $b + 1 = 3c + 3$, this follows from
$$\begin{aligned} f_{b+1} &= f_{3(c+1)} = x_1x_2^{3c+2} - \tfrac{c}{c+1}\,x_2^{3c+3} \\ &= -\tfrac{c}{c+1}\big((x_1x_2 - x_2^2)(x_1x_2^{3c} - x_2^{3c+1}) - x_1x_2^2(x_1x_2^{3c-1} - \tfrac{c-1}{c}\,x_2^{3c})\big) \\ &= -\tfrac{c}{c+1}(f_2f_{3c+1} - f_3f_{3c}) \end{aligned}$$

Secondly, if $b+1 = 3c+4$, it follows from

$$\begin{aligned} f_{b+1} &= f_{3(c+1)+1} = x_1 x_2^{3c+3} - x_2^{3c+4} \\ &= -(x_1 x_2 - x_2^2)(x_1 x_2^{3c+1} - x_2^{3c+2}) + x_1 x_2^2 (x_1 x_2^{3c} - x_2^{3c+1}) \\ &= -(f_2 f_{3c+2} - f_3 f_{3c+1}) \end{aligned}$$

Thirdly, if $b+1 = 3c+5$, it follows from

$$\begin{aligned} f_{b+1} &= f_{3(c+1)+2} = x_1 x_2^{3c+4} - x_2^{3c+5} \\ &= -\tfrac{c+1}{c}\big((x_1 x_2 - x_2^2)(x_1 x_2^{3c+2} - \tfrac{c}{c+1}\, x_2^{3c+3}) \\ &\quad -x_1 x_2^2 (x_1 x_2^{3c+1} - x_2^{3c+2})\big) = -\tfrac{c+1}{c}\,(f_2 f_{3c+3} - f_3 f_{3c+2}) \end{aligned}$$

In all three cases we have $\mathrm{LT}_\sigma(f_{b+1}) = x_1 x_2^b \in \mathrm{gr}_\Psi(S)$, as we wanted to show.

5) Now the argument continues as in the preceding example. We conclude that $\mathrm{gr}_\Psi(S) = \mathbb{Q}[x_1, x_1x_2, x_1x_2^2, \ldots]$ and that S has no finite σ-SAGBI basis.
6) Finally, if σ is a term ordering on $\mathbb{T}^2$ with $x_2 >_\sigma x_1$, we can use a similar argument as in steps 3) and 4) to show that for every $d \geq 1$ there exists an element $x_1^{d-1}x_2 + c_d x_1^d \in S$ with $c_d \in \mathbb{Q}$. Since $x_2 = \mathrm{LT}_\sigma(f_1)$, we get $\mathrm{gr}_\Psi(S) = K[x_2, x_1x_2, x_1^2x_2, \ldots]$, and hence there is no finite σ-SAGBI basis of S.

Altogether, we have shown that S has no finite SAGBI basis.

The remaining part of this subsection is devoted to providing some situations in which finite SAGBI bases do exist. The first result of this kind concerns the univariate case.

Proposition 6.6.9. *Let $P = K[x]$, and let $S \subseteq P$ be a K-subalgebra.*

a) The K-algebra S is finitely generated.
b) Let σ be a term ordering. Then S has a finite σ-SAGBI basis.

Proof. To prove a), we let S be a K-subalgebra of P. If $S = K$, there is nothing to prove. So we may assume that there exists a non-constant polynomial f in S. We let $S_0 = K[f]$ and observe that P is generated by $\{1, x, \ldots, x^{\deg(f)-1}\}$ as an S_0-module. Now Lemma 2.6.5 implies that S is an affine K-algebra.

Next we prove b). Let Ψ be the σ-Gröbner filtration on P. The associated graded ring $\mathrm{gr}_\Psi(S)$ is a graded K-subalgebra of P. By a), it is a finitely generated K-algebra. Since it is also graded, it is generated by finitely many powers of x. Now the claim follows from Corollary 6.6.5.a. □

By combining this proposition with the algorithm for computing finite SAGBI bases given in the third subsection, we can sometimes simplify subalgebras of $K[x]$ considerably.

Example 6.6.10. Let K be a field, let $P = K[x]$, and let $S \subseteq P$ be the K-subalgebra $S = K[x^3 - x,\ x^4,\ x^5 - 1] \subseteq P$. When we compute a `Deg`-SAGBI basis of S (see Example 6.6.31), we find that $G = \{x\}$ is one. In this way SAGBI bases allow us to *discover* that $S = K[x]$.

If we know this equality beforehand, it is easy to *check* it with the help of the Subalgebra Membership Test 3.6.7. In fact, we obtain the representation

$$x = -(x^3 - x)^3 + x^4(x^5 - 1) - 3(x^3 - x)x^4 + x^4 - (x^3 - x)$$

which would have been difficult to guess. This means that it would have been difficult to guess that $S = K[x]$.

Before we are able to deal with the computation of SAGBI bases, we need to develop the theory significantly further. We begin with some additional cases where finite SAGBI bases exist.

Proposition 6.6.11. *Let $f_1, \ldots, f_s \in P \setminus \{0\}$, and let $S = K[f_1, \ldots, f_s]$. If the leading terms $\mathrm{LT}_\sigma(f_1), \ldots, \mathrm{LT}_\sigma(f_s)$ are algebraically independent then $\{f_1, \ldots, f_s\}$ is a σ-SAGBI basis of S.*

Proof. Given $f \in S \setminus \{0\}$, there exists a polynomial $g \in K[y_1, \ldots, y_s]$ such that $f = g(f_1, \ldots, f_s)$. Let $m \in \mathrm{Supp}(g)$ be a term for which $m(\mathrm{LT}_\sigma(f_1), \ldots, \mathrm{LT}_\sigma(f_s))$ is maximal with respect to σ. In the computation of $g(f_1, \ldots, f_s)$, the term $m(\mathrm{LT}_\sigma(f_1), \ldots, \mathrm{LT}_\sigma(f_s))$ does not cancel because for $m' \in \mathrm{Supp}(g)$ and $t_i \in \mathrm{Supp}(f_i)$ we have

$$m'(t_1, \ldots, t_s) \leq_\sigma m'(\mathrm{LT}_\sigma(f_1), \ldots, \mathrm{LT}_\sigma(f_s)) \leq_\sigma m(\mathrm{LT}_\sigma(f_1), \ldots, \mathrm{LT}_\sigma(f_s))$$

and the last inequality is strict for $m' \neq m$ since otherwise $m - m'$ would be a non-trivial algebraic relation among $\mathrm{LT}_\sigma(f_1), \ldots, \mathrm{LT}_\sigma(f_s)$. Hence the term $m(\mathrm{LT}_\sigma(f_1), \ldots, \mathrm{LT}_\sigma(f_s))$ equals $\mathrm{LT}_\sigma(f)$. Consequently, we have shown that $\mathrm{LT}_\sigma(f) \in K[\mathrm{LT}_\sigma(f_1), \ldots, \mathrm{LT}_\sigma(f_s)]$ and the claim follows. □

The following example provides a nice application of this proposition to the algebra of symmetric polynomials. Recall that a polynomial is called symmetric if it is invariant under all permutations of the indeterminates. In Tutorial 12 we showed that the algebra of symmetric polynomials is generated by the elementary symmetric polynomials $s_i = \sum_{j_1 < \cdots < j_i} x_{j_1} \cdots x_{j_i}$ where $i \in \{1, \ldots, n\}$. Here we get an even stronger statement.

Corollary 6.6.12. (Symmetric Polynomials and SAGBI Bases) *Let $S \subseteq P$ be the K-subalgebra consisting of all symmetric polynomials, and let $s_1, \ldots, s_n$ be the elementary symmetric polynomials.*

a) The set $\{s_1, \ldots, s_n\}$ is a σ-SAGBI basis of S.
b) The set $\{s_1, \ldots, s_n\}$ is algebraically independent.

Proof. Up to renaming the indeterminates, we may assume that we have $x_1 >_\sigma x_2 >_\sigma \cdots >_\sigma x_n$. Consequently, the leading terms $\mathrm{LT}_\sigma(s_i) = x_1 \cdots x_i$ of the elementary symmetric polynomials are algebraically independent. Hence the proposition shows that $\{s_1, \ldots, s_n\}$ is a σ-SAGBI basis of S.

To prove b), we argue as in the proof of the proposition and show that for a non-zero polynomial $g \in K[y_1, \ldots, y_n]$ we have the relation $\mathrm{LT}_\sigma(g(s_1, \ldots, s_n)) \in K[\mathrm{LT}_\sigma(s_1), \ldots, \mathrm{LT}_\sigma(s_n)]$, and thus $g(s_1, \ldots, s_n) \neq 0$. □

The next proposition is yet another finiteness result for SAGBI bases.

Proposition 6.6.13. *Let S be a K-subalgebra of P, let σ be a term ordering on $\mathbb{T}^n$, and let Ψ be the filtration on S induced by the σ-Gröbner filtration on P. Suppose that for each $i \in \{1, \ldots, n\}$ there exists an integer $\alpha_i > 0$ such that $x_i^{\alpha_i} \in \mathrm{gr}_\Psi(S)$. Then $\mathrm{gr}_\Psi(S)$ is a finitely generated K-algebra. In particular, there exists a finite σ-SAGBI-basis of S.*

Proof. Let $T = \{x_1^{\beta_1} \cdots x_n^{\beta_n} \in \mathbb{T}^n \mid \beta_j < \alpha_j \text{ for } j = 1, \ldots, n\}$, and let A be the affine K-algebra $A = K[x_1^{\alpha_1}, \ldots, x_n^{\alpha_n}]$. Since every term in P is the product of an element of T with a power product of the terms $x_1^{\alpha_1}, \ldots, x_n^{\alpha_n}$, we see that T generates P as an A-module. Thus the inclusions $A \subseteq \mathrm{gr}_\Psi(S) \subseteq P$ show that also $\mathrm{gr}_\Psi(S)$ is a finitely generated A-module. Now we apply Lemma 2.6.3 to the inclusions $K \subseteq A \subseteq \mathrm{gr}_\Psi(S)$ and get the claim. □

6.6.B Characterization of SAGBI Bases

Many a man fails as an original thinker
simply because his memory is too good.
(Friedrich Nietzsche)

To write the following subsection, we had to do a lot of original thinking. Although our memory is not bad and we remember Chapter 2 quite well, our intention to develop the theory of SAGBI bases in analogy with the theory of Gröbner bases led us onto a bumpy road. One difference between Gröbner bases and SAGBI bases has surfaced already in the previous subsection: we have to pay the price that finite SAGBI bases need not exist at all. So, let us go slowly and try to work out SAGBI versions of the characterizations of Gröbner bases in Chapter 2 using a step-by-step approach. We begin at the beginning and ask for a SAGBI version of special generation (see Proposition 2.1.1).

Proposition 6.6.14. *Let $S \subseteq P$ be a K-subalgebra, let σ be a term ordering on $\mathbb{T}^n$, and let $G \subseteq P \setminus \{0\}$. Then the following conditions are equivalent.*

A_1) *For each $f \in S \setminus \{0\}$, there are $g_1, \ldots, g_s \in G$ and $h \in K[y_1, \ldots, y_s]$ with $f = h(g_1, \ldots, g_s)$ and $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(t(g_1, \ldots, g_s))$ for all $t \in \mathrm{Supp}(h)$.*

A_2) *For each* $f \in S\backslash\{0\}$*, there are* $g_1, \ldots, g_s \in G$ *and* $h \in K[y_1, \ldots, y_s]$ *with* $f = h(g_1, \ldots, g_s)$ *and* $\mathrm{LT}_\sigma(f) = \max_\sigma\{\mathrm{LT}_\sigma(t(g_1, \ldots, g_s)) \mid t \in \mathrm{Supp}(h)\}$.

Proof. Since Condition A_2) obviously implies A_1), it suffices to prove the reverse direction. The inequality "$\geq_\sigma$" in A_2) follows immediately from A_1). The inequality "$\leq_\sigma$" in A_2) follows from Proposition 1.5.3.a. □

Both conditions can be rephrased by using $t(\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s))$ instead of $\mathrm{LT}_\sigma(t(g_1, \ldots, g_s))$. Later we shall see that A_1) and A_2) characterize SAGBI bases. For the time being, we merely note that they are not always satisfied.

Example 6.6.15. Let $P = K[x]$, let $\sigma = \mathtt{Deg}$, and let $S \subseteq P$ be the K-subalgebra generated by $G = \{g_1, g_2, g_3\}$ where $g_1 = x^3 - x$, $g_2 = x^4$, and $g_3 = x^5 - 1$ (see Example 6.6.10). Then $h = y_1^2 + y_1 y_3 - y_2^2 + y_1 + 2y_2$ yields $h(g_1, g_2, g_3) = x^2$. However, we have

$$\mathrm{LT}_\sigma(x^2) = x^2 <_\sigma \min_\sigma\{\mathrm{LT}_\sigma(g_1), \mathrm{LT}_\sigma(g_2), \mathrm{LT}_\sigma(g_3)\}$$

Therefore Conditions A_1) and A_2) do not hold for this set G.

To prove a SAGBI analog of Proposition 2.2.5, we need to introduce some terminology.

Definition 6.6.16. Let σ be a term ordering on $\mathbb{T}^n$, and let $G \subseteq P \setminus \{0\}$.

a) Let $f_1 \in P$, and suppose there exist a constant $c \in K$, polynomials $g_1, \ldots, g_s \in G$, and a term $t \in K[y_1, \ldots, y_s]$ such that the polynomial $f_2 = f_1 - c\,t(g_1, \ldots, g_s)$ satisfies $t(\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)) \notin \mathrm{Supp}(f_2)$. Then we say that f_1 **subalgebra reduces** to f_2 in one step and we write $f_1 \xrightarrow{G}_{\mathrm{ss}} f_2$. The passage from f_1 to f_2 is called a **subalgebra reduction step**.

b) The transitive closure of the relations $\xrightarrow{G}_{\mathrm{ss}}$ is called the **subalgebra rewrite relation** defined by G and is denoted by $\xrightarrow{G}_{\mathrm{s}}$.

c) An element $f_1 \in P$ with the property that there exists no subalgebra reduction step $f_1 \xrightarrow{G}_{\mathrm{ss}} f_2$ for which $f_2 \neq f_1$ is called **irreducible** with respect to $\xrightarrow{G}_{\mathrm{s}}$.

d) The equivalence relation defined by $\xrightarrow{G}_{\mathrm{s}}$ will be denoted by $\xleftrightarrow{G}_{\mathrm{s}}$.

As in the case of the rewrite relations in Gröbner basis theory, the effect of a subalgebra reduction step $f_1 \xrightarrow{G}_{\mathrm{ss}} f_2$ is that a term in the support of f_1 is replaced by other terms, all of which are smaller with respect to σ. Notice that $c = 0$ yields the trivial subalgebra reduction step $f_1 \xrightarrow{G}_{\mathrm{ss}} f_1$ and that a constant polynomial $f = c \in K$ can be subalgebra reduced to zero using $0 = f - c \cdot 1$. Subalgebra rewrite relations have properties similar to the rewrite relations in Section 2.2.

Proposition 6.6.17. *Let σ be a term ordering on $\mathbb{T}^n$, and let $G \subseteq P \setminus \{0\}$.*

a) If $f_1, f_2 \in P$ satisfy $f_1 \xrightarrow{G}_{\mathrm{s}} f_2$ and $f_2 \xrightarrow{G}_{\mathrm{s}} f_1$ then $f_1 = f_2$.

b) If $f_1, f_2 \in P$ satisfy $f_1 \xrightarrow{G}_{\mathrm{s}} f_2$ and if $g \in G$ then we have $gf_1 \xrightarrow{G}_{\mathrm{s}} gf_2$.

c) The rewrite relation $\xrightarrow{G}_{\mathrm{s}}$ is **Noetherian**, *i.e. every chain of subalgebra reduction steps $f_1 \xrightarrow{G}_{\mathrm{ss}} f_2 \xrightarrow{G}_{\mathrm{ss}} \cdots$ becomes eventually stationary.*

d) If $f_1, f_2 \in P$ satisfy $f_1 \xrightarrow{G}_{\mathrm{ss}} f_2$ and if $f_3 \in P$ then there exists a polynomial $f_4 \in P$ such that $f_1 + f_3 \xrightarrow{G}_{\mathrm{s}} f_4$ and $f_2 + f_3 \xrightarrow{G}_{\mathrm{s}} f_4$.

e) If $f_1, f_2, f_3, f_4 \in P$ satisfy $f_1 \xleftrightarrow{G}_{\mathrm{s}} f_2$ and $f_3 \xleftrightarrow{G}_{\mathrm{s}} f_4$, we have the equivalence $f_1 + f_3 \xleftrightarrow{G}_{\mathrm{s}} f_2 + f_4$.

f) If $f_1, f_2 \in P$ satisfy $f_1 \xleftrightarrow{G}_{\mathrm{s}} f_2$ and if $f_3 \in K[G]$ then we have $f_1 f_3 \xleftrightarrow{G}_{\mathrm{s}} f_2 f_3$.

g) For $f \in P$, we have $f \xleftrightarrow{G}_{\mathrm{s}} 0$ if and only if $f \in K[G]$.

h) For $f_1, f_2 \in P$, we have $f_1 \xleftrightarrow{G}_{\mathrm{s}} f_2$ if and only if $f_1 - f_2 \in K[G]$.

Proof. The only parts whose proofs differ slightly from the proofs of the corresponding parts of Proposition 2.2.2 are b) and g). To show b), it suffices to consider a single subalgebra reduction step $f_1 \xrightarrow{G}_{\mathrm{ss}} f_2$. We write $f_2 = f_1 - c\,t(g_1, \ldots, g_s)$ with $c \in K$, $t \in \mathbb{T}(y_1, \ldots, y_s)$ and $g_1, \ldots, g_s \in G$. Letting $t' = t\,y_{s+1}$, we obtain $gf_2 = gf_1 - c\,t'(g_1, \ldots, g_s, g)$. Clearly, the term $\mathrm{LT}_\sigma(t'(g_1, \ldots, g_s, g)) = \mathrm{LT}_\sigma(t(g_1, \ldots, g_s)\,g) = \mathrm{LT}_\sigma(t(g_1, \ldots, g_s))\,\mathrm{LT}_\sigma(g)$ is not contained in $\mathrm{Supp}(gf_2)$. Therefore we have $gf_1 \xrightarrow{G}_{\mathrm{ss}} gf_2$.

It remains to show g). If $f \xleftrightarrow{G}_{\mathrm{s}} 0$, we collect the elements $c_i t_i(g_1, \ldots, g_s)$ used in the various subalgebra reduction steps and obtain a representation $f = \sum_i \pm c_i t_i(g_1, \ldots, g_s) \in K[G]$. Conversely, given a polynomial $f \in P$ with such a representation, it suffices by e) to prove $t_i(g_1, \ldots, g_s) \xleftrightarrow{G}_{\mathrm{s}} 0$, and this follows from $g_j \xleftrightarrow{G}_{\mathrm{s}} 0$ and f). □

Now we are ready to imitate Proposition 2.2.5 and characterize SAGBI bases by the confluence of their associated subalgebra rewrite relation.

Proposition 6.6.18. *Let $G \subseteq P \setminus \{0\}$ and $S = K[G]$. The following conditions are equivalent.*

C_1) For an element $f \in P$, we have $f \xrightarrow{G}_{\mathrm{s}} 0$ if and only if $f \in S$.

C_2) If $f \in S$ is irreducible with respect to $\xrightarrow{G}_{\mathrm{s}}$ then we have $f = 0$.

C_3) For every element $f_1 \in P$, there is a unique element $f_2 \in P$ for which $f_1 \xrightarrow{G}_{\mathrm{s}} f_2$ and f_2 is irreducible with respect to $\xrightarrow{G}_{\mathrm{s}}$.

C_4) The subalgebra rewrite relation $\xrightarrow{G}_{\mathrm{s}}$ is confluent.

Proof. In the light of Proposition 6.6.17, the proof is the same as the proof of Proposition 2.2.5. □

Again we postpone the task of showing that the conditions in this proposition actually characterize SAGBI bases and content ourselves with pointing out that they are not satisfied by every set of generators G.

Example 6.6.19. In the setting of Example 6.6.15, we have already seen that $x^2 \in S$. Let $G = \{g_1, g_2, g_3\}$. Condition C_2) is not satisfied since x^2 is irreducible with respect to $\xrightarrow{G}_{\mathrm{s}}$.

Here we can also construct an explicit counterexample to confluence. Since $x^8 - g_2^2 = 0$, we have $x^8 \xrightarrow{G}_{\mathrm{s}} 0$. On the other hand, since $x^8 - g_1 g_3 = x^6 + x^3 - x$ and $x^6 + x^3 - x - g_1^2 = 2x^4 + x^3 - x^2 - x$ and $2x^4 + x^3 - x^2 - x - 2g_2 = x^3 - x^2 - x$ and $x^3 - x^2 - x - g_1 = -x^2$, we have $x^8 \xrightarrow{G}_{\mathrm{s}} -x^2$. Now the element $-x^2$ is irreducible with respect to $\xrightarrow{G}_{\mathrm{s}}$. Therefore the subalgebra rewrite relation $\xrightarrow{G}_{\mathrm{s}}$ is not confluent.

At this point our plan to produce SAGBI versions of everything in Chapter 2 hits a serious obstacle. How should we formulate the lifting of syzygies? What are "syzygies" in the subalgebra world? The solution is an old friend from Section 3.6 who deserves an official name.

Definition 6.6.20. Let $g_1, \ldots, g_s \in P$ and $\mathcal{G} = (g_1, \ldots, g_s)$. Then the ideal $\{h \in K[y_1, \ldots, y_s] \mid h(g_1, \ldots, g_s) = 0\}$ is called the **ideal of algebraic relations** of $\mathcal{G}$ and is denoted by $\mathrm{Rel}(\mathcal{G})$ or by $\mathrm{Rel}(g_1, \ldots, g_s)$.

In the following we let $P' = K[y_1, \ldots, y_s]$. The ideal of algebraic relations of $\mathcal{G}$ is the kernel of the K-algebra homomorphism $\lambda : P' \longrightarrow P$ given by $y_i \mapsto g_i$ for $i = 1, \ldots, s$. It can be computed using implicitization (see Corollary 3.6.3). Next we want to construct a subalgebra version of the fundamental diagram and show some properties analogous to the ones in Proposition 2.3.6.

Definition 6.6.21. Let $\mathcal{G} = (g_1, \ldots, g_s) \in P^s$ be a tuple of non-zero polynomials, and let σ be a term ordering on $\mathbb{T}^n$.

a) We equip the polynomial ring $P' = K[y_1, \ldots, y_s]$ with the $\mathbb{T}^n$-grading given by $\deg_{\sigma,\mathcal{G}}(y_i) = \mathrm{LT}_\sigma(g_i)$ for $i = 1, \ldots, s$ and $\deg_{\sigma,\mathcal{G}}(1) = 1$. This is called the **induced grading** or the grading **induced by** $(\sigma, \mathcal{G})$.

b) For every polynomial $f \in P' \setminus \{0\}$, we define its σ**-degree** by

$$\deg_{\sigma,\mathcal{G}}(f) = \max_\sigma \{\deg_{\sigma,\mathcal{G}}(t) \mid t \in \mathrm{Supp}(f)\}$$

c) For every polynomial $f \in P' \setminus \{0\}$, we write $f = c_1 t_1 + \cdots + c_r t_r$ with $c_1, \ldots, c_r \in K \setminus \{0\}$ and pairwise distinct terms $t_1, \ldots, t_r \in \mathbb{T}(y_1, \ldots, y_s)$, and we let $d = \deg_{\sigma,\mathcal{G}}(f)$. Then we define the σ**-leading form** of f by

$$\mathrm{LF}_{\sigma,\mathcal{G}}(f) = \sum_{\{i \mid \deg_{\sigma,\mathcal{G}}(t_i) = d\}} c_i t_i$$

For $f = 0$, we let $\mathrm{LF}_{\sigma,\mathcal{G}}(f) = 0$.

The induced grading will play the role of the grading defined in Proposition 2.3.3. For a term $t \in \mathbb{T}(y_1, \ldots, y_s)$, the definition of the induced grading implies $\deg_{\sigma,\mathcal{G}}(t) = \mathrm{LT}_\sigma(t(g_1, \ldots, g_s))$. Taking σ-leading forms yields a map $\mathrm{LF}_{\sigma,\mathcal{G}} : P' \longrightarrow P'$. Moreover, we define a map $\mathrm{LM} : P \longrightarrow P$ which sends 0 to 0 and f to $\mathrm{LM}_\sigma(f)$ if $f \neq 0$. Last but not least we let $\Lambda : P' \longrightarrow P$ be the K-algebra homomorphism defined by $\Lambda(y_i) = \mathrm{LM}_\sigma(g_i)$ for $i = 1, \ldots, s$. In this way we get the following **fundamental SAGBI diagram**.

Proposition 6.6.22. *Let $S = K[g_1, \ldots, g_s]$ be the K-subalgebra of P generated by $\mathcal{G} = (g_1, \ldots, g_s) \in P^s$, let σ be a term ordering on $\mathbb{T}^n$, and let Ψ be the filtration on S induced by the σ-Gröbner filtration on P.*

a) We have a diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & & \mathrm{Rel}(\mathcal{G}) & \longrightarrow & P' & \xrightarrow{\lambda} & S & \longrightarrow & 0 \\ & & & & & \downarrow{\scriptstyle \mathrm{LF}} & & \downarrow{\scriptstyle \mathrm{LM}} & & \\ 0 & \longrightarrow & \mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G})) & & \longrightarrow & P' & \xrightarrow{\Lambda} & \mathrm{gr}_\Psi(S) & & \end{array}$$

b) For every $f \in P' \setminus \mathrm{Rel}(\mathcal{G})$ we have

1) $\mathrm{LT}_\sigma(\lambda(f)) \leq_\sigma \deg_{\sigma,\mathcal{G}}(f)$,
2) $\mathrm{LF}(f) \in \mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G}))$ if and only if $\mathrm{LT}_\sigma(\lambda(f)) <_\sigma \deg_{\sigma,\mathcal{G}}(f)$,
3) $\Lambda(\mathrm{LF}(f)) = \mathrm{LM}(\lambda(f))$ if and only if $\mathrm{LT}_\sigma(\lambda(f)) = \deg_{\sigma,\mathcal{G}}(f)$.

c) For every $f \in \mathrm{Rel}(\mathcal{G})$, we have $\mathrm{LF}(f) \in \mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G}))$. Therefore the map LF induces a map $\mathrm{LF}|_{\mathrm{Rel}(\mathcal{G})} : \mathrm{Rel}(\mathcal{G}) \longrightarrow \mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G}))$ which we denote by LF again.

Proof. To show a) it suffices to note that $\Lambda(f) = f(\mathrm{LM}_\sigma(g_1), \ldots, \mathrm{LM}_\sigma(g_s))$ is contained in $\mathrm{gr}_\Psi(S)$ for every $f \in P'$. Now we prove b). We write $f = c_1 t_1 + \cdots + c_r t_r$ with $c_1, \ldots, c_r \in K \setminus \{0\}$ and pairwise distinct terms $t_1, \ldots, t_r \in \mathbb{T}(y_1, \ldots, y_s)$. Then the first formula follows from

$$\begin{aligned} \mathrm{LT}_\sigma(\lambda(f)) &= \mathrm{LT}_\sigma(c_1 t_1(g_1, \ldots, g_s) + \cdots + c_r t_r(g_1, \ldots, g_s)) \\ &\leq \max_\sigma\{\mathrm{LT}_\sigma(t_1(g_1, \ldots, g_s)), \ldots, \mathrm{LT}_\sigma(t_r(g_1, \ldots, g_s))\} \\ &= \max_\sigma\{\deg_{\sigma,\mathcal{G}}(t_1), \ldots, \deg_{\sigma,\mathcal{G}}(t_r)\} = \deg_{\sigma,\mathcal{G}}(f) \end{aligned}$$

Next we prove the second claim in b). Without loss of generality there exists $1 \leq r' \leq r$ such that $\mathrm{LF}(f) = c_1 t_1 + \cdots + c_{r'} t_{r'}$. Then we have $\mathrm{LF}(f) \in \mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G}))$ if and only if $\sum_{i=1}^{r'} c_i(t_i(\mathrm{LM}_\sigma(g_1), \ldots, \mathrm{LM}_\sigma(g_s))) = 0$, i.e. if and only if $\sum_{i=1}^{r'} c_i \mathrm{LM}_\sigma(t_i(g_1, \ldots, g_s)) = 0$. If this holds true, we see that

$$\begin{aligned} \mathrm{LT}_\sigma(\lambda(f)) &= \mathrm{LT}_\sigma(c_1 t_1(g_1, \ldots, g_s) + \cdots + c_r t_r(g_1, \ldots, g_s)) \\ &<_\sigma \mathrm{LT}_\sigma(t_1(g_1, \ldots, g_s)) = \deg_{\sigma,\mathcal{G}}(f) \end{aligned}$$

Conversely, if $\sum_{i=1}^{r'} c_i \mathrm{LM}_\sigma(t_i(g_1, \ldots, g_s)) \neq 0$, a similar calculation shows that $\mathrm{LT}_\sigma(\lambda(f)) = \deg_{\sigma,\mathcal{G}}(f)$. For the proof of the third claim in b) we note

that $\mathrm{LT}_\sigma(\lambda(f)) \neq \deg_{\sigma,\mathcal{G}}(f)$ implies by 1) and 2) that we have $\Lambda(\mathrm{LF}(f)) = 0$. Since $\lambda(f) \neq 0$, we then get $\mathrm{LM}_\sigma(\lambda(f)) \neq 0 = \Lambda(\mathrm{LF}(f))$. Conversely, if $\mathrm{LT}_\sigma(\lambda(f)) = \deg_{\sigma,\mathcal{G}}(f)$, the claim follows from

$$\begin{aligned}
\mathrm{LM}_\sigma(\lambda(\ \ f\ \ )) &= \mathrm{LM}_\sigma(c_1 t_1(g_1,\dots,g_s) + \cdots + c_r t_r(g_1,\dots,g_s)) \\
&= \mathrm{LM}_\sigma(c_1 t_1(g_1,\dots,g_s)) + \cdots + c_{r'} t_{r'}(g_1,\dots,g_s)) \\
&= c_1 \,\mathrm{LM}_\sigma(t_1(g_1,\dots,g_s)) + \cdots + c_{r'} \,\mathrm{LM}_\sigma(t_{r'}(g_1,\dots,g_s)) \\
&= c_1 t_1(\mathrm{LM}_\sigma(g_1),\dots,\mathrm{LM}_\sigma(g_s)) + \cdots + c_{r'} t_{r'}(\mathrm{LM}_\sigma(g_1),\dots,\mathrm{LM}_\sigma(g_s)) \\
&= \Lambda(c_1 t_1 + \cdots + c_{r'} t_{r'}) = \Lambda(\mathrm{LF}(f))
\end{aligned}$$

Finally we show c). We write $f = c_1 t_1 + \cdots + c_r t_r$ as above and use $\lambda(f) = 0$ to get that the coefficient of $\deg_{\sigma,\mathcal{G}}(f)$ in $\sum_{i=1}^{r} c_i t_i(g_1,\dots,g_s)$ is zero. Hence we have $\Lambda(\mathrm{LF}(f)) = \Lambda(\sum_{i=1}^{r'} c_i t_i) = \sum_{i=1}^{r'} c_i \,\mathrm{LM}_\sigma(t_i(g_1,\dots,g_s)) = 0$. □

As in Section 2.3, we say that an polynomial $f \in P'$ is a **lifting** of $\bar{f} \in P'$ if we have $\mathrm{LF}(f) = \bar{f}$. Using the preceding proposition, we can prove the equivalence of the following conditions.

Proposition 6.6.23. *Let σ be a term ordering on $\mathbb{T}^n$, and let $\mathcal{G} \in P^s$. The following conditions are equivalent.*

D_1) *Every homogeneous element of* $\mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G}))$ *with respect to the induced grading has a lifting in* $\mathrm{Rel}(\mathcal{G})$.

D_2) *There exists a system of generators of* $\mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G}))$ *consisting of elements which are homogeneous with respect to the induced grading and have a lifting in* $\mathrm{Rel}(\mathcal{G})$.

D_3) *There exists a finite system of generators of* $\mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G}))$ *consisting of elements which are homogeneous with respect to the induced grading and have a lifting in* $\mathrm{Rel}(\mathcal{G})$.

Proof. It suffices to show the implication "$D_2) \Rightarrow D_1)$". Let E be a set, let $\{\bar{f}_i\}_{i\in E}$ be a homogeneous system of generators of $\mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G}))$, and let $f_i \in P'$ be a lifting of $\bar{f}_i$ for every $i \in E$. Given a homogeneous element $\bar{h} \in P'$, there exist $i_1,\dots,i_r \in E$ and $c_1,\dots,c_r \in K \setminus \{0\}$ and $t_1,\dots,t_r \in \mathbb{T}(y_1,\dots,y_s)$ such that $\bar{h} = \sum_{j=1}^{r} c_j t_j \bar{f}_{i_j}$. Clearly, we may assume that $\deg_{\sigma,\mathcal{G}}(t_j \bar{f}_{i_j}) = \deg_{\sigma,\mathcal{G}}(\bar{h})$ for $j = 1,\dots,r$. Now we have $\mathrm{LF}(t_j f_{i_j}) = t_j \,\mathrm{LF}(f_{i_j}) = t_j \bar{f}_{i_j}$, and hence $\deg_{\sigma,\mathcal{G}}(t_j f_{i_j}) = \deg_{\sigma,\mathcal{G}}(\bar{h})$. This, in turn, implies $\mathrm{LF}(\sum_{j=1}^{r} c_j t_j f_{i_j}) = \sum_{j=1}^{r} c_j t_j \bar{f}_{i_j} = \bar{h}$, which concludes the proof. □

Our usual example shows that it is not always possible to lift all algebraic relations in $\mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G}))$.

Example 6.6.24. In the setting of Example 6.6.15, the ideal of algebraic relations $\mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G})) = \mathrm{Rel}(x^3, x^4, x^5)$ contains the polynomial $y_1 y_3 - y_2^2$. This polynomial is homogeneous with respect to the induced grading because

$\deg_{\sigma,\mathcal{G}}(y_1y_3) = x^8 = \deg_{\sigma,\mathcal{G}}(y_2^2)$. Since $\lambda(y_1y_3 - y_2^2) = -x^6 - x^3 + x$, the element $y_1y_3 - y_2^2$ is not contained in $\mathrm{Rel}(\mathcal{G})$.

Furthermore, any lifting of $y_1y_3 - y_2^2$ would have to be of the form $f = y_1y_3 - y_2^2 + c_0 + c_1y_1 + c_2y_2 + c_3y_3 + c_4y_1^2 + c_5y_1y_2$ with $c_0, \ldots, c_5 \in K$. Setting $\lambda(f) = 0$ yields $c_5 = 0$, $c_4 = 1$, $c_3 = 0$, $c_2 = 2$, $c_1 = 1$, and $c_0 = 0$. But then $\lambda(y_1y_3 - y_2^2 + y_1 + 2y_2 + y_1^2) = x^2$ shows that the resulting polynomial f is still not contained in $\mathrm{Rel}(\mathcal{G})$, and therefore $y_1y_3 - y_2^2$ has no lifting.

Finally we have all the conditions we want and we are ready to enunciate the fundamental result of this subsection.

Theorem 6.6.25. (Characterization of SAGBI Bases)
Let σ be a term ordering on $\mathbb{T}^n$, let $S = K[G]$ be the K-subalgebra of P generated by a set of polynomials $G \subseteq P \setminus \{0\}$, let $\xrightarrow{G}_{\mathrm{s}}$ be the subalgebra rewrite relation defined by G, and let Ψ be the filtration on S induced by the σ-Gröbner filtration on P. Then the following conditions are equivalent.

A_1) *For each $f \in S\setminus\{0\}$, there are $g_1, \ldots, g_s \in G$ and $h \in K[y_1, \ldots, y_s]$ with $f = h(g_1, \ldots, g_s)$ and $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(t(g_1, \ldots, g_s))$ for all $t \in \mathrm{Supp}(h)$.*

A_2) *For each $f \in S\setminus\{0\}$, there are $g_1, \ldots, g_s \in G$ and $h \in K[y_1, \ldots, y_s]$ with $f = h(g_1, \ldots, g_s)$ and $\mathrm{LT}_\sigma(f) = \max_\sigma\{\mathrm{LT}_\sigma(t(g_1, \ldots, g_s)) \mid t \in \mathrm{Supp}(h)\}$.*

B_1) *The set G is a σ-SAGBI basis of S. By definition, this means that we have $\mathrm{gr}_\Psi(S) = K[\mathrm{LT}_\sigma(G)]$.*

B_2) *The monoid $\{\mathrm{LT}_\sigma(f) \mid f \in S \setminus \{0\}\}$ is generated by $\{\mathrm{LT}_\sigma(g) \mid g \in G\}$.*

C_1) *For an element $f \in P$, we have $f \xrightarrow{G}_{\mathrm{s}} 0$ if and only if $f \in S$.*

C_2) *If $f \in S$ is irreducible with respect to $\xrightarrow{G}_{\mathrm{s}}$ then we have $f = 0$.*

C_3) *For every element $f_1 \in P$, there is a unique element $f_2 \in P$ for which $f_1 \xrightarrow{G}_{\mathrm{s}} f_2$ and f_2 is irreducible with respect to $\xrightarrow{G}_{\mathrm{s}}$.*

C_4) *The subalgebra rewrite relation $\xrightarrow{G}_{\mathrm{s}}$ is confluent.*

D_1) *For every tuple $\mathcal{G} = (g_1, \ldots, g_s)$ of elements of G, every homogeneous element of $\mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G}))$ has a lifting in $\mathrm{Rel}(\mathcal{G})$.*

D_2) *For every tuple $\mathcal{G} = (g_1, \ldots, g_s)$ of elements of G, there exists a homogeneous system of generators of $\mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G}))$ consisting entirely of elements which have a lifting in $\mathrm{Rel}(\mathcal{G})$.*

D_3) *For every tuple $\mathcal{G} = (g_1, \ldots, g_s)$ of elements of G, there exists a finite homogeneous system of generators of $\mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G}))$ consisting entirely of elements which have a lifting in $\mathrm{Rel}(\mathcal{G})$.*

Proof. By Corollary 6.6.5.c and Propositions 6.6.14, 6.6.18, and 6.6.23, the conditions in each block are equivalent. To show that B_2) implies A_1), we argue as in the proof of Proposition 2.1.3. The only changes are that $\mathrm{LT}_\sigma(f)$ is of the form $t(\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s))$ for some elements $g_1, \ldots, g_s \in G$ and some term $t \in K[y_1, \ldots, y_s]$, and that we use $f - \frac{\mathrm{LC}_\sigma(f)}{\mathrm{LC}_\sigma(t(g_1,\ldots,g_s))}\, t(g_1, \ldots, g_s)$ to get the desired contradiction.

To prove "$A_2) \Rightarrow C_2)$" by contradiction, we suppose that there is an element $f \in S \setminus \{0\}$ which is irreducible with respect to $\xrightarrow{G}_{\mathrm{s}}$. By $A_2)$, there exists a representation $f = h(g_1, \ldots, g_s)$ with $g_1, \ldots, g_s \in G$ and with $h \in K[y_1, \ldots, y_s]$ having $\mathrm{LT}_\sigma(f) = \max_\sigma\{\mathrm{LT}_\sigma(t(g_1, \ldots, g_s)) \mid t \in \mathrm{Supp}(h)\}$. Let $t \in \mathrm{Supp}(h)$ be the term for which this maximum is achieved. Then the element $f' = f - \frac{\mathrm{LC}_\sigma(f)}{\mathrm{LC}_\sigma(t(g_1,\ldots,g_s))}\, t(g_1, \ldots, g_s)$ satisfies $f \xrightarrow{G}_{\mathrm{s}} f'$ and $f' \neq f$, a contradiction.

Since the implication "$C_1) \Rightarrow A_2)$" follows by collecting the elements of S used in the reduction steps $f \xrightarrow{G}_{\mathrm{s}} 0$, we show "$A_2) \Rightarrow D_1)$" next. Let $\mathcal{G} = (g_1, \ldots, g_s) \in G^s$, and let $f \in \mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G})) \setminus \{0\}$ be homogeneous with respect to the induced grading. We may suppose that $\lambda(f) \neq 0$, since otherwise f would be a lifting of itself. Using $A_2)$, we get a representation $\lambda(f) = h(g_1, \ldots, g_s)$ with $g_1, \ldots, g_s \in G$ and $h \in K[y_1, \ldots, y_s]$ such that $\mathrm{LT}_\sigma(\lambda(f)) = \max_\sigma\{\mathrm{LT}_\sigma(t(g_1, \ldots, g_s)) \mid t \in \mathrm{Supp}(h)\}$. It follows that we have $f - h \in \mathrm{Ker}(\lambda) = \mathrm{Rel}(\mathcal{G})$ and $\mathrm{LT}_\sigma(\lambda(f)) = \mathrm{LT}_\sigma(\lambda(h)) = \deg_{\sigma,\mathcal{G}}(h)$. Since $\mathrm{LF}(f) = f$ and $\Lambda(\mathrm{LF}(f)) = 0$, Proposition 6.6.22.b2 yields the inequality $\mathrm{LT}_\sigma(\lambda(f)) <_\sigma \deg_{\sigma,\mathcal{G}}(f)$. Altogether, we get $\deg_{\sigma,\mathcal{G}}(f) >_\sigma \deg_{\sigma,\mathcal{G}}(h)$ and $\mathrm{LF}(f - h) = \mathrm{LF}(f) = f$, i.e. $f - h$ is a lifting of f.

Now we prove the implication "$D_1) \Rightarrow A_2)$". For a contradiction, assume that some $f \in S \setminus \{0\}$ cannot be represented as in $A_2)$. We write $f = h(g_1, \ldots, g_s)$ with $g_1, \ldots, g_s \in G$ and $h \in K[y_1, \ldots, y_s]$. Let this representation be chosen such that $\deg_{\sigma,\mathcal{G}}(h)$ is minimal. We cannot have $\deg_{\sigma,\mathcal{G}}(h) = \mathrm{LT}_\sigma(f)$ because otherwise the representation satisfies $A_2)$. Hence Proposition 6.6.22.b1 shows that $\mathrm{LT}_\sigma(f) <_\sigma \deg_{\sigma,\mathcal{G}}(h)$. Then Proposition 6.6.22.b2 yields $\mathrm{LF}(h) \in \mathrm{Rel}(\mathrm{LM}_\sigma(\mathcal{G}))$. By $D_1)$, there exists an element $h' \in \mathrm{Rel}(\mathcal{G})$ with $\mathrm{LF}(h') = \mathrm{LF}(h)$. In particular, this means that $\deg_{\sigma,\mathcal{G}}(h - h') <_\sigma \deg_{\sigma,\mathcal{G}}(h)$ and $\lambda(h - h') = \lambda(h) = f$ which contradicts the minimality of $\deg_{\sigma,\mathcal{G}}(h)$.

Finally we observe that $A_2)$ implies $B_1)$ because for every representation $f = h(g_1, \ldots, g_s)$ there exists a term $t \in \mathrm{Supp}(h)$ such that $\mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(t(g_1, \ldots, g_s)) = t(\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)) \in K[\mathrm{LT}_\sigma(G)]$. □

Notice that we have been very careful in this theorem not to assume finiteness of G. In fact, if we wanted to continue to imitate Chapter 2 we would have to prove the existence of finite σ-SAGBI bases which is impossible given Examples 6.6.7 and 6.6.8. On the other hand, it is possible to continue the imitation and speak of normal forms, a subalgebra membership test and reduced SAGBI bases — this is done in Tutorial 96.

It's kind of fun
to do the impossible.
(Walt Disney)

6.6.C Computation of SAGBI Bases

A strategic turmoil may renew stalled negotiation.
(Moss Sweedler)

At this point we are ready to discuss the algorithmic aspects of SAGBI basis theory. The first question is: are there meaningful algorithms at all? Indeed, we have seen that in certain cases no finite SAGBI basis exists. On the other hand, we have also seen that for some particular subalgebras finite SAGBI bases do exist, and we would like to compute them. Moreover, if we start with a graded subalgebra of P, it is reasonable to expect that finite truncated SAGBI bases always exist, and if this is the case we would like to compute them, too, independent of whether the overall SAGBI basis is finite or not.

In computer science there is a specific notion which generalizes that of an algorithm, namely the notion of a **procedure**. A procedure is a sequence of instructions having the look and feel of an algorithm, except that finiteness is not guaranteed. In fact, for computing SAGBI bases, there exists something slightly better: an **enumerating procedure**. This means that, if a finite result exists, it is found after finitely many steps, and if the result is infinite, it is the union of all elements computed at some point by the procedure. The goal of this subsection is to show that an enumerating procedure for computing SAGBI bases does indeed exist. Furthermore, in Tutorial 96 we shall see that this procedure also computes truncated SAGBI bases in the homogeneous case.

As usual, we let K be a field and $P = K[x_1, \ldots, x_n]$. Moreover, we fix a term ordering σ on $\mathbb{T}^n$. In the following we frequently use the assumption that certain given polynomials are monic. This is clearly no serious restriction and it will help us keep the description lighter. We need two tools for constructing a SAGBI basis procedure. The first tool is a SAGBI version of Definition 2.5.1. For terms $t_1, \ldots, t_s \in \mathbb{T}^n$, Definitions 6.1.1 and 6.6.20 imply that the ideal $\mathrm{Rel}(t_1, \ldots, t_s)$ is the toric ideal associated to the tuple $(t_1, \ldots, t_s)$. By Proposition 6.1.3.c, toric ideals are generated by pure binomials.

Definition 6.6.26. Let $g_1, \ldots, g_s \in P \setminus \{0\}$ be monic polynomials, and let $b = t_1 - t_2$ be a pure binomial in $\mathrm{Rel}(\mathrm{LT}_\sigma(\mathcal{G}))$, where $t_1, t_2 \in \mathbb{T}(y_1, \ldots, y_s)$. Then the polynomial $b(g_1, \ldots, g_s) \in P$ is called the **T-polynomial** of b.

T-polynomials will be for the computation of SAGBI bases what S-polynomials are for the computation of Gröbner bases. The letter "T" reminds us of the "toric origin" of these polynomials and also of the fact that the pair $(\log(t_1), \log(t_2))$ was called a *tête à tête* in the pioneering paper [RS90]. If a T-polynomial reduces to zero, the corresponding pure binomial can be lifted as follows.

Proposition 6.6.27. *Let $G \subseteq P \setminus \{0\}$ be a set of monic polynomials, let $\mathcal{G} = (g_1, \ldots, g_s) \in G^s$, and let $b = t_1 - t_2 \in \mathrm{Rel}(\mathrm{LT}_\sigma(\mathcal{G}))$ be a pure binomial. If we have $b(g_1, \ldots, g_s) \xrightarrow{G}_{\mathrm{s}} 0$ then b has a lifting in $\mathrm{Rel}(\mathcal{G})$.*

Proof. If $b(g_1, \ldots, g_s) = 0$ then b is a lifting of itself. Thus we may assume $b(g_1, \ldots, g_s) \neq 0$. By collecting the terms used in the reduction steps of $b(g_1, \ldots, g_s) \xrightarrow{G}_{\mathrm{s}} 0$, we obtain a representation $b(g_1, \ldots, g_s) = h(g_1, \ldots, g_s)$ with $h \in K[y_1, \ldots, y_s]$ which satisfies condition A_2). Since b is homogeneous with respect to the induced grading, we see that $\Lambda(\mathrm{LF}(h)) = \Lambda(h) = 0$, and Proposition 6.6.22.b2 yields $\deg_{\sigma,\mathcal{G}}(b) >_\sigma \mathrm{LT}_\sigma(h(g_1, \ldots, g_s)) = \deg_{\sigma,\mathcal{G}}(h)$. Therefore the polynomial $p = b - h \in \mathrm{Rel}(\mathcal{G})$ satisfies $\mathrm{LF}(p) = b$, i.e. it is a lifting of b. □

The second tool is the SAGBI variant of the Buchberger Criterion 2.5.3.

Proposition 6.6.28. (The SAGBI Basis Criterion)
Let $G \subseteq P \setminus \{0\}$ be a set of monic polynomials, let $S = K[G]$, and let Ψ be the filtration on S induced by the σ-Gröbner filtration on P. Then the following conditions are equivalent.

a) The set G is a σ-SAGBI basis of S.
b) For every tuple $\mathcal{G} = (g_1, \ldots, g_s)$ of elements of G, there exists a set B of pure binomials in $K[y_1, \ldots, y_s]$ which generates the ideal $\mathrm{Rel}(\mathrm{LT}_\sigma(\mathcal{G}))$ and which satisfies $b(g_1, \ldots, g_s) \xrightarrow{G}_{\mathrm{s}} 0$ for all $b \in B$.

Proof. First we show that a) implies b). If G is a σ-SAGBI basis of S then $b(g_1, \ldots, g_s) \xrightarrow{G}_{\mathrm{s}} 0$ holds for every pure binomial $b \in \mathrm{Rel}(\mathrm{LT}_\sigma(\mathcal{G}))$ by Theorem 6.6.25. Conversely, if b) holds then Proposition 6.6.27 shows that every $b \in B$ has a lifting in $\mathrm{Rel}(\mathcal{G})$. Thus condition D_3) of Theorem 6.6.25 holds. □

Having gathered the necessary tools, we are well equipped to elaborate the promised enumerating procedure for SAGBI bases. Since we need a finite set of input data, we assume that the subalgebra whose SAGBI basis we want to compute is finitely generated.

Theorem 6.6.29. (The SAGBI Basis Procedure)
Let σ be a term ordering on $\mathbb{T}^n$, let $G = \{g_1, \ldots, g_s\} \subseteq P \setminus \{0\}$ be a set of monic polynomials, let $\mathcal{G} = (g_1, \ldots, g_s)$, and let $S = K[G]$ be the K-subalgebra of P generated by G. Consider the following sequence of instructions.

1) Let $s' = s$, let $H = G$, and let $\mathcal{H} = \mathcal{G}$.
2) Using Proposition 6.1.3 or Corollary 6.1.10, compute a set B of pure binomials which generates the ideal $\mathrm{Rel}(\mathrm{LT}_\sigma(\mathcal{H}))$ in $K[y_1, \ldots, y_{s'}]$.
3) If $B = \emptyset$, return the tuple $\mathcal{H}$ and stop. Otherwise, let $B' = \emptyset$.

4) For every $b \in B$, reduce the T-polynomial $b(g_1, \ldots, g_{s'})$ via $\xrightarrow{H}_{\mathrm{s}}$ until an irreducible element $b' \in P$ is found, and if $b' \neq 0$, adjoin the element $\mathrm{LC}_\sigma(b')^{-1}\, b'$ to the set B'.

5) If $B' = \emptyset$ then return the tuple $\mathcal{H}$ and stop. Otherwise, let $t = \#B'$, increase s' by t, and append the elements $g_{s'-t+1}, \ldots, g_{s'}$ of B' to H and $\mathcal{H}$.

6) Using Proposition 6.1.3 or Corollary 6.1.10, compute a set B of pure binomials which generate the ideal $\mathrm{Rel}(\mathrm{LT}_\sigma(\mathcal{H}))$ in $K[y_1, \ldots, y_{s'}]$. Replace B by its subset consisting of those elements which involve at least one of the indeterminates $y_{s'-t+1}, \ldots, y_{s'}$. Then continue with step 3).

This is an enumerating procedure. The set of all elements contained in H at some point is a σ-SAGBI basis of S. The procedure stops if and only if S has a finite σ-SAGBI basis. In this case it returns a tuple $\mathcal{H}$ of polynomials which form a σ-SAGBI basis of S.

Proof. First we show that the set $\overline{H}$ of elements contained in H at some point during the course of the procedure is a σ-SAGBI basis of S. If the procedure stops in step 3), we have $\mathrm{Rel}(\mathrm{LT}_\sigma(\mathcal{G})) = 0$. Hence the leading terms $\{\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\}$ are algebraically independent and $\mathcal{H} = (g_1, \ldots, g_s)$ is a σ-SAGBI basis of S by Proposition 6.6.11.

Otherwise, we use the SAGBI Basis Criterion 6.6.28. Let $\{g_1, \ldots, g_{s'}\}$ be a finite subset of $\overline{H}$. By possibly enlarging it we may assume that we have $\mathcal{H} = (g_1, \ldots, g_{s'})$ after some execution of step 5) is completed. Let B be the system of generators of $\mathrm{Rel}(\mathrm{LT}_\sigma(\mathcal{H}))$ consisting of pure binomials which is the result of the first part of step 6). We write B as a disjoint union of B_1 and B_2 where B_2 are the elements selected in the second part of step 6). For $b \in B_1$, the polynomial $b' \in P$ has been computed in an earlier execution of step 4). We either found $b' = 0$ or $b' \neq 0$ has already been appended to H. In both cases it follows that we have $b(g_1, \ldots, g_s) \xrightarrow{H}_{\mathrm{s}} 0$. For $b \in B_2$, the polynomial $b' \in P$ will be computed in the next execution of step 4). Either we find $b' = 0$ or b' will be appended to H in the next execution of step 5). In both cases it follows that we have $b(g_1, \ldots, g_s) \xrightarrow{H}_{\mathrm{s}} 0$ using the set H after the next execution of step 5). Altogether, we have $b(g_1, \ldots, g_s) \xrightarrow{\overline{H}}_{\mathrm{s}} 0$ for all $b \in B$, as we had to show.

If the procedure stops, this argument proves that the returned tuple $\mathcal{H}$ is a finite σ-SAGBI basis of S. Now suppose that S has a finite σ-SAGBI basis. Since $\overline{H}$ is a σ-SAGBI basis of S, Proposition 6.6.4 implies that the generating set $\{\mathrm{LT}_\sigma(h) \mid h \in \overline{H}\}$ of $\mathrm{gr}_\Psi(S) = K[\mathrm{LT}_\sigma(g) \mid g \in S \setminus \{0\}]$ contains the minimal monomial set of algebra generators, and that the latter set is finite. So, after performing step 5) finitely many times, we have a set H for which $\{\mathrm{LT}_\sigma(h) \mid h \in H\}$ contains the minimal monomial set of algebra generators. Therefore this set H is a σ-SAGBI basis of S. By Proposition 6.6.28, we will therefore get $B' = \emptyset$ in the next execution of

step 5) and the procedure stops. Thus we have now proved all claims of the theorem. □

The SAGBI basis procedure is full of "sagbities". To appreciate some of them, have a look at the following example.

Example 6.6.30. (The Tricky Example)
Let $P = \mathbb{Q}[x_1, x_2]$, let $\sigma = \texttt{DegLex}$, and let $S \subseteq P$ be the $\mathbb{Q}$-subalgebra generated by $G = \{g_1, g_2, g_3, g_4\}$ where $g_1 = x_1^2 x_2$, $g_2 = x_1^2 - x_2^2$, $g_3 = x_1^2 x_2^2 - x_2^4$, and $g_4 = x_1^2 x_2^4$. Let us follows the steps of the SAGBI basis procedure.

1) Let $s' = 4$, $H = \{g_1, g_2, g_3, g_4\}$, and $\mathcal{H} = (g_1, g_2, g_3, g_4)$.
2) We compute $B = \{y_3^2 - y_2 y_4,\ y_2 y_3 - y_1^2\}$.
4) For $b_1 = y_3^2 - y_2 y_4$ we compute $b_1(g_1, g_2, g_3, g_4) \xrightarrow{H}_{\mathrm{s}} -x_1^2 x_2^6 + x_2^8 = b_1'$. For $b_2 = y_2 y_3 - y_1^2$ we compute $b_2(g_1, g_2, g_3, g_4) \xrightarrow{H}_{\mathrm{s}} x_2^6 = b_2'$.
5) Let $t = 2$, $s' = 6$, $g_5 = -b_1'$, $g_6 = b_2'$, $H = \{g_1, \ldots, g_6\}$, and $\mathcal{H} = (g_1, \ldots, g_6)$.
6) We compute $\mathrm{Rel}(\mathrm{LT}_\sigma(\mathcal{H}))$ and get the set $B = \{y_2 y_6 - y_5,\ y_2^2 y_6 - y_3 y_4,\ y_1^2 y_6 - y_4^2\}$ of elements involving y_5, y_6.
4) For $b_3 = y_2 y_6 - y_5$ we compute $b_3(g_1, \ldots, g_6) = 2g_5 \xrightarrow{H}_{\mathrm{s}} 0$. For $b_4 = y_2^2 y_6 - y_3 y_4$ we compute $b_4(g_1, \ldots, g_6) = -g_3 g_6 \xrightarrow{H}_{\mathrm{s}} 0$. For $b_5 = y_1^2 y_6 - y_4^2$ we compute $b_5(g_1, \ldots, g_6) = 0$.
5) Since $B' = \emptyset$, the procedure returns $\mathcal{H} = (g_1, \ldots, g_6)$ and stops.

The upshot of this computation is that S has a finite σ-SAGBI basis, namely $G \cup \{x_1^2 x_2^6 - x_2^8,\ x_2^6\}$.

So, what is so tricky about this example? Suppose you want to modify the procedure described in Theorem 6.6.29 and make it more similar to Buchberger's Algorithm 2.5.5. You might be tempted to modify steps 4) and 5) so that every time a new element $b' \neq 0$ is found, it is appended to H and $\mathcal{H}$ and the new set B is computed. The tricky aspect of our example is that this modified approach *does not work!*

Let us examine what happens. After we compute $b_1' = -x_1^2 x_2^6 + x_2^8$, we append $g_5 = -b_1'$ to H and $\mathcal{H}$ and compute the set of new pure binomials $B = \{y_4^2 - y_3 y_5,\ y_3 y_4 - y_2 y_5\}$. In the next round we start with $b_2 = y_4^2 - y_3 y_5$ and compute $b_2' = 2x_1^2 x_2^{10} - x_2^{12}$. The modified procedure continues in this way appending elements to H and $\mathcal{H}$ indefinitely. The reason is that the elements g_2, g_3, g_4 generate a subalgebra $S' \subseteq P$ which is isomorphic to the one in Example 6.6.8 which does not have a finite σ-SAGBI basis. In every even degree $d \geq 2$, the associated graded ring $\mathrm{gr}_{\Psi'}(S')$ has the K-basis $\{x_1^d,\ x_1^{d-2} x_2^2, \ldots, x_1^2 x_2^{d-2}\}$. No new element appended to H and $\mathcal{H}$ by the procedure can benefit for the possibility to reduce it using g_1. Therefore the procedure *does not terminate!*

With the help of the SAGBI basis procedure, we can also compute the SAGBI basis mentioned in Example 6.6.10.

Example 6.6.31. Let $P = K[x]$, let $\sigma = \mathtt{Deg}$, and let $S \subseteq P$ be the K-subalgebra generated by $g_1 = x^3 - x$, $g_2 = x^4$, and $g_3 = x^5 - 1$. Let us follow the steps of the SAGBI basis procedure.

1) Let $s' = 3$, $H = \{g_1, g_2, g_3\}$ and $\mathcal{H} = (g_1, g_2, g_3)$.
2) We compute $B = \{y_2^2 - y_1y_3,\ y_1^2y_2 - y_3^2,\ y_1^3 - y_2y_3\}$.
4) For $b_1 = y_2^2 - y_1y_3$ we compute $b_1(g_1, g_2, g_3) \xrightarrow{H}_{\mathrm{s}} -x^2 = b_1'$. For $b_2 = g_1^2g_2 - g_3^2$ we compute $b_2(g_1, g_2, g_3) \xrightarrow{H}_{\mathrm{s}} -x^2 + 1 = b_2'$. For $b_3 = y_1^3 - y_2y_3$ we compute $b_3(g_1, g_2, g_3) \xrightarrow{H}_{\mathrm{s}} -x = b_3'$.
5) Let $t = 3$, $s' = 6$, $g_4 = -b_1'$, $g_5 = -b_2'$, $g_6 = -b_3'$, $H = \{g_1, \ldots, g_6\}$ and $\mathcal{H} = (g_1, \ldots, g_6)$.
6) We compute $\mathrm{Rel}(\mathrm{LT}_\sigma(\mathcal{H}))$ and get the set $B = \{y_5 - y_4,\ y_6^2 - y_4,\ y_4y_6 - y_1,\ y_4^2 - y_2,\ y_1y_4 - y_3\}$ of elements involving y_4, y_5, y_6.
4) For $b_4 = y_5 - y_4$ we compute $b_4(g_1, \ldots, g_6) \xrightarrow{H}_{\mathrm{s}} 0$. For $b_5 = y_6^2 - y_4$ we compute $b_5(g_1, \ldots, g_6) = 0$. For $b_6 = y_4y_6 - y_1$ we compute $b_6(g_1, \ldots, g_6) \xrightarrow{H}_{\mathrm{s}} 0$. For $b_7 = y_4^2 - y_2$ we compute $b_7(g_1, \ldots, g_6) = 0$. For $b_8 = y_1y_4 - y_3$ we compute $b_8(g_1, \ldots, g_6) \xrightarrow{H}_{\mathrm{s}} 0$.
5) Since $B' = \emptyset$, the procedure returns $\mathcal{H} = (g_1, \ldots, g_6)$ and stops.

By looking at the leading terms of the computed SAGBI basis, we immediately see that, in fact, the subset $\{g_6\} = \{x\}$ is a σ-SAGBI basis of S. Therefore we have *discovered* that $S = K[x]$, a result which we can *check* using the method explained in Example 6.6.10 and Corollary 3.6.7.

By adding the appropriate amount of bookkeeping to the SAGBI Basis Procedure, we could formulate a version which is analogous to the Extended Buchberger Algorithm 2.5.11, i.e. a version which also computes the subalgebra representations of the elements of $\mathcal{H}$ in terms of the original subalgebra generators. For instance, in the preceding example, it would compute the representation

$$x = -(x^3 - x)^3 + x^4(x^5 - 1) - 3(x^3 - x)x^4 + x^4 - (x^3 - x)$$

mentioned in Example 6.6.10.

Exercise 1. Let $S = K[x,\ xy - y^2,\ xy^2] \subseteq K[x, y]$ where K is a field of characteristic zero.

a) Let σ be a term ordering for which $x >_\sigma y$. Show that S does not have a finite σ-SAGBI basis.
b) Let σ be a term ordering for which $y >_\sigma x$. Show that S has a finite σ-SAGBI basis.

Exercise 2. Formulate and prove a subalgebra analog of the Division Algorithm 1.6.4.

Exercise 3. Formulate and prove a subalgebra analog of the Extended Buchberger Algorithm 2.5.11. Use this algorithm to verify the representation of x as an element of $K[x^3 - x,\, x^4,\, x^5 - 1]$ given above.

Exercise 4. Let K be a field. Show $x_3^2 \in K[x_1^2 - x_3,\, x_1x_2 + x_3,\, x_2^2 - x_3]$ in two ways: using the Subalgebra Membership Test 3.6.7 and using an extended version of the SAGBI Basis Procedure 6.6.29.

Exercise 5. Let K be a field, let $P = K[x_{11}, \ldots, x_{14}, x_{21}, \ldots, x_{24}]$, and let $S \subseteq P$ be the K-subalgebra generated by the 2×2-minors of the matrix $\left(\begin{smallmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \end{smallmatrix}\right)$. Show that the six minors are a `DegLex`-SAGBI basis of S where we let $x_{11} > x_{12} > \cdots > x_{24}$.

Exercise 6. Let K be a field, let $P = K[x_{ij} \mid 1 \leq i, j \leq 3]$, and let $S \subseteq P$ be the K-subalgebra generated by the 2×2-minors of the matrix $(x_{ij}) \in \mathrm{Mat}_3(P)$. Find a SAGBI basis of this algebra with respect to the lexicographic term ordering σ induced by the ordering $x_{ij} >_\sigma x_{k\ell} \iff (i,j) >_{\mathtt{Lex}} (k,\ell)$ on the indeterminates.

Exercise 7. Let K be a field, let $P = K[x]$, and let S be the set of all polynomials $f \in P$ with $f(1) = f(-1)$.

a) Prove that S is a K-subalgebra of P.
b) Show that S is finitely generated and isomorphic to the coordinate ring of a plane node, as described in Tutorial 95.d.
c) Give a "geometric interpretation" of this fact.

Exercise 8. (Gluing Points)
Let K be a field, let $P = K[x_1, \ldots, x_n]$, and let I be an ideal in P. We denote the set $\{c + f \mid c \in K,\, f \in I\}$ by $K + I$.

a) Show that $K + I$ is a K-subalgebra of P.
b) Consider the case where $P = K[x_1, x_2]$ and $I = (x_1)$. Prove that $K + I$ is not a finitely generated K-algebra.
c) Let $\mathbb{X} = \{p_1, \ldots, p_s\} \subseteq K^n$ be an affine point set. Prove that $K + \mathcal{I}(\mathbb{X})$ is a finitely generated K-algebra.
d) Show that the K-subalgebra $K + \mathcal{I}(\mathbb{X})$ of P considered above has a finite σ-SAGBI basis for every term ordering σ.
e) Compute a finite set of K-algebra generators of $K + \mathcal{I}(\mathbb{X})$ for the case $\mathbb{X} = \{(1,0), (-1,0)\}$. Can you explain the difference between this example and that of Exercise 7?

Exercise 9. Let K be a field, and let S be the subalgebra $K[x_1^2, x_1x_2, x_2^2]$ of $K[x_1, x_2]$. Find a set of generators of the S-module $\mathrm{Syz}_S(x_1x_2, x_2^2)$.

Exercise 10. Let K be a field, let $P = K[x_1, \ldots, x_n]$, let $S \subseteq P$ be a K-subalgebra, let σ be a term ordering on $\mathbb{T}^n$, and let Ψ be the filtration on S induced by the σ-Gröbner filtration on P. Prove that we have $\mathrm{gr}_\Psi(S) = P$ if and only if $S = P$.

Tutorial 96: Variations on the SAGBI Theme

Opera is ...
when a guy gets stabbed in the back
and instead of bleeding he sings.
(Edward Gardner)

This tutorial could serve as the starting point for several *magna opera* which elaborate on the idea of creating a subalgebra analog to Gröbner basis theory. Here we content ourselves with sketching some variations on this main theme. We hope that instead of bleeding you dry, they will inspire you to sing along. The libretto is available for free: just have a look at what we did with Gröbner bases in Chapters 2 and 4. Thus we shall perform the following variations: normal forms with respect to subalgebras, reduced SAGBI bases, homogeneous SAGBI bases, truncated SAGBI bases, and a Hilbert driven coda.

In the following let K be a field, let $P = K[x_1, \ldots, x_n]$ be a polynomial ring, let σ be a term ordering on $\mathbb{T}^n$, let $G = \{g_1, \ldots, g_s\} \subseteq P \setminus \{0\}$ be a set of monic polynomials, let $\xrightarrow{G}_{\mathrm{s}}$ be the subalgebra rewrite relation defined by G, and let $S = K[G]$ be the K-subalgebra of P generated by G.

First Variation: Normal Forms

Given a Gröbner basis of an ideal, the normal form of a polynomial with respect to the ideal is the normal remainder of this polynomial after division by the Gröbner basis, and it does not depend on the choice of the Gröbner basis. Our first topic is to construct subalgebra analogs of normal forms. In this variation we assume that $G \subseteq S \setminus \{0\}$ is a σ-SAGBI basis of S.

a) Show that for every $f \in P$ there exists a unique polynomial $f_G \in P$ with the properties that $f - f_G \in S$ and $\mathrm{Supp}(f_G) \cap K[\mathrm{LT}_\sigma(G)] = \emptyset$. *Hint:* Use Condition C_3) of Theorem 6.6.25.

The element f_G is called the **normal form** of f with respect to S. It is denoted by $\mathrm{NF}_{\sigma,S}(f)$, or simply by $\mathrm{NF}_S(f)$ if it is clear which term ordering we are considering.

c) Let $f, f_1, f_2 \in P$. Prove the following rules for normal forms.
   1) $\mathrm{NF}_S(\mathrm{NF}_S(f)) = \mathrm{NF}_S(f)$
   2) $\mathrm{NF}_S(f_1 - f_2) = \mathrm{NF}_S(f_1) - \mathrm{NF}_S(f_2)$
   3) $\mathrm{NF}_S(f_1 f_2) = \mathrm{NF}_S(\mathrm{NF}_S(f_1)\,\mathrm{NF}_S(f_2))$

d) Write a CoCoA function `NFS(...)` which takes f and G and computes the normal remainder $\mathrm{NF}_S(f)$. Apply this function to the following examples where $\sigma =$ `DegLex`.
   1) $f = x_1^4x_2^2 + x_1^2x_2^4$, $G = \{x_1^2 - 1, x_2^2 - 1\} \subseteq \mathbb{Q}[x_1, x_2]$
   2) $f = x_1^3 + x_1^2x_2$, $G = \{x_1 + x_2, x_1x_2\} \subseteq \mathbb{Q}[x_1, x_2]$
   3) $f = x_1^4 + x_1^3x_2 + x_1^2x_2^2 + x_2^4$, $G = \{x_1^2 - x_2^2, x_1^2x_2, x_1^2x_2^2 - x_2^4, x_1^2x_2^4, x_2^6, x_1^2x_2^6 - x_2^8\} \subseteq \mathbb{Q}[x_1, x_2]$

e) Show that a polynomial f satisfies $f \in S$ if and only if $\mathrm{NF}_S(f) = 0$. Thus the existence of a finite SAGBI basis of S yields an efficient subalgebra membership test.

Second Variation: Reduced SAGBI Bases

Let $G \subseteq S \setminus \{0\}$ be a σ-SAGBI basis of S. Imitating Definition 2.4.12, we say that G is a **reduced σ-SAGBI basis** of S if the following conditions are satisfied. (Recall that a σ-SAGBI basis is by definition monic.)

1) The set $\{\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\}$ is the minimal monomial system of algebra generators of $K[\mathrm{LT}_\sigma(G)]$.
2) For $i = 1, \ldots, s$, we have $\mathrm{Supp}(g_i - \mathrm{LT}_\sigma(g_i)) \cap K[\mathrm{LT}_\sigma(G)] = \emptyset$.

Now existence and uniqueness of reduced σ-SAGBI bases can be shown exactly as in Gröbner basis theory (see Theorem 2.4.13).

f) Prove that there exists a unique reduced σ-SAGBI basis of S.
g) Write a CoCoA function `ReducedSAGBI(...)` which takes G and computes the reduced σ-SAGBI basis of S.
h) Using your function `ReducedSAGBI(...)` and the `DegRevLex`-SAGBI basis $G = \{x_1x_2 - x_3^2, x_1^4 - x_2^2x_3^2\}$ of $S = \mathbb{Q}[G]$, show that the reduced `DegRevLex`-SAGBI basis of S is $\{x_2x_3 - x_3^2, x_1^4 - x_3^4\}$.

Third Variation: Homogeneous SAGBI Bases

For this variation, we equip P with the standard grading. We assume that G consists of monic homogeneous polynomials, but it is not necessarily a σ-SAGBI basis of $S = K[G]$.

i) **(The Homogeneous SAGBI Basis Procedure)**
Consider the following sequence of instructions.
   1) Let $B = \emptyset$, $W = G$, $H = \emptyset$, $\mathcal{H} = \emptyset$, and $s' = 0$.
   2) Let d be the smallest degree of an element in B or in W. Form the subset B_d of B, form the subset W_d of W, and delete their entries from B and W, respectively.
   3) Let $B' = \emptyset$. For every $b \in B_d$, reduce the T-polynomial $b(g_1, \ldots, g_{s'})$ via $\xrightarrow{H}_{\mathrm{s}}$ until an irreducible element $b' \in P$ is found, and if $b' \neq 0$, adjoin the element $\mathrm{LC}_\sigma(b')^{-1}b'$ to the set B'.
   4) If $B' \neq \emptyset$ then let $t = \#B'$, increase s' by t, and append the elements $g_{s'-t+1}, \ldots, g_{s'}$ of B' to H and $\mathcal{H}$.
   5) Let $W' = \emptyset$. For every $g \in W_d$, reduce g via $\xrightarrow{H}_{\mathrm{s}}$ until an irreducible element $g' \in P$ is found, and if $g' \neq 0$, adjoin the element $\mathrm{LC}_\sigma(g')^{-1}g'$ to the set W'.
   6) If $W' \neq \emptyset$ then let $t = \#W'$, increase s' by t, and append the elements $g_{s'-t+1}, \ldots, g_{s'}$ of W' to H and $\mathcal{H}$.

7) If $B' \neq \emptyset$ or $W' \neq \emptyset$, compute a set B of pure binomials which generate $\mathrm{Rel}(\mathrm{LT}_\sigma(\mathcal{H}))$ in $K[y_1, \ldots, y_{s'}]$. Replace B by its subset $B_{>d}$. (Here B is homogeneous with respect to the grading given by $\deg(y_i) = \deg(g_i)$.)
8) If $B = \emptyset$ and $W = \emptyset$, return the tuple $\mathcal{H}$ and stop. Otherwise, continue with step 2).

Show that this is an enumerating procedure. The set of all elements contained in H at some point is a homogeneous σ-SAGBI basis of S. The procedure stops if and only if S has a finite σ-SAGBI basis. In this case it returns a deg-ordered tuple $\mathcal{H}$ of polynomials which form a homogeneous σ-SAGBI basis of S.

j) Apply the Homogeneous SAGBI Basis Procedure to the Tricky Example 6.6.30. Compare its result to the result of the SAGBI Basis Procedure 6.6.29.

Fourth Variation: Truncated SAGBI Bases

Let P be standard graded and $G \subseteq S \setminus \{0\}$ be a homogeneous system of generators of $S = K[G]$. Since the Homogeneous SAGBI Basis Procedure proceeds degree by degree, we can interrupt its computations after a particular degree d is finished. In this way we construct SAGBI variants of truncated Gröbner bases. Formally, given a homogeneous σ-SAGBI basis H of S and a number $d \in \mathbb{N}$, we say that $H_{\leq d}$ is a **d-truncated σ-SAGBI basis** of S.

k) Write a CoCoA function `TruncSAGBI(...)` which takes G and d and computes a d-truncated σ-SAGBI basis of S.
l) Apply your function `TruncSAGBI(...)` to the following examples.
   1) $d = 3$, $G = \{x_1^2 - x_2x_3,\ x_1x_2 + x_3^2,\ x_2^2 - x_3^2\} \subseteq \mathbb{Q}[x_1, x_2, x_3]$
   2) $d = 5$, $G = \{x_1 + x_2,\ x_1x_2,\ x_1x_2^2\} \subseteq \mathbb{Q}[x_1, x_2]$
   3) $d = 6$, $G = \{x_1 - x_2,\ x_1x_2 - x_2^2,\ x_1x_2^2\} \subseteq \mathbb{Q}[x_1, x_2]$
m) Explain how one can use truncated SAGBI bases to devise an efficient **homogeneous subalgebra membership test** which works even if S has no finite SAGBI basis. Write a CoCoA function `IsInSubalg(...)` which implements this test and apply it to check whether $f \in K[G]$ holds in the following examples.
   1) $f = x_1x_2^4 - x_2^5$, $G = \{x_1 - x_2,\ x_1x_2 - x_2^2,\ x_1x_2^2\} \subseteq \mathbb{Q}[x_1, x_2]$
   2) $f = x_3^4$, $G = x_1^2 - x_3^2,\ x_1x_2 + x_3^2,\ x_2^2 - 2x_3^2\} \subseteq \mathbb{Q}[x_1, x_2, x_3]$
   3) $f = x_3^4$, $G = x_1^2 - x_3^2,\ x_1x_2 + x_3^2,\ x_2^2 - x_3^2\} \subseteq \mathbb{Q}[x_1, x_2, x_3]$

Give me a laundry list
and I'll set it to music.
(Gioacchino A. Rossini)

Finale: Hilbert Driven SAGBI Basis Computations

The last variation in this tutorial is based on the idea of imitating the methods of Tutorial 69 in the subalgebra setting. In other words, we are looking for a Hilbert driven SAGBI basis procedure. Rather than developing the full theory, we sketch the motive using a specific example: the Tricky Example 6.6.30.

Let $P = \mathbb{Q}[x_1, x_2]$, let $\sigma = \texttt{DegLex}$, and let $S = K[G]$ be the subalgebra of P generated by $G = \{x_1^2 - x_2^2,\ x_1^2x_2,\ x_1^2x_2^2 - x_2^4,\ x_1^2x_2^4\}$. We assume that we know the Hilbert series of the K-algebra $K[\mathrm{LT}_\sigma(f) \mid f \in S \setminus \{0\}]$. In the case at hand, it is $\mathrm{HS}_S(z) = \frac{1+z^4+z^6}{(1-z^2)(1-z^3)} = 1 + z^2 + z^3 + 2z^4 + z^5 + 4z^6 + 2z^7 + \cdots$.

n) Use the result of Example 6.6.30 and CoCoA to verify this Hilbert series.

o) Now let us start the SAGBI Basis Procedure 6.6.29. Initially, we have $K[\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_4)] = K[x_1^2, x_1^2x_2, x_1^2x_2^2, x_1^2x_2^4]$. Using CoCoA, check that the Hilbert series of this algebra is $\frac{1+z^4}{(1-z^2)(1-z^3)} = 1 + z^2 + z^3 + 2z^4 + z^5 + 3z^6 + 2z^7 + \cdots$. This shows that the SAGBI basis is still incomplete and that we are missing an element of degree 6.

p) After performing steps 4) and 5), we have $K[\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_6)] = K[x_1^2, x_1^2x_2, x_1^2x_2^2, x_1^2x_2^4, x_2^6]$. (Notice that $\mathrm{LT}_\sigma(g_5) = \mathrm{LT}_\sigma(g_1)\,\mathrm{LT}_\sigma(g_6)$.) Using CoCoA, check that the Hilbert series of this algebra is $\frac{1+z^4+z^6}{(1-z^2)(1-z^3)}$. Therefore we have now computed the entire SAGBI basis and we can stop. We do not have to go through steps 4) and 5) again, as we did in Example 6.6.30. Instead, we conclude that $\{g_1, \ldots, g_6\}$ is the SAGBI basis of S.

Tutorial 97: Gröbner and SAGBI Bases Under Composition

\$100 placed at 7 percent interest
compounded quarterly for 200 years
will increase to more than \$100,000,000,
by which time it will be worth nothing.
(Lazarus Long)

How much are we expecting to gain if we compose a SAGBI basis with an endomorphism of the polynomial ring? In most cases we gain apparently nothing, in the sense that we end up with another SAGBI basis. But, hey, this is a remarkable performance! Can we prove it? Under which conditions is the SAGBI basis property preserved? And what happens to Gröbner bases under composition? What are the exact conditions for the Gröbner basis property to be preserved? Can we check these conditions using the computer? Obviously, it is easy to go on and on asking questions. What profit are you to pocket from answering them? Will the answers be worth anything by the time you have found them? For sure you will acquire a large pool of knowledge, and

possibly even wisdom. So, let us propose a scheme of work which allows you to assuage your thirst for learning.

Let K be a field, let $P = K[x_1, \ldots, x_n]$, let σ be a term ordering on $\mathbb{T}^n$, and let $f_1, \ldots, f_n \in P \setminus \{0\}$. Then there exists a unique K-algebra homomorphism $\varphi : P \longrightarrow P$ with $\varphi(x_i) = f_i$ for $i = 1, \ldots, n$. Given a finite set of polynomials $G \subseteq P$, we say that G is a σ-Gröbner basis if it is a σ-Gröbner basis of the ideal it generates. Similarly, we say that G is a σ-SAGBI basis if it is a σ-SAGBI basis of the K-subalgebra of P it generates. In this tutorial we address the following two problems.

1) Are there conditions on the map φ which guarantee that, for every σ-Gröbner basis G, the set $\varphi(G)$ is also a σ-Gröbner basis?
2) Are there conditions on the map φ which guarantee that, for every σ-SAGBI basis G, the set $\varphi(G)$ is also a σ-SAGBI basis?

Since the map φ is determined by the tuple $\mathcal{F} = (f_1, \ldots, f_n)$, we are looking for conditions on this tuple which entail the desired properties. To this end, the following notion will come in handy. We say that the map φ is **compatible with** σ if $t_1 >_\sigma t_2$ implies $\mathrm{LT}_\sigma(\varphi(t_1)) >_\sigma \mathrm{LT}_\sigma(\varphi(t_2))$ for all $t_1, t_2 \in \mathbb{T}^n$. Let $\Phi : P \longrightarrow P$ denote the K-algebra homomorphism defined by $\Phi(x_i) = \mathrm{LT}_\sigma(f_i)$ for $i = 1, \ldots, n$. In this setting it is not very difficult to solve the second problem.

a) Prove that $\Phi(t) = \mathrm{LT}_\sigma(\varphi(t))$ for every $t \in \mathbb{T}^n$. Conclude that φ is compatible with σ if and only if $t_1 >_\sigma t_2$ implies $\Phi(t_1) >_\sigma \Phi(t_2)$ for all $t_1, t_2 \in \mathbb{T}^n$.
b) Assume that φ is compatible with σ. For every $f \in P \setminus \mathrm{Ker}(\varphi)$, show that we have $\mathrm{LT}_\sigma(\varphi(f)) = \Phi(\mathrm{LT}_\sigma(f))$.
c) Let $G = \{g_1, \ldots, g_s\} \subseteq P \setminus \{0\}$ be a σ-SAGBI basis. Prove that $\varphi(G)$ is a σ-SAGBI basis if φ is compatible with σ.
Hint: It suffices to show $\mathrm{LT}_\sigma(\varphi(f)) \in K[\mathrm{LT}_\sigma(\varphi(G))]$ for all polynomials $f \in K[G] \backslash \mathrm{Ker}(\varphi)$. Write $\mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(g_1)^{\alpha_1} \cdots \mathrm{LT}_\sigma(g_s)^{\alpha_s}$ with $\alpha_i \in \mathbb{N}$ and use b).
d) Let $V \in \mathrm{Mat}_n(\mathbb{Z})$ be a non-singular matrix, and let $v_1, \ldots, v_n$ be the rows of V. Show that there exists a $\mathbb{Q}$-basis $\{b_1, \ldots, b_n\}$ of $\mathbb{Q}^n$ having the following properties:
   1) $b_1, \ldots, b_n \in \mathbb{Z}^n$
   2) $\langle v_i, b_j \rangle = 0$ for $1 \leq i < j \leq n$
   3) $\langle v_i, b_i \rangle > 0$ for $1 \leq i \leq n$

   Here $\langle\ ,\ \rangle$ denotes the standard scalar product.
   Hint: First find b_n with $\begin{pmatrix} v_1 \\ \vdots \\ v_{n-1} \end{pmatrix} b_n = 0$. Then extend $\{b_n\}$ to a basis of the kernel of $\begin{pmatrix} v_1 \\ \vdots \\ v_{n-2} \end{pmatrix}$, etc.
e) In the setting of d), prove that a vector $d \in \mathbb{Z}^n$ satisfies $V \cdot d >_{\mathtt{Lex}} 0$ if and only if $c\,d = \sum_{j \geq i} a_j b_j$ with $c, a_i \in \mathbb{N}_+$ and $a_{i+1}, \ldots, a_n \in \mathbb{Z}$ for some $i \in \{1, \ldots, n\}$.

f) Let $\sigma = \texttt{Ord}(V)$ be given by a non-singular matrix $V \in \mathrm{Mat}_n(\mathbb{Z})$, let $\{b_1, \ldots, b_n\}$ be chosen as in d), let $\Phi(x_i) = x_1^{\alpha_{1i}} \cdots x_n^{\alpha_{ni}}$ for $i = 1, \ldots, n$, and let $A = (\alpha_{ij}) \in \mathrm{Mat}_n(\mathbb{N})$. Show that A is non-singular and that the following conditions are equivalent.
   1) The map φ is compatible with σ.
   2) For every $d \in \mathbb{Z}^n$ with $V \cdot d \geq_{\texttt{Lex}} 0$, we have $V \cdot A \cdot d \geq_{\texttt{Lex}} 0$.
   3) For $i = 1, \ldots, n$, the first non-zero entry of $V \cdot A \cdot b_i$ is the i^{th} entry and this entry is positive.

g) Write a CoCoA function `IsCompatible1(...)` which takes a tuple $\mathcal{F}$ and checks whether the K-algebra homomorphism $\varphi : P \longrightarrow P$ it defines is compatible with σ.

h) Using your function `IsCompatible1(...)`, show that the following sets of polynomials are `DegLex`-SAGBI bases of $\mathbb{Q}$-subalgebras of $\mathbb{Q}[x_1, x_2, x_3]$.
   1) $F_1 = \{(x_1x_2 + 1)^3, (x_2^2 + x_1)^4, (x_3^2 + x_2)^5\}$
   2) $F_2 = \{(x_1 + x_3)^3x_2^3, (x_2 + x_3)^3x_3^3, x_3^4\}$
   3) $F_3 = \{(x_1 + 1)(x_2 + 1), (x_2 + 1)(x_3 + 1), (x_3 + 1)^3\}$

Next we describe a more intrinsic approach to the problem of checking compatibility. Let $V \in \mathrm{Mat}_n(\mathbb{Z})$ be a non-singular matrix with rows $v_1, \ldots, v_n$, and let $\sigma = \texttt{Ord}(V)$.

i) Prove that there exists a matrix $W \in \mathrm{Mat}_n(\mathbb{Z})$ whose rows are pairwise orthogonal with respect to $\langle\ ,\ \rangle$ which defines the same term ordering σ. A matrix W with this property is called an **orthogonalization** of V.
   Hint: Imitate the **Gram-Schmidt orthonormalization procedure** as follows. The first row of W is v_1 of V. The second row of W is obtained from v_2 by subtracting a suitable multiple of v_1 and clearing denominators, and so on.

j) Write a CoCoA function `Orthog(...)` which takes a non-singular matrix $V \in \mathrm{Mat}_n(\mathbb{Z})$ and computes an orthogonalization of V.

k) We say that two matrices $W_1, W_2 \in \mathrm{Mat}_n(\mathbb{Z})$ are **row-wise proportional** if there exist positive rational numbers $\lambda_1, \ldots, \lambda_n$ such that the i^{th} row of W_1 equals λ_i times the i^{th} row of W_2 for $i = 1, \ldots, n$. Show that any two orthogonalizations of V are row-wise proportional.

l) Let $\Phi(x_i) = x_1^{\alpha_{1i}} \cdots x_n^{\alpha_{ni}}$ for $i = 1, \ldots, n$, and let $A = (\alpha_{ij}) \in \mathrm{Mat}_n(\mathbb{N})$. Show that φ is compatible with σ if and only if the orthogonalizations of V and $V \cdot A$ are row-wise proportional.

m) Write a CoCoA function `IsCompatible2(...)` which takes a tuple $\mathcal{F}$ and uses l) to check whether the K-algebra homomorphism $\varphi : P \longrightarrow P$ it defines is compatible with σ. Using this function, verify your answer to h).

n) Assume that $n = 2$, and let $\Phi(x_i) = x_1^{\alpha_{1i}} x_2^{\alpha_{2i}}$ for $i = 1, 2$. Prove that φ is compatible with σ if and only if we have $\alpha_{11} + \alpha_{21} = \alpha_{12} + \alpha_{22}$ and $\alpha_{11} > \alpha_{12}$.

o) Give examples of pairs $(\mathcal{F}, G)$ satisfying the following conditions.

1) The map φ is compatible with σ, the set G is not a σ-Gröbner basis, but $\varphi(G)$ is a σ-Gröbner basis.
2) The map φ is not compatible with σ, the set G is a σ-Gröbner basis, but $\varphi(G)$ is not a σ-Gröbner basis. (*Hint:* Try $\mathcal{F} = (x_1, x_2, x_3, x_2)$ and $G = \{x_1^2,\, x_1x_2,\, x_3^2 + x_4^2\}$.)

Having found a satisfactory solution to the second problem, we turn our attention to the first, i.e. to Gröbner bases under composition. The following example shows that it is not sufficient to assume that φ is compatible with σ.

p) Let $P = \mathbb{Q}[x_1, x_2, x_3]$, let $\sigma = \texttt{Lex}$, let $\mathcal{F} = (x_1x_2, x_2^2, x_3^2)$, and let $G = \{x_1 + x_3,\, x_2 + x_3\}$. Prove the following claims.
   1) The map φ is compatible with σ.
   2) The set $G = \{f_1, f_2\}$ is a σ-Gröbner basis.
   3) The set $\varphi(G)$ is not a σ-Gröbner basis.

Thus we have to require additional properties of the map φ if we want it to preserve the Gröbner basis property. We say that φ is **compatible with non-divisibility** if $t_1 \nmid t_2$ implies $\Phi(t_1) \nmid \Phi(t_2)$ for all $t_1, t_2 \in \mathbb{T}^n$.

q) Prove that the following conditions are equivalent.
   1) The map φ is compatible with non-divisibility.
   2) For all $t_1, t_2 \in \mathbb{T}^n$ with $t_1 \nmid t_2$, we have $\mathrm{LT}_\sigma(\varphi(t_1)) \nmid \mathrm{LT}_\sigma(\varphi(t_2))$.
   3) There exist a permutation $\pi : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$ and natural numbers $\alpha_1, \ldots, \alpha_n$ such that $\Phi(x_i) = x_{\pi(i)}^{\alpha_i}$ for $i = 1, \ldots, n$.

   Hint: Prove "3)$\Rightarrow$1)" by contradiction. If no such permutation exists, one of the terms $\Phi(x_i)$ involves at least two indeterminates. Then there exists a term $\Phi(x_i)$ which involves only indeterminates dividing $\prod_{j\neq i}\Phi(x_j)$. Now use the fact that x_i does not divide any power product $\prod_{j\neq i} x_j^{\alpha_j}$.

r) Let φ be compatible with non-divisibility. Using Proposition 1.2.7.a and q), show that we have $\Phi(\gcd(t_1, t_2)) = \gcd(\Phi(t_1), \Phi(t_2))$ for all $t_1, t_2 \in \mathbb{T}^n$.

s) Let φ be compatible with σ and non-divisibility, and let $G = \{g_1, \ldots, g_s\}$ be a σ-Gröbner basis consisting of non-zero polynomials in P. Prove that $\varphi(G)$ is a σ-Gröbner basis.
   Hint: Let $\sigma_{ij} = \frac{1}{c_i}t_{ij}\varepsilon_i - \frac{1}{c_j}t_{ji}\varepsilon_j$ be the fundamental syzygy of $\mathrm{LT}_\sigma(g_i)$ and $\mathrm{LT}_\sigma(g_j)$. Show that $\frac{1}{c_i}\Phi(t_{ij})\varepsilon_i - \frac{1}{c_j}\Phi(t_{ji})\varepsilon_j$ is the fundamental syzygy of $\Phi(\mathrm{LT}_\sigma(g_i))$ and $\Phi(\mathrm{LT}_\sigma(g_j))$. Then use b) and Conditions D) of Theorem 2.4.1.

t) Write a CoCoA function `IsNonDivisible(...)` which takes a tuple $\mathcal{F}$ and checks whether the map φ it defines is compatible with non-divisibility.

u) Using your functions `IsCompatible(...)` and `IsNonDivisible(...)`, show that the following sets are `Lex`-Gröbner bases in $\mathbb{Q}[x_1, x_2, x_3]$.
   1) $G_1 = \{(x_1^2 + x_2^2)^3,\, (x_2^2 + x_3^2)^3,\, x_3^8\}$
   2) $G_2 = \{(x_1^2 + x_2x_3)^5,\, (x_2^2 + x_3^2)^5,\, x_3^{10}\}$
   3) $G_3 = \{(x_2^2 + x_3^2)x_3^2 - x_1^2 - x_2x_3,\, (x_3^2 + 1)(x_1^2 + x_2x_3),\, (x_1^2 + x_2x_3)^2\}$

Tutorial 98: Molien's Theorem

Television – a medium.
So called because it is neither rare nor well-done.
(Ernie Kovacs)

I wish there was a knob on the TV to turn up the intelligence.
There's one marked Brightness*, but it doesn't work.*
(Eugene P. Gallagher)

57 channels and nothing on. It is time to turn up our brightness and apply it to compute invariants more efficiently than in Tutorial 40. There we asked you to prove that there are only finitely many fundamental invariants, and we constructed an elementary algorithm for their computation. However, that was not very well done because even for seemingly innocent examples the computation was quite lengthy. In this tutorial we use Molien's Theorem which gives us an explicit formula for the Hilbert series of a ring of invariants. This enables us to compute the fundamental invariants intelligently via a Hilbert driven strategy.

First we recall the basic setting of invariant theory. Let K be a field, and let $P = K[x_1, \ldots, x_n]$ be standard graded. The group $\mathrm{GL}_n(K)$ of all invertible $n \times n$-matrices acts on P via $\mathcal{A} \circ f = f(\mathcal{A} \cdot \mathbf{x})$ where $\mathcal{A} = (a_{ij})$ and $\mathcal{A} \cdot \mathbf{x} = (a_{11}x_1 + \cdots + a_{1n}x_n, \ldots, a_{n1}x_1 + \cdots + a_{nn}x_n)$.

Given a finite subgroup $G \subseteq GL_n(K)$, we say that a polynomial f is **invariant** under G if $f(\mathcal{A} \cdot \mathbf{x}) = f(\mathbf{x})$ for all $\mathcal{A} \in G$. The set of all polynomials in P which are invariant under G form a graded K-subalgebra P^G of P which is called the **ring of invariants**. There are finitely many homogeneous polynomials $f_1, \ldots, f_s$ such that $P^G = K[f_1, \ldots, f_s]$.

Since P^G is a finitely generated, positively $\mathbb{Z}$-graded K-algebra, we consider its Hilbert series $\mathrm{MS}_G(z) = \sum_{i \geq 0} \dim_K(P^G)_i \, z^i \in \mathbb{Q}[[z]]$ and call it the **Molien series** of P^G.

a) Define a homogeneous presentation $P^G \cong K[y_1, \ldots, y_s]/I_G$ and explain how one can use it to compute the Molien series of a ring of invariants. Write a CoCoA function `MolienSeries(...)` which takes a list of matrices in $\mathrm{Mat}_n(K)$ representing the elements of G as in Tutorial 40 and computes the Molien series of P^G.
b) Apply your function `MolienSeries(...)` to compute the Molien series of the rings of invariants of the ten groups in Tutorial 40.a.
c) Find the Molien series of the ring of symmetric polynomials (see Tutorial 12 and Corollary 6.6.12).
d) Let $V = \{v \in K^n \mid \mathcal{A}\, v = v \text{ for all } \mathcal{A} \in G\} \subseteq K^n$ be the invariant vector subspace of G. Prove the formula

$$\dim_K(V) = \tfrac{1}{\#G} \sum_{\mathcal{A} \in G} \mathrm{trace}(\mathcal{A})$$

Hint: Show that the **average matrix** $\mathcal{B} = \frac{1}{\#G} \sum_{\mathcal{A} \in G} \mathcal{A}$ satisfies $\mathcal{B}^2 = \mathcal{B}$ and consider its rank and its eigenvalues.

e) Assume $\mathrm{char}(K) = 0$. Prove **Molien's Theorem** which states that the Molien series of a ring of invariants is given by the formula

$$\mathrm{MS}_G(z) = \frac{1}{\#G} \sum_{\mathcal{A} \in G} \frac{1}{\det(\mathcal{I}_n - z\,\mathcal{A})}$$

Hint: Show that you may assume that K is algebraically closed. Then proceed degree by degree. A matrix $\mathcal{A} \in G$ induces a diagonalizable linear transformation on P_1 with eigenvalues $\lambda_1, \ldots, \lambda_n$. Find the eigenvalues of the induced transformation on P_d and show that its trace is $\sum_{i_1+\cdots+i_n=d} \lambda_1^{i_1} \cdots \lambda_n^{i_n}$. Then use d).

f) Write a CoCoA function `MolienFormula`(...) which takes a list of matrices in $\mathrm{Mat}_n(K)$ representing the elements of G and computes the rational function given by Molien's Theorem.

g) Apply your function `MolienFormula`(...) to the examples in Tutorial 40.a and compare the results with the output of `MolienSeries`(...).

h) The knowledge of the Molien series of a ring of invariants can be used to compute the fundamental invariants using a Hilbert-driven approach. Write a CoCoA function `HDrivenInvariants`(...) which modifies the algorithm of Tutorial 40.g by stopping the computation in a given degree when the Hilbert function of the subring of P^G computed so far agrees with the Hilbert function of P^G in that degree.

i) Apply your function `HDrivenInvariants`(...) to the examples in Tutorial 40.a. Compare its efficiency to that of the function `Invariants`(...) of Tutorial 40.h.

6.7 Automatic Theorem Proving

Post nubila phoebus.
Auf Regen folgt Sonne.
Na regen komt zonneschijn.
Après la pluie le beau temps.
Dopo la pioggia viene il sereno.
After the rain comes the rainbow.
Depois da tempestade vem a bonança.
Después de la lluvia viene el buen tiempo.

A famous physicist once remarked that there are only two kinds of math books: those you cannot read beyond the first sentence, and those you cannot read beyond the first page. So, probably you arrived here by chance while browsing this book. You will not be surprised by the fact that the pattern of this section differs from the rest of the book. Instead, if you arrived here after reading the entire book, we are happy to see that we produced an exception to the physicist's classification. In this case you have endured many difficulties. You have been strong enough to pass through hail storms, snow blizzards, howling gales, and impenetrable fog. It is time for some relief. Finally the sun starts to shine and a beautiful rainbow appears. Gone are the tedious and difficult proofs, gone is the pain of checking every single step: in this section we are about to learn how proofs can automatically be produced by the computer! Isn't this a true case of artificial intelligence? Or is it an unrealizable dream?

The hope of automatically proving *all* theorems in a specific part of mathematics from a small set of axioms was dashed by Kurt Gödel with his famous incompleteness theorem. But what about using machines to prove at least *some* theorems? Although this subject has a long history, it really got off the ground with the advent of electronic computers. To examine it in detail, we concentrate our attention on a well-studied classical subject. We want to explain methods for automatically proving theorems from Euclidean geometry. These methods use Gröbner bases and are meant to provide instances of how computers can help humans with the largely unknown process of proving theorems. Although the entirety of Euclidean geometry looks like a small pond when compared with the ocean of mathematics, you will see that dangerous cross-currents are lurking beneath the apparently calm surface of the water.

Treacherous phenomena start appearing as soon as the first subsection commences. The first counter current comes from the question of what constitutes a correct proof. Should we accept a proof given by a computer? Or should we only rely on what we can verify ourselves? Remember, errors in mathematical books and scholarly papers are commonplace! Some are irrelevant, some are not. For an example of particularly nice deception, check out "Theorem" 6.7.1. Whether the majority of mathematicians accept a given proof as correct depends more on the general consensus than on the logical correctness of each step, because nobody is able to follow all steps starting

from the axioms and ending up with a given claim. Have you ever meditated about the distance which separates the axioms from any profound statement, say in algebraic geometry? But the worst has yet to come.

The process of representing the geometric hypothesis of a statement in Euclidean geometry by polynomial equations is intrinsically subjective. Depending on the chosen model we may very well come to different conclusions about the validity of a geometric theorem. Furthermore, if we represent the hypotheses by polynomials having real coefficients and we want to manipulate them automatically, we face the problem that the field $\mathbb{R}$ is not computable. In addition, our translation of the claim that a certain thesis polynomial follows from the hypothesis polynomials hinges on the applicability of Hilbert's Nullstellensatz which, in turn, requires the base field to be algebraically closed (see for instance Theorem 6.7.3). The next problem which arises is that it is easy to overlook geometric non-degeneracy conditions which have to be imposed to make the theorem true (see Theorem 6.7.4). All of this goes a long way to show that the process of transforming a geometric statement into a problem of Computational Commutative Algebra such as ideal membership is highly non-automatic.

To underpin the actual proving process with a suitable algebraic basis, we start the second subsection by introducing the notion of an algebraically true statement. This means that we formulate a model $\mathcal{T}$ for a geometric statement and check whether the thesis polynomial is contained in the radical of the hypothesis ideal $I_h(\mathcal{T})$. Here the field of definition introduced in Section 2.4 allows us to work in the polynomial ring $P = K[x_1, \ldots, x_n]$ over an algebraic number field K (see Theorem 6.7.9). As expected, the field of definition depends on the choice of a model (see Theorem 6.7.8). Less expected is the squall triggered by the discovery that most geometric statements are algebraically false, even many theorems which we know to be true in Euclidean geometry.

To understand what is happening here, we have to analyze a few cases in detail (see Theorem 6.7.10 and Example 6.7.12). Recall that a radical ideal such as $\sqrt{I_h(\mathcal{T})}$ can be written as an intersection $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$ of prime ideals. The result of our analysis is that a geometric theorem can be algebraically true on some prime components of $\sqrt{I_h(\mathcal{T})}$ but not on all. This is frequently due to the fact that there exist geometric non-degeneracy conditions which are not obvious from the geometric picture but which are essential to make the theorem algebraically true. Since the prime decomposition of an ideal is usually difficult to compute, we have to endure yet another rain shower. But this time around the sun swiftly returns. By requiring a condition of the form $f \neq 0$ with a well-chosen polynomial $f \in P$, we can eliminate the prime components of $\sqrt{I_h(\mathcal{T})}$ on which the theorem is algebraically false. Moreover, the condition ideal, i.e. the ideal of all such conditions, is not difficult to compute. Using the condition ideal, we can change the hypothesis ideal to the optimal hypothesis ideal. In other words, we can change the

hypothesis of the geometric theorem such that we exclude precisely the bad components of the radical of the initial hypothesis ideal.

Alas, the appearance of this beautiful rainbow on the horizon does not prevent one last aggravation. After we have computed the optimal hypothesis ideal, we discover that most of the time we have no reasonable geometric interpretation for the new set of hypotheses. We have proved a theorem, but we do not know which! This brings us to the last step on our way to sunny climes. Given a set of generators G of the condition ideal, we say that the minimal conditions in G are those which remove the bad components of $\sqrt{I_h(\mathcal{T})}$ and as little else as possible. Minimal conditions provide us with a much wider choice, and with a bit of luck we can find one which has a nice geometric meaning. Putting everything together, we obtain the Automatic Prover 6.7.25, an algorithm which takes over a large part of the process of proving geometric theorems. Still, it is a misnomer: *semiautomatic prover* would surely be more appropriate, but much less flashy.

Finally, in Tutorial 99, we turn the tables on you. Instead of asking you to implement the Automatic Prover, we fling the code at you and ask you to make sense of it, and to use it to prove some geometric theorems. You will notice that not just this final tutorial, but the entire section is written in a style which differs significantly from the rest of the book: it is frequently more narrative and occasionally less precise than what you have become used to. The upshot of this section is that artificial intelligence is in some sense an oxymoron. So, soak up the sun and tell everyone to lighten up!

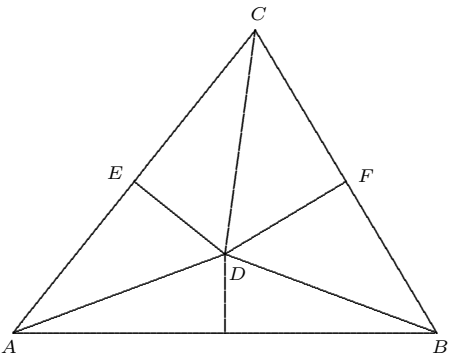
6.7.A The Tribulations of Automation

Someone who thinks logically
is a nice contrast to the real world.
(Anonymous)

In this subsection we show you a few geometric theorems whose proofs contain obstacles to their automation. Even very elementary proofs can contain hidden pitfalls. For instance, the proof of the following theorem uses the standard technique taught in high school.

Geometric Theorem 6.7.1. *Every triangle is isosceles.*

Proof. Let ΔABC be a triangle. Consider the following picture.



It suffices to prove $AC = BC$. Let D be the intersection of the perpendicular bisector of AB and the internal bisector of $\angle ACB$. We drop the perpendiculars from D to AC and to BC and call their endpoints E and F respectively. Then we have $\Delta CDE \cong \Delta CDF$ because $\angle ECD = \angle DCF$ and $\angle DEC = \angle CFD = 90^o$. In particular, this shows that $DE = DF$. Together with $AD = BD$ and $\angle AED = \angle BFD = 90^o$, we obtain $\Delta ADE \cong \Delta BDF$. Hence we see that $AC = AE + EC = BF + FC = BC$. □

What is wrong with this proof? If you feel a little nervous about this example, or you are surprised by this apparent paradox, please relax and you will discover the trick. You will understand that the logic of the proof is a nice contrast to the real world. The picture is misleading because the point D lies outside the triangle!

As the Greek philanderer Isosceles used to say,
there are three sides to every triangle.
(Anonymous)

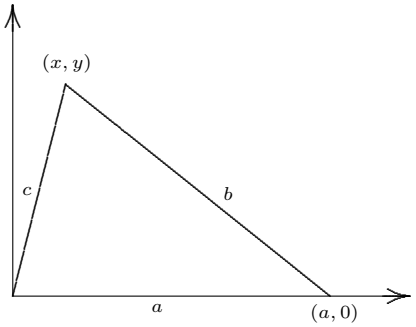
In order to prove geometric theorems automatically, we have to find a more standardized and less fallible procedure. In analytic geometry we usually perform the following steps.

1) We introduce Cartesian coordinates in the Euclidean plane or space.
2) We translate the hypotheses and thesis into algebraic relations among the fundamental geometric data such as coordinates of points and lengths of segments.
3) Let these algebraic relations be expressed as the vanishing of suitable polynomials. Then we prove the theorem by showing that the *thesis polynomial* is a consequence of the *hypothesis polynomials*.

Of course, all of these steps require additional clarification to make them accessible to automation. To begin with, we shall see that it is practically impossible to automate the entire process. For instance, the choice of the coordinate system and some clever simplifications of the input data are part of a preprocessing which has to be done before we can even pass the problem to the computer. The example mentioned in the introduction of Section 3.4 is a case in point.

Geometric Theorem 6.7.2. (Heron's Formula)
Let a, b, and c be the lengths of the sides of a triangle, let $p = (a+b+c)/2$, and let s be the area of the triangle. Then s is determined by the formula $s^2 = p(p-a)(p-b)(p-c)$.

Automatic Proof. To perform step 1) of the above method, we choose an orthogonal system of coordinates. Using the possibility to position the coordinate axes freely, we arrange them as follows.



Now we have to translate the hypotheses into polynomial relations among the input data. We use Pythagoras' Theorem to deduce that $b^2 = (a-x)^2+y^2$ and $c^2 = x^2+y^2$. Furthermore, we observe that $2s = ay$. We can collect these polynomials and form the ideal $I = (b^2 - (a-x)^2 - y^2,\ c^2 - x^2 - y^2,\ 2s - ay)$ in the polynomial ring $\mathbb{R}[x, y, a, b, c, s]$. The simultaneous vanishing of these polynomials corresponds to the geometrical arrangement in the diagram. The thesis corresponds to the vanishing of $f = s^2 - p(p-a)(p-b)(p-c)$ where $p = (a+b+c)/2$.

Finally we have to prove that the thesis polynomial follows from the hypothesis polynomials. This means that every set of concrete values of $a, b, c, x, y,$ and s satisfying the hypothesis polynomials is a zero of the thesis polynomial. This task can indeed be solved using Gröbner basis because we can show that $f \in I$. Then we may conclude that $\mathcal{Z}_{\mathbb{R}}(I) \subseteq \mathcal{Z}_{\mathbb{R}}(f)$.

There is still one obstacle here: in principle it is not possible to perform computations over the base field $\mathbb{R}$. However, this problem can be overcome easily by showing that f is contained in $I \cap \mathbb{Q}[a, b, c, x, y, s]$. □

Notice that, as we explained in the introduction of Section 3.4, in this particular case we could also have discovered the thesis polynomial if we had not known it beforehand. Clearly, in this proof it is not possible to automate the first two steps. But what about the third step? Does it always work so nicely? Unfortunately, it does not, as the next theorem shows.

Geometric Theorem 6.7.3. *Cubes of equal volume have equal sides.*

Automatic Proof. Let us try to follow the above steps again. We choose the coordinate system so that the origin of one of the cubes is one of its vertices and the other vertices are $(a, 0, 0)$, $(0, a, 0)$, $(0, 0, a)$, $(a, a, 0)$, $(0, a, 0)$,

$(0,a,a)$, and (a,a,a) where a is the length of one side. Then we move the other cube to the same position, i.e. so that its vertices are $(0,0,0)$, $(b,0,0)$, etc., where b is the length of one side.

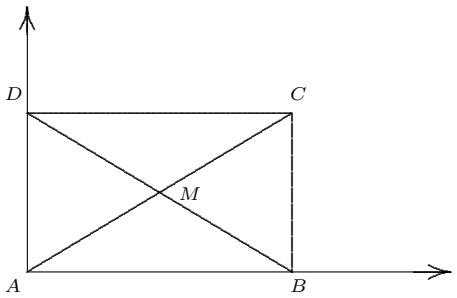
The hypothesis polynomial is a^3-b^3, and the thesis polynomial is $a-b$. The thesis polynomial *does not follow* from the hypothesis polynomial in the sense that not only $a-b \notin (a^3-b^3)$, but even $a-b \notin \sqrt{(a^3-b^3)} \subseteq \mathbb{R}[a,b]$. We cannot use Hilbert's Nullstellensatz 2.6.16 to translate the desired inclusion of zero sets into an ideal-theoretic inclusion because it requires the base field to be algebraically closed.

In fact, if we let $c_1, c_2 \in \mathbb{C} \setminus \mathbb{R}$ be the two conjugate complex cubic roots of unity, we have $a^3-b^3 = (a-b)(a-c_1b)(a-c_2b)$. Hence the variety defined by the hypothesis polynomial has one real component and two complex components, and only the real component corresponds to the thesis polynomial. Therefore the theorem is indeed true over the real numbers, although our automatic proof attempt failed. Of course, the theorem should be considered false over the complex numbers, since for instance $2^3 = (-1+\sqrt{3}\,i)^3$. □

Even if we were able to pass this hurdle, the following obstacle apparently forces us to realize that we are at a dead end.

Geometric Theorem 6.7.4. (Diagonal Bisection)
The diagonals of a rectangle cross each other at their midpoints.

Automatic Proof. Let the vertices of the rectangle be called A, B, C, D, and let O be the point of intersection of the two diagonals AC and BD. We introduce an orthogonal system of coordinates as shown in the following picture.



Then we denote the coordinates of the relevant points by $A = (0,0)$, $B = (x_1,0)$, $C = (x_1,x_2)$, $D = (0,x_2)$, and $M = (x_3,x_4)$. We have to show that $AM = CM$ and $BM = DM$.

Since we have already expressed the fact that $ABCD$ is a rectangle, the only hypotheses still to be translated are that M belongs to the line AC as well as to the line BD. By some elementary considerations, this yields the hypothesis polynomials $h_1 = x_1x_4 - x_2x_3$ and $h_2 = x_1x_2 - x_2x_3 - x_1x_4$. The desired equations $AM = CM$ and $BM = DM$ correspond to the thesis polynomials $t_1 = x_1^2 + x_2^2 - 2x_1x_3 - 2x_2x_4$ and $t_2 = x_1^2 - x_2^2 - 2x_1x_3 + 2x_2x_4$.

To prove the theorem is suffices to show that $\mathcal{Z}_{\mathbb{R}}(h_1, h_2) \subseteq \mathcal{Z}_{\mathbb{R}}(t_1, t_2)$. Let $K \supseteq \mathbb{Q}$ be the base field which we intend to use for the computation. We have already seen that Hilbert's Nullstellensatz translates the desired containment to an algebraic verification only if the base field is algebraically closed. However, the worst is yet to come. The nasty surprise is that no matter over which field K we work, the statements $t_1 \in \sqrt{(h_1, h_2)}$ and $t_2 \in \sqrt{(h_1, h_2)}$ are always false! □

The reason for this failure of our automatic procedure is that we are really looking for the inclusion $\mathcal{Z}_{\mathbb{R}_+}(h_1, h_2) \subseteq \mathcal{Z}_{\mathbb{R}_+}(t_1, t_2)$. If we use the hypotheses $h_1 + h_2 = x_2(x_1 - 2x_3)$ and $h_1 - h_2 = x_1(2x_4 - x_2)$, we see that $x_1 > 0$ and $x_2 > 0$ imply $x_1 = 2x_3$ and $x_2 = 2x_4$, Then the theses follow from $t_1, t_2 \in (x_1 - 2x_3,\, x_2 - 2x_4)$. So, the automatic proof is thwarted by the fact that the hypothesis polynomials allow some degenerate cases in which the theorem is false. Had we defined $x_3 = \frac{1}{2}x_1$ and $x_4 = \frac{1}{2}x_2$ and then asked if AMC and BMD are collinear, there would have been no problem. So the provability of a geometric theorem depends on how we encode it as an algebraic problem.

It happens that many theorems from Euclidean geometry turn out to be false in the algebraic setting, simply because the algebraic translation of some condition encodes more cases than intended. This certainly happens in the preceding proof. We end our little collection of curiosities with an even simpler case.

Geometric Theorem 6.7.5. *Let L be a straight line in the Euclidean plane, let $A, B \in L$, and let C be a point in the plane. Then if C is aligned with A and B, we have $C \in L$.*

Automatic Proof. Let us try to prove this apparently trivial theorem automatically. We choose the coordinate system such that L is the x-axis and $A = (0, 0)$ the origin. Then we write $B = (x, 0)$ and $C = (a, y)$. Now we have to express the hypothesis. At first glance we are tempted to use the hypothesis polynomial $h = y$. However, a more complete description of the hypothesis is given by $\tilde{h} = xy$ since this polynomial takes also the case $A = B$ into account. As the thesis polynomial is clearly $t = y$, we would like to show $y \in \sqrt{(xy)}$ which is clearly not true. Indeed, this is not surprising because in the case $A = B$ every point C is aligned with A and B.

Suppose we want to prove the theorem only in the case $A \neq B$. Algebraically, this means that we consider only the zeros of $(xy) : (x) = (y)$. Using this hypothesis, the thesis polynomial satisfies $t \in (y)$, and the theorem is proved. □

In this proof the hypothesis ideals (xy) and (y) lead to dramatically different results: using (xy), the thesis is false, but using (y) it is true. It is not always easy to make a full *a priori* analysis of the degenerate cases of a geometric theorem. Even then the radical of the hypothesis ideal need

not be a prime ideal. For instance, it is perfectly legitimate to consider a hypothesis of the following type: "Let ΔABC be a triangle which is isosceles or right angled." In this case the radical of the hypothesis ideal will probably have at least two prime components, even if we eliminate degenerate cases beforehand. To get some control over all these cases, we have to put our automatic proofs on a stronger theoretical footing. This is our goal in the next two subsections.

6.7.B Algebraically True Statements

The real *world is* complex.
True *statements may be* false.
(Anonymous)

The simplest case of automatic theorem proving occurs when we can deduce the thesis just by showing ideal membership. Let us describe the process in detail. Given a statement in Euclidean geometry, we introduce a coordinate system and encode the hypotheses as polynomials $h_1, \ldots, h_r$ and the thesis as a polynomial t. This means that we assign indeterminates $x_1, \ldots, x_n$ to some unknown quantities and formulate the geometric hypotheses and theses in terms of those quantities. Each concrete instance of the geometric theorem then corresponds to a tuple $(a_1, \ldots, a_n) \in \mathbb{R}^n$ such that the hypothesis polynomials are satisfied, i.e. to a point in $\mathcal{Z}_{\mathbb{R}}(h_1, \ldots, h_r)$. Of course, these tuples are also real zeros of the radical $\sqrt{(h_1, \ldots, h_r)}$. Thus we are led to the following definition.

Definition 6.7.6. Suppose we are given a statement in Euclidean geometry whose hypotheses and thesis can be expressed by the vanishing of polynomials in $\mathbb{R}[x_1, \ldots, x_n]$.

a) A tuple of polynomials $\mathcal{T} = (h_1, \ldots, h_r, t) \in \mathbb{R}[x_1, \ldots, x_n]^{r+1}$ is called a **model** for the statement if $h_1, \ldots, h_r$ express its hypotheses and t expresses its thesis. The ideal $I_{h,\mathbb{R}}(\mathcal{T}) = (h_1, \ldots, h_r)$ is called the **hypothesis ideal** of $\mathcal{T}$, and t is called the **thesis polynomial** of $\mathcal{T}$.

b) The model $\mathcal{T}$ is said to be **algebraically true** if we have $t \in \sqrt{I_{h,\mathbb{R}}(\mathcal{T})}$. Otherwise, we say that it is **algebraically false**. If it is clear which model we are considering, we simply say that the statement is algebraically true or algebraically false.

For instance, Heron's formula 6.7.2 is algebraically true, whereas the statements of Theorems 6.7.3 and 6.7.4 are algebraically false. Notice that in principle it is possible for a geometric theorem to be algebraically true even if the hypothesis ideal does not have real zeros. In the following we shall assume that we start with an actual geometric object which satisfies the hypothesis ideal, so that this case is avoided.

Furthermore, we have already noted that $\mathbb{R}[x_1, \ldots, x_n]$ is not a computable ring. We have to perform the computation over a smaller base field. Usually the hypothesis and thesis polynomials appearing in actual geometric statements have rational coefficients; and in virtually all cases the coefficients are algebraic numbers. Therefore the field of definition of an ideal introduced in Section 2.4.C helps us to pass to the smallest possible base field.

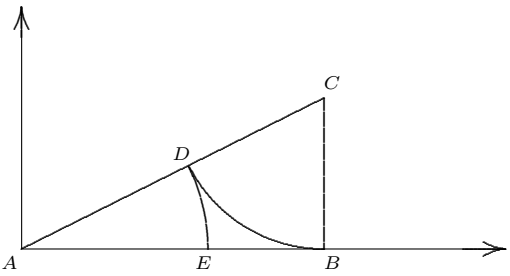
Proposition 6.7.7. *Let $\overline{\mathbb{Q}}$ be the field of algebraic numbers, let $f_1, \ldots, f_r$ be polynomials in $\overline{\mathbb{Q}}[x_1, \ldots, x_n]$, and let $I = (f_1, \ldots, f_r)$. Then the field of definition of I is a finite extension of $\mathbb{Q}$.*

Proof. The claim follows immediately from Theorem 2.4.17, since the prime field of $\mathbb{R}$ is $\mathbb{Q}$ and the polynomials of a reduced Gröbner basis of I have finitely many coefficients. □

Given a statement in Euclidean geometry and a model $\mathcal{T} = (h_1, \ldots, h_r, t)$, the field of definition K of the ideal generated by $\{h_1, \ldots, h_r, t\}$ is also called the **field of definition** of $\mathcal{T}$, or of the statement if it is clear which model we are considering. We let $I_{h,K}(\mathcal{T}) = I_{h,\mathbb{R}}(\mathcal{T}) \cap K[x_1, \ldots, x_n]$. If it is clear over which field of definition we are working, we shall simply write I_h instead of $I_{h,K}$.

The following geometric theorem illustrates the dependence of the field of definition on the choice of the model.

Geometric Theorem 6.7.8. (The Golden Mean)
Let AB be a line segment, let BC be perpendicular to AB and have half its length, let D be the intersection of AC with the circle centered on C and passing through B, and let E be the intersection of AB with the circle centered on A and passing through D. Then the point E is the **golden mean** *of AB, i.e. it satisfies the* **golden ratio** $\frac{AB}{AE} = \frac{1}{2}(1 + \sqrt{5})$.



Automatic Proof 1. First we introduce an orthogonal system of coordinates as shown in the picture. We let $A = (0, 0)$, $B = (x_1, 0)$, $D = (x_2, x_3)$, and $E = (x_4, 0)$, and obtain $C = (x_1, \frac{x_1}{2})$. In this way we have already expressed the hypothesis that BC is perpendicular to AB and has half its length. It remains to express the hypotheses that D is contained in the line AC, that

$BC = CD$, and that $AD = AE$. This yields the hypothesis polynomials $h_1 = x_1x_2 - 2x_1x_3$, $h_2 = x_1^2 - 2x_1x_2 + x_2^2 - x_1x_3 + x_3^2$, and $h_3 = x_2^2 + x_3^2 - x_4^2$. The thesis polynomial is $t = 2x_1 - (1 + \sqrt{5})x_4$.

The field of definition of the model (h_1, h_2, h_3, t) is $\mathbb{Q}(\sqrt{5})$. By performing the appropriate computations in $\mathbb{Q}(\sqrt{5})[x_1, x_2, x_3, x_4]$, we see that the theorem is not algebraically true. □

Automatic Proof 2. An alternative way of posing the problem is to require that AE is the **golden section** of AB, i.e. that $\frac{AB}{AE} = \frac{AE}{BE}$. In this model the thesis polynomial is $\tilde{t} = x_1^4 - 2x_1^3x_4 + x_1^2x_4^2 - x_4^4$. The field of definition of the model $(h_1, h_2, h_3, \tilde{t})$ is $\mathbb{Q}$. In this case we perform all computations in $\mathbb{Q}[x_1, x_2, x_3, x_4]$. It turns out that the theorem is not algebraically true using this model either. It is interesting to observe that the two approaches lead to different computations. □

This theorem is examined further in Tutorial 99. Our next result allows us to check computationally whether a model for a geometric statement is algebraically true.

Proposition 6.7.9. *Let $\mathcal{T} = (h_1, \ldots, h_r, t) \in \mathbb{R}[x_1, \ldots, x_n]^{r+1}$ be a model for a statement in Euclidean geometry, and let K be the field of definition of this model. Then the following conditions are equivalent.*

a) The model $\mathcal{T}$ is algebraically true, i.e. we have $t \in \sqrt{I_{h,\mathbb{R}}(\mathcal{T})}$.

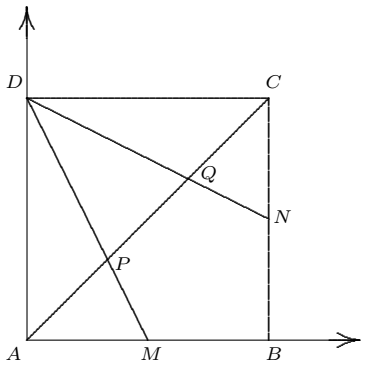
b) We have $t \in \sqrt{I_h(\mathcal{T})}$.

Proof. Since b) clearly implies a), it suffices to prove that a) implies b). Let $i > 0$ be such that $t^i \in I_{h,\mathbb{R}}(\mathcal{T}) \subseteq \mathbb{R}[x_1, \ldots, x_n]$. By assumption, we know that $t \in K[x_1, \ldots, x_n]$. Therefore Proposition 2.6.12 implies that we have $t^i \in I_{h,\mathbb{R}}(\mathcal{T}) \cap K[x_1, \ldots, x_n] = I_h(\mathcal{T})$, and this proves the claim. □

In view of this proposition we shall from now on always work over the field of definition of a model $\mathcal{T}$. Hence we can check computationally whether $\mathcal{T}$ is algebraically true. But this does not solve all problems we encountered in the first subsection. For instance, we saw that Theorem 6.7.4 is algebraically false. Should we conclude that the diagonals of a rectangle are not crossing each other at their midpoint? Let us examine a similar theorem more carefully.

Geometric Theorem 6.7.10. (Diagonal Trisection)
The two lines passing through a vertex of a square and the midpoints of the opposite sides cut the opposite diagonal into three equal parts.

Automatic Proof. First we introduce Cartesian coordinates and place the square as in the following picture.



Let x_1 be the length of the side of the square. Then we have $A = (0,0)$, $B = (x_1,0)$, $C = (x_1,x_1)$, $D = (0,x_1)$, $M = (x_1/2,0)$, and $N = (x_1,x_1/2)$. Moreover, let $P = (x_2,x_2)$ where x_2 is a further indeterminate. By symmetry, we have $Q = (x_1 - x_2, x_1 - x_2)$. In this way we have already expressed that P and Q are contained in the line AC and that $AP = CQ$. The remaining hypotheses are that D, P, and M are aligned and that D, Q, and N are aligned. Both lead to the hypothesis polynomial $h = x_1^2 - 3x_1x_2$. Hence the hypothesis ideal is the principal ideal $I_h(\mathcal{T}) = (h)$. The thesis polynomial is obtained expressing the equality $AP = PQ$. Hence it is given by $t = x_1^2 - 4x_1x_2 + 3x_2^2$. The field of definition of this model is obviously $\mathbb{Q}$. When we check whether $t \in \sqrt{H_{\mathbb{Q}}(\mathcal{T})}$, the answer is no. Therefore the statement is algebraically false. □

Now should be start doubting Euclid? No, we should try to discover why this statement turned out to be algebraically false. Fortunately, this is not difficult. The hypothesis ideal $I_h(\mathcal{T}) = (x_1^2 - 3x_1x_2) = (x_1(x_1 - 3x_2))$ describes two different situations. One is given by $x_1 = 0$, a component over which the statement is algebraically false. The other one is given by $x_1 - 3x_2 = 0$, and the thesis polynomial satisfies $t \in (x_1 - 3x_2)$. Therefore the statement is algebraically true (hence a theorem) if $x_1 \neq 0$, i.e. if the square is not a point. Below we will see that the case $x_1 = 0$ is not a limit case, but a truly different component. This situation suggests the following definition. Recall that a radical ideal in a Noetherian ring is the intersection of its minimal primes (see Proposition 5.6.15.a).

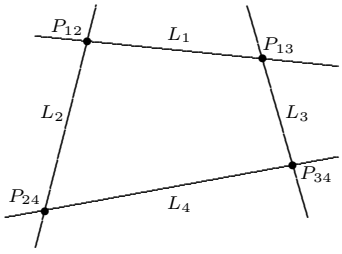
Definition 6.7.11. Suppose we are given a statement in Euclidean geometry. Let K be the field of definition of a model $\mathcal{T} = (h_1, \ldots, h_r, t)$ for it. Furthermore, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the minimal primes of $\sqrt{I_h(\mathcal{T})}$, so that $\sqrt{I_h(\mathcal{T})} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$ is its primary decomposition, and let $i \in \{1, \ldots, s\}$. We say that the model $\mathcal{T}$ is **algebraically true on the component** $\mathfrak{p}_i$ if we have $t \in \mathfrak{p}_i$. If it is clear which model we are considering, we also say that the statement is algebraically true on $\mathfrak{p}_i$.

Therefore a statement can be algebraically false, but true on some of the components, as it happens in the case of Diagonal Trisection 6.7.10. Now let us go back to the Diagonal Bisection 6.7.4.

Example 6.7.12. In the setting of Theorem 6.7.4, it is easy to check that the field of definition of $\mathcal{T}$ is $\mathbb{Q}$ and its hypothesis ideal satisfies $I_h(\mathcal{T}) = \sqrt{I_h(\mathcal{T})} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3 \cap \mathfrak{p}_4$ where $\mathfrak{p}_1 = (x_1 - 2x_3,\, x_2 - 2x_4)$, $\mathfrak{p}_2 = (x_2,\, x_4)$, $\mathfrak{p}_3 = (x_1,\, x_3)$, and $\mathfrak{p}_4 = (x_1,\, x_2)$. Since both thesis polynomials are contained in $\mathfrak{p}_1 \cap \mathfrak{p}_4$, but not in $\mathfrak{p}_2$ and not in $\mathfrak{p}_3$, the statement is algebraically true only on $\mathfrak{p}_1$ and $\mathfrak{p}_4$.

It is clear how we should interpret the components $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_4$. The vanishing of $\mathfrak{p}_2$ represents degeneration to the line segment AB. The vanishing of $\mathfrak{p}_3$ represents degeneration to the line segment AD. Finally, the vanishing of $\mathfrak{p}_4$ represents the case when the rectangle degenerates to the point A. But what is the geometric interpretation of the generators of $\mathfrak{p}_1$? Obviously, the rectangles corresponding to the tuples which are zeros of $\mathfrak{p}_1$, but not $\mathfrak{p}_2 \cap \mathfrak{p}_3 \cap \mathfrak{p}_4$ are the non-degenerate ones. So, the result of our refined automatic proof is that the model is algebraically true for non-degenerate rectangles and for certain (but not all) degenerate cases.

Still more can be deduced from an even finer analysis of this theorem. There are degenerate cases where the theorem is algebraically true, namely the points of $\mathcal{Z}_{\mathbb{R}}(\mathfrak{p}_4)$ for which the corresponding geometric situation is not a limit of non-degenerate rectangles. To help visualize the following discussion, we introduce a schematic picture. Notice that it is of a different nature than the other pictures in this section. For $i = 1, \ldots, 4$, let $L_i \subset \mathbb{P}^3_{\mathbb{R}}$ be the line defined by $\mathfrak{p}_i$.



It is easy to check that L_1 and L_4 are skew, as are L_2 and L_3. The points of intersection are $P_{12} = (2{:}0{:}1{:}0)$, $P_{13} = (0{:}2{:}0{:}1)$, $P_{24} = (0{:}0{:}1{:}0)$, and $P_{34} = (0{:}0{:}0{:}1)$. These lines and points can be interpreted as follows.

a) The set $L_1 \setminus \{P_{12}, P_{13}\}$ represents the non-degenerate rectangles.
b) The point P_{12} represents the cases where the rectangle has degenerated to the side AB and where M is the midpoint of AB. Notice that these degenerate rectangles are continuous limits of non-degenerate ones.

c) Similarly, the point P_{13} represents the cases where the rectangle has degenerated to the side AD and where M is the midpoint of AD. Again these degenerate rectangles are continuous limits of non-degenerate ones.
d) The line L_2 represents the cases where the rectangle has degenerated to the side AB and where M is any point on the line containing AB. It is thus hardly surprising that the model turns out to be algebraically false on the corresponding component $\mathfrak{p}_2$.
e) The line L_3 represents the cases where the rectangle has degenerated to the side AD and where M is any point on the line containing AD. Again the model is algebraically false on this component.
f) The line L_4 represents the case where the rectangle has degenerated to the point A and where M is any point in the plane. The model is algebraically true on this component, but this component does clearly not correspond to a meaningful geometric theorem. Notice that the cases with $M \neq A$ are not even continuous limits of actual geometric situations.

In the light of this example the question arises of how to avoid components on which a model is algebraically true but geometrically meaningless. To investigate this problem further we need more tools. They are developed in the next subsection.

6.7.C Optimal Hypothesis Ideals and Minimal Conditions

How about proving a theorem
without knowing which?
(from "Mathematical Nightmares")

In general, the radical of the hypothesis ideal $I_h(\mathcal{T})$ of a geometric statement is not prime, but since it is a radical ideal it can be expressed as the intersection of several prime ideals. One way to proceed could be first to compute $\sqrt{I_h(\mathcal{T})}$, then to determine its prime decomposition, and finally to check on which prime components of the hypothesis ideal the model $\mathcal{T}$ is algebraically true.

However, this approach is *impractical* for two reasons. The first reason is the complexity of computing the primary decomposition of the radical of an ideal. If you were brave enough to work out the details of Tutorial 79, you will certainly be aware of this. The second reason is even more important: is the difficulty of understanding the geometric meaning of some components. After a lengthy computation we might find out that we have proved a theorem, but we do not know which.

Another possibility which may happen is that the thesis polynomial does not belong to any of the prime components of the hypothesis ideal. Then the statement should be considered to be absolutely false. In Theorem 6.7.18 we shall see that it is possible to detect this case without computing the primary decomposition of the radical of the hypothesis ideal.

In the following we suppose we are given a statement in Euclidean geometry. We let $h_1, \ldots, h_r \in \mathbb{R}[x_1, \ldots, x_n]$ be polynomials expressing the hypotheses of the statement, and we let $t \in \mathbb{R}[x_1, \ldots, x_n]$ be its thesis polynomial. Now let K be the field of definition of the model $\mathcal{T} = (h_1, \ldots, h_r, t)$. Since the polynomial ring $P = K[x_1, \ldots, x_n]$ contains $\{h_1, \ldots, h_r, t\}$, we can perform all necessary computations in P. In particular, we shall use the hypothesis ideal $I_h(\mathcal{T}) = I_{h,\mathbb{R}}(\mathcal{T}) \cap P$. The following technical lemma is routine, but very useful for translating geometric conditions into algebra.

Lemma 6.7.13. *Let R be a Noetherian ring, let I and J be ideals in R, and let $f, g \in R \setminus \{0\}$.*

a) The following conditions are equivalent.
   1) We have $g \in \sqrt{I : f^\infty}$.
   2) We have $f \in \sqrt{I : g^\infty}$.
   3) We have $1 \in I : (fg)^\infty$.

b) We have $\sqrt{I :_R J^\infty} = \sqrt{I} :_R J = \sqrt{I} :_R \sqrt{J}$.

c) We have $I :_R J^\infty = (1)$ if and only if $J \subseteq \sqrt{I}$.

d) We have $f \in \sqrt{I :_R (I :_R f^\infty)^\infty}$.

e) We have $I :_R f^\infty \subseteq \sqrt{I}$ if and only if f is a non-zero divisor for $R/\sqrt{I}$.

Proof. First we prove a). We begin by showing that 1) implies 3). Since $g \in \sqrt{I : f^\infty}$, there exists a number $i \geq 0$ such that $g^i \in I : f^\infty$. Therefore there exists a number $j \geq 0$ such that $(gf)^j \in I$, and hence $1 \in I : (fg)^j$. To prove the converse implication, let $j \geq 0$ be a number with $1 \in I : (fg)^j$. Then we have $g^j \in I : f^\infty$, and thus $g \in \sqrt{I : f^\infty}$. The equivalence of 2) and 3) follows in the same way because condition 3) is symmetric in f and g.

Now let us prove the first equality of b). To show the inclusion "$\subseteq$", we choose an element $g \in \sqrt{I :_R J^\infty}$. Thus we have $g^i \in I :_R J^\infty$ for some $i \geq 0$. Hence it follows that $(gJ)^j \subseteq I$ for some $j \geq 0$, and therefore $gJ \subseteq \sqrt{I}$. This shows that we have $g \in \sqrt{I} :_R J$, as claimed. Conversely, let $g \in \sqrt{I} :_R J$. Then there is a number $k \geq 0$ such that $(gJ)^k \in I$. Thus we obtain $g \in \sqrt{I :_R J^k} \subseteq \sqrt{I : J^\infty}$.

To prove the second equality, it suffices to show $\sqrt{I} :_R J \subseteq \sqrt{I} :_R \sqrt{J}$, since the other inclusion is obvious. Let $g \in R$ be an element with $gJ \subseteq \sqrt{I}$. Then there is a number $i \geq 0$ such that $(gJ)^i \subseteq I$. Let $h \in \sqrt{J}$. Then we have $h^j \in J$ for some $j \geq 0$. Hence it follows that $(gh^j)^i \in I$, and therefore $gh \in \sqrt{I}$. Since $h \in \sqrt{J}$ was chosen arbitrarily, we get $g\sqrt{J} \subseteq \sqrt{I}$, and the claim follows.

It is clear that c) is a consequence of b) since $I :_R J^\infty = (1)$ is equivalent to $\sqrt{I :_R J^\infty} = (1)$. Thus we prove d) next. Let $\{g_1, \ldots, g_s\}$ be a system of generators of $I :_R f^\infty$. Then there is a number $i \geq 0$ such that $g_j f^i \in I$ for $j = 1, \ldots, s$. Therefore we have $f^i (I :_R f^\infty) \subseteq I$. Now $f^i \in I :_R (I :_R f^\infty)$, and the claim follows.

Finally we prove e). Suppose that $I :_R f^\infty \subseteq \sqrt{I}$. Then we see that we have $\sqrt{I :_R f^\infty} \subseteq \sqrt{I}$. Therefore b) yields $\sqrt{I} :_R f = \sqrt{I}$. Consequently, the

element f is a non-zero divisor for $R/\sqrt{I}$. To prove the converse implication, let $f \in R$ be a non-zero divisor for $R/\sqrt{I}$, i.e. an element with $\sqrt{I} :_R f = \sqrt{I}$. Then b) implies $\sqrt{I :_R f^\infty} = \sqrt{I}$ and thus $I :_R f^\infty \subseteq \sqrt{I :_R f^\infty} = \sqrt{I}$. □

Conditional truth of geometric theorems is defined as follows.

Definition 6.7.14. Let $\mathcal{T} = (h_1, \ldots, h_r, t)$ be a model for a geometric statement, and let $f \in P$.

a) We say that $\mathcal{T}$ (or the statement) is **algebraically true under the condition** $f \neq 0$ if we have $t \in \sqrt{I_h(\mathcal{T}) :_P f^\infty}$.
b) The ideal $I_c(\mathcal{T}) = I_h(\mathcal{T}) :_P t^\infty$ is called the **condition ideal** of the model $\mathcal{T}$ (or of the statement).
c) A condition $f \in P$ is called **trivial** if we have $f \in \sqrt{I_h(\mathcal{T})}$.
d) Let $\sqrt{I_h(\mathcal{T})} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$ with prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of P be the primary decomposition of $\sqrt{I_h(\mathcal{T})}$. The model $\mathcal{T}$ (or the statement) is said to be **absolutely false** if we have $t \notin \mathfrak{p}_i$ for $i = 1, \ldots, s$.

The following proposition explains the choices of these names.

Proposition 6.7.15. *Let $\mathcal{T} = (h_1, \ldots, h_r, t)$ be a model for a geometric statement, and let $f \in P$ be such that $\mathcal{T}$ is algebraically true under the condition $f \neq 0$.*

a) Every tuple $(a_1, \ldots, a_n) \in \mathbb{R}^n$ which is a zero of the hypothesis ideal $I_h(\mathcal{T})$ and for which $f(a_1, \ldots, a_n) \neq 0$, i.e. every instance of the statement which satisfies the hypotheses and the condition $f \neq 0$, is contained in the zero set of the thesis polynomial t.
b) We have $f \in \sqrt{I_c(\mathcal{T})}$. In other words, the radical of the condition ideal contains all conditions under which $\mathcal{T}$ is algebraically true.

Proof. To prove a), we choose $i \geq 0$ such that $t^i \in I_h(\mathcal{T}) :_P f^\infty$ and $j \geq 0$ such that $t^i f^j \in I_h(\mathcal{T})$. For every $(a_1, \ldots, a_n) \in \mathcal{Z}_{\mathbb{R}}(I_h(\mathcal{T})) \setminus \mathcal{Z}_{\mathbb{R}}(f)$, it follows from $(t^i f^j)(a_1, \ldots, a_n) = 0$ that we have $t(a_1, \ldots, a_n) = 0$, as we wanted to show. Claim b) follows from the lemma because $t \in \sqrt{I_h(\mathcal{T})} :_P f^\infty$ is equivalent to $f \in \sqrt{I_h(\mathcal{T})} :_P t^\infty = \sqrt{I_c(\mathcal{T})}$. □

Of course, we could also have defined $\sqrt{I_c(\mathcal{T})}$ to be the condition ideal. However, the definition we use has the advantage that it avoids the potentially costly computation of a radical while Theorem 6.7.18 below is valid nevertheless. Let us have a look at some condition ideals.

Example 6.7.16. In the setting of Theorem 6.7.3, the condition ideal is $I_c(\mathcal{T}) = (a^3 - b^3) :_P (a - b)^\infty = (a^2 + ab + b^2)$. Hence this theorem is algebraically true under the condition $a^2 + ab + b^2 \neq 0$. Since the polynomial $a^2 + ab + b^2$ has no real zeros except $(0, 0)$, we conclude that the theorem is algebraically true over $\mathbb{R}$.

Next we determine the condition ideal in the case of the theorem on diagonal bisection.

Example 6.7.17. In the setting of Theorem 6.7.4, we have $I_h(\mathcal{T}) = (h_1, h_2)$ where $h_1 = x_1x_4 - x_2x_3$ and $h_2 = x_1x_2 - x_2x_3 - x_1x_4$. The natural non-degeneracy condition is $x_1x_2 \neq 0$. Under this condition, the theorem is algebraically true because the ideal $I_h(\mathcal{T}) : (x_1x_2)^\infty$ is equal to the ideal $(x_1 - 2x_3, x_2 - 2x_4)$ which contains the two thesis polynomials $t_1 = x_1^2 + x_2^2 - 2x_1x_3 - 2x_2x_4$ and $t_2 = x_1^2 - x_2^2 - 2x_1x_3 + 2x_2x_4$. The two polynomials t_1 and t_2 yield the same condition ideal $I_c(\mathcal{T}) = I_h(\mathcal{T}) :_P t_1^\infty = I_h(\mathcal{T}) :_P t_2^\infty = (x_1x_2, x_1x_4, x_2x_3, x_3x_4)$. Thus the theorem is also algebraically true under the condition $x_3x_4 \neq 0$, i.e. under the condition that the point M is not contained in one of the coordinate axes. This agrees with our analysis in Example 6.7.12.

Our next theorem provides efficient ways for checking whether a statement is algebraically true or absolutely false.

Theorem 6.7.18. *Let $\mathcal{T} = (h_1, \ldots, h_r, t)$ be a model of a statement in Euclidean geometry, let K be its field of definition, and let $P = K[x_1, \ldots, x_n]$.*

a) The model $\mathcal{T}$ is algebraically true if and only if the following equivalent conditions hold true.

1) We have $I_c(\mathcal{T}) = (1)$.

2) We have $\sqrt{I_h(\mathcal{T}) :_P I_c(\mathcal{T})^\infty} = \sqrt{I_h(\mathcal{T})}$

b) The model $\mathcal{T}$ is absolutely false if and only if the following equivalent conditions hold true.

1) We have $I_c(\mathcal{T}) \subseteq \sqrt{I_h(\mathcal{T})}$.

2) We have $I_h(\mathcal{T}) :_P I_c(\mathcal{T})^\infty = (1)$.

c) If the model $\mathcal{T}$ is neither algebraically true nor absolutely false, we have a chain of strict inclusions

$$\sqrt{I_h(\mathcal{T})} \subset \sqrt{I_h(\mathcal{T}) :_P I_c(\mathcal{T})^\infty} \subset (1)$$

Proof. First we prove a). By Proposition 6.7.9, the model $\mathcal{T}$ is algebraically true if and only if $t \in \sqrt{I_h(\mathcal{T})}$. Therefore Lemma 6.7.13.c shows that $\mathcal{T}$ is algebraically true if and only if 1) holds true. Since it is clear that 1) implies 2), it remains to show that 2) implies that $\mathcal{T}$ is algebraically true. This follows from Lemma 6.7.13.d.

Now we prove b). By Lemma 6.7.13.e, the model $\mathcal{T}$ is absolutely false if and only if 1) holds. The equivalence of 1) and 2) is clear. Finally, we note that the first inclusion in c) follows from a) and the second inclusion follows from b). □

This theorem indicates that most of the information about the validity of $\mathcal{T}$ is contained in the ideal $I_h(\mathcal{T}) :_P I_c(\mathcal{T})^\infty$. In particular, we see that if $\mathcal{T}$

is neither algebraically true nor absolutely false, the revised model $\mathcal{T}'$ whose hypothesis ideal is $I_h(\mathcal{T}') = I_h(\mathcal{T}) :_P I_c(\mathcal{T})^\infty$ and whose thesis polynomial is t is algebraically true. But we can provide an even more detailed description of this hypothesis ideal.

Definition 6.7.19. The ideal $I_{opt}(\mathcal{T}) = I_h(\mathcal{T}) :_P I_c(\mathcal{T})^\infty \subseteq P$ is called the **optimal hypothesis ideal** of $\mathcal{T}$.

In order to explain why this ideal deserves its name, we need a further technical result.

Lemma 6.7.20. *Let R be a Noetherian ring, let I be an ideal in R, and let $g \in R$. Let $\sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s \cap \mathfrak{p}_{s+1} \cap \cdots \cap \mathfrak{p}_{s+t}$ be the prime decomposition of $\sqrt{I}$, and assume that $g \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$ and $g \notin \mathfrak{p}_i$ for $i = s+1, \ldots, s+t$.*

a) We have $\sqrt{I :_R g^\infty} = \mathfrak{p}_{s+1} \cap \cdots \cap \mathfrak{p}_{s+t}$.

b) We have $\sqrt{I :_R (I :_R g^\infty)^\infty} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$.

Proof. To show a), we recall from Lemma 6.7.13.b that we have $\sqrt{I :_R g^\infty} = \sqrt{I} :_R g$. Now it is easy to check that

$$(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{s+t}) :_R g = \bigcap_{i=1}^{s+t} (\mathfrak{p}_i :_R g) = \mathfrak{p}_{s+1} \cap \cdots \cap \mathfrak{p}_{s+t}$$

because $\mathfrak{p}_i :_R g = \mathfrak{p}_i$ if $g \notin \mathfrak{p}_i$ and $\mathfrak{p}_i :_R g = R$ otherwise.

Next we prove b). By Lemma 6.7.13.b, we have $\sqrt{I :_R (I :_R g^\infty)^\infty} = \sqrt{I} :_R \sqrt{(I :_R g^\infty)}$. Hence the claim follows from a) and the equality

$$(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{s+t}) :_R (\mathfrak{p}_{s+1} \cap \cdots \cap \mathfrak{p}_{s+t}) = \bigcap_{i=1}^{s+t} (\mathfrak{p}_i :_R (\mathfrak{p}_{s+1} \cap \cdots \cap \mathfrak{p}_{s+t})) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$$

which is a consequence of the fact that $\mathfrak{p}_i :_R (\mathfrak{p}_{s+1} \cap \cdots \cap \mathfrak{p}_{s+t})$ is equal to $\mathfrak{p}_i$ for $i = 1, \ldots, s$ and equal to R for $i = s+1, \ldots, s+t$. □

Now we are ready to discuss the optimality of the optimal hypothesis ideal.

Proposition 6.7.21. *Let $\sqrt{I_h} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_{s+t}$ be the prime decomposition of the radical of the hypothesis ideal of $\mathcal{T}$, and let the numbering of the ideals $\mathfrak{p}_i$ be chosen such that $t \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$ and $t \notin \mathfrak{p}_i$ for $i = s+1, \ldots, s+t$.*

a) We have $\sqrt{I_{opt}(\mathcal{T})} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$. Hence the prime components of $\sqrt{I_{opt}(\mathcal{T})}$ are exactly the components on which $\mathcal{T}$ is algebraically true.

b) The model $\mathcal{T}$ is algebraically true if and only if $\sqrt{I_{opt}(\mathcal{T})} = \sqrt{I_h(\mathcal{T})}$.

c) The model $\mathcal{T}$ is absolutely false if and only if $I_{opt}(\mathcal{T}) = (1)$.

Proof. To prove a), we use part b) of the lemma to get $\sqrt{I_{opt}(\mathcal{T})} = \sqrt{I_h(\mathcal{T}) :_P I_c(\mathcal{T})^\infty} = \sqrt{I_h(\mathcal{T}) :_P (I_h(\mathcal{T}) :_P t^\infty)^\infty} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_s$. Claims b) and c) follow immediately from a) and Theorem 6.7.18. □

At first glance this could be the final point of our investigation. However, if we do the computation in the case of the theorem on diagonal bisection 6.7.4, a surprise is in store for us.

Example 6.7.22. In the setting of Theorem 6.7.4, the optimal hypothesis ideal is $I_{opt}(\mathcal{T}) = (I_h :_P (I_h :_P (t_1, t_2)^\infty)^\infty) = (x_1^2 - 2x_1x_3,\ x_1x_2 - 2x_1x_4,\ x_2^2 - 2x_2x_4,\ x_2x_3 - x_1x_4)$. But what is the geometric meaning of these hypotheses? We have proved a theorem but we do not know exactly which! Suppose that we are able to compute the primary decomposition of the ideal $\sqrt{I_{opt}}$. We get the two components $\mathfrak{p}_1 = (x_1 - 2x_3,\ x_2 - 2x_4)$ and $\mathfrak{p}_4 = (x_1,\ x_2)$. As we observed before, we know how to interpret $\mathfrak{p}_4$ but it is not clear what $\mathfrak{p}_1$ means geometrically.

This example suggests that it could be better to describe the validity of a geometric statement not by listing the components on which it is true, but by excluding the components on which it is algebraically false. The advantage is that we can do that by excluding a hypersurface, i.e. by imposing a single non-vanishing condition. The disadvantage is that we could inadvertently throw away a component on which the theorem is algebraically true, for instance if we impose the condition $x_1x_2 \neq 0$ in the Diagonal Bisection Theorem 6.7.4. Such is life.

In any event, it is worthwhile examining the effect of various conditions further. The ideal $I_c(\mathcal{T})$ may contain polynomials which are also elements of $\sqrt{I_h(\mathcal{T})}$ and other polynomials which are not. A polynomial f of the first kind should be considered useless since it yields $I_h(\mathcal{T}) :_P f^\infty = (1)$. In this case the statement that $\mathcal{T}$ holds under the condition $f \neq 0$ is trivially true and therefore boring. A polynomial f of the second kind yields a proper ideal $\sqrt{I_h(\mathcal{T}) :_P f^\infty} = \sqrt{I_h(\mathcal{T})} :_P f$ which contains $\sqrt{I_h(\mathcal{T})}$ strictly. Therefore the condition $f \neq 0$ excludes some prime components of $\sqrt{I_h(\mathcal{T})}$ but not all. The problem is that it possibly excludes some prime components on which the statement is algebraically true. Nevertheless, there always exist polynomials f of the second kind such that the condition $f \neq 0$ yields exactly the optimal hypothesis ideal. Aren't they the optimum we could hope for? Unfortunately not. Experience shows that these "optimal" polynomials rarely admit a humanly comprehensible geometric interpretation.

To improve our chances of finding conditions which have a nice geometric interpretation and also yield a theorem which is algebraically true on as many components as possible, we introduce the following definition.

Definition 6.7.23. Let $S \subseteq I_c(\mathcal{T})$. A polynomial $f \in S$ is called a **minimal condition in** S if $I_h :_P f^\infty$ is minimal with respect to inclusion in the set of ideals $\{I_h :_P g^\infty \mid g \in S\}$.

Is it always possible to find non-trivial minimal conditions? The following proposition provides a case when this is true.

Proposition 6.7.24. *Let G be a set of generators of the condition ideal $I_c(\mathcal{T})$ of a model $\mathcal{T}$ of a geometric statement. If $\mathcal{T}$ is not absolutely false then every minimal condition in G is non-trivial.*

Proof. Since $\mathcal{T}$ is not absolutely false, Theorem 6.7.18.b implies that $I_c(\mathcal{T})$ is not contained in $\sqrt{I_h(\mathcal{T})}$. Hence there is at least one non-trivial condition $f \in G$. Then we have $I_h(\mathcal{T}) :_P f^\infty \subset I_h(\mathcal{T}) :_P g^\infty = (1)$ for every trivial condition $g \in G$. Therefore g is not a minimal condition in G. □

Our goal is to find as many minimal conditions in some set of generators of the condition ideal as possible. In this way we increase our chances of finding one for which we have a geometric interpretation. In this sense the following algorithm automates the process of proving a geometric theorem as much as possible. Its purpose is to find an optimal set of hypotheses and a set of minimal conditions under which the theorem is algebraically true. Although it may exclude some components on which the theorem is true, these are usually components corresponding to degenerate cases.

Theorem 6.7.25. (The Automatic Prover)
Let $\mathcal{T} = (h_1, \ldots, h_r, t)$ be a model of a statement in Euclidean geometry. Let K be the field of definition of $\mathcal{T}$, let $P = K[x_1, \ldots, x_n]$, and let $I_h(\mathcal{T})$ be the ideal $(h_1, \ldots, h_r)$. Consider the following sequence of instructions.

1) *Compute the ideal $I_c(\mathcal{T}) = I_h(\mathcal{T}) :_P t^\infty$. If $1 \in I_c(\mathcal{T})$, return* `"The model is algebraically true."` *and stop.*
2) *Let $G \subseteq P \setminus \{0\}$ be a set of generators of $I_c(\mathcal{T})$. For every $f \in G$, compute the ideal $I_f = I_h(\mathcal{T}) :_P f^\infty$. If $1 \in I_f$ for all $f \in G$, return* `"The model is absolutely false."` *and stop.*
3) *Determine the polynomials $g_1, \ldots, g_s \in G$ for which I_{g_i} is minimal with respect to inclusion in the set of ideals $\{I_f \mid f \in G\}$, and let S be the set $\{g_1, \ldots, g_s\}$.*
4) *Compute the ideal $I_{opt}(\mathcal{T}) = I_h(\mathcal{T}) :_P I_c(\mathcal{T})$. Then return the pair $(S, I_{opt}(\mathcal{T}))$ and stop.*

This is an algorithm which decides whether $\mathcal{T}$ is algebraically true or absolutely false. If $\mathcal{T}$ is neither algebraically true nor absolutely false, the algorithm finds a set of minimal conditions for $\mathcal{T}$ and the optimal hypothesis ideal.

Proof. Since finiteness is clear, it suffices to prove correctness. By Theorem 6.7.18.a, the model $\mathcal{T}$ is algebraically true if and only if $1 \in I_c(\mathcal{T})$. Thus step 1) gives the correct answer.

In step 2) we check whether we have $1 \in I_c(\mathcal{T}) :_P f^\infty$ for all $f \in G$. This is equivalent to $1 \in \sqrt{I_h(\mathcal{T}) :_P f^\infty} = \sqrt{I_h(\mathcal{T}) :_P f}$, and therefore to $f \in \sqrt{I_h(\mathcal{T})}$. Hence step 2) checks whether we have $I_c(\mathcal{T}) \subseteq \sqrt{I_h(\mathcal{T})}$. By Theorem 6.7.18.b, this holds if and only if $\mathcal{T}$ is absolutely false. Consequently, step 2) gives the correct answer.

If $\mathcal{T}$ is neither algebraically true not absolutely false, steps 3) and 4) do nothing but compute the minimal conditions and the optimal hypothesis ideal for $\mathcal{T}$ via their definitions. □

The result of the automatic prover depends on the choice of the system of generators of $I_c(\mathcal{T})$ in step 2). This choice influences our chances of finding minimal conditions in step 3) which have a meaningful geometric interpretation. Of course, we could also compute the optimal conditions, but as we mentioned before, the chances that these have reasonable geometric interpretations are slim. Thus the usability of the result of the algorithm depends on a certain amount of human intervention. It is really a *semiautomatic prover*. The following optional preprocessing step can be used to change the theorem we try to prove another one for which the Automatic Prover works better.

Remark 6.7.26. Suppose we insert in the Automatic Prover the following step 0).

0) (Optional preprocessing)
Let $f \in P$ be the product of all degeneracy conditions to be excluded *a priori*. Replace $I_h(\mathcal{T})$ be the ideal $I_h(\mathcal{T}) :_P f^\infty$. Let $\mathcal{T}'$ be a model given by a system of generators this new hypothesis ideal and the thesis t.

If we then apply the further steps to the model $\mathcal{T}'$, we get an algorithm which decides whether $\mathcal{T}'$ is algebraically true or absolutely false. For instance, in Theorem 6.7.10 it is obvious that we should assume $x_1 \neq 0$. Thus we can substitute the old hypothesis ideal $I_h = (x_1^2 - 3x_1x_2)$ with the new hypothesis ideal $I_{h'} = I_h :_P x_1^\infty = (x_1 - 3x_2)$ and get immediately an algebraically true model.

So, what is the upshot of this section? It has become clear that computers are best at computing. Proving theorems is not really an "automatic" procedure and contains several steps which cannot be left to a computer: modelling the geometric setting, finding reasonable non-degeneracy conditions, and determining whether the computed minimal or optimal conditions have a reasonable geometric interpretation seem to be activities which are difficult to automate.

Are we now ready for the rainbow and the sunshine? No, first we have to weather one last tutorial. One last gust of rain, one last battle with program code and semiautomatic proofs. But, hey, isn't that what we really love?

I have a beautiful proof
of the incorrectness of your theorem,
but this margin is too small for it.
(Anonymous)

Tutorial 99: To Prove or Not to Prove

Proof by general agreement: "All in favor?"
Proof by tautology: "It's true because it's true."
Proof by plausibility: "It sounds good, it must be true."
Proof by intimidation: "Don't be stupid; of course it's true."
Proof by generalization: "It works for 17, so it works for all integers."
Proof by authority: "Don Knuth says it's true, so it must be!"
Proof by convenience: "It would be nice if it were true."
Proof by insignificance: "Who really cares, anyway?"
Proof by necessity: "It had better be true."

(from "Ontological Proofs of the Existence of Good Provers")

In this last tutorial of the book, we change our strategy. Instead of asking to write CoCoA functions, we provide you with some. But then it is your job to analyze them and to use them to study interesting examples. We start with some CoCoA functions which transform the algorithm of Theorem 6.7.25 into executable code. The goal is to find "good" minimal conditions under which a geometric statement is algebraically true. We hope that with the help of these functions you can prove ... something.

Computing a Minimal Set of Conditions

```
Define MinimalConditions(L)
  MinConditions := [];
  Foreach ElementOfL In L Do
    Inserted := FALSE;
    I := 1;
    While I <= Len(MinConditions) And Not Inserted Do
      If MinConditions[I].Ideal = ElementOfL.Ideal Then
        Append(MinConditions[I].Polys, ElementOfL.Poly);
        Inserted := TRUE;
      ElsIf MinConditions[I].Ideal > ElementOfL.Ideal Then
        MinConditions[I] := Record(Ideal=ElementOfL.Ideal,
                                   Polys=[ElementOfL.Poly]);
        Inserted := TRUE;
      ElsIf MinConditions[I].Ideal < ElementOfL.Ideal Then
        Inserted := TRUE;
      EndIf;
      I := I+1;
    EndWhile;
    If Not Inserted Then
      Append(MinConditions, Record(Ideal=ElementOfL.Ideal,
                                   Polys=[ElementOfL.Poly]));
    EndIf;
  EndForeach;
  Return [X.Polys | X In MinConditions]
EndDefine;
```

The Automatic Prover

```
Define AutoProver(Hypotheses,Thesis)
  ConditionIdeal := Saturation(Ideal(Hypotheses),Ideal(Thesis));
  If ConditionIdeal = Ideal(1) Then
    Return Record(Statement=TRUE);
  EndIf;
  Conditions := Gens(ConditionIdeal);
  ConditionIdealList :=
    [ Record(Ideal=Saturation(Ideal(Hypotheses),Ideal(C)),
             Poly=C) | C In Conditions];
  If [ X In ConditionIdealList | X.Ideal <> Ideal(1) ] = [] Then
    Return  Record(Statement=FALSE, Conditions=[]);
  EndIf;
  Return Record(Statement=FALSE,
                Conditions=MinimalConditions(ConditionIdealList),
                OptimalHypothesisIdeal=IntersectionList([I.Ideal |
                                    I In ConditionIdealList]));
EndDefine;
```

Now let us start proving! First we prove that these functions do what they are supposed to do.

a) Explain how the above CoCoA functions implement the steps of the Automatic Prover 6.7.25.

The Golden Mean Revisited

Next we go back to the setting of the theorem about the golden mean 6.7.8. We begin with the model given in the *"Automatic Proof 1"*.

b) In the preprocessing phase, exclude the possibility that the segment AB degenerates to a point. Find the new hypothesis ideal $I_h(\mathcal{T}')$.

c) Using the function `AutoProver(...)`, show that the theorem is neither algebraically true not completely false. Find a minimal set of conditions and the optimal hypothesis ideal.

d) Show that $f = \{2x_1^3 + (1+\sqrt{5})x_1^2x_4 - (3-\sqrt{5})x_1x_4^2 + (1-\sqrt{5})x_4^3\}$ is a minimal condition for $\mathcal{T}'$ and that there exists a factorization $f = (2x_1 - (1-\sqrt{5})x_4)(x_1 + \frac{1}{2}(1-\sqrt{5})x_4)(x_1 + \frac{1}{2}(1+\sqrt{5})x_4)$.
Hint: Use an elimination ordering for $\{x_2, x_3\}$.

e) Conclude that the theorem is true under the condition that we have $x_1 \notin \{-\frac{1}{2}(1+\sqrt{5})x_4, \pm\frac{1}{2}(1-\sqrt{5})x_4\}$. What is the geometric meaning of this condition?

It is also possible to use the model described in the *"Automatic Proof 2"* of Theorem 6.7.8.

f) Show that the condition ideal is $I_c(\mathcal{T}) = (f_1, f_2, f_3)$ with polynomials $f_1 = x_1^2 + x_1x_4 - x_4^2$, $f_2 = 5x_3 - 2x_1 - x_4$, and $f_3 = 5x_2 - 4x_1 - 2x_4$.

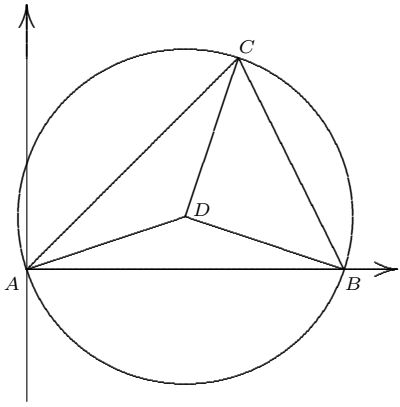
g) Prove that each condition f_i is minimal and that all three of them yield the same saturation ideal $I_h(\mathcal{T}) :_P f_i^\infty$.

h) Show that the theorem is algebraically true under the condition that we have $x_1 \notin \{-\frac{1}{2}(1+\sqrt{5})x_4,\ -\frac{1}{2}(1-\sqrt{5})x_4\}$. Compare this result with e). *Hint:* Use $x_1^2 + x_1x_4 - x_4^2 = (x_1 + \frac{1}{2}(1+\sqrt{5})x_4)(x_1 + \frac{1}{2}(1-\sqrt{5})x_4)$.

Isosceles and Right-Angled Triangles

Geometric Theorem. *For every triangle which is either isosceles or right-angled, the center of the circumscribed circle belongs to one of the sides of the triangle.*

Automatic Proof: First we introduce a Cartesian coordinate system as in the following picture.



In this coordinate system we have $A = (0,0)$, $B = (x_1,0)$, $C = (x_2,x_3)$, and $D = (x_4,x_5)$. Our next task is to construct a suitable model.

i) Show that the hypothesis $AD = BD$ yields $h_1 = 2x_1x_4 - x_1^2$, and the hypothesis $AD = CD$ yields $h_2 = x_2^2 + x_3^2 - 2x_2x_4 - 2x_3x_5$.

j) Without loss of generality assume that the triangle is isosceles or right-angled with a right angle at C. Show that the hypothesis "$AC = BC$ or $AC \perp BC$" yields $h_3 = x_1^3x_2 - 3x_1^2x_2^2 + 2x_1x_2^3 - x_1^2x_3^2 + 2x_1x_2x_3^2$.

k) Prove that the thesis polynomial is $t = x_1x_5$ and that the field of definition is $\mathbb{Q}$.

l) Using the function `AutoProver(...)`, show that the theorem is neither algebraically true not completely false. Find a minimal set of conditions and the optimal hypothesis ideal.

m) Show that $\{x_3x_4 - x_3x_2,\ x_3^3 - x_3x_4^2 - 2x_3^2x_5\}$ is a minimal set of conditions, and that the two conditions yield the same new hypothesis ideal. Conclude that the original theorem becomes true under the conditions that $x_2 \neq x_4$ and $x_3 \neq 0$. What is the correct formulation of the theorem?

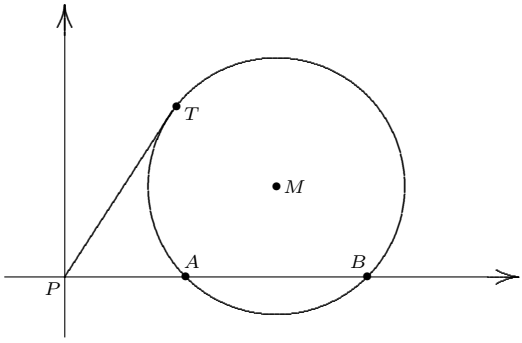
n) Now let us introduce a preprocessing step. Suppose you want to avoid the cases where the triangle degenerates to a line segment. Show that this can be done by replacing $I_h(\mathcal{T})$ with $I_h(\mathcal{T}') = I_h(\mathcal{T}) :_P (x_1x_3)^\infty$ and by using the thesis polynomial $t' = x_5$.

o) Using the function `AutoProver(...)`, show that the new model $\mathcal{T}'$ is neither algebraically true nor completely false. Find a minimal set of conditions and the optimal hypothesis ideal.
p) Is it possible to interpret the optimal hypothesis ideal of $\mathcal{T}'$ geometrically? Under which additional conditions is $\mathcal{T}'$ algebraically true?

Tangents and Secants to a Circle

Geometric Theorem. *Let P be a point outside a circle C, let T be the point of contact of a tangent line to C which contains P, and let A and B be the points of intersection of a secant line of C through P. Then we have $PA \cdot PB = (PT)^2$.*

Automatic Proof: First we introduce a Cartesian coordinate system as in the following picture.



Let M be the center of the circle C. Let the coordinates of the points in the picture be $M = (x_1, y_1)$, $T = (x_2, y_2)$, $A = (x_3, 0)$, and $B = (x_4, 0)$.

q) Show that one model for this statement is $\mathcal{T} = (h_1, h_2, h_3, t)$ where $h_1 = (x_2 - x_1)^2 + (y_2 - y_1)^2 - (x_3 - x_1)^2 - y_1^2$, $h_2 = (x_3 - x_1)^2 - (x_4 - x_1)^2$, $h_3 = x_2(x_2 - x_1) + y_2(y_2 - y_1)$, and $t = x_2^2 + y_2^2 - x_3 x_4$.
r) Prove that the field of definition of this model is $\mathbb{Q}$. Then use the Automatic Prover to show that the model is neither algebraically true nor completely false, and that a minimal set of conditions is $\{x_3 - x_4\}$.

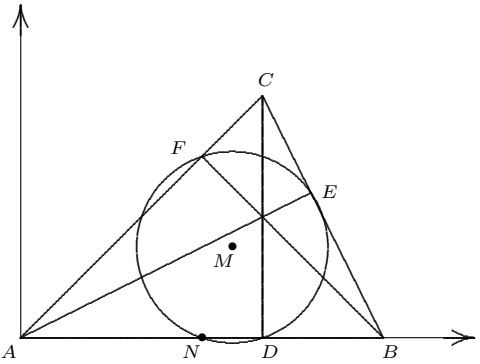
This result comes somehow as a little surprise. It means that the model is false on the component corresponding to $A = B$, i.e. when we do not specify that A and B are two *distinct* points of intersection of the secant line with the circle. This is a typical situation where it is very easy to overlook a degeneracy condition.

Feet and Midpoints

Geometric Theorem. *In every triangle the circle passing through the feet of the three perpendiculars intersects the sides of the triangle in their midpoints.*

Automatic Proof: First we introduce a Cartesian coordinate system and label the points as follows. We let A, B, C be the vertices of the triangle, we let

D, E, F be the feet of the perpendiculars, we let M be the center of the circle through the feet of the perpendiculars, and we let N be the midpoint of the side AB. By symmetry, it suffices to prove the result for the midpoint of just one side.



To begin with, we let the coordinates of the various points be given by $A = (0,0)$, $B = (x_1,0)$, $C = (x_2,x_3)$, $D = (x_2,0)$, $E = (x_4,x_5)$, $F = (x_6,x_7)$, $M = (x_8,x_9)$, and $N = (x_1/2,0)$. As usual, the next step is to translate the geometric setting into hypothesis and thesis polynomials.

s) Show that $F \in AC$ yields the polynomial $h_1 = -x_3x_6+x_2x_7$, $AC \perp FB$ yields the polynomial $h_2 = x_1x_2 - x_2x_6 - x_3x_7$, $E \in CB$ yields the polynomial $h_3 = -x_1x_3 + x_3x_4 + x_1x_5 - x_2x_5$, $AE \perp BC$ yields the polynomial $h_4 = -x_1x_4+x_2x_4+x_3x_5$, $DM = EM$ yields the polynomial $h_5 = -x_2^2 + x_4^2 + x_5^2 + 2x_2x_8 - 2x_4x_8 - 2x_5x_9$, and $DM = FM$ yields the polynomial $h_6 = x_2^2 - x_6^2 - x_7^2 - 2x_2x_8 + 2x_6x_8 + 2x_7x_9$.

t) Show that the thesis $DM = MN$ corresponds to the thesis polynomial $t = 1/4x_1^2 - x_2^2 - x_1x_8 + 2x_2x_8$. Deduce that the field of definition of this model is $\mathbb{Q}$.

To simplify the analysis, we suggest that in the preprocessing phase you exclude some degenerate cases.

u) Explain that, to exclude the possibility that the triangle degenerates to a line segment, it suffices to replace the hypothesis ideal by the ideal $I_h(\mathcal{T}') = (h_1,\ldots,h_6) :_P (x_1x_3)^\infty$.

v) Using the Automatic Prover, show that the theorem is neither algebraically true nor completely false and that a minimal set of conditions is $\{x_2x_5 - x_5x_6\}$.

w) Conclude that the theorem is algebraically true if $x_5 \neq 0$ and $x_2 \neq x_6$. What is the geometric meaning of these conditions?

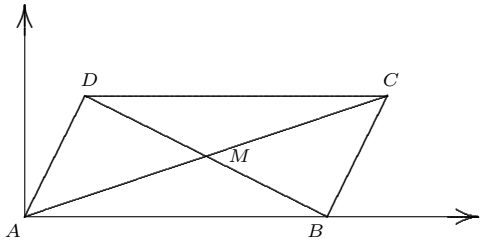
x) Compute the optimal hypothesis ideal of $\mathcal{T}'$. Can you interpret its generators geometrically?

A Strange Parallelogram

Our last example features an automatic proof of a really strange statement. Of course, the Automatic Prover doesn't care.

Geometric Theorem. *Given a parallelogram $ABCD$, the intersection point of the diagonals lies on the side AB.*

Automatic Proof: First we introduce Cartesian coordinates as in the following picture.



Next we write $A = (0,0)$, $B = (x_1,0)$, $C = (x_2,x_3)$, $D = (x_4,x_5)$, and $M = (x_6,x_7)$ where M denotes the intersection point of the diagonals. Now we start the semiautomatic process.

y) Show that the hypothesis $AB \parallel CD$ yields the polynomial $h_1 = -x_1x_3 + x_1x_5$, the hypothesis $AD \parallel BC$ yields the polynomial $h_2 = -x_3x_4 - x_1x_5 + x_2x_5$, the hypothesis $M \in AC$ yields the polynomial $h_3 = -x_3x_6 + x_2x_7$, and the hypothesis $M \in BD$ yields the polynomial $h_4 = -x_1x_5 + x_5x_6 + x_1x_7 - x_4x_7$.

z) Prove that the thesis polynomial is $t = x_7$. Using the Automatic Prover, show that the theorem is neither algebraically true nor completely false. Compute the optimal hypothesis ideal and a minimal set of conditions. Can you interpret the results geometrically? Conclude that the statement is algebraically true for parallelograms which degenerate to a line segment.

The trouble with Automatic Theorem Proving *is over.*

A. The ABC of CoCoA

A: *Writing a good program*
is like writing a good paper,
but a program also needs to be fast.
(John **A**bbott)

B*: Writing a good program*
is like writing a good paper,
but a compiler is a lot fussier than a referee.
(Anna Maria **B**igatti)

C*: In mathematics*
important things are very simple,
but simple things are very difficult.
(Massimo **C**aboara)

Since the first volume of this book appeared, the computer algebra system CoCoA has evolved further and many new features and functions have been added. In this appendix we bring you up-to-date and give you more hints on how to make the most out of the program. First we recapitulate the crucial information: you can download CoCoA freely from the web page

```
http://cocoa.dima.unige.it/
```

Not only will you find there a download area with versions of the program for various operating systems, but you can also access a large amount of additional material: installation instructions, information about CoCoA conferences and the international CoCoA schools, links to the CoCoA discussion groups, and so on.

Before getting down to the nitty-gritty details of CoCoA usage and CoCoA programming, let us delve a bit into the philosophy of CoCoA. If you have tried your hand at some of our 99 tutorials, you will already have experienced one of the main purposes of CoCoA, namely that of providing a user-friendly and easily accessible tool for teaching Computational Commutative Algebra. A further goal is to assist mathematicians in their research. Even if they are not experts in computer programming it enables them to access the power and versatility of a modern computer algebra system without having to create machine-language-like code. For instance, in CoCoA a loop is created by typing

```
For I:=1 To N Do <Commands> EndFor;
```

rather than something like

```
for(i=1;i<=n;i++){<Commands>}
```

And what happens if you are past the prototyping stage? Suppose you want to implement a function which is not interpreted but compiled and executed at the same speed as the built-in functions. With most computer algebra systems, you have reached the end of the line. Their source code is proprietary or incomprehensible. Not so with CoCoA: the latest version, CoCoA 5, is available as a C++ library, ready for you to expand or include in your own application. A detailed discussion of the CoCoA 5 library would not only exceed the scope of this appendix, it would also violate the down-to-earth spirit of this book. However, you can easily obtain it from the above web site.

In the next two appendices, we are going to discuss the following topics:

- how to use the graphical interface of CoCoA
- further tips and tricks for program development
- additional CoCoA programming techniques
- how to use CoCoA in your research
- how to interpret and use the parser's error messages

B. One Graphical Interface for Everybody

We are M CENSORED *t.*
Resistance is futile.
You will be assimilated.
(Anonymous)

Whether you have a computer operating under Linux, Macintosh OS X, or a current version of the Microsoft Windows operating system, there is a version of CoCoA whose graphical interface behaves essentially the same. In this section we describe this interface, including some of its lesser known but useful features, and give you hints how to employ it to full advantage.

After installing the graphical interface of CoCoA, you normally start it by double-clicking on its desktop symbol. You are greeted by a text similar to

```
------------------------------------------------------
---           ___/       ___/         \             ---
--           /     _ \  /     _ \    , \             --
--           \    |   | \    |   |  ___ \            --
---          ____, __/  ____, __/ _/    _\          ---
------------------------------------------------------
--     Version      : 4.4                             --
--     Online Help  : type  ?   or   ?keyword         --
--     Web site     : http://cocoa.dima.unige.it      --
------------------------------------------------------
```

and a line telling you about the current base ring. In fact, this message is displayed in the upper part of a new window. This region is called the *output pane*. Not surprisingly, the lower region is called the *input pane*. Initially the input pane sports the title `Interactive (0)`. Let us discuss the working of these panes separately.

B.1 The Output Pane

As you may already have guessed, the purpose of the output pane is to display the results of CoCoA's computations. For instance, if we type `1+1;` in the input pane and hit `<Ctrl + Enter>`, we get the output

```
1+1;
2
------------------------------
```

in the output pane. It shows that CoCoA passed what is affectionately known as its "sanity test". In the output pane you cannot do much editing, but you can save its contents to a file (using the command `Save Output As` in the `File` menu), or you can copy and paste text from the output pane to the input pane. To achieve the latter task, mark the text in the output pane using the mouse, hit `<Ctrl + C>`, focus on the input pane by clicking on it, and hit `<Ctrl + V>`. That's it!

B.2 The Input Pane

Enter any 11-digit prime number to continue...
(Anonymous)

The input pane offers a much more varied environment than the output pane. Its initial page is part of what is called the *interactive document*. You can open up to nine further documents, called CoCoA *documents*, which have a slightly different behaviour.

The interactive document consists of one or more pages. After typing some CoCoA commands in one of these pages, you can pass them to CoCoA's parser in several ways: by pressing `<Ctrl + Enter>`, by clicking on the gear-wheel in the toolbar, or by using the entry `Execute current command set` in the `CoCoA` menu. In each case CoCoA will perform the required computations and open a new interactive page.

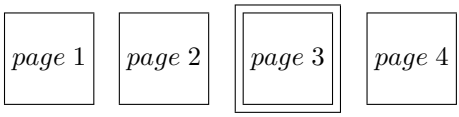
A CoCoA document consists of only one page. You can execute the whole page in the same way you execute an interactive page, or you can mark part of the page with the mouse and execute it analogously. No new page is created after you execute a command set in a CoCoA document. You can save CoCoA documents to a file using `<Ctrl + S>`, and you can read them back into your CoCoA session by pressing `<Ctrl + O>` and selecting the desired file. If you have several documents open, you can move from one to the other by clicking on the appropriate tab above the input pane or via the command `<Alt + N>` where `N` is the number of the document.

In each page you have all the usual editing commands available, including `<Ctrl + C>` for copying the selected text to the clipboard, `<Ctrl + X>` for cutting the selected text and moving it to the clipboard, `<Ctrl + V>` for pasting the text from the clipboard, and `<Ctrl + Q>` for quitting the application.

B.3 The History

Those who fail to learn history
are doomed to repeat it;
those who fail to learn history correctly –
why, they are simply doomed.
(Achem Dro'hm, C.Y. 4971)

The idea underlying the division of the interactive document into separate pages is to introduce the concept of command history. You can imagine the history in the following way:



where the doubly framed rectangle represents the *history cursor*, i.e. the current position in the history. The history cursor can be moved using the keys `<Alt + Left Arrow>` and `<Alt + Right Arrow>` or the corresponding entries in the `CoCoA` menu. The current position of the history cursor is shown in the status bar of the input pane next to the label `HI`. While working on various pages of the command history, you have a number of useful shortcuts available:

1) `<Ctrl + Enter>` Execute the current command set, append it to the end of the history, and move the history cursor there.
2) `<Alt + Enter>` Append the current command set to the history, but do not execute it.
3) `<Shift + Enter>` Replace the current interactive page, but do not execute the command set.
4) `<Shift + Ctrl + Enter>` Execute the current command set, append it to the end of the history, but do not move the history cursor there. (This is useful when you are editing a command set and executing it from time to time to see whether it works or not.)
5) `<Ctrl + Del>` Delete the current page from the history.

The interactive document with its command history pages enables you to quickly enter and debug sequences of CoCoA commands. While you are doing this, the output pane keeps track of your inputs and CoCoA's replies. Take your time to learn the history *correctly* and you will not be doomed.

B.4 More Bells and Whistles

The number you have entered is imaginary.
Please divide by 0 *and try again.*

The number you have entered is irrational.
Please rotate your keyboard by 90° *and try again.*
(Anonymous)

The graphical interface of CoCoA offers you several further conveniences. In the `Settings` menu you can choose whether the input and output lines are wrapped at the window border (option `Normal Wordwrap`), at column 100 (option `Fixed Wordwrap`), or at the maximal possible number of columns (option `No Wordwrap`). Moreover, by activating the option `Autoindenting` in this menu, you can simplify the input of user-defined functions: whenever the interface recognizes a command like `Define` or `For`, it automatically indents the following lines by four additional spaces.

Last but not least you can also use the word completion mode. Activation is achieved via the entry `Autocompleting` in the `Settings` menu, or by typing `<Ctrl + Ins>`. When autocompletion is on, the interface suggests possible completions for any keyword whose initial characters you type. You can cycle through the possible completions using `<Up Arrow>` and `<Down Arrow>`.

For instance, suppose you want to compute the vanishing ideal of a projective point set whose coordinates you know. After you type `Ide`, CoCoA starts offering possible command completions starting with `Ideal`. If you press the `<Down>` key several times, it offers the possible completion `IdealOfProjectivePoints`. To accept this completion, you have two possibilities. If you hit the `<Right>` key, the desired completion is performed and the cursor is positioned at the end of the word. If you hit the `<Left>` key, the word is completed, a pair of parentheses is appended, and the cursor is positioned after `(`. In this way, you are immediately ready to input the coordinates of the points and you never forget to close the parentheses.

B.5 The Programming Environment

The owl and the pussycat went to sea
In a beautiful pea green boat
They took some honey
And plenty of money
Wrapped up in a five pound note
(Edward Lear)

To wrap up the discussion above, let us suggest a way to use the graphical interface for developing CoCoA functions and packages, e.g. for solving the programming parts of the tutorials in this book.

1) Open a new CoCoA document using the entry `New` in the `File` menu or using the key combination `<Ctrl + N>`.
2) Type your first function into the input pane, using `Autoindenting` and `Autocompleting` as described above.
3) When you have finished typing, save your file using the entry `Save` in the `File` menu, or using the key combination `<Ctrl + S>`. Give it the desired name, e.g. `MyFile.coc`.
4) Send the contents of the document containing your program to CoCoA by pressing `<Ctrl + Enter>`.
5) Activate the interactive document. Define the ring over which you intend to work, and enter the data to which you want to apply your function. Use separate interactive pages for the base ring and the data.
6) On the next interactive page, call your function with the necessary arguments. Check the parser's messages (if any) and the output.
7) If something is still wrong, activate `MyFile.coc` and correct your function definition. Resend it to CoCoA. Then return to the interactive document and try your function again. If the result is now the expected one, try out the function using modified inputs by going back to he appropriate page in the command history.
8) Finally, when you are done correcting, save your file `MyFile.coc` again.

After that you can try your hand at the next function. If you work on the same package for a number of CoCoA sessions, you may also want to put a suitable `source` command into your file `userinit.coc`. In this way, your programs are automatically loaded each time you start CoCoA.

Finally, after a lot of effort, you have done it! CoCoA has completed a hard computation, and a huge Gröbner basis `G` consisting of 2000 polynomials is in the memory. What next? Of course, you can print the Gröbner basis in the output pane by typing `G;` in the interactive document. From there you could cut-and-paste it to a standard text editor. But if the output is many thousands of lines long, this is quite cumbersome. A much better idea is to use CoCoA's built-in facilities for this purpose. To print the list `G` nicely to a file, you should use something like the following sequence of instructions.

```
Set Indentation;
D:=OpenOFile("MyGBasis.coc");
PrintLn "G:=" On D;
Print G On D;
PrintLn ";" On D;
Close(D);
```

The end result will be a file called `MyGBasis.coc` on your hard disk which contains the list `G` in a nicely formatted way. To read it back, it suffices to make sure that you are using the correct base ring and to type

```
<< "MyGBasis.coc";
```

C. More on CoCoA Programming

The best way to accelerate a M CENSORED *h*
is at $9.8\ m/s^2$.
(Marcus Dolengo)

After having worked their way through the appendices A, B, C of Computational Commutative Algebra 1, many readers were encouraged to try to solve their own problems with CoCoA. However, sometimes they had to contend with unforeseen obstacles: the computation started but took forever, essential CoCoA functionality seemed to be missing, or there were bugs which successfully escaped detection. If you were one of those readers, this appendix is dedicated to you. We want to show you that it is neither advisable to speed up your computer at $9.8\ m/s^2$ nor necessary to erase CoCoA from memory. Instead, we suggest you work your way through yet another appendix. The reward will be plenty of tricks for watching and managing your computations, for finding that elusive crucial example, for moving between rings effortlessly, for creating and utilizing new data types, as well as for exposing and eradicating errors.

C.1 Trust Is Good, Control Is Better

Computing Gröbner bases, Hilbert bases, border bases, SAGBI bases, and even SuperG bases is not always as easy as we would like it to be. On occasion, you pass the corresponding commands to CoCoA, the program starts computing, continues computing, keeps computing ... After waiting patiently for a while, you begin to wonder whether the computation will ever stop. Will your memory suffice? Is your life-span going to be long enough? And just how long are you willing to wait? Clearly, you need to keep tabs on what is happening inside your chips. There are several possibilities at your disposal.

Firstly, you can watch the computation from the outside. Most operating systems offer you some program to monitor the system performance: the amount of memory allocated to the CoCoA program, the percentage of CPU usage it gets, and the amount of allocated memory which has been swapped to

the hard disk. Using this information, you can frequently get the big picture, i.e. you can make educated guesses as to whether you may be running out of memory soon, or whether CoCoA is mainly computing with data stored on the hard disk and the processor is mostly swapping these data in and out of the main memory.

Secondly, you can furnish your programs with `Time` commands to determine the execution time of an instruction. For instance, if you include the commands

```
Time G:=GBasis(I);
PrintLn;
```

in your function then CoCoA will display the time it took to compute the Gröbner basis `G` on a separate line, and then continue with the remaining commands of your function.

Thirdly, you can place suitable `Print` or `PrintLn` commands at strategic locations in your program. For instance, suppose that a possibly difficult toric ideal has to be found. In this case you could type something like

```
T:=Toric(M);
PrintLn "Toric ideal T has been computed ...";
```

Upon execution of your function you get some feedback about how many lines of code were processed successfully and where the computation got stuck.

Fourthly, if the problem is a particularly nasty Gröbner basis (and it often is!), you should resort to the wonderful *interactive Gröbner framework* of CoCoA. To start an interactive Gröbner basis computation of an ideal `I`, you type

```
GB.Start_GBasis(I);
```

Then there are several ways to proceed. For instance, to perform the first 1000 steps of the Gröbner basis computation and be fully informed what is going on, you should use

```
Set Verbose;
GB.Steps(I,1000);
```

Then CoCoA will print a dot for each step of the computation it has finished, and every 100 steps you will get some intermediate statistics:

```
 IPs  IVs Gens GBases MinGens MinDeg
-----------------------------------
 335    0   41     86      37      6
-----------------------------------
```

From this you see how far your computation has progressed. The data have the following meaning:

`IPs` number of critical pairs still to be processed
`IVs` number of generators still to be processed

`Gens`	number of generators of the original ideal or module
`GBases`	number of Gröbner basis elements found so far
`MinGens`	number of minimal generators found so far
`MinDeg`	minimal degree of a generator or critical pair still to be processed

Depending on this information, you decide how to continue. For instance, you can complete the Gröbner basis computation using `GB.Complete(I);` The part of the Gröbner basis computed so far is contained in `I.GBasis`. After possibly appending the original generators, you can also try to compute the Gröbner basis of the ideal or module generated by this list.

The following CoCoA program automates some of these interactive commands. It computes `N` steps of the Gröbner basis of the ideal or list of polynomials `I`, prints additional intermediate statistics (namely the minimal degree of a Gröbner basis element and the number of polynomials of minimal degree) every 100 steps, and returns the partial Gröbner basis. It is easy to adapt it to your own needs.

```
Define StepsGB(I,N)
  If Type(I)=LIST Then I:=Ideal(I) EndIf;
  Set Verbose;
  $cocoa/gb.Start_GBasis(I);
  TotalSteps:=0;
  For J:=1 To Div(N,100) Do
    $cocoa/gb.Steps(I,100);
    TotalSteps:=TotalSteps+100;
    PrintLn "Total steps computed: ",TotalSteps;
    DegList:=[Deg(F) | F In I.GBasis];
    MinDegGB:=Min([D| D In DegList]);
    PrintLn "Minimal degree in GB: ",MinDegGB;
    PrintLn "Number of polys of min degree: ",
      Len([D In DegList | D=MinDegGB]);
  EndFor;
  Return I.GBasis;
EndDefine;
```

Observe that we had to use the command `$cocoa/gb.Start_GBasis(I);` because the global alias `GB` is not recognized inside a function. Furthermore, observe that the result of an interactive Gröbner basis computation is not always the reduced Gröbner basis; it is necessary to append the command `ReducedGBasis(I);` to achieve this result.

A further useful technique available in the interactive Gröbner framework is *degree truncation*. Before starting the computation, you enter the command `I.DegTrunc:=D;` where `D` is the degree in which you want to truncate. In this way, no generators or critical pairs of degree larger than `D` will be processed. For instance, this technique is useful if `I` is homogeneous and you need to solve an ideal membership problem.

Finally, let us mention that the Gröbner framework can also be applied to compute minimal generators, syzygies, and free resolutions interactively. The corresponding commands

`GB.Start_MinGens` – start an interactive minimal generator calculation
`GB.Start_Syz` – start an interactive syzygy computation
`GB.Start_Res` – start an interactive resolution computation

and their options are explained in the CoCoA manual.

C.2 The Best Place to Find a Helping Hand

The above is the result of
exhaustive research, careful analysis,
and prolonged deliberation...
after which I flipped a coin.
(Anonymous)

In this section we propose some methods for using CoCoA to support your mathematical research. How can a computer algebra system do that? Normally, CoCoA is not much help in proving theorems — except for the geometric theorems mentioned in Section 6.7, of course. More often it is possible to decide whether a statement has a chance of becoming a theorem at all, either by checking many examples or by discovering a counterexample. Hence, to study a certain subject, it may be useful to create a collection of pertinent computer algebra routines. In particular, we provide explicit suggestions for the following three tasks.

1) Create and examine "generic" or "random" examples.
2) Search systematically for examples having special properties and stop if you find one.
3) Create auxiliary rings, do computations there, and move data to and fro.
4) Implement new data types and functions to handle them.

Seek and You Shall Find

Anyone who considers arithmetical methods
of producing random digits is, of course,
in a state of sin.
(John von Neumann)

Suppose we want to study the following *Artinian version* of the Minimal Resolution Conjecture (MRC) we discussed in Tutorial 89.

Conjecture. *Let K be an infinite field, let $P = K[x_1, \ldots, x_n]$ be standard graded, let $s \geq n+2$, let $\alpha \geq 1$ be chosen such that $\binom{\alpha-1+n}{n} \leq s < \binom{\alpha+n}{n}$, and let $V \subseteq P_\alpha$ be a generic K-vector subspace of dimension $\binom{\alpha+n}{n} - s$. Then*

the minimal graded free resolution of the ideal $I = V \oplus P_{\alpha+1} \oplus P_{\alpha+2} \oplus \cdots$ *has the shape*

$$\begin{aligned} 0 \longrightarrow P(-\alpha-n+1)^{a_n} \quad \oplus \quad P(-\alpha-n)^{b_n} \longrightarrow \cdots \longrightarrow \\ \longrightarrow \quad P(-\alpha)^{a_1} \oplus P(-\alpha-1)^{b_1} \longrightarrow I \longrightarrow 0 \end{aligned}$$

where the numbers a_i, b_i *are the numbers predicted by MRC.*

To test this conjecture in many cases, we could do with three auxiliary CoCoA functions: `CreateI(...)` to generate random ideals I of the desired kind, `GrBetti(...)` to compute the matrix of graded Betti numbers of I, and `ExBetti(...)` to list the matrix of expected Betti numbers. The first function requires us to create random homogeneous polynomials of some degree `D` via `Randomized(DensePoly(D))`. Otherwise, it appears to be straightforward to write.

```
Define CreateI(S)
   N:=NumIndets();
   A:=Alpha(S);
   V:=[Randomized(DensePoly(A)) | J In 1..(Bin(A+N,N)-S)];
Return Ideal(V)+Ideal(Indets())^(A+1);
EndDefine;
```

Here `Alpha(...)` is the support function

```
Define Alpha(S)
   N:=NumIndets();
   A:=0;
   While S>= Bin(A+N,N) Do
      A:=A+1;
   EndWhile;
Return A;
EndDefine;
```

The artifice to make the second function work is to employ the Gröbner framework. After calling `Res(I)`, we can access the matrix of graded Betti numbers via `GB.GetBettiMatrix(I)`. Short as it may be, this function includes three subtleties:

```
Define GrBetti(I)
   R:=Res(I);
   M:=Untagged($cocoa/gb.GetBettiMatrix(I));
   N:=NumIndets();
   A:=Min([J In 1..Len(M) | M[J,N]<>0]);
   B:=NewMat(2,N);
   For J:=1 To N Do
      B[1,J]:=M[A-1+J,N+1-J];
      B[2,J]:=M[A+J,N+1-J];
```

```
    EndFor;
Return B;
EndDefine;
```

Firstly, by assigning the resolution to an object R, we avoid having it printed in the output pane. Secondly, the global alias `GB` does not work inside a function and has to be substituted with `$cocoa/gb`. And thirdly, the result of `GB.GetBettiMatrix(I)` is a tagged matrix. By untagging it, we get a normal matrix (see below). The function `ExBetti`(...) was written by you in Tutorial 89.t.

Now let us shift the point of view somewhat. Suppose we work over a finite field. We want to find a homogeneous ideal in $P = K[x_1, \ldots, x_n]$ for which P/I has generic Hilbert function and for which the *linear strand* of the minimal graded free resolution is as long as possible. This means that we want the longest subtuple of $(a_1, \ldots, a_n)$ with non-zero values. Our strategy to find such examples is to create random ideals and compute the length of the linear strand of the resolution until we find interesting ones.

One way of doing this is to use a `While`- or `Repeat`-loop and compute until we find something. For instance, in the case $K = \mathbb{Z}/(3)$, $n = 5$ and $s = 10$ we can write

```
Use S::=Z/(3)[x[1..5]];
Repeat
   I:=CreateI(10);
   B:=GrBetti(I);
   L:=NonZero(B[1]);
Until Len(L)<>3;
```

After thousands of iterations we find an example whose resolution has a linear strand of length four. Another way of searching goes as follows. First we define a random number seed in the global memory. For instance, the command

```
MEMORY.CurrentSeed:=12345;
```

creates such a seed and the function

```
Define NewSeed()
   C:=MEMORY.CurrentSeed;
   S:=Mod(C*37,32003);
   MEMORY.CurrentSeed:=S;
Return S;
EndDefine;
```

generates a new seed in $\{1, 2, \ldots, 32002\}$ and updates the global variable. Then we include the command

```
    Seed(NewSeed());
```

in the function which creates our examples. If the search uncovers an interesting example and stops, the value of the global random number seed enables us to reconstruct the example. This method is particularly useful if the desired example consists of a large amount of data or a long computation.

Do we really have to compute hundreds or even thousands of examples until we discover a new species? Clearly, our chances of success depend on how exotic an animal we look for. But in this game cheating is very much allowed. For example, if you want more syzygies, it may prove worthwhile to fudge your random number generator so that it creates sparse polynomials.

When You're Through Changing You're Through

All truth passes through three stages.
First, it is ridiculed.
Second, it is violently opposed.
Third, it is accepted as being self-evident.
(Arthur Schopenhauer)

Another common task is to perform computations in various rings during the execution of a user-defined function. For instance, suppose we want to implement the method of Tutorial 51.f to compute the ideal I of algebraic relations of a tuple of polynomials $(f_1, \ldots, f_n) \in K[y_1, \ldots, y_m]^n$ where K is a field. The ring $P = K[x_1, \ldots, x_n]$ which contains I should be constructed inside the function. Moreover, we need the auxiliary ring $\overline{Q} = K[x_0, \ldots, x_n, y_1, \ldots, y_m]$ which ought to be destroyed when we have finished using it. Several CoCoA commands come in handy here:

`Using <RingName> Do <Commands> EndUsing` – do computations in another ring without changing the current ring

`BringIn <Object>` – bring objects from another ring into the currently used ring

`Destroy <RingName>` – destroy a ring which is no longer needed

Let us see how we can combine these ingredients to cook up the desired function.

```
Define Implicit(F)
   M:=NumIndets();
   N:=Len(F);
   DF:=[Deg(F[J]) | J In 1..N];
   D:=Concat([1],DF,[1|J In 1..M]);
   C:=Characteristic();
   If C=0 Then
      P::=Q[x[1..N]];
      Qbar::=Q[x[0..N],y[1..M]],Weights(D);
   Else
      P::=Z/(C)[x[1..N]];
```

```
      Qbar::=Z/(C)[x[0..N],y[1..M]],Weights(D);
    EndIf;
    Using Qbar Do
      FQ:=BringIn(F);
      Fhom:=Homogenized(x[0],FQ);
      Jbar:=Ideal([x[I]-Fhom[I] | I In 1..N]);
      E:=Elim(y[1]..y[M],Jbar);
      Edeh:=Subst(E,x[0],1);
    EndUsing;
    Using P Do
      I:=BringIn(Gens(Edeh));
    EndUsing;
    Destroy Qbar;
  Return P::Ideal(I);
  EndDefine;
```

For instance, using the ring `S::=Q[y[1..2]]` and the tuple `F=[y[1]y[2], y[1]^2+y[2]^2, y[1]^3+y[2]^3]` we obtain

```
Implicit(F);
P :: Ideal(-2x[1]^3 + 3x[1]^2x[2] - x[2]^3 + x[3]^2)
------------------------------
```

With the help of `Memory();` and `RingEnvs();` you can check that not only has the ring `Qbar` been destroyed, but also all objects defined over this ring. To harness the full power of the function `Implicit(...)` the call to `Elim(...)` should be substituted with the insertion of a special elimination function for homogeneous settings.

Sometimes the simple way of moving polynomials from one ring to another via the `BringIn`(...) command does not work. In this case you have to define a ring map. For example, assume that we want to define the $\mathbb{Q}$-algebra homomorphism $\varphi : \mathbb{Q}[x_1, x_2, x_3] \longrightarrow \mathbb{Q}[y_1, y_2]$ given by $\varphi(x_1) = y_1 y_2$, $\varphi(x_2) = y_1^2 + y_2^2$, and $\varphi(x_3) = y_1^3 + y_2^3$ in CoCoA, and we want to compute $\varphi(-2x_1^3 + 3x_1^2 x_2 - x_2^3 + x_3^2)$. To achieve this, we apply the CoCoA commands `RMap`(...) and `Image`(...) as follows.

```
P1::=Q[x[1..3]];
Use P2::=Q[y[1..2]];
Phi:=RMap(y[1]y[2],y[1]^2+y[2]^2,y[1]^3+y[2]^3);
Image(P1::Poly(-2x[1]^3+3x[1]^2x[2]-x[2]^3+x[3]^2),Phi);
```

The result is zero, in agreement with the above implicitization. This self-evident truth shows that we are through with changing rings!

Only Dead Fish Swim with the Stream

A man can surely heat his stove by burning his furniture,
yet he should not be deluded into believing
that he has discovered a wonderful new method
for heating his premises.
(Ludwig von Mises)

When man discovered object oriented programming and its applicability to the construction of computer algebra systems, he thought that all he had to do is create a *class* for every data type he encountered in Computational Commutative Algebra, and that he had discovered a wonderful new method for computing everything. Alas, it turned out that these general classes are too inefficient to be of practical value. CoCoA offers you a few important data types which are highly optimized for good performance.

But what if the application you have in mind is not mainstream? Is there a way to make your own data types in CoCoA? How is it possible to define functions which apply to these new data types?

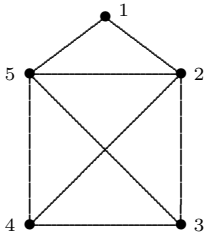
Let us assume that you are working with graphs, e.g. that you are trying to solve Tutorial 26 or 71. It is natural to define a new data type called `"Graph"`. In CoCoA, you can use the built-in data type `Record(...)` for this purpose. A record consists of a sequence of fields. A field is defined by an equation `<FieldName> = <Object>` where `<FieldName>` is an identifier and `<Object>` is, well, a CoCoA object. The function

```
Define Graph(N,L)
   If Not (Type(N)=INT And N>0) Then
      Error("Positive integer expected.");
   EndIf;
   If Not Type(L)=LIST Then Error("List expected.") EndIf;
   M:=Len(L);
   G:=Record(VertNo=N,EdgeNo=M, Edges=L);
Return Tagged(G,"Graph");
EndDefine;
```

does some type checking and creates a record for a graph. It expects the graph to be entered in the format

```
G:=Graph(5,[[1,2],[1,5],[2,3],[2,4],[2,5],[3,4],[3,5],[4,5]]);
```

This definition corresponds to the following graph.



Notice that the above function does not return the record directly, but attaches a *tag* first. A tag is a string which you can think of as an identifier for your new data type. E.g., the query `Type(G);` now yields

```
TAGGED("Graph")
-------------------------------
```

Tags allow you to define special routines for printing and describing objects of your new data type. If you want to be fancy, create functions
`Print_Graph()` – to print graphs in the format you want; if you then type `G;` the graph `G` will be printed according to the new fashion
`Describe_Graph()` – to output an explicit description of the graph
`Help_Graph()` – to generate the reply to the request `Help("Graph");`

So, what can we do with this newly defined data type? For example, the following function creates its graph ideal in a suitable polynomial ring `P`.

```
Define GraphIdeal(G)
   If Not Type(G)=TAGGED("Graph") Then
      Error("Expected a graph");
   EndIf;
   N:=G.VertNo;
   M:=G.EdgeNo;
   P::=Z/(2)[x[1..N]];
   Using P Do
      I:=[x[Pair[1]]*x[Pair[2]] | Pair In G.Edges];
   EndUsing;
Return P::Ideal(I);
EndDefine;
```

Note how we accessed the fields of the record `G` containing our graph: the object `G.EdgeNo` contains the value of the field `EdgeNo` of the graph `G`. Next we could define a function

```
Define MaxDisconnect(G)
   I:=GraphIdeal(G);
   Using P Do
      Return Dim(P/I);
   EndUsing;
EndDefine;
```

to compute the size of a maximal disconnected subgraph (see Tutorial 71.k), and so on.

In the hope that these hints will help you cross the sea of data, record, types and functions, we now invite you to venture out on your own. And keep in mind that if you want to get back safely, you will sometimes have to swim against the stream.

C.3 To Err Is Human

Errare humanum est –
perseverare diabolicum.
(Latin Proverb)

No matter how hard we try, occasionally even the best CoCoA programmers produce an error. In this section we want to point out some ideas on how you can minimize the number of your errors, how you can find and correct them, and how you can avoid making the same error again in the future.

Better Safe than Sorry

Let us begin with the topic of *error prevention.* It is often a good idea to check the data type of the objects you deal with. Make sure that the ideal you were supposed to use as a function argument is actually an ideal by starting your function with a command such as

```
If Type(I)<>IDEAL Then Error("Expected an ideal!") EndIf;
```

If you plan to use your function with several types of arguments, perform the necessary type conversions first. To generate a function which works for both ideals and lists of polynomials, the above example could be extended to

```
If Not(Type(I) IsIn [IDEAL,LIST]) Then
  Error("Expected an ideal or a list!");
ElsIf Type(I)=LIST Then
   I:=Ideal(I);
EndIf;
```

Another method to prevent errors is to modularize your programs. Suppose you are implementing the Homogeneous Buchberger Algorithm 4.5.5. We can think of a number of useful subroutines which you may want to write: `NextDegree(...)`, `PairLoop(...)`, `GensLoop(...)`, or `UpdatePairs(...)` come to mind. By debugging those functions separately, you can decrease the likelihood of an error in your main program substantially. Furthermore, you can then collect these subroutines in a CoCoA package and reuse them on other occasions.

So, what is a CoCoA package? From the outside, it is nothing but a file having the extension `.cpkg` and containing CoCoA functions. You can load it with the `source` command just as you would load any `.coc` file. From the inside, it starts with something like `Package $contrib/MyPkgName`, continues with some function definitions, and ends with `EndPackage;` To access a function called `MyFunc(...)`, you have to type `MyPkgName.MyFunc(...)`. The advantage of doing this extra typing is that if there are two functions with the same name, the first one will not be overwritten when you load the second. To keep the overhead to a minimum, you can also define an alias for your package, e.g. you can enter

```
Alias  My := $contrib/MyPkgName;
```

and thenceforth refer to your function by typing `My.MyFunc(...)`.

The third method for preventing errors is the do-it-yourself method. (The best place to find a helping hand is at the end of your arm.) To apply this method, you proceed as follows. First you think of an example which is neither too difficult nor too trivial for your function. Then you compute this example step by step in the interactive document. Finally, you copy the commands you used one by one into the CoCoA document, all the time modifying them suitably to fit the general scheme. In this way you should get a function which computes the correct result in at least one case.

Last but not least there is a clever way to produce good CoCoA code: look through the packages which come with CoCoA and get inspired!

Keep Your Wits and Get the Message

`ERROR: parse error in line 911 of device`
(CoCoA Error Message)

Our second topic is *error discovery*. The most frequent way you find out that you committed an error is via the above well-known CoCoA error message. Its subtlety is revealed when you realize that the line number does not necessarily correspond to the actual line in which the error occurred. But don't get angry. In most cases you can detect the error by following one simple instruction:

Starting from the line number in the error message,
scan your file upwards until you find the line
where you forgot to put the `;` *Done!*

In the remaining cases, ask yourself the following questions.

1) Did I remember to close all parentheses? (If this error happens frequently, use autocompletion and `<Left>` whenever possible, or use an editor which automatically creates parentheses in pairs.)
2) Did I put the arguments of the built-in CoCoA functions in their correct order? (The CoCoA manual is really helpful here...)
3) Did I close every control structure (e.g. `For` or `While` or `If`) with its corresponding `End`-command (e.g. `EndFor` or `EndWhile` or `EndIf`)?
4) Did I use `:=` for assignments and `=` for logical comparisons and `::=` for ring definitions correctly everywhere?

Another trick the parser uses to confuse you is to claim that it does not recognize a user-defined variable although you have defined it absolutely correctly. What is behind is probably a forgotten `;` or `)` which led the parser astray. If you don't find the error by simply reading the input carefully, you might want to insert suitable `PrintLn` commands to check intermediate results of your program, or you could comment out parts of the code to localize the problem.

This bring us to the topic of *local* versus *global* objects which is a recurrent source of errors. Most CoCoA objects you create are stored in the working memory. For instance, if you have an ideal `I := Ideal(x,y);` over the ring `R` and you switch to the ring `S`, typing `I;` leads to the reply

```
R :: Ideal(x, y)
------------------------------
```

If you define a function which uses an ideal `J` as its argument and contains an assignment to an ideal `I`, it is possible to apply this function to the ideal `I` in `R` because the names `J` and `I` are local to the function. If you want to use some objects globally, i.e. in the working memory and in user-defined functions, you have to write a statement such as

```
MEMORY.N:=4;
```

which creates the integer `N` in the global memory. Then you can access `N` from inside a function by a command such as

```
NewN:=MEMORY.N;
```

Finally, we remind you that the command `Use <Ringname>` is not allowed in user-defined functions and that global aliases (such as `GB` or `HP`) cannot be used either.

This list of sources for trouble is not intended to be comprehensive; maybe it is not even comprehensible. But we hope that it enables you to limit your search for remaining errors to the really difficult ones: mathematical errors.

Good Riddance to Those Beastly Bugs

Just because you're paranoid doesn't mean
they aren't out to get you.
(Anonymous)

Our last topic is *error digestion*. What happens after you have successfully discovered and eliminated an error? Does life continue as usual? We hope not. To prevent yourself from introducing the same error again in a later stage of the programming project, you should keep the following tenet in mind.

Every bug becomes a test.

This means that it is good practise to write a short test function which applies your program to compute a case in which the error occurred. The test function checks whether the computed result is correct. All test functions are combined in a package called the *test suite* for your program. In the main CoCoA program, test suites have usually a filename ending in `.ts` and can be managed using the `ts_lib.cpkg` package. Here is the official way to perform the CoCoA sanity test:

```
Alias TSL := $ts/ts_lib;
Test := Record[ Id = "SanityTest"];
Test.Input := "1+1;";
Test.ExpectedOutput :=
"2
------------------------------
";
TSL.RegisterTest(Test);
TSL.Do();
```

The result should be a file called `SanityTest.result` on your computer which contains the message `Succeeded` and the message

```
-- TestSanityTest : Succeeded
```

in the output pane. Alas, if the test fails, you receive the message `FAILED!` (What else?)

Lastly, if all attempts fail and you get a bit paranoid, there is still a final resort. Get a good night's sleep! In the bright light of a new day, bugs will be spirited away. And remember that even the most powerful man on earth has to admit:

You cannot win the war on error.

C.4 Can't Stop!

A trend in motion continues
until it actually stops!
(James Dines)

Has this appendix been all work and no play? Well, this is about to stop. You can now use CoCoA to play the board game `Can't Stop!` invented by Sid Sackson. As for the rules and the necessary equipment, check out the link provided in the CoCoA manual entry of `CantStop.cpkg`. You get it by typing the command

```
$contrib/CantStop.Man();
```

Moreover, this manual entry will inform you about the available functions and computer opponents. To start a game against one of the computer opponents, simply type

```
CantStop.Play("Me","ComputerAnna");
```

and off you go! The package `CantStop.cpkg` also offers you advice on the probability of success for different moves and allows you to play computer assisted games against human opponents.

D. Suggestions for Further Reading

Financial genius is a rising stock market.
(John Kenneth Galbraith)
Mathematical genius is a benevolent referee.
(Anonymous Referee)

In the introduction to the first volume we wrote that we had decided not to cite anything anywhere. Why then did we write an entire appendix full of references? We still do not believe in the merits of a very extended bibliography. Mathematics is evolving continuously, and many bibliographies are already outdated when they appear. As its title suggests, the intention of this appendix is a different one. We would like to provide you with some ideas of where to look if you want to know more about the subjects treated or mentioned in the two volumes. Our selection is by no means meant to imply any judgement on the merits or relevance of other works. It is merely a very subjective list of some books and papers which we know and deem reasonable possibilities for what to read next.

The bibliography of Volume 2 is disjoint from that of Volume 1. So, if we refer to [AL94] and you do not find the reference here, look at the end of Volume 1. A number of tutorials are based on joint papers of the authors with L. Bazzotti, M. Caboara, G. Dalzotto, and A. Kehrein which are not quoted individually.

D.1 Chapter 1

In the last few years, a number of new introductory text books on various aspects of computer algebra have appeared. In particular, the books [Co99], [Ei02], [GP02], [Stu02], [GG03], [GKW03], [Sc03], [CLS04], [Ste04], and [DE05] contain additional material on many of the topics we discussed.

The presentation of Berlekamp's algorithm in Tutorial 6 is modelled on the version in D. Knuth's well-known book [Kn97]. If you want to know Robbiano's classification of term orderings explicitly, look at [Ro86].

Tutorials 12, 40 and 98 offer some glimpses into computational aspects of invariant theory. Good places to study this theory further are the books [Stu93] and [DK02].

In Tutorial 13 we encounter for the first time the connection between Computational Commutative Algebra and combinatorics. Further examples appear in Tutorials 36 and 38 about integer programming and in Section 6.1 about toric ideals and Hilbert bases. To learn more about this topic, we suggest the books [Stu96] and [MS05].

D.2 Chapter 2

Most of the material in this chapter is standard and contained in virtually every book on Gröbner bases. Tutorial 25 is the first time we discuss possible optimizations of Buchberger's algorithm; further suggestions are made in Tutorials 59 and 69. Some of the best implementations of this algorithm are the ones by J.-C. Faugère described in his papers [Fa99] and [Fa02].

Tutorial 26, and later Tutorials 65 and 71, provide some links between Computational Commutative Algebra and graph theory. More results in this direction are contained in [Vi01] and [Lo04].

Tutorial 27 is the first in a long list of tutorials which treat the interrelations between Computational Commutative Algebra and algebraic geometry. Further items on this list are Tutorials 35, 39, 46, 52, 55, 88, 89 and 95. There exist a number of computer algebra books whose primary topic is computational algebraic geometry, for instance [CLS92], [CLS04], [Ei02] and [Sc03]. Some of them lead up to very advanced algorithms in this area.

D.3 Chapter 3

A more general application of Gröbner bases to the theory of splines than the one in Tutorial 28 is contained in Chapter 8 of [CLS04]. The applications of Gröbner bases to operations on ideals and modules discussed in Sections 3.1 – 3.6 are contained in most of the textbooks cited above. For other classical topics in commutative algebra see for instance [Ku80], [Mat86] and [BH93].

Section 3.7 gives a brief account of some applications of Gröbner bases to solving systems of polynomial equations. Specialized books about this topic are [Ste04] and [DE05], and there are also some relevant chapters in [BW93] and [Co99].

Tutorials 43, 77 and 79 give some pointers to the computation of primary decompositions of polynomial ideals. A more thorough treatment, including further references, is available in [Va98], [GP02] and Chapter 5 of [DE05].

Finally, the topic of modern portfolio theory is discussed extensively by its founder H. Markowitz in [Mar91].

D.4 Chapter 4

For another computationally oriented book containing some parts of the theory of multigraded rings and modules, we refer you to [MS05]. The special properties of degrev type orderings and their relations to generic initial ideals and distractions (explained in Section 4.4, Tutorial 75, and Section 6.2) were studied for instance in the papers [BS87] and [BCR05].

The technique of idealization we use for computing minimal homogeneous presentations and minimal graded free resolutions in Sections 4.7 and 4.8 were introduced into commutative algebra by M. Nagata in [Na62]. Other algorithms for these purposes are, for instance, explained in [AL94], [GP02], and [CLS04].

D.5 Chapter 5

Good introductions to Hilbert functions and related problems from the theoretical point of view are [BH93] and [Val96]. Tutorial 65 is based on a preprint of M. Katzman. If you want to learn more about Ehrhart polynomials (see Tutorial 67), we suggest the books [Stu96] and [MS05].

Different algorithms for computing Hilbert series are compared in [Bi97]. The book [Ga00] discusses Hilbert-driven Gröbner basis computations (see Tutorial 69) and their application to the computation of invariants (see Tutorial 98).

The application of Computational Commutative Algebra to photogrammetry mentioned in Tutorial 72 is just one of the many techniques in [May93]. An extensive discussion of generic initial ideals is contained in [Gr96]. Independent sets of indeterminates are also treated in [BW93]. Their application to computing Noether normalizations is presented for instance in [Va98] and [GP02].

D.6 Chapter 6

The theory of finite sets of points and algorithms for dealing with them are developed further in [GKR93], [Ab00] and [AKR05]. The articles [DGO85] and [EGH96] discuss the history and applications of the Cayley-Bacharach property. An algorithm for computing the resolutions in Tutorial 89 is explained in [BK96]. Tutorial 90 uses the results of J.P. Hansen in [Ha94].

Section 6.4 deals with connections between Computational Commutative Algebra and numerical analysis. A good recent textbook on this subject has been written by H. Stetter (see [Ste04]). Moreover, there are related chapters in [DE05].

The theory of SAGBI bases was initiated by the foundational papers [RS90] and [KM89]. Besides our Section 6.6, further recent additions to this theory are contained in [CHV96], Chapter 11 of [Stu96], and [TUO03]. Tutorial 97 is based on [Ho98] and [No02].

Finally, if you want to know more about automatic theorem proving, e.g. more examples where it succeeds, we suggest that you start with the classical books [Wu94] and [Ch88] and continue with Project 1 in [Co99].

E. Hints for Selected Exercises

Talk is cheap because supply exceeds demand.
(Anonymous)

E.1 Hints for Exercises in Chapter 4

Exercise 4.1.2. If a K-algebra S is graded by W, it is also graded by λW for every $\lambda \in \mathbb{Z}$.

Exercise 4.1.3. Using a), reduce the proof of b) to the case of a term f.

Exercise 4.1.6. For d), consider $F = P^2$ and $M = \langle e_1 + e_2 \rangle$.

Exercise 4.1.12. Write $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. The set of all $(\alpha_1, \ldots, \alpha_n)$ such that $\deg_W(t) = d$ is the solution set of a system of Diophantine equations.

Exercise 4.1.14. To prove b)$\Rightarrow$a), argue by contradiction. Assume that $d \in \Sigma$ is the smallest degree with respect to τ such that $K[a_1, \ldots, a_s]_d \subset A_d$.

Exercise 4.1.15. For every $d \in \mathbb{Z}^m$, look at the K-linear map $\varphi_d : M_d \longrightarrow M_d$.

Exercise 4.2.1. Imitate the proof of Proposition 4.2.3.

Exercise 4.2.2. Let $w_1, \ldots, w_m$ be the rows of W, and let $b_1, \ldots, b_{m-1} \in \mathbb{Z}$ be such that $b_1 w_1 + \cdots + b_{m-1} w_{m-1}$ has positive entries in the positions corresponding to the non-zero columns of W. Then use $v = a_1 w_1 + \cdots + a_{m-1} w_{m-1} + w_m$ with $a_i = c b_i$ and $c \gg 0$.

Exercise 4.2.6. The leading term of $x^2 - y^2$ is either x^2 or y^2.

Exercise 4.2.2. Dehomogenize F, factor, and homogenize again.

Exercise 4.3.3. Use Proposition 3.5.11.b.

Exercise 4.3.5. Show that the inclusion in b) is an equality if the degree form of f is a non-zerodivisor for $P/\operatorname{DF}_W(I)$.

Exercise 4.3.11. First prove $I^{\hom} = (y_2 x_1 - y_1 x_2,\, x_1^2,\, x_1 x_2,\, x_2^2)$.

Exercise 4.4.2. Use Proposition 4.2.3.

Exercise 4.4.3. Consider the case $m = n$.

Exercise 4.4.7. Specialize Corollary 4.4.15 suitably.

Exercise 4.5.7. Use Proposition 2.5.8.

Exercise 4.6.3. Construct a sequence of homogeneous K-linear maps

$$M/(P_+ \cdot M) \xrightarrow{\varphi} M/(P_+ \cdot M' \cap M) \xrightarrow{\psi} M'/(P_+ \cdot M')$$

where $M' = M + \langle g \rangle$, φ is surjective and ψ is injective, but not bijective. Then show that $\dim_K(M'/(P_+ \cdot M')) \leq \dim_K(M/(P_+ \cdot M' \cap M)) + 1$ and conclude that a) and b) are equivalent. To prove that b) and c) are equivalent, use the modular law (see Exercise 4 of Section 3.2).

Exercise 4.6.6. Apply Buchberger's Algorithm with Minimalization 4.6.3.

Exercise 4.7.4. For d), consider the ideal $(x_1, x_2, x_3^2, x_4^2) = (x_1, x_2, x_3^2 - x_1x_2, x_4^2 + x_1x_2)$ in $\mathbb{Q}[x_1, \ldots, x_4]$.

Exercise 4.7.6. To answer b), consider all ideals in $\overline{P}$ which are generated by P-linear forms in $e_1, \ldots, e_r$.

Exercise 4.8.2. To prove b), assume that α, β are inverse to each other. Then prove that the isomorphism $S \oplus F' \cong F \oplus S'$ induces an isomorphism $S \cong S'$.

Exercise 4.8.3. The general shape is

$$0 \to P(-n) \to P(-n+1)^n \to \cdots \to P(-2)^{\binom{n}{2}} \to P(-1)^n \to (x_1, \ldots, x_n) \to 0$$

E.2 Hints for Exercises in Chapter 5

Exercise 5.1.1. By induction on r, show that $\Delta^r f(i) = (i-r)! \cdot p_r(i)$ for $i \gg 0$ with $p_r \in \mathbb{Z}[t]$. Now use Proposition 5.1.11.a.

Exercise 5.1.5. Construct a homogeneous exact sequence of graded P-modules

$$0 \longrightarrow (f_1 f_2) \longrightarrow (f_1) \bigoplus (f_2) \longrightarrow (f_1, f_2) \longrightarrow 0$$

Exercise 5.2.2. Use Theorem 5.2.6.

Exercise 5.2.3. Apply the Binomial Theorem to $(1-t)^n$ and multiply the result by $(1-t)^{-n}$ using Lemma 5.2.9. Then compare coefficients.

Exercise 5.2.5. Use Corollary 5.2.17.

Exercise 5.2.6. Construct a homogeneous exact sequence

$$0 \longrightarrow P/(I \cap J) \longrightarrow P/I \oplus P/J \longrightarrow P/(I+J) \longrightarrow 0$$

Exercise 5.2.10. Use Proposition 5.1.7.c.

Exercise 5.3.5. Use Proposition 5.3.6 and the multiplication sequence corresponding to the element $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

Exercise 5.3.6. Use Proposition 3.7.1.

Exercise 5.3.7. To prove a), deal with the case $m = 1$ first. Then use induction on M. In order to show b), prove the formula

$$\begin{aligned}\mathrm{HN}_{P/I}(z) = 1 - z^{\alpha_1} + (z^{\alpha_1} - z^{\alpha_2})\,\mathrm{HN}_{P/J_1}(z) + \cdots \\ + (z^{\alpha_{m-1}} - z^{\alpha_m})\,\mathrm{HN}_{P/J_{m-1}}(z) + z^{\alpha_m}\,\mathrm{HN}_{P/J_m}(z)\end{aligned}$$

by forming suitable colon ideals. To find further examples in e), you may look at strongly stable monomial ideals (see Tutorial 75).

Exercise 5.4.2. Find the coefficient of z^4.

Exercise 5.4.4. Take suitable linear polynomials f_1, f_2, f_3.

Exercise 5.4.6. Use the homogeneous exact sequence

$$0 \longrightarrow \mathrm{Syz}_P(f_1, \ldots, f_n) \longrightarrow P(-2)^n \longrightarrow (f_1, \ldots, f_n) \longrightarrow 0$$

Exercise 5.4.8. Use Exercise 10 of Section 5.2.

Exercise 5.5.2. Use a `Lex`-segment space of the dimension suggested by Example 5.5.6.

Exercise 5.5.4. Use Proposition 5.4.8.

Exercise 5.5.5. Get some inspiration from Exercise 9 of Section 2.6.

Exercise 5.5.10. For the proof of a), use Theorem 5.5.32. For b), construct a suitable `Lex`-segment ideal.

Exercise 5.5.11. To prove a), use Proposition 5.5.13.c, the equality $\binom{a}{b} = \binom{a}{a-b}$ and Corollary 5.5.34.

Exercise 5.6.9. To prove that b) implies a), let $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ be the maximal ideals in R. Show that the natural homomorphism $\varphi : R \longrightarrow \prod_{i=1}^{r} R/\mathfrak{m}_i$ is bijective.

Exercise 5.7.1. Check out the 24^{th} factor!

Exercise 5.7.3. Using induction, reduce the proof to the case $L = K(a)$ with $a \in L$.

Exercise 5.7.4. Consider $I \cap K[x_1, x_2]$.

Exercise 5.7.7. Use the combinatorial dimension to prove that $\dim(A) \leq \dim(B)$. Use the affine dimension to prove that $\dim(B) \leq \dim(A)$.

Exercise 5.8.1. For a), consider a Laurent series with support in $\{(a_1, a_2) \in \mathbb{Z}^2 \mid 2a_1 + a_2 \geq 0 \text{ and } a_2 \geq 0\}$ and use $\sigma = \mathtt{Lex}$ and $\tau = \mathtt{DegLex}$.

Exercise 5.8.5. Use the multiplication sequence corresponding to f_s and induction on s.

E.3 Hints for Exercises in Chapter 6

Exercise 6.1.1. Proceed as in Example 6.1.19.

Exercise 6.1.2. Consider the equation $z_1 + z_2 - iz_3 = 0$.

Exercise 6.1.7. Combine Tutorial 36 with the method of computing toric ideals explained in Section 6.1. The matrix $\mathcal{A}$ is the coefficient matrix of

$$\begin{cases} z_{11} + z_{12} + z_{13} &= 120 \\ z_{21} + z_{22} + z_{23} &= 204 \\ z_{31} + z_{32} + z_{33} &= 92 \\ z_{41} + z_{42} + z_{43} &= 55 \\ z_{11} + z_{21} + z_{31} + z_{41} &= 183 \\ z_{12} + z_{22} + z_{32} + z_{42} &= 190 \\ z_{13} + z_{23} + z_{33} + z_{43} &= 98 \end{cases}$$

For c), use a cost compatible term ordering and compute a suitable normal form.

Exercise 6.2.4. First consider the leading term of $\gcd(f,g)$ with respect to σ. Then generalize.

Exercise 6.2.5. Combine Theorem 6.2.12.d and Proposition 5.1.16.c.

Exercise 6.2.6. To show a), find the LU-decomposition of $\mathcal{Y}^{-1}$ using standard linear algebra. Then invert. For c), it suffices to prove the inclusion "$\subseteq$" and compare the Hilbert functions. Simlarly, in order to show d), it suffices to prove the inclusion "$\supseteq$" and compare the Hilbert functions.

Exercise 6.3.4. Use Proposition 6.2.8.

Exercise 6.3.6. Show that without loss of generality we may assume $\mathbb{X} \subseteq D_+(x_0)$. Let $\overline{R} = \overline{P}/(\mathcal{I}^+(\mathbb{X}) + (x_0))$. Use the line defined by $(\mathrm{Ann}_{\overline{R}}(\overline{R}_{r_{\mathbb{X}}-1}))_1$.)

Exercise 6.3.7. Apply the modified algorithm to the projective point set $\mathbb{X} = \{(1 : c_1 : c_2) \mid c_1, c_2 \in \{-1, 0, 1, 2\}\} \setminus \{(1 : 2 : 2)\} \subset \mathbb{P}^2_{\mathbb{Q}}$.

Exercise 6.3.8. If the five points are on a line, use Exercise 6.3.5. Then distinguish the cases that four points are on a line and that no four points are on a line.

Exercise 6.4.3. Apply a permutation π to the elements of G. The use parts a) and b) of Proposition 6.4.17.

Exercise 6.4.4. Let $\mathcal{O} = \{1, x\}$. Use Propositions 6.4.15 and 6.4.17 to describe the elements of A via their $\mathcal{O}$-border bases. Then apply Theorem 6.4.30 to construct a set of equations defining A. Finally, examine these equations.

Exercise 6.4.5. For the proof of a), use the inequalities

$$\#\mathcal{O} \leq \dim_K(P/J) \leq \dim_K(P/(\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s))) = \#\mathcal{O}$$

For the proof of b), show that the residue classes of the elements of $\mathcal{O}$ generate P/I and that $\mathcal{O}_\sigma(I) \subseteq \mathcal{O}$. Then apply a). Finally, use Proposition 6.4.18 to prove c).

Exercise 6.4.6. Modify the ordering of the columns of $\mathcal{V}$ in Lemma 6.4.35.

Exercise 6.5.4. For the solution of b) and c), notice that the two filtrations are equal if and only if $I^d J = I^d \cap J$ for all $d \geq 1$.

Exercise 6.5.6. Proceed as in Example 6.5.27. You should obtain the result $\mathrm{LF}_{\mathtt{m}}(J) = (x_1^2 x_2,\ x_1 x_2^2,\ x_2 x_3^6,\ x_1^8 x_4^2)$.

Exercise 6.6.4. Note that, with suitable weights, the subalgebra is graded. Hence it suffices to compute the SAGBI basis up to a certain degree.

Exercise 6.6.5. You may use CoCoA to compute the toric ideal.

Exercise 6.6.6. Besides the nine minors, there are two further SAGBI basis elements of degree four.

Exercise 6.6.7. Show that $S = K + K(x^2 - 1) + K(x^3 - x) + \cdots$.

Exercise 6.6.8. To prove c), choose a term ordering σ and show that P, considered as a $(K + \mathcal{I}(\mathbb{X}))$-module, is generated by $\mathcal{O}_\sigma(\mathcal{I}(\mathbb{X}))$. Then apply Lemma 2.6.5. For the proof of d), you have to refine this argument by looking at the proof of Lemma 2.6.5.

Exercise 6.6.9. Prove that $\mathrm{Syz}_S(x_1 x_2, x_2^2) = \langle (x_1 x_2, -x_1^2),\ (x_2^2, -x_1 x_2) \rangle$.

In the end, everything is a gag.
(Charlie Chaplin)

Notation

1. Special Symbols

$\mathbb{N}_+$	set of positive integers $\{1, 2, 3, \ldots\}$
∞	infinite number
$A \cong B$	object A is isomorphic to object B
$\mathbb{IP}$	set of all integer valued polynomials in $\mathbb{Q}[t]$
$\mathbb{IP}_{\leq r}$	set of all integer valued polynomials of degree $\leq r$
$q \leftrightarrow q'$	corresponding pair
$\mathbb{T}(V)$	monomial basis of a lex-segment space
$\mathfrak{R}$	set of radical monomial ideals of a polynomial ring
$\mathfrak{I}$	set of all monomial ideals of a polynomial ring
D_n	dihedral group of order $2n$
$\prec$	partial ordering by componentwise comparison
$\mathbb{X}$	affine or projective point set
$\mathcal{O}$	order ideal in $\mathbb{T}^n$
$\mathcal{T}$	model for a statement in Euclidean geometry

2. Sets and Tuples

$\mathcal{Z}^+(I)$	projective zero set of a homogeneous ideal
$H^{\inf}$	hyperplane at infinity in $\mathbb{P}^n_K$
$V^{\inf}$	points at infinity of a projective variety
$S_{\leq d}$	set of homogeneous elements of degree $\leq d$ in S
S_d	set of homogeneous elements of degree d in S
$\mathcal{V}_{\leq d}$	subtuple of homogeneous elements of degree $\leq d$ in a tuple
$\mathcal{V}_d$	subtuple of homogeneous elements of degree d in a tuple
$\mathcal{V}_d(\mathbb{P}^n)$	d^{th} Veronese variety
$\mathcal{L}(\mathcal{A})$	set of integer solutions of a system of Diophantine equations
$\mathcal{L}_+(\mathcal{A})$	set of non-negative solutions of a Diophantine system
$\mathcal{L}_N(\mathcal{A})$	set of partially non-negative solutions of a Diophantine system
$\mathrm{UB}(S)$	set of all unitary binomials in S
$\mathrm{PB}(S)$	set of all pure binomials in S
$\mathrm{PB}_N(S)$	set of all N-separated pure binomials in S
$\mathrm{MQ}(r)$	set of magic squares of size $r \times r$

$\mathrm{MQ}(r,s)$	set of magic squares of size $r \times r$ whose magic sum is s
$\mathbb{X}^a$	affine part of a projective point set
$\mathbb{X}^{\inf}$	points at infinity of a projective point set
$\mathcal{O}_\sigma(I)$	order ideal of I with respect to σ
$C_j(\mathbb{X})$	j^{th} Reed-Muller code associated to a projective point set
$C^\perp$	dual code of a linear code
$\partial\mathcal{O}$	border of an order ideal
$\partial^i\mathcal{O}$	higher borders of an order ideal

3. Functions

$\mathrm{HF}_M(d)$	value of the Hilbert function of a module in degree d
Δf	difference function of an integer function
$\Delta^r f$	r^{th} difference function of an integer function
$\Delta_q f$	q-difference function of an integer function
Σf	summation function of an integer function
bin_i	binomial integer Laurent function
EF_S	Ehrhart function of a set
$\mathrm{HF}^a_{P/I}(d)$	value of the affine Hilbert function of an affine algebra
$\mathrm{HF}_{M,W}(d)$	value of the multigraded Hilbert function of a module
$\mathrm{HF}_{\mathbb{X}}(d)$	value of the Hilbert function of a projective point set
$\eta(v,w)$	Hamming distance of two tuples
$\mathrm{HF}_{R,\overline{\mathfrak{q}}}(d)$	value of the $\overline{\mathfrak{q}}$-adic Hilbert function of R in degree d

4. Orderings

$\overline{\sigma}^W$	extension of σ by W
$\mathtt{Pos}{-}\tau$	module term ordering "position first"
$\tau{-}\mathtt{Pos}$	module term ordering "τ first"
$\mathtt{Deg}{-}\tau{-}\mathtt{Pos}$	module term ordering "degree first"

5. Polynomials and Vectors

$\deg_W(f)$	degree of f with respect to the grading given by W
$\frac{\partial f}{\partial x_i}$	partial derivative of f
$\mathrm{DF}_W(v)$	degree form of a vector
f^{hom}	homogenization of a polynomial
F^{deh}	dehomogenization of a polynomial
$\mathrm{HR}_{\sigma,\mathcal{G}}(f)$	head reduction remainder of a polynomial
$\Delta p(t)$	difference polynomial $p(t) - p(t-1)$
$\mathrm{HP}_f(t)$	associated polynomial of an integer function of polynomial type

$\mathrm{HP}_M(t)$	Hilbert polynomial of a module
$\mathrm{LSupp}(f)$	logarithmic support of a polynomial
$\mathrm{EP}_S(t)$	Ehrhart polynomial of a set
$\mathrm{hn}_M(z)$	simplified Hilbert numerator of a module
$\|a\|$	Euclidean norm of a vector in $\mathbb{R}^n$
$a \times b$	vector product in $\mathbb{R}^3$
$\mathrm{HP}^a_{P/I}(t)$	affine Hilbert polynomial of an affine algebra
$\mathbf{x}^a$	extended term $x_1^{a_1} \cdots x_n^{a_n}$ where $a = (a_1, \ldots, a_n)$
$D_\pi(t)$	distraction of a term
$F^{\inf}$	image under $x_0 \mapsto 0$ of a homogeneous polynomial
$\mathrm{NR}_{\mathcal{O},\mathcal{G}}(f)$	normal $\mathcal{O}$-remainder of a polynomial
$\mathrm{NF}_{\mathcal{O},I}(f)$	normal form of f with respect to an order ideal
$\mathrm{BF}_{\mathcal{O}}(f)$	border form of a polynomial
$\mathrm{S}(f,g)$	S-polynomial of two polynomials
$\mathrm{LF}_\Psi(v)$	leading form of a vector with respect to a filtration
$\mathrm{LF}_I(f)$	leading form of f with respect to an I-adic filtration
$\mathrm{WR}_{\sigma,\mathcal{G}}(f)$	weak remainder of a polynomial
$\mathrm{LF}_{\sigma,\mathcal{G}}(f)$	σ-leading form of f with respect to an induced grading
$\mathrm{NF}_{\sigma,S}(f)$	normal form of f with respect to a subalgebra

6. Power Series and Laurent Series

$\mathrm{HS}_f(z)$	associated Laurent series of an integer Laurent function
$\mathrm{HS}_M(z)$	Hilbert series of a module
$\mathrm{HN}_M(z)$	Hilbert numerator of a module
$\mathrm{Ver}_d(f)$	d^{th} Veronese series of a Laurent series
$\mathrm{HS}^a_{P/I}(z)$	affine Hilbert series of an affine algebra
$\mathrm{HN}^a_{P/I}(z)$	affine Hilbert numerator of an affine algebra
$\mathrm{hn}^a_{P/I}(z)$	simplified affine Hilbert numerator of an affine algebra
$\mathrm{HS}_{M,W}(\mathbf{z})$	multivariate Hilbert series of a module
$\mathrm{HN}_M(z_1, \ldots, z_m)$	multivariate Hilbert numerator of a module
$\mathrm{Had}(f,g)(z)$	Hadamard product of two univariate power series
$\mathrm{HS}_{R,\overline{\mathfrak{q}}}(z)$	$\overline{\mathfrak{q}}$-adic Hilbert series of a ring
$\mathrm{MS}_G(z)$	Molien series of a ring of invariants

7. Rings and Fields

R_+	sums of homogeneous elements of positive degree in R
$K[f_1, \ldots, f_s]$	subalgebra of $K[x_1, \ldots, x_n]$ generated by $f_1, \ldots, f_s$
$R[[z_1, \ldots, z_n]]$	(formal) power series ring
$R[[z]]_z$	ring of Laurent series
$R[z, z^{-1}]$	ring of Laurent polynomials
$R^{(d)}$	d^{th} Veronese subring of R

$K[Y]$	K-subalgebra of a polynomial ring generated by the polynomials in Y
$R[[\mathbf{z}, \mathbf{z}^{-1}]]_\sigma$	σ-Laurent series ring
$\mathcal{R}(I)$	Rees ring of an ideal
$\mathrm{Diag}(R)$	diagonal subalgebra of a bigraded ring
$\mathrm{Seg}(R, S)$	Segre product of two standard graded algebras
S^G	invariant ring of S under the action of G
$\mathrm{Slsa}_{(r,s)}(P)$	straight line subalgebra of a polynomial ring
$\mathrm{End}_K(V)$	endomorphism ring of a vector space
$\mathrm{gr}_\Phi(R)$	associated graded ring with respect to a filtration
$\mathrm{gr}_I(R)$	associated graded ring with respect to an I-adic filtration

8. Ideals and Modules

$M_{W,d}$	homogeneous elements of degree d with respect to the grading given by W
$M(d)$	module obtained by shifting degrees
$\mathcal{I}^+(S)$	homogeneous vanishing ideal of $S \subseteq \mathbb{P}^n_K$
$\mathrm{DF}_W(M)$	degree form module
I^{hom}	homogenization of an ideal
I^{deh}	dehomogenization of an ideal
I_W	W-homogeneous part of an ideal
I_{mon}	monomial part of an ideal
$\langle M_{\leq d} \rangle$	submodule generated by the homogeneous elements of degree $\leq d$ in a module
$R \ltimes M$	idealization of a module
$\imath(M)$	ideal of a module in its idealization
I_M	idealization ideal of a module
$\tilde{I}_M$	ideal of the presentation of a module
$M \otimes_K L$	module obtained by base field extension
$V \otimes_K W$	tensor product of vector spaces
$\overline{V}^{\,\ell}$	ℓ-reduction of a vector subspace of the polynomial ring
$\mathtt{Lex}(I)$	Lex-segment ideal associated to I
$\mathrm{gin}_\sigma(I)$	generic initial ideal
I^{top}	top-dimensional (or equi-dimensional) part of an ideal
$R[[\mathbf{z}, \mathbf{z}^{-1}]]$	module of extended power series
I_{Seg}	defining ideal of a Segre product
$I(\mathcal{A})$	toric ideal associated to a matrix
I_V	lattice ideal associated to a set of vectors
$D_\pi(I)$	distraction of a monomial ideal
I^{inf}	image under $x_0 \mapsto 0$ of a homogeneous ideal
$\mathrm{BF}_{\mathcal{O}}(I)$	border form ideal of I with respect to an order ideal
$F_\gamma M$	γ^{th} vector space of a filtration of M
$\mathrm{gr}_\Psi(M)$	associated graded module with respect to a filtration

$F_{<_\sigma \gamma} M$	union of all $F_{\gamma'} M$ for which $\gamma' <_\sigma \gamma$
$\mathrm{LF}_\Psi(N)$	leading form module of a submodule
$\mathrm{LF}_I(J)$	leading form ideal of J with respect to an I-adic filtration
$\mathrm{Rel}(\mathcal{G})$	ideal of algebraic relations of $\mathcal{G}$
$I_{h,K}(\mathcal{T})$	hypothesis ideal of a model
$I_c(\mathcal{T})$	condition ideal of a model
$I_{opt}(\mathcal{T})$	optimal hypothesis ideal of a model

9. Matrices

$\mathcal{M}^{\mathrm{adj}}$	adjoint matrix
$\mathcal{T}_a$	associated antisymmetric matrix of a vector in $\mathbb{R}^3$
$a \otimes b$	Kronecker product of two vectors in $\mathbb{R}^3$
$\overline{\mathcal{A}}$	Lawrence lifting of a matrix
$\mathrm{Jac}(\mathcal{F})$	Jacobian matrix of a tuple of polynomials
$\mathrm{Hess}(\mathcal{F})$	Hessian matrix of a tuple of polynomials

10. Mathematical Operators

$\mathrm{topdeg}_W(f)$	top degree of a polynomial
$\log_{x_i}(t)$	exponent of x_i in a term
$\deg((i,j))$	degree of a critical pair
$\mu(M)$	minimal number of generators of a module
$\beta_{ij}(M)$	graded Betti numbers of a module
α_f	initial degree of an integer Laurent function
$\alpha(M)$	initial degree of a module
$\mathrm{ri}(f)$	regularity index of an integer function of polynomial type
$\mathrm{ri}(M)$	regularity index of a module
$\Sigma\deg(I)$	total degree of a monomial ideal
$\mathrm{hv}(M)$	h-vector of a module
$\dim(M)$	dimension of a module
$\mathrm{mult}(M)$	multiplicity of a module
$n_{[i]}$	binomial representation of n in base i
$\mathrm{Top}_i(n)$	top binomial representation of n in base i
$\mathrm{codim}_K(V)$	codimension of a vector subspace
$\mathrm{ri}^a(P/I)$	affine regularity index of an affine algebra
$\mathrm{Min}(R)$	set of all minimal primes of a ring
$\mathrm{Kdim}(R)$	Krull dimension of a ring
$\mathrm{cdim}(R)$	combinatorial dimension of a ring
$\mathrm{trdeg}_K(L)$	transcendence degree of a field extension L/K
$\mathrm{Ass}(M)$	set of associated primes of a module
a^+, a^-	positive and negative part of a tuple if integers
$\mathrm{Gaps}(B)$	set of gaps of a submonoid of $\mathbb{N}^n$

$\gcd_S(f_1, \ldots, f_r)$	greatest common divisor of a subset
$\operatorname{lcm}_S^+(f_1, \ldots, f_r)$	modified least common multiple of a subset
$\operatorname{fac}_S(f_1, \ldots, f_r)$	quotient of $\gcd_S(f_1, \ldots, f_r)$ by $\operatorname{lcm}_S^+(f_1, \ldots, f_r)$
$r_{\mathbb{X}}$	regularity index of a projective point set
$\deg_{\mathbb{X}}(p)$	degree of a point in a projective point set
$\operatorname{ind}_{\mathcal{O}}(f)$	index of f with respect to an order ideal
$\operatorname{ord}_{\Psi}(v)$	order of a vector with respect to a filtration
$\operatorname{ec}(f)$	écart of a polynomial
$\operatorname{edim}(R_{\mathfrak{m}})$	embedding dimension of a local ring
$\operatorname{Sing}(V)$	singular locus of an affine variety
$\operatorname{Mil}_p(V)$	Milnor number of an affine variety at a point
$\operatorname{Tju}_p(V)$	Tjurina number of an affine variety at a point
$\xrightarrow{G}_{\mathrm{ss}}$	subalgebra reduction step using an element of G
$\xrightarrow{G}_{\mathrm{s}}$	subalgebra rewrite relation defined by G
$\xleftrightarrow{G}_{\mathrm{s}}$	equivalence relation defined by $\xrightarrow{G}_{\mathrm{s}}$
$\deg_{\sigma,\mathcal{G}}(f)$	σ-degree of f with respect to an induced grading
$\operatorname{trace}(\mathcal{A})$	trace of a matrix

Bibliography

[Ab00] J. Abbott, A. Bigatti, M. Kreuzer and L. Robbiano, Computing ideals of points, J. Symb. Comput. **30** (2000), 341–356

[AKR05] J. Abbot, M. Kreuzer, and L. Robbiano, Computing zero-dimensional schemes, J. Symb. Comput. **39** (2005), 31–49

[BK96] S. Beck and M. Kreuzer, How to compute the canonical module of a set of points, in: L. Gonzalez-Vega and T. Recio (eds.), Algorithms in algebraic geometry and applications, Proc. Conf. MEGA 1994, Birkhäuser, Basel 1995

[Bi97] A. Bigatti, Computation of Hilbert-Poincarè series, J. Pure Appl. Alg. **119** (1997), 237–253

[BCR05] A. Bigatti, A. Conca, and L. Robbiano, Generic initial ideals and distractions, Commun. in Algebra (to appear)

[BH93] W. Bruns and J. Herzog, Cohen-Macaulay rings, Cambridge University Press, Cambridge 1993

[BS87] D. Bayer and M. Stillman, A criterion for detecting m-regularity, Invent. Math. **87** (1987), 1–11

[CR90] G. Carrà and L. Robbiano, On superG-bases, J. Pure Appl. Alg. **68** (1990), 279–292

[Ch88] S.-C. Chou, Mechanical geometry theorem proving, Math. and Its Appl. **41**, D. Reidel Publ. Comp., Dordrecht 1988

[Co93] H. Cohen, A course in computational algebraic number theory, Graduate Texts in Math. **138**, Springer, Heidelberg 1993

[Co99] A.M. Cohen, H. Cuypers, and H. Sterk (eds.), Some tapas of computer algebra, Algorithms and Computation in Math. **4**, Springer, Berlin 1999

[CHV96] A. Conca, J. Herzog, and G. Valla, Sagbi bases with applications to blow-up algebras, J. Reine Angew. Math. **474** (1996), 113–138

[CLS04] D. Cox, J. Little, and D. O'Shea, Using algebraic geometry, second ed., Springer, New York 2004

[DGO85] E.D. Davis, A.V. Geramita, and F. Orecchia, Gorenstein algebras and the Cayley-Bacharach theorem, Proc. Amer. Math. Soc. **93** (1985), 593–597

[DE05] A. Dickenstein and I. Emiris (eds.), Solving polynomial equations: foundations, algorithms, and applications, Springer, Berlin 2005

[DK02] H. Derksen and G. Kemper, Computational invariant theory, Springer, Berlin 2002

[EGH96] D. Eisenbud, M. Green, and J. Harris, Cayley-Bacharach theorems and conjectures, Bull. Amer. Math. Soc. **33** (1996), 295–324

[Ei02] D. Eisenbud, D.R. Grayson, M. Stillman, and B. Sturmfels (eds.), Computations in algebraic geometry with Macaulay 2, Algorithms and Computation in Math. **8**, Springer, Berlin 2002

[Fa99] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases (F4), J. Pure Appl. Alg. **139**(1999), 61–88

[Fa02] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), in: Symbolic and algebraic computation, Proc. Int. Symp. ISSAC 2002, ACM Press, New York 2002
[Ga00] K. Gatermann, Computer algebra methods for equivariant dynamical systems, Lect. Notes in Math. **1728**, Springer, Berlin 2000
[GG03] J. von zur Gathen and J. Gerhard, Modern computer algebra, second ed., Cambridge Univ. Press, Cambridge 2003
[GKR93] A.V. Geramita, M. Kreuzer, and L. Robbiano, Cayley-Bacharach schemes and their canonical modules, Trans. Amer. Math. Soc. **339** (1993), 163–189
[GKW03] J. Grabmeier, E. Kaltofen, and V. Weispfenning (eds.), Computer algebra handbook, Springer, Heidelberg 2003
[Gr96] M.L. Green, Generic initial ideals, in: J. Elias, J.M. Giral, R.M. Mirò-Roig, and S. Zarzuela (eds.), Summer School on Commutative Algebra, Vol. II, Centre de Recerca Matemàtica, Barcelona 1996
[GP02] G.-M. Greuel and G. Pfister, A Singular introduction to commutative algebra, Springer, Berlin 2002
[Ha94] J.P. Hansen, Points in uniform position and maximum distance separable codes, in: F. Orecchia and L. Chiantini (eds.), Zero-Dimensional Schemes, Proc. Conf. Ravello 1992, de Gruyter, Berlin 1994
[Ho98] H. Hong, Groebner bases under composition I, J. Symb. Comput. **25** (1998), 643–663
[KM89] D. Kapur and K. Madlener, A completion procedure for computing a canonical basis of a k-subalgebra, in: E. Kaltofen and S. Watt (eds.), Proc. Conf. Computers and Mathematics 1989, MIT Press, Cambridge 1989
[KK04] A. Kehrein and M. Kreuzer, Characterizations of border bases, J. Pure Appl. Algebra **196** (2005), 251–270
[Kn97] D.E. Knuth, The art of computer programming 1: fundamental algorithms, Addison-Wesley, Reading 1997
[Lo04] J. de Loera, R. Hemmeke, J. Tauzer, and R. Yoshida, Effective lattice point counting in rational convex polytopes, J. Symb. Comput. **38** (2004), 1273–1302
[Mar91] H. Markowitz, Portfolio selection, Blackwell Publ., Oxford 1991
[Mat86] H. Matsumura, Commutative ring theory, Cambridge Univ. Press, Cambridge 1986
[May93] S. Maybank, Theory of reconstruction from image motion, Springer Series in Information Sc. **28**, Springer, Berlin 1993
[MS05] E. Miller and B. Sturmfels, Combinatorial commutative algebra, Graduate Texts in Math. **227**, Springer, New York 2004
[Na62] M. Nagata, Local rings, Interscience Tracts in Pure and Appl. Math. **13**, Wiley, New York 1962
[No02] P. Nordbeck, SAGBI bases under composition, J. Symb. Comput. **33** (2002), 67–76
[Ro86] L. Robbiano, On the theory of graded structures, J. Symb. Comput. **2** (1986), 139–170
[RS90] L. Robbiano and M. Sweedler, Subalgebra bases, in: W. Bruns and A. Simis (eds.), Commutative algebra, Proc. Workshop Salvador 1988, Lect. Notes in Math. **1430**, Springer, Berlin 1990, pp. 61–87
[Sc03] H. Schenck, Computational algebraic geometry, London Math. Soc. Stud. Texts **58**, Cambridge Univ. Press, Cambridge 2003
[Ste04] H. Stetter, Numerical polynomial algebra, SIAM, Philadelphia 2004
[Stu93] B. Sturmfels, Algorithms in invariant theory, Texts and Monographs in Symbolic Computation, Springer, Wien 1993
[Stu96] B. Sturmfels, Gröbner bases and convex polytopes, University Lect. Ser. **8**, Amer. Math. Soc., Providence 1996

[Stu02] B. Sturmfels, Solving systems of polynomial equations, CBMS Regional Conference Series in Math. **97**, Amer. Math. Soc., Providence 2002

[TUO03] A. Torstensson, V. Ufnarovski, and H. Öfverbeck, On SAGBI bases and resultants, in: J. Herzog and V. Vuletescu (eds.), Commutative algebra, singularities, and computer algebra, Proc. Sinaia 2002, NATO Science Series, Kluwer, Dordrecht 2003

[Val96] G. Valla, Problems and results on Hilbert functions of graded algebras, in: J. Elias, J.M. Giral, R.M. Mirò-Roig, and S. Zarzuela (eds.), Summer School on Commutative Algebra, Vol. I, Centre de Recerca Matemàtica, Barcelona 1996

[Vi01] R. Villareal, Monomial algebras, Marcel Dekker, New York 2001

[Wu94] W.T. Wu, Mechanical theorem proving in geometries, Texts and Monographs in Symb. Comput., Springer, Berlin 1994

[ZS60] O. Zariski and P. Samuel, Commutative algebra, vol. II, Van Nostrand Company, Princeton 1960

Index