On the Integration of Elementary Functions: Computing the Logarithmic Part

by

Brian L. Miller, B.S. M.S.

A Dissertation

In

Mathematics and Statistics

Submitted to the Graduate Faculty
of Texas Tech University in
Partial Fulfillment of
the Requirements for the Degree of

Doctor of Philosophy

Approved

Lourdes Juan

Kevin Long

Mara Neusel

Arne Ledet
Dean of the Graduate School

May, 2012

ACKNOWLEDGEMENTS

I would like to express my great appreciation and gratitude to my dissertation advisor, Professor Lourdes Juan, for her advice and guidance. I would also like to thank Professor Arne Ledet for several conversations that led to a better understanding of certain aspects of this work. In addition, I would like to thank the Graduate School.

TABLE OF CONTENTS

ABSTRACT

Abstract: We first provide an algorithm to compute the logarithmic part of an integral of an algebraic function. The algorithm finds closed-form solutions that have been difficult to compute by other means. We then provide an algorithm to compute the logarithmic part of a function lying in a transcendental elementary extension. We are able to fully justify the algorithms using techniques of Gröbner bases, differential algebra, and algebraic geometry.

CHAPTER I
INTRODUCTION

The problem of integration in finite terms (also known as integration in closed form) consists of deciding, in a finite number of steps, whether a given element in a field K has an elementary integral over K, and if it does, to compute it.

Both Abel and Liouville addressed this problem in the early 1800s. Although no algorithm was given by them, Liouville established the basis for future algorithms by showing that an elementary function has an elementary integral if and only if it has a representation similar to the partial fraction decomposition of rational functions in calculus (see Liouville's Theorem in Section 2.2). In the 1960s and 1970s, Risch provided in a series of papers a complete decision algorithm for integrating functions that lie in a transcendental elementary extension [27, 28, 29]. However, his recursive approach requires multiple substitutions that can lead to large systems of equations to be solved symbolically, making it difficult to implement. Bronstein in [6] gives a complete decision procedure for integrating in a transcendental elementary extension and practical algorithms for doing so.

The integration of algebraic functions, however, has remained challenging. A solution to this problem was first outlined by Risch in [30], but it has been difficult to implement mainly because the method given does not provide a way to construct or find the required divisors. However, he did set the stage for determining bounds on principal divisors. A new algorithm for integrating algebraic functions was provided in 1981 by Davenport [11], but it depends on Puiseux expansions and the complete splitting of the denominator, which is not always practical or possible to compute.

The use of divisors to attack integrals containing algebraic expressions dates back to the 1890s [13]. Trager, in his PhD thesis [33], developed an algorithm that first removed multiple poles from the integrand and then used divisors to compute the remaining part. A few years later, Bronstein extended Trager's algorithm to include elementary functions: Trager's algorithm is set up for fields of the type $K(x, y)$ where $Dx = 1$ and y is algebraic over $K(x)$ while Bronstein works over a tower of fields that contain some elementary transcendental extensions followed by an algebraic one. Their approach has also encountered obstacles in the implementation.

An algorithm by Kauers [16] uses Gröbner bases instead of divisors to alleviate some of the computational difficulties that arise from the use of divisors in the previous procedures. Even though the algorithm is incomplete [16], it proves to be successful in many cases where the integrators implemented in Axiom, Maple and Mathematica fail.

In the first part of this dissertation, we use the ideas of [16] to produce a new algorithm for computing the so-called logarithmic part of an integral of an algebraic function when the minimal polynomial for the algebraic element has no singularities. Our algorithm allows us to compute integrals that cannot be evaluated using the previous methods. We use techniques of Gröbner bases, differential algebra, and algebraic geometry.

The second part of this dissertation extends Czichowski's observation [10] to compute the logarithmic part of an integral of a function containing elementary and Liouvillian monomials.

The next section lays out the definitions and terminology used henceforth.

CHAPTER II
PRELIMINARIES

2.1 Differential Algebra

We work with differential fields of characteristic 0.

Definition 2.1.1. *A differential field is a pair (K, D) where K is a field and D is an additive map $D : K \longrightarrow K$ satisfying Leibniz's rule $D(ab) = aDb + bDa$ for $a, b \in K$.*

We will sometimes use $'$ instead of D. If there is no ambiguity with the derivation, we simply write K. The set $\mathrm{Const(K)} = \{c \in K \mid Dc = 0\}$ is a subfield of K, called *the subfield of constants*. A differential extension of (K, D) is a differential field (L, Δ) such that $L \supset K$ and $\Delta a = Da$ for all $a \in K$. For more details on differential fields, see for instance [6, 9, 25, 34].

Let K be a differential field and $L \supset K$ a differential field extension. An element $\theta \in L$ is said to be

(i) a *logarithm* over K if $D\theta = Dt/t \in K$ for some $t \in K$

(ii) an *exponential* over K if $D\theta/\theta = Dt$ for some $t \in K$

(iii) *algebraic* over K if $p(\theta) = 0$ for a polynomial p with coefficients in K.

An element $\theta \in L$ is elementary over K if θ is a logarithm, exponential, or algebraic over K. $L = K(\theta_1, \ldots, \theta_n)$ is an *elementary extension* of K if θ_i is elementary over $K(\theta_1, \ldots, \theta_{i-1})$ for $1 \leq i \leq n$. We say that $f \in K$ has an *elementary integral* over K if there exists an elementary extension F of K and $g \in F$ such that $Dg = f$. In this case we write $\int f = g$.

2.2 Liouville's Theorem and Related Computational Aspects

Liouville's Theorem provides a means for determining whether a given elementary function has an elementary integral and gives an explicit formula for such functions. It constitutes the basis for our algorithm.

Theorem 2.1 (Liouville's Theorem)**.** *Let K be a differential field of characteristic zero with constant field C and let $f \in K$. If the equation $g' = f$ has a solution*

$g \in L$ where L is an elementary extension of K having the same constant field C, then there exist $v, u_1, u_2, \ldots, u_n \in E$ and constants $c_1, \ldots, c_n \in C$ such that

$$f = g' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}$$

therefore, $\int f = g + \sum_{i=1}^{n} c_i \log u_i$.

The c_i are residues of f, cf. [33]. The function g is referred to as the *integral* or *rational* part while $\sum_{i=1}^{n} c_i \frac{u_i'}{u_i}$ is called the *logarithmic part*. We are interested in computing the logarithmic part in the setting where $L = K(\theta, \overline{y})$ where θ is elementary over an elementary extension K of the constants and $\overline{y}$ is algebraic over $K(\theta)$, with minimal polynomial $F(y)$ over $K(\theta)$.

2.2.1 The Integral Part

Suppose that f is a rational function in $K(x)[y]/\mathrm{Id}(F(x,y))$ where $\mathrm{Id}(F(x,y))$ denotes the ideal generated by $F(x,y)$, and $F(x,y)$ is the minimal polynomial of $\overline{y}$ as before. Computing the integral part of $\int f$ involves reducing the order of the poles of the denominator to 1 and eliminating factors of the denominator that are special [2]. (A polynomial p is special if $\gcd(p, Dp) \neq 1$.) The algorithms by Trager [33] and Bronstein [2, 4] to compute this part of the integral are essentially Hermite reduction adapted to functions containing algebraic expressions (see [6] or [12] for a discussion of Hermite reduction in an elementary transcendental extension).

2.2.2 The Logarithmic Part

The algorithms for computing the integral part produce a new integrand that has a denominator v, which is normal with respect to D; i.e., $\gcd(Dv, v) = 1$. In order to complete the computation of the logarithmic part, we will need to compute an integral basis for the integral closure of $K[x]$ in $K(x,y)$. That is, we compute a basis for

$$\mathcal{B}_{K[x]} = \{\eta \in K(x, \overline{y}) \mid \eta \text{ is integral over } K[x]\}.$$

There are two reasons why we need to do this. Firstly, rational expressions of integral functions are not unique. However, if $\{b_1, \ldots, b_m\}$ is a basis for $\mathcal{B}_{K[x]}$, any function in $K(x)[y]/\mathrm{Id}(F)$ can be written uniquely in terms of $\{b_1, \ldots, b_m\}$. This aids us in obtaining a more deterministic algorithm. Secondly, writing our integrand in terms of an integral basis allows us to separate elements that have poles from those that do not. Integral elements of $K(x)[y]/\mathrm{Id}(F)$ are defined at all values in K.

Example 2.2.1. Consider the ring $\mathbb{Q}(x)[y]/\mathrm{Id}(y^3 - x^2(x+1))$. A basis for $\mathcal{B}_{\mathbb{Q}[x]}$ is $\left\{1, y, \frac{y^2}{x}\right\}$ as given in [33]. Consider the element $\frac{y^2}{x}$. At first it may appear to have a pole at $x = 0$. However, it satisfies the polynomial $w^3 - x(x+1)^2$. Thus $\left(\frac{y^2}{x}\right)^3 = x(x+1)^2$. Hence $\left(\frac{y^2}{x}\right)^3$, and therefore $\frac{y^2}{x}$, do not have a pole at $x = 0$.

Finding the correct poles of the integrand is essential in this computational endeavor.

2.3 Polynomials and Gröbner Bases

Let $s, t \in K[x_1, x_2, \ldots, x_m]$ be monomials. We can write $s = s_1 s_2$ and $t = t_1 t_2$ where $s_1, t_1 \in K[x_1, \ldots, x_i]$ and $s_2, t_2 \in K[x_{i+1}, \ldots, x_m]$. A block order on $k[x_1, \ldots, x_m]$ is a monomial order $(\leq_1, \leq_2)$ such that $\leq_1$ is an order on $[x_1, x_2, \ldots, x_i]$, $\leq_2$ is an order on $[x_{i+1}, \ldots, x_m]$ and we have that $s = s_1 s_2 < t_1 t_2 = t$ if and only if $s_1 <_1 t_1$ or $s_1 = t_1$ and $s_2 <_2 t_2$. That is, elements in $K[x_1, \ldots, x_m]$ are first ordered using $\leq_1$ and ties are then broken with $\leq_2$ (see [1]).

Our computations will mostly take place in the polynomial ring $K[x, y, z]$. If I is an ideal in this ring, GröbnerBasis(I) will mean a reduced Gröbner Basis of I with respect to the elimination order where the order on $[x, y]$ is a graded order and the order on $[z]$ is the lexicographic order. By a graded order, we mean an order such as Graded Reverse Lex Order as in [8] or the total degree-lexicographic order in [1]. We will usually denote such a term order by $\leq$.

Let $p = \sum_{i=0}^{n} a_i x^i$ be a polynomial in a unique factorization domain. The *content* of p with respect to x is $\gcd(a_0, \ldots, a_n)$. The *primitive part* of p is then $\mathrm{pp}_x = \frac{p}{\mathrm{content}(p)}$.

A multivariate polynomial is *absolutely irreducible* over K if it remains irreducible over any finite algebraic extension of K. Throughout, $F(x, y)$, or simply F, will always be the monic irreducible polynomial for $\overline{y}$ over $K(\theta)$. We write it as a function of x as well as of y to emphasize the fact that θ is an elementary function of x, such a logarithm or exponential, and K itself can be an elementary extension of the constants by such functions. We will assume that $F(x, y)$ is absolutely irreducible over K and is nonsingular.

Resultants play an important role in integration algorithms. For convenience we provide a few definitions and results relating to resultants.

Definition 2.3.1. *Let $f, g \in K[x]\{0\}$ such that $f = a_n x^n + \cdots + a_1 x + a_0$ and*

$g = b_m x^m + \cdots + b_1 x + b_0$ *where* $a_n \neq 0$, $b_m \neq 0$, *and either* n *or* m *is nonzero. The* **Sylvester matrix** *of* f *and* g *is the* $(n+m) \times (n+m)$ *matrix:*

$$S(f,g) = \begin{pmatrix} a_n & \cdots & \cdots & \cdots & a_1 & a_0 & & \\ & & & \ddots & & & & \\ & & a_n & \cdots & \cdots & \cdots & a_1 & a_0 \\ b_m & \cdots & b_1 & b_0 & & & & \\ & & \ddots & & & & & \\ & & & \ddots & & & & \\ & & & & \ddots & & & \\ & & & & b_m & \cdots & b_1 & b_0 \end{pmatrix}.$$

The **resultant** *of* f *and* g *is the determinant of* $S(f,g)$.

We will abbreviate resultant(f,g) as res(f,g). In the case that f and g are multivariate, we will use a subscript on res to indicate which variable the resultant is being applied.

Example 2.3.2. Let $f = 2x^2 - t^2 - 1$ and $g = x^2 + t^2 x - t + 1$ where $f, g \in \mathbb{Q}[x,t]$. We then have $S(f,g)$, with respect to t:

$$\begin{pmatrix} -1 & 0 & 2x^2-1 & 0 \\ 0 & -1 & 0 & 2x^2-1 \\ x & -1 & x^2+1 & 0 \\ 0 & x & -1 & x^2+1 \end{pmatrix}.$$

Thus $\text{res}_t(f,g) = (x+1)(4x^5 - 3x^3 + 5x^2 - 4x + 2)$. However, $S(f,g)$ with respect to x is given by

$$\begin{pmatrix} 2 & 0 & -t^2-1 & 0 \\ 0 & 2 & 0 & -t^2-1 \\ 1 & t^2 & -t+1 & 0 \\ 0 & 1 & t^2 & -t+1 \end{pmatrix}.$$

Hence $\text{res}_x(f,g) = (1-t)(2t^5 + 2t^4 + 3t^3 + 7t^2 - 3t + 9)$.

Proposition 2.3.1. *Let* $f, g \in K[x] \setminus \{0\}$. *Then* $res_x(f,g) = 0$ *if and only if there exists* $\gamma \in \overline{K}$ *such that* $f(\gamma) = g(\gamma) = 0$.

Proof. See Corollary 1.4.1 [6]. □

Another important result pertaining to resultants that we will use later is stated below.

Proposition 2.3.2. *Let $f, g \in K[x] \setminus \{0\}$. Suppose that $\alpha_1, \ldots, \alpha_n$ are the zeros of f. Then*

$$res_x(f,g) = c \prod_{i=1}^{n} g(\alpha_i).$$

Proof. See Theorem 9.3 [12]. □

Throughout we will use ˆ to indicate an element of K.

2.4 Commutative Algebra and Algebraic Geometry

Commutative algebra and algebraic geometry play a central role in our algorithm and its justification. Next we present a few definitions that will be used in the sequel.

Definition 2.4.1. *The set of all common zeros of an ideal I in $K[x, y, z]$ is called the* **variety** *of I.*

A variety V is irreducible if for any varieties V_1 and V_2 with $V = V_1 \bigcup V_2$, we have $V = V_1$ or $V = V_2$.

Definition 2.4.2. *The field E is a function field in r variables over K if E is finitely generated over K and has transcendence degree r over K.*

Definition 2.4.3. *Let V be an irreducible variety. The field of fractions of the coordinate ring $K[V]$ is the* **function field** *or* **field of rational functions of** *V, and is denoted $K(V)$.*

Definition 2.4.4. *The* **dimension** *of V, denoted $\dim V$, is the transcendence degree of the function field $K(V)$. If $W \subset V$ is a closed subvariety of V, then $\dim X - \dim Y$ is the* **codimension** *of W in V.*

Definition 2.4.5. *A rational function $f \in K(V)$ is regular at $\hat{p}$ if it can be written in the form $f = \frac{\phi}{\psi}$ with $\phi, \psi \in K[V]$ and $\psi(\hat{p}) \neq 0$.*

An ideal with a finite number of zeros is called *zero-dimensional*. The nomenclature arises from the fact that a variety consisting of a finite number of points has dimension 0.

If V is irreducible, and $\hat{p} \in V$, $\mathcal{O}_{\hat{p}}$ is the subring of $K(V)$ consisting of all functions that are regular at $\hat{p}$. That is, $\mathcal{O}_{\hat{p}}$ consists of fractions $\frac{\phi}{\psi}$ with $\phi, \psi \in K[V]$ and $\psi(\hat{p}) \neq 0$.

Definition 2.4.6. *Functions* $\pi_1, \ldots, \pi_n \in \mathcal{O}_{\hat{p}}$ *are* **local parameters***, or* **uniformizing parameters***, at* $\hat{p}$ *if* $\pi_1, \ldots, \pi_n$ *generate the maximal ideal of* $\mathcal{O}_{\hat{p}}$*.*

CHAPTER III
COMPUTING THE LOGARITHMIC PART

3.1 Residues of the Integrand

Write the integrand f in the form $f = \frac{u(x,y)}{v(x)}$. In the case where $Dx = 1$ and K is a field of constants, Trager [33] devised an algorithm to find the residues. For brevity and without having to introduce additional definitions and formulas, we repeat the argument in [12] here to justify Trager's algorithm. Let $\hat{x}$ be a pole of f. Using the polynomial $F(x, y)$, we can find a value $\hat{y}$ such that $F(\hat{x}, \hat{y}) = 0$. We then have that $\hat{z}$ is a residue of f at $(\hat{x}, \hat{y})$ if and only if $\frac{u(\hat{x},\hat{y})}{v'(\hat{x})} = \hat{z}$ [12]. That is, using the latter equation, $\hat{z}$ is a residue of f if and only if it is a solution of $u(\hat{x}, \hat{y}) - zv'(\hat{x}) = 0$. Recall that the resultant of two polynomials is 0 if and only if they share a common factor (or zero). We will use res for resultant. Given a value $\hat{x}$ such that $v(\hat{x}) = 0$, we are interested in values $\hat{y}$ and $\hat{z}$ that make $\text{res}_y(u(\hat{x}, y)-zv'(\hat{x}), F(\hat{x}, y)) = 0$. The primitive part of $\text{res}_y(u(\hat{x}, y) - zv'(\hat{x}), F(\hat{x}, y))$ is taken to remove any false zeros, i.e., those coming from any factors that $\text{res}_y(u(\hat{x}, y)-zv'(\hat{x}), F(\hat{x}, y))$ may have with $v(x)$. Since the $\hat{x}$'s are solutions to $v(x) = 0$, we want all the solutions to

$$\text{res}_x(\text{pp}_z(\text{res}_y(u(x, y) - zv'(x), F(x, y))), v(x)).$$

Bronstein would later extend this to the case when K is an elementary extension of $k(t_1, \ldots, t_n)$ where k is a field and t_i is elementary over $k(t_1, \ldots, t_{i-1})$ for i in $\{1, \ldots, n\}$. Bronstein proceeds by first writing the integrand in terms of an integral basis $\{b_1, \ldots, b_m\}$ of $\mathcal{B}_{K[x]}$. So let $f = \frac{G(x,y)}{v(x)}$, where $G(x, y) = \sum_{i=1}^{d} A_i b_i$ and $A_i \in K(x)$, be our integrand written in terms of this basis. Write $G(x, y) = \frac{U(x,y)}{h(x)}$ where $U(x, y) \in K[x, y]$ and $h(x) \in K[x]$. Thus we may write our integrand as $\frac{U(x,y)}{h(x)v(x)}$. More precisely, Bronstein showed that if the integral is elementary, then $R_z = \text{res}_x(\text{pp}_z(\text{res}_y(u(x, y)-zh(x)v'(x), F(x, y))), v(x)) = \alpha P(z)$ where $\alpha \in K$ and $P(z) \in K[z]$ is monic and has constant coefficients.

In the transcendental case, e.g. when $E = K(t)$, t transcendental over K, it can be shown that $u_i = \gcd(u - c_i v', v)$ where u and v are the numerator and denominator of the integrand and c_i is a residue of the integrand. In our case, the integrand lies in a ring that is not necessarily a unique factorization domain; thus the existence of a greatest common divisor is not always guaranteed. Therefore, we need to find an alternative way to compute the u_i.

To describe the integrand at a point $(\hat{x}, \hat{y})$ where it has residue c_i, we need a function u_i that vanishes at $(\hat{x}, \hat{y})$. This will give the logarithmic differential $\frac{u_i'}{u_i}$ a pole at $(\hat{x}, \hat{y})$, and will therefore have residue at $(\hat{x}, \hat{y})$. Even though our ring may not have unique factorization, we do, however, have unique factorization in the discrete valuation rings of our ring. (If R is a discrete valuation ring, then every element in R can be written as at^n where $n \geq 0$ for a unit $a \in R$ and a uniformizing parameter t.) Since the notion of vanishing at a point corresponds to a valuation ν on our ring, it suffices to find a uniformizing parameter for that valuation ring. This has been a computational difficulty in integrating functions that contain algebraic expressions; i.e., it has been difficult to construct functions in $K(x)[y]/\mathrm{Id}(F)$ that vanish or have poles at a prescribed set of points where the integrand has residue. Furthermore, if a function is found, it is also necessary to find a valuation on $K(x)[y]/\mathrm{Id}(F)$ that returns an integer corresponding to the order of the zero or the pole. Section 4.1.3 explains how this is accomplished.

3.2 Outline of the algorithm

Let $I = \mathrm{Id}(u(x,y) - zv(x)', v(x), F(x,y))$. By the *zeros of I*, we mean $\mathbf{V}(I)$, the variety of I. Each zero of I will have an associated residue, i.e., the zeros of I are the triples $(\hat{x}, \hat{y}, \hat{z})$ such that $(\hat{x}, \hat{y})$ is a point where the integrand has residue $\hat{z}$.

Because I is zero-dimensional (which will be shown below), every prime ideal P with $I \subset P$, is the associated prime of some primary component by Lemma 8.60 in [1]. Additionally by the same lemma, every primary component of I is isolated and monadic. (A primary ideal is monadic if its associated prime is maximal.)

Since the prime ideals containing I are maximal, any $H(x,y,z) \in K[x,y,z]$ that vanishes at a point where the integrand has residue will be in an intersection of certain associated primes of a primary component of I. It is in these radical ideals where we begin our search for the u_i.

The algorithm works as follows:

1. Find $G = \text{GröbnerBasis}(I)$. Denote the minimal element of G by R_z. As shown below,

$$\widetilde{R} = \mathrm{res}_x(\mathrm{pp}_z(\mathrm{res}_y(u(x,y) - zh(x)v'(x), F(x,y))), v(x)) \in I$$

has the same zeros as R_z. (Recall that the order we are using is $[x,y] > [z]$.

Thus the minimal element in G will contain z.) Using a result from Bronstein, if the integral is elementary then $\widetilde{R} = \alpha P(z)$ where $P \in K[z]$ is monic and has constant roots and $\alpha \in K$. Thus if the integral is elementary, then R_z will be a polynomial in z. So, we can write $R_z = r_1^{e_1} \cdots r_m^{e_m}$ where the r_i are irreducible pairwise relatively prime factors over K.

2. From (1), we have $R_z = r_1^{e_1} \cdots r_t^{e_t}$. We then write $\widetilde{I} = \bigcap J_i$ where $J_i = \mathrm{Id}(I, r_i)$ and $r_i(0) \neq 0$. We do not need the exponent on the r_i since we will take the radical of the primary components of J_i at a later step. The zeros of J_i are the 3-tuples $(\hat{x}, \hat{y}, \hat{z})$ where $r_i(\hat{z}) = 0$ and $(\hat{x}, \hat{y})$ is where the integrand has residue $\hat{z}$ [33].

3. For each i, we perform a primary decomposition on J_i. Thus we write $J_i = \bigcap_j Q_{ij}$. Because each J_i is zero-dimensional, each Q_{ij} is isolated (the associated prime of Q_{ij} does not properly contain the associated prime of some other primary component) and monadic. Each zero of J_i will necessarily be a zero of one of the Q_{ij}.

4. From the previous step we have $J_i = \bigcap_j Q_{ij}$. We now compute $\sqrt{Q_{ij}} = P_{i,j}$ for each j over each i. The ideals $P_{i,j}$ are maximal and therefore prime. We will later take intersections of these prime ideals to form radical ideals. We compute a reduced Gröbner basis of each one of these ideals to look for generators that satisfy the removal condition in Section 4.1.6. We then partition the list of ideals $P_{i,j}$ on the condition that two ideals are in the same partition Ω_ℓ if they have had the same generators removed and the same univariate polynomial in z.

5. From (4), we take $\mathscr{P}_i = \left\{\bigcap_{P\in\Omega_1} P, \bigcap_{P\in\Omega_2} P, \ldots, \bigcap_{P\in\Omega_\ell} P\right\}$. (There are several examples in Section V that illustrate this.) Each ideal $\mathfrak{h} \in \mathscr{P}_i$ is radical by Lemma 3.2; thus any polynomial that vanishes on $\mathbf{V}(\mathfrak{h})$ will necessarily be contained in $\mathfrak{h}$, by the Hilbert Nullstellensatz.

6. To find a uniformizing parameter, we find a reduced Gröbner basis for $\mathfrak{h}$; set $\mathfrak{g}_1 = \mathrm{GröbnerBasis}(\mathfrak{h})$. We proceed in a way similar to Kauers [16]. For each $g \in \mathfrak{g}_1$, we test if $\mathrm{Id}(r_i, F, g) = \mathrm{Id}(r_i, F) + \mathfrak{h}$. This test is necessary because we want a polynomial that vanishes on the same set of zeros as the system $\{r_i, F, u - zv', v\}$. If we fail to find a g that satisfies this condition, then set

$\mathfrak{g}_2 = \text{GröbnerBasis}(\text{Id}(r_i, F) + \mathfrak{h}^2)$. We then test for each $g \in \mathfrak{g}_2$ whether $\text{Id}(r_i, F, g) = \text{Id}(r_i, F) + \mathfrak{h}^2$. If we fail to find a satisfactory g, we then use $\mathfrak{h}^3$ in place of $\mathfrak{h}^2$ and continue. We will provide an upper bound for the number of iterations needed to either produce a satisfactory g or stop trying to find one.

3.3 Initial results

We first want to see that the minimal element in the Gröbner basis of $\text{Id}(u(x,y) - zv', F, v)$ has the same zeros as the polynomial $P(z)$ where

$$\text{res}_x(\text{pp}_z(\text{res}_y(u(x,y) - zhv'(x), F(x,y))), v(x)) = \alpha P(z),$$

$\alpha \in K$, and $P(z) \in K[z]$. Since we have assumed F to be nonsingular, $h(x) = 1$. We can safely assume that $R(z)$ is nonconstant. If $R(z)$ were constant, there would be no residues. Thus there would be nothing to integrate.

Proposition 3.3.1. *Let*

$$R(z) = res_x(pp_z(res_y(u(x,y) - zh(x)v'(x), F(x,y))), v(x))$$

and $I = Id(u - zv', v, F)$. *Then if* $R(z) \neq 0$, $R(z)$ *and the minimal element of GröbnerBasis*(I) *have the same zeros.*

Proof. Let $\hat{x}_1, \ldots, \hat{x}_n$ be the zeros of $v(x)$ in $\overline{K}$. Since $v(x)$ is square-free, $\hat{x}_1, \ldots, \hat{x}_n$ are all distinct. For each $1 \leq i \leq n$, let $\hat{y}_{i1}, \ldots, \hat{y}_{ir}$ be the zeros of $F(\hat{x}_i, y)$ in $\overline{K}$. From Proposition 2.6 [2], we have

$$R(z) = c \prod_{i=1}^{n} \prod_{j=1}^{r} c_i(u(\hat{x}_i, \hat{y}_{ij}) - zh(\hat{x}_i)v'(\hat{x}_i))$$

where $c, c_1, \ldots, c_n \in \overline{K} \setminus \{0\}$.

Because the order that we are using to compute the Gröbner basis of I is the elimination order $[x, y] > [z]$, the minimal element of GröbnerBasis(I), denoted G_z, is the unique monic generator of $I \bigcap K[z]$. In $\overline{K}$, each solution of G_z extends to a solution of $\mathbf{V}(I)$ by the Extension Theorem [7]. Thus any $\hat{z} \in \overline{K}$ such that $R(\hat{z}) = 0$ satisfies $G_z(\hat{z}) = 0$. Conversely, any $\hat{z}$ such that $G_z(\hat{z}) = 0$ satisfies $R(\hat{z}) = 0$ since $\hat{z}$ extends to a solution of the system $\{u(x,y) - zv'(x), F(x,y), v(x)\}$. □

Lemma 3.1. *$I = Id(u(x,y) - zv(x)', v(x), F(x,y))$ is zero-dimensional.*

Proof. Suppose that the polynomial $v(x)$ has degree d. Thus, at least over the algebraic closure of K, v has d roots. Let $\hat{x}$ be a zero of $v(x)$. Since $F = y^n + \sum_{i=1}^{n-1} f_i(x)y^i$ where $f_i(x) \in K[x]$, we can solve $F(\hat{x}, y) = 0$ for y. Hence for any $\hat{x}$ such that $v(\hat{x}) = 0$, we have a finite number of solutions $\hat{y}$. Furthermore, since v is normal, any solution of v is not a solution of v'. Hence using $\hat{x}, \hat{y}$, we can always solve for z in the relation $u(\hat{x}, \hat{y}) - zv(\hat{x})' = 0$. This yields a finite number of zeros for the ideal J. □

By Lemma 8.60 [1], the preceeding Lemma implies that there is only one primary decomposition of I.

Lemma 3.2. *Let $I = Id(u - zv', v, F)$ and $I = \bigcap_{i=1}^{n} Q_i$ the primary decomposition of I. Let $P_i = \sqrt{Q_i}$. Then any nonempty intersection of the P_i is radical.*

Proof. Let $\mathscr{L}$ be any subset of $\{P_1, \ldots, P_n\}$. By Proposition 4.3.16 [8], for any two ideals I and J, $\sqrt{I \bigcap J} = \sqrt{I} \bigcap \sqrt{J}$. Hence

$$\begin{aligned} \sqrt{\bigcap_{P \in \mathscr{L}} P} &= \bigcap_{P \in \mathscr{L}} \sqrt{P} \\ &= \bigcap_{P \in \mathscr{L}} P. \end{aligned}$$

□

We use the same notation as above. Notes:

- GröbnerBasis(Id(J)) computes the reduced Gröbner Basis with respect to a block order on $[x, y, z]$ where $[x, y]$ is ordered by graded reverse lexicographic as in [7] (or total degree-inverse-lexicographic order in [1]) and $[z]$ by lexicographic order, and orders the polynomials in the basis from least to greatest.
- If the minimal element in the Gröbner basis does not have constant roots, then the integral is not elementary and the algorithm should stop for elementary integrals.
- The left arrow $\leftarrow$ indicates an assignment from right to left.

CHAPTER IV
THE ALGORITHM

Specifications: $\sum c_i \log u_i \leftarrow \int \frac{u(x,y)}{v(x)}$

begin

$I \leftarrow \mathrm{Id}(u - zv'(x), F(x,y), v(x))$

$R_z \leftarrow$ minimal element of GröbnerBasis(I)

if $R_z$has nonconstant roots **then**

  return "Integral is not elementary" and **stop**

else

  continue

$N \leftarrow$ upper bound described below

$r_1^{e_1} \cdots r_n^{e_n} \leftarrow R_z$ (factor R_z into irreducible factors and $r_i(0) \neq 0$)

Write $\widetilde{I} = \bigcap_{i=1}^{n} J_i$ where $J_i = \mathrm{Id}(I, r_i)$

integral $\leftarrow 0$

for $i = 1$ to n **do**:

  $\mathscr{P} \leftarrow \{\}$

  $P_{i,1}, \ldots, P_{i,\ell} \leftarrow$ PrimeDecomposition(J_i)

  for j **from** 1 **to** ℓ **do**

    $G \leftarrow$ GröbnerBasis($P_{i,j}$)

  end for

  $\{\Omega_1, \ldots, \Omega_q\} \leftarrow$Partition $\{P_{i,1} \ldots, P_{i,\ell}\}$ (as explained in (4) in Section 4.1.6)

  $\mathscr{P} \leftarrow \{\bigcap_{P \subset \Omega_1} P, \ldots, \bigcap_{P \subset \Omega_q} P\}$

  for $\mathfrak{h} \in \{\Omega_1, \ldots, \Omega_q\}$ **do**

    $\mu \leftarrow 1$

    while $\mu \leq N$ **do**

      $\mathfrak{t} \leftarrow \mathrm{Id}(F, r_i) + \mathfrak{h}^\mu$

      $G \leftarrow$ GröbnerBasis($\mathfrak{t}$)

      for $p \in G$ **do**

        if $G =$ GröbnerBasis(Id(F, r_i, p) **then**

          integral $\leftarrow$ integral + $\sum_{\gamma : r_i(\gamma)=0} \frac{\gamma}{\mu} \log p(x,y,\gamma)$

          Go to next $\mathfrak{h} \in \mathscr{P}$

        end if

      end for

      $\mu \leftarrow \mu + 1$

end while
end for
end for
end

4.1 Justification

The set $\{\Omega_1, \ldots, \Omega_q\}$ is a collection of radical ideals. Let $\mathfrak{h} \in \{\Omega_1, \ldots, \Omega_q\}$ and $\mathfrak{h} = \bigcap_{i=0}^{n} M_i$ where M_i are maximal ideals for $1 \leq i \leq n$. Denote the univariate polynomial generator of $\mathfrak{h} \bigcap K[z]$ by r_z. For $\mu \in \mathbb{Z}_{>0}$, let $\mathfrak{t}_\mu = \mathrm{Id}(r_z, F) + \mathfrak{h}^\mu$ and $\mathfrak{g}_\mu = \text{GröbnerBasis}(\mathfrak{t}_\mu)$. By construction, we have $\mathfrak{t}_1 \supset \mathfrak{t}_2 \supset \cdots \supset \mathfrak{t}_\mu \supset \cdots$.

4.1.1 Multiplicity

The algorithm searches for a $p \in \mathfrak{g}_\mu$ that satisfies the relation

$$\mathrm{Id}(r_z, F, p) \quad = \quad \mathrm{Id}(r_z, F) + \mathfrak{h}^\mu \tag{4.1}$$

for some $\mu \in \mathbb{Z}_{>0}$. If a $p \in \mathfrak{g}_\mu$ is found such that (4.1) is satisfied for some μ, we have that $\frac{p'}{p}$ has residue μ (see below). Moreover, p vanishes only on $\mathbf{V}(\mathfrak{h})$ (see below). Thus $\sum_{\gamma : r_z(\gamma)=0} \frac{\gamma}{\mu} \log p$ becomes a contribution to the logarithmic part of the integral. Also, we will give an explicit formula for the bound N in the algorithm. The order of a zero of a function plays a significant role in proving these statements. Therefore, we will need to define a discrete valuation on a field that contains all the possible functions p that could potentially satisfy (4.1).

Lemma 4.1. *The ideal $\mathfrak{t}_\mu$ is zero-dimensional for all $\mu \in \mathbb{Z}_{>0}$.*

Proof. Let $\mu \in \mathbb{Z}_{>0}$. The ideal I is zero-dimensional by Lemma 3.1. Since $\mathfrak{h} \supset I$, $\mathfrak{h}$ is zero-dimensional by Lemma 6.49 [1]. By Lemma 8.46 [1], $\mathfrak{h}^\mu$ is zero-dimensional because $\mathfrak{h}$ is zero-dimensional. Lemma 6.49 [1] gives us that $\mathfrak{t}_\mu$ is zero-dimensional since $\mathfrak{h}^\mu \subset \mathfrak{t}_\mu = \mathrm{Id}(r_z, F) + \mathfrak{h}^\mu$. □

Lemma 4.2. *Let $\mu \in \mathbb{Z}_{>0}$, then $\mathfrak{t}_\mu \neq \mathfrak{t}_{\mu+1}$.*

Proof. Let $\mu \in \mathbb{Z}_{>0}$. Denote $R = K[x, y, z]$. Since $\mathfrak{h}^{\mu+1} \subset \mathfrak{h}^\mu$, $\mathfrak{t}_{\mu+1} \subseteq \mathfrak{t}_\mu$. By Proposition 4.4.9 [8], for any two ideals I and J in a polynomial ring, $J \subset I$ if and only if the ideal quotient $I : J$ is equal to the polynomial ring. We will use this proposition to show that $\mathfrak{t}_\mu \not\subset \mathfrak{t}_{\mu+1}$. That is, we will show that $\mathfrak{t}_{\mu+1} : \mathfrak{t}_\mu \neq R$. Using Proposition 4.4.10 [8] part (3), we have $\mathfrak{t}_{\mu+1} : \mathfrak{t}_\mu = \mathfrak{t}_{\mu+1} : (\mathrm{Id}(r_z, F) + \mathfrak{h}^\mu) = (\mathfrak{t}_{\mu+1} : \mathrm{Id}(r_z, F)) \bigcap (\mathfrak{t}_{\mu+1} : \mathfrak{h}^\mu)$. We have $\mathrm{Id}(r_z, F) \subset \mathfrak{t}_\mu$, so $\mathfrak{t}_\mu : \mathrm{Id}(r_z, F) = R$. Hence it remains to show that $\mathfrak{t}_{\mu+1} : \mathfrak{h}^\mu \neq R$. Because $\mathfrak{h}$ is zero-dimensional, by Theorem 6.54 [1], for any term order there exist $g_x \in \text{GröbnerBasis}(\mathfrak{h})$ such that the head monomial of g_x is a pure power of x. If the Gröbner basis of $\mathfrak{h}$ is given by $\{g_x, g_2, \ldots, g_n\}$, then a Gröbner basis of $\mathfrak{h}^\mu$, denoted by $\mathfrak{b}$, is given by products of the form $g_x^{\alpha_1} g_2^{\alpha_2} \cdots g_n^{\alpha_n}$ where $\sum_{i=1}^n \alpha_i = \mu$. By Proposition 4.4.10 [8], $\mathfrak{t}_{\mu+1} : \mathfrak{h}^\mu = \bigcap_{g \in \mathfrak{b}} (\mathfrak{t}_{\mu+1} : \mathrm{Id}(g))$. Thus if we show that $\mathfrak{t}_{\mu+1} : \mathrm{Id}(g_x^\mu) \neq R$, we are done. We claim that $\mathfrak{t}_{\mu+1} : \mathrm{Id}(g_x^\mu) = \mathfrak{h}$. Theorem 4.4.11 [8] implies that if $\{h_1, \ldots, h_p\}$ is a basis for $\mathfrak{t}_{\mu+1} \bigcap \mathrm{Id}(g_x^\mu)$, then $\{h_1/g_x^\mu, \ldots, h_p/g_x^\mu\}$ is a basis for $\mathfrak{t}_{\mu+1} : \mathrm{Id}(g_x^\mu)$. A basis for $\mathfrak{h}^{\mu+1}$ is given by products of the form $g_x^{\beta_1} g_2^{\beta_2} \cdots g_n^{\beta_n}$ where $\sum_{i=1}^n \beta_i = \mu + 1$. Let $\{f_1, \ldots, f_q\}$ denote this basis of $\mathfrak{h}^{\mu+1}$. Thus $\{f_1, \ldots, f_q, r_z, F\}$ is a basis for $\mathfrak{t}_{\mu+1}$. For each $g \in \{g_x, g_2, \ldots, g_n\}$, we have that $g_x^\mu g \in \mathfrak{t}_{\mu+1} \bigcap \mathrm{Id}(g_x^\mu)$. Now suppose that $f \in \mathfrak{t}_{\mu+1} \bigcap \mathrm{Id}(g_x^\mu)$. Since any polynomial in $\mathfrak{t}_{\mu+1}$ is in $\mathfrak{h}$, it is a linear combination of $\{g_x, g_2, \ldots, g_n\}$. Hence $f = (c_1 g_x + \cdots + c_n g_n) g_x^\mu$ where $c_1, \ldots, c_n \in R$. Applying Theorem 4.4.11 [8] to $\{g_x^\mu g_x, g_x^\mu g_2, \ldots, g_x^\mu g_n, f\}$, we have $\{g_x, g_2, \ldots, g_n, c_1 g_x + \cdots + c_n g_n\}$ as a basis for $\mathfrak{t}_{\mu+1} : \mathrm{Id}(g_x^\mu)$. But the element $c_1 g_x + \cdots + c_n g_n$ is not needed as a basis element since it is a linear combination of the other basis elements. Hence $\mathfrak{t}_{\mu+1} : \mathrm{Id}(g_x^\mu) = \mathfrak{h} \neq R$. □

Lemma 4.3. *Let $p \in \mathfrak{t}_\mu$. If p satisfies (4.1), then $p \notin \mathfrak{t}_{\mu+1}$.*

Proof. Let $p \in \mathfrak{t}_\mu$ and suppose that p satisfies (4.1). Since $\mathfrak{t}_{\mu+1} \subset \mathfrak{t}_\mu$, every $g \in \mathfrak{t}_{\mu+1}$ is reduced to 0 by $\mathfrak{g}_\mu$. The ideal $\mathrm{Id}(\mathfrak{g}_\mu)$ can be obtained from the polynomials r_z, F, p. Thus, because r_z and F are in $\mathfrak{t}_{\mu+1}$, if $p \in \mathfrak{t}_{\mu+1}$, this would contradict Lemma 4.2. □

Corollary 4.1. *Any $p \in \mathfrak{a} = \bigcap_{\mu>0} \mathfrak{t}_\mu$ cannot satisfy (4.1).*

Proof. This is immediate from Lemma 4.3. □

4.1.2 Multiplicities

By construction, the multiplicity of the z-coordinate in $\mathbf{V}(\mathfrak{t}_\mu)$ will always be 1 for any μ. However, we are interested in the multiplicity of a point $\hat{p} \in \mathbf{V}(\mathfrak{t}_\mu)$ without the z coordinate. In order to compute the multiplicity of $\hat{p}$ correctly, we will need to move to the algebraic closure of K. Recall that $\mathfrak{t}_1 = \bigcap_{i=1}^n P_i$ and that the removal condition (see 4.1.6) has been applied to P_i for $1 \leq i \leq n$. We can assume that no element of P_i satisfies the removal condition; otherwise, if an element satisfies the removal condition we have a solution to (4.1). Although each P_i for $1 \leq i \leq n$ is irreducible in $K[x,y,z]$, when regarded as an ideal in $\overline{K}[x,y,z]$, it may no longer be irreducible. Let $\mathfrak{t}_1 = \bigcap_{i=1}^{m} M_i$ where the M_i are maximal ideals in $\overline{K}[x,y,z]$. Note that for each $1 \leq i \leq m$, $M_i = \mathrm{Id}(x-\hat{x}, y-\hat{y}, z-\hat{z})$ where $(\hat{x},\hat{y},\hat{z}) \in \overline{K}^3$. Denote $\overline{M}_i = \mathrm{Id}(x-\hat{x}, y-\hat{y})$. It is clear that $(x-\hat{x})^\mu$ is the univariate polynomial of $\mathrm{Id}(F) + \overline{M}_i^\mu$. The removal condition eliminates the possibility of elements in $\mathrm{Id}(F) + \overline{M}^\mu$ reducing to $(x-\hat{x})^\epsilon$ where $\epsilon < \mu$. Similarly, $(y-\hat{y})^\mu$ is the univariate polynomial of $\mathrm{Id}(F) + \overline{M}_i^\mu$ with respect to y. The ideal $\mathrm{Id}(F) + \overline{M}_i^\mu$ therefore has μ zeros, all of which are $(\hat{x},\hat{y})$. Hence the multiplicity of $(\hat{x},\hat{y})$ in $\mathbf{V}(\mathrm{Id}(F) + \overline{M}_i^\mu)$ is μ.

Definition 4.1.1. *Let $\hat{p} \in \mathbf{V}(\mathfrak{h})$. For an element $h \in K[x,y,z]$, we define the multiplicity of h at $\hat{p}$ as follows:*

(i) $\nu_{\hat{p}}(h) = 0$ *if* $h \notin \mathfrak{t}_\mu$ *for all* μ,

(ii) $\nu_{\hat{p}}(h) = +\infty$ *if* $h \in \mathfrak{t}_\mu$ *for all* $\mu \in \mathbb{Z}^+_{>0}$,

(iii) $\nu_{\hat{p}}(h) = \mu$ *for the greatest* μ *such that* $h \in \mathfrak{t}_\mu$ *and* $h \notin \mathfrak{t}_{\mu+1}$.

In the next section we verify that p, and therefore π, vanish only on $\mathbf{V}(\mathfrak{h})$ when regarded as functions on $\mathbf{V}(F(x,y))$. Also, we will utilize multiplicity to justify dividing the residue by μ.

4.1.3 Divisors and Uniformizing Parameters

Definition 4.1.2. *Let X be an irreducible variety. A collection of irreducible subvarieties $U_1, \ldots, U_m$ of codimension 1 in X together with assigned integer multiplicities n_i is a divisor on X, denoted $\delta = n_1U_1 + \cdots + n_mU_m$..*

For an irreducible variety X, any rational function in the coordinate ring, $K(X)$, defines a principal divisor, c.f. [18, 32]. A principal divisor is written $\mathrm{div}\, f = n_1U_1 + \cdots + n_mU_m$. The multiplicities n_i correspond to the order of a zero or pole of f on U_i.

We now describe our situation. Because F is irreducible, $\mathrm{Id}(F(x,y))$ is prime, which implies that $V = \mathbf{V}(\mathrm{Id}(F(x,y)))$ is an irreducible variety. Recall that $\mathfrak{h} = \bigcap_{i=1}^{n} P_i$ where $P_i \in K[x,y,z]$ is prime for all $1 \leq i \leq n$. Let $\mathbf{V}(P_i) = U_i$. The ideals P_i are also maximal since they are zero-dimensional. By construction, $F \in P_i$ for all $1 \leq i \leq n$. From the fact that $\mathrm{Id}(F(x,y)) \subset P_i$, we have $U_i \subset V$. The variety U_i is closed since P_i is prime, and it has dimension 0 since P_i is zero-dimensional. Thus the codimension of U_i in V is 1.

Let p satisfy (4.1) for some μ. Viewed as an element of $K[x,y,z]$, p defines a hypersurface, and consequentially $\mathbf{V}(p)$ may have an infinite number of points. Trager [33] has shown that the minimal algebraic extension needed to express the logarithmic part is extending K by the roots of R_z. However, we are interested in the zeros of p as an element in the ring $K(c_1,\ldots,c_n)(x)[z,y]/\mathrm{Id}(F(x,y))$ where the c_i are residues of the integrand since this is where our integrand lies. We will show that this set of zeros is $\mathbf{V}(\mathfrak{h})$. This statement is equivalent to showing $\mathbf{V}(\mathrm{Id}(r_z,F,p)) = \mathbf{V}(\mathfrak{h})$.

Lemma 4.4. *We have*

$$\begin{aligned}\mathfrak{t}_\mu &= Id(r_z,F) + P_1^\mu \bigcap \cdots \bigcap P_m^\mu \\ &= (Id(r_z,F) + P_1^\mu) \bigcap \cdots \bigcap (Id(r_z,F) + P_m^\mu)\end{aligned}$$

for all $\mu \in \mathbb{Z}_{>0}$.

Proof. Let $J = \mathrm{Id}(r_z,F)$. Since $J \bigcap P_i^\mu \subset J$, we have

$$\begin{aligned}(J+P_1^\mu)\bigcap\cdots\bigcap(J+P_m^\mu) &= [(J+P_1^\mu)\bigcap(J+P_2^\mu)]\bigcap\cdots\bigcap(J+P_m^\mu) \\ &= \left(J\bigcap J + J\bigcap P_1^\mu + P_1^\mu\bigcap J + P_1^\mu\bigcap P_2^\mu\right)\bigcap\cdots\bigcap(J+P_m^\mu) \\ &= \left(J + P_1^\mu\bigcap P_2^\mu\right)\bigcap\cdots\bigcap(J+P_m^\mu) \\ &= \left(J\bigcap J + J\bigcap P_3^\mu + P_1^\mu\bigcap P_2^\mu\bigcap J + P_1^\mu\bigcap P_2^\mu\bigcap P_3^\mu\right)\bigcap \\ &\qquad \cdots\bigcap(J+P_m^\mu) \\ &= \left(J + P_1^\mu\bigcap P_2^\mu\bigcap P_3^\mu\right)\bigcap\cdots\bigcap P_m^\mu \\ &= J + P_1^\mu\bigcap\cdots\bigcap P_m^\mu.\end{aligned}$$

□

Theorem 4.1. *Let P_i and U_i be as above, and let p satisfy (4.1) with $\nu_{\hat{p}}(p) = \mu$. Then div $p = \mu\delta$ where $\delta = U_1 + U_2 + \cdots + U_n$. I.e., div p is a principal divisor for $\mathbf{V}(\mathfrak{h})$ on $\mathbf{V}(F)$.*

Proof. Since $\nu_{\hat{p}}(p) = \mu$, $p \in \mathfrak{t}_\mu$. Let $M_{P_i,\mu} = \mathrm{Id}(r_z,F) + P_i^\mu$ and $\mathfrak{h} = \bigcap_{i=1}^n P_i$.

Since $p \in \mathfrak{h}$, which is a radical ideal, p vanishes on $\mathbf{V}(\mathfrak{h})$. However, p may vanish on points in $\mathbf{V}(r_z, F)$ that may not be in $\mathbf{V}(\mathfrak{h})$. Recall that we are interested in the zeros of p when p is considered as an element in $K(c_1, \ldots, c_n)[x, y, z]/\mathrm{Id}(F(x, y))$. This is equivalent to wanting to know where p vanishes when it is considered a function on $\mathbf{V}(F(x, y))$ as a member of $K(c_1, \ldots, c_n)[x, y, z]$. By Theorem 4.3.4 [8],

$$\mathrm{Id}(r_z, F, p) = \mathrm{Id}(r_z, F) + \mathrm{Id}(p)$$

implies

$$\mathbf{V}(\mathrm{Id}(r_z, F, p)) = \mathbf{V}(\mathrm{Id}(r_z, F)) \bigcap \mathbf{V}(\mathrm{Id}(p)).$$

Since $\mathrm{Id}(r_z, F, p) = \mathfrak{t}_\mu$, we have

$$\mathbf{V}(\mathrm{Id}(\{r_z, F\})) \bigcap \mathbf{V}(\mathrm{Id}(p)) = \mathbf{V}(\mathfrak{t}_\mu).$$

Since $\sqrt{\mathfrak{t}_\mu} = \mathfrak{h}$, we have $\mathbf{V}(\mathrm{Id}(\{r_z, F\})) \bigcap \mathbf{V}(\mathrm{Id}(p)) = \mathbf{V}(\mathfrak{h})$. This last equality says that the zeros of p that coincide with the zeros of F are the same zeros of $\mathfrak{h}$.

Now that we know that given the relation $F(x, y) = 0$, p vanishes on $\mathbf{V}(\mathfrak{h}) = U_1 \bigcup \cdots \bigcup U_n$ and only on those points, we need to show that p, when restricting the map $\nu_{\hat{p}}$ to U_i, vanishes to the order of μ on U_i for $1 \leq i \leq n$. Since $P_1, \ldots, P_n$ are comaximal ideals,

$$(P_1 \bigcap \cdots \bigcap P_m)^\mu = P_1^\mu \bigcap \cdots \bigcap P_m^\mu.$$

Thus from Lemma 4.4, we have

$$\mathfrak{t}_\mu = M_{P_1,\mu} \bigcap \cdots \bigcap M_{P_m,\mu}.$$

We claim that $\mathrm{Id}(p) + M_{P_i,\mu+1} = M_{P_i,\mu}$. Suppose that $p \in M_{P_i,\mu+1}$. We then have:

$$\begin{aligned}
M_{P_i,\mu+1} &= \mathrm{Id}(p) + \mathrm{Id}(r_z, F) + P_i^{\mu+1} \\
&= \mathrm{Id}(r_z, F, p) + P_i^{\mu+1} \\
&= \mathfrak{t}_\mu + P_i^{\mu+1} \\
&= (M_{P_1,\mu} \bigcap \cdots \bigcap M_{P_m,\mu}) + P_i^{\mu+1} \\
&= \bigcap_{j=1}^{m} \left(\mathrm{Id}(r_z, F) + P_j^{\mu}\right) + P_i^{\mu+1} \\
&= \bigcap_{j=1}^{m} (\mathrm{Id}(r_z, F) + P_j^{\mu} + P_i^{\mu+1}) \\
&= \mathrm{Id}(1) \bigcap (\mathrm{Id}(r_z, F) + P_i^{\mu} + P_i^{\mu+1}) \\
&= \mathrm{Id}(r_z, F, p) + P_i^{\mu}.
\end{aligned}$$

The next to last line arises from the fact that since $P_i^{\mu+1}$ and P_j^{μ} are comaximal for $i \neq j$, $P_i^{\mu+1} + P_j^{\mu} = \mathrm{Id}(1)$ by exercise 12 in 4.3 [8]. The last line above holds because $P_i^{\mu+1} \subset P_i^{\mu}$. Thus we can conclude that $p \notin M_{i,\mu+1}$. This implies p vanishes to the order μ on U_i. Whence p is a principal divisor for $\mathbf{V}(\mathfrak{h})$ on $\mathbf{V}(F)$. □

4.1.4 The Resulting Integral

Since U_i has codimension 1 in V for all $1 \leq i \leq n$, Theorem 2.3.1.1 [32] gives us that U_i has a local equation, say π_i, in a neighborhood of any nonsingular point in V. Thus from Theorem 4.1 above and the discussion in 3.1.2 [32], we have $p = \prod_{i=1}^{n} \pi_i^{\mu}$.

Hence from

$$p' \;=\; \mu\pi_1^{\mu-1}\pi_1'(\pi_2^{\mu}\cdots\pi_n^{\mu}) \;+\; \mu\pi_2^{\mu-1}\pi_2'(\pi_1^{\mu}\pi_3^{\mu}\cdots\pi_n^{\mu}) \;+\; \cdots \;+\; \mu\pi_n^{\mu-1}\pi_n'(\pi_1^{\mu}\cdots\pi_{n-1}^{\mu})$$

we have

$$\frac{p'}{p} = \mu\frac{\pi_1'}{\pi_1} + \cdots + \mu\frac{\pi_n'}{\pi_n}.$$

Since

$$\begin{aligned}\operatorname{div}(p) &= \operatorname{div}\left(\prod_{i=1}^{n}\pi_i^{\mu}\right)\\ &= \operatorname{div}(\pi_1^{\mu}) + \cdots + \operatorname{div}(\pi_n^{\mu})\\ &= \mu U_1 + \cdots + \mu U_n,\end{aligned}$$

we can conclude that π_i vanishes only on U_i. Otherwise, if π_i vanished on U_i and U_j for $i \neq j$, then from above we would have

$$\begin{aligned}&\operatorname{div}(\pi_1^{\mu}) + \cdots + \operatorname{div}(\pi_i^{\mu}) + \cdots + \operatorname{div}(\pi_j^{\mu}) + \cdots + \operatorname{div}(\pi_n^{\mu})\\ &\qquad = \mu U_1 + \cdots + \mu(U_i + U_j) + \cdots + \mu U_j + \cdots + \mu U_n\\ &\qquad\qquad = \mu U_1 + \cdots + \mu U_i + \cdots + 2\mu U_j + \cdots + \mu U_n,\end{aligned}$$

which contradicts Theorem 4.1. Whence the residue of $\frac{p'}{p}$ is μ. Thus $\frac{c_i}{\mu}\frac{p'}{p}$ has residue c_i wherever the integrand has residue c_i. This yields a logarithmic term in the logarithmic part as in Liouville's Theorem.

4.1.5 Termination of the Algorithm

Since we have been able to connect our algorithm to divisors, the termination of the algorithm relies on the "Problem of the Points of Finite Order." The problem consists of two parts. The first part of the problem is to determine an integer n such that given a divisor δ, $n\delta$ is principal. If it is determined that $n\delta$ is principal, the second part of the problem addresses finding a function f such that $n\delta = \operatorname{div}(f)$. We have a test for determining whether a function gives rise to a principal divisor, so we need to know when we should stop testing, as it may turn out that a divisor may never be principal.

Two divisors δ_1 and δ_2 are *linearly equivalent* if $\delta_1 - \delta_2$ is a principal divisor. We also say that a divisor δ is rationally equivalent to 0 if it is principal. The set of all divisors on a curve form a group which is denoted $\operatorname{Div}(X)$. The set of all principal divisors form a subgroup of $\operatorname{Div}(X)$. The quotient of $\operatorname{Div}(X)$ by this subgroup is called the divisor class group of X and is denoted $\operatorname{Cl}(X)$. If X is any projective nonsingular curve, then $\operatorname{Cl}(X)$ is isomorphic to the group of closed points of an abelian variety called the *Jacobian variety* of X, c.f. [14]. All abelian groups contain a torsion subgroup by Lemma 2.2.2.5 [15]. The size of the torsion portion of the Jacobian variety is known as the *torsion* of the group, or of the curve. A divisor that is principal must lie in the torsion part of the curve. Hence the order of any divisor that is principal must divide the torsion of the curve [11]. Thus our problem has been reduced to bounding the number of points in the Jacobian variety [29, 11]. As proved in [11], this bound is given by $(\sqrt{q^r}+1)^{2g}$ where q is a prime and r is a positive integer.

From Theorem 4.1, any $p \in \mathfrak{t}_\mu$ such that $\mathrm{Id}(r_z, F, p) = \mathfrak{t}_\mu$ for some μ, div p is a principal divisor. Theorem 9.3 [17] tells us that the degree of every principal divisor is 0. This allows us to use the bound given by Bronstein [5] and Davenport [11]. Bronstein [5] describes a criterion for a suitable power of a prime to bound the torsion on our divisor. The criterion of Bronstein is that the image of the discriminant of F in $\mathbb{F}_{q^r}$ must be 0. Thus once we have reached the bound $(1+\sqrt{q^r})^{2g}$, if we have not found a solution to (4.1), we restart the algorithm and instead of testing each individual Gröbner basis element, we test combinatorial sums of them. See the section entitled "Examples."

4.1.6 Removal Condition

One reason why the algorithm given by Kauers [16] fails to find the full integral in some cases is because although it may find a correct logand, the order computed by the algorithm is incorrect. To correct this problem we proceed as follows. The constructed ideal $\mathfrak{h}$ is radical and zero-dimensional. By Theorem 6.54 [1], for any term order there exist elements g_x and g_y in $\mathfrak{g} = \mathrm{GröbnerBasis}(\mathfrak{h})$ such that the leading monomials of g_x and g_y are pure powers of x and y, respectively. If we can write $F(x,y) = g_y^d + g g_x$ where $d \in \mathbb{Z}_{>0}$ and $g \in K[x,y]$, then g_y is a candidate for removal from $\mathfrak{g}$ in the algorithm. The decision to remove g_y is based on if both the equalities $\mathrm{Id}(r_z, F, g_y) = \sqrt{\mathrm{Id}(r_z, F, g_y^d)} = \mathrm{Id}(\mathfrak{g}_1)$ and $\sqrt{\mathrm{Id}(r_z, F, g_x)} = \mathrm{Id}(\mathfrak{g}_1)$ hold. The first equality ensures that g_y vanishes only $\mathbf{V}(\mathfrak{h})$ when considered as a function on $\mathbf{V}(F)$. Taking the radical of $\mathrm{Id}(r_z, F, g_x)$ in the second equality is necessary since $\mathrm{GröbnerBasis}(\mathrm{Id}(r_z, F, g_x))$ could possibly contain g_y^d instead of g_y. Hence g_x would not satisfy (4.1). In the ring $K(x)[y]/\mathrm{Id}(F(x,y))$, g_y^d is identified with $-g g_x$. Thus it is actually g_y^d that has order 1.

4.2 Liouvillian Extensions

$K(x)$ is a Liouvillian extension of K if one of the following conditions hold

(i) $x' \in K$

(ii) $x'/x \in K$

(iii) x is algebraic over K.

If x is transcendental and Liouvillian over K, and $K(x)$ has the same set of constants as K, then x is a Liouvillian monomial over K. Since our algorithm uses polynomials, our results also apply to extensions $K(x, \overline{y})$ when x is a Liouvillian monomial over K. Being a Liouvillian monomial ensures that x' is a polynomial in $K[x]$. Thus Gröbner basis algorithms could still be utilized.

CHAPTER V
EXAMPLES

5.0.1 Example 1

This example is Example 6 in Appendix 2 of [11]. Consider $\int \frac{\sqrt{x+\sqrt{A^2+x^2}}}{x}$ where A is a constant. Let $F(x,y) = y^4 - 2xy^2 - A^2$. An integral basis for the integral closure of $\mathbb{Q}[x]$ in $\mathbb{Q}(x)[y]/\mathrm{Id}(F)$ is given by $\{1, y, y^2, y^3\}$. Expressing the integrand in terms of this integral basis yields the numerator as y and the denominator as x.

Computing a reduced Gröbner basis of $\mathrm{Id}(u - zv', v, F)$, we find that $R_z = z^4 - A^2$. This yields $\widetilde{I} = \mathrm{Id}(z^4 - A^2, y - z, x)$. The primary decomposition of $\widetilde{I}$ is given by $\mathrm{Id}(A + z^2, x, y - z) \bigcap \mathrm{Id}(A - z^2, x, y - z)$. Note that the primary components are prime.

For the ideal $\mathrm{Id}(A+z^2, x, y-z)$, we have $\mathrm{Id}(A+z^2, F, y-z) = \mathrm{Id}(A+z^2, x, y-z)$. Thus $\sum_{\gamma:A+\gamma^2=0} \gamma \log(y - z)$ is a contribution to the logarithmic part. Additionally, we have $\mathrm{Id}(A - z^2, F, y - z) = \mathrm{Id}(A - z^2, x, y - z)$. Thus we can conclude that $\int \frac{y}{x} = \sum_{\gamma:A+\gamma^2=0} \gamma \log(y - \gamma) + \sum_{\gamma:A-\gamma^2=0} \gamma \log(y - \gamma)$. That is,

$$\int \frac{\sqrt{x\sqrt{A^2+x^2}}}{x} = \sum_{\gamma:\gamma^2-A=0} \gamma \log(\sqrt{x+\sqrt{A^2+x^2}} - \gamma) +$$
$$\sum_{\gamma:\gamma^2+A=0} \gamma \log(\sqrt{x+\sqrt{A^2+x^2}} - \gamma)$$

Davenport reports the answer as $\log(-\sqrt{A}\sqrt{A^2+x^2}y + A\sqrt{A^2+x^2} - A\sqrt{A}y + \sqrt{A}xy + A^2) + \log(-i\sqrt{A}\sqrt{A^2+x^2}y - A\sqrt{A^2+x^2} + iA\sqrt{A}xy + i\sqrt{A}xy + A^2) - \sqrt{A}(1+i)\log x + 2y$ where $i^2 = -1$. We note that both Mathematica and Maple return the integral as a hypergeometric series. Axiom returns the integral unevaluated. Kauers' algorithm returns the same answer as our algorithm.

5.0.2 Example 2

Let $f = \frac{-36x^3+15x(x^2+1)^{2/3}+5x(x^2+1)^{1/3}-33x}{5(27x^2+26)(x^2+1)}$ and consider $\int f$. Let $F(x,y) = y^3 - x^2 - 1$. A basis for $\mathcal{O}_{\mathbb{Q}[x]}$ is given by $\{1, y, y^2\}$. We then write the integrand as $g = \frac{-36x^3+15xy^2+5xy-33x}{5(27x^2+26)(x^2+1)}$. For this example, we will go through the steps of the algorithm in detail again.

We set $I = \mathrm{Id}(36x^3 - 15xy^2 - 5xy + 33x - z(10x(54x^2 + 53)), y^3 - x^2 - 1, 5(27x^2 + 26)(x^2 + 1))$. After computing the reduced Gröbner basis for I, we have $\min G = z(2z - 1)(10z + 3)^3$. Thus $R_z = (2z - 1)(10z + 3)$. We write $\widetilde{I} = J_1 \bigcap J_2$ where $J_1 = \mathrm{Id}(2z - 1, 3y - 1, 27x^2 + 26)$ and $J_2 = \mathrm{Id}(10z + 3, y, x^2 + 1)$.

The ideal J_1 is prime, and the Gröbner basis for J_1 is $\{2z - 1, 3y - 1, 27x^2 + 26\}$. Testing each element in the Gröbner basis, we arrive at $\mathrm{Id}(2z-1, y^3-x^2-1, 3y-1) = \mathrm{Id}(2z - 1, y^3 - x^2 - 1, 3y - 1, 27x^2 + 26)$. This yields our first desired logand, $3y - 1$. Thus at this point our integral is $\frac{1}{2}\log(3y - 1)$.

Since $\sqrt{\mathrm{Id}(10z + 3, F, y)} = J_2$ and $\sqrt{\mathrm{Id}(10z + 3, F, x)} = J_2$, y meets the Removal Condition. Removing it yields the ideal $\mathrm{Id}(10z + 3, x^2 + 1)$. This test also gives us that $\frac{3}{10}\log(x^2 + 1)$ is a contribution to the logarithmic part. Thus our integral is now $\frac{1}{2}\log(3y - 1) - \frac{3}{10}\log(x^2 + 1)$. Indeed, $D\left(\frac{1}{2}\log(3y - 1) - \frac{3}{10}\log(x^2 + 1)\right) = g$.

5.0.3 Example 3

Consider $\int \frac{(3xe^x+3)\sqrt[3]{(\log x+e^x)^2} - xe^x - 1}{24x\sqrt[3]{(\log x+e^x)^2}(\log x+e^x - \sqrt[3]{\log x+e^x})}$. Let $f = \frac{(3xt_2+3)y^2-(xt_2+1)}{24xy^2(t_1+t_2-y)}$ where $Dt_1 = 1/x$, $Dt_2 = t_2$, and $F(y, t_2) = y^3 - t_1 - t_2$. Now consider $\int f$ where $f \in \mathbb{Q}(x, t_1, t_2)$. An integral basis for the integral closure of $\mathbb{Q}[x]$ in $\mathbb{Q}(x, t_1)[t_2]$ is given by $1, y, y^2$. We use the block order where $[t_2, y]$ is ordered by graded reverse lexicographic and $[z]$ is ordered lexicographically. (Using the block order where $[t_1, y]$ is ordered by graded reverse lexicographic and $[z]$ is ordered lexicographically yields the same result.)

The minimal element of the Gröbner basis of $\mathrm{Id}(u - zv', v, F)$ is $R_z = z(8z - 1)(24z - 1)^2$. We then have $\widetilde{I} = \mathrm{Id}(I, 8z - 1) \bigcap \mathrm{Id}(I, 24z - 1)$. This yields $J_1 = \mathrm{Id}(8z - 1, y^2 - 1, t_1 + t_2 - y)$ and $J_2 = \mathrm{Id}(24z - 1, y, t_1 + t_2)$. We then have $J_1 = \mathrm{Id}(8z - 1, y - 1, t_2 + t_1 - 1) \bigcap \mathrm{Id}(8z - 1, y + 1, t_2 + t_1 - 1)$ as the prime decomposition of J_1. Neither $y - 1$ nor $y + 1$ satisfy the Removal Condition. However, since $y^3 = t_1 + t_2$, we remove y from J_2. Hence we have $\mathscr{P} = \{\mathrm{Id}(8z - 1, y^2 - 1, t_1 + t_2 - y), \mathrm{Id}(24z - 1, t_1 + t_2)\}$.

At $\mu = 1$, $\mathrm{Id}(8z - 1, F, y^2 - 1) = \mathrm{Id}(8z - 1, y^2 - 1, t_1 + t_2 - y)$, so we have $\frac{1}{8}\log(y^2 - 1)$ as a contribution to the logarithmic part. Also at $\mu = 1$, $\mathrm{Id}(24z - 1, F, t_1 + t_2) = \mathrm{Id}(24z - 1, t_1 + t_2)$. Thus the logarithmic part of $\int f$ is given by $\frac{1}{8}\log(y^2 - 1) + \frac{1}{24}\log(t_1 + t_2)$. In fact, it can be readily shown that this is the full integral. We note that Mathematica, Maple, and Axiom all fail to provide an antiderivative. The algorithm by Kaeuers fails to return the correct integral on its first run.

5.0.4 Example 4

This example was created in order to stump the major computer algebra systems; i.e., Mathematica, Maple, and Axiom all fail to provide an antiderivative. Let $F(x,y) = y^3 - x^4 - x^3 - x^2 - x + 1$ and consider $f = D\log(x - (x^4 + x^3 + x^2 + x - 1)^{1/3}) = \frac{u}{v} \in \mathbb{Q}(x)[y]$ where $u = -4x^3 - 3x^2 - 2x - 1 + 3(x^4 + x^3 + x^2 + x - 1)^{2/3}$ and $v = 3((x^4 + x^3 + x^2 + x - 1)^{1/3} + x)(x^4 + x^3 + x^2 + x - 1)^{2/3}$. A basis for $\mathcal{O}_{\mathbb{Q}[x]}$ is given by $\{1, y, y^2\}$. Writing f in terms of this basis, we have $g = \frac{\widetilde{u}}{\widetilde{v}}$ where $\widetilde{u} = (x^4 - x^2 - 2x + 3)y^2 + (x^5 - x^3 - 2x^2 + 3x)y + 4x^7 + 6x^5 + 7x^4 + 4x^6 - x^3 + 3x^2 - x - 1$ and $\widetilde{v} = 3(x^4 + x^3 + x^2 + x - 1)(x^4 + x^2 + x - 1)$.

Computing the reduced Gröbner basis G of $\mathrm{Id}(u - zv', v, F)$ yields $\min G = z^3(z - 1)$. Hence we take $R_z = z - 1$. We then set $\widetilde{I} = \mathrm{Id}(I, z-1) = J_1 = \mathrm{Id}(x+1, x-y, z-1, x^4 + x^2 + x - 1) \bigcap \mathrm{Id}(y - x, z - 1, x^3 - x^2 + 2x - 1, x^4 + x^2 + x - 1)$. Since no basis element satisfies the removal condition, we have $\mathfrak{p} = \mathrm{Id}(z - 1, y^4 + y^2 + y - 1, x - y)$. Because $\mathrm{Id}(z - 1, F, x - y) = \mathfrak{p}$, $x - y$ is a desired logand. Hence $\int f = \log(x - y)$.

5.0.5 Example 5

Let $F(x,y) = y^3 - x^9 - 1$. A basis for $\mathcal{O}_{\mathbb{Q}[x]}$ is given by $\{1, y, y^2\}$. Now, consider $f = \frac{u}{v} \in \mathbb{Q}(x)[y]$ where $u = 11x^{24} - 31x^{22} + 29x^{20} - 9x^{18} - 53x^{13} + 49x^{11} - 21x^9 + 8x^6 - 22x^4 + 20x^2 - 12 + (-3x^{15} + 9x^{13} - 4x^{11} - 3x^6 + 9x^4 - 7x^2 + 6)y + (-3x^{15} + 14x^{13} - 17x^{11} + 6x^9 - 3x^6 + 11x^4 - 11x^2 + 6)y^2$ and $v = x(x^9 + 1)(x^{15} - 3x^{13} + 3x^{11} - x^9 + x^6 - 3x^4 + 3x^2 - 2)$.

Computing the reduced Gröbner basis of $\mathrm{Id}(u - zv', v, F)$ yields $R_z = (z-1)(z-9)$. We then have $\widetilde{I} = J_1 \bigcap J_2$ where $J_1 = \mathrm{Id}(z - 1, x^2y - y - 1, y^5 - xy^3 - x^3 - 4xy^2 - y^3 - 6xy - 3x, x^5 - y^5 + 2x^3 + xy^2 + 4xy + y^2 + 3x)$ and $J_2 = \mathrm{Id}(z - 9, y^2 + y + 1, x)$. Note that J_1 and J_2 are prime.

Since $\mathrm{Id}(z - 1, F, x^2y - y - 1) = J_1$, $\log(x^2y - y - 1)$ is a contribution to the logarithmic part. The relation $\mathrm{Id}(z - 9, F, g) = J_2$ does not hold for any $g \in J_2$, so we compute $\mathfrak{t}_2 = \mathrm{Id}(z - 9, F) + J_2^2$. We then have $\mathfrak{g}_2 = \mathrm{Id}(z - 9, y^2 + y + 1, x^2)$. In fact, (4.1) does not hold for $\mu = 1, \ldots, 8$. At $\mu = 9$, we have $\mathfrak{g}_9 = \mathrm{Id}(z - 9, y^2 + y + 1, x^9)$. We then have $\mathrm{Id}(z - 9, F, y^2 + y + 1) = \mathfrak{g}_9$. Hence $\log(y^2 + y + 1)$ is a contribution to the logarithmic part. The full integral is given by $\log(x^2y - y - 1) + \log(y^2 + y + 1)$. Note that Mathematica, Maple, and Axiom do not return an antiderivative.

5.0.6 Example 6

This is example 10 in [16]. We illustrate with this example that our algorithm can find the logarithmic part of an integral in one application. Let $u = 2x^3 + 6x^2 -$

$7 - 7 - (x-1)(3x+1)y$ and $v = (x^2-1)x(x^2-x-1)$. Consider $\int \frac{u}{v} \in \mathbb{Q}(x)[y]$.

A basis for $\mathcal{O}_{\mathbb{Q}[x]}$ is given by $\{1, y\}$. Finding a reduced Gröbner basis of $\mathrm{Id}(u - zv', v, F)$ where $F = y^2 - x - 1$, we have $R_z = (z-3)(z-2)(z+6)(z+8)$. We have $\widetilde{I} = J_1 \bigcap J_2 \bigcap J_3 \bigcap J_4$ where $J_1 = \mathrm{Id}(z+6, x, y-1)$, $J_2 = \mathrm{Id}(z-3, y^2-2, x-1)$, $J_3 = \mathrm{Id}(z-2, x^2+y-1, y^2-x-1, xy+x+1)$, and $J_4 = \mathrm{Id}(z+8, y+1, x)$. The ideals J_1, J_2, and J_4 are prime. We have $\mathrm{Id}(z+6, F, y-1) = J_1$, $\mathrm{Id}(z-3, F, x-1) = J_2$, and $\mathrm{Id}(z+8, F, y+1) = J_4$. Hence $-6\log(y-1) + 3\log(x+1) - 8\log(y+1)$ is a contribution to the logarithmic part of $\int \frac{u}{v}$.

Let $P_1 \bigcap P_2$ be the prime decomposition of J_3 where $P_1 = \mathrm{Id}(z-2, x+y, y^2+y-1)$ and $P_2 = \mathrm{Id}(z-2, y, x+1)$. Since $\sqrt{\mathrm{Id}(z-2, F, y^2)} = P_1$ and $\sqrt{\mathrm{Id}(z-2, F, x+1)} = P_1$, we remove y from the list of generators and consider the ideal $\mathrm{Id}(z-2, x+1)$. No generator in $\mathrm{Id}(z-2, x+y, y^2+y-1)$ satisfies the Removal Condition, so we consider these two ideals separately. Since $\sqrt{\mathrm{Id}(z-2, F, x+1)} = P_1$, we obtain $2\log(x+1)$ as a contribution to the logarithmic part. We then have $\mathrm{Id}(z-2, F, x+y) = P_2$, giving $2\log(x+y)$ as a contribution. Hence $2\log(x+y) + 2\log(x+1)$ is the total contribution to the logarithmic part from the ideal J_3. In fact, $\int \frac{u}{v} = -6\log(y-1) + 3\log(x+1) - 8\log(y+1) + 2\log(x+y) + 2\log(x+1)$.

5.0.7 Example 7

This example is Example 4 from the section "Conclusions" in [11]. Consider

$$\int \frac{2(x^2-1)\log x + x^2\overline{y}}{x(x^2-1)(\log^2 x - \overline{y})}$$

where $\overline{y}$ satisfies $F(x,y) = y^2 - x^2 + 1$. Let t be such that $Dt = \frac{1}{x}$ and consider $\int f$ where $f = \frac{2(x^2-1)t + x^2y}{x(x^2-1)(t^2-y)} \in \mathbb{Q}(x,t,y)$. Let $K = \mathbb{Q}(x)$. An integral basis for the integral closure of K in $K(t, \overline{y})$ is given by $\{1, y\}$. Using this basis, we write f as $g = \frac{2(x^2-1)t^3 - x^2yt^2 + (2x^2y - 2y)t + x^4 - x^2}{x(x-1)(x+1)(x^2-1-t^4)}$. When computing Gröbner bases for this example, we use the graded reverse lexicographic order where $t > y$ and z is order lexicographically.

The minimal element of the reduced Gröbner basis of $\mathrm{Id}(u - zv', v, F)$ where $Dx = 1$, $Dt = 1/x$ is $z(x-1)$. We then have $\widetilde{I} = \mathrm{Id}(z-1, y+t^2, -t^4+x^2-1)$. Since $\mathrm{Id}(z-1, F, y+t^2) = \mathrm{Id}(z-1, y+t^2, -t^4+x^2-1)$, we conclude that $\int f = \log(y+t^2)$. Indeed, the integrand was obtained by Davenport by differentiating $\log(y + \log^2 x)$. We note that both Mathematica and Maple return the integral unevaluated.

5.0.8 Example 8

The previous examples considered integrating in radical extensions. This example considers integrating an element not in a radical extension. Let $f = \frac{\widetilde{u}}{\widetilde{v}} \in \mathbb{Q}(x, y)$ where $\widetilde{u} = -3x^2y + y^2$ and $\widetilde{v} = (y-1)(5y^4 + x^3 - 2xy)$. A basis for $\mathcal{O}_{\mathbb{Q}[x]}$ is given by $\{1, y, y^2, y^3, y^4\}$. Let g be f written in terms of this basis so that $g = \frac{u}{v} \in \mathbb{Q}(x)[y]$.

Computing the reduced Gröbner basis of $\mathrm{Id}(u - zv', v, F)$ where $F = y^5 - xy^2 + x^3y + 2$, we have $R_z = z - 1$. We then have $\widetilde{I} = \mathrm{Id}(z - 1, y - 1, x^3 - x + 3)$. Since $\mathrm{Id}(z - 1, F, y - 1) = \widetilde{I}$, $\log(y - 1)$ is a contribution to the logarithmic part of $\int g$. It can be readily verified that $D \log(y - 1) = g$.

5.0.9 Example 9

Consider

$$\int \frac{(t_1 + t_2 + t_3)(2t_1 - 3) + (t_1 - 2t_2 - 2t_3)\overline{y}}{2(t_1 + t_2 + t_3)(t_1^2 - t_1 - t_2 - t_2)}$$

where $Dt_1 = 1, Dt_2 = 1, Dt_3 = 1$, and the minimal polynomial for $\overline{y}$ over $\mathbb{Q}(t_1, t_2)(t_3)$ is $F(y, t_3) = y^2 - (t_1 + t_2 + t_3)$. Computing the reduced Gröbner basis of $\mathrm{Id}(u - zv', F, v)$ yields $R_z = z^2(z - 1)$. We then have $\widetilde{I} = (I, z - 1) = \mathrm{Id}(z - 1, t_1 + y, t_1^2 - t_1 - t_2 - t_3)$. This ideal is prime, so there is no decomposition to perform. Since $\mathrm{Id}(z - 1, F, t_1 + y) = \widetilde{I}$, $\log(t_1 + y)$ is a contribution to the logarithmic part. It can be readily verified that $D \log(t_1 + y)$ is equal to our integrand.

5.0.10 Example 10

This is Example 9 from Kauers [16]. Consider the integral $\displaystyle\int \frac{\sqrt{x^2+1}+1}{(x^2+1)(x+1)}$. Let $F(x, y) = y^2 - x^2 - 1$ and write the integrand as $\frac{y+1}{(x^2+1)(x+1)}$. We then have $I = \mathrm{Id}(y + 1 - z(2x(x + 1) + x^2 + 1), (x^2 + 1)(x + 1), y^2 - x^2 - 1)$.

The genus of F is 0, so if there is a principal divisor, we are guaranteed that one exists of order 1. Thus $J_1 = \mathrm{Id}(4z^2 - 4z - 1, x + 1, y + 1 - 2z)$ and $J_2 = \mathrm{Id}(8z^2 + 4z + 1, x + 1 + 4z, y)$, of which both are given in terms of a Gröbner basis. No element p in J_1 satisfies $\mathrm{Id}(4z^2 - 4z - 1, F, p) = J_1$. However, for $p = x + 1 + y + 1 - 2z$, we have $\mathrm{Id}(4z^2 - 4z - 1, F, x + 1 + y + 1 - 2z) = J_1$. Hence $\displaystyle\sum_{\gamma:4\gamma^2-4\gamma-1=0} \gamma \log(x + 1 + y + 1 - 2\gamma)$ is a contribution to the logarithmic part.

We also have that no element p in J_2 satisfies $\mathrm{Id}(8z^2 + 4z + 1, F, p) = J_2$. For $p = x + y + 1 + 4z$, we have $\mathrm{Id}(8z^2 + 4z + 1, F, p) = J_2$. Hence $\displaystyle\sum_{\gamma:8\gamma^2+4\gamma+1=0} \gamma \log(x +$

$y + 1 + 4\gamma)$ is a contribution to the logarithmic part. Thus the full integral is $\sum_{\gamma:4\gamma^2-4\gamma-1=0} \gamma \log(x+1+\sqrt{x^2+1}+1-2\gamma) + \sum_{\gamma:8\gamma^2+4\gamma+1=0} \gamma \log(x+\sqrt{x^2+1}+1+4\gamma)$.

CHAPTER VI
TRANSCENDENTAL CASE

For $K = C(t)$, $Dt = 1$, and $f \in K$, Rothstein and Trager [31, 33] developed an algorithm to express $\int f$ in terms of logarithms. Because the calculation required to find greatest common divisors of polynomials and prime factorizations over algebraic extensions of C, another algorithm was developed by Lazard and Rioboo [20] , and independently by Trager[1], to compute $\int f$ by the use of subresultants (Lazard-Rioboo-Trager). Both algorithms compute the logarithmic part of $\int f$ as

$$\sum_{c:R(c)=0} c \cdot \log(\gcd(u(t) - c \cdot Dv(t), v(t)))$$

where $Dt = 1$ and c is a solution of $R(z) = \text{resultant}_t(u(t) - zDv(t), v(t))$. In fact, in [12] and [6], the above also holds when t is exponential, logarithmic, or tangent over k. We should note that the above formula is not always the complete story when t is exponential, logarithmic, or tangent. I.e., if g denotes the logarithmic part given above, then $h = f - Dg \in C[t]$, and h is still to be integrated using other methods.

Czichowski [10] showed that the reduced Gröbner Basis $\mathscr{B}$ of the ideal $I = \langle u(t) - z \cdot Dv(t), v(t)\rangle$ w.r.t. the lexicographical order $t > z$ and the usual derivation $Dt = 1$, can replace the computations of the resultant and subresultant in the previous algorithms. It will be shown here that Czichowski's observation can be generalized to include elements t that are exponential, logarithmic, or tanget over k. We say that t is an exponential over k if $t'/t = w$ for some $w \in k$. Likewise, t is said to be logarithmic over k if $t' = w'/w$ for some $w \in k$, and t is called a tangent over k if $t'/(t^2 + 1) = w'$ for some $w \in k$.

If U is a unique factorization domain, $h = \sum_{i=0}^{m} a_i t^i \in U[t]$, the content of h is defined to be $\text{content}_t(P) = \gcd(a_0, \ldots, a_n) \in U$. The primitive part of h is $\text{pp}(h) = h/\ \text{content}(h) \in U[t]$. Furthermore, an element $t \in K$, where K a differential extension of k, is a monomial over k if t is transcendental over k and $Dt \in k[t]$.

[1] As stated in [2], Trager implemented this algorithm but did not publish it.

6.1 Main Statement

Theorem 6.1.0.1. *Let t be an arbitrary monomial over a constant field K. Let $f \in K(t)$ be simple and $\gcd(u, v) = 1$. Denote $I = \langle u - zDv, v \rangle$, where z is a new indeterminate over K, and $\mathscr{B}$ the reduced Gröbner Basis with respect to the lexicographical order $t > z$. Write $\mathscr{B} = \{P_1, P_2, \ldots, P_m\}$ such that P_{i+1} has higher term than P_i with respect to $t > z$. Then, the logarithmic part of $\int f$ is given by*

$$\sum_{i=1}^{m-1} \sum_{c:Q_i(c)=0} c \cdot \log(pp_t(P_{i+1})(t, c))$$

where $Q_i = content_t(P_i)/content_t(P_{i+1}) \in K[z]$.

The case where $Dt = 1$ has already been done by Czichowski [10]. Our proofs here are similar to his proof. We do it in a series of lemmas.

Lemma 6.1.0.1. *Let t, u, v, and the ideal I be as in the theorem above. Then I is*

1. *zero-dimensional*
2. *in normal position with respect to t (all zeros (t, z) have different t parts)*
3. *and maximal with respect to its set of zeros.*

Proof. Regarded as a polynomial in t, v has finite degree, say d. Thus, at least over the algebraic closure of K, v has d roots. This says that the associated variety $\mathbf{V}(I)$ is finite; i.e., I is zero-dimensional. The second statement follows from $\gcd(u, v) = \gcd(v, Dv) = 1$.

Using the lexicographical order $z > t$, there is a Gröbner Basis $\mathscr{B}_1 := \{z - H(t), v\}$ of I. (Since $\gcd(v, Dv) = 1$, there exist polynomials $F(t), G(t) \in K[t]$ such that $Fv + GDv = 1$. Multiplying through by z, we have $zFv + zGDv = z$, or $zGDv = z - zFv$. From $u - zDv$, we have $-Gu + zGDv = -Gu + z - zFv$. Reducing $Gu + z - zFv$ by v yields $z + H(t)$ where $H(t) = Gu$.) If $F(t, z)$ is a polynomial that vanishes on the zeros of I, then $\overline{F(t, z)}^{\mathscr{B}_1}$ yields $\tilde{v}(t)$ where $\deg(\tilde{v}(t)) < \deg(v)$. (Dividing $F(t, z)$ by $z - H(t)$ gives $F(t, H(t))$; division of $F(t, H(t))$ by v reduces the degree of $F(t, H(t))$ to be less than that of v.) Because $\tilde{v}(t)$ must vanish on the same zeros as v, $\tilde{v}(t) \equiv 0$. Whence $F(t, z) \in I$. □

Lemma 6.1.0.2. *Let I and $\mathscr{B}$ be as before. Suppose that every $P_i \in \mathscr{B}$ is written so that $LT(P_{i+1}) > LT(P_i)$ using the lexicographical order with $t > z$ and $P_i = R_i(z)t^{n_i} + \cdots$. Then*

1. *$R_{i+1}(z) | R_i(z)$*

2. *$R_i(z) | P_i(t,z)$, i.e., $P_i(t,z) = R_i(z) \cdot S_i(t,z)$*

3. *$R_1(z)$ is the radical of $R(z) = resultant_t(u - zDv, v)$; i.e., $R_1(z)$ is square-free and has the same roots as $R(z)$.*

Proof. Recall that $\mathscr{B}$ is a reduced Gröbner basis ordered with respect to $t > z$. Since $P_i = R_i(z)t^{n_i} + \cdots$, we must have that $n_i < n_{i+1}$ and $\deg(R_i(z)) > \deg(R_{i+1}(z))$.

Let $g(z) = \gcd(R_i, R_{i+1})$, and let $\alpha(z)$ and $\beta(z)$ be such that $g(z) = \alpha(z)R_i(z) + \beta(z)R_{i+1}(z)$. Then, we have

$$\alpha(z)t^{n_{k+1}-n_k}P_i(t,z) + \beta(z)P_{i+1}(t,z) = g(z)t^{n_{k+1}} + \cdots \in I.$$

Thus it must be reduced to zero by $\mathscr{B}$. But, its leading term can only be reduced with respect to highest term degrees by P_{i+1}. Whence $\deg(\gcd(R_i, R_{i+1})) \geq \deg(R_{i+1})$ and thus $R_{i+1}|R_i$. Since I is zero dimensional, by the finiteness theorem [CLO2] $P_1(t,z) = R_1(z)$.

Because $R_{k+1}|R_k$, let $Q_k(z) \in K[z]$ be such that $R_k(z) = Q_k(z) \cdot R_{k+1}(z)$. From this we have $R_1(z) = Q_1(z)Q_2(z)\cdots Q_k(z)R_{k+1}(z)$, $R_2(z) = Q_2(z)Q_3(z)\cdots Q_k(z)R_{k+1}(z)$, $\ldots$, $R_k(z) = Q_k(z)R_{k+1}(z)$.

Let $P(t,z)$ be the polynomial $Q_k(z)P_{k+1}(t,z) - t^{n_{k+1}-n_k} \cdot P_k(t,z) = Q_k(z)(R_{k+1}(z)t^{n_{k+1}} + \cdots) - t^{n_{k+1}-n_k}(R_k(z)t^{n_k} + \cdots) = Q_k(z)(R_{k+1}(z)t^{n_{k+1}} + \cdots) - t^{n_{k+1}-n_k}(Q_k(z)R_{k+1}(z)t^{n_k} + \cdots)$ in I. Note that $\overline{P(t,z)}^{\mathscr{B}} = F_1(t,z) \cdot P_1(t,z) + F_2(t,z) \cdot P_2(t,z) + \cdots + F_k(t,z) \cdot P_k(t,z) + 0 \cdot P_{k+1}(t,z) + 0 \cdot P_{k+2}(t,z) + \cdots = 0$. So, $Q_k(z)P_{k+1}(t,z) = \sum_{i=1}^{k} F_i(t,z)P_i(t,z)$. Thus dividing by Q_k, it follows that $R_{k+1}|P_{k+1}$.

Proposition 1 in section 6 chapter 3 of [8] gives that $R(z)$ is in the first elimination ideal $\langle u - zDv, v\rangle \bigcap K[z]$. By the Elimination Theorem, c.f. [8], this ideal has the Gröbner Basis given by $\{R_1(z)\}$. Because $\mathscr{B}$ is reduced and I is maximal with respect to its set of zeros, $R_1(z)$ is square-free. □

Lemma 6.1.0.3. *From Lemma 2, we have $R_{i+1}|R_i$. Define $Q_i(z)$ as the polynomial such that $R_i(z) = Q_i(z)R_{i+1}(z)$. If c denotes a zero of $R_1(z) = 0$ and k is the smallest index such that $Q_k(c) = 0$, $Q_{k+1}(c) \neq 0$, then $S_{k+1}(t,c)$ is a gcd of $P_{k+1}(t,c), \ldots, P_m(t,c)$; i.e.,*

$$S_{k+1}(t,c) = \gcd(u - cDv, v).$$

Proof. Let $j > k$ and let P denote the polynomial,

$$Q_j(z) \cdot P_{j+1}(t,z) - t^{n_{j+1}-n_j} \cdot P_j(t,z).$$

P is in I since it is a combination of P_{j+1} and P_j. Thus $\overline{P}^{\mathscr{B}} = 0$. As in a similar argument from Lemma 2, P can only be reduced by $P_1, \ldots, P_j$. So, we have

$$Q_j(z) \cdot P_{j+1}(t,z) = \sum_{i=1}^{j} C_i(t,z) \cdot P_i(t,z).$$

Since $P_i(t,z) = R_i(z)S_i(t,z) = Q_i(z)R_{i+1}(z)S_i(t,z)$ and $Q_i(c) = 0$ for $1 \leq i \leq k$, we have

$$Q_j(c) \cdot P_{j+1}(t,c) = \sum_{i=k+1}^{j} C_i(t,c) \cdot P_i(t,c).$$

For $j = k+1$, we have

$$\begin{aligned} Q_{k+1}(c)P_{k+2}(t,c) &= C_{k+1}(t,c)P_{k+1}(t,c) \\ P_{k+2}(t,c) &= \frac{C_{k+1}(t,c)}{Q_{k+1}(c)} P_{k+1}(t,c), \end{aligned}$$

which shows that $P_{k+1}(t,c)$ divides P_{k+2}. For $j = k+2$, we have

$$\begin{aligned} Q_{k+2}(c)P_{k+3}(t,c) &= C_{k+1}(t,c)P_{k+1}(t,c) + C_{k+2}(t,c)P_{k+2}(t,c) \\ P_{k+3}(t,c) &= \frac{C_{k+1}(t,c)}{Q_{k+2}(c)} P_{k+1}(t,c) + \frac{C_{k+2}(t,c)}{Q_{k+2}(c)} P_{k+2}(t,c). \end{aligned}$$

Since we already have that $P_{k+1}(t,c)$ divides $P_{k+2}(t,c)$, we have that $P_{k+1}(t,c)$ divides $P_{k+3}(t,c)$. Continuing this argument, $P_{k+1}(t,c)$ divides $P_j(t,c)$ for all $j > k$. Since $P_{k+1}(t,c) = R_{k+1}(c)S_{k+1}(t,c)$, we have that $S_{k+1}(t,c)$ divides $P_j(t,c)$ for all $j > k$. By the maximality of I, $S_{k+1}(t,c)$ is a gcd of $P_{k+1}(t,c), \ldots, P_m(t,c)$. □

In [2] and [5], the Rothstein-Trager and Lazard-Rioboo-Trager algorithms are generalized for arbitrary monomials t. The generalization is that the logarithmic part of $\int f$, where $f = p + \frac{u}{v} \in K(t)$, f is simple, $\deg(u) < \deg(v)$, $\gcd(v,u) = 1$ is

$$\sum_{i=1}^{n} \sum_{\gamma : G_i(\gamma)=0} \gamma \log(\gcd(u - \gamma Dv, v)) \tag{6.1}$$

where each G_i is an irreducible factor of $R(z) = \text{resultant}_t(u - zDv, v)$. Note that $\langle u - zDv, v\rangle = \langle pv + u - zDv, v\rangle$, so the Gröbner basis for both ideals will be the same. From Lemma 2, $R_1(z)$ is the radical of $R(z)$. Lemma 2 also gives us that $R_i(z) = Q_i(z)R_{i+1}(z)$, each $Q_i(z)$ corresponds to to a $G_j(z)$ for some j. This additionally gives us that there are $m - 1$ factors of $R_1(z)$. Hence the sums in Theorem 1 and above coincide. Lemma 3 gives us that $S_{i+1}(t, c) = \gcd(u - cDv, v)$, where i is the least index such that $Q_i(c) = 0$. Taking $R_i(z) = \text{content}_t(P_i(t, z))$ gives $S_i(t, z) = \text{pp}_t(P_i(t, z))$. Whence Theorem 1 is shown.

6.1.1 Example

Consider $\int f$ where $f = (9t^3 - 6t^2 + 7t)/((t-3)(t^2+1)) \in \mathbb{Q}(t)$ and $Dt = t$. We have $u = 9t^3 - 6t^2 + 7t$, and $v = (t-3)(t^2+1)$. Since $Dv = t(3t^2 - 6t + 1)$, $\gcd(v, Dv) = 1$. The hypothesis of Theorem 1 is thus satisfied. Finding a reduced Gröbner basis of $\langle u - zDv, v\rangle$ yields $\mathscr{B} = \{(z-1)(z-7), (z-1)(t-3), 3t^2 - 5z + 8\}$. We then have that $Q_1(z) = z - 7$ and $Q_2(z) = z - 1$. This gives that $S_2(t, 7) = \text{pp}_t(P_2(t, 7)) = t - 3$ and $S_3(t, 1) = \text{pp}_t(P_3)(t, 1) = t^2 + 1$. Thus the logarithmic part of $\int f$ is

$$\sum_{i=1}^{2} \sum_{c:Q_i(c)=0} c \log(S_{i+1}(t, c)) = 7\log(t-3) + \log(t^2+1).$$

Computing $f - D(7\log(t-3) + \log(t^2+1)) = 0$. So, $\int f = 7\log(t-3) + \log(t^2+1)$.

6.1.2 Example

Let $f = \frac{-4t^4}{t^6-4} \in \mathbb{Q}(t)$ and $Dt = t^2$. We will compute the logarithmic part of $\int f$. Since $Dv = D(6t^7)$, $\gcd v, Dv = 1$. We then have $I = \langle u - zDv, v\rangle = \langle -4t^4 - z(6t^7), t^6 - 4\rangle$. The reduced Gröbner basis is $\{9z^2 - 1, t^3 + 6z\}$. Thus $R_1(z) = 9z^2 - 1$, $Q_1(z) = 9z^2 - 1$, and $S_2(t, z) = t^3 + 6z$. Since $Q_1(c) = 0$ when $c = -\frac{1}{3}, \frac{1}{3}$, we have

$$\sum_{c:Q_1(c)=0} c \log(S_2(t, c)) = \frac{1}{3}\log(t^3+2) - \frac{1}{3}\log(t^3-2).$$

6.2 Extension to Multiple Towers

We now extend our results for finding the logarithmic part of $\int f$ for $f \in K(t) = k(t_1, \ldots, t_{n-1})(t)$ and each t_i is a monomial over $k(t_1, \ldots, t_{i-1})$ for $1 \le i \le n - 1$.

Theorem 6.2.0.1. *Let t be an arbitrary monomial over a differential field $K = k(t_1, \ldots, t_{n-1})$ and D the total derivation. Let $f \in K(t)$ where $f = \frac{u(t)}{v(t)}$ be simple, v monic, and* $\gcd(u, v) = 1$. *Denote $I = \langle u - zDv, v \rangle$, where z is a new indeterminate over K, and $\mathscr{B}$ the reduced Gröbner Basis with respect to the lexicographical order $t > z$. Write $\mathscr{B} = \{P_1, P_2, \ldots, P_m\}$ such that P_{i+1} has higher term than P_i with respect to $t > z$. Then, the logarithmic part of $\int f$ is given by*

$$\sum_{i=1}^{m-1} \sum_{c:Q_i(c)=0} c \cdot \log(pp_t(P_{i+1})(t, c))$$

where $Q_i = content_t(P_i)/content_t(P_{i+1}) \in K[z]$.

We prove Theorem 6.2.0.1 by a series of 4 lemmas.

Lemma 6.2.0.1. *Let t, u, v, and the ideal I be as in theorem 6.2.0.1. Then I is*

1. *zero-dimensional*
2. *in normal position with respect to t (all zeros (t, z) have different t parts)*

Proof. Regarded as a polynomial in t, v has finite degree, say d. Thus, at least over the algebraic closure of K, v has d roots. This says that the associated variety $\mathbf{V}(I)$ is finite; i.e., I is zero-dimensional. The second statement follows from $\gcd(u, v) = \gcd(v, Dv) = 1$.

□

Lemma 6.2.0.2. *Let f and I be as in theorem 6.2.0.1. Then I a radical ideal.*

Proof. By the hypothesis of Theorem 6.2.0.1, v is normal, and thus square-free. Let $v = v_1 \cdots v_m$ where each v_i is irreducible over K. Using the lexicographical order $z > t$, there is a Gröbner Basis $\mathscr{B}_1 := \{z - H(t), v\}$ of I. (Since $\gcd(v, Dv) = 1$, there exist polynomials $F(t), G(t) \in K[t]$ such that $Fv + GDv = 1$. Multiplying through by z, we have $zFv + zGDv = z$, or $zGDv = z - zFv$. From $u - zDv$, we have $-Gu + zGDv = -Gu + z - zFv$. Reducing $Gu + z - zFv$ by v yields $z + H(t)$ where $H(t) = Gu$.) Thus $I = \langle z - H(t), v_1 \cdots v_m \rangle$. Since $v(t) \in K[t]$ is a generator, v is the unique minimal monic univariate polynomial generator in $I \bigcap K[t]$. Lemma 6.2.0.1 gives that I is in normal position with respect to t and zero-dimensional, thus by Proposition 8.69 [Becker-Weispfenning] the primary decomposition of I is $\bigcap_{i=1}^{m} \mathrm{Id}(I, v_i)$ where $\mathrm{Id}(I, v_i)$ means the ideal generated by I and v_i. Let $Q_i =$

$\mathrm{Id}(I, v_i)$. Since $v_i | v$, we have $Q_i = \mathrm{Id}(z - H(t), v_i)$. A Gröbner Basis for Q_i using lexicographic order $z > t$ is $\{v_i, z - H(t)\}$. We will now use Theorem 7.44 in [1]. For clarity, we state the theorem here: Let I be an ideal of the ring $K[X_1, \ldots, X_n]$ and assume that I has a Gröbner Basis, G, such that G has n elements and $LT(g_i) = X_i^{\nu_1}$ $\nu_i \geq 1$ for $1 \leq i \leq n$ using lexicographic order $X_n > X_{n-1} > \cdots > X_1$. Assume further that for $1 \leq i \leq n$ there does not exist a representation $g_i = f_1 f_2 + \sum_{j=1}^{i-1} q_j g_j$ with $f_1, f_2, q_1, \ldots, q_{i-1} \in K[t, z]$ such that $f_1, f_2 \neq 0$ and $\deg_{X_i}(f_1) < \deg_{X_i}(g_i)$ and $\deg_{X_i}(f_2) < \deg_{X_i}(g_i)$. For each i $(1 \leq i \leq m)$, denote $g_1 = v_i$ and $g_2 = z - H(t)$. We have:

$$g1 = v_i \neq f_1 f_2$$

for any $f_1, f_2 \in K[t]$ since v_i is irreducible by assumption. Furthermore, since $\deg_z(z - H(t)) = 1$, $\deg_z(f_1), \deg_z(f_2) < \deg_z(z - H(t))$ means that f_1 and f_2 are polynomials purely in t. So, in the representation

$$g_2 = z - H(t) = f_1 f_2 + q_1 v_i$$

the z term on the LHS must come from q_1. But, since v_i is a polynomial in t, any z term in q_1 would contribute a zt term in the product $q_1 v_i$. Since there is no zt term on the LHS, we cannot have a representation as above. Thus Q_i is zero-dimensinoal and prime. Since $I = \bigcap_{i=1}^m \langle z - H(t), v_i \rangle$, I is radical. (From [8] Ex 11 in section 7 chapter 4, $\sqrt{I} = \bigcap_{i=1}^m P_i$ where P_i are the primes belonging to I. A theorem by Lasker and Noether give that the primes belonging to I are the radicals of the ideals of a minimal primary decomposition. Since $\sqrt{Q_i} = Q_i$, the result follows.) □

Since I is radical, it is maximal with respect to its zeros. Proposition 1 in section 6 chapter 3 of [8] gives that $R(z)$ is in the first elimination ideal $\langle u - zDv, v \rangle \bigcap K[z]$. By the Elimination Theorem, c.f. [8], this ideal has the Gröbner Basis given by $\{R_1(z)\}$.

Lemma 6.2.0.3. *Let I and $\mathscr{B}$ be as before. Suppose that every $P_i \in \mathscr{B}$ is written so that $LT(P_{i+1}) > LT(P_i)$ using the lexicographical order with $t > z$ and $P_i = R_i(z)t^{n_i} + \cdots$. Then*

1. *$R_{i+1}(z) | R_i(z)$*
2. *$R_i(z) | P_i(t, z)$, i.e., $P_i(t, z) = R_i(z) \cdot S_i(t, z)$*

Proof. Recall that $\mathscr{B}$ is a reduced Gröbner basis ordered with respect to $t > z$. Since $P_i = R_i(z)t^{n_i} + \cdots$, we must have that $n_i < n_{i+1}$ and $\deg(R_i(z)) > \deg(R_{i+1}(z))$.

Let $g(z) = \gcd(R_i, R_{i+1})$, and let $\alpha(z)$ and $\beta(z)$ be such that $g(z) = \alpha(z)R_i(z) + \beta(z)R_{i+1}(z)$. Then, we have

$$\alpha(z)t^{n_{k+1}-n_k}P_i(t,z) + \beta(z)P_{i+1}(t,z) = g(z)t^{n_{k+1}} + \cdots \in I.$$

Thus it must be reduced to zero by $\mathscr{B}$. But, its leading term can only be reduced with respect to highest term degrees by P_{i+1}. Whence $\deg(\gcd(R_i, R_{i+1})) \geq \deg(R_{i+1})$ and thus $R_{i+1}|R_i$. Since I is zero dimensional, by the finiteness theorem [CLO2] $P_1(t,z) = R_1(z)$.

Because $R_{k+1}|R_k$, let $Q_k(z) \in K[z]$ be such that $R_k(z) = Q_k(z) \cdot R_{k+1}(z)$. From this we have $R_1(z) = Q_1(z)Q_2(z) \cdots Q_k(z)R_{k+1}(z)$, $R_2(z) = Q_2(z)Q_3(z) \cdots Q_k(z)R_{k+1}(z)$, $\ldots$, $R_k(z) = Q_k(z)R_{k+1}(z)$.

Let $P(t,z)$ be the polynomial $Q_k(z)P_{k+1}(t,z) - t^{n_{k+1}-n_k} \cdot P_k(t,z) = Q_k(z)(R_{k+1}(z)t^{n_{k+1}} + \cdots) - t^{n_{k+1}-n_k}(R_k(z)t^{n_k} + \cdots) = Q_k(z)(R_{k+1}(z)t^{n_{k+1}} + \cdots) - t^{n_{k+1}-n_k}(Q_k(z)R_{k+1}(z)t^{n_k} + \cdots)$ in I. Note that $\overline{P(t,z)}^{\mathscr{B}} = F_1(t,z) \cdot P_1(t,z) + F_2(t,z) \cdot P_2(t,z) + \cdots + F_k(t,z) \cdot P_k(t,z) + 0 \cdot P_{k+1}(t,z) + 0 \cdot P_{k+2}(t,z) + \cdots = 0$. So, $Q_k(z)P_{k+1}(t,z) = \sum_{i=1}^{k} F_i(t,z)P_i(t,z)$. Thus dividing by Q_k, it follows that $R_{k+1}|P_{k+1}$. □

Lemma 6.2.0.4. *From Lemma 2, we have $R_{i+1}|R_i$. Define $Q_i(z)$ as the polynomial such that $R_i(z) = Q_i(z)R_{i+1}(z)$. If c denotes a zero of $R_1(z) = 0$ and k is the smallest index such that $Q_k(c) = 0$, $Q_{k+1}(c) \neq 0$, then $S_{k+1}(t,c)$ is a gcd of $P_{k+1}(t,c), \ldots, P_m(t,c)$; i.e.,*

$$S_{k+1}(t,c) = \gcd(u - cDv, v).$$

Proof. Let $j > k$ and let P denote the polynomial,

$$Q_j(z) \cdot P_{j+1}(t,z) - t^{n_{j+1}-n_j} \cdot P_j(t,z).$$

P is in I since it is a combination of P_{j+1} and P_j. Thus $\overline{P}^{\mathscr{B}} = 0$. As in a similar argument from Lemma 2, P can only be reduced by $P_1, \ldots, P_j$. So, we have

$$Q_j(z) \cdot P_{j+1}(t,z) = \sum_{i=1}^{j} C_i(t,z) \cdot P_i(t,z).$$

Since $P_i(t,z) = R_i(z)S_i(t,z) = Q_i(z)R_{i+1}(z)S_i(t,z)$ and $Q_i(c) = 0$ for $1 \le i \le k$, we have

$$Q_j(c) \cdot P_{j+1}(t,c) = \sum_{i=k+1}^{j} C_i(t,c) \cdot P_i(t,c).$$

For $j = k+1$, we have

$$\begin{aligned} Q_{k+1}(c)P_{k+2}(t,c) &= C_{k+1}(t,c)P_{k+1}(t,c) \\ P_{k+2}(t,c) &= \frac{C_{k+1}(t,c)}{Q_{k+1}(c)} P_{k+1}(t,c), \end{aligned}$$

which shows that $P_{k+1}(t,c)$ divides P_{k+2}. For $j = k+2$, we have

$$\begin{aligned} Q_{k+2}(c)P_{k+3}(t,c) &= C_{k+1}(t,c)P_{k+1}(t,c) + C_{k+2}(t,c)P_{k+2}(t,c), \\ P_{k+3}(t,c) &= \frac{C_{k+1}(t,c)}{Q_{k+2}(c)} P_{k+1}(t,c) + \frac{C_{k+2}(t,c)}{Q_{k+2}(c)} P_{k+2}(t,c). \end{aligned}$$

Since we already have that $P_{k+1}(t,c)$ divides $P_{k+2}(t,c)$, we have that $P_{k+1}(t,c)$ divides $P_{k+3}(t,c)$. Continuing this argument, $P_{k+1}(t,c)$ divides $P_j(t,c)$ for all $j > k$. Since $P_{k+1}(t,c) = R_{k+1}(c)S_{k+1}(t,c)$, we have that $S_{k+1}(t,c)$ divides $P_j(t,c)$ for all $j > k$. By the maximality of I, $S_{k+1}(t,c)$ is a gcd of $P_{k+1}(t,c), \ldots, P_m(t,c)$. □

The specific cases when t is exponential or logarithmic over K can be found in [12]. For an arbitrary monomial t over K, [6] and [5] gives the logarithmic part of $\int f$ as 6.1.

6.3 Examples

6.3.1 Example

Consider $\int f$ where $f = ((54x^2+3)/(2x) \cdot t^3 + (-48x^3 - 6x)/(2x) \cdot t^2 + (18x^3 + 45x)/(2x) \cdot t - 27x)/(t^3 - xt^2 + 3xt - 3x^2) \in \mathbb{Q}(x, t_1)$ and $Dt = 2xt$. We have $Dv = 6xt^3 - (4x^2+1)t^2 + (6x^2+3)t - 6x$ and $v = (t^2+3x)(t-x)$. So, $\gcd(v, Dv) = 1$. The reduced Gröbner Basis is $\mathscr{B} = \{(2z-3)(z-6), (z-6)(t-x), 9t^2 + 2(z-6)x^2 + 3(2z-3)x\}$.

From $P_2 = (z-6)(t-x)$, we have $R_2(z) = z-6$. This gives $Q_1 = R_1/R_2 = 2z-3$. Evaluating P_2 at $z = 3/2$, we have $P_2 = \frac{9}{2}(x-t)$. Hence $S_2(t, 3/2) = x - t$. We now have $R_3 = 1$, which gives $Q_2(z) = R_2/R_3 = z - 6$. P_3 evaluated at $z = 6$ yields $27x + 9t^2$. Whence $\mathrm{pp}_t(S)_3(t,6) = 3x + t^2$. By Theorem 2, $g =$

$3/2\log(x-t)+6\log(t^2+3x)$.

Computing $h = f - Dg$, $h = \frac{3}{2x}$. But, $\int h = \frac{3}{2}\log x$. Whence $\int f = 3/2\log(x - t_1) + 6\log(t_1^2 + 3x) + \frac{3}{2}\log x$.

6.3.2 Example

This is taken from [Br]. Let $f = \frac{2t^2-t-x^2}{t^3-x^2t} \in \mathbb{Q}(x,t)$ where $Dt = 1/x$ and let us consider $\int f$. In this case, writing $f = p + \frac{u}{v}$, we have $p = 0$, $u = 2t^2 - t - x^2$, and $v = t^3 - x^2t$.

Computing a reduced Gröbner basis, we have $\mathscr{B} = \{(2z-1)(2z+1)(x-z), (4x^2-1)t + 2x(x-z)(4zx+1)\}$. This gives $R_1(z) = (2z-1)(2z+1)(x-z)$. The factor $x - z$ has no constant roots, thus $\int f$ is not elementary. However, we can use the constant roots to construct the elementary parts of the integral. We now have $P_2(t, 1/2) = (4x^2-1)t + (4x^2-1)x$, which gives $\hat{S}_2(t, 1/2) = t + x$. Similarly, $P_2(t, -1/2) = (4x^2-1)t - (4x^2-1)x$, which gives $\hat{S}_2(t, -1/2) = t - x$. Putting his all together yields $g = 1/2\log(t+x) - 1/2\log(t-x)$. Since $\int f$ is not elementary, we are not guaranteed that $f - Dg \in \mathbb{Q}(x)[t]$. Nonetheless, computing $h = f - Dg$, we have $h = \frac{1}{t}$. I.e., $h = \frac{1}{\log x}$. It is known that $\int h$ is not elementary, which reaffirms that $\int f$ is not elementary. Finally, we have $\int f = 1/2\log(t+x) - 1/2\log(t-x) + \int \frac{1}{t}$.

6.3.3 Example

Consider $\int f$ where

$$f = \frac{(144x^5t_1 + 414x^4t_1 + 270x^3t_1 + 6x^2 + 6x)(t_2^3+1) + (-9x^2t_1+3)t_2^2}{(3x^2t_1-1)(t_2^3+3x^2)(x+1)} \in \mathbb{Q}(x, t_1, t_2),$$

$Dt_1 = t_1$ and $Dt_2 = \frac{1}{x+1}$. (I.e., $t_1 = e^x$ and $t_2 = \log(x+1)$.)

Writing $f = p + \frac{u}{v}$, where $\deg(u) < \deg(v)$ and v monic, we have $p = \frac{24xt_1(x+2)}{3x^2t_1-1}$, $u = \frac{-3t_2^2-6x^2-6x}{2(x+2)}$, and $v = t_2^3 + 3x^2$. Since $Dv = \frac{3t_2^2}{x+1} + 6x$, we have $\gcd(v, Dv) = 1$. Thus f is simple.

The reduced Gröbner basis is given by $\mathscr{B} = \{2z+1, t_2^3x+1\}$. Since $R_1(z) = 2z+1$ has only constant roots, $\int f$ is elementary. By Theorem 1, we have $g = -\frac{1}{2}\log(t_2^3 + 3x^2)$. Computing $h = f - Dg$, we have $h = \frac{24xt_1(x+2)}{3x^2t_1-1}$. The variable t_2 has been eliminated, thus leaving $h \in \mathbb{Q}(x, t_1)$ to be integrated.

Continuing, write $h = p + \frac{u}{v}$ with $p = \frac{8(x+2)}{x}$, $u = \frac{8(x+2)}{3x^3}$, and $v = t_1 - \frac{1}{3x^2}$. Note that $u, v \in \mathbb{Q}(x)[t_1]$. It is clear that $\gcd(v, Dv) = 1$. Now we have $\mathscr{B} = \{z-8, 3x^2t_1-1\}$.

This gives $z = 8$ and we have $g_2 = 8\log(3x^2t_1 - 1)$. Computing $h_2 = h_1 - Dg_2 = 0$, so we are done.

Putting all the pieces together, we have $\int f = g_1 + g_2 = 8\log(3x^2t_1 - 1) - \frac{1}{2}\log(t_2^3 + 3x^2)$. Verifying by computing $H = f - D(g_1 + g_2)$, we have $H = 0$.

BIBLIOGRAPHY

[1] Becker, Thomas and Volker Weispfenning. *Gröbner Bases A Computational Approach to Commutative Algebra*. Springer, 1993. In cooperation with Heinz Kredel.

[2] Bronstein, Manuel. Integration of elementary functions. *Journal of Symbolic Computation*, 9:117–173, 1990.

[3] Bronstein, Manuel. Risch differential equation on an algebraic curve. *ISSAC '91 Proceedings*, 1991.

[4] Bronstein, Manuel. Lazy hermite reduction. *Rapport de Recherche RR-3562, INRIA*, 1998.

[5] Bronstein, Manuel. Symbolic integration tutorial. *ISSAC'98*, 1998.

[6] Bronstein, Manuel. *Symbolic Integration I Transcendental Functions*. Springer, second edition, 2005.

[7] Cox, David, John Little, and Donal O'Shea. *Using Algebraic Geometry*. Springer, second edition, 2005.

[8] Cox, David, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer, third edition, 2007.

[9] Crespo, T., and Z. Hajto. *Introduction to Differential Galois Theory*. Politechnika Krakowska, 2007.

[10] Czichowski, Günter. A note on gröbner bases and integration of rational functions. *Journal of Symbolic Computation*, 20(2):163–167, 1995.

[11] James H. Davenport. *On the Integration of Algebraic Functions*. Springer-verlag, 1981.

[12] Geddes, Keith O., Stephen R. Czapor, and George Labahn. *Algorithms for Computer Algebra*. Kluwer Academic Publishers, 1992.

[13] Goursat, E. Sur les intégrales abeliennes qui s'experiment par logarithms. *C.R. Acad. Sci. Paris*, 118:515–517, 1894.

[14] Hartshorne, Robin. *Algebraic Geometry*. Springer, 1977.

[15] Hungerford, Thomas W. *Algebra*. Springer, 1974.

[16] Kauers, Manuel. Integration of algebraic functions: A simple heuristic for finding the logarithmic part. *ACM*, 2008.

[17] Knapp, Anthony W. *Advanced Algebra.* Birkäuser, 2007.

[18] Kuntz, Ernst. *Introduction to Commutative Algebra and Algebraic Geometry.* Birkäuser, 1985.

[19] Lang, Serge. *Abelian Varieties.* Springer, 1959.

[20] Lazard, D., and R. Rioboo. Integration of rational functions: Rational computation of the logarithmic part. *Journal of Symbolic Computation*, 9:113–116, 1990.

[21] Liouville, J. Premier mémoire sur la détermination des intégrales dont la valeur est algébrique. *Journal de l'Ecole Polytechnique*, 14:124–148, 1833.

[22] Liouville, J. Second mémoire sur la détermination des intégrales dont la valeur est algébrique. *Journal de l'Ecole Polytechnique*, 14:149–193, 1833.

[23] Liouville, J. Mémoire sur l'intégration d'une classe de fonctions transcendentes. *Journal für die reine und angewandte Mathematik*, 13:93–118, 1835.

[24] Mark van Hoeij. An algorithm for computing an integral basis in an algebraic function field. *J. Symbolic Computation*, 1994.

[25] Magid, Andy. *Lectures on Differential Galois Theory.* AMS, 1994.

[26] Risch, Robert. On the integration of elementary functions which are built up using algebraic operations. *Report SP-2801/002/00. System Development Corp., Santa Monica, GA*, 1968.

[27] Risch, Robert. Further results on elementary functions. *Report ILC-2402. IBM Corp., Yorktown Heights, NY*, 1969.

[28] Risch, Robert. The problem of integration in finite terms. *Transactions American Mathematical Society*, 139:167–169, 1969.

[29] Risch, Robert. The solution of the problem of lntegragion in finite terms. *Bulletin American Mathematical Society*, 78:605–608, 1970.

[30] Rothsetin, M. A new algorithm for the integration of exponential and logarithmic functions. *Proceedings of the 1977 MACSYMA Users Conference*, pages 263–274, 1977.

[31] Shafarevich, Igor R. *Basic Algebraic Geometry 1.* Springer, 1994.

[32] Trager, Barry M. *Integration of Algebraic Functions.* PhD thesis, Massachusetts Institute of Technology, 1984.

[33] van der Put, M., and M. Singer. *Galois Theory of Linear Differential Equations.* Springer-Verlag, 2003.

[34] Walker, Robert J. *Algebraic Curves.* Springer, 1978.

[35] Wall, C.T.C. *Singular Points of Plane Curves.* Cambridge University Press, 2004.