Geometrie der Zahlen

SS 2001
Uwe Schnell

Inhaltsverzeichnis

1 Grundlagen **2**
- 1.1 Konvexe Körper . . . 2
- 1.2 Gitter . . . 5

2 Konvexe Körper und Gitterpunkte **9**
- 2.1 Der erste Satz von Minkowski . . . 9
- 2.2 Der zweite Satz von Minkowski . . . 11
- 2.3 Extremalkörper . . . 12
- 2.4 Das inhomogene Minimum . . . 13
- 2.5 Anwendungen auf Polarkörper . . . 14
- 2.6 Konvexe Körper und beliebige Gitter . . . 14

3 Reduktionstheorie **16**
- 3.1 Einführung . . . 16
- 3.2 Minkowski–Reduktion . . . 17
- 3.3 Korkine–Zolotarev–Reduktion . . . 18
- 3.4 LLL–Reduktion . . . 19

4 Die kritische Determinante **22**
- 4.1 Der Auswahlsatz von Mahler . . . 22
- 4.2 Sternkörper und kritische Determinanten . . . 23
- 4.3 Der Satz von Minkowski–Hlawka . . . 25
- 4.4 Die Überdeckungskonstante . . . 26

5 Packungen und Überdeckungen **28**
- 5.1 Die Packungsdichte . . . 28
- 5.2 Die Überdeckungsdichte . . . 31
- 5.3 Packungen und Überdeckungen in der Ebene . . . 32
- 5.4 Kugelpackungen . . . 34
- 5.5 Kugelpackungen und Codierungstheorie . . . 36

Literatur

[1] Cassels, J. W. S: An introduction to Geometry of Numbers, Springer, Berlin, 1971.

[2] Conway, J. H., Sloane, N. J. A: Sphere packings, lattices and groups, Springer, New York, 1998.

[3] Grötschel, M., Lovasz, L., Schrijver, A.: Geometric algorithms and Combinatorial Optimization, Springer, Berlin, 1988.

[4] Gruber, P. M.: Geometry of Numbers, North–Holland, Amsterdam, 1987.

[5] Hardy, G. H., Wright, H. M.: Einführung in die Zahlentheorie, Oldenbourg, München, 1956.

[6] Jones, G. A., Jones, J. M.: Elementary number theory, Springer, London, 1998.

[7] Olds, C. D., Lax, A., Davidoff, G.: The Geometry of Numbers, Springer, Berlin, 2000.

[8] Rogers, C. A.: Packing and Covering, Cambridge University Press, Cambridge, 1964.

[9] Siegel, C. L.: Lectures on the Geometry of Numbers, Springer, Berlin, 1989.

[10] Zong, C.: Sphere packings, Springer, New York, 1999.

Index

Überdeckungsdichte, 31
Überdeckungsgitter, 26
Überdeckungskonstante, 26

Abstand von Gittern, 22
affin reguläres Sechseck, 33
affine Hülle, 2
Auswahlsatz von Mahler, 23

Basis eines Gitters, 5
beschränkte Menge von Gittern, 23
binärer Code, 36
Blaschke–Santalo
    Ungleichung von, 14
Blichfeldt
    Satz von, 9, 34, 35
Bourgain–Milman
    Ungleichung von, 14
Busemann–Feller
    Satz von, 4

Code, 36
    binärer, 36
    fehlerkorrigierender, 37
    linearer, 37
    sphärischer, 39
Codewort, 36

Determinante eines Gitters, 7
Dichtefunktion, 34
Dimension, 2
Dirichlet
    Satz von, 9
Diskriminante einer quadratischen Form, 10
Distanzfunktion, 4
duales Gitter, 8

einbeschriebenes Polytop, 33
endlicher Typ, 23
Extremalkörper, 12

Facette, 3
fehlerkorrigierender Code, 37
Fundamentalzelle, 8

Gaußscher Kanal, 38
Generatormatrix, 37
Gewicht eines Codewortes, 37
Gitter, 5
Gitterüberdeckung, 12, 31
Gitterüberdeckungsdichte, 31
Gitterpackung, 12, 29
Gitterpackungsdichte, 29
Gitterpflasterung, 12

Hadamard
    Satz von, 16
Hamming–Abstand, 36
Hamming–Code, 37
Hamming–Kugel, 37
Hermite
    Satz von, 9
homogene Linearform, 9

Index eines Untergitters, 7
inhomogene Minimum, 13

Körper, 2
Kissing number, 39
Konstruktion A, 38
Konstruktion B, 38
konvexe Hülle, 2
konvexe Menge, 2
Konvexkombination, 2
Korkine–Zolotarev–reduzierte Basis, 18
Kreuzpolytop, 2
Kristalle, 10
kritische Determinante, 23
kritisches Gitter, 24
Kugel, 2

lineare Hülle, 2
linearer Code, 37
LLL–Reduktion, 20
LLL–reduzierte Basis, 19
Lotabbildung, 3

Mahler
    Auswahlsatz von, 23
    Vermutung von, 14
maximales Überdeckungsgitter, 26
Minimalabstand, 36
Minimalgewicht eines Codes, 37
Minimalwinkel, 39
Minkowski
    1. Satz von, 9
    2. Satz von, 11
Minkowski–Hlawka
    Satz von, 25
Minkowski–reduzierte Basis, 17

Newton–Zahl, 39

obere Dichte, 28
orthogonaler Defekt, 16

Packungsdichte, 29
Packungsgitter, 26
parametrische Dichte, 10
Parkettierung, 8
periodische Überdeckung, 31
periodische Überdeckungsdichte, 31
periodische Packung, 29
periodische Packungsdichte, 29
polares Gitter, 8
Polarkörper, 5
polyedrische Menge, 3
Polytop, 3
primitive Menge, 6

quadratische Formen, 10

Reduktionstheorie, 16

sphärischer Code, 39
Stützfunktion, 4
Stützhyperebene, 3
Sternkörper, 24
strikt zulässiges Gitter, 23
sukzessive Minima, 11
Swinnerton–Dyer
    Satz von, 25

umbeschriebenes Polytop, 33
unendlicher Typ, 23
unimodulare Matrix, 7
untere Dichte, 28
Untergitter, 7

Würfel, 2
Wulff–shape, 10

zentralsymmetrische Menge, 2
zulässiges Gitter, 23

Einführung

Die 'Geometrie der Zahlen' wurde als eigenständiges Gebiet der Mathematik von Hermann Minkowski (1864–1909) begründet. Seine geniale Idee war es, geometrische Methoden (z. B. aus der Konvexgeometrie) anzuwenden, um zahlentheoretische Ergebnisse (z. B. in der Diophantischen Approximation) zu erhalten. Das Besondere dabei ist die Verknüpfung von 'diskreten' bzw. unstetigen Aspekten wie Ganzzahligkeit und Gitter und den stetigen Aspekten der Geometrie.
Eine wichtige Rolle in der Geometrie der Zahlen spielen Packungen und Überdeckungen. Erste Untersuchungen hierzu wurden von Kepler (1611) durchgeführt. Er stellte die Frage, welches die 'dichteste' (unendliche) Kugelpackung im $\mathbb{R}^3$ ist und vermutete, daß die Lösung 'gitterförmig' ist. Das heißt, die Kugeln sind in einer gewissen regelmäßigen Form angeordnet, wie man es etwa von gestapelten Apfelsinen oder Kanonenkugeln kennt. Dieses scheinbar einfache Problem ist erst vor kurzem mit intensivem Einsatz von Computern gelöst worden. Weitere Beiträge wurden von Lagrange und Gauß geliefert. Wichtige Vertreter aus dem 20. Jahrhundert sind Blichfeldt, Davenport, Hlawka, Mahler, Rogers und Voronoi. In den letzten Jahrzehnten sind zunehmend auch algorithmische Aspekte betrachtet worden. Ferner sind Anwendungen und Beziehungen zu diversen Bereichen der Mathematik hinzugekommen, etwa Codierungstheorie, Kryptographie, ganzzahlige Optimierung, numerische Integration oder Kristallographie.

1 Grundlagen

1.1 Konvexe Körper

Die Geometrie der Zahlen ist die „Anwendung von geometrischen Methoden in der Zahlentheorie“. Daher werden zunächst einige (konvex–) geometrische Begriffe eingeführt. Es sei im folgenden $\mathbb{R}^n$ der **Euklidische Raum** $\mathbb{R}^n = \{x : x = (x_1, \ldots, x_n)\}$ mit **Skalarprodukt** $xy = \sum_{i=1}^n x_i y_i$ und **Norm** $|x| = (xx)^{1/2}$.

Definition 1.1 *(a) Eine Menge $M \subset \mathbb{R}^n$ heißt* **konvex**, *wenn für alle $x, y \in M$ und alle $\lambda \in [0,1]$ gilt $\lambda x + (1-\lambda)y \in M$, d.h. mit je zwei Punkten ist auch die Verbindungsstrecke in M enthalten.*

(b) Zu $x^1, \ldots, x^r \in \mathbb{R}^n$ und $\lambda_1, \ldots, \lambda_r \geq 0$ mit $\sum_{i=1}^r \lambda_i = 1$ heißt $x = \sum_{i=1}^r \lambda_i x^i$ **Konvexkombination** *der x^i.*

(c) Zu $M \subset \mathbb{R}^n$ heißt die Menge der Konvexkombinationen von Punkten aus M die **konvexe Hülle** *von M. Bezeichnung:* $\operatorname{conv}(M)$.

(d) Eine Menge $M \subset \mathbb{R}^n$ heißt **Körper**, *wenn sie kompakt ist und nichtleeres Inneres besitzt. Die Menge aller konvexen Körper sei mit $\mathcal{K}^n$ bezeichnet.*

(e) Eine Menge $M \subset \mathbb{R}^n$ heißt **zentralsymmetrisch**, *wenn $M = -M$, d.h. wenn mit $x \in M$ auch $-x \in M$. Die Teilmenge aller zentralsymmetrischen konvexen Körper wird mit $\mathcal{K}_0^n$ bezeichnet.*

Beispiele:

(1) Die **Kugel** $B^n = \{x \in \mathbb{R}^n : |x| \leq 1\}$,

(2) Der **Würfel** $C^n = \{x \in \mathbb{R}^n : |x_i| \leq 1,\ i = 1, \ldots, n\}$,

(3) Das **Kreuzpolytop** $\operatorname{conv}\{\pm a^1, \ldots, \pm a^n\}$ mit linear unabhängigen $a^1, \ldots, a^n$.

Definition 1.2 *Sei $X \subset \mathbb{R}^n$ und $\mathcal{L}(X)$ die Familie aller linearen (affinen) Teilräume L mit $X \subset L$. Dann heißt $L(X) = \bigcap_{L \in \mathcal{L}(X)} L$* **lineare (affine) Hülle** *von X. Die* **Dimension von X** *wird als Dimension der affinen Hülle von X definiert.*

Konvexe Mengen besitzen die folgenden einfachen Eigenschaften.

Lemma 1.3 *Sei $\{K_i : i \in I\}$ eine nichtleere Familie von konvexen Mengen im $\mathbb{R}^n$. Dann ist $\bigcap_{i \in I} K_i$ konvex.*

Lemma 1.4 *Es seien $K, L \in \mathcal{K}^n$ und $A : \mathbb{R}^n \to \mathbb{R}^n$ eine lineare Abbildung. Dann sind $K + L = \{x + y : x \in K,\ y \in L\}$ und $AK = \{Ax : x \in K\}$ konvex. Insbesondere ist αK, für $\alpha \geq 0$, konvex.*

Lemma 1.5 *Für konvexes $M \subset \mathbb{R}^n$ mit $\operatorname{int}(M) \neq \emptyset$ sind $\operatorname{int}(M)$ und $\overline{M}$ konvex und es gilt $\overline{\operatorname{int}(M)} = \overline{M}$.*

Lemma 1.6 *Sei $K \in \mathcal{K}^n$ und $\alpha_1, \ldots, \alpha_r \geq 0$. Dann gilt $\sum_{i=1}^r (\alpha_i K) = (\sum_{i=1}^r \alpha_i) \cdot K$.*

Für $a \in \mathbb{R}^n,\ a \neq 0,\ \beta \in \mathbb{R}$ sind die **abgeschlossenen Halbräume** H^+, H^- gegeben durch

$$H^+ = \{x \in \mathbb{R}^n : ax \geq \beta\}, \quad H^- = \{x \in \mathbb{R}^n : ax \leq \beta\}.$$

Natürlich sind H^+, H^- konvex.

Definition 1.7 *$K \in \mathcal{K}^n$ heißt* **polyedrische Menge**, *falls $K = \bigcap_{i=1}^m H_i^+$ gilt. Eine beschränkte polyedrische Menge heißt* **Polytop**.

Bemerkung: Nach Lemma 1.3 sind polyedrische Mengen konvex.

Definition 1.8 *Sei $K \in \mathcal{K}^n$. Dann heißt die Hyperebene $H \subset \mathbb{R}^n$* **Stützhyperebene** *von K, falls gilt:*

$$H \cap K \neq \emptyset \quad \text{und} \quad \left(K \subset H^+ \quad \text{oder} \quad K \subset H^-\right).$$

F heißt **Facette** *von K, falls eine Stützhyperebene H existiert mit $F = H \cap K$ und $\dim F = n - 1$.*

Als nächstes wird gezeigt, daß jeder Randpunkt von K in einer Stützhyperebene enthalten ist. Dazu dient

Definition 1.9 *Sei $K \in \mathcal{K}^n$. Dann heißt die Abbildung $\Phi : \mathbb{R}^n \to K$ mit*

$$\Phi(p) = \begin{cases} p & : \quad p \in K \\ p' & : \quad p \notin K \end{cases},$$

wobei $p' \in K$ gegeben ist durch $|p - p'| = \min\{|p - q| : q \in K\}$ die **Lotabbildung** *von K.*

Lemma 1.10 *Sei $K \in \mathcal{K}^n$. Dann gilt*

(a) Die Lotabbildung $\Phi : \mathbb{R}^n \to K$ von K ist wohldefiniert, d. h. zu $p \notin K$ gibt es genau ein $\Phi(p) \in K$ mit minimalem Abstand.

(b) Für alle $x \in K$ und $p \in \mathbb{R}^n$ gilt

$$(p - \Phi(p)) \cdot x \leq (p - \Phi(p)) \cdot \Phi(p) \leq (p - \Phi(p)) \cdot p.$$

Lemma 1.11 (Busemann–Feller) *Sei $K \in \mathcal{K}^n$. Dann gilt*

$$|\Phi(p) - \Phi(q)| \leq |p - q|, \quad \text{für alle } p, q \in \mathbb{R}^n.$$

Insbesondere ist Φ stetig.

Satz 1.12 *Sei $K \in \mathcal{K}^n$ und $p \in \operatorname{bd} K$. Dann existiert eine Stützhyperebene H von K mit $p \in H$.*

Zur Beschreibung konvexer Körper sind besonders die folgenden beiden Funktionen geeignet.

Definition 1.13 *Für $K \in \mathcal{K}_0^n$ ist definiert*

(a) Die **Distanzfunktion** *$f : \mathbb{R}^n \to \mathbb{R}$ durch $f(x) = \min\{\lambda \geq 0 : x \in \lambda K\}$.*

(b) Die **Stützfunktion** *$h : \mathbb{R}^n \to \mathbb{R}$ durch $h(x) = \max\{y \cdot x : y \in K\}$.*

Einige Eigenschaften von f, h gibt

Satz 1.14 *Sei $K \in \mathcal{K}_0^n$. Dann gilt für die Distanz – bzw. Stützfunktion $g = f, h$ von K*

(a) $g(0) = 0,\ g(x) > 0,$ für $x \neq 0$,

(b) $g(x + y) \leq g(x) + g(y),$ für alle $x, y \in \mathbb{R}^n$,

(c) $g(\alpha x) = |\alpha| \cdot g(x),$ für alle $x \in \mathbb{R}^n,\ \alpha \in \mathbb{R}$,

(d) g ist stetig,

(e) $K = \{x \in \mathbb{R}^n : f(x) \leq 1\}$,

(f) $K = \{x \in \mathbb{R}^n : x \cdot y \leq h(y),$ für alle $y \in \mathbb{R}^n\}$.

Es gilt folgende Umkehrung von Satz 1.14:

Satz 1.15 *Genügt $g : \mathbb{R}^n \to \mathbb{R}$ (a), (b), (c) aus Satz 1.14, dann gilt*

(a) $K_1 = \{x \in \mathbb{R}^n : g(x) \leq 1\} \in \mathcal{K}_0^n$ und $f_{K_1} = g$,

(b) $K_2 = \{x \in \mathbb{R}^n : x \cdot y \leq g(y),$ für alle $y \in \mathbb{R}^n\} \in \mathcal{K}_0^n$ (und $h_{K_2} = g$).

Definition 1.16 *Sei $K \in \mathcal{K}_0^n$. Dann ist der* **Polarkörper** *K^* von K definiert durch*

$$K^* = \{x \in \mathbb{R}^n \,:\, x \cdot y \leq 1, \text{ für alle } y \in K\}.$$

Lemma 1.17 *Sei $K \in \mathcal{K}_0^n$ mit Distanzfunktion f. K^* habe die Distanzfunktion g. Dann gilt für alle $x, y \in \mathbb{R}^n$ $f(x)g(y) \geq x \cdot y$.*

Satz 1.18 *Sei $K \in \mathcal{K}_0^n$. Dann gilt $K^* \in \mathcal{K}_0^n$, $f_{K^*} = h_K$, $h_{K^*} = f_K$ und $K^{**} = K$.*

Beispiele:

(1) Einheitskugel $B = B^n$: $B^* = B$.

(2) Für den Würfel $C^n = \{x = (x_1, \ldots, x_n) \in \mathbb{R}^n \,:\, |x_i| \leq 1\}$ ist die Stützfunktion gegeben durch $h(y_1, \ldots, y_n) = \max\{\sum x_i y_i \,:\, (x_1, \ldots, x_n) \in C^n\} = \sum |y_i|$. Dies ist die Distanzfunktion des Kreuzpolytops $\operatorname{conv}\{\pm e^1, \ldots, \pm e^n\}$.

Satz 1.19 *Für $K \in \mathcal{K}_0^n$ und nichtsinguläres A gilt $(AK)^* = A^*K^*$, wobei $A^* = (A^{-1})^T$.*

1.2 Gitter

Definition 1.20 *Seien $a^1, \ldots, a^n$ n linear unabhängige Punkte des $\mathbb{R}^n$. Dann heißt die Menge Λ*

$$\Lambda = \{u_1 a^1 + \ldots + u_n a^n \,:\, u_1, \ldots, u_n \in \mathbb{Z}\}$$

Gitter. *Das Punktesystem $a^1, \ldots, a^n$ heißt* **Basis** *von Λ.*

A bezeichnet im folgenden sowohl die Matrix (a_{ij}) mit Spalten $a^1, \ldots, a^n$ als auch die durch A definierte lineare Abbildung des $\mathbb{R}^n$ als auch die Basis $\{a^1, \ldots, a^n\}$.
Sind die a^i die Koordinateneinheitsvektoren e^i, erhält man das Gitter Y der Punkte mit ganzzahligen Koordinaten. Für das allgemeine Gitter Λ gilt damit

$$\Lambda = AY$$

mit einer nichtentarteten Transformation A.

Satz 1.21 *Ein Gitter bildet eine diskrete Untergruppe des $\mathbb{R}^n$.*

Es gilt auch die folgende Umkehrung:

Satz 1.22 *Sei Λ eine diskrete Untergruppe des $\mathbb{R}^n$, die in keinem $(n-1)$-dimensionalen Unterraum des $\mathbb{R}^n$ enthalten ist. Dann ist Λ ein Gitter.*

Satz 1.23 *Seien $b^1, \ldots, b^n$ linear unabhängige Punkte eines Gitters Λ. Dann existiert eine Basis $\{a^1, \ldots, a^n\}$ von Λ, so daß*

$$b^i \in L(a^1, \ldots, a^i),\ i = 1, \ldots, n$$

gilt.

Korollar 1.24 *Seien $b^1, \ldots, b^n$ im Gitter Λ linear unabhängig. Dann existiert eine Basis $\{a^1, \ldots, a^n\}$ von Λ mit*

$$b^i = u_{1i}a^1 + \ldots + u_{ii}a^i,\ u_{ii} > 0,\ 0 \leq u_{ki} < u_{ii},\ k < i,\ i = 1, \ldots, n.$$

Für gegebene b^i ist die Basis $\{a^1, \ldots, a^n\}$ eindeutig bestimmt. Weiter ist $\{b^1, \ldots, b^n\}$ genau dann eine Basis, wenn $u_{ii} = 1,\ i = 1, \ldots, n$ gilt.

Im $\mathbb{R}^2$ gibt es das folgende einfache Kriterium dafür, wann $\{b^1, b^2\}$ eine Basis ist:

Satz 1.25 *Seien b^1, b^2 linear unabhängige Gitterpunkte des Gitters Λ im $\mathbb{R}^2$. Dann ist $\{b^1, b^2\}$ genau dann eine Basis, wenn das Dreieck* conv $\{0, b^1, b^2\}$ *keine weiteren Gitterpunkte enthält.*

Beispiel: Der Satz ist im $\mathbb{R}^n,\ n \geq 3$, falsch.
Gegenbeispiel: $\Lambda = Y,\ b^1 = (1, 0, 0),\ b^2 = (0, 1, 0),\ b^3 = (1, 1, 2)$.

Gilt im vorigen Korollar $u_{ii} = 1$, für $i = 1, \ldots, k$, so ist $b^i = a^i$, für $i = 1, \ldots, k$, so daß für jedes $y \in L(b^1, \ldots, b^k) \cap \Lambda$

$$(*) \qquad y = y_1 b^1 + \ldots + y_k b^k \quad \text{mit } y_i \in \mathbb{Z},\ i = 1, \ldots, k$$

gilt. Man definiert daher

Definition 1.26 *Ein System von $k \leq n$ linear unabhängigen Punkten $b^1, \ldots, b^k$ in einem Gitter Λ heißt* **primitiv**, *wenn jedes $y \in L(b^1, \ldots, b^k) \cap \Lambda$ die Darstellung (*) hat.*

Insbesondere heißt $b^1 \in \Lambda$ primitiv, falls $b^1 \neq 0$ und conv $\{0, b^1\}$ keinen weiteren Gitterpunkt enthält.

Satz 1.27 *Eine Menge von $k \leq n$ Punkten aus Λ ist genau dann primitiv, wenn sie zu einer Basis ergänzt werden kann.*

Lemma 1.28 *Sei $\Lambda \subset \mathbb{R}^n$ ein Gitter und $a^1, \ldots, a^n$ eine Basis von Λ. Ferner sei $c \in \Lambda$ mit $c = \sum_{i=1}^{n} z_i a^i,\ z_i \in \mathbb{Z},\ i = 1, \ldots, n$. Dann kann $a^1, \ldots, a^{r-1}, c$ genau dann zu einer Basis von Λ ergänzt werden, wenn $\operatorname{ggt}(z_r, \ldots, z_n) = 1$ gilt.*

Definition 1.29 *Ein* **Untergitter** Λ_1 *von* Λ *ist ein Gitter* Λ_1 *mit* $\Lambda_1 \subset \Lambda$. *Sei* $\{b^1, \ldots, b^n\}$ *eine Basis von* Λ_1 *und* $\{a^1, \ldots, a^n\}$ *die entsprechende Basis von* Λ *gemäß Korollar 1.24. Sei* A *die Matrix* $(a^1, \ldots, a^n)$ *und* B *die Matrix* $(b^1, \ldots, b^n)$. *Dann heißt* $|\det B / \det A|$ **Index** *des Untergitters* Λ_1 *in Bezug auf* Λ.

Bemerkung: Die Wohldefiniertheit des Index folgt mit dem späteren Begriff der Determinante eines Gitters oder auch aus der Tatsache, daß der Index die Anzahl der Nebenklassen von Λ_1 in der additiven Gruppe Λ ist (Übung).

Der folgende Satz gibt ein Kriterium dafür, wann ein System $\{b^1, \ldots, b^n\}$ Basis ist. Dazu zunächst:

Definition 1.30 *(a) Eine Matrix $A = (a_{ij})$ heißt* **ganzzahlig**, *wenn $a_{ij} \in \mathbb{Z},\ i, j = 1, \ldots, n$.*

(b) Eine ganzzahlige Matrix U heißt **unimodular**, *wenn $\det U = \pm 1$.*

Bemerkung: Ist U unimodular, so auch U^{-1} und es gilt $UY = Y$.

Satz 1.31 *Sei Λ ein Gitter mit Basis $\{a^1, \ldots, a^n\}$ und $b^1, \ldots, b^n \in \Lambda$. Dann ist $B = \{b^1, \ldots, b^n\}$ genau dann Basis von Λ, wenn eine unimodulare Matrix U existiert mit $B = AU$.*

Bemerkung: (1) Ist A eine Basis von Λ und B ein beliebiges System von n Punkten in Λ, so gilt $B = AV$ mit $V \in \mathbb{Z}^{n \times n}$. Satz 1.31 besagt, daß B genau dann eine Basis von Λ ist, wenn V unimodular ist.

(2) Entsprechend ist Korollar 1.24 äquivalent zu der Aussage, daß jedes $V \in \mathbb{Z}^{n \times n},\ V$ nichtsingulär, eine Darstellung $V = UT$, U unimodular, $T \in \mathbb{Z}^{n \times n}$ obere Dreiecksmatrix, hat.
Für $V = \{v^1, \ldots, v^n\}$ ergibt damit die Anwendung der unimodularen Transformation U^{-1}:

$$U^{-1} v^i \in L(e^1, \ldots, e^i).$$

Nach Satz 1.31 ist für jedes Gitter Λ und Basis A $|\det A|$ unabhängig von der Wahl der Basis. Daher definiert man

Definition 1.32 *Ist Λ ein Gitter mit Basis A, dann heißt $|\det A|$ die* **Determinante** *des Gitters. Bezeichnung: $d(\Lambda)$.*

Beispiel: $d(Y) = 1$.

Definition 1.33 *Sei Λ ein Gitter und $\{a^1, \ldots, a^n\}$ eine Basis von Λ. Dann heißt das halboffene Parallelepiped*

$$P = \{\vartheta_1 a^1 + \ldots + \vartheta_n a^n \,:\, 0 \leq \vartheta_i < 1\}$$

eine **Fundamentalzelle** *von Λ.*

$|\det A|$ ist damit das Volumen einer Fundamentalzelle und alle Fundamentalzellen haben gleiches Volumen.

Lemma 1.34 *Sei L ein Gitter und P eine zugehörige Fundamentalzelle. Dann ist $P + \Lambda$ eine* **Parkettierung** *des $\mathbb{R}^n$, d. h. $\mathbb{R}^n = P + \Lambda$ und $(u + P) \cap (v + P) = \emptyset,\ u, v \in \Lambda,\ u \neq v$.*

Lemma 1.35 *Es seien $A, B, C \in \mathbb{R}^{n\times n}$ nichtsingulär und $\Lambda = AY$. Dann gilt*

(a) $C\Lambda$ *ist ein Gitter mit* $d(C\Lambda) = |\det C| \cdot d(\Lambda)$.

(b) $A^{**} = A, \quad \det A^* = (\det A)^{-1}, \quad (AB)^* = A^* B^*$.

(c) $\{x \in \mathbb{R}^n \,:\, x \cdot y \in \mathbb{Z}$, *für alle* $y \in Y\} = Y$.

(d) $x \cdot y = (Ax) \cdot (A^* y)$, *für alle* $x, y \in \mathbb{R}^n$.

Satz 1.36 *Ist Λ ein Gitter mit Basis A, dann ist $\{y \in \mathbb{R}^n \,:\, x \cdot y \in \mathbb{Z}$, für alle $x \in \Lambda\}$ ein Gitter mit der Basis A^*.*

Definition 1.37 *Ist $\Lambda = AY$ ein Gitter, dann heißt A^*Y das* **polare** *(oder* **duale***) Gitter. Bezeichnung: Λ^*.*

Satz 1.38 *Sei Λ ein Gitter mit Basis $\{a^1, \ldots, a^n\}$ und C nichtsingulär. Dann gilt*

(a) $d(\Lambda^*) = d(\Lambda)^{-1}$,

(b) $(C\Lambda)^* = C^*\Lambda^*$,

(c) $\Lambda^{**} = \Lambda$,

(d) Man erhält eine Basis von Λ^* durch Lösung der Gleichungssysteme

$$a^i b^j = \delta_{ij} \qquad (i, j = 1, \ldots, n),$$

wobei δ_{ij} das Kroneckersymbol bezeichnet.

2 Konvexe Körper und Gitterpunkte

2.1 Der erste Satz von Minkowski

Der folgende Satz von Minkowski verknüpft das Volumen eines konvexen Körpers mit seiner Lage im Gitter. Durch diese Verknüpfung stetiger (Volumen) und diskreter (Gitter) Eigenschaften ist er das zentrale Ergebnis in der Geometrie der Zahlen und er hat zahlreiche Anwendungen. Dabei versteht man unter dem Volumen eines konvexen Körpers K sein n–dimensionales Jordan–Maß oder Lebesgue–Maß (Schreibweise $V(K)$). Man kann leicht zeigen, daß jeder konvexe Körper Jordan–meßbar ist. Wir setzen das hier als bekannt voraus.

Lemma 2.1 (Blichfeldt, 1914) *Sei $M \subset \mathbb{R}^n$ kompakt und meßbar mit $(u + \operatorname{int}(M)) \cap (v + \operatorname{int}(M)) = \emptyset$, für alle $u, v \in Y,\ u \neq v$. Dann gilt $V(M) \leq 1$.*

Enthält ein zentralsymmetrischer konvexer Körper außer 0 keine weiteren Gitterpunkte, so kann er nicht 'allzu groß' sein. Anschaulich gesprochen ist er entweder 'kurz und dick' oder 'lang und schmal'. Eine genaue Schranke gibt der folgende Satz.

Satz 2.2 (erster Satz von Minkowski, 1896) *Sei $K \in \mathcal{K}_0^n$ und $V(K) \geq 2^n$. Dann existiert ein $u \in Y \cap K$ mit $u \neq 0$.*

Die Menge der zulässigen Punkte ist für viele Probleme durch einen konvexen Körper gegeben. Mit Hilfe des Satzes von Minkowski erhält man dann eine Aussage über ganzzahlige Lösungen.

Eine lineare Abbildung $\xi : \mathbb{R}^n \to \mathbb{R}$ heißt auch **homogene Linearform**, d. h. $\xi(x) = \xi_1 x_1 + \ldots + \xi_n x_n$.

Satz 2.3 (Dirichlet, 1842) *Seien $\xi_1, \ldots, \xi_n$ homogene Linearformen mit Determinante $\Delta = \det(\xi_{ij}) \neq 0$. Dann existiert zu $\tau_1, \ldots, \tau_n \geq 0$ mit $\tau_1 \cdot \ldots \cdot \tau_n = |\Delta|$ ein $x \in \mathbb{Z}^n \backslash \{0\}$ mit*

$$|\xi_i(x)| \leq \tau_i,\ i = 1, \ldots, n.$$

Satz 2.4 (Hermite, 1850) *Seien $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$. Dann gibt es unendlich viele $(p_1, \ldots, p_n, q) \in \mathbb{Z}^{n+1}$ mit $q > 0$ und*

$$|q\alpha_i - p_i| \leq q^{-1/n},\ i = 1, \ldots, n.$$

Bemerkung: Satz 2.4 kann nicht wesentlich verbessert werden. Man kann zeigen: Zu gegebenem n existiert ein $\gamma > 0$ und $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$, so daß es nur endlich viele Lösungen von $|q\alpha_i - p_i| \leq \gamma \cdot q^{-1/n},\ i = 1, \ldots, n$ gibt (Beweis siehe GL, S. 479).

Ein Gegenstück zu Satz 2.4 ist der folgende über das Minimum einer gegebenen Linearform:

Satz 2.5 *Seien $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$. Dann gibt es unendlich viele $(u_1, \ldots, u_{n+1}) \in \mathbb{Z}^{n+1}$ mit $\max |u_i| > 0$, die*

$$|u_1\alpha_1 + \ldots + u_n\alpha_n - u_{n+1}| \leq (\max |u_i|)^{-n}$$

genügen.

Die nächste Anwendung bezieht sich auf positiv definite **quadratische Formen**, d. h. Abbildungen der Form $Q(x) = x^T \cdot S \cdot x > 0$, für $x \neq 0$. Man kann o. E. davon ausgehen, daß die Matrix S symmetrisch ist. Die Zahl $D = \det S$ heißt **Diskriminante** von Q. Aus der Analysis ist das Volumen κ_n der n–dimensionalen Einheitskugel $B^n = \{x \in \mathbb{R}^n : |x| \leq 1\}$ bekannt. Es gilt $\kappa_n = \pi^{n/2}(\Gamma(1 + n/2))^{-1}$. Für eine positiv definite quadratische Form Q mit Diskriminante D ist $\{x \in \mathbb{R}^n : Q(x) \leq \lambda\}$ ein Ellipsoid E mit 0 als Mittelpunkt und $V(E) = \kappa_n \lambda^{n/2} D^{-1/2}$ (vgl. Übung).

Satz 2.6 *Sei $Q(x) = Q(x_1, \ldots, x_n) = x^T \cdot S \cdot x$, $S^T = S$, eine positiv definite quadratische Form mit Diskriminante D. Dann existiert ein $u \in Y$, $u \neq 0$, mit $Q(u) \leq 4(\kappa_n^{-2} D)^{1/n}$.*

Bemerkung: Mit geschickter Anwendung des Satzes von Minkowski kann man das Lemma von Fermat und den Satz von Lagrange über die Darstellbarkeit als Summe von Quadraten zeigen (vgl. Übung).

Abschließend eine Anwendung für die Modellierung von Kristallen mit Hilfe von dichten endlichen Packungen. Hierzu sei Λ ein Gitter, so daß sich die Kugeln $\{u + B^n : u \in \Lambda\}$ nicht überlappen. Für gegebene Anzahl k von Kugeln (Atomen) kann man die Frage stellen, welches die 'dichteste' Anordnung C_k mit $C_k \subset \Lambda$ ist. Dabei wird die Güte der Packung mit der sogenannten **parametrischen Dichte**

$$\frac{k\kappa_n}{V(\operatorname{conv} C_k + \varrho B^n)}$$

gemessen, wobei $\varrho > 0$ ein Parameter ist, der den Einfluß des Randes kontrolliert (vgl. Dicke der Ummantelung eines Kabelstrangs). Für gegebene Anzahl k ist die Bestimmung der optimalen Anordnung sehr schwierig. Doch man kann zeigen, daß die optimalen Anordnungen für $k \to \infty$ gegen eine gewisse Gestalt konvergieren. Diese stimmt mit der aus der Kristallographie bekannten **Wulff–shape** überein und ist gegeben durch

$$W(\Lambda, \varrho) = \left\{ x \in \mathbb{R}^n : \frac{u}{|u|} \cdot x \leq 1 - \frac{1}{2\varrho|u|},\ \forall u \in \Lambda^* \backslash \{0\} \right\}.$$

Für Parameter $\varrho > \varrho_\Lambda = \max\limits_{u \in \Lambda^* \backslash \{0\}} 1/(2|u|)$ ist diese Menge nicht leer. $W(\Lambda, \varrho)$ ist per Definition der Durchschnitt von unendlich vielen Halbräumen. Verantwortlich für die flächenartige Gestalt vieler Kristalle ist jedoch folgender Satz.

Satz 2.7 *Für $\varrho > \varrho_\Lambda$ ist $W(\Lambda, \varrho)$ ein Polytop.*

2.2 Der zweite Satz von Minkowski

Eine Verschärfung des ersten Satzes von Minkowski kann mit Hilfe der sukzessiven Minima gegeben werden.

Definition 2.8 *Für $M \subset \mathbb{R}^n$ sei $\lambda_i,\ i = 1, \ldots, n$ definiert durch*

$$\lambda_i = \inf\{\lambda\ :\ \lambda > 0,\ \dim(\lambda M \cap Y) \geq i\}.$$

Die λ_i heißen **sukzessive Minima** *von M ($\lambda_i = \infty$ ist möglich).*

Die Bezeichnung rührt von der Vorstellung, die Menge M 'aufzublasen', bis sie einen Gitterpunkt $u^1 \neq 0$ enthält. Dann weiter, bis ein linear unabhängiges u^2 hinzukommt ...

Beispiel: Sei K 'Zigarrenschachtel' mit Kantenlängen $2a_1 \leq \ldots \leq 2a_n$.
Dann gilt $\lambda_i = 1/a_{n-i+1}$.

Bemerkung:

(1) Nach Definition gilt $\lambda_1 \leq \ldots \leq \lambda_n$.

(2) Für $M = K,\ K \in \mathcal{K}_0^n$, werden die Infima angenommen.

(3) Nach Konstruktion folgt die Existenz von $u^1, \ldots, u^n \in Y$ mit $u^i \in \lambda_i K,\ u^i \notin L(u^1, \ldots, u^{i-1})$.

(4) Für die u^i gilt $u^i \in \operatorname{bd} \lambda_i K,\ i = 1, \ldots, n$.

(5) K definiert die λ_i eindeutig, aber keineswegs die u^i (z. B. beim Würfel nicht).

(6) Ist U eine unimodulare Transformation, so ist $\lambda_i(UK) = \lambda_i(K),\ i = 1, \ldots, n$ (Übung).

Da $\lambda_1 \cdot K$ keine Gitterpunkte im Innern enthält, folgt nach Satz 2.2 $\lambda_1^n V(K) \leq 2^n$. Es gilt die folgende Verschärfung.

Satz 2.9 (Zweiter Satz von Minkowski) *Sei $K \in \mathcal{K}_0^n$ mit sukzessiven Minima $\lambda_1, \ldots, \lambda_n$. Dann gilt*

$$\lambda_1 \cdot \ldots \cdot \lambda_n \cdot V(K) \leq 2^n.$$

Für die sukzessiven Minima gilt folgende einfache untere Schranke:

Satz 2.10 *Sei $K \in \mathcal{K}_0^n$ mit den sukzessiven Minima $\lambda_1, \ldots, \lambda_n$. Dann gilt*

$$\lambda_1 \cdot \ldots \cdot \lambda_n \cdot V(K) \geq 2^n/n!.$$

Bemerkung: (1) Sei Λ das von $(u^1, \ldots, u^n)$ aufgespannte Untergitter von Y. Dann gilt für den Index $I(\Lambda) \leq n!$ (Übung).

(2) $I \neq 1$ ist möglich, d. h. $\{u^1, \ldots, u^n\}$ ist nicht unbedingt eine Basis (Übung).

2.3 Extremalkörper

Definition 2.11 *$K \in \mathcal{K}_0^n$ heißt* **extremal**, *falls $V(K) = 2^n$ und $\lambda_1(K) = 1$.*

Beispiel: Würfel

Definition 2.12 *Sei $M \subset \mathbb{R}^n$ kompakt, Λ ein Gitter. $M + \Lambda$ heißt* **(Gitter–)Packung**, *falls $(\operatorname{int} M + u) \cap (\operatorname{int} M + v) = \emptyset$, für $u, v \in \Lambda,\ u \neq v$.*
$M + \Lambda$ heißt **(Gitter–) Überdeckung**, *falls $\mathbb{R}^n = M + \Lambda$.*
$M + \Lambda$ heißt **(Gitter–) Pflasterung**, *falls $M + \Lambda$ Gitterüberdeckung und Gitterpackung ist.*

Lemma 2.13 *Sei $K \in \mathcal{K}^n$. Dann gilt $Y + K$ ist Packung $\Leftrightarrow$ $\lambda_1(K - K) \geq 1$.*

Extremalkörper können wie folgt charakterisiert werden.

Satz 2.14 *Sei $K \in \mathcal{K}_0^n$. K ist genau dann extremal, falls $\frac{1}{2}K + Y$ eine Pflasterung ist.*

Jedes extremale K ist ein Polytop:

Satz 2.15 *Sei $K \in \mathcal{K}_0^n$ mit $\lambda_1(K) \geq 1$.*

(a) Dann existiert ein Polytop $K_1 \in \mathcal{K}_0^n$ mit $K \subset K_1$ und $\lambda_1(K_1) \geq 1$.

(b) Ist K extremal, so ist K ein Polytop.

Bemerkung: Ist K extremal und damit ein Polytop, dann enthält jede Facette F einen Gitterpunkt in ihrem (relativen) Inneren, denn sonst erhielte man durch Verschieben von F und $-F$ ein $K' \in \mathcal{K}_0^n$ mit $\lambda_1(K') \geq 1,\ K \subset K'$ und $V(K') > V(K)$.

Die Extremalkörper haben folgende Eigenschaften:

Satz 2.16 *Sei $K \in \mathcal{K}_0^n$ extremal. Dann gilt*

(a) Höchstens $2(2^n - 1)$ Gitterpunkte liegen in den Inneren der Facetten von K.

(b) K hat höchstens $2(2^n - 1)$ Facetten.

(c) Auf dem Rand von K liegen mindestens $2(2^n - 1)$ Gitterpunkte.

Konstruiert man K_1 wie in Satz 2.15, dann hat jede Facette von K_1 einen Gitterpunkt im Innern. Wie im Beweis von Satz 2.16 liegen diese in verschiedenen Äquivalenzklassen $\neq 0$. Darum ist die Anzahl der Facetten $\leq 2(2^n - 1)$. Es gilt also die folgende Verschärfung von Satz 2.15.

Satz 2.17 *Sei $K \in \mathcal{K}_0^n$ und $\lambda_1(K) \geq 1$. Dann existiert ein Polytop $K_1 \in \mathcal{K}_0^n$ mit höchstens $2(2^n - 1)$ Facetten, so daß $K \subset K_1$ und $\lambda_1(K_1) \geq 1$ gilt.*

Bemerkung: In der Ebene gibt es nur zwei wesentlich verschiedene Typen von Extremalkörpern, nämlich Quadrat und Sechseck. Im $\mathbb{R}^3$ gibt 5 verschiedene Typen (Würfel, hexagonales Prisma, Rhombendodekaeder, hexarhombisches Dodekaeder und das Kuboktaeder). Im $\mathbb{R}^4$ gibt es schon 52 verschiedene Typen und für $n \geq 5$ ist die Anzahl noch unbekannt.

2.4 Das inhomogene Minimum

Das Gegenstück zu

$$\lambda_1(K) = \max\{\lambda > 0 \,:\, \frac{\lambda}{2} \cdot K + Y \text{ Packung}\}$$

liefert

Definition 2.18 *Für $K \in \mathcal{K}_0^n$ heißt*

$$\mu(K) = \min\{\sigma > 0 \,:\, \sigma \cdot K + Y \;\; \textit{Überdeckung}\}$$

das **inhomogene Minimum** *von K.*

Bemerkung:

(1) Wegen $\operatorname{int} K \neq \emptyset$ gilt $\mu < \infty$.

(2) Wegen K kompakt wird das Minimum angenommen.

(3) Wegen K konvex und symmetrisch gilt $\sigma K + Y = \mathbb{R}^n$, für alle $\sigma \geq \mu$.

Alternative Definition:

$$\mu = \tilde{\mu}(K) = \min\{\sigma > 0 \,:\, (\sigma K + z) \cap Y \neq \emptyset,\ \forall z \in \mathbb{R}^n\}.$$

Beispiel: Für extremales K gilt nach Satz 2.14: $\mu = 1/2$.

Das inhomogene Minimum läßt sich in Beziehung zu den λ_i setzen.

Satz 2.19 *Sei $K \in \mathcal{K}_0^n$. Dann gilt*

$$\frac{1}{2}\lambda_n \leq \mu \leq \frac{1}{2} \cdot (\lambda_1 + \ldots + \lambda_n).$$

2.5 Anwendungen auf Polarkörper

Hier soll der Satz von Minkowski auf Polarkörper angewandt werden. Zunächst wird gezeigt, daß gewisse Größen von zueinander polaren konvexen Körpern in Beziehung stehen.

Satz 2.20 *Sei $K \in \mathcal{K}_0^n$. Dann gilt*

$$4^n(n!)^{-2} \leq V(K) \cdot V(K^*) \leq 4^n.$$

Bemerkung: Beide Ungleichungen können verbessert werden. Die (optimale) obere Schranke κ_n^2 wird durch die Ungleichung von Blaschke–Santalo gegeben. Gleichheit gilt für $K = B^n$. Die Vermutung von Mahler besagt, daß die optimale untere Schranke $4^n/n!$ ist, mit Gleichheit für Würfel und Kreuzpolytop. Die bisher beste untere Schranke von Bourgain–Milman ist $\alpha^n \kappa_n^2$, für ein $\alpha > 0$.

Satz 2.21 *Sei $K \in \mathcal{K}_0^n$ mit den sukzessiven Minima $\lambda_1, \ldots, \lambda_n$. Weiter seien $\lambda_1^*, \ldots, \lambda_n^*$ die sukzessiven Minima des Polarkörpers K^*. Dann gilt*

$$1 \leq \lambda_i \cdot \lambda_{n+1-i}^* \leq (n!)^2, \quad i = 1, \ldots, n.$$

Bemerkung: Mit Methoden aus der Funktionalanalysis kann diese Schranke erheblich verbessert werden. Es gilt $\lambda_i \lambda_{n+1-i}^* \leq \beta n$, mit einer Konstanten $\beta > 0$.

2.6 Konvexe Körper und beliebige Gitter

Die bisherigen Ergebnisse lassen sich leicht auf den Fall beliebiger Gitter übertragen. Ein Gitter Λ im $\mathbb{R}^n$ hat die Form $\Lambda = AY$ mit $A \in \mathbb{R}^{n \times n}$ nichtsingulär. Anwendung von A^{-1} ergibt $A^{-1}\Lambda = Y$, $V(A^{-1}K) = |\det A|^{-1} \cdot V(K)$. Es gilt $u \in K \Rightarrow A^{-1}u \in A^{-1}K$. Damit überträgt sich Satz 2.2:

Satz 2.22 *Sei Λ ein Gitter und $K \in \mathcal{K}_0^n$ mit $V(K) \geq 2^n \cdot d(\Lambda)$. Dann existiert ein $u \in \Lambda$ mit $u \neq 0$ und $u \in K$.*

Für $M \subset \mathbb{R}$ und Gitter Λ sind die sukzessiven Minima definiert durch

$$\lambda_i(M, \Lambda) = \inf\{\lambda : \dim(\lambda M \cap \Lambda) \geq i\}, \ i = 1, \ldots, n.$$

Für $\Lambda = AY$ gilt $A^{-1}(\lambda M \cap \Lambda) = \lambda A^{-1} M \cap Y$, so daß die λ_i affin invariant sind ($\lambda_i(AK, AY) = \lambda_i(K, Y)$). Damit übertragen sich Satz 2.9 und 2.10:

Satz 2.23 *Ist Λ ein Gitter und $K \in \mathcal{K}_0^n$, so gilt*

$$(n!)^{-1} \cdot 2^n \cdot d(\Lambda) \leq \lambda_1(K, \Lambda) \cdot \ldots \cdot \lambda_n(K, \Lambda) \cdot V(K) \leq 2^n \cdot d(\Lambda).$$

Das inhomogene Minimum $\mu(M, \Lambda)$ von $M \subset \mathbb{R}^n$ in Bezug auf das beliebige Gitter Λ ist definiert durch

$$\mu(M, \Lambda) = \inf\{\sigma > 0 \,:\, \sigma M + \Lambda = \mathbb{R}^n\}.$$

Damit ist das inhomogene Minimum ebenfalls affin invariant und so

Satz 2.24 *Sei $K \in \mathcal{K}_0^n$ und Λ ein Gitter. Dann gilt*

$$\frac{1}{2}\lambda_n(K, \Lambda) \leq \mu(K, \Lambda) \leq \frac{1}{2}(\lambda_1(K, \Lambda) + \ldots + \lambda_n(K, \Lambda)).$$

Für den Spezialfall der Kugel $K = B^n$ kann die obere Schranke in Satz 2.24 verbessert werden:

Satz 2.25 *Sei Λ ein Gitter. Dann gilt*

$$\mu(B^n, \Lambda)^2 \leq \frac{1}{4} \cdot (\lambda_1(B^n, \Lambda)^2 + \ldots + \lambda_n(B^n, \Lambda)^2).$$

Nach Satz 1.19 ist für $K \in \mathcal{K}_0^n$ und eine nichtsinguläre Transformation A: $(A^{-1}K)^* = (A^*)^{-1}K^*$. Anwendung des Konzeptes des polaren Gitters (Definition 1.37) ergibt aus Satz 2.21

Satz 2.26 *Sei $K \in \mathcal{K}_0^n, K^*$ der Polarkörper von K und Λ ein Gitter. Dann gilt*

$$1 \leq \lambda_i(K, \Lambda) \cdot \lambda_{n+1-i}(K^*, \Lambda^*) \leq (n!)^2, \;\; i = 1, \ldots, n.$$

3 Reduktionstheorie

3.1 Einführung

Zu einem Gitter gibt es bekannter Weise unendlich viele verschiedene Basen. Jedoch können dabei beliebig lange Basisvektoren und beliebig spitze Winkel zwischen diesen auftreten. Die Reduktionstheorie beschäftigt sich mit der Konstruktion von „guten“ Basen. Als Maß für die Güte dient die folgende Definition.

Definition 3.1 *Sei Λ ein Gitter. Dann wird zu einer Basis $B = \{b^1, \ldots, b^n\}$ der Quotient*

$$\frac{|b^1| \cdot \ldots \cdot |b^n|}{d(\Lambda)}$$

der **orthogonale Defekt** *genannt.*

Lemma 3.2 *Sei $\Lambda \subset \mathbb{R}^n$ ein Gitter und $b^1, \ldots, b^n$ eine Basis von Λ. Desweiteren sei für $1 \leq j \leq n$ gemäß Gram–Schmidt*

$$g^j = b^j - \sum_{i=1}^{j-1} \mu_{ji} \cdot g^i, \quad \textit{mit} \quad \mu_{ji} = \frac{b^j \cdot g^i}{|g^i|^2}. \tag{3.1}$$

Dann gilt

(a) $g^i \cdot g^j = 0$, *für* $1 \leq i, j \leq n$ *und* $i \neq j$,

(b) $|g^j| \leq |b^j|$, *für* $j = 1, \ldots, n$.

(c) $|g^1| \cdot \ldots \cdot |g^n| = d(\Lambda)$,

(d) $|b| \geq \min\{|g^1|, \ldots, |g^n|\}$, *für alle* $b \in \Lambda \backslash \{0\}$.

Es folgt sofort eine untere Schranke für den orthogonalen Defekt.

Lemma 3.3 (Hadamard) *Der orthogonale Defekt einer Basis ist ≥ 1.*

Zur Konstruktion von Basen mit kleinem orthogonalen Defekt gibt es diverse Reduktionsverfahren, etwa von Lagrange, Gauß, Minkowski, Dirichlet, Hermite, Korkine–Zolotarev und Voronoi. Diesen ist gemeinsam, daß jeweils kurze Gittervektoren gesucht werden. Dies führt insbesondere zu folgendem Problem.

Problem: Gegeben sei ein Gitter $\Lambda \subset \mathbb{Q}^n$. Man bestimme ein $u \in \Lambda \backslash \{0\}$ mit minimaler Länge, d. h. $|u| = \lambda_1(\Lambda) = \lambda_1(B^n, \Lambda)$.

Der erste Satz von Minkowski gewährleistet, daß es ein $u \in \Lambda \backslash \{0\}$ gibt mit

$$|u| \leq 2 \cdot \left(\frac{d(\Lambda)}{\kappa_n} \right)^{1/n} \sim c \cdot \sqrt{n} \cdot d(\Lambda)^{1/n}.$$

Jedoch wird kein konstruktives Verfahren angegeben, um dieses u zu bestimmen.

Ein verwandtes Problem ist es, zu einem gegebenen Punkt den nähesten Gitterpunkt zu bestimmen.

Problem: Gegeben sei ein Gitter $\Lambda \subset \mathbb{Q}^n$ und ein Punkt $b \in \mathbb{Q}^n$. Man bestimme ein $u \in \Lambda$ mit minimalem Abstand zu b, d. h. $|b-u| = \min\{|b-v| \,:\, v \in \Lambda\}$.

Bemerkung: (1) Es gibt immer ein $u \in \Lambda$ mit $|b-u| \leq \mu(\Lambda)$. Jedoch ist die Bestimmung von μ und u algorithmisch nicht effizient möglich.

(2) Im Gegensatz zu λ_1 gibt es für μ keine Schranke, die nur von der Dimension und der Determinante abhängt.

3.2 Minkowski–Reduktion

Nach Definition der sukzessiven Minima gibt es linear unabhängige Vektoren $u^1, \ldots, u^n$ mit $\lambda_i(\Lambda) = \lambda_i(B^n, \Lambda) = |u^i|,\ i = 1, \ldots, n$. Jedoch bilden diese im Allgemeinen keine Basis.

Beispiele: (1) Sei $\Lambda = Y$ und K der Würfel. Dann kann man $u^i = e^i$, für $i = 1, \ldots, n-2$ und $u^{n-1} = e^{n-1} + e^n,\ u^n = e^{n-1} - e^n$ wählen. Diese liefern offensichtlich keine Basis. Jedoch kann man die Wahl der u^i leicht so abändern, daß sie eine Basis bilden.

(2) Sei $\Lambda \subset \mathbb{R}^5$ mit Basis $\{2e^1, 2e^2, 2e^3, 2e^4, e^1 + \ldots + e^5\}$ und $K = B^5$. Dann haben zwangsweise alle u^i die Länge 2 (man beachte: $2e^5 \in \Lambda$). Also sind $u^1, \ldots, u^n$ nicht so wählbar, daß sie eine Basis bilden.

Das Verfahren von Minkowski beruht auf der folgenden Verschärfung.

Definition 3.4 *Eine Basis $b^1, \ldots, b^n$ heißt* **Minkowski–reduziert**, *falls für $i = 1, \ldots, n$*

(i) $\{b^1, \ldots, b^i\}$ *primitiv,*

(ii) $|b^i| = \min\,\{|b| \,:\, \{b^1, \ldots, b^{i-1}, b\}$ *primitiv* $\}$.

Die Vektoren b^i können sukzessive gewählt werden und es gilt offensichtlich
$|b^1| \leq |b^2| \leq \ldots \leq |b^n|$.

Beispiel: In dem obigen Beispiel (2) ist die angegebene Basis Minkowski–reduziert.

Satz 3.5 *Es sei Λ ein Gitter mit sukzessiven Minima $\lambda_1, \ldots, \lambda_n$ ($\lambda_i = \lambda_i(B^n, \Lambda)$). Ferner sei $\{b^1, \ldots, b^n\}$ eine Minkowski–reduzierte Basis und $\mu_i := |b^i|$. Dann gilt*

$$\lambda_i \leq \mu_i \leq \delta_i \lambda_i,$$

mit

$$\delta_1 = \delta_2 = \delta_3 = \delta_4 = 1 \quad \textit{und} \quad \delta_i = \left(\frac{5}{4}\right)^{(i-4)/2}, \quad i = 5, 6, \ldots, n.$$

Satz 3.6 *Zu jedem Gitter $\Lambda \subset \mathbb{R}^n$ existiert eine Basis $\{b^1, \ldots, b^n\}$, so daß $|b^1| \cdot \ldots \cdot |b^n| \leq \delta(n) \cdot d(\Lambda)$ gilt (für eine nur von n abhängige Konstante $\delta(n)$).*

3.3 Korkine–Zolotarev–Reduktion

Definition 3.7 *Sei Λ ein Gitter, $\{b^1, \ldots, b^n\}$ eine Basis von Λ und μ_{ji} wie in (3.1). $\{b^1, \ldots, b^n\}$ heißt* **Korkine–Zolotarev–reduziert***, falls gilt*

(i) b^1 ist ein Vektor aus Λ mit minimaler Länge,

(ii) b^i hat minimalen positiven Abstand zu $L(b^1, \ldots, b^{i-1})$, für $i = 2, \ldots, n$,

(iii) $|\mu_{ji}| \leq 1/2$, für $1 \leq i < j \leq n$.

Bemerkung: (1) Die Vektoren $b^1, \ldots, b^n$ lassen sich nacheinander bestimmen. Die Bedingung (iii) ist äquivalent zu der Tatsache, daß die Orthogonalprojektion von b^i auf $L(b^1, \ldots, b^{i-1})$ in $P = \{x \in \mathbb{R}^n : x = \sum_{j=1}^{i-1} \lambda_j g^j, \ |\lambda_j| \leq 1/2\}$ liegt. Da $P + \mathbb{Z} \cdot b^1 + \ldots + \mathbb{Z} \cdot b^{i-1}$ eine Pflasterung von $L(b^1, \ldots, b^{i-1})$ ist, kann dies erfüllt werden, indem von b^i geeignete Vielfache der $b^1, \ldots, b^{i-1}$ abgezogen werden.

(2) Sei $E_i = L(b^1, \ldots, b^{i-1})^\perp$. Dann ist Λ / E_i ein $(n - i + 1)$–dimensionales Gitter. Die Bedingung (ii) ist äquivalent dazu, einen kürzesten Gittervektor $\neq 0$ in Λ / E_i zu finden.

(3) Für Korkine–Zolotarev–reduzierte Basen ist die Schranke aus Satz 3.6 zu n^n, der bisher besten Schranke, verbessert worden.

Beispiel: Sei $\Lambda = \{(x, y, z)^T \in \mathbb{Z}^3 : x + y + z \equiv 0 \bmod 2\}$. Λ ist ein Gitter mit Basis $\{(1, 0, 1)^T, \ (0, 1, 1)^T, \ (0, 0, 2)^T\}$.

$i = 1$: Offensichtlich gilt $\lambda_1(\Lambda) = \sqrt{2}$. Man kann also z. B. $b^1 = (1, 0, 1)^T$ setzen.

$i = 2$: $\{c^1 = 1/\sqrt{2} \cdot (1, 0, -1)^T, \ c^2 = (0, 1, 0)^T\}$ ist eine Orthonormalbasis von E_2. In dieser Basis haben die Projektionen von $(0, 1, 1)^T$ und $(0, 0, 2)^T$ die Koordinaten $(1/\sqrt{2}, 1)^T$ und $(-\sqrt{2}, 0)$. Damit ist $(1/\sqrt{2}, 1)^T$ ein kürzester Vektor $\neq 0$ in Λ / E_2. Dieser kommt von $(0, 1, 1)^T$ (auch $(1, 1, 0)^T$ ist möglich). Setze also $b^2 = (0, 1, 1)^T$. Dann gilt auch $\mu_{21} = 1/2$ und damit $g^2 = (-1/2, 1, 1/2)$.

$i = 3$: Es gilt $E_3 = L((1,1,-1)^T)$. Der Abstand zu $L(b^1, b^2)$ wird also durch das Skalarprodukt mit $(1,1,-1)^T$ gemessen. Wegen $x + y - z \equiv 0 \bmod 2$ ist dies mindestens 2. Man kann also z. B. $b^3 = (1,1,0)^T$ setzen (dies liefert $\mu_{31} = 1/2$ und $\mu_{32} = 1/3$).

3.4 LLL–Reduktion

Der Nachteil der Reduktionsverfahren von Minkowski und Korkine–Zolotarev ist, daß sie bisher nicht 'schnell' (d. h. in polynomialer Zeit) durchgeführt werden können. A. K. Lenstra, H. W. Lenstra und L. Lovász (LLL) haben den Begriff der Korkine–Zolotarev–reduzierten Basis so modifiziert, daß eine reduzierte Basis 'schnell' zu finden ist.

Definition 3.8 *Sei Λ ein Gitter, $\{b^1, \ldots, b^n\}$ eine Basis von Λ und g^j, μ_{ji} wie in (3.1). $\{b^1, \ldots, b^n\}$ heißt* **LLL–reduziert***, falls gilt*

(i) $|\mu_{ji}| \leq 1/2$, *für* $1 \leq i < j \leq n$,

(ii) $|g^{j+1} + \mu_{j+1,j} \cdot g^j|^2 \geq \frac{3}{4} \cdot |g^j|^2$, *für* $j = 1, \ldots, n-1$.

Die Bedingung (i) ist die gleiche wie bei der Korkine–Zolotarev–Reduktion und gewährleistet, daß die Basis 'fast orthogonal' ist. Die seltsam wirkende Bedingung (ii) ist technisch bedingt und die Konstante 3/4 ist willkürlich gewählt. Sie besagt, daß sich beim Tausch von b^j und b^{j+1} die Länge von g^j nicht zu stark vermindert.

Satz 3.9 *Sei $\Lambda \subset \mathbb{R}^n$ ein Gitter und $\{b^1, \ldots, b^n\}$ eine LLL–reduzierte Basis und $g^1, \ldots, g^n$ wie in (3.1). Dann gilt*

(a) $|g^i|^2 \leq 2^{j-i} \cdot |g^j|^2$, *für* $i = 1, \ldots, j-1$,

(b) $|b^1| \leq 2^{(n-1)/4} \cdot d(\Lambda)^{1/n}$,

(c) $|b^1| \leq 2^{(n-1)/2} \cdot \lambda_1(\Lambda)$,

(d) $|b^1| \cdot \ldots \cdot |b^n| \leq 2^{n(n-1)/4} \cdot d(\Lambda)$.

Eine LLL–reduzierte Basis kann mit folgendem einfachen Verfahren bestimmt werden.

Algorithmus 3.10 (LLL–Reduktion)
Eingabe: Linear unabhängige Vektoren $a^1, \ldots, a^n \in \mathbb{Q}^n$.
Ausgabe: Eine LLL–reduzierte Basis.
begin
Setze $b^i := a^i$, für $i = 1, \ldots, n$.
ende := FALSE;
repeat
Bestimme $g^1, \ldots, g^n$ zu $b^1, \ldots, b^n$ mit zugehörigen μ_{ji};
for $j := 2$ **to** n **do**
for $i := j - 1$ **downto** 1 **do**
begin
$b^j := b^j - \lceil \mu_{ji} \rfloor \cdot b^i$; (* dabei sei $\lceil x \rfloor \in \mathbb{Z}$ mit $|x - \lceil x \rfloor| \leq 1/2$ *)
for $k := 1$ **to** $i - 1$ **do** $\mu_{jk} := \mu_{jk} - \lceil \mu_{ji} \rfloor \cdot \mu_{ik}$;
$\mu_{ji} := \mu_{ji} - \lceil \mu_{ji} \rfloor$;
end;
(* Hier ist die Bedingung (i) erfüllt *);
$j := 0$;
repeat
$j := j + 1$;
$w_1 := 3/4 \cdot |g^j|^2$;
$w_2 := |g^{j+1} + \mu_{j+1,j} \cdot g^j|^2$;
until $(w_1 > w_2)$ **or** $(j = n - 1)$;
if $w_1 \leq w_2$ **then** ende := TRUE
else vertausche b^j und b^{j+1};
until ende;
end.

Bemerkung: (1) In dem ersten Schritt (die beiden FOR–Schleifen) wird die Basis so geändert, daß die Bedingung (i) aus Definition 3.8 erfüllt ist. Man beginnt mit $i = j - 1$ und ersetzt b^j durch

$$b^j - \lceil \mu_{j,j-1} \rfloor \cdot b^{j-1} = g^j + (\mu_{j,j-1} - \lceil \mu_{j,j-1} \rfloor) \cdot g^{j-1} + \sum_{k=1}^{j-2} (\mu_{jk} - \lceil \mu_{j,j-1} \rfloor \cdot \mu_{j-1,k}) \cdot g^k$$

Nach der Änderung werden die μ_{jk} entsprechend modifiziert. Dann gilt $|\mu_{j,j-1}| \leq 1/2$ und dies bleibt auch bei den weiteren Operationen für $i = j - 2, \ldots, 1$ erhalten.

(2) In dem zweiten Schritt wird geprüft, ob die Bedingung (ii) aus Definition 3.8 erfüllt ist. Falls dies nicht zutrifft, werden zwei Vektoren getauscht und der erste Schritt wird wiederholt.

Satz 3.11 *Algorithmus 3.10 bestimmt nach endlich vielen Schritten eine LLL–reduzierte Basis.*

Bemerkung: (1) Eine Untersuchung der Komplexität von Algorithmus 3.10 zeigt, daß es sich um ein polynomiales Verfahren handelt. Insbesondere werden die Nenner der rationalen Zahlen im Laufe des Verfahrens nicht zu groß.

(2) Der technische Faktor 3/4 kann durch eine größere Zahl < 1 ersetzt werden. Dadurch verbessern sich die Schranken in Satz 3.9, aber die Laufzeit wird verlängert.

Mit dem LLL–Reduktionsverfahren können viele zahlentheoretische Probleme konstruktiv gelöst werden. Ein erstes Beispiel ist die folgende algorithmische Version von Satz 2.4.

Satz 3.12 *Seien $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}$ und $0 < \epsilon < 1$. Dann können (in polynomialer Zeit) $p_1, \ldots, p_n, q \in \mathbb{Z}$ bestimmt werden, so daß*

$$|q\alpha_i - p_i| \leq \epsilon, \ (i = 1, \ldots, n) \quad \textit{und} \quad 1 \leq q \leq 2^{n(n+1)/4} \cdot \epsilon^{-n}.$$

Satz 3.13 *Seien $\alpha_1, \ldots, \alpha_n \in \mathbb{Q}$ und $0 < \epsilon < 1$. Dann können (in polynomialer Zeit) $u_1, \ldots, u_{n+1} \in \mathbb{Z}$ mit $\max_{i=1,\ldots,n} |u_i| > 0$ bestimmt werden, so daß*

$$|u_1\alpha_1 + \ldots + u_n\alpha_n - u_{n+1}| \leq \epsilon \quad \textit{und} \quad |u_i| \leq 2^{(n+1)/4} \cdot \epsilon^{-1/n}.$$

Satz 3.9 liefert eine algorithmische Lösung des Problems des kürzesten Gittervektors (in abgeschwächter Form, d. h. bis auf einen Faktor). Die LLL–Reduktion liefert aber auch eine entsprechende Lösung des Problems des nähesten Gittrerpunktes.

Satz 3.14 *Sei $\Lambda \subset \mathbb{Q}^n$ ein Gitter und $b \in \mathbb{Q}^n$. Dann kann (in polynomialer Zeit) ein $u \in \Lambda$ bestimmt werden, so daß*

$$|b - u| \leq 2^{n/2} \cdot \min\{|b - v| \ : \ v \in \Lambda\}.$$

Bemerkung: (1) Das LLL–Reduktionsverfahren, besonders in der Form der Diophantischen Approximation, hat viele Anwendungen, z. B.

(a) Faktorisierung von Polynomen $f \in \mathbb{Q}[x]$ in irreduzible Faktoren,

(b) Widerlegung der sogenannten Mertens–Vermutung aus der Zahlentheorie,

(c) Brechen eines bestimmten (Rucksack–) Verfahrens (von Merkle–Hellman) in der Kryptographie.

(2) Das LLL–Verfahren kann verallgemeinert werden, indem die Euklidische Norm durch eine beliebige ersetzt wird. Es gilt dann eine analoge Aussage zu Satz 3.9. Ferner kann damit eine algorithmische Version des Satzes von Minkowski gegeben werden.

4 Die kritische Determinante

4.1 Der Auswahlsatz von Mahler

Sei $\mathcal{L}$ die Menge der Gitter im $\mathbb{R}^n$ (mit Determinante > 0). Um von einer konvergenten Folge von Gittern sprechen zu können, soll hier ein Maß für den Abstand zweier Gitter gegeben werden. Da Gitterbasen nicht eindeutig sind, kann man nicht einfach den 'Abstand' zweier Basen nehmen. Darum wird der folgende Umweg gegangen.

Für eine Matrix $B \in \mathbb{R}^{n\times n}$ sei $|B|_1 = \max_{1\le i\le n} \sum_{j=1}^{n} |b_{ij}|$ die Zeilensummennorm. Aus der linearen Algebra ist bekannt, daß es sich dabei um eine Matrixnorm handelt. Insbesondere gilt $|A \cdot B|_1 \le |A|_1 \cdot |B|_1$. Ferner ist $|\cdot|_1$ verträglich mit der Maximumnorm $|x|_{\max} = \max_{1\le i\le n} |x_i|$, d. h. für alle $x \in \mathbb{R}^n$ gilt $|Ax|_{\max} \le |A|_1 \cdot |x|_{\max}$.

Definition 4.1 *Seien $\Lambda_1, \Lambda_2 \in \mathcal{L}$ und $T(\Lambda_1, \Lambda_2) = \{Q \in \mathbb{R}^{n\times n} : \Lambda_1 = Q\Lambda_2\}$ die Menge der Matrizen, die Λ_2 in Λ_1 überführen. Ferner sei*

$$\gamma(\Lambda_1, \Lambda_2) = \inf \{|Q - I_n|_1 : Q \in T(\Lambda_1, \Lambda_2)\}.$$

Dann heißt

$$\delta(\Lambda_1, \Lambda_2) = \max \{ \log(1 + \gamma(\Lambda_1, \Lambda_2)),\ \log(1 + \gamma(\Lambda_2, \Lambda_1)) \}$$

der **Abstand** *der Gitter Λ_1 und Λ_2.*

Lemma 4.2 *In der obigen Definition kann ' $\inf$ ' durch ' $\min$ ' ersetzt werden.*

Satz 4.3 *Die Abbildung $\delta : \mathcal{L} \times \mathcal{L} \to \mathbb{R}$ ist eine Metrik auf dem Raum der Gitter.*

Somit ist ein Konvergenzbegriff auf der Menge der Gitter gegeben. Ferner sind in $\mathcal{L}$ Kompaktheit und Folgenkompaktheit äquivalent.

Die Konvergenz von Gittern kann durch die der Basen charakterisiert werden. Dabei konvergiert eine Folge von Matrizen A_r gegen eine Matrix A, wenn $|A - A_r|_1 \to 0$ $(r \to \infty)$ (oder bzgl. irgendeiner anderen Matrixnorm).

Satz 4.4 *Eine Folge von Gittern Λ_r konvergiert genau dann gegen Λ, wenn es zu jeder Basis A von Λ Basen A_r von Λ_r gibt mit $A_r \to A$.*

Bemerkung: Wie der Beweis zeigt, reicht es schon aus, daß es eine Basis A gibt, für die dies gilt.

Die Konvergenz von Gittern kann mit der der einzelnen Gitterpunkte in Verbindung gebracht werden.

Satz 4.5 *Sei $\Lambda_r \to \Lambda$. Dann gilt*

(a) Zu jedem $x \in \Lambda$ existiert eine Folge $\{x^r\}$, $x^r \in \Lambda_r$, mit $x^r \to x$.

(b) Ist $\{x^r\}$, $x^r \in \Lambda_r$, eine Folge mit $x^r \to x$, so gilt $x \in \Lambda$.

Bemerkung: Die Umkehrung gilt nicht: Aus (a), (b) folgt noch nicht die Konvergenz von $\{\Lambda_r\}$ (Übung). Die Konvergenz folgt, falls jeder Häufungspunkt von $\{x^r\}$ in Λ liegt (Beweis siehe GL, S. 179).

Eine Menge von Gittern kann in zweierlei Weise entarten. Sie kann eine Folge von Gittern enthalten, die 'immer dünner' wird oder eine Folge, deren Basen 'fast niederdimensional' sind. Um beides zu verhindern, wird der Begriff der beschränkten Menge eingeführt.

Definition 4.6 *Sei $\mathcal{M}$ eine Menge von Gittern. $\mathcal{M}$ heißt* **beschränkt**, *falls es $\varrho, \sigma > 0$ gibt, so daß*

(i) $\lambda_1(\Lambda) \geq \varrho$, für alle $\Lambda \in \mathcal{M}$,

(ii) $d(\Lambda) \leq \sigma$, für jedes $\Lambda \in \mathcal{M}$.

Äquivalente Definition: Es gibt $\eta, \xi > 0$ mit

(i) $d(\Lambda) \geq \xi$, für alle $\Lambda \in \mathcal{M}$,

(ii) Jedes $\Lambda \in \mathcal{M}$ hat eine Basis in $\eta \cdot B^n$.

Eine Aussage für Gitter analog zum Satz von Bolzano–Weierstraß ist der folgende Auswahlsatz von Mahler.

Satz 4.7 (Auswahlsatz von Mahler) *Eine beschränkte Folge von Gittern enthält stets eine konvergente Teilfolge.*

4.2 Sternkörper und kritische Determinanten

Definition 4.8 *Sei $M \subset \mathbb{R}^n$.*

(a) Das Gitter Λ heißt **zulässig für M** *oder* **M–zulässig**, *falls* $\operatorname{int}(M) \cap \Lambda \backslash \{0\} = \emptyset$.

(b) Λ heißt **strikt zulässig für M**, *falls $M \cap \Lambda \backslash \{0\} = \emptyset$.*

(c) Die **kritische Determinante** *$\Delta(M)$ von M ist definiert durch*

$$\Delta(M) = \inf\{d(\Lambda) \,:\, \Lambda \text{ ist strikt zulässig für } M\} \quad (\text{wobei } \inf \emptyset = \infty).$$

(d) M heißt vom **endlichen (unendlichen) Typ**, *wenn $\Delta(M) < \infty$ ($\Delta(M) = \infty$).*

Beispiel: Für $M = \mathbb{Q}^n$ ist jedes Gitter M–zulässig. Aber z .B. gilt sogar $Y \subset \mathbb{Q}^n$. Da $\sqrt{2}/r \cdot Y$ strikt zulässig ist für $r = 1, 2, \ldots$, gilt $\Delta(M) = 0$.

Definition 4.9 *$S \subset \mathbb{R}^n$ heißt* **Sternkörper**, *falls*

(i) $S \neq \emptyset$,

(ii) *Für* $x \in S$ *und* $0 \leq \lambda < 1$ *gilt* $\lambda x \in \text{int}\,(S)$,

(iii) S *ist abgeschlossen,*

(iv) S *ist zentralsymmetrisch.*

Weiter sei $\mathcal{S}^n = \{S \subset \mathbb{R}^n \,:\, S \text{ ist Sternkörper }\}$.

Bemerkung: (1) Jedes $K \in \mathcal{K}_0^n$ ist ein Sternkörper.

(2) Sternkörper müssen weder konvex noch beschränkt sein.

Beispiel: $S = \{x \in \mathbb{R}^n \,:\, |x_1 \cdot \ldots \cdot x_n| \leq 1\}$ ist ein Sternkörper.

Anschaulich ist die kritische Determinante von M die Determinante des kleinsten Gitters, das bis auf 0 zu $\text{int}\,(M)$ disjunkt ist.

Satz 4.10 *Für* $S \in \mathcal{S}^n$ *gilt* $\Delta(S) = \inf\{d(\Lambda) \,:\, \Lambda$ *ist zulässig für* $S\}$. *Ist* $\Delta(S) < \infty$, *so wird das Infimum angenommen.*

Beispiel: Im Allgemeinen gilt nicht $\Delta(M) = \inf\{d(\Lambda) \,:\, \Lambda \text{ ist zulässig für } M\}$. Setze z. B. $M = (B^n \cap \mathbb{Q}^n) \cup ((\mathbb{R}^n \cap B^n) \cap (\mathbb{R}^n \backslash \mathbb{Q}^n))$. Einerseits ist wegen $\text{int}\,(M) = \emptyset$ jedes Gitter zulässig für M. Andererseits gilt für jedes strikt zulässige Gitter $\lambda_1(\Lambda) \geq 1$ und damit $d(\Lambda) \geq \kappa_n/2^n$.

In Anbetracht von Satz 4.10 wird definiert

Definition 4.11 *Sei* $S \in \mathcal{S}^n$ *vom endlichen Typ. Das Gitter* Λ *heißt* **kritisch** *für* S, *falls* Λ *zulässig ist und* $d(\Lambda) = \Delta(S)$ *gilt.*

Nach Satz 4.10 existiert daher zu jedem $S \in \mathcal{S}^n$ vom endlichen Typ ein kritisches Gitter.

Beispiel: Für $W = \{x \in \mathbb{R}^n \,:\, |x_i| \leq 1/2\}$ ist Y ein kritisches Gitter. Denn einerseits ist Y zulässig for W. Andererseits gilt für jedes W–zulässige Gitter Λ nach Minkowski $2^n = V(W) \leq 2^n \cdot d(\Lambda)$, also $d(\Lambda) \geq 1 = d(Y)$.

Satz 4.12 *(a) Sei* $M \subset \mathbb{R}^n$ *mit* $\Delta(M) > 0$ *und* Λ *ein Gitter mit* $d(\Lambda) < \Delta(M)$. *Dann existiert ein* $x \in M \cap \Lambda \backslash \{0\}$.

(b) $M \subset M' \subset \mathbb{R}^n \;\Rightarrow\; \Delta(M) \leq \Delta(M')$.

(c) Sei A *eine nichtsinguläre lineare Transformation des* $\mathbb{R}^n$. *Dann gilt* $\Delta(AM) = |\det A| \cdot \Delta(M)$. *Insbesondere ist* $\Delta(\lambda M) = \lambda^n \cdot \Delta(M)$, *für* $\lambda > 0$.

Für $K \in \mathcal{K}_0^n$ mit kritischem Gitter Λ betrachte man $\operatorname{card}(K \cap \Lambda)$. Per Definition ist klar, daß es auf dem Rand mindestens n linear unabhängige Gitterpunkte gibt, da man sonst das Gitter in einer Richtung stauchen und so die Determinante verkleinern könnte. Es gilt aber sogar die folgende Verbesserung.

Satz 4.13 (Swinnerton–Dyer(1953)) *Sei $K \in \mathcal{K}_0^n$ und Λ ein kritisches Gitter von K. Dann gilt*

$$\operatorname{card}\{\Lambda \cap K\} \geq n(n+1)+1.$$

Für $K \in \mathcal{K}_0^n$ ist nach Satz 2.22 kein Gitter Λ mit $d(\Lambda) < 2^{-n}V(K)$ (strikt) zulässig. Also

Satz 4.14 *Für $K \in \mathcal{K}_0^n$ gilt* $\Delta(K) \geq \dfrac{V(K)}{2^n}$.

Bemerkung: Wie das Beispiel des Würfels zeigt, kann Satz 4.14 nicht verbessert werden.

Ist S ein Sternkörper, so existiert ein $\epsilon > 0$ mit $\epsilon \cdot B^n \subset S$. Nach Satz 4.12 und Satz 4.14 folgt $\Delta(S) \geq \Delta(\epsilon \cdot B^n) \geq V(\epsilon \cdot B^n)/2^n$ und darum $\Delta(S) > 0$.

Für beliebige Mengen ermöglicht der Satz 2.1 (von Blichfeldt) eine entsprechende Aussage für die 'Differenzenmenge'.

Satz 4.15 *Sei M meßbar und abgeschlossen. Dann gilt $V(M) \leq \Delta(M-M)$.*

4.3 Der Satz von Minkowski–Hlawka

Nach Satz 4.14 kann für $K \in \mathcal{K}_0^n$ die kritische Determinante im Vergleich zu $V(K)$ nicht zu klein werden. Andererseits kann sie aber auch nicht zu groß werden, d. h. mit vorgegebenem Volumen V kann man nicht alle Gitter Λ mit $d(\Lambda) = V$ 'einfangen'.

Satz 4.16 (Minkowski–Hlawka) *Sei $M \subset \mathbb{R}^n$ beschränkt und meßbar. Dann gilt $\Delta(M) \leq V(M)$.*

Für Sternkörper kann die Bedingung der Beschränktheit entfallen.

Korollar 4.17 *Für Sternkörper S gilt* $\Delta(S) \leq V(S)$.

Bemerkung: (1) Der Beweis des Satzes von Minkowski–Hlawka zeigt nur die Existenz eines zulässigen Gitters mit kleiner Determinante.

(2) Es gibt viele verschiedene Beweise und Verschärfungen des Satzes von Minkowski–Hlawka. Die beste stammt von Schmidt: $\Delta(M) \leq (\alpha_n \cdot n)^{-1} \cdot V(M)$ mit $\alpha_n \to \log\sqrt{2}$.

4.4 Die Überdeckungskonstante

Definition 4.18 *Ein Gitter Λ heißt ein* **Packungsgitter** *von einem konvexen Körper K, wenn $K + \Lambda$ eine Packung ist.*

Satz 4.19 *Λ ist genau dann ein Packungsgitter von $K \in \mathcal{K}^n$ ($K \in \mathcal{K}_0^n$), wenn Λ für $K - K$ (bzw. $2K$) zulässig ist.*

Eine unmittelbare Konsequenz ist die folgende Interpretation der kritischen Determinante eines konvexen Körpers $K \in \mathcal{K}_0^n$:

$$\Delta(K) = \inf \{d(\Lambda) : \Lambda \text{ Packungsgitter von } 1/2 \cdot K\}.$$

Ersetzt man 'Packung–' durch 'Überdeckung–', so erhält man eine –in einem gewissen Sinne– duale Theorie.

Definition 4.20 *Sei $M \subset \mathbb{R}^n$.*

(a) Das Gitter Λ heißt **Überdeckungsgitter** *von M, falls $M + \Lambda = \mathbb{R}^n$.*

(b) Die **Überdeckungskonstante** *$\Gamma(M)$ ist gegeben durch*

$$\Gamma(M) = \sup \{d(\Lambda) : \Lambda \text{ ist Überdeckungsgitter von } M\}.$$

Falls kein Überdeckungsgitter existiert, setzt man $\Gamma(M) = 0$.

(c) Ist Λ ein Überdeckungsgitter mit $d(\Lambda) = \Gamma(M)$, so heißt Λ **maximales Überdeckungsgitter** *von M.*

Satz 4.21 *(a) Sei $M \subset \mathbb{R}^n$ mit $\Gamma(M) < \infty$ und Λ ein Gitter mit $d(\Lambda) > \Gamma(M)$. Dann existiert ein $x \in \mathbb{R}^n$ mit $x \notin \Lambda + M$.*

(b) $M \subset M' \subset \mathbb{R}^n \Rightarrow \Gamma(M) \leq \Gamma(M')$.

(c) Sei A eine nichtsinguläre lineare Transformation des $\mathbb{R}^n$. Dann gilt $\Gamma(AM) = |\det A| \cdot \Gamma(M)$. Insbesondere ist $\Gamma(\lambda M) = \lambda^n \cdot \Gamma(M)$, für $\lambda > 0$.

(d) Für $\operatorname{int}(M) \neq \emptyset$ gilt $\Gamma(M) > 0$,

(e) Für $t \in \mathbb{R}^n$ gilt $\Gamma(t + M) = \Gamma(M)$.

Der folgende Satz ist analog zu Satz 4.15.

Satz 4.22 *Für meßbares $M \subset \mathbb{R}^n$ gilt $\Gamma(M) \leq V(M)$.*

Beispiel: Für $W = \{x \in \mathbb{R}^n : |x_i| \leq 1/2\}$ gilt $\Gamma(W) = V(W) = 1$ und Y ist ein maximales Überdeckungsgitter.

Satz 4.23 *Ist M kompakt und $0 \in \operatorname{int}(M)$, so hat M ein maximales Überdeckungsgitter.*

Bemerkung: Es gibt abgeschlossene Mengen M, die kein maximales Überdeckungsgitter haben (Übung).

Für Sternkörper kann man die Distanzfunktion definieren wie in Definition 1.13. Im Fall beschränkter Sternkörper läßt sich das inhomogene Minimum mit Hilfe der Distanzfunktion ausdrücken.

Satz 4.24 *Sei $S \in S^n$ beschränkt mit Distanzfunktion f und Λ ein Gitter. Dann existiert für jedes $z \in \mathbb{R}^n$ das Minimum* $\min\{f(z-x) : x \in \Lambda\}$. *Die Funktion $\psi = \psi_\Lambda : \mathbb{R}^n \to \mathbb{R}$ definiert durch $\psi(z) = \min\{f(z-x) : x \in \Lambda\}$ ist stetig und periodisch modulo Λ. Ferner gilt*

$$\mu(S, \Lambda) = \max_{z \in \mathbb{R}^n} \psi(z) = \max_{z \in \mathbb{R}^n} \min_{x \in \Lambda} f(z-x).$$

5 Packungen und Überdeckungen

5.1 Die Packungsdichte

Ist $K \subset \mathbb{R}^n$ eine meßbare beschränkte Menge, so nennt man ein System von Translaten $\mathcal{K} = \{K + t^i : i \in \mathbb{N}\}$ eine Packung, wenn sich die verschiedenen Translate nicht überlappen, d. h. disjunktes Inneres haben. Im folgenden soll eine 'Dichte' von Packungen eingeführt werden. Anschaulich ist die Dichte einer Packung die Wahrscheinlichkeit ($\in [0,1]$) einen 'günstigen' Punkt zu treffen. Man betrachtet zunächst beschränkte Ausschnitte und bestimmt das Verhältnis von günstigem Bereich zu gesamten Bereich und läßt diesen Ausschnitt dann immer größer werden.

Definition 5.1 *Sei $K \subset \mathbb{R}^n$ meßbar und beschränkt und $\mathcal{K} = \{K + t^i : i \in \mathbb{N}\}$ eine Menge von Translaten von K. Ferner sei W ein achsenparalleler Würfel mit Kantenlänge s. Dann sei*

(a) $\varrho_+(\mathcal{K}, W) = \dfrac{1}{V(W)} \cdot \displaystyle\sum_{(K+t^i)\cap W \neq \emptyset} V(K + t^i),$

(b) $\varrho_-(\mathcal{K}, W) = \dfrac{1}{V(W)} \cdot \displaystyle\sum_{(K+t^i)\subset W} V(K + t^i),$

(c) $\varrho_+(\mathcal{K}) = \limsup\limits_{s(W)\to\infty} \varrho_+(\mathcal{K}, W)$ *die* **obere Dichte** *für $\mathcal{K}$,*

(d) $\varrho_-(\mathcal{K}) = \liminf\limits_{s(W)\to\infty} \varrho_-(\mathcal{K}, W)$ *die* **untere Dichte** *für $\mathcal{K}$.*

Bemerkung: (1) Zieht man die Analogie zum Integral, so entspricht ϱ_+ einer Obersumme und ϱ_- einer Untersumme.

(2) Offensichtlich gilt $\varrho_-(\mathcal{K}) \leq \varrho_+(\mathcal{K})$.

(3) $\varrho_+(\mathcal{K})$ und $\varrho_-(\mathcal{K})$ sind auch definiert, wenn $\mathcal{K}$ keine Packung ist. In diesem Fall kann die (obere oder untere) Dichte als 'Erwartungswert' für die Anzahl der Translate, die man trifft, interpretiert werden.

(4) Statt eines Würfels kann man auch einen anderen konvexen Körper benutzen. Man kann aber zeigen, daß dabei die gleichen Dichten herauskommen.

Für Packungen ist die folgende Ungleichung anschaulich klar.

Satz 5.2 *Sei $K \subset \mathbb{R}^n$ meßbar und beschränkt und $\mathcal{K}$ eine Packung, dann gilt $\varrho_+(\mathcal{K}) \leq 1$.*

Definition 5.3 *Die* **Packungsdichte** $\delta(K)$ *einer meßbaren beschränkten Menge* $K \subset \mathbb{R}^n$ *ist definiert als*

$$\delta(K) = \sup_{\mathcal{K}} \varrho_+(\mathcal{K}),$$

wobei das Supremum über alle Packungen für K *genommen wird.*

Von besonderem Interesse sind die folgenden speziellen Typen von Packungen.

Definition 5.4 *Sei* $K \subset \mathbb{R}^n$ *beschränkt und meßbare Menge und* $\mathcal{K} = T + K$*, mit* $T = \{t^1, t^2, \ldots\}$*, eine Packung.*

(a) $\mathcal{K} = \mathcal{K}_\Lambda$ *heißt eine* **Gitterpackung***, falls* $T = \Lambda$ *ein Gitter ist. Man definiert die* **Gitterpackungsdichte** *durch* $\delta_L(K) = \sup_{\mathcal{K}_\Lambda} \varrho_+(\mathcal{K}_\Lambda)$.

(b) $\mathcal{K} = \mathcal{K}_P$ *heißt eine* **periodische Packung***, falls* $T = P = \{t^1, \ldots, t^N\} + s \cdot \mathbb{Z}^n$ *periodisch ist. Man definiert die* **periodische Packungsdichte** *durch* $\delta_P(K) = \sup_{\mathcal{K}_P} \varrho_+(\mathcal{K}_P)$.

Bemerkung: (1) Auch Packungen mit $T = \{t^1, \ldots, t^N\} + \Lambda$, Λ Gitter, werden periodisch genannt. Diese können aber durch eine lineare Abbildung auf die Form in Definition 5.4 gebracht werden.
(2) Offensichtlich gilt $\delta_L(K) \le \delta_P(K) \le \delta(K) \le 1$.

(3) Bis heute ist kein K bekannt mit $\delta_L(K) < \delta(K)$.

Satz 5.5 *Sei* $K \subset \mathbb{R}^n$ *beschränkt und meßbar und* A *eine nichtsinguläre affine Transformation. Ferner sei* $\mathcal{K}_P = K + \{t^1, \ldots, t^N\} + s \cdot \mathbb{Z}^n$ *und* W *ein Würfel mit Kantenlänge* $s(W) = s$*. Dann gilt*

$$\varrho_+(A\mathcal{K}_P) = \varrho_-(A\mathcal{K}_P) = \varrho_+(\mathcal{K}_P) = \varrho_-(\mathcal{K}_P) = \frac{N \cdot V(K)}{V(W)}.$$

Bemerkung: Für beliebige Packungen gilt i. a. nicht $\varrho_+(\mathcal{K}) = \varrho_-(\mathcal{K})$. Für den Einheitswürfel W betrachte man die folgende Packung. Man startet mit W. Dann wird die Kantenlänge verdoppelt und es werden soviele Exemplare von W eingefügt, daß die Dichte $1/2$ beträgt. Dann wird wieder die Kantenlänge verdoppelt und soviele Exemplare von W eingefügt, daß die Dichte $1/4$ ist, dann wieder mit $1/2, 1/4, \ldots$. Dann gilt offensichtlich $\varrho_+ \ge 1/2$ aber $\varrho_- \le 1/4$.

Beispiel: Sei $\Lambda \subset \mathbb{R}^3$ ein Gitter mit Basis $\{(3,0,3)^T, (3,3,0)^T, (-4,4,4)^T\}$ und $P = \Lambda \cup (\Lambda + (0,3,3)^T)$. Dann ist $\mathcal{P} = P + \frac{3\sqrt{2}}{2} \cdot B^3$ eine periodische Packung mit Dichte $\pi/(3\sqrt{2})$ (Übung).

Für den Spezialfall $N = 1$ erhält man sofort die Dichte einer Gitterpackung.

Satz 5.6 *Sei $K \subset \mathbb{R}^n$ beschränkt und meßbar und $\mathcal{K}_\Lambda = K + \Lambda$ eine Gitterpackung. Dann gilt*

$$\varrho_+(\mathcal{K}_\Lambda) = \varrho_-(\mathcal{K}_\Lambda) = \frac{V(K)}{d(\Lambda)}.$$

Bemerkung: Die Dichte kann auch betrachtet werden als Quotient des Volumens des in einer (repräsentativen) Zelle enthaltenen günstigen Bereiches zu dem Volumen dieser Zelle. In dieser Zelle ist aber K (in Bruchstücken) genau einmal enthalten.

Im folgenden sollen Packungen konvexer Körper betrachtet werden. Für diese gilt:

(1) Nach Satz 4.19 wird die Dichte einer Gitterpackung maximal, wenn Λ kritisches Gitter von $K - K$ ist, d. h. die Suche nach einer dichtesten Packung ist äquivalent zur Bestimmung eines kritischen Gitters.
(2) Da Λ ein Packungsgitter für K ist, genau dann, wenn dies für $1/2 \cdot (K - K)$ zutrifft, reicht es, symmetrische K zu betrachten.

Satz 5.7 *Für $K \in \mathcal{K}_0^n$ gilt* $\delta_L(K) = \dfrac{V(K)}{\Delta(2K)} = \dfrac{V(K)}{2^n \cdot \Delta(K)}$.

Bemerkung: Für beliebige $K \in \mathcal{K}^n$ gilt $\delta_L(K) = \dfrac{V(K)}{\Delta(K - K)}$.

Aus Satz 5.7 folgt eine gewisse Verschärfung des Satzes von Minkowski.

Satz 5.8 *Ist Y zulässig für $K \in \mathcal{K}_0^n$, dann gilt $V(K) \leq 2^n \cdot \delta_L(K)$.*

Eine untere Schranke für $\delta(K)$ (die leider nicht konstruktiv ist) gibt der Satz von Minkowski–Hlawka.

Satz 5.9 *Für $K \in \mathcal{K}_0^n$ gilt* $\delta_L(K) \geq \dfrac{1}{2^n}$.

Die Packungsdichten sind affin invariant. Ferner ist die Packungsdichte gleich der periodische Packungsdichte.

Satz 5.10 *Sei $K \subset \mathbb{R}^n$ beschränkt und meßbar und A eine nichtsinguläre affine Transformation. Dann gilt*

$$\delta(AK) = \delta_P(K) = \delta(K), \qquad \delta_L(AK) = \delta_L(K).$$

5.2 Die Überdeckungsdichte

Für eine meßbare beschränkte Menge $K \subset \mathbb{R}^n$ wird $\mathcal{K} = \{K + t^i : i \in \mathbb{N}\}$ eine Überdeckung genannt, wenn jedes $x \in \mathbb{R}^n$ in einem Translat $K + t^i$ liegt. Für Überdeckungen läßt sich eine analoge Theorie wie für die Packungen des vorigen Abschnitts entwickeln.

Satz 5.11 *Sei $K \subset \mathbb{R}^n$ beschränkt und meßbar und $\mathcal{K}$ eine Überdeckung, dann gilt $\varrho_-(\mathcal{K}) \geq 1$.*

Definition 5.12 *Die* **Überdeckungsdichte** $\vartheta(K)$ *einer meßbaren und beschränkten Menge $K \subset \mathbb{R}^n$ ist definiert als*

$$\vartheta(K) = \inf_{\mathcal{K}} \varrho_-(\mathcal{K}),$$

wobei das Infimum über alle Überdeckungen für K genommen wird.

Definition 5.13 *Sei $K \subset \mathbb{R}^n$ beschränkt und meßbar und $\mathcal{K} = T + K$, mit $T = \{t^1, t^2, \ldots\}$, eine Überdeckung.*

(a) $\mathcal{K} = \mathcal{K}_\Lambda$ heißt eine **Gitterüberdeckung**, *falls $T = \Lambda$ ein Gitter ist. Man definiert die* **Gitterüberdeckungsdichte** *durch $\vartheta_L(K) = \inf_{\mathcal{K}_\Lambda} \varrho_-(\mathcal{K}_\Lambda)$.*

(b) $\mathcal{K} = \mathcal{K}_P$ heißt eine **periodische Überdeckung**, *falls $T = P = \{t^1, \ldots, t^N\} + s \cdot \mathbb{Z}^n$ periodisch ist. Man definiert die* **periodische Überdeckungsdichte** *durch $\vartheta_P(K) = \inf_{\mathcal{K}_P} \varrho_-(\mathcal{K}_P)$.*

Bemerkung: Offensichtlich gilt $\vartheta_L(K) \geq \vartheta_P(K) \geq \vartheta(K) \geq 1$. Zum Beispiel für Extremalkörper gilt überall Gleichheit.

Satz 5.14 *Sei $K \subset \mathbb{R}^n$ beschränkt und meßbar und A eine nichtsinguläre affine Transformation. Dann gilt*

$$\vartheta(AK) = \vartheta_P(K) = \vartheta(K), \qquad \vartheta_L(AK) = \vartheta_L(K).$$

Satz 5.15 *Sei $\mathcal{K}_\Lambda = K + \Lambda$ eine Gitterüberdeckung. Dann gilt*

$$\varrho_+(\mathcal{K}_\Lambda) = \varrho_-(\mathcal{K}_\Lambda) = \frac{V(K)}{d(\Lambda)}.$$

Die Überdeckungsdichte wird minimal, wenn die Determinante maximal ist.

Satz 5.16 *Für eine meßbare beschränkte Menge $K \subset \mathbb{R}^n$ gilt* $\vartheta_L(K) = \dfrac{V(K)}{\Gamma(K)}$.

Für konvexe Körper K sind $\delta_L(K)$ und $\vartheta_L(K)$ nicht unabhängig voneinander.
Für jedes K–kritische Gitter Λ_0 gilt $\lambda_1(K, \Lambda_0) = \ldots = \lambda_n(K, \Lambda_0) = 1$. Nach Satz 2.24 folgt $\mu(K, \Lambda_0) \leq n/2$. Also ist $\Lambda_0 + n/2 \cdot K$ eine Überdeckung und damit $\Gamma(K) \geq d(2/n \cdot \Lambda_0) = (2/n)^n \cdot \Delta(K)$. Mit Satz 5.7 folgt

$$\vartheta_L(K) = \frac{V(K)}{\Gamma(K)} \leq n^n \frac{V(K)}{2^n \Delta(K)} = n^n \cdot \delta_L(K).$$

Die Abschätzung von μ für kritische Gitter läßt sich wesentlich verbessern.

Satz 5.17 *Für $K \in \mathcal{K}_0^n$ gilt* $\vartheta_L(K) \leq 3^{n-1} \delta_L(K)$.

Wegen $\delta_L(K) \leq 1$ folgt sofort

Korollar 5.18 *Für $K \in \mathcal{K}_0^n$ gilt $\vartheta_L(K) \leq 3^{n-1}$.*

Für Überdeckungen durch Translate kann die Ungleichung noch verbessert werden.

Satz 5.19 *Für $K \in \mathcal{K}_0^n$ gilt* $\vartheta(K) \leq 2^n \cdot \delta(K)$.

Bemerkung: Eine bessere Schranke als die in dem Korollar stammt von Rogers:

$$\vartheta(K) \leq \vartheta_L(K) \leq n^{\log_2 \log n + O(1)} \text{ für } n \to \infty$$

($\log_2$ Logarithmus zur Basis 2).

5.3 Packungen und Überdeckungen in der Ebene

In diesem Abschnitt sei stets $K \in \mathcal{K}_0^2$. Das folgende Lemma gibt eine Konstruktionsmöglichkeit für zulässige Gitter.

Lemma 5.20 *Seien $x^1, x^2, x^3 \in \operatorname{bd} K$ mit $x^3 = x^2 - x^1$. Dann ist das von x^1, x^2 erzeugte Gitter K–zulässig.*

Für ein kritisches Gitter ist diese Bedingung auch notwendig.

Lemma 5.21 *Sei Λ_0 ein kritisches Gitter von K. Dann existieren $x^1, x^2, x^3 \in \operatorname{bd} K$ mit $x^3 = x^2 - x^1$ und $\{x^1, x^2\}$ ist eine Basis von Λ_0.*

Definition 5.22 *Sei $K \in \mathcal{K}^n$ ein konvexer Körper.*

(a) Man nennt ein Polytop P dem konvexen Körper K **einbeschrieben***, wenn alle Ecken von P im Rand von K liegen (insbesondere gilt $P \subset K$).*

(b) Man nennt ein Polytop P dem konvexen Körper K **umbeschrieben***, wenn P der Durchschnitt von endlich vielen Stützhyperebenen an K ist (insbesondere gilt $K \subset P$).*

Definition 5.23 *Ein Sechseck $P = \operatorname{conv}\{\pm x^1, \pm x^2, \pm x^3\}$ heißt* **affin regulär***, wenn es eine lineare Abbildung A gibt, so daß AP ein reguläres Sechseck ist.*

Bemerkung: Sei $P = \operatorname{conv}\{x^1, \ldots, x^6\}$ ein Sechseck, $x^7 = x^1$, $x^8 = x^2$ und x^i, x^{i+1}, $i = 1, \ldots, 6$, seien benachbarte Ecken. Dann ist P genau dann affin regulär, wenn $x^{i+2} = x^{i+1} - x^i$, für $i = 1, \ldots, 6$.

Satz 5.24 *Unter den affin regulären und K einbeschriebenen Sechsecken existiert eines mit minimaler Fläche $\alpha(K)$ und es gilt $\Delta(K) = \alpha(K)/3$.*

Lemma 5.25 *Für jedes 0–symmetrische Sechseck P gibt es ein Gitter Λ, so daß $P + \Lambda$ eine Pflasterung der Ebene ist.*

Satz 5.26 *Es existiert ein K umbeschriebenes 0–symmetrisches Sechseck mit minimaler Fläche $\beta(K)$ und $\Delta(K) = \beta(K)/4$.*

Satz 5.27 *(a)* $\delta_L(K) = \dfrac{3}{4} \cdot \dfrac{V(K)}{\alpha(K)} = \dfrac{V(K)}{\beta(K)}$,

(b) $\delta_L(K) \geq \dfrac{3}{4}$,

(c) $\delta_L(B^2) = \dfrac{\pi}{2\sqrt{3}}$.

Bemerkung: (1) Man kann zeigen, daß sogar $\delta_L(K) > \sqrt{3}/2$ gilt.

(2) Es gibt konvexe Körper, die eine dünnere Packung als der Kreis liefern.

Lemma 5.28 *Sei Λ ein Überdeckungsgitter von K. Dann existiert ein (möglicherweise entartetes) 0–symmetrisches Sechseck $P \subset K$, so daß $P + \Lambda$ eine Pflasterung bildet.*

Satz 5.29 *K enthält ein 0–symmetrisches konvexes Sechseck (evtl. Viereck) P mit maximaler Fläche $\gamma(K)$ und es gilt $\Gamma(K) = \gamma(K)$.*

Satz 5.30 *(a)* $\vartheta_L(K) = \dfrac{V(K)}{\gamma(K)}$,

(b) $\vartheta_L(B^2) = \dfrac{2\pi}{3\sqrt{3}}$.

Bemerkung: Man kann folgende Aussagen zeigen:

(1) $\vartheta_L(K) \leq 2\pi/(3\sqrt{3})$ und Gleichheit gilt genau für Ellipsen.

(2) Für alle $K \in \mathcal{K}_0^2$ gilt $\delta_L(K) = \delta(K)$ und $\vartheta_L(K) = \vartheta(K)$.

5.4 Kugelpackungen

Für konkrete Körper $K \in \mathcal{K}_0^n$ kann man nach Abschätzungen von $\delta_L(K)$ bzw. $\delta(K)$ nach oben fragen. Von besonderem Interesse ist dabei die Einheitskugel B^n. Der Satz von Minkowski–Hlawka (vgl. Satz 5.9) lieferte bereits 2^{-n} als untere Schranke für die maximale Dichte einer Kugelpackung. Hier soll nun eine obere Schranke bestimmt werden. Der Ansatz hierfür ist es, keine 'harten' Kugeln zu betrachten, sondern 'weiche', die im Raum 'verschmiert' sind und sich überlappen können. Dabei soll aber die Summe der Dichten durch 1 beschränkt sein.

Definition 5.31 *Eine Funktion $\delta : \mathbb{R}_+ \to \mathbb{R}_+$ mit δ stetig, $\delta \geq 0$ und $\delta(t) = 0$, für $t > t_0$ mit passendem t_0 heißt* **Dichtefunktion**.

Satz 5.32 (Blichfeldt(1929)) *Sei δ eine Dichtefunktion. Weiter gelte für jede Packung $\{B^n + x^r\}_{r=1}^{\infty}$*

$$\sum_{r=1}^{\infty} \delta(|x - x^r|) \leq 1, \quad \text{für alle } x \in \mathbb{R}^n. \tag{5.1}$$

Dann gilt $\delta(B^n) \leq I^{-1}$ mit

$$I = n \cdot \int_0^{t_0} t^{n-1} \cdot \delta(t)\, dt.$$

Hier soll die Dichtefunktion $\delta(t) = \max\{0, 1 - t^2/2\}$, für $t \geq 0$, benutzt werden. Zum Nachweis von (5.1) dient die folgende Hilfsaussage.

Lemma 5.33 *Sei $m \in \mathbb{N}$ und $x, x^1, \ldots, x^m \in \mathbb{R}^n$. Dann gilt*

$$\sum_{j,k=1}^{m} |x^j - x^k|^2 \leq 2m \sum_{j=1}^{m} |x - x^j|^2.$$

Satz 5.34 (Blichfeldt(1930)) $\delta_L(B^n) \leq \delta(B^n) \leq \dfrac{n+2}{2} \cdot \dfrac{1}{2^{n/2}}$.

Satz 5.35 (Gauß(1831)) $\Delta(B^3) = 2^{-1/2}$ *und* $\delta_L(B^3) = \dfrac{\pi}{3\sqrt{2}}$.

Bemerkung: (1) Die Frage, ob $\delta(B^3) = \delta_L(B^3)$ gilt, ist die Kepler–Vermutung (1611). Sie ist erst kürzlich unter intensiver Ausnutzung von Computern bewiesen worden.

(2) Auch für $n = 4, \ldots, 8$ ist $\delta_L(B^n)$ bekannt.

n	κ_n	$\Delta(B^n)$	$\delta_L(B^n)$
2	$\pi = 3.1415\ldots$	$\frac{\sqrt{3}}{2}$	$\frac{\pi}{2\sqrt{3}} = 0.9069\ldots$
3	$\frac{4\pi}{3} = 4.1887\ldots$	$\frac{\sqrt{2}}{2}$	$\frac{\pi}{3\sqrt{2}} = 0.7404\ldots$
4	$\frac{\pi^2}{2} = 4.9348\ldots$	$\frac{1}{2}$	$\frac{\pi^2}{16} = 0.6168\ldots$
5	$\frac{8\pi^2}{15} = 5.2637\ldots$	$\frac{\sqrt{2}}{4}$	$\frac{\pi^2}{30}\sqrt{2} = 0.4652\ldots$
6	$\frac{\pi^3}{6} = 5.1677\ldots$	$\frac{\sqrt{3}}{8}$	$\frac{\pi^3}{144}\sqrt{3} = 0.3729\ldots$
7	$\frac{16\pi^3}{105} = 4.7247\ldots$	$\frac{1}{8}$	$\frac{\pi^3}{105} = 0.2952\ldots$
8	$\frac{\pi^4}{24} = 4.0587\ldots$	$\frac{1}{16}$	$\frac{\pi^4}{384} = 0.2536\ldots$

5.5 Kugelpackungen und Codierungstheorie

Bei der Übertragung von Daten (etwa über Telefonleitungen, Glasfaserkabel oder Funkverbindungen) oder beim Speichern von Daten (z. B. Disketten, Compact Discs, etc.) können Fehler auftreten. Man kann dieses Problem lösen, indem eine künstliche Redundanz eingebaut wird. Den Daten wird eine Struktur gegeben, so daß trotz einer gewissen Anzahl von Übertragungsfehlern die ursprüngliche Nachricht rekonstruiert werden kann. Man vergleiche die Redundanz in der Sprache. Trotz einiger Druckfehler kann man meist erkennen, welches Wort gemeint sein mußte.

Definition 5.36 *Sei X eine endliche Menge. Dann wird eine Teilmenge $C \subset X^n$ mit M Elementen ein* $(\mathbf{n}, \mathbf{M})$**–Code** *genannt. Die Elemente von C werden* **Codewörter** *genannt.*

Der Abstand von zwei sogenannten Codewörtern $x, y \in C$ kann durch die Anzahl der Koordinaten gemessen werden, in denen sie sich unterscheiden.

Definition 5.37 *Sei X eine endliche Menge. Der* **Hamming–Abstand** *auf X^n ist definiert durch*

$$d(x, y) = d((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = \text{ card } \{i : x_i \neq y_i\}.$$

Bemerkung: Der Hamming–Abstand ist eine Metrik auf X^n.

Im allgemeinen wählt man als Menge $X = \mathbb{F}$ einen endlichen Körper. Damit kann man dem Code C eine algebraische Struktur geben. Im folgenden betrachten wir nur **binäre Codes**, d. h. $X = \mathbb{F}_2$ ist der Körper mit den zwei Elementen 0 und 1.

Beispiel: $X = \{0, 1\}$, $n = 3$ und $C = \{000, 111\}$. Es wird 0 als 000 und 1 als 111 codiert. Geschieht bei der Übertragung ein Fehler, so kann man diesen erkennen und sogar korrigieren. Wird z. B. 111 gesendet und 101 empfangen, so **decodiert** man zu dem häufiger vorkommenden Symbol, also zu 1.

Natürlich geht die gewonnene Sicherheit zu Lasten der Datenmenge. Gesucht sind also möglichst effiziente Codes, die eine hohes Maß an Sicherheit gewährleisten und nicht zu redundant sind (wegen der Übertragungszeit und –energie).

Definition 5.38 *Sei X eine endliche Menge. Ein* $(\mathbf{n}, \mathbf{M}, \mathbf{d})$**–Code** *auf X ist eine M–elementige Teilmenge C von X^n, für die*

$$d(x, y) \geq d, \text{ für alle } x, y \in C \text{ mit } x \neq y$$

gilt und für die es auch $x, y \in C$ gibt mit $d(x, y) = d$. Die Zahl d heißt der **Minimalabstand** *von C.*

Bemerkung: (1) In obigem Beispiel ist $d = 3$.

(2) Sind bei der Übertragung $t < d/2$ Fehler aufgetreten, so kann man die Ausgangsnachricht fehlerfrei rekonstruieren (decodieren). Man nennt einen (n, M, d)–Code mit $d = 2e+1$ darum auch einen **e–fehlerkorrigierenden Code**.

Definition 5.39 *Ein (binärer) (n, M, d)–Code C heißt* **linear**, *wenn C ein Unterraum des Vektorraumes $\mathbb{F}_2^n = \{0, 1\}^n$ ist.*

Es gilt dann $M = 2^k$, für ein k (die Dimension des Unterraumes) und wir bezeichnen einen solchen Code als $[n, k, d]$–Code (die eckigen Klammern deuten einen linearen Code an).
Für lineare Codes ist die Bestimmung von d besonders einfach. Dazu definieren wir

Definition 5.40 *Es sei $x \in \mathbb{F}_2^n$. Das* **Gewicht** *$w(x)$ ist die Anzahl der Koordinaten ungleich 0 von x. Das* **Minimalgewicht** *von C ist*

$$\min\{w(c) \,:\, c \in C \backslash \{0\}\}.$$

Lemma 5.41 *(a) Für $x, y \in \mathbb{F}_2^n$ gilt $d(x, y) = w(x - y)$,*

(b) Für einen linearen Code ist der Minimalabstand gleich dem Minimalgewicht.

Definition 5.42 *Sei C ein (binärer) $[n, k, d]$–Code. Wenn $a_1, \ldots, a_r$ ein Erzeugendensystem von C bilden, so heißt die Matrix mit den Spalten $a_1, \ldots, a_r$ eine* **Generatormatrix** *für C.*

Der Code läßt sich auf offensichtliche Weise durch eine Generatormatrix G darstellen:

$$C = \{G \cdot x : x \in \mathbb{F}_2^r\}.$$

Beispiel: Sei $C \subset \mathbb{F}_2^7$ der von

$$(1,0,0,0,0,1,1)^T,\ (0,1,0,0,1,0,1)^T,\ (0,0,1,0,1,1,0)^T,\ (0,0,0,1,1,1,1)^T$$

erzeugte Unterraum. C ist ein linearer $[7, 4, 3]$–Code und wird der $(7, 4)$–**Hamming Code** genannt.

Durch einen $(n, M, 2e + 1)$–Code wird eine 'Packung' der **Hamming–Kugeln** $K(x) = \{y \in \mathbb{F}_2^n \,:\, d(x, y) \leq e\},\ x \in C$ gegeben. Das Problem, einen guten Code zu finden, ist also äquivalent zu dem Packungsproblem, die Anzahl M der Kugeln zu maximieren.

Aus Codes lassen sich periodische Kugelpackungen konstruieren.

Satz 5.43 (Konstruktion A) *Sei C ein binärer (n, M, d)–Code und $r = \min\{1, \sqrt{d}/2\}$. Dann ist $\mathcal{K} = r \cdot B^n + C + 2 \cdot \mathbb{Z}^n$ eine (periodische) Kugelpackung mit Dichte $\frac{M \cdot \kappa_n \cdot r^n}{2^n}$ (dabei wird C als Teilmenge von $\mathbb{Z}^n$ aufgefaßt). Ferner ist $\mathcal{K}$ eine Gitterpackung genau dann, wenn C ein linearer Code ist.*

Beispiel: Sei $C = \{00, 11\}$. Dann gilt $d = 2$, $r = 1/\sqrt{2}$ und Konstruktion A ergibt die Packung $rB^2 + C + 2\mathbb{Z}^2 = rB^2 + \Lambda$, wobei $\Lambda = \{(x, y)^T : x + y \equiv 0 \bmod 2\}$ ein Gitter mit Determinante 2 ist. Die Dichte ist $\frac{2 \cdot \pi \cdot 1/2}{4} = \frac{\pi}{4} = 0.785\ldots$.

Die folgende Konstruktion ist eine Modifikation von Konstruktion A. Ein Teil der Gitterpunkte wird entfernt, wodurch der Radius der Kugel eventuell vergrößert und die Dichte eventuell verbessert werden kann.

Beispiel: Sei $C = \{000, 011, 101, 110\}$. Dann gilt $d = 2$, $r = 1/\sqrt{2}$ und Konstruktion A ergibt die Packung $rB^3 + C + 2\mathbb{Z}^3 = rB^3 + \Lambda$, wobei $\Lambda = \{(x, y, z)^T : x + y + z \equiv 0 \bmod 2\}$ ein Gitter mit Determinante 2 ist. Die Dichte ist $\frac{4 \cdot 4/3 \cdot \pi \cdot 1/(2\sqrt{2})}{8} = \frac{\pi}{3\sqrt{2}}$, also optimal.

Satz 5.44 (Konstruktion B) *Sei C ein binärer (n, M, d)–Code und jedes Codewort habe gerades Gewicht. Es sei*

$$T = \{t \in \mathbb{Z}^n : t \equiv c \bmod 2, \text{ für ein } c \in C, \quad \text{und} \quad t_1 + \ldots + t_n \equiv 0 \bmod 4\}$$

und $r = \min\{\sqrt{2}, \sqrt{d}/2\}$. Dann ist $\mathcal{K} = r \cdot B^n + T$ eine (periodische) Kugelpackung mit Dichte $\frac{M \cdot \kappa_n \cdot r^n}{2^{n+1}}$. Ferner ist $\mathcal{K}$ eine Gitterpackung genau dann, wenn C ein linearer Code ist.

Bemerkung: Sei $C_1 = \{c \in C : c_1 + \ldots + c_n \equiv 0 \bmod 4\}$ und $C_2 = \{c \in C : c_1 + \ldots + c_n \equiv 2 \bmod 4\}$. Dann gilt $C = C_1 \cup C_2$. Setzt man $\Lambda_1 = \{x \in 2\mathbb{Z}^n : x_1 + \ldots + x_n \equiv 0 \bmod 4\}$ und $\Lambda_2 = 2\mathbb{Z}^n \backslash \Lambda_1$, so folgt

$$T = (C_1 + \Lambda_1) \cup (C_2 + \Lambda_2).$$

Beispiel: Sei $C = \{00, 11\}$. Dann gilt $d = 2$, $r = 1/\sqrt{2}$ und Konstruktion B ergibt die Packung $rB^2 + \{(0,0)^T, (2,2)^T, (3,1)^T, (1,3)^T\} + 4\mathbb{Z}^2 = rB^2 + \Lambda$, wobei Λ Gitter mit Basis $\{(4,0)^T, (-1,1)^T\}$ ist und damit $d(\Lambda) = 4$. Die Dichte ist $\frac{2 \cdot \pi \cdot 1/2}{8} = \frac{\pi}{8} = 0.392\ldots$.

Beispiel: Sei $C = \{0^8, 1^8\}$. Dann gilt $d = 8$, $r = \sqrt{2}$ und Konstruktion B ergibt die Packung $rB^8 + \Lambda$, wobei $\Lambda = \{x \in \mathbb{Z}^8 : x_1 + \ldots + x_8 \equiv 0 \bmod 4 \text{ und } x_1 \equiv \ldots \equiv x_8 \bmod 2\}$ ein Gitter mit Determinante 2^8 ist. Die Dichte ist $\frac{2 \cdot \kappa_8 \cdot 2^4}{2^9} = \frac{\kappa_8}{2^4} = \frac{\pi^4}{384}$, also optimal.

Bisher haben wir nur Kanäle betrachtet, in denen diskrete Signale übertragen werden. In einem **Gaußschen Kanal** werden stetige Signale übertragen. Ein Signal f

wird in periodischen Abständen $0, t, 2t, \ldots, (n-1)t$ 'gesampled'. Dann wird der Vektor $(f(0), f(t), f(2t), \ldots, f((n-1)t)) \in \mathbb{R}^n$ übertragen, wobei ein 'weißes Rauschen' hinzugefügt wird. Ein Code für diesen Kanal ist dann einfach eine Menge von Punkten im $\mathbb{R}^n$. Die Energie des Signals entspricht der Euklidischen Länge des Vektors. Von besonderem Interesse sind Codes, in denen alle Codewörter die gleiche Länge (Energie) haben. Dies führt zu dem sogenannten **Diktatorenproblem:** Man verteile auf der Oberfläche einer Kugel (Welt) eine Anzahl von Punkten (Paläste der Diktatoren) so, daß der minimale Abstand zweier Punkte möglichst groß ist. Äquivalent dazu ist das Problem, auf der Kugeloberfläche eine möglichst große Anzahl von Kugelkappen zu packen.

Definition 5.45 *Sei $\Omega_n = \mathrm{bd}\,(B^n)$ die Oberfläche der Einheitskugel.*

(a) Eine Menge $C \subset \Omega_n$ heißt **sphärischer Code**.

(b) Zu $C \subset \Omega$ ist der **Minimalwinkel** *von C die größte Zahl ϕ mit $x \cdot y \leq \cos\phi$, für $x, y \in C,\ x \neq y$.*

(c) $A(n, \phi)$ sei die maximale Anzahl von Punkten in einem sphärischen Code mit Minimalwinkel ϕ.

Bemerkung: Die Bestimmung von $A(n, \pi/3)$ ist äquivalent zu der Frage, wieviele nichtüberlappende Kugeln eine feste Kugel berühren können. Diese Zahl wird auch **Newton–Zahl** (oder **Kissing number**) genannt. Es gilt z. B. $A(2, \pi/3) = 6$ und $A(3, \pi/3) = 12$.

Abschätzungen für sphärische Codes liefern Schranken für die Kugelpackungsdichte.

Lemma 5.46 *In einer Kugel rB^n mit Radius r gibt es mindestens $\delta(B^n) \cdot r^n$ Punkte, die paarweise Abstand ≥ 2 haben.*

Satz 5.47 *Für Winkel $0 < \phi \leq \pi$ gilt $\delta(B^n) \leq sin(\phi/2) \cdot A(n+1, \phi)$.*

Bemerkung: Mit Hilfe von Satz 5.47 zeigten Kabatjanski und Levenštein die bisher beste obere Schranke für die Kugelpackungsdichte:

$$\delta(B^n) \leq 2^{-0.599n + o(n)}.$$

Es ist bis heute nicht klar, in welchem Bereich des Intervalls $[0.599, 1]$ die Zahl $-1/n \cdot \log_2(\delta(B^n))$ liegt.