Vorlesungen von Prof. Dr. C.P. Schnorr:

Gitter und Kryptographie

an der Johann Wolfgang Goethe-Universität Frankfurt/Main
im Wintersemester 2003/2004

$\boxed{\boxed{\beta_5\text{-Version}}}$

28. Oktober 2005

Inhaltsverzeichnis

Kapitel 1

Gitter in linearen Räumen

Gitter als Punktmengen des Vektorraums $\mathbb{R}^m$ sind Gegenstand der Geometrie der Zahlen, die Minkowski um 1900 entwickelt hat. Der ganzzahlige Lösungsraum eines linearen, reellen Gleichungssystems ist ein Gitter, der größere reelle Lösungsraum ist ein linearer Raum. Gitter sind also ein diskretes Analogon zu linearen Räumen. Probleme der Linearen Algebra werden durch Gitter diskretisiert. Dabei geht es insbesondere um die Konstruktion kleiner Lösungen, also kurzer Gittervektoren. Die älteren Arbeiten von Hermite, Gauß und Korkine - Zolotareff behandeln Gitter in der Sprache der quadratischen Formen.

Ein Gitter ist eine diskrete, additive Untergruppen eines reellen Vektorraums $\mathbb{R}^m$. Wir behandeln Gittterbasen sowie ihre Teilbasen, primitive Systeme, die Gitterdeterminante, das einer Basis zugehörige Orthogonalsystem, isometrische Transformationen und die QR-Zerlegung von Basen. Wir definierenen ferner duale Gitter und duale Basen, Hermite-Normalformen, sowie elementare Algorithmen zur Reduktion von Gitterbasen. Der Leser sollte mit Linearer Algebra vertraut sein.

Gitter-Notation. Es bezeichne $\mathbb{R}$ die Menge der reellen Zahlen und $\mathbb{Z}$ die der ganzen Zahlen, fener sei $\mathbb{R}^m$ der reelle Vektorraum der Dimension m. Es seien $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ beliebige Vektoren und $B = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{R}^{m \times n}$ die Matrix mit Spaltenvektoren $\mathbf{b}_1, \ldots, \mathbf{b}_n$. Dann bezeichnet

$$\mathcal{L}(B) = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) =_{\text{def}} \{B\mathbf{z} | \mathbf{z} \in \mathbb{Z}^n\} = \textstyle\sum_{i=1}^n \mathbf{b}_i \mathbb{Z}$$

die von den Vektoren $\mathbf{b}_1, ..., \mathbf{b}_n$ erzeugte additive Untergruppe des $\mathbb{R}^n$. Sind die Vektoren $\mathbf{b}_1, ..., \mathbf{b}_n$ linear unabhängig, so nennen wir $\mathcal{L}(B)$ ein *Gitter* mit *Basis* $\mathbf{b}_1, ..., \mathbf{b}_n$ bzw. B und *Dimension* oder *Rang* $\dim(\mathcal{L}) =_{\text{def}} \text{rang}(B)$. Der vom Gitter $\mathcal{L} = \mathcal{L}(B)$ aufgespannte lineare Raum ist $\text{span}(\mathcal{L}) =_{\text{def}} \{B\mathbf{z} | \mathbf{z} \in \mathbb{R}^n\} = \sum_{i=1}^n \mathbf{b}_i \mathbb{R}$. Alle Basen B von $\mathcal{L}$ erzeugen denselben linearen Raum $\text{span}(\mathcal{L})$ und haben damit denselben Rang.

1.1 Die Geometrie der Gitter

Es sei $\langle \cdot, \cdot \rangle : \mathbb{R}^m \times \mathbb{R}^m \to \mathbb{R}$ das Standard-Skalarprodukt, $\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^t \mathbf{y}$. Es bezeichne $\|\mathbf{x}\| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$ die Länge des Vektors $\mathbf{x}$. Die multiplikative Gruppe $GL_n(\mathbb{Z})$ der ganzzahligen $n \times n$-Matrizen mit Determinante ± 1 nennt man die *allgemeine lineare Gruppe* über $\mathbb{Z}$. Die Matrizen $U \in GL_n(\mathbb{Z})$ heißen *unimodular*. Die Basen $\bar{B}$ eines Gitters sind die transformierten einer beliebigen Basis $B \in \mathbb{R}^{m \times n}$, transformiert durch unimodulare Matrizen.

Satz 1.1.1
Die Basen des Gitters $\mathcal{L}(B)$ mit $B \in \mathbb{R}^{m \times n}$ sind genau die Matrizen BU mit $U \in GL_n(\mathbb{Z})$.

Beweis. Sei $\bar{B}$ eine weitere Basis zu $\mathcal{L}(B)$. Dann gibt es ein $U \in \mathbb{Z}^{n\times n}$ mit $\bar{B} = B\,U$, denn jeder Spaltenvektor von $\bar{B}$ ist ganzzahlige Linearkombination von Spaltenvektoren von B. Wegen $\mathrm{rang}(\bar{B}) = \mathrm{rang}(B)$ gilt $\det U \neq 0$, und somit $\bar{B}\,U^{-1} = B$. Wegen $\mathcal{L}(\bar{B}) = \mathcal{L}(B)$ ist U^{-1} ganzzahlig, und somit $|\det U| = 1$ und $U \in GL_n(\mathbb{Z})$.

Umgekehrt gilt für $U \in GL_n(\mathbb{Z})$ offenbar dass $\mathcal{L}(B\,U) = \mathcal{L}(B)$, somit ist $B\,U$ Basis zu $\mathcal{L}(B)$. $\square$

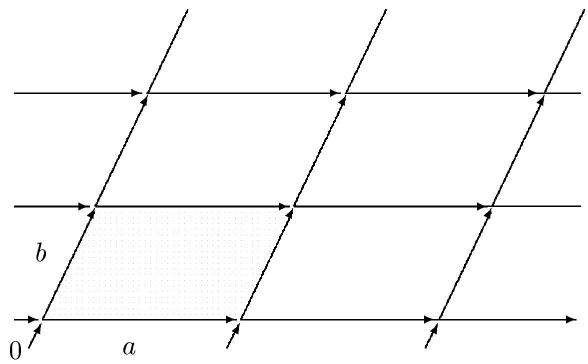

Abbildung 1.1.1: Grundmasche des Gitters mit Basis $\mathbf{a}, \mathbf{b} \in \mathbb{R}^2$

Grundmasche, Determinante, Gram-Matrix. Die *Grundmasche* zur Basis $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ ist das Parallelepiped

$$\mathcal{P} = \mathcal{P}(B) = \{\textstyle\sum_{i=1}^{n} t_i \mathbf{b}_i \mid 0 \leq t_1, \ldots, t_n < 1\} \subset \mathrm{span}(\mathcal{L})\,.$$

Jeder Punkt $\mathbf{x} \in \mathrm{span}(\mathcal{L})$ hat eine eindeutige Zerlegung $\mathbf{x} = \mathbf{b} + \mathbf{m}$ mit $\mathbf{m} \in \mathcal{P}$ und $\mathbf{b} \in \mathcal{L}$. Damit ist der Raum $\mathrm{span}(\mathcal{L})$ zerlegt in die verschobenen Maschen $\mathbf{b} + \mathcal{P}(B)$ mit $\mathbf{b} \in \mathcal{L}$ und es gilt $\mathrm{span}(\mathcal{L}) = \bigcup_{\mathbf{b}\in\mathcal{L}} \mathbf{b} + \mathcal{P}(B) = \mathcal{P} + \mathcal{L}$.

Die *Determinante* $\det \mathcal{L}$ des Gitters $\mathcal{L} = \mathcal{L}(B) \subset \mathbb{R}^m$ ist das Volumen von $\mathcal{P}(B) \subset \mathrm{span}(\mathcal{L})$,

$$\det \mathcal{L} =_{\mathrm{def}} \mathrm{vol}\,\mathcal{P}(B) = (\det B^t B\,)^{\frac{1}{2}}.$$

Die Gleichheit $\mathrm{vol}\,\mathcal{P}(B) = (\det B^t B\,)^{\frac{1}{2}}$ gilt offensichtlich für Basen $B \in \mathbb{R}^{n\times n}$. Sie gilt allgemein weil sie bei Isometrie erhalten bleibt, siehe Lemma 1.1.3.

Die Determinante $\det(B^t B)$ ist unabhängig von der Wahl der Basis B von $\mathcal{L}$. Denn seien $B, \bar{B}$ Basen des Gitters mit $\bar{B} = B\,U$, $U \in GL_n(\mathbb{Z})$. Wegen $|\det U| = 1$ und der Multiplikativität der Determinante gilt $\det(B^t B)^{\frac{1}{2}} = \det(U^t B^t B U)^{\frac{1}{2}} = \det(\,\bar{B}^t \bar{B}\,)^{\frac{1}{2}}$.

Die *Gram-Matrix* zur Basis B ist die $n \times n$-Matrix $B^t B = [\langle \mathbf{b}_i, \mathbf{b}_j\rangle]_{1\leq i,j\leq n}$ bestehend aus den Skalarprodukten der Basisvektoren.

Theorem 1.1.2
Sei $\mathcal{L} \subset \mathbb{R}^m$ Gitter und $\mathcal{B}(\mathbf{0}, r) \subset \mathrm{span}(\mathcal{L})$ die Kugel mit Mittelpunkt $\mathbf{0}$ und Radius r. Dann gilt

$$\lim_{r\to\infty} |\,\mathcal{L} \cap \mathcal{B}(\mathbf{0}, r)\,| / \mathrm{vol}\,\mathcal{B}(\mathbf{0}, r) = 1/\det \mathcal{L}(B),$$

d.h. $\det \mathcal{L}(B)$ *ist der Kehrwert der Dichte der Gitterpunkte.*

Beweis. Sei $\mathcal{L} = \mathcal{L}(B)$ Gitter mit Grundmasche $\mathcal{P}(B)$. Dann ist $\mathrm{span}(\mathcal{L})$ die disjunkte Vereinigung der um Gitterpunkte $\mathbf{b}$ verschobenen Grundmasche, $\mathrm{span}(\mathcal{L}) = \bigcup_{\mathbf{b}\in\mathcal{L}} \mathbf{b} + \mathcal{P}(B)$.

Da $\mathbf{b} + \mathcal{P}(B)$ nur den Gitterpunkt $\mathbf{b}$ enthält, gibt es pro $\det \mathcal{L}$ Volumeneinheiten genau einen Gitterpunkt. Diejenigen Gitterpunkte $\mathbf{b}$, deren Maschen $\mathbf{b} + \mathcal{P}(B)$ die Kugel $\mathcal{B}(\mathbf{0}, r)$ echt schneiden, können entweder in $\mathcal{L} \cap \mathcal{B}(\mathbf{0}, r)$ oder im Komplement liegen. Dies führt in der Gleichung

$|\,\mathcal{L} \cap \mathcal{B}(\mathbf{0},r)\,|/\mathrm{vol}\,\mathcal{B}(\mathbf{0},r) = 1/\det\mathcal{L}(B) + O(\frac{1}{r})$ zu einem Fehler $O(\frac{1}{r})$, der proportional zum Verhältnis Oberfläche zu Volumen von $\mathcal{B}(\mathbf{0},r)$ ist. □

Beispiel-Gitter. Wir behandeln Gitter zu dichtesten Kugelpackungen. Das erste sukzessive Minimum λ_1 ist die Länge des kürzesten Gittervektors ungleich $\mathbf{0}$. Die *(Packungs-) Dichte* des Gitters $\mathcal{L}$ mit $\dim\mathcal{L} = n$ ist $\triangle(\mathcal{L}) = (\lambda_1/2)^n V_n(1)/\det\mathcal{L}$ mit $V_n(1) = \mathrm{vol}\,\mathcal{B}(\mathbf{0},1)$, siehe Abschnitt 3.2.. Das Gitter

$$\mathbb{A}_n := \left\{(x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1} \;\middle|\; \textstyle\sum_{i=0}^n x_i = 0\right\}$$

hat die Basis

$$B = \begin{bmatrix} -1 & 0 & 0 & \cdots & \cdots & 0 \\ 1 & -1 & 0 & & & 0 \\ 0 & \ddots & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & -1 & 0 \\ 0 & & & 0 & 1 & -1 \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{bmatrix} \in \mathbb{Z}^{(n+1)\times n}.$$

Offenbar gilt $\lambda_1 = \sqrt{2}$, $\det\mathbb{A}_n = \sqrt{n+1}$. Die Dichte ist $\triangle(\mathbb{A}_n) = V_n(1)\,2^{-n/2}(n+1)^{-1/2}$.

Das *Schachbrettgitter*

$$\mathbb{D}_n := \{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid \textstyle\sum_{i=1}^n x_i = 0 \mod 2\}$$

hat die Basis

$$B = \begin{bmatrix} 2 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 1 & 0 \\ 0 & & & 0 & 1 & 1 \\ 0 & \cdots & \cdots & 0 & 0 & 1 \end{bmatrix} \in \mathbb{Z}^{n\times n}.$$

Offenbar gilt $\lambda_1 = \sqrt{2}$ und $\det(\mathbb{D}_n) = 2$. Die Dichte ist $\triangle(\mathbb{D}_n) = V_n(1)\,2^{-n/2-1}$.

Das Gitter $\mathbb{E}_n$ hat für $n = 0 \bmod 4$ die einfache Form

$$\mathbb{E}_n := \left\{ (x_1, \ldots, x_n) \in \mathbb{Z}^n \;\middle|\; \begin{array}{l} \sum_{i=1}^n x_i = 0 \mod 4 \text{ und} \\ x_j = x_{j+1} \mod 2 \text{ für } 1 \le j < n. \end{array} \right\}$$

Es hat die Basen

$$B = \begin{bmatrix} 4 & 2 & 0 & \cdots & 0 & 1 \\ 0 & 2 & 2 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots \\ \vdots & & \ddots & 2 & 2 & 1 \\ 0 & & & 0 & 2 & 1 \\ 0 & \cdots & \cdots & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 4 & 2 & 2 & \cdots & 2 & 1 \\ 0 & 2 & 0 & \cdots & 0 & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & 2 & 0 & 1 \\ 0 & & & 0 & 2 & 1 \\ 0 & \cdots & \cdots & 0 & 0 & 1 \end{bmatrix} \in \mathbb{Z}^{n\times n}.$$

Offenbar gilt für $n \ge 8$ dass $\lambda_1 = \sqrt{8}$ und $\det\mathbb{E}_n = 2^n$, $\triangle(\mathbb{E}_n) = V_n(1)\,2^{-n/2}$.

Die Gitter $\mathbb{E}_6, \mathbb{E}_7$ sind Untergitter von $\mathbb{E}_8$,

$$\mathbb{E}_6 := \{\mathbf{x} \in \mathbb{E}_8 \mid x_6 = x_7 = x_8\}, \quad \mathbb{E}_7 := \{\mathbf{x} \in \mathbb{E}_8 \mid x_7 = x_8\}.$$

Isometrie, orthogonale Matrix, Äquivalenz. Eine lineare Abbildung $T : V \to W$ mit linearen Räumen V, W heißt *isometrisch*, bzw. eine *Isometrie* (von V), wenn T das Skalarprodukt erhält, d.h. wenn $\langle \mathbf{b}, \mathbf{b}' \rangle = \langle T(\mathbf{b}), T(\mathbf{b}') \rangle$ für alle $\mathbf{b}, \mathbf{b}' \in V$. Eine Matrix $Q \in \mathbb{R}^{m\times n}$, $m \geq n$, heißt *isometrisch*, bzw.*Isometrie*, wenn die Abbildung $x \mapsto Qx$ isometrisch ist. Damit ist $Q \in \mathbb{R}^{m\times n}$ genau dann isometrisch, wenn $Q^tQ = I_n$ die Einheitsmatrix $I_n \in \mathbb{R}^{n\times n}$ ist. Das Produkt von isometrischen Matrizen ist isometrisch. Eine isometrische Quadratmatrix $Q \in \mathbb{R}^{n\times n}$ bezeichnet man als *orthogonale Matrix.* Q ist orthogonal genau dann, wenn $Q^{-1} = Q^t$. Mit Q ist auch Q^t orthogonal. Damit ist $Q \in \mathbb{R}^{m\times n}$ genau dann isometrisch, wenn Q durch Hinzunahme von Spalten zu einer orthogonalen Matrix ergänzbar ist.

Zwei Gitter $\mathcal{L}, \bar{\mathcal{L}}$ heißen *isometrisch*, wenn es eine Isometrie T von $\mathrm{span}(\mathcal{L})$ gibt mit $T(\mathcal{L}) = \bar{\mathcal{L}}$. Zwei Basen $B, \bar{B}$ heißen *isometrisch*, wenn es eine Isometrie Q gibt mit $\bar{B} = QB$. Offenbar sind $\bar{B}, B$ genau dann isometrisch, wenn $B^tB = \bar{B}^t\bar{B}$. Offenbar erzeugen isometrische Basen $B, \bar{B}$ isometrische Gitter $\mathcal{L}(B), \mathcal{L}(\bar{B})$. Umgekehrt haben isometrische Gitter stets isometrische Basen.

Zwei Gitter $\mathcal{L}, \bar{\mathcal{L}}$ heißen *äquivalent* oder *ähnlich*, wenn es ein $c > 0$ gibt so dass $\mathcal{L}$ und $c\bar{\mathcal{L}}$ isometrisch sind, Bez.: $\mathcal{L} \cong \bar{\mathcal{L}}$. Die Gitter $\mathcal{L}$, $c\mathcal{L}$ heißen *proportional* oder bis auf Skalierung gleich.

Beispiel isometrischer Basen.

$$B := \begin{bmatrix} \sqrt{2} & 1/\sqrt{2} \\ 0 & \sqrt{3/2} \end{bmatrix}, \qquad \bar{B} := \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad B^tB = \bar{B}^t\bar{B} = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Geometrische Größen sind Größen, die bei isometrischen Abbildungen erhalten bleiben, also Invarianten von Isometrien. Volumeninhalte, Determinanten, Skalarprodukte und Längen von Vektoren sind geometrische Größen. Ein Gitter $\mathcal{L} \subset \mathbb{R}^m$ heißt *vollständig*, wenn $\dim \mathcal{L} = m$. Vollständige Gitter reichen für geometrische Betrachtungen aus, weil jedes Gitter nach Lemma 1.1.3(2) isometrisch zu einem vollständigen Gitter ist. Für kombinatorische und algorithmische Untersuchungen reichen vollständige Gitter dagegen nicht. Isometrische Abbildungen erhalten nicht die Ganzzahligkeit von Vektoren.

Orthogonalsystem, orthogonale Projektion. Zur Basis $\mathbf{b}_1, ..., \mathbf{b}_n \in \mathbb{R}^m$ bezeichne $\pi_i : \mathbb{R}^m \to \mathrm{span}(\mathbf{b}_1, \dots, \mathbf{b}_{i-1})^\perp$ die orthogonale Projektion, derart dass für alle $\mathbf{b} \in \mathbb{R}^m$

$$\pi_i(\mathbf{b}) \in \mathrm{span}(\mathbf{b}_1, \dots, \mathbf{b}_{i-1})^\perp, \qquad \mathbf{b} - \pi_i(\mathbf{b}) \in \mathrm{span}(\mathbf{b}_1, \dots, \mathbf{b}_{i-1}).$$

Offenbar sind die Vektoren $\widehat{\mathbf{b}}_i := \pi_i(\mathbf{b}_i)$ für $i = 1, ..., n$ paarweise orthogonal. Man berechnet $\widehat{\mathbf{b}}_1, \dots, \widehat{\mathbf{b}}_n$ durch das Gram-Schmidt-Verfahren

$$\widehat{\mathbf{b}}_1 := \mathbf{b}_1, \qquad \widehat{\mathbf{b}}_i := \pi_i(\mathbf{b}_i) = \mathbf{b}_i - \textstyle\sum_{j=1}^{i-1} \frac{\langle \mathbf{b}_i, \widehat{\mathbf{b}}_j \rangle}{\langle \widehat{\mathbf{b}}_j, \widehat{\mathbf{b}}_j \rangle} \widehat{\mathbf{b}}_j \qquad \text{für } i = 2, 3, \dots, n.$$

Für die *Gram-Schmidt-Koeffizienten* $\mu_{i,j} := \frac{\langle \mathbf{b}_i, \widehat{\mathbf{b}}_j \rangle}{\langle \widehat{\mathbf{b}}_j, \widehat{\mathbf{b}}_j \rangle}$ gilt insbesondere $\mu_{i,i} = 1$ und $\mu_{i,j} = 0$ für $j > i$, sowie $\mathbf{b}_i = \widehat{\mathbf{b}}_i + \sum_{j=1}^{i-1} \mu_{i,j} \widehat{\mathbf{b}}_j$ für $i = 1, ..., n$. In Matrizenschreibweise bedeutet dies

$$[\mathbf{b}_1, \dots, \mathbf{b}_n] = [\, \widehat{\mathbf{b}}_1, \dots, \widehat{\mathbf{b}}_n] \, [\mu_{i,j}]^t_{1 \leq i,j \leq n}.$$

***QR*-Zerlegung und geometrische Normalform (GNF).** Die QR-Zerlegung $B = QR$ der Basis $B = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{R}^{m\times n}$ ist die eindeutige Zerlegung $B = QR$, so dass $Q \in \mathbb{R}^{m\times n}$ isometrisch ist und $R \in \mathbb{R}^{n\times n}$ obere Dreiecksmatrix mit positiven Diagonalelementen. Wir nennen R die *geometrische Normalform* (GNF) der Basis, Bez.: $R = GNF(B)$. Es gilt $Q := [\widehat{\mathbf{b}}_1/\|\widehat{\mathbf{b}}_1\|, ..., \widehat{\mathbf{b}}_n/\|\widehat{\mathbf{b}}_n\|] \in \mathbb{R}^{m\times n}$ und

$$R := \begin{bmatrix} \|\widehat{\mathbf{b}}_1\| & 0 & \cdots & \cdots & 0 \\ 0 & \|\widehat{\mathbf{b}}_1\| & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \|\widehat{\mathbf{b}}_{n-1}\| & 0 \\ 0 & \cdots & \cdots & 0 & \|\widehat{\mathbf{b}}_n\| \end{bmatrix} \begin{bmatrix} 1 & \mu_{2,1} & \mu_{3,1} & \cdots & \mu_{n,1} \\ 0 & 1 & \mu_{3,2} & & \mu_{n,2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & \mu_{n,n-1} \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}.$$

Lemma 1.1.3
1. *Zwei Basen B, $\bar{B}$ sind genau dann isometrisch, wenn $GNF(B) = GNF(\bar{B})$.*
   Insbesondere ist $R = GNF(B)$ eindeutig bestimmt.
2. *$\mathcal{L}(B)$ ist isometrisch zum vollständigen Gitter $\mathcal{L}(R)$ mit $R = GNF(B)$.*

Beweis. 1. Aus $B^tB = \bar{B}^t\bar{B}$ mit QR-Zerlegungen $B = QR$ und $\bar{B} = \bar{Q}\bar{R}$ folgt $R^tR = \bar{R}^t\bar{R}$. Weil $R, \bar{R}$ obere Dreiecksmatrizen mit positiven Diagonalelementen sind, folgt $R = \bar{R}$. Umgekehrt folgt aus $GNF(B) = R = GNF(\bar{B})$, dass $B^tB = R^tR = \bar{B}^t\bar{B}$, und damit sind $B, \bar{B}$ isometrisch.
3. Für jede QR-Zerlegung $B = QR$ sind $\mathcal{L}(B), \mathcal{L}(R)$ isometrisch mit der Isometrie Q. □

Für beliebige Basen $B = QR$ gilt $\det(B^tB) = \det(R^tR) = \prod_{i=1}^n \|\widehat{\mathbf{b}}_i\|^2$. Insbesondere bleibt $\det \mathcal{L}(B) = (\det B^tB)^{\frac{1}{2}}$, bei Isometrie erhalten.

Das orthogonale Gitter. Das zum Vektor $\mathbf{a} = (a_1, \ldots, a_n)^t \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ orthogonale Gitter ist

$$\mathcal{L}_{\mathbf{a}} := \operatorname{span}(\mathbf{a})^\perp \cap \mathbb{Z}^n = \{\mathbf{z} \in \mathbb{Z}^n \mid \langle \mathbf{a}, \mathbf{z} \rangle = 0\}.$$

Wir zeigen $\det \mathcal{L}_{\mathbf{a}} = \|\mathbf{a}\| / \operatorname{ggT}(a_1, \ldots, a_n)$.
Offenbar gilt $\dim \mathcal{L}_{\mathbf{a}} = n - 1$. Sei $\mathbf{b}_2, \mathbf{b}_3, \ldots, \mathbf{b}_n$ eine Basis von $\mathcal{L}_{\mathbf{a}}$. Wegen $\operatorname{span}(\mathcal{L}_{\mathbf{a}}) \cap \mathbb{Z}^n = \mathcal{L}_{\mathbf{a}}$ ist diese Basis nach Satz 1.3.3 zu einer Basis von $\mathbb{Z}^n$ ergänzbar. Es gibt ein $\mathbf{b}_1 \in \mathbb{Z}$ mit $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \mathbb{Z}^n$. Die Einträge des Vektors $\mathbf{b}_1$ sind teilerfremd, da $\mathbf{b}_1$ ein primitiver Vektor von $\mathbb{Z}^n$ ist. Der Anteil von $\mathbf{b}_1$, der senkrecht auf $\mathcal{L}_{\mathbf{a}}$ steht, ist $\frac{\langle \mathbf{b}_1, \mathbf{a} \rangle}{\|\mathbf{a}\|^2} \mathbf{a}$ und hat die Länge $\frac{|\langle \mathbf{b}_1, \mathbf{a} \rangle|}{\|\mathbf{a}\|}$. Die Grundmasche $\mathcal{P}(B)$ von $\mathbb{Z}^n$ hat die Grundfläche $\det \mathcal{L}_{\mathbf{a}}$ und Höhe $\frac{|\langle \mathbf{b}_1, \mathbf{a} \rangle|}{\|\mathbf{a}\|}$. Die Determinante von $\mathbb{Z}^n$ ist vol(Grundmasche) = Fläche × Höhe, $1 = \det \mathbb{Z}^n = (\det \mathcal{L}_{\mathbf{a}}) \frac{|\langle \mathbf{b}_1, \mathbf{a} \rangle|}{\|\mathbf{a}\|}$. Also gilt $\det \mathcal{L}_{\mathbf{a}} = \|a\| / |\langle \mathbf{b}_1, \mathbf{a} \rangle|$.

Nach Konstruktion von $\mathbf{b}_1$ ist $|\langle \mathbf{b}_1, \mathbf{a} \rangle|$ die kleinste, positive, ganze Zahl in $\sum_{i=1}^n \mathbb{Z}\, a_i = \mathbb{Z} \operatorname{ggT}(a_1, \ldots, a_n)$. Somit gilt $|\langle \mathbf{b}_1, \mathbf{a} \rangle| = |\operatorname{ggT}(a_1, \ldots, a_n)|$ und die Behauptung.

1.2 Dualität

Duales Gitter. Das *duale* (bzw. *polare, reziproke)* Gitter $\mathcal{L}^*$ zum Gitter $\mathcal{L}$ ist

$$\mathcal{L}^* =_{\text{def}} \{\mathbf{x} \in \operatorname{span}(\mathcal{L}) \mid \langle \mathbf{x}, \mathbf{b} \rangle \in \mathbb{Z} \text{ für alle } \mathbf{b} \in \mathcal{L}\}.$$

Aufgrund der Identität $(A^{-1})^t = (A^t)^{-1}$ für $A \in \mathbb{R}^{n \times n}$, kürzen wir ab $A^{-t} := (A^{-1})^t$. Es gilt $(AB)^{-t} = A^{-t}B^{-t}$.

Satz 1.2.1
1. *Für jede QR-Zerlegung $B = QR \in \mathbb{R}^{m \times n}$ gilt $\mathcal{L}(B)^* = \mathcal{L}(QR^{-t})$,*
2. $\dim \mathcal{L}^* = \dim \mathcal{L}$, *3.* $\det \mathcal{L}^* = 1/\det \mathcal{L}$, *4.* $(\mathcal{L}^*)^* = \mathcal{L}$,
5. *Ist B^tB Gram-Matrix zu $\mathcal{L}$ dann ist $(B^tB)^{-1} = B^{-1}B^{-t}$ Gram-Matrix zu $\mathcal{L}^*$.*

Die Basis B ist genau dann invertierbar, wenn $\mathcal{L}(B)$ vollständig ist. Dann gilt nach Satz 1.2.1 $\mathcal{L}(B)^* = \mathcal{L}(B^{-t})$ wegen $Q^{-1} = Q^t$ und $B^{-t} = (QR)^{-t} = Q^{-t}R^{-t} = Q\,R^{-t}$.

Beweis. 1. Offenbar gilt für $\bar{B} := Q\,R^{-t}$ wegen $Q^tQ = I_n$ dass

$$B^t\bar{B} = (QR)^tQ\,R^{-t} = R^tQ^tQ\,R^{-t} = I_n.$$

Wegen $B^t\bar{B} = I_n$ liefern die Vektoren $\bar{\mathbf{b}} \in \mathcal{L}(\bar{B})$ alle ganzzahligen Wertekombinationen $(\langle \mathbf{b}_1, \bar{\mathbf{b}}\rangle, ..., \langle \mathbf{b}_n, \bar{\mathbf{b}}\rangle) \in \mathbb{Z}^n$ zu den Basisvektoren $\mathbf{b}_1, ..., \mathbf{b}_n$. Damit gilt $\mathcal{L}^* = \mathcal{L}(\bar{B})$.

2. - 5. Aus $\dim \mathcal{L} = \operatorname{rang}(R) = \operatorname{rang}(R^{-1})$ folgt $\dim \mathcal{L}^* = \dim \mathcal{L}$. Weiter folgt $\det \mathcal{L}^* = 1/\det \mathcal{L}$ aus $\det \mathcal{L} = \det R = 1/\det R^{-t}$. Mit $(R^{-t})^{-t} = R$ gilt somit $(\mathcal{L}^*)^* = \mathcal{L}$. Schließlich gilt 5. wegen $\bar{B}^t\bar{B} = R^{-1}R^{-t} = (R^tR)^{-1} = (B^tB)^{-1}$. □

Duale Basis. Zur Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ von $\mathcal{L}$ ist die *duale Basis* $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ von $\mathcal{L}^*$ definiert durch $\langle \mathbf{b}_i, \mathbf{b}_{n-j+1}^*\rangle = \delta_{i,j}$. Die QR-Zerlegung $B = QR$ liefert die duale Basis $B^* = Q\,R^{-t}U_n$. Die Multiplikation mit $U_n =_{\text{def}} \begin{bmatrix} & & 1 \\ & \cdot & \\ 1 & & \end{bmatrix} \in \mathbb{R}^{n\times n}$, der Matrix mit Einsen in der Gegendiagonalen, invertiert die Spaltenreihenfolge der Basis $Q\,R^{-t}$, so dass $R^{-t}U_n$ obere Dreiecksmatrix ist.

Die QR-Zerlegung der dualen Basis B^* zu $B = QR$ ist $B^* = (QU_n)\,(U_nR^{-t}U_n)$. Denn zur QR-Zerlegung $B = QR$ ist R^{-t} untere Dreiecksmatrix und $U_nR^{-t}U_n$ obere Dreiecksmatrix. Der Übergang von R^{-t} nach $U_nR^{-t}U_n$ invertiert die Spalten- und die Zeilenreihenfolge in R^{-t}. Wegen $u_n^t = U_n = U_n^{-1}$ ist QU_n isometrisch.

Korollar 1.2.2
Zur Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ mit Orthogonalsystem $\widehat{\mathbf{b}}_1, \ldots, \widehat{\mathbf{b}}_n$ ist $\widehat{\mathbf{b}}_n/\|\widehat{\mathbf{b}}_n\|^2, \ldots, \widehat{\mathbf{b}}_1/\|\widehat{\mathbf{b}}_1\|^2$ das Orthogonalsystem der dualen Basis $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$.

Beweis. Es gilt $\langle \widehat{\mathbf{b}}_i, \widehat{\mathbf{b}}_j/\|\widehat{\mathbf{b}}_j\|^2\rangle = \delta_{i,j}$ für $1 \le i, j \le n$. □

Satz 1.2.3
Für jedes Gitter $\mathcal{L}$ und jede Isometrie T von $\operatorname{span}(\mathcal{L})$ gilt $T(\mathcal{L}^*) = T(\mathcal{L})^*$.

Beweis. Sei $\mathcal{L} = \mathcal{L}(B)$ mit QR-Zerlegung $B = QR \in \mathbb{R}^{m\times n}$ und sei $T : x \mapsto \bar{Q}x$ eine Isometrie. Weil QR^{-t} Basis von $\mathcal{L}^*$ ist, gilt nach Satz 1.2.1

$$\mathcal{L}^* = \mathcal{L}(Q\,R^{-t}),\ T(\mathcal{L}^*) = \mathcal{L}(\bar{Q}Q\,R^{-t}).$$

Andererseits ist $\bar{Q}Q$ isometrisch und damit ist $(\bar{Q}Q)\,R$ die QR-Zerlegung der Basis $\bar{Q}QR$ von $T(\mathcal{L})$. Es folgt

$$T(\mathcal{L})^* = \mathcal{L}(\bar{Q}QR)^* = \mathcal{L}(\bar{Q}Q\,R^{-t}) = T(\mathcal{L}^*).$$ □

Selbstduale und ganze Gitter. Ein Gitter $\mathcal{L}$ heißt *selbstdual* oder *unimodular*, wenn die Gram-Matrix B^tB unimodular ist, d.h., B^tB ist ganzzahlig und $\det B^tB = 1$. Ein Gitter $\mathcal{L}$ heißt *ganz* (*integral*), wenn B^tB ganzzahlig ist. Ein Gitter $\mathcal{L}$ ist also genau dann ganz, wenn $\mathcal{L} \subset \mathcal{L}^*$. $\mathcal{L}$ ist damit genau dann unimodular, wenn $\mathcal{L} = \mathcal{L}^*$.

1.3 Diskretheit, Primitive Systeme

Diskretheit. Eine Menge $S \subset \mathbb{R}^m$ heißt *diskret*, wenn S keinen Häufungspunkt in $\mathbb{R}^m$ hat.

Für jede additive Untergruppe $G \subset \mathbb{R}^m$ sind offenbar folgende Aussagen äquivalent:

1. G ist diskret,
2. $\mathbf{0}$ ist kein Häufungdpunkt von G,
3. Es gibt einen kürzesten Vektor in $G \setminus \{\mathbf{0}\}$.

Jedes Gitter ist diskret. Zum Nachweis der Diskretheit sei $\varphi : \mathbb{R}^n \to \operatorname{span}(\mathcal{L}(B)) \subset \mathbb{R}^m$ die lineare Abbildung $\varphi : \mathbf{z} \mapsto B\mathbf{z}$. φ ist ein Isomorphismus der Vektorräume $\mathbb{R}^n$ und $\operatorname{span}(\mathcal{L})$ mit $\varphi(\mathbb{Z}^n) = \mathcal{L}$. Weil $\mathbb{Z}^n$ diskret und φ^{-1} stetig auf $\operatorname{span}(\mathcal{L})$, ist auch $\mathcal{L}$ diskret.

Umgekehrt, ist jede diskrete additive Untergruppe von $\mathbb{R}^m$ ein Gitter. Die Diskretheit charakterisiert also die Gitter unter den additiven Untergruppen des $\mathbb{R}^m$.

Satz 1.3.1
Jede diskrete, additive Untergruppe des $\mathbb{R}^m$ ist ein Gitter erzeugt von einer Basis.

Beweis. Sei $\mathcal{L} \subset \mathbb{R}^m$ eine diskrete, additive Untergruppe und n die Maximalzahl linear unabhängiger Vektoren in $\mathcal{L}$. Offenbar gilt $n \leq m$. Durch Induktion über n zeigen wir die Existenz einer Basis.

$n = 1$: Sei $\mathbf{b} \in \mathcal{L}$ ein kürzester Vektor mit $\mathbf{b} \neq \mathbf{0}$ (ein solcher Vektor existiert, da $\mathbf{0}$ kein Häufungspunkt von $\mathcal{L}$ ist). Dann gilt $\mathcal{L}(\mathbf{b}) = \mathcal{L}$.

$n > 1$: Wähle $\mathbf{b}_1 \in \mathcal{L} \setminus \{\mathbf{0}\}$ derart dass $\frac{1}{k}\mathbf{b}_1 \notin \mathcal{L}$ für alle $k \geq 2$. Offenbar gilt $\mathcal{L}(\mathbf{b}_1) = \mathcal{L} \cap \operatorname{span}(\mathbf{b}_1)$. Betrachte die orthogonale Projektion $\pi : \mathbb{R}^m \to \operatorname{span}(\mathbf{b}_1)^\perp$ mit $\pi(\mathbf{b}) = \mathbf{b} - \frac{\langle \mathbf{b}_1, \mathbf{b}\rangle}{\langle \mathbf{b}_1, \mathbf{b}_1\rangle}\mathbf{b}_1$. Die Induktionsbehauptung ergibt sich aus den beiden Aussagen

1. $\pi(\mathcal{L})$ ist diskret und ein Gitter vom Rang $n-1$,
2. Für jede Basis $\pi(\mathbf{b}_2), \ldots, \pi(\mathbf{b}_n)$ von $\pi(\mathcal{L})$ mit $\mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathcal{L}$ gilt $\mathcal{L} = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$.

Beweis von 1. Wir zeigen, dass $\mathbf{0}$ kein Häufungspunkt von $\pi(\mathcal{L})$ ist. Angenommen, die paarweise verschiedenen Vektoren $\pi(\mathbf{y}^{(i)})$ mit $\mathbf{y}^{(i)} \in \mathcal{L}$ konvergieren gegen $\mathbf{0}$. Wir konstruieren unendlich viele kurze Vektoren in $\mathcal{L}$, im Widerspruch zur Diskretheit von $\mathcal{L}$.

Zu den Vektoren $\pi(\mathbf{y}^{(i)})$ erhalten wir kurze π-Urbilder $\bar{\mathbf{y}}^{(i)} \in \mathcal{L}$ nach der Vorschrift $\bar{\mathbf{y}}^{(i)} := \mathbf{y}^{(i)} - \lceil \langle \mathbf{y}^{(i)}, \mathbf{b}_1 \rangle / \langle \mathbf{b}_1, \mathbf{b}_1 \rangle \rfloor \mathbf{b}_1$. Dabei bezeichnet $\lceil r \rfloor := \lceil r - \frac{1}{2} \rceil$ die nächste ganze Zahl zur reellen Zahl r. Offenbar gilt $\|\bar{\mathbf{y}}^{(i)} - \pi(\mathbf{y}^{(i)})\| \leq \frac{1}{2}\|\mathbf{b}_1\|$. Wegen $\lim_{i\to\infty} \|\pi(\bar{\mathbf{y}}^{(i)})\| = 0$ gibt es unendlich viele Vektoren $\bar{\mathbf{y}}^{(i)} \in \mathcal{L}$ mit $\|\pi(\bar{\mathbf{y}}^{(i)})\| \leq \|\mathbf{b}_1\|$, im Widerspruch zur Diskretheit von $\mathcal{L}$.

Beweis zu 2. Die Maximalzahl der linear unabhängigen Vektoren in $\pi(\mathcal{L})$ ist $n-1$. Nach Induktionsvoraussetzung ist $\pi(\mathcal{L})$ ein Gitter vom Rang $n-1$. Sei $\pi(\mathbf{b}_2), \ldots, \pi(\mathbf{b}_n)$ eine Basis von $\pi(\mathcal{L})$ mit $\mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathcal{L}$. Die Vektoren $\mathbf{b}_1, ..., \mathbf{b}_n$ sind linear unabhängig. Wir zeigen, dass $\mathcal{L} \subset \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$. Zu beliebigem $\mathbf{b} \in \mathcal{L}$ gilt $\pi(\mathbf{b}) \in \pi(\mathcal{L}) = \mathcal{L}(\pi(\mathbf{b}_2), \ldots, \pi(\mathbf{b}_n))$, somit gibt es ein $\bar{\mathbf{b}} \in \mathcal{L}(\mathbf{b}_2, \ldots, \mathbf{b}_n)$ mit $\pi(\mathbf{b}) = \pi(\bar{\mathbf{b}})$. Es gilt $\mathbf{b} - \bar{\mathbf{b}} \in \operatorname{span}(\mathbf{b}_1)$. Nach Wahl von $\mathbf{b}_1$ gilt $\mathcal{L}(\mathbf{b}_1) = \mathcal{L} \cap \operatorname{span}(\mathbf{b}_1)$ und somit $\mathbf{b} - \bar{\mathbf{b}} \in \mathcal{L}(\mathbf{b}_1)$. Es folgt $\mathbf{b} \in \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$. □

Primitive Systeme. Wir charakterisieren Teilbasen $\mathbf{b}_1, ..., \mathbf{b}_k$ mit $k \leq n$ von Gitterbasen $\mathbf{b}_1, ..., \mathbf{b}_n$. Offenbar gilt für Teilbasen $\mathbf{b}_1, ..., \mathbf{b}_k$ dass

1. $\mathbf{b}_1, \ldots, \mathbf{b}_k$ sind linear unabhängig, 2. $\operatorname{span}(\mathbf{b}_1, \ldots, \mathbf{b}_k) \cap \mathcal{L} = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_k)$.

Eine Menge von Gittervektoren $\mathbf{b}_1, ..., \mathbf{b}_k$ nennt man ein *primitives System* zum Gitter $\mathcal{L}$, wenn 1. und 2. gilt. Ein einzelner Vektor $\mathbf{b} \in \mathcal{L}$ ist *primitiv*, wenn $\frac{1}{k}\mathbf{b} \notin \mathcal{L}$ für alle $k \in \mathbb{Z}$ mit $|k| \geq 2$.

Satz 1.3.2
Genau dann können die Gittervektoren $\mathbf{b}_1, \ldots, \mathbf{b}_k$ zu einer Basis von $\mathcal{L}$ ergänzt werden, wenn sie ein primitives System zu $\mathcal{L}$ bilden.

Beweis. Teilbasen bilden offenbar primitive Systeme. Sei nun umgekehrt $\mathbf{b}_1, \ldots, \mathbf{b}_k$ ein primitives System und $\pi : \operatorname{span}(\mathcal{L}) \to \operatorname{span}(\mathbf{b}_1, \ldots, \mathbf{b}_k)^\perp$ die orthogonale Projektion. Aus dem Beweis zu Satz 1.3.1 folgt, dass $\pi(\mathcal{L})$ ein Gitter der Dimension $n-k$ ist. Das Gitter $\pi(\mathcal{L})$ habe die Basis $\pi(\mathbf{b}_{k+1}), \ldots, \pi(\mathbf{b}_n)$ mit $\mathbf{b}_{k+1}, \ldots, \mathbf{b}_n \in \mathcal{L}$.

Wir zeigen, dass $\mathbf{b}_1, ..., \mathbf{b}_n$ Basis von $\mathcal{L}$ ist. Nach Konstruktion sind $\mathbf{b}_1, ..., \mathbf{b}_k$ linear unabhängig. Sei $\mathbf{b} \in \mathcal{L}$. Wegen $\pi(\mathbf{b}) \in \mathcal{L}(\pi(\mathbf{b}_{k+1}), \ldots, \pi(\mathbf{b}_n))$ gibt es ein $\bar{\mathbf{b}} \in \mathcal{L}(\mathbf{b}_{k+1}, \ldots, \mathbf{b}_n)$ mit $\pi(\bar{\mathbf{b}}) = \pi(\mathbf{b})$, also ist $\mathbf{b} - \bar{\mathbf{b}} \in \operatorname{span}(\mathbf{b}_1, \ldots, \mathbf{b}_k)$. Weil $\mathbf{b}_1, \ldots, \mathbf{b}_k$ nach Voraussetzung ein primitives System bildet, gilt $\mathbf{b} - \bar{\mathbf{b}} \in \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_k)$. Somit gilt $\mathbf{b} \in \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ und $\mathbf{b}_1, ..., \mathbf{b}_n$ ist Basis von $\mathcal{L}$. □

1.4 Elementare Reduktionsverfahren

Ziel der Reduktionsverfahren sind Gitterbasen bestehend aus kurzen Gittervektoren.

Definition 1.4.1
Die Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *ist* längenreduziert, *wenn* $|\mu_{i,j}| \leq \frac{1}{2}$ *für* $1 \leq j < i \leq n$.

Für jede längenreduzierte Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ gilt wegen $\mathbf{b}_i = \widehat{\mathbf{b}}_i + \sum_{j=1}^{i-1} \mu_{i,j} \widehat{\mathbf{b}}_j$ und $|\mu_{i,j}| \leq \frac{1}{2}$

$$\|\mathbf{b}_i\|^2 \leq \|\widehat{\mathbf{b}}_i\|^2 + \tfrac{1}{4} \textstyle\sum_{j=1}^{i-1} \|\widehat{\mathbf{b}}_j\|^2 \qquad \text{für } i = 1, \ldots, n$$

Algorithmus 1.4.1 zur Längenreduktion

EINGABE: Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$

FOR $i = 2, \ldots, n$ DO

FOR $j = i-1, \ldots, 1$ DO $\mathbf{b}_i := \mathbf{b}_i - \lceil \mu_{i,j} \rfloor \cdot \mathbf{b}_j$

AUSGABE: Längenreduzierte Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$

Korrektheit.

- Der Schritt $\mathbf{b}_i := \mathbf{b}_i - \lceil \mu_{i,j} \rfloor \mathbf{b}_j$ bewirkt, dass $\mu_{i,j}^{\text{neu}} := \mu_{i,j}^{\text{alt}} - \lceil \mu_{i,j}^{\text{alt}} \rfloor \mu_{j,j} = \mu_{i,j}^{\text{alt}} - \lceil \mu_{i,j}^{\text{alt}} \rfloor$.
- Insbesondere gilt dann $\left|\mu_{i,j}^{\text{neu}}\right| \leq \frac{1}{2}$, und die $\mu_{i,\nu}$ bleiben für $\nu > j$ unverändert.

Die Orthogonalvektoren bleiben erhalten. Die Längenreduktion ist nur eine schwache Reduktion.

Definition 1.4.2
Die Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *nennen wir* paarweise reduziert, *wenn*

1. $\frac{|\langle \mathbf{b}_i, \mathbf{b}_j \rangle|}{\|\mathbf{b}_j\|^2} \leq \frac{1}{2}$ *für* $1 \leq j < i \leq n$, *2.* $\|\mathbf{b}_i\| \leq \|\mathbf{b}_{i+1}\|$ *für* $i = 1, \ldots, n-1$.

Die Eigenschaft 1. bezieht sich *nicht* auf den Gram-Schmidt-Koeffizienten $\mu_{i,j} = \frac{\langle \mathbf{b}_i, \widehat{\mathbf{b}}_j \rangle}{\|\widehat{\mathbf{b}}_j\|^2}$. Die Eigenschaft 2. bedeutet, dass die Basisvektoren nach aufsteigender Länge geordnet sind

$$\|\mathbf{b}_1\| \leq \cdots \leq \|\mathbf{b}_n\|.$$

Die Eigenschaft 1. ist äquivalent zu $\|\mathbf{b}_i\| \leq \|\mathbf{b}_i \pm \mathbf{b}_j\|$ für $1 \leq j < i \leq n$, denn wegen

$$\|\mathbf{b}_i \pm \mathbf{b}_j\|^2 = \langle \mathbf{b}_i \pm \mathbf{b}_j, \mathbf{b}_i \pm \mathbf{b}_j \rangle = \|\mathbf{b}_i\|^2 \pm 2\, \langle \mathbf{b}_i, \mathbf{b}_j \rangle + \|\mathbf{b}_j\|^2 \text{ gilt}$$

$$\|\mathbf{b}_i\|^2 \leq \|\mathbf{b}_i \pm \mathbf{b}_j\|^2 \iff \pm \langle \mathbf{b}_i, \mathbf{b}_j \rangle \leq \tfrac{1}{2}\, \|\mathbf{b}_j\|^2 \iff |\langle \mathbf{b}_i, \mathbf{b}_j \rangle| \leq \tfrac{1}{2}\, \|\mathbf{b}_j\|^2.$$

Algorithmus 1.4.2 zur paarweise Reduktion

EINGABE: Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$

1. Ordne $\mathbf{b}_1, \ldots, \mathbf{b}_n$ so, dass $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \cdots \leq \|\mathbf{b}_n\|$

2. FOR $i = 1, \ldots, n$ DO

FOR $j = 1, \ldots, i-1$ DO

$r := \langle \mathbf{b}_i, \mathbf{b}_j \rangle \, \|\mathbf{b}_j\|^{-2}$

IF $|r| > \frac{1}{2}$ THEN $\mathbf{b}_i := \mathbf{b}_i - \lceil r \rfloor \mathbf{b}_j$, GO TO **1.**

AUSGABE: paarweise reduzierte Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$

Satz 1.4.3
Jedes Gitter hat eine paarweise reduzierte Basis.

Dies folgt aus der Korrektheit von Algorithmus 1.4.2 zur paarweise Reduktion. Algorithmus 1.4.2 ist korrekt, weil bei Abbruch des Verfahrens eine paarweise reduzierte Basis vorliegt und weil der Algorithmus terminiert. Bei jedem Reduktionsschritt wird nämlich ein Basisvektor echt kleiner, und die übrigen Basisvektoren bleiben verändert.

Das Verfahren zur paarweisen Reduktion läuft nicht Polynomial-Zeit. Führt man den Schritt $\mathbf{b}_i := \mathbf{b}_i - \lceil r \rfloor \mathbf{b}_j$ jedoch nur durch, wenn $\|\mathbf{b}_i^{\text{neu}}\| \leq \delta \, \|\mathbf{b}_i^{\text{alt}}\|$ für ein konstantes $\delta < 1$, dann wird die Laufzeit ploynomiell. Für die Ausgabebasis gilt dann $|\langle \mathbf{b}_i, \mathbf{b}_j \rangle| / \|\mathbf{b}_j\|^2 \leq \frac{1}{2} + O(1-\delta)$ für $1 \leq j < i \leq n$.

Kapitel 2

Hermite Normalform, Untergitter

2.1 Hermite-Normalform

Ganzzahlige und rationale Matrizen haben eine eindeutig bestimmte Hermite-Normalform (HNF). Für reelle Matrizen und relle Gitterbasen gilt dies nicht. Aus der HNF einer Transformationsmatrix $T \in \mathbb{Z}^{n\times n}$ kann man $\det \mathcal{L}(B)/\det \mathcal{L}(BT) = |\det T|$ ablesen.

Definition 2.1.1
Eine Matrix $A = [a_{ij}] \in \mathbb{R}^{m\times n}$ *mit* $n \leq m$ *ist in* Hermite-Normalform *(kurz HNF), wenn*

1. $a_{ij} = 0$ *für* $j > i$, *d.h.* A *ist eine untere Dreiecksmatrix.*
2. $a_{ii} > 0$ *für* $i = 1, 2, \ldots, m$.
3. $0 \leq a_{ij} < a_{ii}$ *für* $j < i$.

Die Hermite-Normalform ist eine reduzierte Basis, in dem Sinne dass der i-te Basisvektor die i-te Koordinate minimiert unter der Bedingung, dass seine ersten $i-1$ Koordinaten Null sind. Für eine HNF $A = [a_{ij}] = [\mathbf{a}_1, ..., \mathbf{a}_n]$ mit Spaltenvektoren $\mathbf{a}_1, ..., \mathbf{a}_n$ ist a_{ii} also die absolut kleinste i-te Koordinate $\neq 0$ der Vektoren in $\mathcal{L}(\mathbf{a}_i, ..., \mathbf{a}_n)$. Dabei ist $\mathcal{L}(\mathbf{a}_i, ..., \mathbf{a}_n)$ das Teilgitter, dessen Vektoren in den ersten $i-1$ Koordinaten Null sind.

In der Definition der HNF kann man statt einer 'unteren' Dreiecksmatrix ebenso gut eine 'obere' Dreiecksmatrix verlangen. Der zulässige Bereich der Zahlen a_{ij} in 3. ist ein Intervall der Länge $|a_{ii}|$, die Lage dieses Intervals ist willkürlich. In [DKT87] fordern die Autoren

$$a_{ij} \leq 0 \text{ und } |a_{ij}| < a_{ii} \quad \text{für } j < i.$$

A. Paz und C.P. Schnorr [PaSchn87] fordern, dass die Elemente links der Diagonalen betragsmäßig minimal sind:

$$|a_{ij}| < \tfrac{1}{2}\,|a_{ii}| \quad \text{für } j < i.$$

Die verschiedenen Varianten von Hermite-Normalformen sind einfach ineinander überführbar. Ist z.B. $A \in \mathbb{R}^{m\times n}$ untere Dreiecksmatrix, dann ist $U_m\,A\,U_n$ obere Dreiecksmatrix für die Matrizen U_m, U_n mit Einsen auf der Gegendiagonalen.

Nach C. Hermite [Hermite1850] gilt folgender Satz.

Satz 2.1.2 (Hermite 1850)
Zu jeder Matrix $A \in \mathbb{Q}^{m\times n}$ *mit* $\mathrm{Rang}(A) = n$ *gibt es genau eine HNF* $A\,U$ *mit* $U \in GL_n(\mathbb{Z})$.

Beweis. *Konstruktion der HNF.* Sei $\mathcal{L}(A) \subset \mathbb{R}^m$ das Gitter zur Basis A. Konstruiere die Vektoren $\mathbf{a}'_1, ..., \mathbf{a}'_n \in \mathcal{L}(A)$, $[\mathbf{a}'_1, ..., \mathbf{a}'_n] = [a'_{ij}] \in \mathbb{R}^{m\times n}$ so dass

$$a'_{ii} = \min\{\, |a_i| \mid (a_1, ..., a_n)^t \in \mathcal{L}(A), a_1 = \cdots = a_{i-1} = 0, a_i \neq 0\}.$$

Weil A rational ist, existiert das Minimum der Absolutwerte $|a_i|$. Wegen der Dreiecksform von $[\mathbf{a}'_1, ..., \mathbf{a}'_j]$ ist $\mathbf{a}'_1, ..., \mathbf{a}'_j$ ein primitives System, und $\mathbf{a}'_1, ..., \mathbf{a}'_n$ ist Basis zu $\mathcal{L}(A)$. $\mathbf{a}' := [\mathbf{a}'_1, ..., \mathbf{a}'_n]$ hat die HNF-Eigenschaften 1. und 2. Um die HNF-Eigenschaft 3. zu sichern, transformiert man $\mathbf{a}'_2, ..., \mathbf{a}'_n$ gemäß

$$\mathbf{a}'_i := \mathbf{a}'_i - \lceil a'_{ij}/a'_{jj} \rceil\, \mathbf{a}'_j \qquad \text{für } j = 1, ..., i-1.$$

Eindeutigkeit der HNF. Die Diagonalelemente a'_{ii} der HNF sind offenbar durch obige Formel eindeutig bestimmt. Angenommen $0 < a'_{ij} < a''_{ij} < a'_{ii}$ sind verschiedene Elemente zweier HNF's mit $j < i$ und i ist minimal gewählt. Dann gilt für $j' < j$ dass $a'_{ij'} = a''_{ij'}$ und es folgt $|a'_{ij} - a''_{ij}| \geq a'_{ii}$, im Widerspruch zu $|a'_{ij} - a''_{ij}| < a'_{ii}$. □

Reelle Matrizen haben im allgemeinen keine HNF, weil die Koordinaten der Gittervektoren kein absolutes Minimum annehmen müssen. Die Basis

$$A := \begin{bmatrix} 1 & \sqrt{2} \\ 3 & 4 \end{bmatrix} \in \mathbb{R}^{2\times 2}.$$

erzeugt ein Gitter $\mathcal{L}(A)$ mit absolut beliebig kleinen ersten Koordinaten der Gittervektoren.

Teilgitter, Untergitter. Sind $\mathcal{L}', \mathcal{L}$ Gitter mit $\mathcal{L}' \subset \mathcal{L}$, so heißt $\mathcal{L}'$ *Teilgitter* von $\mathcal{L}$. Haben $\mathcal{L}'$ und $\mathcal{L}$ gleichen Rang, dann heißt $\mathcal{L}'$ *Untergitter* von $\mathcal{L}$.

Die Basis $A = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$ erzeugt das Untergitter $2\,\mathbb{Z}^2$ von $\mathbb{Z}^2$. Die Faktorgruppe $\mathbb{Z}^2/\mathcal{L}(A)$ besteht aus den vier Äquivalenzklassen, $[\mathbb{Z}^n : \mathcal{L}(A)] = 4$.

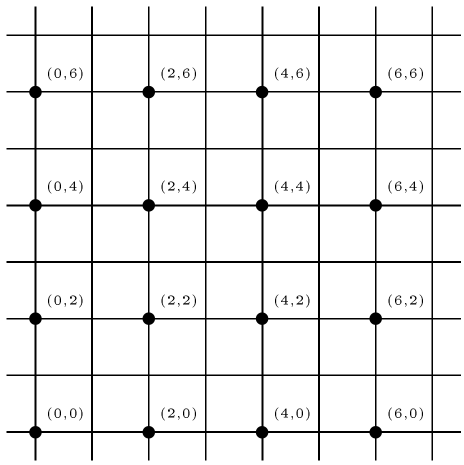

Abbildung 2.1.1: Untergitter $\mathcal{L}(A)$ von $\mathbb{Z}^2$

Lemma 2.1.3
Sei $\mathcal{L} = \mathcal{L}(B)$ Gitter und $\mathcal{L}' = \mathcal{L}(BT)$ Untergitter von $\mathcal{L}$ mit $T \in \mathbb{Z}^{n\times n}$. Dann gilt $\det \mathcal{L}' = \det \mathcal{L} \cdot |\det T|$.

Index des Untergitters. Die ganze Zahl $|\det T| = \frac{\det \mathcal{L}'}{\det \mathcal{L}}$ aus Lemma 2.1.3 ist die Elementzahl und 'Ordnung' der Faktorgruppe $\mathcal{L}/\mathcal{L}'$, genannt der *Index* des Untergitters $\mathcal{L}'$ in $\mathcal{L}$, Bez.: $[\mathcal{L} : \mathcal{L}']$.

Sei $\mathcal{L}' = \mathcal{L}(BT)$ Untergitter von $\mathcal{L} = \mathcal{L}(B)$ und $T = [t_{ij}] \in \mathbb{Z}^{n\times n}$ eine obere (bzw. untere) Dreiecksmatrix. Dann gilt

$$[\mathcal{L} : \mathcal{L}'] = \frac{\det \mathcal{L}'}{\det \mathcal{L}} = \det T = \prod_{i=1}^{n} |t_{ii}|\,.$$

Insbesondere gilt $\mathcal{L}' = \mathcal{L}$ genau dann wenn $|\det T| = 1$.

Korollar 2.1.4
Zu $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$, $b \in \mathbb{N}$ *hat das Gitter* $\mathcal{L}_{\mathbf{a},b} = \{\mathbf{x} \in \mathbb{Z}^n \mid \mathbf{x}^t\mathbf{a} = 0 \pmod b\}$ *die Determinante* $\det \mathcal{L}_{\mathbf{a},b} = b/\operatorname{ggT}(a_1, \ldots, a_n, b)$.

Beweis. $\mathcal{L}_{\mathbf{a},b} \subset \mathbb{Z}^n$ ist offenbar Gitter der Dimension n. Sei O.B.d.A. $\operatorname{ggT}(a_1, ..., a_n, b) = 1$, denn durch Herausdividieren des ggT aus $a_1, ..., a_n, b$ ändert sich $\mathcal{L}_{\mathbf{a},b}$ nicht. Die Faktorgruppe $\mathbb{Z}^n / \mathcal{L}_{\mathbf{a},b}$ besteht den Restklassen

$$R_i := \left\{\mathbf{x} \in \mathbb{Z}^n \;\middle|\; \mathbf{x}^t\mathbf{a} = i \pmod b\right\} \qquad \text{für } i = 0, ..., b-1.$$

Offenbar sind diese Restklassen nicht leer. Es folgt $[\mathbb{Z}_n : \mathcal{L}_{\mathbf{a},b}] = b$ und damit $\det \mathcal{L}_{\mathbf{a},b} = b$. □

Satz 2.1.5
Sei $\mathcal{L}'$ *ein Untergitter von* $\mathcal{L} = \mathcal{L}(B)$. *Dann gibt es eine untere (bzw. obere) Dreiecksmatrix* $T \in \mathbb{Z}^{n\times n}$ *mit* $\mathcal{L}' = \mathcal{L}(BT)$. *Umgekehrt gibt es zu jeder Basis* B' *von* $\mathcal{L}'$ *eine Basis* $\bar{B}$ *von* $\mathcal{L}$ *und eine untere (bzw. obere) Dreiecksmatrix* $T \in \mathbb{Z}^{n\times n}$ *mit* $B' = \bar{B}\,T$.

Beweis. Wir weisen die unteren Dreiecksmatrizen nach, Die oberen Dreiecksmatrizen erhält man durch Transfomation mit Umkehrmatrizen U_n, U_m. Sei $\bar{B}'$ eine beliebige Basis zu $\mathcal{L}'$ und $\bar{B}' = B\,T$ mit $T \in \mathbb{Z}^{n\times n}$. Dann gibt es ein $S \in GL_n(\mathbb{Z})$ so dass $T\,S$ eine HNF von T ist. Es folgt $\bar{B}'S = B(TS)$ und TS ist untere Dreiecksmatrix. Also ist die Basis $B' := \bar{B}'\,S$ von $\mathcal{L}'$ von der gewünschten Form.

Ist umgekehrt B' gegeben und B von der Form $B' = B\,T$, dann wählt man $S \in GL_n(\mathbb{Z})$ so dass $S\,T$ eine untere Dreiecksmatrix ist. Zur Basis B von $\mathcal{L}$ ist dann $B\,S^{-1}$ eine Basis der gewünschten Form. □

Kapitel 3

Sukzessive Minima, Minkowski-Sätze und Hermite-Konstante

Die sukzessiven Minima $\lambda_1 \leq ... \leq \lambda_n$ eines Gitters der Dimension n sind wichtige geometrische Invarianten. Eine Gitterbasis gilt als "reduziert", wenn die Länge des i-ten Vektors proportional zu λ_i ist. Für Gitter $\mathcal{L}$ der Dimension n gilt $\lambda_1 \leq \sqrt{\gamma_n}\,(\det(\mathcal{L})^{\frac{1}{n}}$, dabei ist γ_n die Hermite-Konstante. Die Sätze von Minkowski beschreiben diesen Zusammenhang.

3.1 Sukzessive Minima und erster Satz von Minkowski

Sukzessive Minima. Sei $\|\cdot\|$ eine beliebige Norm. Zu einem Gitter $\mathcal{L} \subset \mathbb{R}^m$ mit $\dim \mathcal{L} = n$ sind die sukzessiven Minima $\lambda_1, \ldots, \lambda_n$ bezüglich der Norm $\|\cdot\|$ definiert durch

$$\lambda_i = \lambda_i(\mathcal{L}) := \inf \left\{ r > 0 \;\middle|\; \begin{array}{l} \text{Es gibt } i \text{ linear unabhängige} \\ \text{Vektoren } \mathbf{c}_1, \ldots, \mathbf{c}_i \in \mathcal{L} \\ \text{mit } \|\mathbf{c}_j\| \leq r \text{ für } j = 1, \ldots, i \end{array} \right\} \qquad \text{für } i = 1, \ldots, n.$$

Offenbar gilt $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$. Die Definition der sukzessiven Minima geht auf H. Minkowski zurück. Wenn nicht anders vermerkt bezieht sich λ_i stets auf die Euklidische Norm, $\lambda_{i,\infty}(\mathcal{L})$ bezieht sich auf die sup-Norm $\|\ \|_\infty$. Die sukzessiven Minima zur Euklidischen Norm sind geometrische Invarianten, sie bleiben bei isometrischen Transformationen erhalten. Die Größe $\lambda_{1,\infty}(\mathcal{L})$ ist keine geometrische Invariante. Für Gitter $\mathcal{L} \subset \mathbb{R}^m$ und $\mathbf{x} \in \mathbb{R}^m$ gilt $\|\mathbf{x}\|_\infty \leq \|\mathbf{x}\| \leq \sqrt{m}\,\|\mathbf{x}\|_\infty$ und somit

$$\lambda_{1,\infty}(\mathcal{L}) \leq \lambda_1(\mathcal{L}) \leq \sqrt{m} \cdot \lambda_{1,\infty}(\mathcal{L}).$$

Die sukzessiven Minima sind Maßstab für die Reduziertheit einer Gitterbasis. Eine Basis gilt als „reduziert“, wenn die Größen $\|\mathbf{b}_i\| / \lambda_i$ für $i = 1, \ldots, n$ „klein“ sind. Für reduzierte Basen sind deren Vektoren nahezu orthogonal. Im allgemeinen gibt es keine Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ mit $\|\mathbf{b}_i\| = \lambda_i$ für $i = 1, \ldots, n$. Betrachte beispielsweise das Gitter $\mathcal{L} := \mathbb{Z}^n + \mathbb{Z}\,(\frac{1}{2}, \ldots, \frac{1}{2})^t$. Für $n \geq 5$ ist$\lambda_1 = \lambda_2 = \cdots = \lambda_n = 1$, doch die kanonischen Einheitsvektoren bilden keine Basis. Damit gibt es keine Basis bestehend aus Vektoren der Länge 1.

Satz 3.1.1 (Minkowski 1896)
Für beliebige Gitter $\mathcal{L}$ mit $\dim \mathcal{L} = n$ gilt $\lambda_{1,\infty}(\mathcal{L}) \leq (\det \mathcal{L})^{\frac{1}{n}}$.

Diese Schranke ist scharf, denn es gilt $\lambda_1(\mathbb{Z}^n) = 1 = (\det \mathbb{Z}^n)^{\frac{1}{n}}$. Aus Satz 3.1.1 folgt $\lambda_1(\mathcal{L}) \leq \sqrt{n} \cdot (\det \mathcal{L})^{\frac{1}{n}}$. Der Beweis zu Satz 3.1.1 benutzt ein Lemma von H.F. Blichfeldt [Blich14]:

Lemma 3.1.2 (Blichfeldt 1914)
Sei $\mathcal{L}$ Gitter und $S \subset \operatorname{span}(\mathcal{L})$ kompakt mit $\operatorname{vol}(S) \geq \det \mathcal{L}$. Dann gibt es ein $\mathbf{b} \in \mathcal{L} \setminus \{\mathbf{0}\}$ mit $S \cap (S + \mathbf{b}) \neq \emptyset$, d.h. es existieren $\mathbf{x}, \mathbf{y} \in S$ mit $\mathbf{x} - \mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}$.

Beweis. Zu $i \in \mathbb{N}$ sind die Mengen $\left(1 + \frac{1}{i}\right) S$ und $\left(1 + \frac{1}{i}\right) S + b_i$ mit $b_i \in \mathcal{L} \setminus \{0\}$ nicht paarweise disjunkt, weil das Volumen von $\left(1 + \frac{1}{i}\right) S$ das der Grundmasche übersteigt. Zu jedem i gibt es ein $b_i \in \mathcal{L} \setminus \{0\}$, so dass der folgende Durchschnitt nicht-leer ist und wir aus ihm $\mathbf{y}_i$ wählen können:

$$\mathbf{y}_i \in \left(1 + \tfrac{1}{i}\right) S \cap \left[\left(1 + \tfrac{1}{i}\right) S + b_i\right] \qquad\qquad i = 1, 2, \ldots$$

Da S kompakt ist, hat die Folge $(\mathbf{y}_i)_{i \in \mathbb{N}}$ einen Häufungspunkt $\mathbf{y} \in S$, so dass eine Teilfolge $\left(\mathbf{b}_{\alpha(i)}\right)_{i \in \mathbb{N}} \subset \mathcal{L}$ gegen $\mathbf{y}$ konvergiert. Die Folge $\left(\mathbf{b}_{\alpha(i)}\right)_{i \in \mathbb{N}} \subset \mathcal{L}$ ist beschränkt und durchläuft nur endlich viele Gitterpunkte. Mindestens ein Gitterpunkt $\mathbf{b} \in \mathcal{L} \setminus \{0\}$ wird unendlich oft durchlaufen. Es folgt: $\mathbf{y} \in S \cap (S + \mathbf{b})$. □

Beweis. [zu Satz 3.1.1] Sei $\mathcal{L} \subset \mathbb{R}^m$ Giite mit $\dim \mathcal{L} = n$. Wir wenden Lemma 3.1.2 an auf den m-dimensionalen Würfel $S \subset \mathbb{R}^m$ mit Kantenlänge $(\det \mathcal{L})^{\frac{1}{n}}$

$$S := \{\mathbf{x} \in \mathbb{R}^m \mid \|\mathbf{x}\|_\infty \leq \tfrac{1}{2}(\det \mathcal{L})^{\frac{1}{n}}\}.$$

Offenbar gilt $\operatorname{vol}(S \cap \operatorname{span}(\mathcal{L})) \geq \det \mathcal{L}$, denn $\operatorname{vol}(S \cap \operatorname{span}(Q\mathcal{L}))$ ist für isometrische Q minimal, wenn $\operatorname{span}(Q\mathcal{L}) = \mathbb{R}^n$, also im Fall $m = n$. Nach Lemma 3.1.2 gibt es ein $\mathbf{b} \in \mathcal{L} \setminus \{0\}$ und ein $\mathbf{y} \in S \cap (S + \mathbf{b})$. Wegen $\mathbf{y}, \mathbf{y} - \mathbf{b} \in S$ gilt

$$\|\mathbf{y}\|_\infty \leq \tfrac{1}{2}(\det \mathcal{L})^{\frac{1}{n}}, \quad \|\mathbf{y} - \mathbf{b}\|_\infty \leq \tfrac{1}{2}(\det \mathcal{L})^{\frac{1}{n}}.$$

Aus der Dreiecksungleichung folgt $\|\mathbf{b}\|_\infty \leq \|\mathbf{y}\|_\infty + \|\mathbf{y} - \mathbf{b}\|_\infty \leq (\det \mathcal{L})^{\frac{1}{n}}$. □

Konvexe, nullsymmetrische Menge. $S \subset \mathbb{R}^m$ heißt konvex, falls mit $\mathbf{x}, \mathbf{y} \in S$ und $\xi \in [0, 1]$ auch $\xi\mathbf{x} + (1 - \xi)\mathbf{y} \in S$ gilt. S heißt nullsymmetrisch, falls mit $\mathbf{x}$ auch $-\mathbf{x}$ in S liegt.

Satz 3.1.1 mit $n = m$ ist ein Spezialfall von Minkowski's Convex Body Theorem.

Satz 3.1.3 (Erster Satz von Minkowski 1893)
Sei $\mathcal{L} \subset \mathbb{R}^n$ ein vollständiges Gitter und $S \subset \mathbb{R}^n$ konvex, nullsymmetrisch, kompakt mit $\operatorname{vol}(S) \geq 2^n \det L$. Dann enthält S mindestens zwei Vektoren $\pm\mathbf{y} \in \mathcal{L}$ ungleich $\mathbf{0}$.

Beweis. Betrachte $\frac{1}{2}S = \left\{\frac{1}{2}\mathbf{x} \;\middle|\; \mathbf{x} \in S\right\} \subset \mathbb{R}^n$. Es gilt $\operatorname{vol}\left(\frac{1}{2}S\right) = 2^{-n} \operatorname{vol}(S) \geq \det \mathcal{L}$. Wir wenden Blichfeldts Lemma 3.1.2 auf $\frac{1}{2}S$ an. Es existiert ein $\mathbf{b} \in \mathcal{L} \setminus \{0\}$ mit $\left(\frac{1}{2}S\right) \cap \left(\frac{1}{2}S + \mathbf{b}\right) \neq \emptyset$. Sei $\mathbf{y}$ im Durchschnitt. Dann gilt $\mathbf{y} \in \frac{1}{2}S$ und $\mathbf{y} = \mathbf{x} + \mathbf{b}$ mit $\mathbf{x} \in \frac{1}{2}S$. Es gilt $\mathbf{b} = \mathbf{y} - \mathbf{x}$ mit $\mathbf{x}, \mathbf{y} \in \frac{1}{2}S$. Weil S nullsymmetrisch und konvex ist, folgt $\mathbf{b} \in S$. □

Satz 3.1.3 angewandt auf $S = \{\mathbf{x} \in \mathbb{R}^m : \|\mathbf{x}\|_\infty \leq \det \mathcal{L}\}$ liefert Satz 3.1.1 für $n = m$, da $\operatorname{vol}(S) = 2^n \det \mathcal{L}$. Satz 3.1.3 liefert folgenden Satz von G. L. Dirichlet [Di1842] über die simultane Approximation reeller Zahlen durch rationale Zahlen.

Satz 3.1.4 (Dirichlet 1842)
Zu beliebigen reellen Zahlen $\alpha_1, \ldots, \alpha_n$ und $\epsilon \in \left]0, \frac{1}{2}\right[$ gibt es ganze Zahlen $p_1, \ldots, p_n$ und q mit $0 < q \leq \epsilon^{-n}$, so dass $|\alpha_i - p_i/q| \leq \epsilon/q$ für $i = 1, \ldots, n$.

Beweis. Wende Satz 3.1.3 an mit $\mathcal{L} = \mathbb{Z}^{n+1}$ und

$$S := \left\{(p_1, \ldots, p_n, q) \in \mathbb{R}^{n+1} \ : \ |q| \le \epsilon^{-n}, \quad |p_i - q\alpha_i| \le \epsilon \text{ für } i = 1, \ldots, n\right\}.$$

S ist ein Quader mit Kantenlänge 2ϵ in den ersten n Richtungen und $2\epsilon^{-n}$ in der letzten,

$$\mathrm{vol}(S) = (2\epsilon)^n 2\epsilon^{-n} = 2^{n+1} \det(\mathbb{Z}^{n+1}).$$

S ist konvex, nullsymmetrisch und kompakt. Nach Satz 3.1.3 gibt es $(p_1, \ldots, p_n, q) \in S \cap \mathbb{Z}^{n+1}$ ungleich $\mathbf{0}$. Es ist $q \neq 0$, weil sonst $(p_1, \ldots, p_n, q) = \mathbf{0}$. Es folgt die Behauptung. □

Dirichlet hat diesen Satz mit dem Schubfachprinzip bewiesen. Dirichlet's Beweis ist wie der obige Beweis inkonstruktiv, er liefert kein Verfahren zur Konstruktion einer Lösung $(p_1, ..., p_n, q)$.

Konstruktion von $(\mathbf{p_1}, ..., \mathbf{p_n}, \mathbf{q})$. Eine Lösung findet man durch Konstruktion eines kürzesten Vektors in der sup-Norm $\| \ \|_\infty$ zum Gitter $\mathcal{L}(B)$ mit folgender Gitterbasis

$$B = \begin{bmatrix} 1 & 0 & \cdots & 0 & \alpha_1 \\ 0 & 1 & \ddots & \vdots & \alpha_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & & 0 & 1 & \alpha_n \\ 0 & \cdots & \cdots & 0 & \epsilon^{n+1} \end{bmatrix} \in \mathbb{Z}^{(n+1)^2}.$$

Es gilt $\det B = \epsilon^{n+1}$ und nach Satz 3.11 gilt $\lambda_{1,\infty}(\mathcal{L}(B)) \le (\det B)^{\frac{1}{n+1}} = \epsilon^{n+1}$. Für jeden $\| \ \|_\infty$-kürzesten Gittervektor $(p_1, ..., p_n, q)$ gilt also $|\,\alpha_i q - p_i\,| \le \epsilon$ und $|q\epsilon^{n+1}| \le \epsilon$ und somit $|q| \le \epsilon^{-n}$.

3.2 Packungsdichte, Hermite-Konstante, kritische Gitter

Es bezeichne $\mathcal{B}_n(\mathbf{b}, r) := \{\mathbf{x} \in \mathrm{span}(\mathcal{L}) \ : \ \|\mathbf{x} - \mathbf{b}\| \le r\}$ die n-dimensionale Kugel mit Radius r mit Mittelpunkt $\mathbf{b}$ in einem geeigneten linearen Raum der Dimension n. Ihr Volumen ist

$$V_n(r) \ := \ \pi^{\frac{n}{2}} r^n / \Gamma(1 + \tfrac{n}{2}) \ \approx \ (\tfrac{2\,e\pi}{n})^{\frac{n}{2}} / \sqrt{\pi n}\ (1 + O(\tfrac{1}{n})). \tag{3.1}$$

Für die Gamma-Funktion gilt $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$ und $\Gamma(n+1) = n!$ für $n \in \mathbb{N}$ und $\Gamma(x+1) = x\ \Gamma(x)$ für $x \in \mathbb{R}^n$. Für $x \in \mathbb{R}_{>0}$ gilt die Stirling'sche Approximation $\Gamma(x+1) = \sqrt{2\pi x}\ (\frac{x}{e})^x\ (1 + O(\frac{1}{x}))$.

Gitterartige Kugelpackung. Die *gitterartige Kugelpackung* $\bigcup_{\mathbf{b} \in \mathcal{L}} \mathcal{B}_n(\mathbf{b}, \lambda_1/2)$ zu $\mathcal{L}$ besteht aus allen Kugeln $\mathcal{B}_n(\mathbf{b}, \lambda_1/2)$ mit Radius $\lambda_1/2$ und Mittelpunkt $\mathbf{b} \in \mathcal{L}$.

Dichte des Gitters. Die (Packungs-)Dichte $\triangle(\mathcal{L})$ des Gitters $\mathcal{L}$ ist der Volumenanteil der Kugeln der gitterartigen Kugelpackung zu $\mathcal{L}$ bezogen auf $\mathrm{span}(\mathcal{L})$,

$$\triangle(\mathcal{L}) =_{\mathrm{def}} \frac{V_n(\lambda_1/2)}{\det \mathcal{L}} = \frac{\lambda_1^n}{\det \mathcal{L}} \frac{V_n(1)}{2^n}.$$

$\triangle(\mathcal{L})$ hängt nur von der Äquivalenklasse von $\mathcal{L}$ ab, bleibt also bei Isometrie und Skalierung erhalten. Für konstante n und λ_1 ist die Dichte maximal, wenn $\det \mathcal{L}$ minimal ist.

Hermite-Konstante. Zum Gitter $\mathcal{L}$ der Dimension n ist $\gamma(\mathcal{L}) := \lambda_1(\mathcal{L})^2 / (\det \mathcal{L})^{\frac{2}{n}}$ die *Hermite-Invariante.* Es gilt $\gamma(\mathcal{L}) = (\triangle(\mathcal{L}) 2^n / V_n(1))^{\frac{2}{n}}$ Die *Hermite-Konstante* γ_n der Dimension n ist

$$\gamma_n := \sup\{\gamma(\mathcal{L}) \mid \mathcal{L} \text{ Gitter mit} \dim \mathcal{L} = n\}.$$

Es genügt das Supremum über die vollständigen Gitter $\mathcal{L}$ mit $\lambda_1(\mathcal{L}) = 1$ (bzw. mit $\det \mathcal{L} = 1$) zu nehmen, denn $\gamma(\mathcal{L})$ bleibt bei Äquivalenz erhalten. Weil geeignet beschränkte Basen dieser Gitter über einen kompakten Bereich des $\mathbb{R}^{n\times n}$ variieren, wird das Supremum angenommen, ist also ein Maximum.

Global extreme, kritische Gitter. Ein Gitter $\mathcal{L} \subset \mathbb{R}^n$ heißt *global extrem* oder *kritisch*, wenn $\gamma(\mathcal{L}) = (\gamma_n)^{\frac{n}{2}}$. Ein Gitter $\mathcal{L}$ mit $\dim(\mathcal{L}) = n$ ist also genau dann kritisch, wenn die gitterartige Kugelpackung zu $\mathcal{L}$ maximale Dichte für die Dimension n hat.

Der analoge Kode zum Gitter $\mathcal{L}$. Nachrichten werden in Gittervektoren $\mathbf{b} \in \mathcal{L}$ kodiert. Die Kodeworte $\mathbf{b} \in \mathcal{L}$ werden mit reellen Fehlervektoren $\mathbf{e} \in \operatorname{span}(\mathcal{L})$ übertragen. Ein gestörtes Kodewort $\mathbf{b} + \mathbf{e}$ ist genau dann eindeutig dekodierbar, wenn $\|\mathbf{e}\| < \lambda_1/2$. Dann ist $\mathbf{b}$ nämlich nächster Gittervektor zu $\mathbf{b} + e$. Mit der Dichte $\triangle(\mathcal{L})$ von $\mathcal{L}$ wächst also das Korrekturpotential des analogen Kodes (bei fester Determinante $\det \mathcal{L}$).

Extreme Gitter. Ein Gitter $\mathcal{L}$ heißt *extrem*, wenn $\lambda_1(\mathcal{L})^2/(\det \mathcal{L})^{\frac{2}{n}}$ bei infinitesimal kleiner Veränderung der Basisvektoren nicht zunimmt. Diese Eigenschaft hängt nicht von der Wahl der Basis von $\mathcal{L}$ ab. Jedes kritische Gitter ist extrem, aber es gibt extreme Gitter, die nicht kritisch sind. Die der Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ eines extremen Gitters zugeordnete Form $F(x_1, \ldots, x_n) := \sum_{i=1}^n \langle \mathbf{b}_i, \mathbf{b}_j \rangle \, x_i x_j$ nennt man *Extremform.*

Wegen $\lambda_1(\mathcal{L}) \le \sqrt{n}\, \lambda_{1,\infty}(\mathcal{L}) \le \sqrt{n}\, (\det \mathcal{L})^{\frac{1}{n}}$ zeigt Satz 3.1.1 dass $\gamma_n \le n$. Diese Schranke kann man mit Satz 3.1.3 verbessern. Wir geben einen direkten Beweis.

Satz 3.2.1
$\gamma_n \le \frac{4}{\pi}\, \Gamma\left(1 + \frac{n}{2}\right)^{\frac{2}{n}} \le \frac{2n}{e\pi} + o(n) \approx 0{,}2342\, n + o(n).$

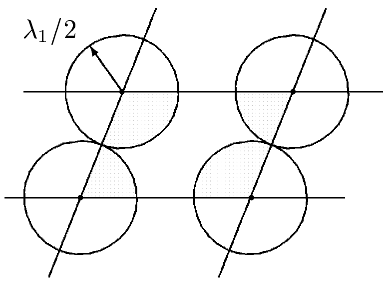

Abbildung 3.2.1: Veranschaulichung von $V_n(\lambda_1/2) < \det \mathcal{L}$

Beweis. Sei $\mathcal{L}$ Gitter mit $\dim(\mathcal{L}) = n$ und $\gamma_n = \lambda_1(\mathcal{L})^2/(\det \mathcal{L})^{\frac{2}{n}}$ sowie $\det \mathcal{L} = 1$. Nach Abbildung 3.2.1 ergeben die 2^n Kugelteile in der Grundmasche des Gitters zusammen gerade eine Kugel vom Radius $\lambda_1/2$. Es folgt $V_n(\lambda_1/2) < \det \mathcal{L} = 1$. Für $r = \Gamma(1 + \frac{n}{2})^{\frac{1}{n}}/\pi^{\frac{1}{2}}$ gilt $V_n(r) = 1$ und somit $\lambda_1 < 2r$. Es folgt $\gamma_n = \lambda_1(\mathcal{L})^2 \le (2r)^2 = \frac{4}{\pi}\, \Gamma\left(1 + \frac{n}{2}\right)^{\frac{2}{n}}$. $\square$

Die obere Schranke $\gamma_n = \frac{2n}{e\pi} + O(1)$ für die Hermite-Konstante aus Satz 3.2.1 hat H.F. Blichfeldt [Blich14] verbessert zu

$$\gamma_n \le \frac{2}{\pi}\, \Gamma\left(2 + \frac{n}{2}\right)^{\frac{2}{n}} \le \frac{n}{e\pi} + \mathrm{o}(n). \tag{3.2}$$

Diese Schranke berücksichtigt, dass im Beweis von Satz 3.2.1 nur ein kleiner Anteil des Raumes von Kugeln mit Radius $\lambda_1/2$ überdeckt wird und schätzt diesen Anteil durch $\left(\sqrt{2} + \mathrm{o}(1)\right)^{-n}$ nach oben ab. Es gilt zum Beispiel $\gamma_{10} \le \frac{2}{\pi}(6!)^{0,2} \approx 2{,}373$. G.A. Kabatiansky und V.I. Levenshtein [KaLe78] zeigen

$$\gamma_n \le \frac{1{,}744}{2e\pi}\, n + \mathrm{o}(n) \approx 0{,}1021\, n + \mathrm{o}(n).$$

Somit ist Minkowskis erster Satz über konvexe Körper, Satz 3.1.3, für die Kugeln nicht optimal. Der folgende Satz von H. Minkowski und E. Hlawka [Hlawka44] angewandt auf Kugeln $S := \mathcal{B}_n(\mathbf{0}, r)$ zeigt

$$\gamma_n \geq \tfrac{1}{\pi}\Gamma(1+\tfrac{n}{2})^{\frac{2}{n}} \geq \tfrac{n}{2\,e\pi} + o(n).$$

Damit gilt für die Hermite-Konstante γ_n

$$\frac{n}{2e\pi} + o(n) \leq \gamma_n \leq \frac{1,744}{2e\pi}\, n + \mathrm{o}(n)\,.$$

Vermutlich sind die Hermite-Konstanten γ_n als Funktion in n monoton wachsend. Weder dies noch die Existenz des Grenzwertes $\lim_{n\to\infty} \gamma_n/n$ ist bewiesen.

Das Volumen einer Menge. Im folgenden bezeichne $\mathrm{vol}(S)$ das elementare Maß von $S \subset \mathbb{R}^n$ nach Riemann und Jordan. $\mathrm{vol}(S)$ ist erklärt, wenn der topologische Rand von S das Lebegues-Maß 0 hat und stimmt dann mit dem Lebesgues-Maß überein.

Satz 3.2.2 (Minkowski, Hlawka)
Zu $S \subset \mathbb{R}^n$ mit $\mathrm{vol}(S) < 1$ gibt es stets ein vollständiges Gitter $\mathcal{L} \subset \mathbb{R}^n$ mit $\det \mathcal{L} = 1$ und $(\mathcal{L} \cap S) \setminus \{\mathbf{0}\} = \emptyset$.

Beweis. Siehe [GrLek87, Theorem 1, Paragraph 19, Kapitel 3]. Der Beweis ist allerdings nicht konstruktiv, es wird nur die Existenz solcher Gitter nachgewiesen, explizite Konstruktionen solcher Gitter sind nicht bekannt. □

Die bekannten Hermite-Konstanten. Die Hermite-Konstanten $\gamma_2, \gamma_3, \gamma_4, \gamma_5$ wurden im 19. Jahrhunderts von C.F. Gauß (γ_3) sowie A. Korkine und G. Zolotareff (γ_4, γ_5) [KoZo1872, KoZo1873, KoZo1877] bestimmt. H.F. Blichfeldt [Blich35] hat $\gamma_6, \gamma_7, \gamma_8$ ermittelt. Blichfeldts Beweis ist kompliziert und wurde von G.L. Watson [Watson66] und N.M. Vetchinkin [Vetchin82] bestätigt. Für $n = 2, \ldots, 8$ sind die kritischen Gitter der Dimension n mit bis auf Äquivalenz (Isometrie und Skalierung) eindeutig bestimmt. Dies wurde von E.S. Barnes [Barnes59] und N.M. Vetchinkin [Vetchin82] bewiesen. Die folgende Übersicht zeigt die bewiesenen $(\gamma_n)^n$, die gerundeten Quotienten von γ_n dividiert durch Blichfeldt's obere Schranke (3.2), sowie kritische Beispiel-Gitter.

n	2	3	4	5	6	7	8
$(\gamma_n)^n$	$\frac{4}{3}$	2	4	8	$\frac{2^6}{3}$	$\frac{2^7}{2}$	2^8
$\gamma_n/\frac{2}{\pi}\,\Gamma(2+\frac{n}{2})^{\frac{2}{n}}$	$0,907$	$0,887$	$0,907$	$0,892$	$0,907$	$0,918$	$0,949$
kritische Gitter	$\mathbb{A}_2$	$\mathbb{A}_3 \cong \mathbb{D}_3$	$\mathbb{D}_4$	$\mathbb{D}_5$	$\mathbb{E}_6$	$\mathbb{E}_7$	$\mathbb{E}_8$

Diese Gitter haben Basen mit besonders einfacher geometrischer Normalform (GNF).

Einfache GNF's der kritischen Gitter. Die kritischen Gitter der Dimension $n = 1, ..., 8$, skaliert zu $\lambda_1 = \sqrt{2}$ haben eine Basis $B_n = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$, so dass für $1 \leq i, j \leq n$ gilt

$$\langle \mathbf{b}_i, \mathbf{b}_j \rangle = \begin{cases} 2 & \text{für } i = j \\ 1 & \text{für } 1 \leq |i-j| \leq 2\,. \\ 0 & \text{sonst} \end{cases} \tag{3.3}$$

Die Gram-Matrizen

$$B_n^t B_n := \begin{bmatrix} 2 & 1 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 1 & 2 & 1 & \ddots & \ddots & & & \vdots \\ 1 & 1 & 2 & \ddots & & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & & & \ddots & \vdots \\ \vdots & \ddots & & & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & & \ddots & 2 & 1 & 1 \\ \vdots & & & \ddots & \ddots & 1 & 2 & 1 \\ 0 & \cdots & \cdots & \cdots & 0 & 1 & 1 & 2 \end{bmatrix} \in \mathbb{Z}^{n\times n}$$

steigen auf $B_1^t B_1 \subset B_2^t B_2 \subset \cdots \subset B_n^t B_n$ charakterisieren die kritischen Gitter der Dimension $n = 1, ..., 8$. Nach Lemma 1.1.4 hat die QR-Zerlegung $B_n = Q_n R_n$ eine eindeutig bestimmte obere Dreiecksmatrix R_n, die GNF von B_n. Es gilt $R_1 \subset R_2 \subset \cdots \subset R_8$ und R_8 hat Form

$$R_8 := \sqrt{2} \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2}\sqrt{3} & \frac{1}{2\sqrt{3}} & \frac{1}{\sqrt{3}} & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{\frac{2}{3}} & \frac{1}{\sqrt{2\cdot 3}} & \frac{1}{2}\sqrt{\frac{3}{2}} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{2}\sqrt{\frac{3}{2}} & \frac{1}{\sqrt{2\cdot 3}} & \sqrt{\frac{2}{3}} \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{3}} & \frac{1}{2}\frac{1}{\sqrt{3}} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{bmatrix}.$$

Für $n = 1, ..., 8$ bezeichne Λ_n das Gitter $\mathcal{L}(R_n)$. Nach Lemma 3.2.3 gilt $\lambda_1(\Lambda_n) = \sqrt{2}$. Man rechnet leicht nach, dass $(\gamma_n)^n = \lambda_1^2/(\det \Lambda_n)^2$ für $i = 1, ..., 8$. Damit realisieren die Gitter $\Lambda_n := \mathcal{L}(R_n)$ für $n = 1, ..., 8$ die Hermite-Konstanten γ_n. Diese Gitter sind somit kritisch und äquivalent sind zu $\mathbb{Z}, \mathbb{A}_2, ..., \mathbb{D}_8$.

Das Schema (3.3) kann nicht auf $n \geq 9$ fortgesetzt werden. Die Matrix $B_9^t B_9$ mit (3.3) ist singulär. Das Gitter Λ_8 ist wegen $\det R_8 = 1$ *selbstdual*, es gilt $\Lambda_8 = (\Lambda_8)^*$. Damit ist jeder Vektor $\mathbf{b} \in \operatorname{span}(\Lambda_8)$ mit $\langle \mathbf{b}_i, \mathbf{b}\rangle \in \mathbb{Z}$ für $i = 1, ..., 8$ bereits in Λ_8. Die für $n = 9$ maximale bekannte Dichte $\triangle(\mathcal{L}(R_9)) = V_9(1)2^{-\frac{9}{2}}$ erfordert eine nicht ganze Erweiterung R_9 von R_8, d.h., $R_8 \subset R_9$ mit $R_9^t R_9 \notin \mathbb{Z}^{9\times 9}$, es gibt aber halbzahlige solche $R_9^t R_9 \in \frac{1}{2}\mathbb{Z}^{9\times 9}$.

Lemma 3.2.3
Für jede ganze Gram-Matrix $B^t B \in \mathbb{Z}^{n\times n}$ mit $\langle \mathbf{b}_i, \mathbf{b}_i\rangle = 2$ gilt $\lambda_1(\mathcal{L}(B)) = \sqrt{2}$.

Beweis. Wegen $\|\mathbf{b}_1\| = \sqrt{2}$ gilt $\lambda_1(\mathcal{L}) \leq \sqrt{2}$. Wir zeigen dass $\|\mathbf{b}\| \geq \sqrt{2}$ für alle $\mathbf{b} = \sum_{i=1}^n t_i \mathbf{b}_i \in \mathcal{L} \setminus \{\mathbf{0}\}$. Aus (3.3) und $(t_1, ..., t_n) \neq \mathbf{0}$ folgt

$$\|\mathbf{b}\|^2 = \|\textstyle\sum_{i=1}^n t_i \mathbf{b}_i\|^2 = \sum_{1\leq i,j\leq n} \langle \mathbf{b}_i, \mathbf{b}_j\rangle\, t_i t_j = \sum_{i=1}^n t_i^2 \langle \mathbf{b}_i, \mathbf{b}_i\rangle + 2\sum_{j<i} t_i t_j \langle \mathbf{b}_i, \mathbf{b}_j\rangle \in 2\,\mathbb{Z}.$$

Es folgt $\|\mathbf{b}\|^2 \geq 2$ und somit $\lambda_1 = \sqrt{2}$. □

Die Konstruktion der Basis R_8 zeigt dass die dichteste Kugelpackung im $\mathbb{R}^n$, $n \leq 8$, die dichteste Kugelpackung im $\mathbb{R}^{n-1}$ erweitert. Die Gitter $\Lambda_1, ..., \Lambda_8$ kann man unabhängig von (3.3) als geschichtete Gitter erzeugen und dieser Prozess ist in beliebige Dimension fortsetzbar. Die Gitter Λ_n für $n = 1, ..., 8$ sind äquivalent zu den geschichteten Gittern Λ_n in [CoSl88] und sind dort zu $\lambda_1 = 2$ skaliert.

Definition 3.2.4
Der Punkt $\mathbf{z} \in \mathrm{span}(\mathcal{L})$ *heißt* tiefes Loch *des Gitters* $\mathcal{L}$, *wenn*

$$\|\mathbf{z} - \mathcal{L}\| = \max\{\|z' - \mathcal{L}\| \,:\, z' \in \mathrm{span}(L)\}.$$

Der Abstand $\|\mathbf{z} - \mathcal{L}\| = \min\{\|\mathbf{z} - \mathbf{y}\| \,:\, \mathbf{y} \in \mathcal{L}\}$ *zum tiefen Loch* $\mathbf{z}$ *ist der* Überdeckungsradius *(covering radius) von* $\mathcal{L}$.

Definition 3.2.5
Das Gitter $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ *ist* geschichtet *(laminated) bezüglich* $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$, *wenn* $\mathbf{b}_n - \widehat{\mathbf{b}}_n \in \mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$ *tiefes Loch des Gitters* $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$ *ist.*

Die Gitter Λ_n für $n = 1, ..., 8$ sind geschichtet. Zu ihrer Konstruktion, wählen wir $(1, 0, \ldots, 0) \in \mathbb{R}^n$ und $\mathbf{b}_2, \ldots, \mathbf{b}_n$ so, dass jeweils $\mathbf{b}_n - \widehat{\mathbf{b}}_n$ tiefes Loch von $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$ ist und $\|\mathbf{b}_n\|^2 = 2$. Offenbar liefert diese Konstruktion geschichtete Gitter Λ_n beliebiger Dimension. Für $n = 11, 12, 13$ und $n > 24$ gibt es jedoch mehrere Isometrieklassen, siehe [CoSl88] Figur 6.1.

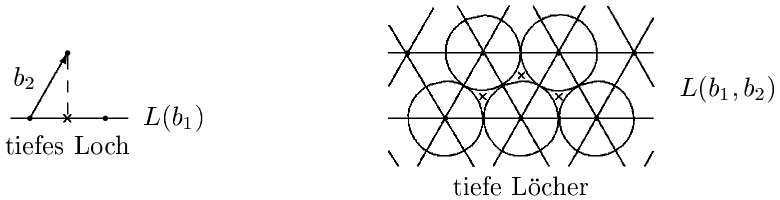

Abbildung 3.2.2: Tiefe Löcher in Λ_1 und Λ_2

3.2.1 Allgemeine Minkowski-Ungleichungen.

Die folgende Ungleichung von H. Minkowski verschärft die Ungleichung $\lambda_1^2 \leq \gamma_n (\det \mathcal{L})^{\frac{2}{n}}$.

Satz 3.2.6 (Minkowski'sche Ungleichung)
Für jedes Gitter $\mathcal{L}$ *mit* $\dim \mathcal{L} = n$ *gilt* $\prod_{i=1}^n \lambda_i(\mathcal{L}) \leq (\gamma_n)^{\frac{n}{2}} \det \mathcal{L}$.

Für kritische Gitter $\mathcal{L}$ gilt $\lambda_1^n = (\gamma_n)^{\frac{n}{2}} \det \mathcal{L}$, wegen $\lambda_i \geq \lambda_1$ folgt somit $\lambda_1 = \lambda_2 = \cdots = \lambda_n$.

Beweis. Seien $\mathbf{a}_1, ..., \mathbf{a}_n \in \mathcal{L}$ linear unabhängige Vektoren, so dass

$$\|\mathbf{a}_i\| = \lambda_i \qquad \text{für } i = 1, \ldots, n.$$

$\mathcal{L}_1 = \mathcal{L}(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ ist ein Untergitter von $\mathcal{L}$. Wähle die Basis $\mathbf{b}_1, ..., \mathbf{b}_n$ von $\mathcal{L}$ so dass mit einer oberen Dreiecksmatrix $T \in M_{n,n}(\mathbb{Z})$ nach Satz 2.1.4 gilt $[\mathbf{b}_1, \ldots, \mathbf{b}_n]\, T = [\mathbf{a}_1, \ldots, \mathbf{a}_n]$.

Für alle $\mathbf{b} \in \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ und $s = 2, ..., n$ gilt dann

$$b \notin \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{s-1}) \quad \Longrightarrow \quad \|\mathbf{b}\| \geq \lambda_s. \tag{3.4}$$

Denn aus $\mathbf{b} \notin \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{s-1})$ und $\mathbf{b} \in \mathcal{L}$ folgt $\mathbf{b} \notin \operatorname{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{s-1}) = \operatorname{span}(_1, \ldots, _{s-1})$ und somit $\|\mathbf{b}\| \geq \lambda_s$.

Wir setzen $\bar{\mathbf{b}}_i := \sum_{j=1}^{i} \mu_{i,j} \widehat{\mathbf{b}}_j / \lambda_j$ für $i = 1, \ldots, n$ und betrachten das Gitter $\bar{\mathcal{L}} := \mathcal{L}\left(\bar{\mathbf{b}}_1, \ldots, \bar{\mathbf{b}}_n\right)$. Wir zeigen $\lambda_1(\bar{\mathcal{L}}) \geq 1$.

Sei $\bar{\mathbf{b}} := \sum_{i=1}^{s} t_i \bar{\mathbf{b}}_i \in \bar{\mathcal{L}} \setminus \{\mathbf{0}\}$ ein beliebiger Vektor und $\mathbf{b} := \sum_{i=1}^{s} t_i \mathbf{b}_i$. Dann gilt

$$\left\|\bar{\mathbf{b}}\right\|^2 = \sum_{j=1}^{s} (\sum_{i=j}^{s} t_i \mu_{i,j})^2 \|\widehat{\mathbf{b}}_j\|^2 \lambda_j^{-2} \geq \sum_{j=1}^{s} (\sum_{i=j}^{s} t_i \mu_{i,j})^2 \|\widehat{\mathbf{b}}_j\|^2 \lambda_s^{-2} = \lambda_s^{-2} \|\mathbf{b}\|^2,$$

so dass wegen (3.4) und $t_s \neq 0$ die Behauptung $\|\bar{\mathbf{b}}\|^2 \geq 1$ und damit $\lambda_1(\bar{\mathcal{L}}) \geq 1$ folgt.

Aus $\det \bar{\mathcal{L}} = \det \mathcal{L} / \prod_{i=1}^{n} \lambda_i$ sowie $\lambda_1(\bar{\mathcal{L}}) \geq 1$ und nach Definition von γ_n folgt

$$1 \leq \lambda_1 \left(\bar{\mathcal{L}}\right)^2 \leq \gamma_n \left(\det \bar{\mathcal{L}}\right)^{\frac{2}{n}} = \gamma_n (\det \mathcal{L})^{\frac{2}{n}} \left(\prod_{i=1}^{n} \lambda_i\right)^{-\frac{2}{n}}.$$

Erhebt man diese Ungleichung in die Potenz $\frac{n}{2}$ und multipliziert mit $\prod_{i=1}^{n} \lambda_i$, so folgt die Behauptung $\prod_{i=1}^{n} \lambda_i(\mathcal{L}) \leq (\gamma_n)^{\frac{n}{2}} \det \mathcal{L}$. □

Satz 3.2.7
Für jedes Gitter $\mathcal{L}$ mit $\dim \mathcal{L} = n$ *gilt* $\prod_{i=1}^{n} \lambda_i \geq \det \mathcal{L}$.

Beweis. Seien $a_1, \ldots, a_n$ linear unabhängige Gittervektoren mit $\|a_i\| = \lambda_i$ für $i = 1, \ldots, n$. Weil $\mathcal{L}(a_1, \ldots, a_n)$ ein Untergitter von $\mathcal{L}$ ist, gilt $\det \mathcal{L}(a_1, \ldots, a_n) \geq \det \mathcal{L}$.

Andererseits gilt nach der Ungleichung von Hadamard $\prod_{i=1}^{n} \|a_i\| \geq \det \mathcal{L}(a_1, \ldots, a_n)$.
Somit folgt die Behauptung $\prod_{i=1}^{n} \lambda_i \geq \det \mathcal{L}$. □

Minkowski-Sätze für beliebige Normen. Die Sätze von Minkowski gelten allgemein für beliebige Normen $\| \ \|$, siehe u.a. [GrLek87, Siegel89]. Sei $\| \ \| : \mathbb{R}^m \to \mathbb{R}$ eine beliebige Norm. Wir ordnen der Norm $\| \ \|$ ihren *Eichkörper* $K \subset \mathbb{R}^m$ zu gemäß $K := \{x \in \mathbb{R}^m \ : \ \|x\| \leq 1\}$.

Der Eichkörper zur ℓ_2-Norm ist $K := \left\{(x_1, \ldots, x_n) \in \mathbb{R}^n \ : \ x_1^2 + x_2^2 + \cdots + x_n^2 \leq 1\right\}$.

Der Eichkörper zur sup-Norm ist $K := \{(x_1, \ldots, x_n) \in \mathbb{R}^n \ : \ |x_i| \leq 1 \text{ für } i = 1, \ldots, n\}$.

Satz 3.2.8 (Erster Satz von Minkowski)
Für beliebige Norm $\| \ \|$ mit Eichkörper $K \subset \mathbb{R}^m$ und $\operatorname{vol}(K) \geq 2^m$ *gilt* $\lambda_{1, \| \ \|}(\mathbb{Z}^m) \leq 1$.

Beweis. Siehe [Siegel89, Theoreme 10 und 11]. □

Die Aussage von Satz 3.3.1 kann man verschärfen zum zweiten Satz von Minkowski:

Satz 3.2.9 (Zweiter Satz von Minkowski 1907)
Seien $\lambda_1, \ldots, \lambda_n$ die sukzessiven Minima des Gitters $\mathbb{Z}^n$ bezüglich einer beliebigen Norm mit Eichkörper $K \subset \mathbb{R}^n$, dann gilt $1/n! \leq \prod_{i=1}^{n} \lambda_i \operatorname{vol}(K) 2^{-n} \leq 1$.

Beweis. Siehe Paragraph 9.1 in Kapitel 2 in [GrLek87]. Für die obere Schranke siehe auch Theorem 16 [Siegel89]. □

Hieraus erhält man die Minkowski'sche Ungleichung für beliebige Normen:

Satz 3.2.10
Seien $\lambda_1, \dots, \lambda_n$ die sukzessiven Minima des vollständigen Gitters $\mathcal{L} \subset \mathbb{R}^n$ bezüglich einer beliebigen Norm mit Eichkörper $K \subset \mathbb{R}^n$. Dann gilt $\det \mathcal{L}/n! \leq \prod_{i=1}^n \lambda_i \operatorname{vol}(K)\, 2^{-n} \leq \det \mathcal{L}$.

Im Fall der sup-Norm, d.h. für $K := \{(x_1, \dots, x_n) \in \mathbb{R}^n \ : \ |x_i| \leq 1 \text{ für } i = 1, \dots, n\}$, gilt $\operatorname{vol}(K) = 2^n$. Für vollständige Gitter $\mathcal{L} \subset \mathbb{R}^n$ gilt somit $\prod_{i=1}^n \lambda_{i,\infty} \leq \det \mathcal{L}$.

Kapitel 4

Gauß-Reduktion

Ziel ist es, für Gitter der Dimension 2 eine Basis a, b zu finden, bestehend aus einem kürzesten Vektor $a \neq 0$ und einem dazu kürzesten, linear unabhängigen Vektor b. Für beliebige Norm $\| \ \|$ sind dies genau die Basen mit $\|a\| \leq \|b\| \leq \|a \pm b\|$. Wir behandeln Reduktionsverfahren, erst für die Euklidische Norm dann für eine allgemeine Norm.

4.1 Reduzierte Basis

Reduzierte Basis. Sei $\| \ \| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ eine beliebige Norm. Eine geordnete Gitterbasis $a, b \in \mathbb{R}^n$ ist *reduziert* bezüglich der Norm $\|\cdot\|$ wenn $\|a\| \leq \|b\| \leq \|a \pm b\|$.

Ist die Basis a, b reduziert, so sind auch $\pm a, \pm b$ reduzierte Basen des Gitters $L(a, b)$. Abgesehen von Ausnahmegittern gibt es nur diese vier reduzierten Basen. Die Basen $\pm a, \pm b$ sind in natürlicher Weise äquivalent. Wir nennen zwei Basen a, b und a', b' *äquivalent*, wenn $a = \pm a'$, $b = \pm b'$. Zwei der reduzierten Basen $\pm a, \pm b$ erfüllen die Zusatzbedingung $\|a - b\| \leq \|a + b\|$. Der folgende Satz gilt für eine allgemeine Norm $\| \ \|$.

Satz 4.1.1
Für jede reduzierte Basis $a, b \in \mathbb{R}^n$ ist a ein kürzester Gittervektor $\neq 0$ und b ein dazu linear unabhängiger kürzester Gittervektor.

Beweis. Zu zeigen ist für allgemeine Norm

$$\begin{aligned} \|a\| &\leq \|ra + sb\| && \text{for all}(r, s) \in \mathbb{Z}^2 \setminus \{(0, 0)\}, \\ \|b\| &\leq \|ra + sb\| && \text{for all}(r, s) \in \mathbb{Z}^2 \setminus \{(0, 0), (1, 0)\}, s \neq 0. \end{aligned}$$

Abb. 4.1.1 illustriert die Lage einer reduzierten Basis a, b. Betrachte das Parallelepiped $\mathcal{P}$ mit den Eckpunkten $\pm a \pm b$. Die Reduktionsbedingungen bedeuten, dass auf jeder der vier dicken Kanten von $\mathcal{P}$ der mittlere Gitterpunkt $\pm a$, $\pm b$ minimale Norm gegenüber den beiden Eckpunkten hat:

$$\begin{array}{ccccc} \|\pm a - b\| & \geq & \|\pm a\| & \leq & \|\pm a + b\| \\ \|-a \pm b\| & \geq & \|\pm b\| & \leq & \|a \pm a\|. \end{array}$$

Für eine allgemeine Norm und $c > 0$ ist der Bereich der Vektoren $K_c = \{x \mid \|x\| \leq c\}$ konvex. Wegen dieser Konvexität hat die Norm auf jeder der vier Grenzgeraden von $\mathcal{P}$, den Geraden $\pm a + tb$, $\pm b + ta$ für $t \in \mathbb{R}$, ihr Minimum jeweils auf der Kante des Randes von $\mathcal{P}$. Damit nimmt die Norm in jedem der vier gepunkteten Bereiche der Abb. 4.1.1 ihr Minimum im jeweiligen Eckpunkt $\pm a \pm b$ an. Daher sind a, b offenbar zwei kleinste, linear unabhängige Gitterpunkte. ∎

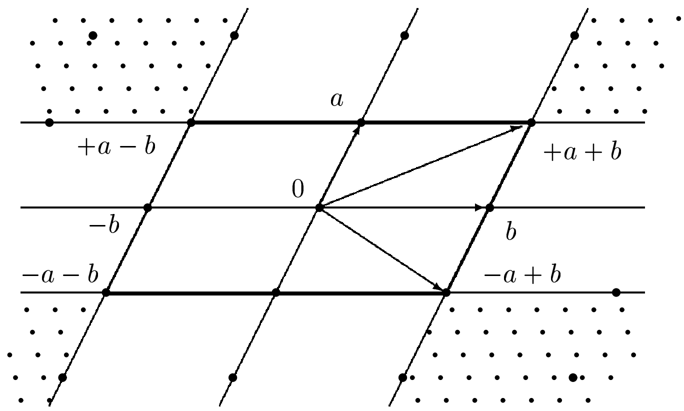

Abbildung 4.1.1: Reduzierte Basis a, b

4.2 Reduktionsverfahren für die Euklidische Norm

Für die Euklidischen Norm $\|x\| = \sqrt{x^\top x}$ gilt offenbar mit $\mu_{2,1} = a^\top b \, \|a\|^{-2}$ dass

$$\begin{array}{rclcrcl} \mu_{2,1} & \leq & \frac{1}{2} & \Longleftrightarrow & \|b\| & \leq & \|a-b\|\,, \\ \mu_{2,1} & \geq & 0 & \Longleftrightarrow & \|a-b\| & \leq & \|a+b\|\,. \end{array}$$

Damit ist die Basis a, b genau dann reduziert, wenn $\|a\| \leq \|b\|\,,\ |\mu_{2,1}| \leq \frac{1}{2}$. Wir betrachten nur reduzierte Basen mit der Zusatzbedingung $\mu_{2,1} \geq 0$.

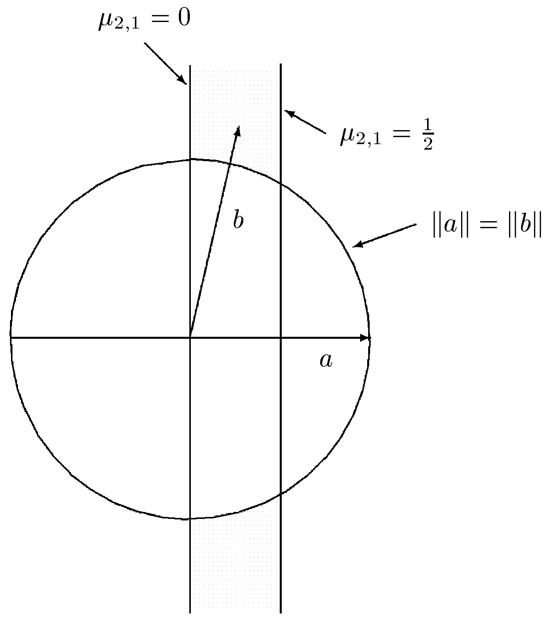

Abbildung 4.2.1: Bereich der reduzierten Basen a, b mit $\mu_{2,1} \geq 0$

Abbildung 4.2.1 zeigt zu festem a den gepunkteten Bereich der Vektoren b der reduzierten Basen a, b mit $\mu_{2,1} \geq 0$. Sei $\phi = \angle(a, b)$ der Winkel zwischen den Gittervektoren a, b, $\cos\phi = \frac{a^\top b}{\|a\| \cdot \|b\|}$. Für reduzierte Basen a, b gilt $60^\circ \leq \phi \leq 90^\circ$.

Im Fall $\mu_{2,1} = \frac{1}{2}$ ist mit a, b auch $a, a-b$ reduziert. Im Fall $\|a\| = \|b\|$ ist mit a, b auch b, a reduziert. In den übrigen Fällen gibt es nur die reduzierten Basen $\pm a, \pm b$.

Algorithmus 4.2.1 Gauß-Reduktionsverfahren für die Euklidische Norm

EINGABE: Gitterbasis $b_1, b_2 \in \mathbb{R}^n$ mit $\|b_1\| \leq \|b_2\|$

WHILE $|\mu_{2,1}| > \frac{1}{2}$ DO /* $\mu_{2,1} = b_1^\top b_2 \|b_1\|^{-2}$ */

1. $b_2 := b_2 \cdot \operatorname{sign}(\mu_{2,1})$ /* wir erreichen $\mu_{2,1} \geq 0$ */

2. $b_2 := b_2 - \lceil \mu_{2,1} \rfloor b_1$

3. IF $\|b_1\| > \|b_2\|$ THEN vertausche b_1 und b_2

AUSGABE: Reduzierte Basis b_1, b_2

Eine *Runde* der Schritte **1. 2. 3.** sichert in Schritt **1.** durch Vorzeichenwahl von b_2 dass $\mu_{2,1} \geq 0$, reduziert in Schritt **2.** gemäß $b_2 := b_2 - \lceil \mu_{2,1} \rfloor b_1$ und vertauscht in Schritt **3.** sofern nicht schon $\|b_1\| \leq \|b_2\|$ gilt. Nach Schritt **1.** gilt stets $\|b_1\| \leq \|b_2\|$ und $\mu_{2,1} \geq 0$. Die Schritte **2. 3.** lauten bei Vertauschung in Matrizenschreibweise

$$[b_1, b_2] := [b_1, b_2] \begin{bmatrix} -\lceil \mu_{2,1} \rfloor & 1 \\ 1 & 0 \end{bmatrix}.$$

In Schritt **3.** wird bis auf die letzte Runde notwendigerweise vertauscht.

Zu gegebener reduzierten Ausgabebasis b_1, b_2 und Rundenzahl k der Gauß-Reduktion identifizieren wir eine *minimale* Eingabebasis, welche in k Runden auf b_1, b_2 reduziert wird. Die Minimalität der Basis bedeutet, dass ihre Vektoren minimale Länge haben. Eine solche Eingabebasis heißt eine *minimale k-te Vorgängerbasis* zu b_1, b_2.

Satz 4.2.1

1. *Zur reduzierten Basis b_1, b_2 und Rundenzahl k ist $[b_1, b_2]\, A_k$ minimale k-te Vorgängerbasis mit*

$$A_k =_{def} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^{k-2} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

2. *Algorithmus 4.2.1 macht zur Eingabe b_1, b_2 höchstens* $\log_{1+\sqrt{2}}(\|b_1\| / \lambda_2) + 2.54$ *Runden.*

Wohlgeordnete Basis. Eine Basis b_1, b_2 heißt zur Euklidischen Norm *wohlgeordnet* wenn $\|b_1\| \leq \|b_2\|$ und $\mu_{2,1} > \frac{1}{2}$. Dabei ist im Falle $\|b_1\| \leq \|b_2\|$ die Bedingung $\mu_{2,1} > \frac{1}{2}$ gleichbedeutend mit $\|b_2 - b_1\| < \|b_2 + b_1\|$. In Schritt **1.** wird also eine wohlgeordnete Basis erzeugt, es sei denn die Basis ist schon reduziert. Offenbar gelten folgende Aussagen.

Lemma 4.2.2

Für jede nicht reduzierte Basis mit $\|b_1\| \leq \|b_2\|$ ist genau eine der Basen $b_1, \pm b_2$ wohlgeordnet.

Lemma 4.2.3

*Wendet man die Schritte **2. 3.** an auf zwei aquivalente Basen b_1, b_2 und b_1', b_2', so bleibt die Äquivalenz erhalten.*

Wegen Lemma 4.2.3 gibt es zu gegebener reduzierten Basis eine minimale k-te Vorgängerbasis, bei deren Reduktion das Vorzeichen von b_2 in Schritt **1.** nie verändert wird. Dies folgt aus dem Lemma, weil äquivalente Basen in der Länge der Vektoren gleich sind.

Die Gauß-Reduktion mit k Runden erzeugt in Schritt **1.** eine Folge wohlgeordneter Basen (b_{k+1}, b_{k+2}), $(b_k, b_{k+1}), \ldots, (b_2, b_3)$ und schließlich die reduzierte Basis (b_1, b_2). Bleibt das Vorzeichen von b_2 in Schritt **1.** stets unverändert, und wird in der letzten Runde in Schritt **3.** getauscht, dann ist die k-te Vorgängerbasis (b_{k+1}, b_{k+2}) zur reduzierten Basis (b_1, b_2) von der Form

$$[b_k, b_{k+1}] = [b_1, b_2] \prod_{i=1,\dots,k} \begin{bmatrix} 0 & 1 \\ 1 & \mu^{(i)} \end{bmatrix}.$$

Dabei ist $\mu^{(i)} = \lceil \mu_{2,1} \rfloor$ der ganzzahlige Reduktionskoeffizient der i-ten Runde. Die behauptete Form von (b_{k+1}, b_{k+2}) folgt, weil $\begin{bmatrix} 0 & 1 \\ 1 & \mu^{(i)} \end{bmatrix}$ die Inverse zur Matrix $\begin{bmatrix} -\mu^{(i)} & 1 \\ 1 & 0 \end{bmatrix}$ ist, welche die Schritte **2.** **3.** beschreibt. Wegen $\mu_{2,1} > \frac{1}{2}$ gilt $\mu^{(i)} \geq 1$.

Lemma 4.2.4
Sei $b_1, b_2 \in \mathbb{R}^n$ wohlgeordnete Basis, welche durch die Schritte **2.** **3.** *in die wohlgeordnete Basis $b_1' = b_2 - \lceil \mu_{2,1} \rfloor b_1$, $b_2' = b_1$ transformiert wird. Im Fall $\angle(b_1, b_1') < 30^o$ gilt $\mu_{2,1}' > \frac{3}{2}$.*
Im Fall $\angle(b_1, b_1') \geq 30^o$ gibt es eine reduzierte Basis bestehend aus den Vektoren $b_1', b_2', b_2' - b_1'$.

Das Lemma zeigt, dass der ganzzahlige Reduktionskoeffizient $\mu^{(i)} = \lceil \mu_{2,1} \rfloor$ stets mindestens 2 ist, ausgenommen die erste und letzte Runde.

Beweis. Wir betrachten nur den Fall dass $\langle b_1, b_1' \rangle \|b_1\|^{-2} = \frac{1}{2}$, weil dann $\|b_1'\| / \|b_1\|$ maximal ist.

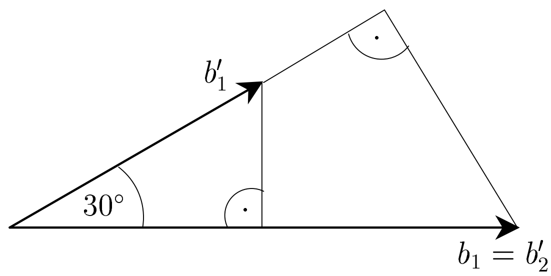

Abbildung 4.2.2: Der Fall $\angle(b_1, b_1') = 30^o$, $\langle b_1, b_1' \rangle \|b_1\|^{-2} = \frac{1}{2}$

Im Fall $\angle(b_1, b_1') = 30^o$ gilt $\frac{3}{4}\|b_1'\|^2 = \frac{1}{4}\|b_1\|^2$. Daher gilt im Falle $\angle(b_1, b_1') < 30^o$ offenbar $\|b_1\|^2 < 3\,\|b_1'\|^2$. Es folgt die Behauptung

$$\mu_{2,1}' = \langle b_1, b_1' \rangle \|b_1'\|^{-2} \geq 3\,\langle b_1, b_1' \rangle \|b_1\|^{-2} > \tfrac{3}{2}.$$

Im Falle $\angle(b_1, b_1') > 30^o$ gilt $\frac{1}{2} < \mu_{2,1}' < \frac{3}{2}$. Sofern die Basis b_1', b_2' nicht schon reduziert ist, wird in der nächsten Runde $b_2' - b_1'$ gebildet und die Reduktion bricht ab. ■

Beweis von Satz 4.2.1. Betrachte nun den Fall dass $(b_2, b_3) = (b_1', b_2')$ direkte Vorgängerbasis ist zur reduzierten Basis b_1, b_2 gemäß Lemma 4.2.4. Es sei also b_1, b_2 eine Auswahl von $b_1', b_2', b_2' - b_1'$. Dann ist

$$[b_{k+1}, b_{k+2}] = [b_1, b_2] \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^{k-2} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

eine minimale k-te Vorgängerbasis (b_{k+1}, b_{k+2}) zur reduzierten Basis (b_1, b_2). Wegen Lemma 4.2.4 gilt nämlich $\mu^{(i)} \geq 2$ für die ganzzahligen Reduktionskoeffizienten mit $1 < i < k$ und $\mu^{(1)} = \mu^{(k)} = 1$. Offenbar wird b_{k+1}, b_{k+2} minimal, wenn in der letzten Runde in Schritt **3.** getauscht wird.

Die Koeffizienten a_k der Matrix $\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^k = \begin{bmatrix} a_{k-2} & a_{k-1} \\ a_{k-1} & a_k \end{bmatrix}$ genügen der Rekursion $a_0 = 0, a_1 = 1, a_2 = 2$ und $a_k = 5\,a_{k-2} + 2\,a_{k-3}$ für $k \geq 3$. Es gilt $2a_{k-3} + a_{k-2} \geq 1.5\,(1+\sqrt{2})^{k-3}$.

Somit gilt
$$[b_{k+1}, b_{k+2}]\,[b_{k+1}, b_{k+2}]^\top = A_k\ [b_1, b_2]^\top [b_1, b_2] A_k^\top$$
für die Matrix $A_k = \begin{bmatrix} a_{k-2} & a_{k-2} + a_{k-3} \\ a_{k-4} + a_{k-3} & a_{k-4} + 2a_{k-3} + a_{k-2} \end{bmatrix}$. Wegen $\langle b_1, b_2 \rangle \geq 0$ folgt
$$\|b_{k+1}\| \geq (a_{k-4} + 2a_{k-3} + a_{k-2})\|b_2\| \geq 1.5\,(1+\sqrt{2})^{k-3}\,\lambda_2.$$
Somit gilt $k \leq 2.54 + \log_{1+\sqrt{2}}(\|b_{k+1}\|/\lambda_2)$, weil $2.54 > 3 - \log 1.5/\log(1+\sqrt{2})$. ■

Algorithmus 4.2.2 Gauß-Reduktionsverfahren für beliebige Norm

EINGABE: Gitterbasis $b_1, b_2 \in \mathbb{R}^n$ mit $\|b_1\| \leq \|b_2\|$

WHILE $\|b_2\| > \|b_1 - b_2\|$ DO

1. IF $\|b_1 + b_2\| < \|b_1 - b_2\|$ THEN $b_2 := -b_2$

2. $b_2 := b_2 - \mu b_1$ mit $\mu \in \mathbb{Z}$ derart, dass $\|b_2 - \mu b_1\|$ minimal ist

3. IF $\|b_1\| > \|b_2\|$ THEN vertausche b_1 und b_2

AUSGABE: Reduzierte Basis b_1, b_2

Nach Schritt **1.** gilt $\|b_1\| \leq \|b_2\|$, $\|b_1 - b_2\| < \|b_1 + b_2\|$, es sei denn dass b_1, b_2 schon reduziert ist. Eine Basis mit $\|b_1\| \leq \|b_2\|$, $\|b_1 - b_2\| < \|b_1 + b_2\|$ nennen wir *wohlgeordnet*. Die Bedingung $\|b_1 - b_2\| < \|b_1 + b_2\|$ lautet im speziellen Fall der Euklidischen Norm $\mu_{2,1} > \frac{1}{2}$.

Die Rundenzahl für dieses Verfahren ist beschränkt durch $\log_{1+\sqrt{2}}(\|b_1\|/\lambda_{2,\|\ \|}) + \mathcal{O}(1)$. Dabei ist $\lambda_{2,\|\ \|}$ das zweite sukzessive Minimum zur Norm $\|\ \|$. Eine ausführliche Analyse findet sich in [KaSchn96] von M. Kaib und C.P. Schnorr sowie in M. Kaibs Dissertation [Kaib94]. Dort werden effiziente Algorithmen für den Schritt **2.** in der l_1- und sup-Norm vorgestellt.

Kapitel 5

LLL-reduzierte Gitterbasen

Der LLL-Reduktionsbegriff für geordnete Gitterbasen $b_1, \ldots, b_n \in \mathbb{R}^m$ beliebigen Ranges n wurde 1982 von A.K. Lenstra, H.W. Lenstra und L. Lovász [LLL82] vorgeschlagen. Das Verfahren zur LLL-Reduktion ist das erste Reduktionsverfahren für ganzzahlige Gitterbasen mit einer polynomiellen Laufzeit. Es basiert auf der Gauß-Reduktion in Dimension $n = 2$.

5.1 Definition und Eigenschaften

Wir führen den Begriff der LLL-reduzierten Basis ein und zeigen, dass die Längen der Basisvektoren die sukzessiven Minima des Gitters grob approximieren. Seien $\widehat{b}_1, ..., \widehat{b}_n$ das der Basis $b_1, ..., b_n$ zugeordnete Orthogonalsystem und $\mu_{i,j}$ die Gram-Schmidt-Koeffizienten.

Definition 5.1.1 (LLL-reduzierte Basis)
Eine geordnete Gitterbasis $b_1, ..., b_n \in \mathbb{R}^m$ heißt LLL-reduziert *mit δ, $\frac{1}{4} < \delta \leq 1$, wenn*

1. $|\mu_{i,j}| \leq \frac{1}{2}$ *für* $1 \leq j < i \leq n$,
2. $\delta \, \|\widehat{b}_{k-1}\|^2 \leq \|\widehat{b}_k\|^2 + \mu_{k,k-1}^2 \, \|\widehat{b}_{k-1}\|^2$ *für* $k = 2, \ldots, n$.

Basen mit der Eigenschaft *1.* heißen *längenreduziert.* Der Parameter δ kontrolliert die Güte der reduzierten Basis: je kleiner δ um so schwächer ist die Reduktion. A.K. Lenstra, H.W. Lenstra und L. Lovász [LLL82] studieren die LLL-Reduktion speziell für den Parameter $\delta = \frac{3}{4}$. Für $\delta < 1$ hat das LLL-Reduktionsverfahren polynomielle Laufzeit.

Für $\delta = 1$ und $n = 2$ ist eine Basis LLL-reduziert mit δ genau dann wenn sie Gauß-reduziert ist. Mit der orthogonalen Projektion $\pi_k : \mathbb{R}^m \to \operatorname{span}(b_1, ..., b_{k-1})^{\perp}$ ist die Bedingung $\delta \, \|\widehat{b}_{k-1}\|^2 \leq \|\widehat{b}_k\|^2 + \mu_{k,k-1}^2 \, \|\widehat{b}_{k-1}\|^2$ äquivalent zu $\delta \, \|\pi_{k-1}(b_{k-1})\|^2 \leq \|\pi_{k-1}(b_k)\|^2$. Eine Basis $b_1, ..., b_n$ ist somit LLL-reduziert mit δ wenn sie längenreduziert ist und wenn die Basen $\pi_{k-1}(b_{k-1}), \pi_{k-1}(b_k)$ LLL-reduziert sind mit δ. Letzteres bedeutet dass die Spalten der 2×2-Matrix $\begin{bmatrix} \|\widehat{b}_{k-1}\| & \mu_{k,k-1}\|\widehat{b}_{k-1}\| \\ 0 & \|\widehat{b}_k\| \end{bmatrix}$ LLL-reduziert sind mit δ.

Lemma 5.1.2
Ist $b_1, ..., b_n$ LLL-reduziert mit δ, dann gilt mit $\alpha = (\delta - \frac{1}{4})^{-1}$ dass

$$\|\widehat{b}_i\|^2 \leq \alpha^{j-i} \, \|\widehat{b}_j\|^2 \quad \textit{für } 1 \leq i \leq j \leq n.$$

Für $\delta = \frac{3}{4}$, $\alpha = 2$, $i = 1$ gilt $\|b_1\|^2 \leq 2^{j-1}\,\|\widehat{b}_j\|^2$, so dass die Längenquadrate $\|\widehat{b}_j\|^2$ für große j nicht beliebig klein werden.

Beweis. Die Eigenschaften einer LLL-reduzierten Basis implizieren

$$\delta\,\|\widehat{b}_i\|^2 \stackrel{2}{\leq} \|\widehat{b}_{i+1}\|^2 + \mu_{i+1,i}^2\,\|\widehat{b}_i\|^2 \stackrel{1}{\leq} \|\widehat{b}_{i+1}\|^2 + \tfrac{1}{4}\,\|\widehat{b}_i\|^2,$$

und somit $\underbrace{\left(\delta - \frac{1}{4}\right)}_{=1/\alpha}\|\widehat{b}_i\|^2 \leq \|\widehat{b}_{i+1}\|^2$. Durch Induktion über $j-i$ folgt $\|\widehat{b}_i\|^2 \leq \alpha^{j-i}\,\|\widehat{b}_j\|^2$. ∎

Lemma 5.1.3
Für jede Basis $b_1, \ldots, b_n$ des Gitters L gilt $\lambda_j(L) \geq \min_{i=j,\ldots,n}\|\widehat{b}_i\|$ für $j = 1, \ldots, n$.

Beweis. Es gibt linear unabhängige Vektoren $a_1, \ldots, a_n \in L$, so dass $\|a_j\| = \lambda_j(L)$ für $j = 1, \ldots, n$. Sei

$$a_k = \textstyle\sum_{i=1}^n t_{ik} b_i = \sum_{i=1}^n \bar{t}_{ik}\widehat{b}_i \quad \text{für } k = 1, \ldots, n.$$

Dabei sind die Koeffizienten t_{ik} ganzzahlig und die $\bar{t}_{ik}$ reell. Sei $\mu(k) := \max\{i \,:\, t_{ik} \neq 0\}$.

Wegen $b_i = \sum_{j=1}^i \mu_{i,j}\widehat{b}_j$ und $\mu_{i,i} = 1$, ist $\bar{t}_{\mu(k),k} = t_{\mu(k),k}$ ganzzahlig. Wegen der linearen Unabhängigkeit der Vektoren $a_1, \ldots, a_j$ gibt es zu jedem j ein $k \leq j$ mit $\mu(k) \geq j$. Denn aus der Annahme $\mu(k) < j$ für $k = 1, \ldots, j$ folgt $a_1, \ldots, a_j \in \operatorname{span}(b_1, \ldots, b_{j-1})$, so dass $a_1, \ldots, a_j$ linear abhängig sind — Widerspruch. Aus $k \leq j$, $\mu(k) \geq j$ folgt

$$\lambda_j^2 \;\geq\; \lambda_k^2 \;=\; \|a_k\|^2 \;\geq\; \bar{t}_{\mu(k),k}^2\|\widehat{b}_{\mu(k)}\|^2 \;\geq\; \|\widehat{b}_{\mu(k)}\|^2 \;\geq\; \min_{i=j,\ldots,n}\|\widehat{b}_i\|^2. \qquad ∎$$

Die untere Schranke zu λ_j in Lemma 5.1.3 gilt für beliebige Basen. Für LLL-reduzierten Basen ist $\|b_j\|$ grobe Approximation zu λ_j, es gilt nämlich

Satz 5.1.4 (Lenstra, Lenstra, Lovász 1982)
Jede mit δ LLL-reduzierte Basis $b_1, \ldots, b_n$ des Gitters L erfüllt mit $\alpha = (\delta - \frac{1}{4})^{-1}$

1. $\alpha^{1-j} \leq \|\widehat{b}_j\|^2 \lambda_j(L)^{-2}$ *für $j = 1, \ldots, n$,*
2. $\|b_j\|^2\,\lambda_j(L)^{-2} \leq \alpha^{n-1}$ *für $j = 1, \ldots, n$,*
3. $\|b_k\|^2 \leq \alpha^{j-1}\,\|\widehat{b}_j\|^2$ *für $k \leq j$.*

Beweis. Wir zeigen zunächst die erste und dritte Aussage. Offenbar gibt es ein k mit $1 \leq k \leq j$ und $\lambda_j \leq \|b_k\|$. Es folgt

$$\begin{aligned} \lambda_j^2 &\leq \|b_k\|^2 \leq \|\widehat{b}_k\|^2 + \tfrac{1}{4}\textstyle\sum_{i=1}^{k-1}\|\widehat{b}_i\|^2 \\ &\leq \|\widehat{b}_j\|^2(\alpha^{j-k} + \tfrac{1}{4}\textstyle\sum_{i=1}^{k-1}\alpha^{j-i}) \qquad \text{(nach Lemma 5.1.2)} \\ &= \|\widehat{b}_j\|^2\alpha^{j-1}(\alpha^{1-k} + \tfrac{1}{4}\textstyle\sum_{i=1}^{k-1}\alpha^{1-i}). \end{aligned}$$

Damit gilt die obere Schranke für $\|b_k\|^2$ für alle k und j mit $k \leq j$. Es bleibt noch zu zeigen, dass

$$\alpha^{1-k} + \tfrac{1}{4}\textstyle\sum_{i=1}^{k-1}\alpha^{1-i} \leq 1.$$

Für $k = 1$ gilt die Ungleichung offenbar. Für $k \geq 2$ gilt mit $\alpha^{-1} = \delta - \frac{1}{4} \leq \frac{3}{4}$ dass

$$\alpha^{1-k} + \tfrac{1}{4}\underbrace{\textstyle\sum_{i=1}^{k-1}\alpha^{1-i}}_{\text{geom. Reihe}} \leq \left(\tfrac{3}{4}\right)^{k-1} + \tfrac{1}{4}\,\frac{1-\left(\frac{3}{4}\right)^{k-1}}{1-\frac{3}{4}} = \tfrac{1}{4}\,\frac{1}{1-\frac{3}{4}} = 1.$$

Damit sind die erste und die dritte Behauptung gezeigt. Nach Lemma 5.1.3 gibt es ein $k \geq j$, so dass $\lambda_j \geq \|\widehat{b}_k\|$. Es folgt

$$\begin{aligned}
\lambda_j^2 &\geq \|\widehat{b}_k\|^2 \geq \alpha^{-k+j}\,\|\widehat{b}_j\|^2 && \text{(wegen Lemma 5.1.2)}\\
&\geq \alpha^{-k+1}\,\|b_j\|^2 && \text{(wegen 3. Aussage des Satzes mit } k=j)\\
&\geq \alpha^{-n+1}\,\|b_j\|^2 && \text{(wegen } k \leq n \text{ und } \alpha \geq 1)
\end{aligned}$$

■

Korollar 5.1.5
Jede mit δ LLL-reduzierte Basis $b_1, \ldots, b_n$ erfüllt

1. $\|b_1\|^2 \leq \alpha^{\frac{n-1}{2}} (\det L)^{\frac{2}{n}}$,
2. $\prod_{i=1}^{n} \|b_i\|^2 \leq \alpha^{\binom{n}{2}} (\det L)^2$.

Beweis. Aus $\prod_{i=1}^n \|\widehat{b}_i\|^2 = (\det L)^2$ und $\|b_1\|^2 \leq \|\widehat{b}_i\|^2\,\alpha^{i-1}$ (Lemma 5.1.2) folgt

$$\|b_1\|^{2n} \leq \alpha^1 \alpha^2 \cdots \alpha^{n-1} \textstyle\prod_{i=1}^n \|\widehat{b}_i\|^2 = \alpha^{\binom{n}{2}}\,(\det L)^2,$$

und somit

$$\|b_1\|^2 \leq \alpha^{\frac{n-1}{2}} (\det L)^{\frac{2}{n}}.$$

Die zweite Aussage folgt aus $\prod_{i=1}^n \|\widehat{b}_i\|^2 = (\det L)^2$ und $\|b_i\|^2 \leq \|\widehat{b}_i\|^2 \alpha^{i-1}$, der dritten Aussage von Satz 5.1.4 für $k = j = i$. ■

5.2 Das LLL-Reduktionsverfahren

Wir beschreiben ein Verfahren zur LLL-Reduktion von ganzzahligen Gitterbasen mit polynomieller Laufzeit. Es handelt sich bis auf kleine Verbesserungen um das Verfahren von A.K. Lenstra, H.W. Lenstra und L. Lovász [LLL82]. Wir zählen die Anzahl der arithmetischen Schritte auf ganzen Zahlen und beschränken den Absolutwert der im Verfahren auftretenden ganzen Zahlen.

5.2.1 LLL-Verfahren

Algorithmus 5.2.1 transformiert eine ganzzahlige Gitterbasis in eine mit δ LLL-reduzierte Basis desselben Gitters. Der Algorithmus reduziert sukzessive einen möglichst großen Anfangsabschnitt $b_1, ..., b_{k-1}$ der Basis. Bei Eintritt in Stufe k ist die Basis $b_1, \ldots, b_{k-1}$ stets LLL-reduziert mit δ. Am Ende ist $k = n + 1$ und die gesamte Basis $b_1, \ldots, b_n$ ist reduziert.

Das Verfahren ist wohldefiniert, und operiert auf Stufe k mit den rationalen Zahlen $\mu_{i,j}$, $\|\widehat{b}_i\|^2$ für $1 \leq i, j \leq k$ und den ganzzahligen Vektoren $b_1, ..., b_k$, siehe Lemma 5.2.2. Die Längenreduktion von b_k sichert, dass die im Verfahren auftretenden ganzen Zahlen polynomielle Bitlänge zur Länge der Eingabe haben. Dies gilt insbesondere für Zähler und Nenner der rationalen Zahlen $\mu_{k,j}$, $\|\widehat{b}_k\|^2$, siehe Satz 5.2.6. Es bezeichne

$$M := \max(\,\|b_1\|^2, ..., \|b_n\|^2\,),$$

(5.1) $$D_i := \det L(b_1, \ldots, b_i)^2 = \det\,[\langle b_s, b_t\rangle]_{1 \leq s,t \leq i} = \textstyle\prod_{j=1}^i \|\widehat{b}_j\|^2 \in \mathbb{N},$$

$$D := \textstyle\prod_{i=1}^{n-1} D_i, \qquad \overline{M} := \max_{i=1,\ldots,n}(\,\|b_i\|^2, D_i\,).$$

Algorithmus 5.2.1 zur LLL-Reduktion

EINGABE: Gitterbasis $b_1, \dots, b_n \in \mathbb{Z}^m$, δ mit $\frac{1}{4} < \delta < 1$

1. $k := 2$, $\|\widehat{b}_1\|^2 := \|b_1\|^2$ /* k ist die *Stufe* */

2. WHILE $k \leq n$ DO

/* $b_1, \dots, b_{k-1}$ ist stets LLL-reduziert */

berechne $\mu_{k,j}$ für $j = 1, \dots, k$ und $\|\widehat{b}_k\|^2$ gemäß Lemma 5.2.2

Längenreduziere b_k, aktualisiere $\mu_{k,1}, \dots, \mu_{k,k-1}$

IF $\delta \|\widehat{b}_{k-1}\|^2 > \|\widehat{b}_k\|^2 + \mu_{k,k-1}^2 \|\widehat{b}_{k-1}\|^2$

THEN vertausche b_{k-1} und b_k /* *kurz* $b_{k-1} \leftrightarrow b_k$ */

IF $k = 2$ THEN aktualisiere $\|\widehat{b}_1\|^2$

$k := \max(k-1, 2)$

ELSE $k := k+1$ *end while*

AUSGABE: LLL-reduzierte Basis $b_1, ..., b_n$.

Die Gram-Determinante D_i ist die Determinante der Gram-Matrix der Teilbasis $b_1, ..., b_i$. Die Größen $M, \overline{M}$ beziehen sich im Folgenden immer auf die Eingabebasis, während D_i und D sich bei Basistransformationen ändern. D^{Start} ist der Wert von D zur Eingabe.

Korrektheit. Auf Stufe k ist die Teilbasis $b_1, ..., b_{k-1}$ stets LLL-reduziert. Dies folgt durch Induktion über die Abfolge der Iterationen. Eine *Iteration* ist die Abfolge der Schritte der WHILE-Schleife bis zur Aktualisierung von k.

Lemma 5.2.1
Die LLL-Reduktion führt zu gegebener ganzzahligen Basis $b_1, ..., b_n \in \mathbb{Z}^m$ höchstens $\log_{1/\delta}\left(D^{Start}\right) \leq n \log_{1/\delta} \overline{M}$ Austausche $b_{k-1} \leftrightarrow b_k$ durch.

Beweis. Die Gram-Determinante D_i ist ganzzahlig und positiv. Wir zeigen, dass jeder Austausch $b_{k-1} \leftrightarrow b_k$ D um den Faktor δ erniedrigt, $D^{neu} \leq \delta\, D^{alt}$. Wegen $D^{\text{Ende}} \in \mathbb{N}$ folgt dann

$$D^{\text{Start}} \geq D^{\text{Ende}} \, (1/\delta)^{\#\text{Austausche}} \geq (1/\delta)^{\#\text{Austausche}}. \tag{5.2}$$

Die Gitter $L(b_1, \dots, b_i)$ mit $i \neq k-1$ werden beim Austausch $b_{k-1} \leftrightarrow b_k$ nicht verändert. Also bleiben die Determinanten D_i mit $i \neq k-1$ erhalten. Im LLL-Verfahren wird nur ausgetauscht wenn

$$\delta \, \|\widehat{b}_{k-1}\|^2 \;>\; \|\widehat{b}_k\|^2 + \mu_{k,k-1}^2 \, \|\widehat{b}_{k-1}\|^2 \;=\; \|\widehat{b}_{k-1}^{\text{neu}}\|^2.$$

Wegen $D_{k-1} = \prod_{i=1}^{k-1} \|\widehat{b}_i\|^2$ bewirkt der Austausch $b_{k-1} \leftrightarrow b_k$, dass

$$D_{k-1}^{\text{neu}} \leq \delta \, D_{k-1}^{\text{alt}} \text{und } D^{\text{neu}} \leq \delta \, D^{\text{alt}}.$$

Nach (5.2) ist die Anzahl der Austausche höchstens $\log_{1/\delta}\left(D^{\text{Start}}\right)$. Wegen $D_i^{\text{Start}} \leq D_i \leq \overline{M}$ folgt $D^{\text{Start}} = \prod_{i=1}^{n-1} D_i \leq \overline{M}^{n-1}$ und somit #Austausche $\leq (n-1) \log_{1/\delta} \overline{M}$. ∎

Wieviele arithmetische Schritte führt das LLL-Verfahren pro Austausch durch ? Wieviele Schritte kostet die Berechnung von $\mu_{k,1}, ..., \mu_{k,k}$ und $\|\widehat{b}_k\|^2$ auf Stufe k ?

Lemma 5.2.2
Die Berechnung von $\mu_{k,1}, ..., \mu_{k,k}$ und $\|\widehat{b}_k\|^2$, sowie die Längenreduktion von b_k auf Stufe k gehen in $\mathcal{O}(km)$ arithmetischen Schritten.

Beweis. Die $\mu_{k,j}$ für $j = 1, ..., k$ und $\|\widehat{b}_k\|^2$ werden durch folgende $\mathcal{O}(km)$ Schritte berechnet

FOR $j = 1, \dots, k-1$ DO $\mu_{k,j} := (\langle b_k, b_j\rangle - \sum_{i=1}^{j-1} \mu_{k,i}\, \mu_{j,i}\, \|\widehat{b}_i\|^2)/\|\widehat{b}_j\|^2$,

$\mu_{k,k} := 1, \qquad \|\widehat{b}_k\|^2 := \langle b_k, b_k\rangle - \sum_{j=1}^{k-1} \mu_{k,j}^2 \|\widehat{b}_j\|^2.$

Die Längenreduktion von b_k geht mit folgenden $\mathcal{O}(km)$ Schritten

FOR $j = k-1, ..., 1$ DO $\quad b_k := b_k - \lceil \mu_{k,j} \rfloor b_j, \quad \mu_{k,i} := \mu_{k,i} - \lceil \mu_{k,j} \rfloor \mu_{j,i}$ für $i = 1, ..., k$.

■

Aufgrund von Lemma 5.2.1 und 5.2.2 führt das LLL-Verfahren höchstens $\mathcal{O}(n^2 m \log_{1/\delta} \overline{M})$ arithmetischen Schritte aus, siehe Satz 5.2.6. Wie groß werden aber die während des LLL-Verfahrens auftretenden ganzen Zahlen ? Wir schätzen in den nächsten drei Lemmata die Absolutwerte der Zähler und Nenner der rationalen Zahlen $\mu_{j,i}$, $\|\widehat{b}_i\|^2$ während der LLL-Reduktion ab.

Lemma 5.2.3
Für jede ganzzahlige Eingabebasis $b_1, ..., b_n \in \mathbb{Z}^m$ gilt 1. $D_{i-1}\, \widehat{b}_i \in \mathbb{Z}^m$, 2. $D_j\, \mu_{i,j} \in \mathbb{Z}$.

Beweis. 1. Aus $[b_1, ..., b_n] = [\widehat{b}_1, \dots, \widehat{b}_n]\, [\mu_{i,j}]^\top$ folgt für $[\nu_{i,j}] := [\mu_{i,j}]^{-1}$ dass

$$[\widehat{b}_1, \dots, \widehat{b}_n] \;=\; [b_1, ..., b_n]\, [\nu_{i,j}]^\top.$$

Dabei sind $[\nu_{i,j}]^\top$, $[\mu_{i,j}]^\top \in \mathbb{Q}^{n\times n}$ obere Dreiecksmatrizen mit Einsen auf der Diagonalen. Wegen $\langle \widehat{b}_i, b_j\rangle = 0$ für $j = 1, 2, \dots, i-1$ folgt aus $\widehat{b}_i = b_i + \sum_{t=1}^{i-1} \nu_{i,t} b_t$ und $\nu_{i,i} = 1$ dass

$$-\langle b_i, b_j\rangle = \sum_{t=1}^{i-1} \nu_{i,t}\, \langle b_t, b_j\rangle \qquad \text{für } j = 1, 2, \dots, i-1.$$

Diese $i-1$ Gleichungen definieren $\nu_{i,1}, \nu_{i,2}, \dots, \nu_{i,i-1}$. Die Determinante des Gleichungssystems ist $D_{i-1} = \det[\langle b_j, b_k\rangle]_{1\le j,k\le i-1} \neq 0$. Nach der Cramer'schen Regel gilt

$$D_{i-1}\, \nu_{i,j} \in \mathbb{Z} \qquad \text{für } j = 1, \dots, i-1.$$

Aus $\widehat{b}_i = b_i + \sum_{j=1}^{i-1} \nu_{i,j} b_j$ folgt $D_{i-1}\, \widehat{b}_i \in \mathbb{Z}^m$.

2. Wegen $D_j = \prod_{i=1}^{j} \|\widehat{b}_i\|^2$ gilt

$$D_j\, \mu_{i,j} = D_j\, \frac{\langle b_i, \widehat{b}_j\rangle}{\|\widehat{b}_j\|^2} = D_{j-1}\, \langle b_i, \widehat{b}_j\rangle = \langle b_i, D_{j-1}\, \widehat{b}_j\rangle.$$

Aus $D_{j-1}\, \widehat{b}_j \in \mathbb{Z}^m$ folgt somit $D_j\, \mu_{i,j} \in \mathbb{Z}$.

■

Lemma 5.2.4
Auf Stufe k des LLL-Verfahrens gilt stets

1. $\|b_i\|^2 \le \frac{i+3}{4}\, M$ *für* $i = 1, \dots, k$,
2. $|\mu_{i,j}|^2 \le \frac{i+3}{4}\, M\, \alpha^{j-1}$ *für* $1 \le j < i < k$.

Beweis. 1. Im LLL-Verfahren bleiben bis auf die Längenreduktion von b_k auf Stufe k die Längen der Basisvektoren unverändert. Nach der Längenreduktion von b_k gilt

$$\|b_k\|^2 = \sum_{j=1}^{k} \mu_{k,j}^2 \|\widehat{b}_j\|^2 \le \|\widehat{b}_k\|^2 + \tfrac{k-1}{4} \max(\|\widehat{b}_1\|, ..., \|\widehat{b}_{k-1}\|^2) \le \tfrac{k+3}{4}\, M.$$

Denn im LLL-Verfahren gilt stets $\max_i \|\widehat{b}_i\|^2 \le M := \max(\|b_1\|^2, ..., \|b_n\|^2)$.
Für jeden Austausch $b_{k-1} \leftrightarrow b_k$ gilt nämlich $\|\widehat{b}_{k-1}^{\text{neu}}\|^2 \le \delta \, \|\widehat{b}_{k-1}^{\text{alt}}\|^2$, $\|\widehat{b}_k^{\text{neu}}\|^2 \le \|\widehat{b}_{k-1}^{\text{alt}}\|^2$.

2. Nach Definition der Gram-Schmidt-Koeffizienten und der Cauchy-Schwarz-Ungleichung gilt

$$|\mu_{i,j}|^2 = \frac{|\langle b_i, \widehat{b}_j\rangle^2|}{\|\widehat{b}_j\|^4} \le \frac{\|b_i\|^2 \, \|\widehat{b}_j\|^2}{\|\widehat{b}_j\|^4} \le \frac{\|b_i\|^2}{\|\widehat{b}_j\|^2}.$$

Weil $b_1, ..., b_{k-1}$ LLL-reduziert ist, gilt

$$\begin{aligned} |\mu_{i,j}|^2 &\le \tfrac{i+3}{4}\, M \, \|\widehat{b}_j\|^{-2} && \text{(wegen } \|b_i\|^2 \le \tfrac{i+3}{4} M) \\ &\le \tfrac{i+3}{4}\, M \, \alpha^{j-1} \, \|\widehat{b}_1\|^{-2} && \text{(nach Lemma 5.1.2)} \\ &\le \tfrac{i+3}{4}\, M \, \alpha^{j-1} && \text{(weil } \|b_1\|^2 = \|\widehat{b}_1\|^2 \in \mathbb{Z}). \end{aligned}$$

■

Lemma 5.2.5
Während der Längenreduktion von b_k auf Stufe k gilt $|\mu_{k,j}|^2 \le \frac{k+3}{4}\, M \, \left(\frac{9\alpha}{4}\right)^{k-1}$ für $j < k$.

Beweis. Der Reduktionsschritt

$$b_k := b_k - \lceil \mu_{k,i} \rfloor \, b_i \qquad \text{für } i < k$$

der Längenreduktion wird begleitet von

(5.3) $$\mu_{k,j} := \mu_{k,j} - \lceil \mu_{k,i} \rfloor \underbrace{\mu_{i,j}}_{|\mu_{i,j}| \le 1/2} \qquad \text{für } j = 1, 2, ..., k-1.$$

Jeder dieser $k-1$ Schritte verändert $M_k := \max_{j<k} |\mu_{k,j}|$ wegen $\lceil \mu_{k,i} \rfloor \le M_k + \frac{1}{2}$ derart dass

(5.4) $$M_k^{\text{neu}} \le M_k^{\text{alt}} + \tfrac{1}{2}\left(M_k^{\text{alt}} + \tfrac{1}{2}\right) \le \tfrac{3}{2}\, M_k^{\text{alt}} + \tfrac{1}{4}$$

Nach Lemma 5.2.4 gilt vor der Längenreduktion von b_k dass

$$M_k \le \sqrt{\tfrac{k+3}{4}\, M \, \alpha^{k-1}}.$$

Wegen (5.4) erhöht sich die Größe M_k während der Längenreduktion von b_k höchstens um den Faktor $\left(\frac{3}{2}\right)^{k-1}$ (der Summand $\frac{1}{4}$ kann vernachlässigt werden). Also gilt

$$|\mu_{k,j}|^2 \le \left(\tfrac{3}{2}\right)^{2(k-1)} \left(\tfrac{k+3}{4}\, M \, \alpha^{k-1}\right) = \tfrac{k+3}{4}\, M \, \left(\tfrac{9\alpha}{4}\right)^{k-1}.$$

■

Satz 5.2.6
Zu gegebener ganzzahliger Basis $b_1, \ldots, b_n \in \mathbb{Z}^m$ liefert Algorithmus 5.2.1 eine LLL-reduzierte Basis. Mit $\overline{M} := \max_i(\|b_i\|^2, D_i)$ macht der Algorithmus höchstens $\mathcal{O}(n^2 m \log_{1/\delta} \overline{M})$ arithmetische Schritte auf den Koordinaten der b_i und den rationalen Zahlen $\mu_{i,j}, \|\widehat{b}_i\|^2$. Die Bitlänge der auftretenden ganzen Zahlen, insbesondere der Zähler und Nenner von $\mu_{i,j}, \|\widehat{b}_i\|^2$ ist höchstens $\mathcal{O}(n + \log_2 \overline{M})$.

Beweis. Nach Lemma 5.2.1 gilt

$$\#\text{Austausche} \leq \log_{1/\delta} D^{\text{Start}} \leq (n-1)\log_{1/\delta} \overline{M} \leq \tbinom{n}{2} \log_2 M.$$

Die LLL-Reduktion beginnt mit Stufe $k = 2$ und endet mit Stufe $k = n + 1$. Jeder Austausch erniedrigt die Stufe k gemäß $k := \min(k-1, 2)$. Zu jeder Iteration mit Austausch und Stufenerniedrigung gibt es höchstens eine Iteration mit Stufenerhöhung $k := k + 1$ ohne Austausch. Es folgt

$$\#\text{Iterationen} \leq n - 1 + 2\,\#\text{Austausche} = n + 2n \log_{1/\delta} \overline{M}.$$

Jede Iteration erfordert $\mathcal{O}(km) = \mathcal{O}(nm)$ arithmetische Schritte. Damit ist die Schrittzahl höchstens $\mathcal{O}(n^3 m \log_{1/\delta} \overline{M})$.

Nach Lemma 5.2.3, 5.2.4 und 5.2.5 sind die auftretenden Zahlen wie folgt beschränkt

$$|\mu_{k,j}|^2 \leq \tfrac{k+3}{4}\, M \,\left(\tfrac{9\alpha}{4}\right)^{k-1}, \quad \|b_k\|^2 \leq k\, \tfrac{k+3}{4}\, M\, \left(\tfrac{9\alpha}{4}\right)^{k-1},$$

und für $i < k$:

$$|\mu_{i,j}|^2 \leq \tfrac{i+3}{4}\, M\, \alpha^{j-1}, \quad \|b_i\|^2 \leq \tfrac{i+3}{4}\, M.$$

Der Nenner von $\mu_{i,j}$ ist absolut beschränkt durch $D_{j-1} \leq \overline{M}$. Damit ist der Zähler von $\mu_{i,j}$ absolut beschränkt durch

$$\sqrt{\tfrac{n+3}{4}}\, M^{\frac{1}{2}} \left(\tfrac{9\alpha}{4}\right)^{\frac{n-1}{2}} \overline{M}.$$

Zähler und Nenner von $\|\widehat{b}_j\|^2 = \frac{D_j}{D_{j-1}}$ sind durch $\overline{M}$ beschränkt. Damit sind alle im Verfahren auftretenden, ganzen Zahlen absolut beschränkt durch

$$n\, M^{\frac{1}{2}} \left(\tfrac{9\alpha}{4}\right)^{\frac{n-1}{2}} \overline{M}$$

und haben somit eine Bitlänge $\mathcal{O}(n + \log_2 \overline{M})$ mit einer $\mathcal{O}$-Konstante nahe 1,5 für $\delta \approx 1$. ∎

Nach dem Austausch $b_{k-1} \leftrightarrow b_k$ kann man die Gram-Schmidt-Koeffizienten $\mu_{k-1,1}, \ldots, \mu_{k-1,k-2}$, sowie das Längenquadrat $\|\widehat{b}_{k-1}\|^2$ schnell aktualisieren. Die Aktualisierung erfordert nur $\mathcal{O}(1)$ Rechenschritte und $\mathcal{O}(k)$ Datentransporte während die Neuberechnung nach Lemma 5.2.2 $\mathcal{O}(k\,m)$ Rechenschritte erfordert. .

Lemma 5.2.7
Der Austausch $b_{k-1} \leftrightarrow b_k$ bewirkt mit $\mu := \mu_{k,k-1}$ dass

1. $\mu_{\text{neu}} = \mu \dfrac{\|\widehat{b}_{k-1}\|^2}{\|\widehat{b}^{\text{neu}}_{k-1}\|^2}$ *mit* $\|\widehat{b}^{\text{neu}}_k\|^2 = \mu^2 \|\widehat{b}_{k-1}\|^2 + \|\widehat{b}_k\|^2$,
2. $[\mu^{\text{neu}}_{k,i}\,,\, \mu^{\text{neu}}_{k-1,i}] = [\mu_{k-1,i}\,,\, \mu_{k,i}]$ *für* $i = 1, \ldots, k-2$.

Beweis. 1. Es gilt $\mu_{\text{neu}} = \frac{\langle b^{\text{neu}}_k, \widehat{b}^{\text{neu}}_{k-1}\rangle}{\|\widehat{b}^{\text{neu}}_{k-1}\|^2} = \frac{\langle \pi_{k-1}(b^{\text{neu}}_{k-1}), \pi_{k-1}(b^{\text{neu}}_k)\rangle}{\|\widehat{b}^{\text{neu}}_{k-1}\|^2}$.
Weil $\langle \pi_{k-1}(b_{k-1}), \pi_{k-1}(b_k)\rangle$ bei der Vertauschung $b_{k-1} \leftrightarrow b_k$ erhalten bleibt, folgt dass $\mu_{\text{neu}} = \mu\, \|\widehat{b}_{k-1}\|^2 / \|\widehat{b}^{\text{neu}}_{k-1}\|^2$. 2. ist offensichtlich. ∎

Algorithmus 5.3.1 LLL-Reduktion von ganzzahligen Erzeugendensystemen

EINGABE : Erzeugendensystem $b_1, \ldots, b_n \in \mathbb{Z}^m \setminus \{0\}$, δ mit $\frac{1}{4} < \delta < 1$
/* $L := \sum_{i=1}^n b_i \mathbb{Z}$ ist ein Gitter */

1. $k := 2$, $\|\widehat{b}_1\|^2 := \|b_1\|^2$ /* k ist die *Stufe* */

2. WHILE $k \leq n$ DO

/* $b_1, \ldots, b_{k-1}$ ist LLL-reduziert */

berechne $\mu_{k,j}$ für $j = 1, \ldots, k$ und $\|\widehat{b}_k\|^2$ gemäß Lemma 5.2.2

Längenreduziere b_k, aktualisiere $\mu_{k,1}, \ldots, \mu_{k,k-1}$

IF $b_k = 0$ THEN entferne b_k aus dem Erzeugendensystem, $n := n - 1$ RETURN

IF $\delta \|\widehat{b}_{k-1}\|^2 > \|\widehat{b}_k\|^2 + \mu_{k,k-1}^2 \|\widehat{b}_{k-1}\|^2$

THEN vertausche b_{k-1} und b_k /* *kurz* $b_{k-1} \leftrightarrow b_k$ */

IF $k = 2$ THEN aktualisiere $\|\widehat{b}_1\|^2$

$k := \max(k-1, 2)$

ELSE $k := k + 1$ *end while*

AUSGABE : LLL-reduzierte Basis $b_1, ..., b_n$ des Gitters L.

5.3 LLL-Reduktion ganzzahliger Erzeugendensysteme

Wir erweitern die LLL-Reduktion auf ganzzahlige Erzeugendensysteme $b_1, \ldots, b_n \in \mathbb{Z}^m \setminus 0$. Es genügt, die im LLL-Verfahren entstehenden Nullvektoren zu eliminieren. Der Nullvektor kann nur durch Längenreduktion von b_k auf Stufe k entstehen.

Korrektheit. Algorithmus 5.3.1 ist wohldefiniert und operiert auf Stufe k mit den rationalen Zahlen $\mu_{i,j}, \|\widehat{b}_i\|^2$ für $i, j \leq k$ und den ganzzahligen Basisvektoren. Das Verfahren ist korrekt, weil die Vektoren $b_1, \ldots, b_{k-1}$ auf Stufe k stets linear unabhängig und somit LLL-reduziert sind. Sind nämlich nach der Längereduktion von b_k die Vektoren $b_1, \ldots, b_k$ erstmals linear abhängig, so gilt $b_k \in L(b_1, \ldots, b_{k-1})$. Die Längenreduktion von b_k erzeugt den Nullvektor. Dieser wird sofort entfernt.

Laufzeitanalyse. Zu den Teilgittern $L(b_1, \ldots, b_i) = \sum_{j=1}^i b_j \mathbf{Z}$ und den Gram-Determinanten $D_i = (\det L(b_1, \ldots, b_i))^2$ setzt man wieder

$$D := \prod_{i=1}^{n-1} D_i \ ,$$

$$M := \max_i \|b_i\|, \quad \overline{M} := \max_i (\|b_i\|^2, D_i) \ .$$

Dann gilt

$$\#\text{Austausche} \leq \log_{1/\delta} D^{\text{Start}} \leq (n-1) \log_{1/\delta} \overline{M}$$

$$\#\text{Iterationen} \leq n - 1 + 2\,\#\text{Austausche} \leq n + 2n \log_{1/\delta} \overline{M}$$

$$\#\text{arithm. Schritte} = \mathcal{O}(n^2 m \log_{1/\delta} \overline{M}).$$

Damit überträgt sich der Beweis von Satz 5.2.6. Insbesondere gelten die Zahlen-Schranken von Lemma 5.2.3 5.2.4 und 5.2.5 auch für die Werte im Verlauf von Algorithmus 5.3.1. Somit gilt der

Satz 5.3.1
Zu gegebenen ganzzahligen Vektoren $b_1, ..., b_n \in \mathbb{Z}^m \backslash 0$ *liefert Algorithmus 5.3.1 eine LLL-reduzierte Basis des von* $b_1, ..., b_n$ *erzeugten Gitters. Mit* $\overline{M} := \max_i(\|b_i\|^2, D_i)$ *macht das LLL-Verfahren höchstens* $\mathcal{O}(n^2 m \log_{1/\delta} \overline{M})$ *arithmetische Schritte auf den Koordinaten der* b_i *und den rationalen Zahlen* $\mu_{i,j}, \|\widehat{b}_i\|^2$. *Die Bitlänge der auftretenden ganzen Zahlen, insbesondere der Zähler und Nenner von* $\mu_{i,j}, \|\widehat{b}_i\|^2$ *ist höchstens* $\mathcal{O}(n + \log_2 \overline{M})$.

5.4 LLL-Reduktion mit Gleitkomma-Arithmetik

Für eine schnelle LLL-Reduktion muß man die Rechnung überwiegend in Gleitkomma-Arithmetik durchführen. Ein Schritt in Gleitkomma-Arithmetik geht in einem Maschinenzyklus, die Arithmetik auf langen ganzen Zahlen erfordert dagegen spezielle Software und ist recht langsam. Die Rechnung auf den Basisvektoren $b_1, \ldots, b_n$ wird in exakter Arithmetik durchgeführt. Für die Rechnung auf den rationalen Zahlen $\mu_{i,j}, \|\widehat{b}_i\|^2$ für $i, j \leq k$ genügen dagegen gute Näherungen in Gleitkomma-Arithmetik.

Definition 5.4.1 (Relativer Fehler)
Eine Näherung f' *zu* $f \in \mathbf{R}$ *hat* relativen Fehler $\varepsilon > 0$, *wenn* $|f - f'| \leq \varepsilon \min(|f|, |f'|)$. [1]

Wir betrachten die LLL-Reduktion nach Algorithmus 5.2.1 für den Fall, dass alle rationalen Zahlen $\mu_{i,j}, \|\widehat{b}_j\|^2$ mit relativem Fehler ε berechnet werden. Dann führt die Längenreduktion des Vektors b_k nur zu $|\mu_{k,j}| \leq \frac{1}{2} + \varepsilon$ anstelle von $|\mu_{k,j}| \leq \frac{1}{2}$ für $j = 1, \ldots, k-1$. Wir vernachlässigen diese geringfügige Abschwächung der Längenreduktion.

Satz 5.4.2
Haben bei der LLL-Reduktion mit δ *die rationalen Zahlen* $\|\pi_{k-1}(b_{k-1})\|^2, \|\pi_{k-1}(b_k)\|^2$ *bei der Entscheidung über den Austausch* $b_{k-1} \leftrightarrow b_k$ *stets relativen Fehler* ε, *dann ist die Ausgabebasis LLL-reduziert mit* $\delta_- := \delta(1-\varepsilon)/(1+\varepsilon)$. *Die Anzahl der Austausche* $b_{k-1} \leftrightarrow b_k$ *ist höchstens* $n \log_{1/\delta_+} \overline{M}$ *mit* $\delta_+ := \delta(1+\varepsilon)/(1-\varepsilon)$, *sofern* $\delta_+ < 1$.

Beweis. Angenommen, bei der LLL-Reduktion mit δ_- und exakter Rechnung erfolgt ein Austausch $b_{k-1} \leftrightarrow b_k$. Dann gilt $\delta_- \|\pi_{k-1}(b_{k-1})\|^2 > \|\pi_{k-1}(b_k)\|^2$. Für die Näherungen mit relativem Fehler ε folgt — es bezeichnet stets f' eine Näherung zu f:

$$\delta_-(1+\varepsilon)\|\pi_{k-1}(b_{k-1})\|'^2 > \|\pi_{k-1}(b_k)\|'^2(1-\varepsilon).$$

Somit erfolgt der Austausch $b_{k-1} \leftrightarrow b_k$ auch mit $\delta = \delta_-(1+\varepsilon)/(1-\varepsilon)$ und Näherungen. Weil alle Austausche $b_{k-1} \leftrightarrow b_k$ der LLL-Reduktion mit δ_- und exakter Rechnung korrekt ausgeführt werden, ist die Ausgabebasis LLL-reduziert mit δ_-

Wir zeigen noch, dass die LLL-Reduktion mit Näherungen abbricht sofern $\delta_+ < 1$. Erfolgt nämlich ein Austausch $b_{k-1} \leftrightarrow b_k$ mit δ und Näherungen, dann gilt

$$\delta\|\pi_{k-1}(b_{k-1})\|'^2 > \|\pi_{k-1}(b_k)\|'^2$$

und somit $\delta(1+\varepsilon)\|\pi_{k-1}(b_{k-1})\|^2 > \|\pi_{k-1}(b_k)\|^2(1-\varepsilon)$. Dann wird D_{k-1} beim Austausch $b_{k-1} \leftrightarrow b_k$ um den Faktor $\delta_+ = \delta(1+\varepsilon)/(1-\varepsilon)$ erniedrigt, sofern $\delta_+ < 1$. Damit ist die Anzahl der Austausche höchstens $n \log_{1/\delta_+}(\overline{M})$. ■

Wegen Satz 5.4.2 gilt es bei der LLL-Reduktion mit Gleitkomma-Zahlen $\mu_{i,j}, \|\widehat{b}_j\|$ den relativen Fehler zu begrenzen. Wichtigste Punkte dabei sind

[1] Wir definieren den relativen Fehler ε von f' zu f symmetrisch in f und f', üblich ist es nur $|f - f'| \leq \varepsilon |f|$ zu fordern.

1. War vor der Längenreduktion von b_k auf Stufe k $|\mu_{k,j}| \approx 2^m$, dann gehen bei der Reduktion auf $|\mu_{k,j}| \leq \frac{1}{2}$ die $m+1$ führenden Bits der Gleitkomma-Zahl $\mu'_{k,j}$ verloren. Man kann den relativen Fehler von $\mu'_{k,j}$ wieder klein machen durch Neuberechnung von $\mu_{k,j}$ gemäß Lemma 5.2.2.

2. Bei der Neuberechnung von $\mu_{k,j}$ gemäß Lemma 5.2.2 rechnet man $\langle b'_k, b'_j \rangle$ in Gleitkomma. Im Falle dass $|\langle b_k, b_j \rangle| \approx 2^{-m} \|b_k\| \|b_j\|$, gehen dabei m Präzisionsbits verloren. Ist m zu groß, rechnet man besser $\langle b_k, b_j \rangle$ exakt.

Mit diesen Maßnahmen haben Schnorr, Euchner [SchnEu91] ein LLL-Verfahren implementiert. Dieser Algorithmus ist stabil, etwa bis zur Dimension 350.

Auf Stufe k sind die $\mu_{i,j}$ mit $i, j > k$ im allgemeinen sehr groß. Statt der Schranke von Lemma 5.2.4 gilt nur $|\mu_{i,j}|^2 \leq \frac{i+3}{4} D_{j-1}$. Unsere Variante des LLL-Verfahrens vermeidet die Gram-Schmidt-Koeffizienten $\mu_{i,j}$ mit $i, j > k$ und rechnet auf Stufe k nur mit den Größen $\mu_{i,j}$, $\|\widehat{b}_j\|^2$ mit $1 \leq j \leq i \leq k$ nach den Formeln von Lemma 5.2.2. Diese sind geeignet für das Rechnen mit Gleitkommazahlen $\mu_{i,j}, \|\widehat{b}_j\|^2$. Weil die Basis $b_1, \ldots, b_{k-1}$ stets LLL-reduziert ist, gilt nach Lemma 5.1.2

$$\|\widehat{b}_j\|^2 \geq \|b_1\|^2 \, \alpha^{1-j} \qquad \text{für } j = 1, \ldots, k-1.$$

Die Divisoren $\|\widehat{b}_j\|^2$ bei der Berechnung von $\mu_{k,j}$ gemäß Lemma 5.2.2 sind daher nicht beliebig klein. Dies ist wichtig für die Begrenzung von Gleitkommafehlern.

5.5 LLL-Reduktion mit ganzzahliger Gram-Matrix

Für die LLL-Reduktion einer Basismatrix $B \in \mathbb{R}^{m \times n}$ in ganzzahliger Arithmetik ist es nicht erforderlich, daß B ganzzahlig ist. Es genügt, die Ganzzahligkeit der Gram-Matrix $B^\top B$. Ist $B^\top B \in \mathbb{Z}^{n \times n}$ gegeben, so kann man mit den Einträgen von $B^\top B$ rechnen. Genauer gesagt, genügen die $\binom{n+1}{2}$ Einträge $\langle b_i, b_j \rangle$ für $1 \leq i \leq j \leq n$. Gegebenenfalls führt man auch die Transformationsmatrix $T \in \mathbb{Z}^{n \times n}$ mit, welche die Startbasis B^{Start} in die aktuelle Basis B überführt, $B = B^{\text{Start}} T$.

Aktualisierung von $\mathbf{B^\top B}$. Beim Schritt $b_k := b_k - \mu b_j$ der Längenreduktion von b_k auf Stufe k wird $B^\top B$ wie folgt aktualisiert:

$$\begin{aligned} \langle b_k, b_i \rangle &:= \langle b_k, b_i \rangle - \mu \langle b_j, b_i \rangle \quad \text{für } i = 1, \ldots, n, i \neq k \\ \langle b_k, b_k \rangle &:= \langle b_k, b_k \rangle - 2\mu \langle b_k, b_j \rangle + \mu^2 \langle b_j, b_j \rangle \end{aligned}$$

Die Aktualisierung von $B^\top B$ bei der Längenreduktion von b_k geht in $O(kn)$ arithmetischen Schritten.

Aktualisierung von T. Die Aktualisierung von $T = [t_{i,j}]_{1 \leq i,j \in n}$ beim Schritt $b_k := b_k - \mu \, b_j$ geht in $\mathcal{O}(n)$ Schritten

$$t_{j,i} := t_{j,i} + \mu \, t_{k,i} \qquad \text{für } i = 1, \ldots, n.$$

Dann geht die Aktualisierung von T bei der Längenreduktion von b_k in $\mathcal{O}(kn)$ arithmetischen Schritten. Beim Austausch $b_{k-1} \leftrightarrow b_k$ werden $B^\top B$ und T durch $\mathcal{O}(n)$ Datentransporte aktualisiert, indem $\mathcal{O}(n)$ Einträge in $B^\top B$ und T getauscht werden. Damit kostet eine Iteration der LLL-Reduktion $\mathcal{O}(n^2)$ Schritte und es folgt der

Satz 5.5.1
Zu gegebener ganzzahliger Gram-Matrix $B^\top B \in \mathbb{Z}^{n \times n}$ geht die LLL-Reduktion gemäß Alg. 5.2.1 in $\mathcal{O}(n^3 \log_{1/\delta} \overline{M})$ arithmetischen Schritten auf ganzen Zahlen der Bitlänge $\mathcal{O}(n + \log_2 \overline{M})$.

Dabei ist $\overline{M}$ wie für ganzzahlige Eingabebasen erklärt. Im Falle einer ganzzahligen Basis $B \in \mathbb{Z}^{m \times n}$ mit $m >> n$ ist es wegen Satz 5.5.1 günstig, vorweg $B^\top B$ in $\mathcal{O}(n^2 m)$ Schritten zu berechnen. Die LLL-Reduktion geht so in $\mathcal{O}(n^2 m + n^3 \log_{1/\delta} \overline{M})$ Schritten, gegenüber $\mathcal{O}(n^2 m \log_{1/\delta} \overline{M})$ Schritten von Algorithmus 5.2.1.

Kapitel 6

Lösen von Subsetsum-Problemen durch Gitterreduktion

In diesem Kapitel lernen wir die erste Anwendung der Gitterreduktion kennen: Wir nehmen an, es gäbe ein Gitterorakel, daß uns den kürzesten, nichttrivialen Gittervektor liefert und reduzieren das Subsetsum-Problem auf das Finden eines kürzesten Gittervektors. Wir stellen zunächst die Lagarias-Odlyzko- und anschließend die verbesserte CJLOSS-Gitterbasis vor. Für kleine Dimensionen können wir das Gitterorakel durch Reduktionsalgorithmen annährend ersetzen.

6.1 Einleitung

Wir versuchen, die folgende Aufgabe mit Hilfe eines Gitterorakels bzw. durch Gitterreduktion zu lösen:

Definition 6.1.1 (Subsetsum-Problem)
Das Subsetsum-Problem lautet:

- *Gegeben:* $n \in \mathbb{N}$, *Gewichte* $a_1, \ldots, a_n \in \mathbb{N}$ *und* $s \in \mathbb{N}$
- *Finde* $e \in \{0,1\}^n$ *mit* $\sum_{i=1}^{n} a_i e_i = s$ *oder zeige, daß kein solcher Vektor existiert.*

Das Subsetsum-Problem nennt man in der Literatur auch Knapsack- bzw. Rucksack-Problem. Nach Satz 11.2.5 auf Seite 101 ist das Subsetsum-Problem $\mathcal{NP}$-vollständig.

Sei $A \in \mathbb{N}$ eine beliebige Konstante. Wir betrachten Gewichte $(a_1, \ldots, a_n)$, welche über dem Bereich $[1, A]^n$ variieren. Zusätzlich setzen wir voraus, daß stets eine Lösung existiert: Sei $e = (e_1, \ldots, e_n) \in \{0,1\}^n \setminus \{0^n\}$ beliebig, aber fest. Setze

$$s := \sum_{i=1}^{n} a_i e_i$$

Die Wahrscheinlichkeiten und die „fast alle"-Aussagen in diesem Kapitel beziehen sich auf rein zufällig gewählte Tupel aus $[1, A]^n$. Zur Subsetsum-Aufgabe formulieren wir das inverse Problem:

Definition 6.1.2 (Inverses Subsetsum-Problem)
Die inverse Aufgabe zu einem Subsetsum-Problem lautet:

- *Gegeben:* $n \in \mathbb{N}$, *Gewichte* $a_1, \ldots, a_n \in \mathbb{N}$ *und* $s \in \mathbb{N}$
- *Finde* $\overline{e} \in \{0,1\}^n$ *mit* $\sum\limits_{i=1}^{n} a_i \overline{e}_i = \sum\limits_{i=1}^{n} a_i - s =: \overline{s}$ *oder zeige, daß kein solcher Vektor existiert.*

Sei e eine Lösung zum Subsetsum-Problem und $\overline{e}$ zum Inversen. Dann gilt:

$$\overline{e}_i := 1 - e_i \qquad i = 1, \ldots, n$$

Aus der Lösung zum inversen Problem erhalten wir unmittelbar eine Lösung des Ausgangsproblems. Durch den möglichen Übergang zum inversen Problem können wir stets erreichen, daß die Summe der Einsen im Lösungsvektor e bzw. $\overline{e}$ maximal $\frac{n}{2}$ beträgt.

Um die Aufgabe zu lösen, setzen wir ein Gitterorakel voraus. Das Gitterorakel liefert zu gegebener, ganzzahliger Basis zum Gitter L einen Vektor $x \in L$ mit $\|x\| = \lambda_1(L)$ (Euklidische Norm). Wir werden zeigen, daß wir mit dem Gitterorakel die Aufgabe fast immer lösen können (also die Wahrscheinlichkeit, daß wir es nicht lösen können, fällt mit n gegen unendlich gegen 0), wenn die Dichte niedrig ist:

Definition 6.1.3 (Dichte eines Subsetsum-Problems)
Zu einem Subsetsum-Problem mit Gewichten $a_1, \ldots, a_n \in \mathbb{N}$ *definieren wir die Dichte* d *als:*

$$d := \frac{n}{\log_2 \left(\max\limits_{i=1,\ldots,n} a_i \right)}$$

Für Dichte $d \gg 1$ gibt es bei zufälliger Wahl der Gewichte $a_1, \ldots, a_n$ und der Summe s „in der Regel“ viele Lösungen, als am schwierigsten gelten zufällige Subsetsum-Problem mit Dichte etwa 1. Aus gegebener Dichte d und der Anzahl n erhalten wir eine untere Schranke für die Gewichte $a_1, \ldots, a_n$:

$$\max_{i=1,\ldots,n} a_i \geq 2^{\frac{n}{d}} \tag{6.1}$$

In der Praxis versucht man, statt durch Fragen an das Orakels, einen der kürzesten Gittervektor mit Hilfe der Gitterbasenreduktion zu finden (siehe u.a. [SchnHö95, SchnEu91, Hörner94]). Dies bietet auch eine Angriffsmöglichkeit auf Kryptographie-Schemata, die auf Subsetsum-Problemen basieren. C.P. Schnorr und H.H. Hörner [SchnHö95, Hörner94] haben das Chor-Rivest-System [CR88] mittels Gitterreduktion angegriffen.

6.2 Lagarias-Odlyzko-Gitterbasis

J.C. Lagarias und A.M. Odlyzko [LaOd85] haben 1985 eine Gitterbasis vorgestellt, um Subsetsum-Aufgaben mit Hilfe eines Gitterorakels zu lösen. Unsere Darstellung orientiert sich an [CJLOSS92]. Die Lagarias-Odlyzko-Gitterbasis besteht aus folgenden $n+1$ ganzzahligen Zeilenvektoren, wobei N eine hinreichend große Zahl ist:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \\ b_{n+1} \end{bmatrix} := \begin{bmatrix} 1 & 0 & \cdots & 0 & Na_1 \\ 0 & 1 & & 0 & Na_2 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & & 1 & Na_n \\ 0 & 0 & \cdots & 0 & Ns \end{bmatrix} \tag{6.2}$$

Im Beweis wählen wir $N > \sqrt{\frac{1}{2}n}$. Die Motivation: Ein kurzer Gittervektor hat dann in der letzten Komponente den Wert 0, und wir erhalten aus den ersten n Komponenten eine Lösung des Subsetsum-Problems. Sei

$$L_{\mathrm{LO}} := L(b_1, \ldots, b_{n+1})$$

Der Lösung e des Subsetsum-Problems, die nach Voraussetzung existiert, ist der folgende Lösungsvektor zugeordnet:

$$\widehat{e} := \left(\sum_{i=1}^{n} e_i b_i \right) - b_{n+1} = (e_1, \ldots, e_n, 0) \tag{6.3}$$

Satz 6.2.1
Sei $A > 0$ beliebig, aber fest. Die Subsetsum-Aufgabe wird für hinreichend große n für fast alle ganzzahligen Gewichte $(a_1, \ldots, a_n) \in_{\mathrm{R}} [1, A]^n$ mit Dichte $d < 0{,}6463$ durch zweifache Anwendung des Gitterorakels auf die Lagarias-Odlyzko-Basis effizient gelöst.

Beweis. Wir wenden das Orakel auf das Problem und sein inverses Problem an: Zuvor entfernen wir diejenigen Gewichte, die wir im voraus einer Lösung zuordnen können.

Sei $t := \sum_{i=1}^{n} a_i$. Wir reduzieren das Problem: Solange ein a_i mit $a_i > \min(s, t-s)$ existiert, entferne dieses Gewichte aus der Liste, vermindere n um 1 und aktualisiere s und t. Ein a_i mit $a_i > t - s$ muß Summand in $\sum_{i=1}^{n} e_i a_i$ sein. Ein a_i mit $a_i > s$ muß Summand in $\sum_{i=1}^{n}(1 - e_i) a_i$ sein.

Jede Lösung des reduzierten Problems liefert eine Lösung der Aufgabe. Für die reduzierte Aufgabe gilt

$$\tfrac{1}{n} \cdot t \leq s \leq t - \tfrac{1}{n} \cdot t, \tag{6.4}$$

weil alle kleineren und größeren Gewichte entfernt wurden. Die Ungleichung bleibt bestehen, wenn man auf das inverse Problem übergeht. Die folgende Analyse bezieht sich auf dasjenige Problem mit $\sum_{i=1}^{n} e_i \leq \frac{1}{2} n$.

Es bleibt die Wahrscheinlichkeit abzuschätzen, daß das Orakel einen kürzesten Gittervektor $\widehat{x} = (x_1, \ldots, x_{n+1}) \neq \pm \widehat{e}$ ausgibt, da wir dann aus der Antwort nicht die gesuchte Subsetsum-Lösung erhalten. Für den Vektor $\widehat{x}$ gilt:

$$\begin{aligned} \|\widehat{x}\| &\leq \|\widehat{e}\| \leq \sqrt{\tfrac{1}{2}n} \\ \widehat{x} &\in L_{\mathrm{LO}} = L(b_1, \ldots, b_{n+1}) \\ \widehat{x} &\notin \{0, \pm \widehat{e}\} \end{aligned} \tag{6.5}$$

Für $N > \sqrt{\frac{1}{2}n}$ folgt, daß $x_{n+1} = 0$ ist. Setze

$$x := (x_1, \ldots, x_n) \tag{6.6}$$

Definiere:

$$y := \frac{1}{s} \sum_{i=1}^{n} x_i a_i \tag{6.7}$$

Dann gilt

$$|y| \leq n \cdot \sqrt{\tfrac{1}{2}n}, \tag{6.8}$$

da aus der Cauchy-Schwarz-Ungleichung und $a \in \mathbb{N}^n$

$$|y| = \frac{|\langle x, a\rangle|}{s} \leq \frac{\|x\| \cdot \|a\|}{s} \leq \frac{\|x\|\,\|a\|_1}{s} \leq \frac{\|x\|}{s} \cdot \sum_{i=1}^{n} a_i$$

folgt und wir wegen $t = \sum_{i=1}^{n} a_i$ sowie (6.4),(6.5) und $x_{n+1} = 0$ erhalten:

$$|y| \leq \frac{t \cdot \|x\|}{s} \leq n \cdot \sqrt{\tfrac{1}{2}n}$$

Es bezeichne im weiteren

$$P(n) := \mathrm{Ws}[\,\text{Es existiert ein } \widehat{x} \text{ mit } (6.5)]$$

die Wahrscheinlichkeit bezüglich zufälliger, gleichverteilter und unabhängiger $(a_1, \ldots, a_n)$ aus $[1, A]^n$. Zu zeigen: Für Dichte $d < 0,6463$ gilt $\lim_{n\to\infty} P(n) = 0$. Es ist:

$$P(n) = \mathrm{Ws}\left[\begin{array}{l} \exists \widehat{x} \in L_{\mathrm{LO}}, \exists y \in \mathbb{Z}, \text{ so daß:} \\ \|\widehat{x}\| \leq \|\widehat{e}\|, \quad |y| \leq n \cdot \sqrt{\tfrac{1}{2}n}, \quad \widehat{x} \notin \{0, \pm\widehat{e}\}, \quad \sum_{i=1}^{n} a_i x_i = ys \end{array}\right]$$

$$\leq \overbrace{\mathrm{Ws}\left[\sum_{i=1}^{n} a_i x_i = ys, \quad x \in \mathbb{Z}^n \text{ und } y \in \mathbb{Z} \text{ fest}, \quad \|x\| \leq \|\widehat{e}\|, \quad |y| \leq n \cdot \sqrt{\tfrac{1}{2}n}, \quad x \notin \{0, \pm\widehat{e}\}\right]}^{\text{Faktor 1}}$$

$$\cdot \underbrace{\left|\left\{x \in \mathbb{Z}^n \ :\ \|x\| \leq \sqrt{\tfrac{1}{2}n}\right\}\right|}_{\text{Faktor 2}} \cdot \underbrace{\left|\left\{y \in \mathbb{Z} \ :\ |y| \leq n \cdot \sqrt{\tfrac{1}{2}n}\right\}\right|}_{\text{Faktor 3}}$$

Wir schätzen die drei Faktoren nach oben ab:

1. Seien $x \in \mathbb{Z}^n$ und $y \in \mathbb{Z}$ beliebig, aber fest mit den angegebenen Eigenschaften. Mit $z_i := x_i - ye_i$ für $i = 1, \ldots, n$ gilt wegen $\sum_{i=1}^{n} e_i a_i = s$:

   $$\sum_{i=1}^{n} a_i x_i = ys \qquad \Longleftrightarrow \qquad \sum_{i=1}^{n} a_i z_i = 0$$

   Der Vektor $z = (z_1, \ldots, z_n)$ ist fest. Es gilt $z \neq 0$, da sonst aus $x = y\widehat{e}$ und $x \notin \{0, \pm\widehat{e}\}$ folgt $|y| \geq 2$ und $\|x\| \geq 2\|\widehat{e}\|$ — Widerspruch zu $\|x\| \leq \|\widehat{e}\|$.
   Sei $z_j \neq 0$ für ein festes j. Für fest gewählte a_i mit $i \neq j$ ist die Gleichung $\sum_{i=1}^{n} a_i z_i = 0$ für höchstens ein $a_j \in [1, A]$ erfüllt. Es folgt:

   $$\text{Faktor 1} \leq \mathrm{Ws}\left[\sum_{i=1}^{n} a_i z_i = 0\right] \leq \frac{1}{A}$$

2. J.C.Lagarias und A.M. Odlyzko [LaOd85] haben gezeigt, daß für hinreichend große n gilt:

   $$\left|\left\{x \in \mathbb{Z}^n \ :\ \|x\| \leq \sqrt{\tfrac{1}{2}n}\right\}\right| \leq 2^{c_0 n} \qquad \text{mit } c_0 = 1,54725$$

3. Es gilt:

   $$\left|\left\{y \in \mathbb{Z} \ :\ |y| \leq n \cdot \sqrt{\tfrac{1}{2}n}\right\}\right| \leq 1 + 2\left(n \cdot \sqrt{\tfrac{1}{2}n}\right)$$

Damit ergibt sich:

$$P(n) \leq \frac{2^{c_0 n}}{A} \cdot \left(1 + 2n \cdot \sqrt{\tfrac{1}{2}n}\right)$$

Wegen $\frac{1}{d} > 1,547269 > c_0$ und der unteren Schranke (6.1) auf Seite 48

$$A \geq \max_{i=1,\ldots,n} a_i \geq 2^{\frac{n}{d}},$$

gilt $\lim_{n\to\infty} P(n) = 0$. ■

6.3 CJLOSS-Gitterbasis

1992 haben M.J. Coster, A. Joux, B.A. LaMacchina, A.M. Odlyzko, C.P. Schnorr und und J. Stern [CJLOSS92] durch Modifikation des Vektors b_{n+1} der Lagarias-Odlyzko-Basis die Grenzdichte auf $0,9408$ erhöht. Die CJLOSS-Basis erhält man aus der Lagarias-Odlyzko-Gitterbasis (6.2), indem der Zeilenvektor b_{n+1} durch $b'_{n+1} := (\frac{1}{2}, \ldots, \frac{1}{2}, Ns)$ ersetzt wird:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \\ b'_{n+1} \end{bmatrix} := \begin{bmatrix} 1 & 0 & \cdots & 0 & Na_1 \\ 0 & 1 & & 0 & Na_2 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & & 1 & Na_n \\ \frac{1}{2} & \frac{1}{2} & \cdots & \frac{1}{2} & Ns \end{bmatrix} \tag{6.9}$$

N ist eine hinreichend große Zahl, im Beweis wählen wir $N > \frac{1}{2}\sqrt{n}$. Sei

$$L_{\text{CJLOSS}} := L(b_1, \ldots, b_{n+1})$$

Der Lösung e des Subsetsum-Problems, die nach Voraussetzung existiert, ist der folgende Lösungsvektor zugeordnet:

$$\widehat{e}' := \left(\sum_{i=1}^{n} e_i b_i\right) - b'_{n+1} = \left(e_1 - \tfrac{1}{2}, e_2 - \tfrac{1}{2}, \ldots, e_n - \tfrac{1}{2}, 0\right) \tag{6.10}$$

Da $e_i \in \{0,1\}$, gilt $\|\widehat{e}'\| = \frac{1}{2}\sqrt{n}$. Im Vergleich zum Lösungsvektor e der Lagarias-Odlyzko-Basis (6.3) ist $e' = e_i - \frac{1}{2}$. Der Vorteil der CJLOSS-Basis liegt darin, daß ihr Lösungsvektor bis zu einem Faktor $\sqrt{2}$ kleiner als der Lösungsvektor $\widehat{e}$ der Lagarias-Odlyzko-Basis ist.

Satz 6.3.1
Sei $A > 0$ beliebig, aber fest. Die Subsetsum-Aufgabe wird für hinreichend große n für fast alle ganzzahligen Gewichte $(a_1, \ldots, a_n) \in_R [1, A]^n$ mit Dichte $d < 0,9408$ durch zweifache Anwendung des Gitterorakels auf die CJLOSS-Basis effizient gelöst.

Beweis. Wir schätzen die Wahrscheinlichkeit ab, daß das Orakel einen kürzesten Gittervektor $\widehat{x} = (x_1, \ldots, x_{n+1}) \neq \pm\widehat{e}'$ liefert. Für den Vektor $\widehat{x}$ gilt:

$$\begin{aligned} \|\widehat{x}\| &\leq \|\widehat{e}'\| \leq \tfrac{1}{2}\sqrt{n} \\ \widehat{x} &\in L_{\text{CJLOSS}} = L(b_1, \ldots, b_n, b'_{n+1}) \\ \widehat{x} &\notin \{0, \pm\widehat{e}'\} \end{aligned} \tag{6.11}$$

Seien $y_1, \ldots, y_n, y \in \mathbb{Z}$ die Koeffizienten der Darstellung von $\widehat{x}$ als Linearkombination der Basisvektoren:

$$\widehat{x} = \sum_{i=1}^{n} y_i b_i + y b'_{n+1}$$

Betrachten wir die letzte Komponente: Wegen $\sum_{i=1}^n y_i a_i + ys \in \mathbb{Z}$ gilt für $N > \frac{1}{2}\sqrt{n}$, daß $x_{n+1} = 0$ ist. Ferner gilt:

$$x_i = y_i + \tfrac{1}{2}y \qquad \text{für } i = 1, \ldots, n \tag{6.12}$$

$$x_{n+1} = N\left(\sum_{i=1}^n a_i y_i + ys\right) \tag{6.13}$$

Wegen $x_{n+1} = 0$ folgt aus (6.13):

$$\sum_{i=1}^n a_i y_i = -ys \tag{6.14}$$

Wir erhalten mit $t := \sum_{i=1}^n a_i$:

$$\begin{aligned}
\sum_{i=1}^n x_i a_i &= \sum_{i=1}^n a_i\left(y_i + \tfrac{1}{2}y\right) && \text{(wegen (6.12))}\\
&= \sum_{i=1}^n y_i a_i + \tfrac{1}{2}y\sum_{i=1}^n a_i\\
&= -ys + \tfrac{1}{2}yt && \text{(wegen (6.14))}\\
&= \tfrac{1}{2}y\,(t-2s)
\end{aligned}$$

Aus diesem Resultat folgt mit $\alpha := \max_{i=1,\ldots,n} a_i$:

$$\begin{aligned}
|y(t-2s)| &\le 2 \cdot \sum_{i=1}^n |x_i a_i| && \text{(Dreiecksungleichung)}\\
&\le 2\alpha \cdot \|\widehat{x}\|_1 && \text{(wobei } \|\cdot\|_1 \text{ die 1-Norm ist)}\\
&\le 2\alpha\sqrt{n} \cdot \|\widehat{x}\|_2 && \text{(wobei } \|\cdot\|_2 \text{ die Euklidische Norm ist)}\\
&\le \alpha n && \text{(wegen (6.11): } \|\widehat{x}\| \le \|\widehat{e}'\| = \tfrac{1}{2}\sqrt{n})
\end{aligned} \tag{6.15}$$

Um eine geeignete Schranke für $|y|$ zu erhalten, reduzieren wir die Subsetsum-Aufgabe, so daß dann für das Problem gilt

$$|y| \le 2n \tag{6.16}$$

Falls $|t-2s| \ge \frac{1}{2}\alpha$, wird nicht reduziert, da wegen (6.15) bereits $|y| \le \frac{\alpha n}{|t-2s|} \le 2n$ gilt. Falls $|t-2s| < \frac{1}{2}\alpha$, dann entferne ein Gewicht a_i mit $a_i = \alpha$ aus der Aufgabe. Wir können zwei Probleme lösen: Eines mit a_i in der Teilmenge, die sich zu s summiert, und ein anderes mit a_i in der Teilmenge, die sich zu $t-s$ summiert.

Für das erste Problem gilt mit $s_{\text{neu}} = s - \alpha$ und $t_{\text{neu}} = t - \alpha$:

$$|t_{\text{neu}} - 2s_{\text{neu}}| = |t - \alpha - 2s + 2\alpha| > \tfrac{1}{2}\alpha$$

Für das andere Problem gilt mit $s_{\text{neu}} = s$ und $t_{\text{neu}} = t - \alpha$:

$$|t_{\text{neu}} - 2s_{\text{neu}}| = |t - \alpha - 2s - 2\alpha| > \tfrac{1}{2}\alpha$$

Beide reduzierte Probleme erfüllen die Ungleichung $|t-2s| \ge \frac{1}{2}\alpha$. Aus (6.15) folgt, daß die Forderung (6.16), also $|y| \le 2n$, erfüllt ist.

Wir wenden das Orakel, sofern reduziert wurde, auf beide Probleme an. Es bleibt die Wahrscheinlichkeit abzuschätzen, daß das Orakel einen kürzesten Gittervektor $\widehat{x}$ mit Eigenschaften (6.11) liefert. Es bezeichne im weiteren

$$P(n) := \text{Ws}[\,\text{Es existiert ein } \widehat{x} \text{ mit (6.11)}]$$

die Wahrscheinlichkeit bezüglich zufälliger und gleichverteilter $(a_1, \ldots, a_n)$ aus $[1, A]^n$. Zu zeigen: Für Dichte $d < 0,94080$ gilt $\lim_{n\to\infty} P(n) = 0$. Aus

$$P(n) = \mathrm{Ws}\left[\begin{array}{l} \exists \widehat{x} \in L_{\mathrm{CJLOSS}}, \exists y \in \mathbb{Z}, \text{ so daß:} \\ \\ \|\widehat{x}\| \le \|\widehat{e}'\|, \quad |y| \le 2n, \quad \widehat{x}' \notin \{0, \pm\widehat{e}'\}, \quad \sum_{i=1}^n a_i x_i = \frac{1}{2} y(t-2s) \end{array}\right]$$

folgt:

$$P(n) \le \overbrace{\mathrm{Ws}\left[\begin{array}{l} \sum\limits_{i=1}^n a_i x_i = \frac{1}{2} y(t-2s),\ x \in \mathbb{Z}^n + \mathbb{Z}\left(\frac{1}{2}, \ldots, \frac{1}{2}\right),\ y \in \mathbb{Z} \text{ fest}, \\ \|x\| \le \|e\|,\ |y| \le n \cdot \sqrt{2n},\ x \notin \{0, \pm e\} \end{array}\right]}^{\text{Faktor 1}}$$

$$\cdot \underbrace{\left|\left\{x \in \mathbb{Z}^n + \left(\tfrac{1}{2}, \ldots, \tfrac{1}{2}\right)\mathbb{Z} \ :\ \|x\| \le \tfrac{1}{2}\sqrt{n}\right\}\right|}_{\text{Faktor 2}} \cdot \underbrace{\left|\{y \in \mathbb{Z} \ :\ |y| \le 2n\}\right|}_{\text{Faktor 3}}$$

Wir schätzen die drei Faktoren nach oben ab:

1. Seien $x \in \mathbb{Z}^n + \mathbb{Z}\left(\frac{1}{2}, \ldots, \frac{1}{2}\right)$ und $y \in \mathbb{Z}$ beliebig, aber fest mit den angegebenen Eigenschaften. Für

$$z_i := x_i + y\left(e_i - \tfrac{1}{2}\right) = x_i + y e_i' \qquad \text{für } i = 1, \ldots, n$$

gilt:

$$\sum_{i=1}^n a_i x_i = \tfrac{1}{2} \cdot y \cdot (t-2s) \qquad \Longleftrightarrow \qquad \sum_{i=1}^n a_i z_i = 0$$

Der Vektor $z = (z_1, \ldots, z_n)$ ist fest. Es gilt $z \ne 0$, da sonst aus $x = ye'$ und $x \notin \{0, \pm e'\}$ folgt $|y| \ge 2$ und $\|x\| \ge 2\,|e'|$ — Widerspruch zu $\|x\| \le \|e'\|$.

Sei $z_j \ne 0$ für ein festes j. Für fest gewählte a_i mit $i \ne j$ ist die Gleichung $\sum_{i=1}^n a_i z_i = 0$ für höchstens ein $a_j \in [1, A]$ erfüllt. Es folgt:

$$\text{Faktor 1} \le \mathrm{Ws}\left[\sum_{i=1}^n a_i z_i = 0\right] \le \frac{1}{A}$$

2. J.C.Lagraias und A.M. Odlyzko [LaOd85] haben die Anzahl der Gitterpunkte von $\mathbb{Z}^n$ in einer Kugel mit Radius $\sqrt{\alpha n}$ um den Ursprung

$$N(n, \alpha) := \left|\left\{x \in \mathbb{Z}^n \ :\ \|x\|^2 \le \alpha \cdot n\right\}\right|$$

untersucht. Für hinreichend große n zeigen sie, daß für jedes $u > 0$ gilt

$$N(n, \alpha) \le 2^{(\log_2 e) \cdot \delta(\alpha, u) \cdot n}$$

mit $\delta(\alpha, u) = \alpha u + \ln\theta(e^{-u})$ und der Theta-Funktion $\theta(z) = 1 + 2\sum_{i=1}^\infty z^{i^2}$. Für festes α kann man die Minimalstelle u_0 von $\delta(\alpha, u)$ numerisch annähern. Für $\alpha = \frac{1}{4}$ erhalten wir $u_0 \approx 1,8132$. Es folgt:

$$\min_{u>0} \delta\left(\tfrac{1}{4}, u\right) \le \delta\left(\tfrac{1}{4}; 1,8132\right) \approx 0,7367$$

Wir können daher den zweiten Faktor nach oben abschätzen durch:

$$\left|\left\{x \in \mathbb{Z}^n + \left(\tfrac{1}{2}, \ldots, \tfrac{1}{2}\right)\mathbb{Z} \ :\ \|x\| \le \tfrac{1}{2} \cdot \sqrt{n}\ \right\}\right| \le 2^{c_0' n} \qquad \text{mit } c_0' = 1,0629$$

3. Es gilt:

$$|\{y \in \mathbb{Z} \, : \, |y| \leq 2n\}| \leq 1 + 4n$$

Damit ergibt sich:

$$P(n) \leq (4n+1) \cdot \frac{2^{c_0' n}}{A}$$

Wegen $\frac{1}{d} > 1,062925 > c_0'$ und $A \geq \max_{i=1,\dots,n} a_i \geq 2^{\frac{n}{d}}$ gilt: $\lim_{n \to \infty} P(n) = 0$. ■

Kapitel 7

HKZ- und β-reduzierte Gitterbasen

Im Kapitel 5 haben wir den Reduktionsbegriff der LLL-reduzierten Basis $b_1, \ldots, b_n$ kennengelernt. Zwar arbeitet der Reduktionsalgorithmus **??** in Polynomialzeit, aus der Eigenschaft „LLL-reduziert“ haben wir in Satz 5.1.4 nur zeigen können, daß die Länge des kürzesten Basisvektors maximal ein in n exponentielles Vielfaches des ersten sukzessiven Minimums ist. Aus diesem Grund benötigen wir stärkere Reduktionsbegriffe. In diesem Kapitel lernen wir Begriff einer HKZ-reduzierten Gitterbasis kennen. Die Verallgemeinerung, β-reduzierte Gitterbasen, umfaßt sowohl LLL- als auch HKZ-reduzierte Basen.

7.1 HKZ-reduzierte Gitterbasen

Zu einer Basis $b_1, \ldots, b_n$ des Gitters L sind die die projizierten Gitter L_i, $i = 1, \ldots, n$, erklärt durch:

$$L_i = \pi_i(L) := L\left(\pi_i(b_i), \pi_i(b_{i+1}), \ldots, \pi_i(b_n)\right)$$

C. Hermite [Hermite1850] sowie unabhängig A. Korkine und G. Zolotareff [KoZo1873, KoZo1877] haben die folgende Definition einer reduzierten Basis in der Sprache quadratischer Formen formuliert:

Definition 7.1.1 (HKZ-reduzierte Basis)
Eine geordnete Basis $b_1, \ldots, b_n \in \mathbb{R}^m$ ist nach Hermite und Korkine-Zolotareff reduziert (eine HKZ-reduzierte Basis), wenn:

a) $|\mu_{i,j}| \leq \frac{1}{2}$ *für* $1 \leq j < i \leq n$

b) $\|\widehat{b}_i\| = \lambda_1(L_i)$ *für* $i = 1, \ldots, n$

Insbesondere ist $\|b_1\| = \lambda_1(L)$, d.h. der Vektor b_1 ist ein kürzester, nichttriviale Gittervektor. Für eine HKZ-reduzierte Basis $b_1, \ldots, b_n$ ist auch für $1 \leq j \leq n$

$$\pi_j(b_j), \pi_j(b_{j+1}), \ldots, \pi_j(b_n)$$

eine HKZ-reduzierte Basis. Wie gut approximieren der Basisvektoren die kürzesten, nicht-trivialen Gittervektoren?

Satz 7.1.2
Für jede $b_1, \dots, b_n$ HKZ-reduzierte Basis von L gilt für $i = 1, \dots, n$:

$$\frac{4}{i+3} \leq \frac{\|b_i\|^2}{\lambda_i(L)^2} \leq \frac{i+3}{4}$$

Zum Vergleich: Für eine LLL-reduzierte Basis $b_1, \dots, b_n$ gilt nach Satz 5.1.4 auf Seite 36 mit $\alpha = \frac{1}{\delta - \frac{1}{4}}$:

$$\alpha^{1-i} \leq \frac{\|\widehat{b}_i\|^2}{\lambda_i(L)^2} \leq \frac{\|b_i\|^2}{\lambda_i(L)^2} \leq \alpha^{n-1}$$

Beweis (zu Satz 7.1.2). Wir zeigen zunächst die obere Schranke $\frac{\|b_i\|^2}{\lambda_i(L)^2} \leq \frac{i+3}{4}$. Für das Gitter $L_i = \pi_i(L)$ gilt:

$$\|\widehat{b}_i\| = \lambda_1(L_i) \leq \lambda_i(L) \tag{7.1}$$

Die Gleichheit folgt aus der HKZ-Eigenschaft. Die Abschätzung gilt, denn es gibt i linear unabhängige Gittervektoren $a_1, \dots, a_i \in L$ mit

$$\|a_1\| \leq \|a_2\| \leq \cdots \|a_i\| \leq \lambda_i(L),$$

und es existiert ein j mit $j \leq i$ und $\pi_i(a_j) \neq 0$, also $\pi_i(a_j) \in L_i \setminus \{0\}$. Wir erhalten aus den Eigenschaften einer HKZ-reduzierten Basis und (7.1):

$$\begin{aligned}
\|b_i\|^2 &= \|\widehat{b}_i\|^2 + \sum_{j=1}^{i-1} (\mu_{i,j})^2 \cdot \|\widehat{b}_j\|^2 \\
&\leq \lambda_i(L)^2 + \tfrac{1}{4} \sum_{j=1}^{i-1} \lambda_j(L)^2 && \text{(wegen (7.1) und Basis längenreduziert)} \\
&\leq \tfrac{i+3}{4} \cdot \lambda_i(L)^2
\end{aligned}$$

Wir zeigen die untere Schranke $\frac{4}{i+1} \leq \frac{\|b_i\|^2}{\lambda_i(L)^2}$. Aus der Definition einer HKZ-reduzierten Basis erhalten wir für $j \leq i$:

$$\|\widehat{b}_j\|^2 = \lambda_1(L_j)^2 \leq \|\pi_j(b_i)\|^2 \leq \|b_i\|^2$$

Es gilt:

$$\|b_j\|^2 = \|\widehat{b}_j\|^2 + \sum_{t=1}^{j-1} (\mu_{j,t})^2 \, \|\widehat{b}_t\|^2 \leq \tfrac{j+3}{4} \cdot \|b_i\|^2$$

Wir erhalten die Behauptung:

$$\lambda_i(L)^2 \leq \max_{j=1,\dots,i} \|b_j\|^2 \leq \max_{j=1,\dots,i} \left\{ \frac{j+3}{4} \cdot \|b_i\|^2 \right\} \leq \frac{i+3}{4} \, \|b_i\|^2$$

∎

Weitere Sätze über HKZ-reduzierte Gitterbasen finden sich in der Originalarbeit [LLS90] von J.C. Lagarias, H.W. Lenstra und C.P. Schnorr.

7.2 β-reduzierte Gitterbasen

C.P. Schnorr [Schnorr87, Schnorr94a] hat die Begriffe der HKZ- und der LLL-reduzierten Basen zu β-reduzierten Basen verallgemeinert. Während alle bekannten Reduktionsalgorithmen zu HKZ-Basen expontielle Laufzeit haben, gibt es für kleine Blockgrößen praktikable Reduktionsalgorithmen mit Laufzeiten wie bei der schwächeren LLL-Reduktion. Allerdings ist offen, ob diese Algorithmen polynomielle Laufzeit haben.

Definition 7.2.1 (β-reduzierte Basis)
Sei $b_1, \ldots, b_n \in \mathbb{R}^m$ eine geordnete Basis und $\beta \in \{2, 3, \ldots, n\}$ gegeben. Die geordnete Basis $b_1, \ldots, b_n \in \mathbb{R}^m$ heißt β-reduziert (blockreduziert mit Blockgröße β), wenn:

a) $|\mu_{i,j}| \leq \frac{1}{2}$ für $1 \leq j < i \leq n$

b) $\pi_i(b_i), \pi_i(b_{i+1}), \ldots, \pi_i(b_{i+\beta-1})$ ist HKZ-reduzierte Basis für $i = 1, \ldots, n - \beta + 1$.

Jede $(\beta + 1)$-reduzierte Basis ist auch β-reduziert und eine n-reduzierte Basis $b_1, \ldots, b_n$ ist eine HKZ-reduzierte Basis. Die zweite Eigenschaft bedeutet:

$$\|\widehat{b}_i\| \leq \lambda_1\Big(\pi_i\big(L(b_1, \ldots, b_{\min(i+\beta-1,n)})\big)\Big)$$

Wir werden in Defintion 7.4.1 im Abschnitt 7.4 den Begriff der β-reduzierten Basis zur (β, δ)-reduzierten Basis verallgemeinern. Die LLL-Reduktion ist ein Spezialfall der Blockreduktion mit $\beta = 2$:

Satz 7.2.2
Die 2-reduzierten Basen entsprechen genau den LLL-reduzierten Basen mit $\delta = 1$.

Beweis. Sei $b_1, \ldots, b_n$ eine 2-reduzierte Basis. Dann gilt für $i = 1, \ldots, n-1$:

$$\lambda_1\big(L(\pi_i(b_i), \pi_i(b_{i+1}))\big)^2 = \|\widehat{b}_i\|^2 \leq \|\pi_i(b_{i+1})\|^2 = \|\widehat{b}_{i+1}\|^2 + \mu_{i+1,i}^2\|\widehat{b}_i\|^2$$

Mit $\delta = 1$ ist dies das zweite Kriterium von LLL-reduziert:

$$\delta \cdot \|\widehat{b}_i\|^2 \leq \|\widehat{b}_{i+1}\|^2 + \mu_{i+1,i}^2\|\widehat{b}_i\|^2 \qquad \text{für } i = 1, \ldots, n-1$$

Weil jede β-reduzierte Basis längenreduziert ist, erfüllt $b_1, \ldots, b_n$ die LLL-Eigenschaften.

Umgekehrt zeigen wir, jede mit $\delta = 1$ LLL-reduzierte Basis $b_1, \ldots, b_n$ ist auch 2-reduziert, also jeder Vektor in $L(\pi_i(b_i), \pi_i(b_{i+1}))$ ungleich dem Nullvektor ist nicht kürzer als $\pi_i(b_i) = \widehat{b}_i$. Wegen

$$\|u \cdot \pi_i(b_i) + v \cdot \pi_i(b_{i+1})\|^2 = (u + v \cdot \mu_{i+1,i})^2 \cdot \|\widehat{b}_i\|^2 + v^2\|\widehat{b}_{i+1}\|^2$$

ist zu zeigen, daß für alle $(u, v) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ gilt:

$$(u + v\mu_{i+1,i})^2 \cdot \|\widehat{b}_i\|^2 + v^2 \cdot \|\widehat{b}_{i+1}\|^2 \geq \|\widehat{b}_i\|^2 \tag{7.2}$$

Die Ungleichung (7.2) gilt für $v = 0$, da dann der Koeffizient $u \in \mathbb{Z}$ ungleich Null ist. Da die Basis mit Parameter $\delta = 1$ LLL-reduziert ist, gilt nach dem zweiten LLL-Kriterium

$$\underbrace{\delta}_{=1} \cdot \|\widehat{b}_i\|^2 \leq \|\widehat{b}_{i+1}\|^2 + \mu_{i+1,i}^2 \cdot \|\widehat{b}_i\|^2 \tag{7.3}$$

und wir erhalten unmittelbar Ungleichung (7.2) den Fall $v = 1$. Da die Basis längenreduziert ist, gilt $\mu_{i+1,i}^2 \leq \frac{1}{4}$ und nach (7.3) folgt $\frac{3}{4} \cdot \|\widehat{b}_i\|^2 \leq \|\widehat{b}_{i+1}\|^2$. Für den Fall $|v| \geq 2$ erhalten wir aus

$$(u + v\mu_{i+1,i})^2 \cdot \|\widehat{b}_i\|^2 + v^2 \cdot \|\widehat{b}_{i+1}\|^2 \geq v^2 \cdot \|\widehat{b}_{i+1}\|^2 \geq 4 \cdot \|\widehat{b}_{i+1}\|^2 \geq 3 \cdot \|\widehat{b}_i\|^2$$

die Ungleichung (7.2). ■

Wir untersuchen die Eigenschaften β-reduzierter Basen. Wir geben zwei Sätze über β-reduzierte Basen an, die wir später in diesem Abschnitt beweisen werden:

Satz 7.2.3
Für jede β-reduzierte Basis $b_1, \ldots, b_n$ des Gitters L gilt:

a) $\dfrac{\|\widehat{b}_i\|^2}{\lambda_i(L)^2} \leq (\gamma_\beta)^{2 \cdot \frac{n-i}{\beta-1}}$ *für* $i = 1, \ldots, n$

b) $\dfrac{\|b_i\|^2}{\lambda_i(L)^2} \leq (\gamma_\beta)^{2 \cdot \frac{n-i}{\beta-1}} \cdot \dfrac{i+3}{4}$ *für* $i = 1, \ldots, n$

Dabei ist γ_β die Hermite-Konstante der Dimension β.

Wir betrachten eine untere Schranke für $\frac{\|b_i\|^2}{\lambda_i(L)^2}$, also eine obere Schranke für $\frac{\lambda_i(L)^2}{\|b_i\|^2}$.

Satz 7.2.4
Für jede β-reduzierte Basis $b_1, \ldots, b_n$ des Gitters L gilt:

$$\frac{\lambda_i(L)^2}{\|b_i\|^2} \leq (\gamma_\beta)^{2 \cdot \frac{i-1}{\beta-1}} \cdot \frac{i+3}{4} \qquad \text{für } i = 1, \ldots, n.$$

Für $i \leq \beta$ können wir die Schranken der Sätze 7.2.3 und 7.2.4 durch die stärkeren Schranken aus 7.1.2 ersetzen, da die β-reduzierten Basen für $i \leq \beta$ HKZ-reduzierte Basen sind. Die Werte $(\gamma_\beta)^{\frac{2}{\beta-1}}$ aus den Sätzen 7.2.3 und 7.2.4 sind bekannt für $\beta = 2, 3, \ldots, 8$:

β	2	3	4	5	6	7	8
$(\gamma_\beta)^{\frac{2}{\beta-1}}$	$\frac{4}{3}$	$2^{1/3}$	$2^{1/3}$	$2^{3/10}$	$2^{2/5} \cdot 3^{-1/15}$	$2^{2/7}$	$2^{2/7}$
$\approx$	$1,333$	$1,260$	$1,260$	$1,231$	$1,226$	$1,219$	$1,219$

Es ist ein offenes Problem, minimale Konstanten $C_{\beta,n}$ zu finden, so daß

$$\frac{\|b_1\|^2}{\lambda_1(L)^2} \leq C_{\beta,n}$$

für alle β-reduzierten Basen $b_1, \ldots, b_n$ vom Rang n gilt. Die Schranke aus Satz 7.2.3 ist für $n \geq 3$ nicht scharf. Bisher weiß man:

- $C_{2,n} = \left(\frac{4}{3}\right)^{n-1}$ aus [BaKa84]
- $C_{3,n} = \left(\sqrt{\frac{3}{2}}\right)^{n-3}$ für ungerade $n \geq 3$ aus [Schnorr94a]

Es gilt:

Lemma 7.2.5
Für jede β-reduzierte Basis $b_1, \ldots, b_n \in \mathbb{R}^m$ gilt

$$\|b_1\| \leq (\gamma_\beta)^{\frac{n-1}{\beta-1}} \cdot M$$

mit $M := \max\left\{\|\widehat{b}_{n-\beta+2}\|, \|\widehat{b}_{n-\beta+3}\|, \ldots, \|\widehat{b}_n\|\right\}$.

Beweis. Wir erweitern die Basis $b_1, \dots, b_n$ durch $\beta - 2$ linear unabhängige Vektoren zu

$$b_{-\beta+3}, b_{-\beta+4}, \dots, b_{-1}, b_0, b_1, \dots, b_n \tag{7.4}$$

so, daß gilt:

$$\|b_i\| = \|b_1\| \qquad \text{für } i \leq 0 \tag{7.5}$$

$$\langle b_i, b_j \rangle = 0 \qquad \text{für } i \leq 0,\ i \leq j \text{ und } j = -\beta+3, -\beta+4, \dots, n \tag{7.6}$$

Dazu betten wir die Basis in den $\mathbb{R}^{m+\beta-2}$ ein: Wir wählen zum Beispiel $b_{-\beta+3}, b_{-\beta+4}, \dots, b_{-1}, b_0$ als $\|b_1\|$-Vielfaches der kanonischen Einheitsvektoren in die zusätzlichen $\beta - 2$ Richtungen. Die Gitterbasis (7.4) ist β-reduziert und besteht aus mindestens $2(\beta - 1)$ Vektoren Für jedes i mit $-\beta + 3 \leq i \leq n - \beta + 1$ bilden die Vektoren

$$\pi_i(b_i), \pi_i(b_{i+1}), \dots, \pi_i(b_{i+\beta-1})$$

eine β-reduzierte und damit eine HKZ-reduzierte Basis des Gitters $L\left(\widehat{b}_i, \widehat{b}_{i+1}, \dots, \widehat{b}_{i+\beta-1}\right)$ (Beachte Eigenschaft (7.6)), so daß gilt:

$$\|\widehat{b}_i\|^2 \leq \lambda_1\left(L\left(\widehat{b}_i, \widehat{b}_{i+1}, \dots, \widehat{b}_{i+\beta-1}\right)\right)^2$$

Aus der Definition der Hermite-Konstanten

$$\gamma_\beta = \sup\left\{ \frac{\lambda_1(L)^2}{(\det L)^{2/\beta}} \,\middle|\, \mathrm{Rang}(L) = \beta \right\}$$

folgt für $i = -\beta + 3, -\beta + 4, \dots, n - \beta + 1$:

$$\|\widehat{b}_i\|^\beta \leq (\gamma_\beta)^{\frac{\beta}{2}} \prod_{s=0}^{\beta-1} \|\widehat{b}_{i+s}\|$$

Durch Multiplikation der $n - 1$ Ungleichungen erhalten wir:

$$\begin{aligned}\prod_{i=-\beta+3}^{n-\beta+1} \|\widehat{b}_i\|^\beta \leq (\gamma_\beta)^{\frac{\beta(n-1)}{2}} & \|\widehat{b}_{-\beta+3}\|^1 \cdot \|\widehat{b}_{-\beta+4}\|^2 \cdots \|\widehat{b}_1\|^{\beta-1} \\ & \cdot \|\widehat{b}_2\|^\beta \cdot \|\widehat{b}_3\|^\beta \cdots \|\widehat{b}_{n-\beta+1}\|^\beta \\ & \cdot \|\widehat{b}_{n-\beta+2}\|^{\beta-1} \cdots \|\widehat{b}_{n-1}\|^2 \cdot \|\widehat{b}_n\|^1\end{aligned}$$

Dies impliziert:

$$\begin{aligned}&\|\widehat{b}_{-\beta+3}\|^{\beta-1} \cdot \ldots \|\widehat{b}_0\|^2 \cdot \|\widehat{b}_1\|^1 \\ \leq (\gamma_\beta)^{\frac{\beta(n-1)}{2}} & \|\widehat{b}_{n-\beta+2}\|^{\beta-1} \cdot \|\widehat{b}_{n-\beta+2}\|^{\beta-1} \cdots \|\widehat{b}_{n-1}\|^2 \cdot \|\widehat{b}_n\|^1\end{aligned} \tag{7.7}$$

Wegen Eigenschaft (7.5) ist $\|\widehat{b}_i\| = \|b_1\|$ für $i \leq 0$, so daß aus Abschätzung (7.7) folgt

$$\|b_1\|^{\binom{\beta}{2}} \leq (\gamma_\beta)^{\frac{\beta(n-1)}{2}} \cdot M^{\binom{\beta}{2}}$$

mit $M := \max\left\{\|\widehat{b}_{n-\beta+2}\|, \|\widehat{b}_{n-\beta+3}\|, \dots, \|\widehat{b}_n\|\right\}$. Wir erhalten die Behauptung:

$$\|b_1\| \leq (\gamma_\beta)^{\frac{n-1}{\beta-1}} \cdot M$$

■

Wie gut approximiert der erste Vektor einer β-reduzierten Basis einen kürzesten, nicht-trivialen Vektor?

Korollar 7.2.6
Für jede β-reduzierte Basis $b_1, \ldots, b_n$ des Gitters L gilt:

$$\|b_1\| \leq (\gamma_\beta)^{\frac{n-1}{\beta-1}} \cdot \lambda_1(L)$$

Beweis. Induktion über n:

- Für $n = \beta$ ist $b_1, \ldots, b_n$ eine HKZ-reduzierte Basis und es gilt $\|b_1\| = \lambda_1(L)$. Weil für die Hermite-Konstante $\gamma_n \geq 1$ gilt, erhalten wir die Behauptung.
- Sei $n > \beta$ und v einer der kürzesten Gittervektoren ungleich dem Nullvektor. O.B.d.A. sei $v \notin L(b_1, b_2, \ldots, b_{n-1})$, denn sonst betrachte die Basis $b_1, \ldots, b_{n-1}$ und die Behauptung folgt aus der Induktionsannahme. Wegen $v \notin L(b_1, \ldots, b_{n-1})$. gilt $\pi_i(v) \neq 0$ für $i = n-\beta+1, n-\beta+2, \ldots, n-1$. Wir erhalten mit $L_i = \pi_i(L)$ für $i = n-\beta+1, n-\beta+2, \ldots, n$:

$$\lambda_1(L) = \|v\| \geq \lambda_1(L_i) = \|\widehat{b}_i\|$$

Die Gleichheit $\lambda_1(L_i) = \|\widehat{b}_i\|$ gilt, da $\pi_{n-\beta+1}(b_i)$, $i = n-\beta+1, n-\beta+2, \ldots, n$ eine HKZ-reduzierte Basis ist. Wegen

$$\begin{aligned}\lambda_1(L) &\geq \max\left\{\|\widehat{b}_i\| \;:\; i = n-\beta+1, n-\beta+2, \ldots, n\right\}\\ &\geq \max\left\{\|\widehat{b}_i\| \;:\; i = n-\beta+2, n-\beta+3, \ldots, n\right\} = M\end{aligned}$$

folgt die Behauptung unmittelbar aus Lemma 7.2.5:

$$\|b_1\| \leq (\gamma_\beta)^{\frac{n-1}{\beta-1}} \cdot M \leq (\gamma_\beta)^{\frac{n-1}{\beta-1}} \cdot \lambda_1(L)$$

■

Beweis (zu Satz 7.2.3). Korollar 7.2.6 liefert für die Gitter $L_i = \pi_i(L)$ mit $i = 1, \ldots, n$:

$$\|\widehat{b}_i\| \leq (\gamma_\beta)^{\frac{n-i}{\beta-1}} \lambda_1(L_i) \tag{7.8}$$

Ferner ist $\lambda_1(L_i) \leq \lambda_i(L)$, denn es gibt i linear unabhängige Gittervektoren v, deren Länge höchstens $\lambda_i(L)$ ist und von denen ein Vektor $\pi_i(v) \neq 0$ erfüllt. Also:

$$\lambda_1(L_i) \leq \pi_i(v) \leq \lambda_i(L)$$

Wir erhalten die erste Behauptung, daß für $i = 1, \ldots, n$ gilt:

$$\frac{\|\widehat{b}_i\|^2}{\lambda_i(L)^2} \leq (\gamma_\beta)^{2\cdot\frac{n-i}{\beta-1}}$$

Aus (7.8), $\mu_{i,j}^2 \leq \frac{1}{4}$ (die Basis ist längenreduziert) und $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_j$ folgt:

$$\begin{aligned}\|b_i\|^2 &= \|\widehat{b}_i\|^2 + \sum_{j=1}^{i-1} (\mu_{i,j})^2 \|\widehat{b}_j\|^2\\ &\leq (\gamma_\beta)^{2\cdot\frac{n-i}{\beta-1}} \cdot \lambda_i(L)^2 + \frac{1}{4}\sum_{j=1}^{i-1} (\gamma_\beta)^{2\cdot\frac{n-j}{\beta-1}} \cdot \lambda_j(L)^2\\ &\leq (\gamma_\beta)^{2\cdot\frac{n}{\beta-1}} \cdot \left((\gamma_\beta)^{2\cdot\frac{-i}{\beta-1}} + \frac{1}{4}\sum_{j=1}^{i-1} (\gamma_\beta)^{2\cdot\frac{-j}{\beta-1}}\right) \cdot \lambda_i(L)^2\end{aligned}$$

Wir schätzen die Summanden durch $(\gamma_\beta)^{2\cdot\frac{-1}{\beta-1}}$ nach oben ab und erhalten:

$$\begin{aligned}\|b_i\|^2 &\leq (\gamma_\beta)^{2\cdot\frac{n}{\beta-1}} \cdot (\gamma_\beta)^{2\cdot\frac{-1}{\beta-1}} \cdot \left(1 + \frac{i-1}{4}\right) \cdot \lambda_i(L)^2 \\ &\leq (\gamma_\beta)^{2\cdot\frac{n-1}{\beta-1}} \cdot \frac{i+3}{4} \cdot \lambda_i(L)^2\end{aligned}$$

Damit haben wir die zweite Behauptung auch gezeigt. ■

Beweis (zu Satz 7.2.4). Nach Definition der sukzessiven Minima gilt:

$$\lambda_i^2 \leq \max_{j=1,\dots,i} \|b_j\|^2$$

Aus

$$\|b_i\|^2 = \|\widehat{b}_i\|^2 + \sum_{j=1}^{i-1} (\mu_{i,j})^2 \|\widehat{b}_j\|^2$$

und $\mu_{i,j}^2 \leq \frac{1}{4}$ folgt:

$$\|b_i\|^2 \leq \left(1 + (i-1)\cdot\tfrac{1}{4}\right) \cdot \max_{j=1,\dots,i} \|\widehat{b}_j\|^2$$

Wir erhalten:

$$\lambda_i^2 \leq \tfrac{i+3}{4} \cdot \max_{j=1,\dots,i} \|\widehat{b}_j\|^2 \tag{7.9}$$

Lemma 7.2.5 angewandt auf die β-reduzierte Basis $\pi_j(b_j), \pi_j(b_{j+1}), \dots, \pi_j(b_i)$ liefert für $1 \leq j \leq i-\beta+1$:

$$\|\widehat{b}_j\| \leq (\gamma_\beta)^{\frac{i-j}{\beta-1}} \max\left\{\|\widehat{b}_{i-\beta+2}\|, \|\widehat{b}_{i-\beta+3}\|, \dots, \|\widehat{b}_i\|\right\} \tag{7.10}$$

Andererseits gilt für $i-\beta+2 \leq j \leq i$:

$$\|\widehat{b}_j\| \leq \|\pi_j(b_j)\| \leq \|b_i\| \tag{7.11}$$

Aus (7.10) und (7.11) erhalten wir für $1 \leq j \leq i$:

$$\|\widehat{b}_j\| \leq (\gamma_\beta)^{\frac{i-j}{\beta-1}} \|b_i\|$$

Diese Ungleichung liefert mit (7.9) die Behauptung, daß für $i = 1, \dots, n$ gilt:

$$\frac{\lambda_i(L)^2}{\|b_i\|^2} \leq (\gamma_\beta)^{2\cdot\frac{i-1}{\beta-1}} \cdot \frac{i+3}{4}$$

■

7.3 Kritische β-reduzierte Basen für $\beta = 2,3$

In diesem Abschnitt konstruieren wir für $\beta = 2,3$ kritische β-reduzierte Basen.

Definition 7.3.1 (kritische β-reduzierte Basis)
Eine β-reduzierte Basis $b_1, \dots, b_n$ des Gitters L heißt kritisch für n und β, falls $\frac{\|b_1\|}{\lambda_1(L)}$ maximal für alle β-reduzierten Basen vom Rang n ist.

Für $\beta = 2$ konstruieren wir die Basismatrix $A_n := [b_1, \ldots, b_n] \in M_{n,n}(\mathbb{R})$ wie folgt. Sei $\rho := \sqrt{\frac{3}{4}}$:

$$A_n := \begin{bmatrix} 1 & \frac{1}{2} & 0 & \cdots & \cdots & 0 \\ 0 & \rho & \frac{1}{2}\rho & \ddots & 0 & \vdots \\ \vdots & 0 & \rho^2 & \frac{1}{2}\rho^2 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ \vdots & & & \ddots & \rho^{n-2} & \frac{1}{2}\rho^{n-2} \\ 0 & \cdots & \cdots & \cdots & 0 & \rho^{n-1} \end{bmatrix} \tag{7.12}$$

Es gilt

$$A_2 := \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \sqrt{\frac{3}{4}} \end{bmatrix}$$

und für $n \geq 2$ die Rekursion:

$$A_n := \begin{bmatrix} 1 & \frac{1}{2} & 0 & \cdots & 0 \\ 0 & & & & \\ \vdots & & & \rho \cdot A_{n-1} & \\ 0 & & & & \end{bmatrix}$$

Satz 7.3.2
Seien $b_1, \ldots, b_n$ die Spaltenvektoren der Matrix A_n aus (7.12). *Für $\rho = \sqrt{\frac{3}{4}}$ und das Gitter $L = L(b_1, \ldots, b_n)$ gilt:*

a) $b_1, \ldots, b_n$ *ist eine kritische, 2-reduzierte Basis.*

b) $\dfrac{\|b_1\|}{\lambda_1(L)} = \dfrac{1}{\rho^{n-2}} = \rho^{-n+2}$

c) $\lambda_1(L) = \rho^{2(n+2)} \left(\frac{1}{4} + \rho^2\right) = \rho^{2(-n+2)}$

Beweis. Siehe [Schnorr94a, Theorem 9]. ■

Für $\beta = 3$ definieren wir die Basismatrix $B_n := [b_1, \ldots, b_n] \in M_{n,n}(\mathbb{R})$ wie folgt (zur Konstruktion siehe [Schnorr94a]):

$$B_4 := \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{\sqrt{3}}{2} & \frac{-1}{2\sqrt{3}} & \frac{1}{2\sqrt{3}} \\ 0 & 0 & \sqrt{\frac{2}{3}} & \frac{1}{2}\sqrt{\frac{2}{3}} \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} \tag{7.13}$$

Die Matrizen B_2, B_3 seien die 2×2- bzw. 3×3-Matrizen in der linken, oberen Ecke von B_4. Für $n \geq 4$ definieren wir die Basismatrix B_n rekursiv:

$$B_n := \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & \cdots & 0 \\ 0 & \frac{\sqrt{3}}{2} & \frac{-1}{2\sqrt{3}} & \frac{1}{2\sqrt{3}} & 0 & \cdots & 0 \\ 0 & 0 & & & & & \\ \vdots & \vdots & & \sqrt{\frac{2}{3}} \cdot B_{n-2} & & & \\ 0 & 0 & & & & & \end{bmatrix} \tag{7.14}$$

Es gilt:

Satz 7.3.3
Seien $b_1, \ldots, b_{2k+1}$ die Spaltenvektoren der Basismatrix B_{2k+1} aus (7.14) bzw. (7.13). Dann ist $b_1, \ldots, b_{2k+1}$ für $k = 1, 2, \ldots$ eine kritische, 3-reduzierte Basis.

Beweis. Siehe [Schnorr94a, Theorem 14]. ■

7.4 Praktisches Verfahren zur β-Reduktion

Wir modifizieren die Bedingung für β-reduziert durch Einführung eines Parameters δ für die Praxis (siehe [SchnEu91, Ritter97]):

Definition 7.4.1 ((β, δ)-reduzierte Basis)
Sei $b_1, \ldots, b_n \in \mathbb{R}^m$ eine geordnete Basis, $\beta \in \{2, 3, \ldots, n\}$ und δ mit $\frac{1}{4} < \delta < 1$ gegeben. Die geordnete Basis $b_1, \ldots, b_n \in \mathbb{R}^m$ heißt (β, δ)-reduziert, wenn:

a) $|\mu_{i,j}| \leq \frac{1}{2}$ *für* $1 \leq j < i \leq n$

b) $\delta \cdot \|\widehat{b}_j\|^2 \leq \lambda_1 \left(\pi_j(L(b_j, b_{j+1}, \ldots, b_k)\right)^2$ *für* $j = 1, \ldots, n$

Der Algorithmus 7.4.1 aus [SchnEu91] transformiert eine gegebene Basis in eine β-reduzierte Basis des gleichen Gitters. Das Unterprogramm L^3FP zur LLL-Reduktion für Gleitkommazahlen haben wir auf Seite **??** angegeben. Das Unterprogramm ENUM (Algorithmus 8.1.1) bzw. GAUSS-ENUM (zur geschnittenen Aufzählung) stellen wir im nächsten Kapitel vor.

Die Variable j wird zyklisch durch die Zahlen $1, \ldots, n-1$ geschoben. Die Variable z zählt die Zahl der Positionen j, welche die Ungleichung

$$\delta \cdot \|\widehat{b}_j\|^2 \leq \lambda_1 \Big(\pi_j\big(L(b_j, b_{j+1}, \ldots, b_k)\big)\Big)^2 \tag{7.15}$$

erfüllen. Falls diese Ungleichung nicht für j gilt, fügen wir den Vektor b_j^{neu} in die Basis ein, rufen den LLL-Algorithmus auf und setzen $z = 0$. Den Fall $j = n$ überspringen wir, da (7.15) dann trivialerweise gilt.

Offenbar ist eine Basis $b_1, \ldots, b_n$ (β, δ)-reduziert, falls sie längenreduziert ist und $z = n - 1$ gilt. Da vor Terminierung der LLL-Algorithmus aufgerufen wird, ist die ausgegebene Basis längenreduziert. Einen Beweis, daß der Algorithmus in polynomieller Zeit arbeitet, gibt es bisher nicht. In der Praxis [SchnEu91, LARIFARI] hat sich der Algorithmus jedoch bewährt.

Algorithmus 7.4.1 Block-Korkine-Zolotareff-Reduktion (kurz BKZ)

EINGABE: ▹ Gitterbasis $b_1, \ldots, b_n \in \mathbb{Z}^n$,
▹ $\delta \in \left]\frac{1}{2}; 1\right[$
▹ $\beta \in \{3, 4, \ldots, n-1\}$

1. $L^3FP(b_1, \ldots, b_n, \delta)$, $z := 0$, $j := 0$

2. WHILE $(z < n-1)$ DO

2.1. $j := j + 1$
$k := \min(j + \beta - 1, n)$
IF $j = n$ THEN $j := 1$, $k := \beta$

/* $b_j, b_{j+1}, \ldots, b_k$ ist LLL-reduziert mit δ */

2.2. ENUM(j, k)

/* Finde Minimalstelle $(u_j, u_{j+1}, \ldots, u_k) \in \mathbb{Z}^{k-j+1} \setminus \{0\}$ zu:

$$c_j(u_j, u_{j+1}, \ldots, u_k) := \sum_{s=j}^{k} \sum_{s=i}^{k} (u_i \mu_{i,s})^2 c_s = \left\| \pi_j \left(\sum_{i=j}^{k} u_i b_i \right) \right\|^2$$

und $b_j^{\text{neu}} := \sum_{s=j}^{k} u_s b_s$. Sei $\overline{c}_j$ der Minimalwert. */

2.3. $h := \min(k + 1, n)$

2.4. IF $\delta c_j > \overline{c}_j$ THEN

2.4.1. Ergänze $b_1, \ldots, b_{j-1}, b_j^{\text{neu}}$ zur Basis von $L(b_1, \ldots, b_h)$

2.4.2. $L^3FP\left(b_1, \ldots, b_{j-1}, b_j^{\text{neu}}, b_{j+1}^{\text{neu}}, \ldots, b_h^{\text{neu}}, \delta\right)$ /* Stufe j mit F :=true */

2.4.3. $z := 0$

ELSE

2.4.1. $z := z + 1$

2.4.2. $L^3FP(b_1, \ldots, b_h, \delta)$ /* auf Stufe $h - 1$ */

END if

END while

AUSGABE: (β, δ)-reduzierte Basis $b_1, \ldots, b_n$

Kapitel 8

Konstruktion eines kürzesten Gittervektors

Im Kapitel 7.4 haben wir einen Algorithmus zur Block-Reduktion vorgestellt. Als Unterprogramm mußte der kürzeste, nicht-triviale Gittervektor berechnet werden. Wir lernen in diesem Kapitel einen solchen Algorithmus kennen, der durch vollständige Aufzählung einen kürzesten Gittervektor findet. Anschließend werden wir durch die Volumen-Heuristik versuchen, die Aufzählung zu beschränken. Polynomialzeit-Verfahren sind nicht bekannt.

8.1 Algorithmus mit vollständiger Aufzählung

Wir möchten zu einer gegebenen Gitterbasis $b_1, \ldots, b_n \in \mathbb{R}^m$ bezüglich der Euklidischen Norm einen kürzesten Gittervektor konstruieren. Sei $b_1, \ldots, b_n \in \mathbb{R}^m$ die Basis mit zugehörigem Orthogonalsystem $\widehat{b}_1, \ldots, \widehat{b}_n$ und Gram-Schmidt-Koeffizienten $\mu_{i,j}$, also:

$$b_i = \sum_{j=1}^{i} \mu_{i,j} \widehat{b}_j \qquad i = 1, \ldots, n,$$

Zur orthogonalen Projektion $\pi_i : \mathbb{R}^m \to \operatorname{span}(b_1, \ldots, b_i)^{\perp}$ bezeichne:

$$c_t(u_t, u_{t+1}, \ldots, u_n) := \left\| \pi_t \left(\sum_{i=t}^{n} u_i b_i \right) \right\|^2 = \left\| \sum_{i=t}^{n} \sum_{s=t}^{n} u_i \mu_{i,s} \widehat{b}_s \right\|^2 = \sum_{s=t}^{n} \left(\sum_{i=t}^{n} u_i \mu_{i,s} \right)^2 \cdot \|\widehat{b}_s\|^2$$

C.P. Schnorr und M. Euchner stellen in [SchnEu91] den ENUM-Algorithmus (Algorithmus 8.1.1) vor. Die Funktion $a' := \operatorname{next}(a, r)$ liefert zu $a \in \mathbb{Z}$ und $r \in \mathbb{R}$ die in der Reihenfolge nach a betragsmäßig nächste, ganze Zahl zur reellen Zahl r (siehe Grafik 8.1.1). Es gilt:

- $|a - r| \leq |a' - r| \leq |a - r| + 1$
- $\operatorname{sign}(a' - r) \neq \operatorname{sign}(a - r)$

Falls es zu r zwei ganze Zahlen mit Abstand $\frac{1}{2}$ gibt, fordern wir zusätzlich, daß zunächst der kleinere Wert gewählt wird, also aus $|a - r| = |a' - r|$ folgt $a < r < a'$.

Die Korrektheit des ENUM-Algorithmus' 8.1.1 folgt aus den folgenden Beobachtungen:

- Stets gilt: $\tilde{c}_t = c_t(\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n)$. Beweis durch Induktion über Anzahl der Iterationen. Durch die Zuweisungen im ersten Schritt gelten die Behauptungen vor der ersten Iteration

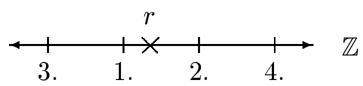

Abbildung 8.1.1: Reihenfolge der Approximationen bei $\mathrm{next}(\,\cdot\,, r)$

Algorithmus 8.1.1 ENUM: kürzester Gittervektor (vollständige Aufzählung)

EINGABE: $\|\widehat{b}_i\|^2, \mu_{i,t}$ für $1 \le t \le i \le n$

1. FOR $i = 1, \ldots, n$ DO $\tilde{c}_i := u_i := \tilde{u}_i := y_i := 0$

2. $\tilde{u}_1 := u_1 := 1$; $t := 1$;

3. $c_1^{\min} := \tilde{c}_1 := \|\widehat{b}_1\|^2$

/* stets gilt: $\tilde{c}_t = c_t(\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n)$ und $c_1^{\min}$ ist aktuelles Minimum der Funktion c_1 */

4. WHILE $t \le n$ DO

4.1. $\tilde{c}_t := \tilde{c}_{t+1} + (y_t + \tilde{u}_t)^2 \cdot \|\widehat{b}_t\|^2$

4.2. IF $\tilde{c}_t < c_1^{\min}$ THEN

IF $t > 1$ THEN

$t := t - 1$

$y_t := \sum_{i=t+1}^{n} \tilde{u}_i \mu_{i,t}$

$\tilde{u}_t := \lfloor -y_t \rceil$

ELSE

$c_1^{\min} = \tilde{c}_1$

FOR $i = 1, \ldots, n$ DO $u_i := \tilde{u}_i$

END if

ELSE

$t := t + 1$

/* $t_{\max}$ bezeichne den bisherigen maximalen Wert von t vor Erhöhung */

$$\tilde{u}_t := \begin{cases} \tilde{u}_t + 1 & \text{falls } t = t_{\max} \\ \mathrm{next}(\tilde{u}_t, -y_t) & \text{sonst} \end{cases}$$

END if

END while

AUSGABE: Minimalstelle $(u_1, \ldots, u_n) \in \mathbb{Z}^n \setminus \{0\}$ und Minimalwert $c_1^{\min}$ für Funktion c_1

(Induktionsverankerung). Induktionsschluß:

$$\begin{aligned} c_t(\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n) &= \underbrace{c_{t+1}(\tilde{u}_{t+1}, \tilde{u}_{t+2}, \ldots, \tilde{u}_n)}_{\text{nach Ind.Annahme: } = \tilde{c}_{t+1}} + \left(\sum_{i=t}^{n} \tilde{u}_i \mu_{i,t} \right)^2 \cdot \|\widehat{b}_t\|^2 \\ &= \tilde{c}_{t+1} + (y_t + \tilde{u}_t)^2 \cdot \|\widehat{b}_t\|^2 \end{aligned}$$

Bei der letzten Umformung nutzen wir, daß $y_t = \sum\limits_{i=t+1}^{n} \tilde{u}_i \mu_{i,t}$ und $\tilde{u}_t = \tilde{u}_t \cdot 1 = \tilde{u}_t \cdot \mu_{t,t}$.

- Der Algorithmus zählt (engl. enumerate) in Depth-First-Order alle Vektoren

$$(\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n) \in \mathbb{Z}^{n-t+1} \setminus \{0\}$$

für $t = 1, \ldots, n$ auf, für die gilt ($c_1^{\min}$ ist das aktuelle Minimum der Funktion c_1):

$$c_t(\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n) < c_1^{\min}$$

Alle Vektoren erfüllen $\tilde{u}_i > 0$ für das größte i mit $\tilde{u}_i \neq 0$.

- Für feste $\tilde{u}_{t+1}, \tilde{u}_{t+2}, \ldots, \tilde{u}_n$ gilt für die Folge der $\tilde{u}_t$-Werte, erzeugt durch $\operatorname{next}(\,\cdot\,, -y_t)$, daß $c_t(\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n)$ monoton wachsend ist. Falls die Abfrage $\tilde{c}_t < \overline{c}$ negativ für den aktuellen Vektor $(\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n)$ ist, kann die Aufzählung der Vektoren $(u, \tilde{u}_{t+1}, \ldots, \tilde{u}_n)$, wobei u für die weiteren Werte der $\operatorname{next}(\,\cdot\,, -y_t)$-Funktion steht, entfallen. Denn nach den vorherigen Überlegungen führen diese Vektoren nicht zum Minimum der c_1-Funktion.

Am Ende des ENUM-Algorithmus gilt $c_1^{\min} = \lambda_1^2$.

8.2 Algorithmus mit geschnittener Aufzählung

Um die Laufzeit des Aufzählungsverfahrens zu verkürzen, führen wir eine Heuristik ein, um die Aufzählung abzubrechen, wenn wir in diesem Teil der Aufzählung mit hoher Wahrscheinlichkeit keinen kürzeren Vektoren finden werden (vergleiche [SchnHö95, Ritter97]).

8.2.1 Volumen-Heuristik und Gauß-ENUM

Folgende Heuristik geht auf C.F. Gauß zurück:

Lemma 8.2.1 (Volumen-Heuristik)
Sei $S \subseteq \operatorname{span}(L)$ Jordan-meßbar, $z \in \operatorname{span}(L)$ zufällig, dann gilt:

$$\mathrm{E}_z\left[\,|(z+S) \cap L|\right] = \frac{\operatorname{vol}(S)}{\det L}$$

Beweis. Denn:

$$\frac{1}{\det L} = \frac{\text{Anzahl Gitterpunkte}}{\text{Volumen Grundmasche}} = \frac{\text{Anzahl Gitterpunkte}}{\text{Volumeneinheit}}$$

■

Angenommen, wir haben $(\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n) \in \mathbb{Z}^{n-t+1} \setminus \{0\}$ fest und suchen

$$\tilde{u}_1, \ldots, \tilde{u}_{t-1} \in \mathbb{Z}$$

mit $c_1(\tilde{u}_1, \ldots, \tilde{u}_n) < c_1^{\min}$. Setze:

$$\overline{L} := L(b_1, \ldots, b_{t-1})$$

Wir möchten zu gegebenem Gittervektor $b = \sum_{i=t}^{n} \tilde{u}_i b_i$ einen Vektor

$$\overline{b} = \sum_{i=1}^{t-1} \tilde{u}_i b_i \in \overline{L}$$

addieren, so daß $\left\|b+\overline{b}\right\|^2 < c_1^{\min}$. Wir zerlegen b in orthogonale Anteile:

$$b = \underbrace{\sum_{j=1}^{t-1}\sum_{i=1}^{n} \tilde{u}_i \mu_{i,j} \widehat{b}_j}_{=:-z\in\operatorname{span}(\,\overline{L}\,)} + \underbrace{\sum_{j=t}^{n}\sum_{i=t}^{n} \tilde{u}_i \mu_{i,j} \widehat{b}_j}_{=:y\in\operatorname{span}(\,\overline{L}\,)^{\perp}} \tag{8.1}$$

Das bedeutet, wir suchen nach einem Gitterpunkt $\overline{b} \in \overline{L}$ in

$$\left(b+\overline{L}\,\right) \cap S_{t-1}\left(\sqrt{c_1^{\min} - \tilde{c}_t}, y\right) = \overline{L} \cap S_{t-1}\left(\sqrt{c_1^{\min} - \tilde{c}_t}, y\right),$$

wobei $S_d(r, c)$ eine d-dimensionale Sphäre mit Radius r und Zentrum c ist. Grafik 8.2.1 verdeutlicht die Aufgabe. Wir wenden die Volumen-Heuristik auf das Gitter $\overline{L}$ und die Sphäre

$$S_{t-1}\left(\sqrt{\,c_1^{\min} - \tilde{c}_t}, y\right) \subseteq \operatorname{span}\left(\,\overline{L}\,\right)$$

an und erhalten:

$$\mathrm{E}_z\left[\,\left|\left\{(\tilde{u}_1, \ldots, \tilde{u}_{t-1}) \in \mathbb{Z}^{t-1} \,:\, c_1(\tilde{u}_1, \ldots, \tilde{u}_{t-1}) < c_1^{\min}\right\}\right|\,\right] = \frac{\operatorname{vol}\left(S_{t-1}\left(\sqrt{c_1^{\min} - \tilde{c}_t}, y\right)\right)}{\det \overline{L}}$$

Wir werden die Anwendung der Volumen-Heuristik anschließend rechtfertigen.

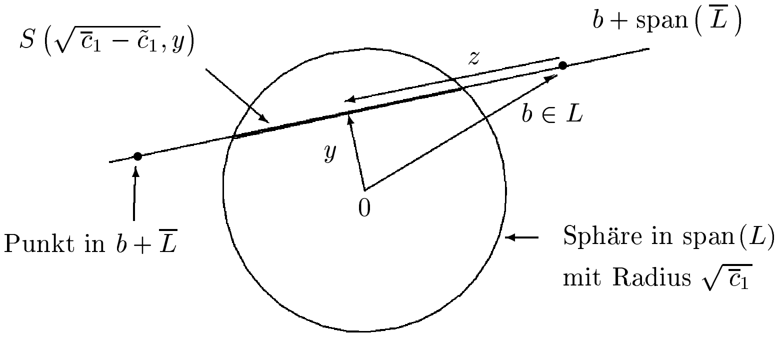

Abbildung 8.2.1: Volumenheuristik bei Gauß-ENUM

Wir beenden die weitere Aufzählung (engl. pruning), falls der Quotient kleiner als 2^{-p}, p fest vorgegeben, ist. Je größer p, desto umfangreicher die Aufzählung. Für $p = \infty$ erhalten wir die vollständige Aufzählung. Wähle $\eta_{t,p}$ als

$$2^{-p} = \frac{\operatorname{vol}\left(S_{t-1}\left(\sqrt{\eta_{t,p}}\right)\right)}{\det \overline{L}}.$$

Aus der Stirling'schen Approximation (siehe (**??**) auf Seite **??**) erhalten wir:

$$2^{-p} = \frac{\operatorname{vol}\left(S_{t-1}\left(\sqrt{\eta_{t,p}}\right)\right)}{\det \overline{L}} = \frac{(\pi \cdot \eta_{t,p})^{\frac{t-1}{2}}}{\Gamma\left(1 + \frac{t-1}{2}\right)} \cdot \frac{1}{\prod_{i=1}^{t-1} \|\widehat{b}_i\|} \approx \frac{\left(\frac{2e\pi}{t-1} \cdot \eta_{t,p}\right)^{\frac{t-1}{2}}}{\sqrt{\pi(t-1)} \cdot \prod_{i=1}^{t-1} \|\widehat{b}_i\|}$$

Es folgt:

$$\eta_{t,p} = \frac{1}{\pi} \cdot \Gamma\left(1 + \frac{t-1}{2}\right)^{\frac{2}{t-1}} \cdot \left(2^{-p} \cdot \prod_{i=1}^{t-1} \|\widehat{b}_i\|\right)^{\frac{2}{t-1}} \approx \frac{t-1}{2e\pi}\left(\sqrt{\pi(t-1)} \cdot 2^{-p} \cdot \prod_{i=1}^{t-1} \|\widehat{b}_i\|\right)^{\frac{2}{t-1}}$$

Im Algorithmus 8.1.1 (Seite 66) ersetzen wir Schritt 4.2 durch

$$\text{IF } \tilde{c}_t < c_1^{\min} - \eta_{t,p}$$

Den erhaltenen Algorithmus 8.2.1 nennen wir Gauß-ENUM. Eine Analyse, mit welcher Wahrscheinlichkeit der kürzeste Gittervektor gefunden wird, erweist sich als schwierig.

Algorithmus 8.2.1 Gauß-ENUM: kürzester Gittervektor (geschnittene Aufzählung)

EINGABE: $\|\widehat{b}_i\|^2, \mu_{i,t}$ für $1 \leq t \leq i \leq n$

1. FOR $i = 1, \ldots, n$ DO $\tilde{c}_i := u_i := \tilde{u}_i := y_i := 0$

2. $\tilde{u}_1 := u_1 := 1$; $t := 1$;

3. $c_1^{\min} := \tilde{c}_1 := \|\widehat{b}_1\|^2$

/* stets gilt: $\tilde{c}_t = c_t(\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n)$ und $c_1^{\min}$ ist aktuelles Minimum der Funktion c_1 */

4. WHILE $t \leq n$ DO

    4.1. $\tilde{c}_t := \tilde{c}_{t+1} + (y_t + \tilde{u}_t)^2 \cdot \|\widehat{b}_t\|^2$

    4.2. IF $\tilde{c}_t < c_1^{\min} - \eta_{t,p}$ THEN

        IF $t > 1$ THEN

            $t := t - 1$

            $y_t := \sum_{i=t+1}^{n} \tilde{u}_i \mu_{i,t}$

            $\tilde{u}_t := \lfloor -y_t \rceil$

        ELSE

            $c_1^{\min} = \tilde{c}_1$

            FOR $i = 1, \ldots, n$ DO $u_i := \tilde{u}_i$

        END if

    ELSE

        $t := t + 1$

        /* $t_{\max}$ bezeichne den bisherigen maximalen Wert von t vor der Erhöhung */

$$\tilde{u}_t := \begin{cases} \tilde{u}_t + 1 & \text{falls } t = t_{\max} \\ \text{next}(\tilde{u}_t, -y_t) & \text{sonst} \end{cases}$$

    END if

END while

AUSGABE: Wahrscheinliche Minimalstelle $(u_1, \ldots, u_n) \in \mathbb{Z}^n \setminus \{0\}$ und Minimalwert $c_1^{\min}$ für die Funktion c_1

Wir müssen noch die Anwendung der Volumen-Heuristik rechtfertigen.

Lemma 8.2.2
Sei $\overline{L} := L(b_1, \ldots, b_{t-1})$, $(\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n) \in \mathbb{Z}^{n-t+1} \setminus \{0\}$ *fest und der Punkt* z *aus* (8.1). *Dann*

gilt, sofern $z \in_{\mathrm{R}} \operatorname{span}\left(\overline{L}\right)$*:*

$$\mathrm{E}_z\left[\left|\left\{(\tilde{u}_1,\ldots,\tilde{u}_{t-1}) \in \mathbb{Z}^{t-1} \,:\, c_1(\tilde{u}_1,\ldots,\tilde{u}_n) \le c_1^{\min}\right\}\right|\right] = \frac{\operatorname{vol}\left(S_{t-1}\left(\sqrt{c_1^{\min}-\tilde{c}_t}, z\right)\right)}{\det \overline{L}}$$

Weiter:

$$\mathrm{E}_z\left[\left|\left\{(\tilde{u}_1,\ldots,\tilde{u}_{t-1}) \in \mathbb{Z}^{t-1} \,:\, c_1(\tilde{u}_1,\ldots,\tilde{u}_n) \le c_1^{\min}\right\}\right|\right] \ge 2^{-p} \qquad \Longleftrightarrow \qquad \tilde{c}_t \le c_1^{\min} - \eta_{t,p}$$

Beweis. Wir setzen:

$$S := S_{t-1}\left(\sqrt{c_1^{\min} - \eta_{t,p}}\right)$$

und $L := \overline{L}$. Es gilt:

$$|(z+S)\cap L| = \left|\left\{(\tilde{u}_1,\ldots,\tilde{u}_{t-1}) \in \mathbb{Z}^{t-1} \,:\, c_1(\tilde{u}_1,\ldots,\tilde{u}_n) \le c_1^{\min}\right\}\right|$$

Aus Lemma 8.2.1 folgt die Behauptung, da nach Voraussetzung $z \in_{\mathrm{R}} \operatorname{span}\left(\overline{L}\right)$. ■

Zu $r \in \mathbb{R}$ bezeichne $\{r\} \in [0,1[$ die Nachkommastellen.

Definition 8.2.3 (gleichverteilt mod L (kurz: u.d. mod L))
Für ein Gitter L mit der Basis $b_1,\ldots,b_n$ *heißt eine Wahrscheinlichkeitsverteilung der Punkte* $\sum_{i=1}^n t_i b_i$ *in* $\operatorname{span}(L)$ *gleichverteilt (uniformly distributed) modulo L (kurz: u.d. mod L), falls der Vektor* $(\{t_1\},\{t_2\},\ldots,\{t_n\})$ *gleichverteilt auf* $[0,1[^n$ *ist.*

Bemerkung 8.2.4
Diese Eigenschaft bleibt bei Basiswechsel und Übergang zum Orthogonalsystem erhalten. In den Lemmata 8.2.1 und 8.2.2 genügt es, daß z gleichverteilt mod L ist, denn:

$$z \equiv \overline{z} \pmod{L} \quad \Rightarrow \quad |z + S \cap L| = |\overline{z} + S \cap L|$$

Wir wenden Lemma 8.2.2 und Bemerkung 8.2.4 auf die Situation in ENUM an mit:

- festen $\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n$,
- $\tilde{c}_t = c_t(\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n)$,
- $c_1^{\min} > \tilde{c}_t$,
- wir suchen einen Gitterpunkt aus $\overline{L}$ mit der Sphäre $\left(\sqrt{c_1^{\min}-\tilde{c}_t}, z\right)$ und Zentrum:

$$z = -\sum_{j=1}^{t-1}\sum_{i=t}^{n} \tilde{u}_i \mu_{i,j} \widehat{b}_j$$

Satz 8.2.5
Sei $(\{\mu_{i,j}\} \mid 1 \le j < i \le n)$ *gleichverteilt in* $[0,1[^{\binom{n}{2}}$*. Dann folgt in obiger Situation für festes* $(\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n) \in \mathbb{Z}^{n-t-1}$*:*

- *z ist uniformly distributed modulo* $\overline{L}$*.*
- $\mathrm{E}_z\left[\left|\left\{(\tilde{u}_1,\ldots,\tilde{u}_{t-1}) \in \mathbb{Z}^{t-1} \,:\, c_1(\tilde{u}_1,\ldots,\tilde{u}_n \le c_1^{\min}\right\}\right|\right]$

Beweis. Wir nehmen an, daß $\tilde{u}_n \neq 0$, denn sonst können wir n vermindern. Die Eigenschaft $\{\mu\} \in_{\mathrm{R}} [0,1[$ bleibt bei Multiplikation mit einer ganzen Zahl $z \in \mathbb{Z} \setminus \{0\}$ erhalten, d.h. $\{z \cdot \mu\} \in_{\mathrm{R}} [0,1[$. Die Vektoren

$$(\{\tilde{u}_n \mu_{n,j}\} \mid j = 1, \ldots, t-1)$$
$$\left(\left\{\sum\nolimits_{i=t}^{n} \tilde{u}_n \mu_{i,j}\right\} \mid j = 1, \ldots, t-1\right)$$

sind unabhängig und gleichverteilt in $[0,1[^{t-1}$. Daraus folgt, daß

$$\left(\left\{\tilde{u}_n \mu_{n,j} - \sum\nolimits_{i=t}^{n} \tilde{u}_n \mu_{i,j}\right\} \mid j = 1, \ldots, t-1\right)$$

gleichverteilt in $[0,1[^{t-1}$ ist. Die Behauptung folgt aus Lemma 8.2.2. ■

8.3 Bemerkung zur LLL-reduzierten Basis

Der folgende Satz zeigt, daß es Verteilungen von Gitterbasen gibt, für die die LLL-Reduktion nur sehr schwache Approximationen des kürzesten Gittervektors liefert (vergleiche Satz 5.1.4 auf Seite 36):

Satz 8.3.1
Sei $b_1, \ldots, b_n$ zufällige Gitterbasis, so daß:

$$(\mu_{i,j} \mid 1 \leq i < j \leq n) \in_{\mathrm{R}} [0,1[^{\binom{n-1}{2}}$$

Es gibt eine Verteilung D auf $[0,1[^{\binom{n-1}{2}}$, so daß die Gitterbasis $b_1, \ldots, b_n$ mit

$$(\mu_{i,j} \mid 1 \leq i < j \leq n) \in_{D} [0,1[^{\binom{n-1}{2}}$$

stets LLL-reduziert ist und für den Erwartungswert gilt:

$$\mathrm{E}_D \left[\frac{\lambda_1^2}{\|b_1\|^2} \right] \leq \gamma_n \cdot \left(\frac{11}{12}\right)^{\frac{n-1}{2}},$$

wobei γ_n die Hermite-Konstante der Dimension n ist.

Beweis. Sei:

$$(\mu_{i,j} \mid 1 \leq i < j \leq n) \in_{\mathrm{R}} \left[-\tfrac{1}{2}; +\tfrac{1}{2}\right[^{\binom{n-1}{2}}$$

Definiere Basis $b_1, \ldots, b_n$ des Gitters L durch das zugehörige Orthogonalsystem: Wähle $\|\widehat{b}_i\|^2$, $i = 1, \ldots, n$, mit:

$$\begin{aligned} \|\widehat{b}_1\| &= 1 \\ \|\widehat{b}_{i+1}\|^2 &= \|\widehat{b}_i\|^2 \cdot (1 - \mu_{i+1,i}^2) \qquad i = 1, \ldots, n-1 \end{aligned}$$

Die Basis ist LLL-reduziert mit $\delta = 1$, da nach Konstruktion:

$$\|\pi_i(b_{i+1})\|^2 = \|\widehat{b}_{i+1}\|^2 + \mu_{i+1,i}^2 \|\widehat{b}_i\| = \|\widehat{b}_i\|^2$$

Aus der Definition der Hermite-Konstanten $\gamma_n := \sup\left\{\frac{\lambda_1(L)^2}{(\det L)^{2/n}} \,\middle|\, \mathrm{Rang}(L) = n\right\}$ folgt:

$$\lambda_1^2 \leq \gamma_n \cdot (\det L)^{\frac{2}{n}} = \gamma_n \cdot \prod_{i=1}^{n} \|\widehat{b}_i\|^{\frac{2}{n}} = \gamma_n \cdot \|\widehat{b}_1\|^{\frac{2}{n}} \cdot \prod_{i=1}^{n-1} (1 - \mu_{i+1,i}^2)^{\frac{n-i}{n}}$$

Wir erhalten für x gleichverteilt in $\left[-\frac{1}{2}; +\frac{1}{2}\right[$:

$$\begin{aligned}
\mathrm{E}_x\left[\frac{\lambda_1^2}{\|b_1\|^2}\right] &\leq \gamma_n \cdot \mathrm{E}\left[\prod_{i=1}^{n-1}(1-\mu_{i+1,i}^2)^{\frac{n-i}{n}}\right] && \text{(für } i \neq j \text{ sind } \mu_{i+1,i} \text{ und } \mu_{j+1,j} \text{ unabhängig)} \\
&= \gamma_n \cdot \prod_{i=1}^{n-1} \mathrm{E}_x\left[1-x^2\right]^{\frac{n-i}{n}} \\
&\leq \gamma_n \cdot \prod_{i=1}^{n-1} \mathrm{E}_x\left[1-x^2\right]^{\frac{n-i}{n}} && \left(\text{es gilt: } \mathrm{E}_x\left[1-x^2\right] = 1 - \tfrac{1}{12} = \tfrac{11}{12}\right) \\
&\leq \gamma_n \cdot \left(\frac{11}{12}\right)^{\frac{1}{n}\sum_{i=1}^{n-1} i} \\
&\leq \gamma_n \cdot \left(\frac{11}{12}\right)^{\frac{1}{n}\binom{n-1}{2}} \\
&\leq \gamma_n \cdot \left(\frac{11}{12}\right)^{\frac{n-3}{2}}
\end{aligned}$$

Im letzten Schritt nutzen wir die folgende Abschätzung (da $\frac{11}{12} < 1$, müssen wir für eine obere Schranke den Exponenten nach unten abschätzen):

$$\frac{1}{n} \cdot \binom{n-1}{2} = \frac{(n-1)(n-2)}{2n} = \frac{n^2 - 3n + 2}{2n} = \frac{n}{2} - \frac{3}{2} + \frac{1}{n} > \frac{n-3}{2}$$

■

Kapitel 9

Gitterreduktion in beliebiger Norm

Bisher haben wir Gitter bezüglich der Euklidischen Norm reduziert. In diesem Kapitel betrachten wir allgemeine Normen. Besonders die sup-Norm ist von Interesse (siehe Kapitel 10). Bis auf den Gauß-Reduktionsalgorithmus aus Kapitel 4 für aus zwei Vektoren bestehende Basen ist die Reduktion in beliebiger Norm in der Praxis „schwierig“.

9.1 Grundbegriffe

Sei $\|\cdot\| : \mathbb{R}^m \to \mathbb{R}$ eine beliebige Norm, d.h. es gilt für alle $u, v \in \mathbb{R}^m$ und $\mu \in \mathbb{R}$:

$$
\begin{aligned}
\|\mu v\| &= |\mu| \cdot \|v\| && \text{(positive Homogenität)}\\
\|u+v\| &\leq \|u\| + \|v\| && \text{(Dreiecksungleichung)}\\
\|u\| &\geq 0 \qquad \text{für } u \neq 0 && \text{(positive Definitheit)}
\end{aligned}
$$

Wir definieren zu einer gegebenen fest geordneten Gitterbasis Abstandsfunktionen:

Definition 9.1.1 (Abstandsfunktion F_i)
Sei $b_1, \ldots, b_n \in \mathbb{R}^m$ eine fest geordnete Gitterbasis. Die i-te Abstandsfunktion (auch Höhen- oder Distanzfunktion) für $1 \leq i \leq n$

$$F_i : \operatorname{span}(b_1, \ldots, b_n) \to \mathbb{R}$$

ist bezüglich der gegebenen Norm $\|\cdot\|$ definiert als:

$$
\begin{aligned}
F_1(x) &:= \|x\|\\
F_i(x) &:= \min_{t_1,\ldots,t_{i-1} \in \mathbb{R}} \left\| x - \sum\nolimits_{j=1}^{i-1} t_j b_j \right\| = \min_{t \in \mathbb{R}} F_{i-1}\left(x - t b_{i-1}\right) \qquad i = 2, 3, \ldots, n
\end{aligned}
$$

Die Höhe F_i eines Vektors ist sein Abstand zu dem von $b_1, \ldots, b_{i-1}$ erzeugten Unterraum. Es gilt $F_i(x) = 0$ genau dann, wenn $x \in \operatorname{span}(b_1, \ldots, b_{i-1})$. Man rechnet leicht nach, daß jede Abstandsfunktion F_i eine Norm auf $\operatorname{span}(b_1, \ldots, b_{i-1})^{\perp}$ ist. Im Fall der Euklidischen Norm ist $F_i(b_i) = \|\widehat{b}_i\|_2$. Die Determinante des Gitters $L = L(b_1, \ldots, b_n)$ ist:

$$\det L = \prod_{i=1}^{n} \|\widehat{b}_i\|_2$$

Wie sieht die Gleichung $\det L = \prod_i \|\widehat{b}_i\|$ bezüglich $F_1, \ldots, F_n$ aus? Zu gegebener Norm $\|\cdot\|$ definieren wir:

$$S_{\|\cdot\|}(1) := \{x \in \mathbb{R}^m \ : \ \|x\| \leq 1\}$$

Diese Menge ist konvex, nullsymmetrisch und abgeschlossen. Zu gegebener Norm $\|\cdot\|$ und Gitterbasis $b_1, \ldots, b_n \in \mathbb{R}^m$ definiere

$$V_i := \operatorname{vol} \underbrace{\{x \in \operatorname{span}(b_1, \ldots, b_i) \ : \ \|x\| \leq 1\}}_{=\operatorname{span}(b_1,\ldots,b_i) \cap S_{\|\cdot\|}(1)} \qquad i = 1, \ldots, n \tag{9.1}$$

Man beachte, daß sich Volumen stets auf die Euklidische Metrik bezieht.

Lemma 9.1.2
Für jede Basis $b_1, \ldots, b_n \in \mathbb{R}^m$ gilt:

$$\frac{2^n}{n!} \cdot \prod_{i=1}^{n} \frac{\|\widehat{b}_i\|_2}{F_i(b_i)} \leq V_n \leq 2^n \cdot \prod_{i=1}^{n} \frac{\|\widehat{b}_i\|_2}{F_i(b_i)}$$

Bevor wir das Lemma beweisen, eine Folgerung: Da V_n unabhängig von der Basis ist, gilt:

Korollar 9.1.3
Seien $b_1, \ldots, b_n$ und $b'_1, b'_2, \ldots, b'_n$ Basen des Gitters L, dann gilt:

$$\prod_{i=1}^{m} F_i(b_i) \leq n! \prod_{i=1}^{m} F'_i(b'_i) \qquad \textit{oder} \qquad \prod_{i=1}^{m} F'_i(b'_i) \leq n! \prod_{i=1}^{m} F_i(b_i)$$

Beweis (zu Lemma 9.1.2). Wir zeigen durch Induktion über n:

$$\frac{2^n}{n!} \cdot \prod_{i=1}^{n} \frac{\|\widehat{b}_i\|_2}{F_i(b_i)} \leq V_n \leq 2^n \cdot \prod_{i=1}^{n} \frac{\|\widehat{b}_i\|_2}{F_i(b_i)}$$

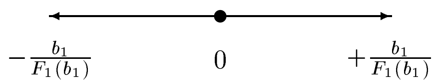

Abbildung 9.1.1: Induktionsverankerung im Beweis zu Lemma 9.1.2

- Induktionsverankerung $n = 1$: Es gilt (vergleiche Abbildung 9.1.1):

$$V_1 = 2 \cdot \frac{\|b_1\|_2}{\|b_1\|} = 2 \cdot \frac{\|\widehat{b}_1\|_2}{F_1(b_1)}$$

- Induktionsschluß von $n-1$ auf n: Wir wählen einen Punkt $z = b_n - \sum_{i=1}^{n-1} t_i b_i \in \mathbb{R}^n$ mit $\|z\| = F_n(b_n)$ (siehe Abbildung 9.1.2). Man erhält eine obere Schranke für V_n durch:

$$V_n \leq 2 \cdot V_{n-1} \cdot \frac{\|\widehat{b}_n\|_2}{F_n(b_n)}$$

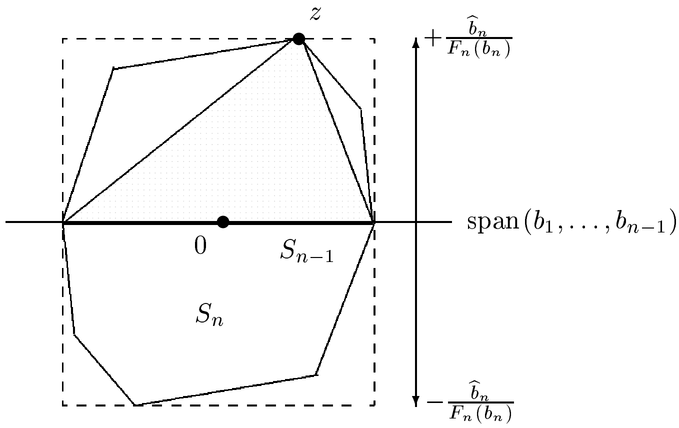

Abbildung 9.1.2: Induktionsschluß im Beweis zu Lemma 9.1.2

Die konvexe Hülle von S_{n-1} und z (gepunktetes Gebiet in Abbildung 9.1.2) ist in S_n enthalten. Da es sich um eine Pyramide mit Grundfläche S_{n-1} und Höhe $\frac{\|\widehat{b}_n\|_2}{F_n(b_n)}$ handelt, gilt:

$$\frac{V_{n-1}}{n} \cdot \frac{\|\widehat{b}_n\|_2}{F_n(b_n)} = \mathrm{vol}_n(\text{konvexe Hülle von } S_{n-1} \text{ und } z) \leq \frac{V_n}{2}$$

Es folgt wegen der Symmetrie:

$$2 \cdot \frac{V_{n-1}}{n} \cdot \frac{\|\widehat{b}_n\|_2}{F_n(b_n)} \leq V_n$$

Aus der Induktionsannahme erhalten wir:

$$V_n \geq 2 \cdot \frac{V_{n-1}}{n} \cdot \frac{\|\widehat{b}_n\|}{F_n(b_n)} \geq \left[\frac{2}{n} \cdot \frac{\|\widehat{b}_n\|}{F_n(b_n)}\right] \cdot \left[\frac{2^{n-1}}{(n-1)!} \cdot \prod_{i=1}^{n-1} \frac{\|\widehat{b}_i\|_2}{F_i(b_i)}\right] = \frac{2^n}{n!} \cdot \prod_{i=1}^{n} \frac{\|\widehat{b}_i\|_2}{F_i(b_i)}$$

Für die obere Schranke betrachten wir den Quader mit Grundfläche S_{n-1} und Höhe $\frac{\|\widehat{b}_n\|}{F_n(b_n)}$. Da S_n in zwei dieser Quader enthalten ist (siehe Abbildung 9.1.2), gilt:

$$V_n \leq 2 \cdot V_{n-1} \cdot \frac{\|\widehat{b}_n\|_2}{F_n(b_n)}$$

Aus der Induktionsannahme erhalten wir:

$$V_n \leq 2 \cdot V_{n-1} \cdot \frac{\|\widehat{b}_n\|_2}{F_n(b_n)} \leq 2 \cdot \frac{\|\widehat{b}_n\|_2}{F_n(b_n)} \cdot 2^{n-1} \cdot \prod_{i=1}^{n-1} \frac{\|\widehat{b}_i\|_2}{F_i(b_i)} = 2^n \cdot \prod_{i=1}^{n} \frac{\|\widehat{b}_i\|_2}{F_i(b_i)}$$

■

Es gilt für das erste sukzessive Minimum:

Satz 9.1.4 (Kaib 1994)
Für jede Gitterbasis $b_1, \ldots, b_n \in \mathbb{R}^m$ gilt:

$$\min_{i=1,\ldots,n} F_i(b_i) \leq \lambda_{1,\|\cdot\|} \leq \left(n! \cdot \prod_{i=1}^{n} F_i(b_i)\right)^{\frac{1}{n}}$$

Zum Vergleich für die ℓ_2-Norm: Wir wissen aus der Minkowski'schen Ungleichung 3.2.6 (Seite 25), daß wegen $\lambda_{1,\|\cdot\|} \leq \lambda_{2,\|\cdot\|} \leq \cdots \leq \lambda_{n,\|\cdot\|}$ für das Gitter $L = L(b_1, \ldots, b_n)$ gilt:

$$\min_{i=1,\ldots,n} \|\widehat{b}_i\| \leq \lambda_{i,\ell_2} \leq (\gamma_n)^{\frac{1}{2}} \cdot (\det L)^{\frac{1}{n}}$$

Beweis (zu Satz 9.1.4). Betrachten wir beide Abschätzungen:

- Wir zeigen:

  $$\min_{i=1,\ldots,n} F_i(b_i) \leq \lambda_{i,\|\cdot\|}$$

  Sei $b = \sum_{i=1}^n t_i b_i \in L$ mit $\|b\| = \lambda_{1,\|\cdot\|}$. Setze $s := \max\{i \mid t_i \neq 0\}$. Wegen $t_s \in \mathbb{Z} \setminus \{0\}$ gilt:

  $$\lambda_{1,\|\cdot\|} = \|b\| \geq F_s(b) = F_s(t_s b_s) = \underbrace{|t_s|}_{\geq 1} \cdot F_s(b_s) \geq F_s(b_s)$$

  Die Behauptung folgt aus:

  $$\min_{i=1,\ldots,n} F_i(b_i) \leq F_s(b_s) \leq \lambda_{i,\|\cdot\|}$$

- Sei $L = L(b_1, \ldots, b_n)$. Aus dem zweiten Satz von Minkowski **??** (Seite **??**) folgt wegen $\lambda_{1,\|\cdot\|} \leq \lambda_{2,\|\cdot\|} \leq \cdots \leq \lambda_{n,\|\cdot\|}$:

  $$V_n \cdot \lambda_{1,\|\cdot\|}^n \leq 2^n \cdot \det L \tag{9.2}$$

  Aus Lemma 9.1.2 wissen wir:

  $$\frac{n!}{2^n} \cdot \prod_{i=1}^n \frac{F_i(b_i)}{\|\widehat{b}_i\|_2} \geq \frac{1}{V_n} \tag{9.3}$$

  Aus $\det L = \prod_{i=1}^n \|\widehat{b}_i\|_2$ erhalten wir:

  $$\begin{aligned} \lambda_{1,\|\cdot\|}^n &\leq 2^n \cdot V_n^{-1} \cdot \prod_{i=1}^n \|\widehat{b}_i\|_2 && \text{(wegen (9.2))} \\ &\leq 2^n \cdot \left(\frac{n!}{2^n} \cdot \prod_{i=1}^n \frac{F_i(b_i)}{\|\widehat{b}_i\|_2} \right) \cdot \left(\prod_{i=1}^n \|\widehat{b}_i\|_2 \right) && \text{(wegen (9.3))} \\ &= n! \cdot \prod_{i=1}^n F_i(b_i) \end{aligned}$$

■

Es gilt für das Produkt der sukzessiven Minima:

Satz 9.1.5
Für jede Gitterbasis $b_1, \ldots, b_n \in \mathbb{R}^m$ gilt:

$$\frac{1}{n!} \cdot \prod_{i=1}^n F_i(b_i) \leq \prod_{i=1}^n \lambda_{i,\|\cdot\|} \leq n! \cdot \prod_{i=1}^n F_i(b_i)$$

Zum Vergleich: Die Minkowski'sche Ungleichung für die ℓ_2-Norm, Satz 3.2.6 auf Seite 25, besagt:

$$\prod_{i=1}^n \lambda_{i,\ell_2} \leq (\gamma_n)^{\frac{n}{2}} \cdot \det L$$

Beweis (zu Satz 9.1.5). Die Behauptung folgt aus dem Beweis zu Satz 9.1.4 durch Anwenden des zweiten Satzes von Minkowski **??** auf Seite **??**:

$$\frac{\det L}{n!} \leq \frac{V_n}{2^n} \cdot \prod_{i=1}^{n} \lambda_{i,\|\cdot\|} \leq \det L$$

∎

9.2 Reduzierte Basen zur Norm $\|\cdot\|$

Analog zur Euklidischen Norm führen wir Reduktionsbegriffe ein und versuchen, Eigenschaften reduzierter Basen zu beweisen.

9.2.1 Definitionen

Wir übertragen die Reduktionsbegriffe auf den Fall einer beliebig vorgegebenen Norm:

Definition 9.2.1 (HKZ-reduzierte Basis zu $\|\cdot\|$)
Eine geordnete Basis $b_1, \ldots, b_n \in \mathbb{R}^m$ ist eine HKZ-reduzierte Basis zur Norm $\|\cdot\|$, wenn:

a) $F_j(b_i) \leq F_j(b_i \pm b_j)$ *für* $1 \leq j < i \leq n$ *(längenreduziert)*

b) $F_i(b_i) = \min\{F_i(b) \mid b \in L(b_i, b_{i+1}, \ldots, b_n) \setminus \{0\}\}$ *für* $i = 1, \ldots, n$

Beim zweiten Kriterium kann b auch aus $L(b_1, \ldots, b_n) \setminus \{0\}$ gewählt werden. Für die Eigenschaft „längenreduziert" gilt mit $1 \leq j < i \leq n$:

$$F_j(b_i) \leq F_j(b_i \pm b_j) \qquad \Longleftrightarrow \qquad F_j(b_i) = \min_{t \in \mathbb{Z}} F_j\left(b_i + t \cdot b_j\right)$$

Diese Äquivalenz nutzt die Konvexität der Norm F_j. Die „$\Leftarrow$"-Richtung folgt unmittelbar und für die „$\Rightarrow$"-Richtung beachtet man, daß gilt:

$$F_j(b_i) \leq F_j(b_i - b_j) \qquad \text{und} \qquad F_j(b_i) \leq F_j(b_i + b_j)$$

Definition 9.2.2 (β-reduzierte Basis zu $\|\cdot\|$)
Sei $b_1, \ldots, b_n \in \mathbb{R}^m$ eine geordnete Basis und $\beta \in \{2, 3, \ldots, n\}$ gegeben. $b_1, \ldots, b_n \in \mathbb{R}^m$ heißt β-reduziert (blockreduziert mit Blockgröße β) zur Norm $\|\cdot\|$, wenn:

a) $F_j(b_i) \leq F_j(b_i \pm b_j)$ *für* $1 \leq j < i \leq n$

b) $F_i(b_i) = \min\left\{F_i(b) \;\middle|\; b \in L(b_i, b_{i+1}, \ldots, b_{\min(i+\beta-1,n)}) \setminus \{0\}\right\}$ *für* $i = 1, \ldots, n-1$

Wir betrachten den Spezialfall einer 2-reduzierten Basis zu $\|\cdot\|$: Die geordnete Basis $b_1, \ldots, b_n \in \mathbb{R}^m$ ist 2-reduziert zur Norm $\|\cdot\|$, wenn:

a) $F_j(b_i) \leq F_j(b_i \pm b_j)$ für $1 \leq j < i \leq n$

b) $F_i(b_i) = \min\left\{F_i(sb_i + tb_{i+1}) \;\middle|\; (s,t) \in \mathbb{Z}^2 \setminus \{(0,0)\}\right\}$ für $i = 1, \ldots, n-1$

Eine 2-reduzierte Basis zur ℓ_2-Norm ist eine LLL-reduzierte Basis.

9.2.2 Eigenschaften 2-reduzierter Gitterbasen

Wir untersuchen die Eigenschaften 2-reduzierter Basen und vergleichen die Resultate, die wir im Spezialfall der ℓ_2-Norm (LLL-reduziert) in Kapitel **??** (Seite **??** und folgende) bewiesen haben.

Satz 9.2.3
Sei $b_1, \ldots, b_n \in \mathbb{R}^m$ eine 2-reduzierte Basis zur Norm $\|\cdot\|$. Dann gilt für $i = 1, \ldots, n-1$:

$$F_{i+1}(b_{i+1}) \geq \tfrac{1}{2} \cdot F_i(b_i)$$

Zum Vergleich: Für die ℓ_2-Norm ist mit $\delta = \frac{3}{4}$ nach Lemma 5.1.2 auf Seite 35 $\|\widehat{b}_i\|_2^2 \leq 2 \cdot \|\widehat{b}_{i+1}\|_2^2$, also:

$$\|\widehat{b}_{i+1}\|_2 \geq \sqrt{\tfrac{1}{2}} \cdot \|\widehat{b}_i\|_2$$

Beweis (zu Satz 9.2.3). Nach Definition gilt

a) $F_j(b_i) \leq F_j(b_i \pm b_j)$ für $1 \leq j < i \leq n$ und

b) $F_i(b_i) = \min\left\{F_i(sb_i + tb_{i+1}) \;\middle|\; (s,t) \in \mathbb{Z}^2 \setminus \{(0,0)\}\right\}$ für $i = 1, \ldots, n-1$.

Die Behauptung $F_i(b_i) \leq \frac{1}{2} \cdot F_i(b_{i+1})$ erhalten wir aus:

$$\begin{aligned}
F_i(b_i) &\leq F_i(b_{i+1}) && \text{(wegen Eigenschaft b))}\\
&\leq \min\{F_i(b_{i+1} - tb_i) \mid t \in \mathbb{Z}\} && \text{(wegen Eigenschaft a))}\\
&\leq F_i(b_{i+1}) + \tfrac{1}{2} \cdot F_i(b_i)
\end{aligned}$$

Wir nutzen, daß die Abstandsfunktionen F_i jeweils Normen auf $\operatorname{span}(b_1, \ldots, b_{i-1})^\perp$ sind:

$$\begin{aligned}
F_{i+1}(b_{i+1}) &= \min\{F_i(b_{i+1} - sb_i) \mid s \in \mathbb{R}\} && \text{(Definition)}\\
&= \min\left\{F_i\big(b_{i+1} - (r+t)b_i\big) \;\middle|\; t \in \mathbb{Z}, r \in \left[-\tfrac{1}{2}, +\tfrac{1}{2}\right]\right\}\\
&\leq \min\{F_i(b_{i+1} - tb_i) \mid t \in \mathbb{Z}\} + F_i\left(\tfrac{1}{2} \cdot b_i\right) && \text{(Dreiecksungleichung)}\\
&\leq \min\{F_i(b_{i+1} - tb_i) \mid t \in \mathbb{Z}\} + \tfrac{1}{2} \cdot F_i(b_i) && \text{(Linearität)}
\end{aligned}$$

■

Im folgenden Satz untersuchen wir, wie gut im allgemeinen Fall der erste Vektor der 2-reduzierten Basis das erste sukzessive Minimum approximiert.

Satz 9.2.4
Sei $b_1, \ldots, b_n \in \mathbb{R}^m$ eine 2-reduzierte Basis zur Norm $\|\cdot\|$. Dann gilt:

$$\|b_1\| \leq 2^{n-1} \cdot \lambda_{1,\|\cdot\|}$$

Zum Vergleich: Für die ℓ_2-Norm wissen wir mit $\delta = \frac{3}{4}$ aus Satz 5.1.4 auf Seite 36:

$$\|b_1\|_2 \leq \left(\tfrac{4}{3}\right)^{\frac{n-1}{2}} \cdot \lambda_{1,\ell_2}$$

Beweis. Sei $b = \sum_{i=1}^{n} t_i b_i$ $\|\cdot\|$-minimaler Vektor in $L = (b_1, \dots, b_n) \setminus \{0\}$. O.B.d.A. sei $t_n \in \mathbb{Z} \setminus \{0\}$. Es gilt:

$$\begin{aligned}
\|b\| &\geq F_n(b) \\
&= \min_{t_1,\dots,t_{n-1}\in\mathbb{R}} \left\| b - \sum_{j=1}^{n-1} t_j b_j \right\| && \text{(Definition)} \\
&= F_n(t_n b_n) \\
&= |t_n| \cdot F_n(b_n) && \text{(Linearität der Norm } F_n\text{)} \\
&\geq F_n(b_n) && \text{(wegen } t_n \in \mathbb{Z} \setminus \{0\}\text{)} \\
&\geq 2^{-n+1} \cdot F_1(b_1) && \text{(induktiv aus Satz 9.2.3)} \\
&= \|b_1\| \cdot 2^{-n+1} && \text{(wegen } F_1(b_i) = \|b_i\| \text{ und } \widehat{b}_1 = b_1\text{)}
\end{aligned}$$

Wegen $\lambda_{1,\|\cdot\|} = \|b\|$ folgt die Behauptung. ■

9.2.3 Eigenschaften HKZ-reduzierter Basen

Wir untersuchen die Eigenschaften von HKZ-Basen und vergleichen die Resultate, die wir im Spezialfall der ℓ_2-Norm in Kapitel 7.1 (Seite 55 und folgende) bewiesen haben. Es gilt für HKZ-reduzierte Basen zur Norm $\|\cdot\|$:

Satz 9.2.5 (Lovász, Scarf 1992)
Sei $b_1, \dots, b_n$ eine HKZ-reduzierte Basis zu $\|\cdot\|$ des Gitters L. Es gilt für $i = 1, \dots, n$:

$$\frac{2}{i+1} \cdot \|b_i\| \leq \lambda_{i,\|\cdot\|} \leq \frac{i+1}{2} \cdot F_i(b_i) \leq \frac{i+1}{2} \cdot \|b_i\|$$

Zum Vergleich: Für die ℓ_2-Norm wissen wir aus Satz 7.1.2 auf Seite 56, daß für $i = 1, \dots, n$ gilt:

$$\frac{i+3}{4} \cdot \|b_i\| \leq \lambda_{i,\ell_2} \leq \frac{i+1}{4} \|b_i\|$$

Beweis (zu Satz 9.2.5). Wir zeigen die untere und obere Schranke:

- Wir zeigen $\frac{2}{i+1} \cdot \|b_i\| \leq \lambda_{i,\|\cdot\|}$ für $i = 1, \dots, n$. Angenommen, $h_1, \dots, h_n \in L$ realisieren die sukzessiven Minima $\lambda_1, \dots, \lambda_n$, d.h. es ist $\|h_i\| = \lambda_{i,\|\cdot\|}$ für $i = 1, \dots, n$, und die Vektoren $h_1, \dots, h_n$ sind linear unabhängig. Es gilt

  $$\max_{j\leq i} F_i(h_j) \geq F_i(b_i), \tag{9.4}$$

  weil:

  - wegen $\dim(\operatorname{span}(h_1, \dots, h_i)) = i$ ist $\max_{j\leq i} F_i(h_j) \neq 0$ und
  - $b_1, \dots, b_n$ eine HKZ-reduzierte Basis ist, also

    $$F_i(b_i) = \min\{F_i(b) \mid b \in L(b_i, \dots, b_n) \setminus \{0\}\}$$

    gilt.

  Wir erhalten aus (9.4) und $\lambda_{1,\|\cdot\|} \leq \lambda_{2,\|\cdot\|} \leq \cdots \leq \lambda_{n,\|\cdot\|}$:

  $$\lambda_{i,\|\cdot\|} = \|h_i\| = \max_{j\leq i} \|h_i\| \geq F_i(b_i) \tag{9.5}$$

Wir wenden aus Beweis zu Satz 9.2.3 die Ungleichung

$$\min_{\mu \in \mathbb{Z}} F_j(x + \mu \cdot b_j) \leq F_{j+1}(x) + \tfrac{1}{2} \cdot F_j(b_j)$$

rekursiv beginnend mit $x := b_i$ und $j = i - 1$ an:

$$\begin{aligned} F_{i-1}(b_i) &\leq F_{i-1}(b_i + \mu_{i,i-1} \cdot b_{i-1}) && \text{für alle } \mu_{i,i-1} \in \mathbb{Z} \\ &\leq F_i(b_i) + \tfrac{1}{2} \cdot F_{i-1}(b_{i-1}) && \text{für Minimalstelle } \mu_{i,i-1} \in \mathbb{Z} \end{aligned}$$

Im nächsten Schritt sei $x := b_i + \mu_{i,i-1} \cdot b_{i-1}$ mit Minimalstelle $\mu_{i,i-1} \in \mathbb{Z}$ und $j := i - 1$ usw. Nach $i - 1$ Schritten erhalten wir mit Abschätzung (9.5) die Behauptung:

$$\|b_i\| = F_1(b_i) \leq F_1\left(b_i + \sum_{j=1}^{i-1} \mu_{i,j} \cdot b_j\right) \leq \frac{i+1}{2} \cdot \lambda_{i,\|\cdot\|} \tag{9.6}$$

- Wir zeigen für $i = 1, \ldots, n$:

$$\lambda_{i,\|\cdot\|} \leq \frac{i+1}{2} \cdot F_i(b_i) \leq \frac{i+1}{2} \cdot \|b_i\|$$

Es gilt:

$$\begin{aligned} \lambda_{i,\|\cdot\|} &\leq \max_{j \leq i} F_1(b_j) && (\text{wegen } F_1(b) = \|b\|) \\ &\leq \max_{j \leq i} \left\{ F_j(b_j) + \tfrac{1}{2} \cdot \sum_{t=1}^{j-1} F_t(b_t) \right\} && (\text{wegen } (9.6)) \\ &\leq \max_{j \leq i} \left\{ \tfrac{j+1}{2} \cdot F_j(b_j) \right\} && (\text{wegen } (9.6)) \\ &\leq \tfrac{i+1}{2} \cdot F_1(b_i) && (\text{wegen } F_t(b_t) \leq F_1(b_j) \text{ für } t < j) \\ &\leq \tfrac{i+1}{2} \cdot \|b_i\| && (\text{wegen } F_1(b_i) = \|\widehat{b}_i\| \leq \|b\|) \end{aligned}$$

■

9.2.4 Eigenschaften β-reduzierter Gitterbasen

Wir untersuchen die Eigenschaften von HRZ-Basen und vergleichen die Resultate, die wir im Spezialfall der ℓ_2-Norm in Kapitel 7.2 (Seite 57 und folgende) bewiesen haben. Wir definieren:

Definition 9.2.6 (α_β)
Wir setzen:

$$\alpha_\beta := \sup \left\{ \frac{\|b_1\|}{F_\beta(b_\beta)} \;\middle|\; \begin{array}{l} b_1, \ldots, b_n \text{ HKZ-reduzierte} \\ \text{Basis und } \|\cdot\| \text{ Norm} \end{array} \right\}$$

Satz 9.2.7
Für jede β-reduzierte Basis $b_1, \ldots, b_n$ zu $\|\cdot\|$ gilt:

$$\|b_1\| \leq \alpha_\beta^{\left\lceil \frac{n-1}{\beta-1} \right\rceil} \cdot \lambda_{1,\|\cdot\|}$$

Beweis. Sei $h_i := F_i(b_i)$. Bestimme Index μ mit minimalem h_μ. Nach Satz 9.1.4 gilt $h_\mu \leq \lambda_{1,\|\cdot\|}$. Für $j < \beta$ sind die Basen $b_i, b_{i+1} \ldots, b_{i+j}$ HKZ-reduzierte Basen zur Norm F_i. Nach Definition von α_β und wegen $\alpha_k \leq \alpha_{k+1}$ gilt:

$$h_i \leq \alpha_\beta \cdot h_{i+j} \tag{9.7}$$

Wir erhalten durch wiederholtes Anwenden von (9.7):

$$h_1 \leq \alpha_\beta \cdot h_{1+1(\beta-1)} \leq \alpha_\beta^2 \cdot h_{1+2(\beta-1)} \leq \alpha_\beta^3 \cdot h_{1+3(\beta-1)} \leq \ldots \leq \alpha_\beta^{\left\lfloor \frac{\mu-1}{\beta-1} \right\rfloor} \cdot h_{1+\left\lfloor \frac{\mu-1}{\beta-1} \right\rfloor (\beta-1)}$$

Insgesamt erhalten wir:

$$h_1 \leq \alpha_\beta^{\left\lceil \frac{\mu-1}{\beta-1} \right\rceil} \cdot h_\mu \leq \alpha_\beta^{\left\lceil \frac{n-1}{\beta-1} \right\rceil} \cdot \lambda_{1,\|\cdot\|}$$

■

Für die ℓ_2-Norm zeigt C.P. Schnorr [Schnorr87, Korollar 2.5], daß für

$$\alpha_{\beta,\ell_2} := \sup \left\{ \frac{\|b_1\|_2}{\|\widehat{b}_\beta\|} \ : \ b_1, \ldots, b_n \text{ HKZ-reduzierte Basis} \right\} \tag{9.8}$$

gilt, wobei α_{β,ℓ_2} als Quadrat von (9.8) definiert und als Korkine-Zolotareff-Konstante bezeichnet wird):

$$\alpha_{\beta,\ell_2} \leq k^{\frac{1+\ln k}{2}}$$

Analog zeigt man für beliebige Norm:

$$\alpha_k \leq k(k-1)^{\ln(k-1)}$$

Satz 9.2.8
Jede β-reduzierte Basis $b_1, \ldots, b_n$ erfüllt für $i = 1, \ldots, n$

$$\frac{2}{i+1} \cdot \gamma_\beta'^{\,-\frac{i-\beta/2}{\beta-1}} \leq \frac{\|b_i\|}{\lambda_{i,\|\cdot\|}} \leq \frac{i+1}{2} \cdot \gamma_\beta'^{\,\frac{n-\beta/2}{\beta-1}}$$

mit $\gamma'_\beta = (\beta!)^{\frac{2}{\beta}} \approx \left(\frac{\beta}{e}\right)^2$.

Zum Vergleich: In der ℓ_2-Norm gilt für die Hermite-Konstante γ_β nach Satz 7.2.3 auf Seite 58:

$$\sqrt{\frac{4}{i+3}} \cdot \gamma_\beta^{-\frac{i-1}{\beta-1}} \leq \frac{\|b_i\|}{\lambda_{i,\ell_2}} \leq \sqrt{\frac{i+3}{4}} \cdot \gamma_\beta^{\frac{n-1}{\beta-1}}$$

Der Beweis zu Satz 9.2.8 ist im wesentlichen analog zum Beweis zur ℓ_2-Norm. Wichtiger „Baustein“ ist folgendes Analogon zu Lemma 7.2.5 auf Seite 58: Für jede β-reduzierte Basis $b_1, \ldots, b_n$ gilt:

$$\|b_1\| \leq \gamma_\beta'^{\,\frac{m-\beta/2}{\beta-1}} \cdot M \qquad \text{mit} \quad M := \max_{n-\beta+2 \leq i \leq n} F_i(b_i)$$

9.3 Konstruktion einer HKZ-reduzierten Gitterbasis

Gegeben sei ein Gitter L vom Rang n. Wir konstruieren eine HKZ-reduzierte Basis in zwei Schritten, wobei die Konstruktion allerdings nicht effizient ist.

1. Wir wählen für $i = 1, \dots, n$ ein $b_i \in L$ mit:

$$F_i(b_i) = \min \{F_i(b) \mid b \in L, F_i(b) \neq 0\}$$

Beachte, $F_i(b)$ ist definiert, da wir im i-ten Schritt bereits $b_1, \dots, b_{i-1}$ festgelegt haben. Es gilt genau dann $F_i(b) \neq 0$, wenn $b \notin \operatorname{span}(b_1, \dots, b_{i-1})$. Die Vektoren $b_1, \dots, b_n$ bilden eine Basis von L: Falls dies nicht der Fall ist, existiert ein minimales i, so daß $b_1, \dots, b_i$ kein primitives System ist:

$$L \cap \operatorname{span}(b_1, \dots, b_{i-1}) = L(b_1, \dots, b_{i-1}) \tag{9.9}$$

$$L \cap \operatorname{span}(b_1, \dots, b_i) \supsetneq L(b_1, \dots, b_i) \tag{9.10}$$

Wegen 9.10 existiert ein $b \in L \cap \operatorname{span}(b_1, \dots, b_i) \setminus L(b_1, \dots, b_i)$ mit:

$$b = \sum_{j=1}^{i-1} t_j b_j + t_i b_i \qquad \text{mit } t_1, \dots, t_{i-1} \in \mathbb{Z} \text{ und } t_i \notin \mathbb{Z}$$

Sei $k > 1$ der Index der additiven Untergruppe $L(b_1, \dots, b_i)$ in $\operatorname{span}(b_1, \dots, b_i) \cap L$. Wegen (9.9) gilt:

$$t_i \in \tfrac{1}{k} + \mathbb{Z}$$

Wähle $t' = t_i \mod \mathbb{Z}$, d.h. $t' = \frac{1}{k} \in]0,1[$. Es folgt der Widerspruch zur Minimalität:

$$F_i(t_1 b_1 + t_2 b_2 + \dots + t' b_i) = F_i(t' b_i) = |t'| \cdot F_i(b_i) < F_i(b_i).$$

2. Längenreduktion: Für $i = 1, \dots, n$, für $j = i-1, i-2, \dots, 1$ wähle $\mu_{i,j} \in \mathbb{Z}$, so daß:

$$F_j(b_i + \mu_{i,i-1} b_{i-1} + \mu_{i,i-2} b_{i-2} + \dots + \mu_{i,j} b_j)$$

minimal ist. Setze:

$$b_i := b_i + \sum_{j=1}^{i-1} \mu_{i,j} b_j$$

Die Längenreduktion sichert $F_j(b_j) \leq F_j(b_i \pm b_j)$ für $j < i$.

Lemma 9.3.1
Obige Konstruktion liefert eine HKZ-reduzierte Basis $b_1, \dots, b_n$ des Gitters L.

Beweis. Nachrechnen! ■

9.4 Alternative zur Reduktion in $\|\cdot\|$

Alternativ zur Reduktion in $\|\cdot\|$ kann man $S_{\|\cdot\|}(1)$ durch $S_{\|\cdot\|_{\mathrm{E}}}(1)$ mit Ellipsoid-Norm $\|\cdot\|_{\mathrm{E}}$ approximieren und die Reduktion in der Ellipsoid-Norm durchführen.

$$\|x\|_{\mathrm{E}}^2 := x^{\mathsf{T}} B^{\mathsf{T}} B x$$

Die Sätze für die ℓ_2-Norm übertragen sich. Nach [John48] gilt: Zu jeder Norm $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}$ gibt es eine Ellipsoid-Norm $\|\cdot\|_{\mathrm{E}}$ mit

$$\|x\|_{\mathrm{E}} \leq \|x\| \leq \sqrt{n} \cdot \|x\|_{\mathrm{E}}$$

Dann folgt für die $\|\cdot\|_{\mathrm{E}}$ β-reduzierte Basis nach Satz 7.2.3:

$$\tfrac{1}{n} \cdot \sqrt{\tfrac{4}{i+3}} \cdot \gamma_\beta^{-\frac{i-1}{\beta-1}} \leq \frac{\|b_i\|}{\lambda_{i,\|\cdot\|}} \leq n \cdot \sqrt{\tfrac{i+3}{4}} \cdot \gamma_\beta^{\frac{n-1}{\beta-1}} \tag{9.11}$$

Dabei geht ein Faktor $\sqrt{n}$ verloren bei der Approximation von $\|\cdot\|$ durch $\|\cdot\|_{\mathrm{E}}$. Ein weiterer Faktor $\sqrt{n}$ geht verloren durch die Approximation von $\lambda_{i,\|\cdot\|}$ durch λ_{i,ℓ_2}.

Für kleine Blockweiten β ist die Aussage (9.11) schärfer als Satz 9.2.8, weil $\gamma'_\beta = \Theta\left(\gamma_\beta^2\right)$. Für große Blockweiten $\beta \approx n$ ist Satz 9.2.8 schärfer. Für $\beta = n$ sind die Schranken für HKZ-reduzierte Basen zu $\|\cdot\|$ um den Faktor $\sqrt{n}$ besser als die Schranken (9.11).

9.5 Konstruktion eines $\|\cdot\|$-kürzesten Gittervektors

Wir übertragen unseren Algorithmus zur Bestimmung eines kürzesten Gittervektors für die Euklidische Norm aus Kapitel 8.1 auf beliebige Normen. H. Ritters [Ritter96, Ritter97] gibt eine Übersicht über die Aufzählung kürzester Gittervektoren in der sup-Norm.

9.5.1 ENUM-Algorithmus für beliebige Norm

Wir verallgemeinern Algorithmus 8.1.1 von Seite 66. Es bezeichne:

$$c_t(u_t, u_{t+1}, \ldots, u_n) := F_t\left(\sum_{i=t}^n u_i b_i\right)$$

Wir bezeichnen zu $\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n$ mit $\mathrm{next}_{F_t}(u)$ die erste, ganzzahlige Minimalstelle u' von

$$\left| F_t\left(u \cdot b_t + \sum_{i=t}^n \tilde{u}_i b_i\right) - F_t\left(u' \cdot b_t + \sum_{i=t}^n \tilde{u}_i b_i\right)\right| \tag{9.12}$$

und mit $\mathrm{next}_{F_t}(\tilde{u}_t, u)$ die nächste, ganzzahlige Nullstelle von (9.12) nach $\tilde{u}_t$. Falls $S_{\|\cdot\|}$ ein Polytop ist, z.B. für die 1- und sup-Norm, kann F_t durch lineare Optimierung bestimmt werden.

9.5.2 Gauß-ENUM-Algorithmus für beliebige Norm

Betrachten wir Schritt 2 des Algorithmus' 9.5.1. Gegeben sind $b_1, \ldots, b_n$ sowie $\tilde{u}_1, \ldots, \tilde{u}_n$ und $c_1^{\min}$. Sei $\overline{L} := L(b_1, \ldots, b_{t-1})$ und setze:

$$z := -\sum_{i=t}^n \tilde{u_i} b_i$$

Dann gilt:

$$\begin{aligned}\left|\left\{(\tilde{u}_1, \ldots, \tilde{u}_{t-1}) \in \mathbb{Z}^{t-1} \,:\, c_1(\tilde{u}_1, \ldots, \tilde{u}_{t-1}) \leq c_1^{\min}\right\}\right| &= \left|\left(\overline{L} + w\right) \cap S_{\|\cdot\|}(\,c_1^{\min})\right| \\ &= \left|\overline{L} \cap \left(S_{\|\cdot\|}(\,c_1^{\min}) + z\right)\right|\end{aligned}$$

Algorithmus 9.5.1 $\|\cdot\|$-ENUM: kürzester Gittervektor (vollständige Aufzählung)

EINGABE: Gitterbasis $b_1, \ldots, b_n \in \mathbb{R}^m$

1. FOR $i = 1, \ldots, n$ DO $\tilde{c}_i := u_i := \tilde{u}_i := y_i := 0$

2. $\tilde{u}_1 := u_1 := 1$; $t := 1$;

3. $c_1^{\min} := \tilde{c}_1 := \|b_1\|^2$

/* stets gilt: $\tilde{c}_t = c_t(\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n)$ und $c_1^{\min}$ ist aktuelles Minimum der Funktion c_1 */

4. WHILE $t \leq n$ DO

4.1. $\tilde{c}_t := c_t(\tilde{u}_t, \tilde{u}_{t+1}, \ldots, \tilde{u}_n) = F_t\left(\sum_{i=t}^{n} \tilde{u}_i b_i\right)$

4.2. IF $\tilde{c}_t < c_1^{\min}$ THEN

IF $t > 1$ THEN

$t := t - 1$

u reelle Minimalstelle von $F_t\left(u b_t + \sum_{i=t+1}^{n} \tilde{u}_i b_i\right)$

$\tilde{u}_t := \text{next}_{F_t}(u)$

ELSE

$c_1^{\min} := \tilde{c}_1$

FOR $i = 1, \ldots, n$ DO $u_i := \tilde{u}_i$

END if

ELSE

$t := t + 1$

/* $t_{\max}$ bezeichne den bisherigen maximalen Wert von t vor der Erhöhung */

$$\tilde{u}_t := \begin{cases} \tilde{u}_t + 1 & \text{falls } t = t_{\max} \\ \text{next}_{F_t}(\tilde{u}_t, u) & \text{sonst} \end{cases}$$

END if

END while

AUSGABE: Minimalstelle $(u_1, \ldots, u_n) \in \mathbb{Z} \setminus \{0\}$ und Minimalwert $c_1^{\min}$ für die Funktion c_1

Nach der Volumenheuristik ist:

$$\begin{aligned} \left|\overline{L} \cap \left[S_{\|\cdot\|}(c_1^{\min}) + z\right]\right| &\approx \frac{\text{vol}_{t-1}\left(\text{span}(\overline{L}) \cap \left[S_{\|\cdot\|}(c_1^{\min}) + z\right]\right)}{\det \overline{L}} \\ &= \frac{\text{vol}_{t-1}\left(\left[w + \text{span}(\overline{L})\right] \cap S_{\|\cdot\|}(c_1^{\min})\right)}{\det \overline{L}} \end{aligned}$$

Wann gilt die Volumen-Heuristik streng? Hinreichende Voraussetzung: Bei festem y ist z uniformly distributed modulo $\overline{L}$ (vergleiche Definition 8.2.3 auf Seite 70):

$$b = \underbrace{\sum_{j=1}^{t-1}\sum_{i=1}^{n} \tilde{u}_i \mu_{i,j} \widehat{b}_j}_{=-z\in\operatorname{span}(\overline{L})} + \underbrace{\sum_{j=t}^{n}\sum_{i=t}^{n} \tilde{u}_i \mu_{i,j} \widehat{b}_j}_{:=y\in\operatorname{span}(\overline{L})^{\perp}}$$

Die Menge $\left(b+\operatorname{span}(\overline{L})\right) \cap S_{\|\cdot\|}(c_1^{\min})$ hängt nur von z, aber nicht von y ab. Es folgt aus der Volumenheuristik Lemma 8.2.1 (Seite 67):

Lemma 9.5.1
Angenommen, z ist uniformly distributed modulo $\overline{L}$ und unabhängig von y. Dann gilt

$$\mathrm{E}\left[\,\left|[w+\overline{L}\,] \cap S_{\|\cdot\|}(c_1^{\min})\right|\right] = \frac{\operatorname{vol}_{t-1}\left([y+\operatorname{span}(\overline{L})] \cap S_{\|\cdot\|}(c_1^{\min})\right)}{\det \overline{L}},$$

wobei $y+\operatorname{span}(\overline{L}) = b+\operatorname{span}(\overline{L})$.

Wir erhalten analog zu Satz 8.2.5:

Satz 9.5.2
Angenommen, $(\{\mu_{i,j}\} : 1 \leq j < i \leq n)$ ist gleichverteilt in $[0,1[^{\binom{n}{2}}$. Dann gilt in Algorithmus 9.5.1 $\|\cdot\|$-ENUM stets:

- *z ist uniformly distributed modulo $\overline{L}$ und unabhängig von y.*
- $\mathrm{E}\left[\,\left|[w+\overline{L}\,] \cap S_{\|\cdot\|}(c_1^{\min})\right|\right] = \dfrac{\operatorname{vol}_{t-1}\left([y+\operatorname{span}(\overline{L})] \cap S_{\|\cdot\|}(c_1^{\min})\right)}{\det \overline{L}}$

Wir erhalten Gauß-$\|\cdot\|$-ENUM aus Algorithmus' 9.5.1, indem wir Schritt 2 ersetzen durch:

$$\text{IF } \frac{\operatorname{vol}_{t-1}\left([y+\operatorname{span}(\overline{L})] \cap S_{\|\cdot\|}(c_1^{\min})\right)}{\det \overline{L}} \geq 2^{-p}$$

Kapitel 10

Anwendungen der Gitterreduktion

In Kapitel 6 (Seite 47 und folgende) haben wir versucht, Subsetsum-Aufgaben durch Gitterreduktion zu lösen. In diesem Kapitel werden wir weitere Anwendungen der Gitterreduktion kennenlernen: Lösen des 3-SAT-Problems, Angriff auf Dåmgards Hashfunktion (finde zwei verschiedene Vektoren, denen der gleiche Werte zugewiesen wird) und Faktorisieren ganzer Zahlen. Für weitere Anwendungen der Gitterreduktion in der Kryptographie verweisen wir auf die Arbeit [JoSt94] von A. Joux und J. Stern.

Für eine effiziente Aufzählung kürzester Gittervektor in der sup-Norm verweisen wir auf H. Ritters Arbeit [Ritter96], in der er mit Hilfe der Gitterreduktion G. Ortons [Orton1994] Kryptosystem basierend auf dem Subsetsum-Problem mit Dichte größer als 1 bricht. Die Methoden können auf beliebige Normen ℓ_p übertragen werden.

10.1 Gitterbasis zu 3-SAT

Wir beschreiben zunächst die konjunktive Normalform. Seien $x_1, \ldots, x_n$ Boole'sche Variablen. Wir schreiben $x_i^{-1} := \neg\, x_i$, $x_i^1 := x_i$ und $x_i^0 := 0$. Die Klauseln der konjunktiven Normalform (KNF) schreiben wir als:

$$C_j = x_1^{a_{j1}} \vee x_2^{a_{j2}} \vee \cdots \vee x_n^{a_{jn}}$$

mit $(a_{j1}, a_{j2}, \ldots, a_{jn}) \in \{0, \pm 1\}^n$. Falls eine Variable x_i nicht in der Klausel C_j auftritt, setze $a_{ji} := 0$. Die KNF γ hat folgenden Aufbau

$$\gamma(x_1, \ldots, x_n) := \bigwedge_{j=1}^{m} C_j(x_1, \ldots, x_n)$$

Wir betrachten nur konjunktive Normalformen, deren Klauseln aus maximal drei Literalen bestehen, also $\sum_{i=1}^{n} |a_{ji}| \leq 3$ für $j = 1, \ldots, m$. Beim 3-SAT-Problem ist zu entscheiden, ob eine erfüllende Belegung für die konjunktive Normalform existiert:

Definition 10.1.1 (3-SAT)
Das 3-SAT-Problem lautet:

- *Gegeben: KNF* $\gamma(x_1, \ldots, x_n) := \bigwedge_{j=1}^{m} C_j(x_1, \ldots, x_n)$ *mit max. 3 Literalen pro Klausel*
- *Finde* $(y_1, \ldots, y_n) \in \{0,1\}^n$ *mit* $\gamma(y_1, \ldots, y_n) = 1$ *oder zeige, daß keine erfüllende Belegung existiert.*

Das 3-SAT-Problem ist $\mathcal{NP}$-vollständig [GaJo79]. Wir ordnen dem 3-SAT-Problem eine Gitterbasis zu und versuchen, durch Gitterreduktion in der sup-Norm eine erfüllende Belegung der konjunktiven Normalform zu bestimmen.

Wir reduzieren zunächst 3-SAT auf $\{0,1\}$-Integer-Programming, indem wir ein äquivalentes Ungleichungssystem bilden:

$$c_j := 2 - |\{i \,:\, a_{ji} = -1\}| \leq 1 \qquad \text{für } j = 1, \ldots, m$$

Betrachte das folgende Ungleichungssystem in den Unbekannten $y_1, \ldots, y_n \in \{0,1\}$:

$$\left| \sum_{i=1}^{n} a_{ji} y_i - c_j \right| \leq 1 \qquad \text{für } j = 1, \ldots, m \tag{10.1}$$

Beispiel:

$$\begin{aligned} x_1 \vee x_2 \vee x_3 \quad &\leftrightarrow \quad |y_1 + y_2 + y_3 - 2| \leq 1 \\ \neg\, x_1 \vee x_2 \vee x_3 \quad &\leftrightarrow \quad |-y_1 + y_2 + y_3 - 1| \leq 1 \end{aligned}$$

Wir können jede Restriktion in zwei $\leq$-Relationen aufspalten. Durch Fallunterscheidung über die Anzahl negierter/nicht-negierter Literale in der Klausel folgt:

Lemma 10.1.2
Die $\{0,1\}$-IP-Aufgabe (10.1) hat genau dann eine Lösung $y \in \{0,1\}^n$, wenn $\gamma(y) = 1$.

Die Gitterbasis zum 3-SAT-Problem besteht aus den folgenden $n+1$ ganzzahligen Zeilenvektoren $b_1, \ldots, b_{n+1} \in \mathbb{Z}^{n+m+1}$:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \\ b_{n+1} \end{bmatrix} := \begin{bmatrix} 2 & 0 & \cdots & 0 & a_{11} & a_{21} & \cdots & a_{m1} & 0 \\ 0 & 2 & & 0 & a_{12} & a_{22} & \cdots & a_{m2} & 0 \\ \vdots & & \ddots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & & 2 & a_{1n} & a_{2n} & \cdots & a_{mn} & 0 \\ -1 & -1 & \cdots & -1 & -c_1 & -c_2 & \cdots & -c_m & +1 \end{bmatrix} \tag{10.2}$$

Sei $y = (y_1, \ldots, y_n)$ eine erfüllende Belegung der KNF. Der zugehörige Lösungsvektor ist:

$$b(y) = \sum_{i=1}^{n} y_i b_i + b_{n+1}$$

Dieser Vektor liegt wegen (10.1) in $\{\pm 1\}^n \times \{\pm 1, 0\}^m \times \{+1\}$.

Satz 10.1.3
Sei L das von den Zeilenvektoren $b_1, \ldots, b_{n+1}$ aus (10.2) erzeugte Gitter. Dann gilt für alle Gittervektoren $z \in L$:

Es existiert eine erfüllende Belegung $y \in \{0,1\}^n$ zu $\gamma(y)$ mit $z = \pm b(y)$ $\iff$ $\|z\|_\infty = 1$

Beweis. Wir zeigen beide Richtungen:

„$\Rightarrow$" Wegen $b(y) \in \{\pm 1, 0\}^{n+m+1}$ gilt $\|z\|_\infty = 1$.

„$\Leftarrow$" Gegeben ist ein Vektor $z \in L$ mit $\|z\|_\infty = 1$. Der Vektor habe die Darstellung

$$z = \sum_{i=1}^{n+1} y'_i b_i \tag{10.3}$$

mit $y'_1, y'_2, \ldots, y'_{n+1} \in \mathbb{Z}$. Wegen $\|z\|_\infty = 1$ folgt aus der letzten Komponente der Basisvektoren, daß $y'_{n+1} = \pm 1$ ist. Aus den ersten n Einträgen erhalten wir nach Fallunterscheidung:

1. Aus $y_{n+1} = +1$ folgt $(y'_1, y'_2, \ldots, y'_n) \in \{0, +1\}^n$.
2. Aus $y_{n+1} = -1$ folgt $(y'_1, y'_2, \ldots, y'_n) \in \{0, -1\}^n$.

Setze:

$$y := y'_{n+1} \cdot (y'_1, y'_2, \ldots, y'_n)$$

Es ist $y \in \{0, +1\}^n$ und $(y, 1) = y'_{n+1} \cdot y'$. Wegen $\|z\|_\infty = 1$ und $y'_{n+1} \in \{\pm 1\}$ gilt nach (10.3)

$$\left| \sum_{i=1}^{n} a_{ji} y_i - c_j \right| = \left| y'_{n+1} \right| \cdot \left| \sum_{i=1}^{n} a_{ji} y_i - c_j \right| \leq \|z\|_\infty \leq 1$$

für $j = 1, \ldots, m$. Nach Lemma 10.1.2 ist y eine erfüllende Belegung.

■

Wir versuchen durch Gitterreduktionen, einen in der sup-Norm kürzesten, nicht-trivalen Gittervektor zu finden, um eine erfüllende Belegung der konjunktive Normalformen mit höchstens drei Literalen pro Klausel zu bestimmen. Unter der Cook'schen Hypothese $\mathcal{P} \neq \mathcal{NP}$ ist dies in einigen Fällen schwierig, denn das 3-SAT-Problem ist $\mathcal{NP}$-vollständig.

Wir haben mit Satz 10.1.3 einen alternativen Beweis zu Korollar 11.2.9 von Seite 103 kennengelernt: Das Problem $\|\cdot\|_\infty$-kürzester Gittervektor ist $\mathcal{NP}$-vollständig.

10.2 Angriff auf Dåmgards Hashfunktion

I.B. Dåmgard [Dåmgard89] hat der EuroCrypt-Konferenz 1989 die folgende kryptographische Hashfunktion basierend auf dem Subsetsum-Problem vorgestellt. Wähle zufällig und unabhängig

$$a = (a_1, \ldots, a_n) \in_{\mathrm{R}} [1, 2^m - 1]^n$$

und definiere zu a die Hashfunktion:

$$\begin{array}{rcll} h_a & : & \{0,1\}^n & \to \mathbb{N} \\ & & (x_1, \ldots, x_n) & \mapsto \sum_{i=1}^n a_i x_i \end{array}$$

Eine *Kollision* nennen wir $x, x' \in \{0,1\}^n$, $x \neq x'$, mit $h_a(x) = h_a(x')$. Als *Pseudo-Kollision* bezeichnen wir $x, x' \in \{0,1\}^n$, $x \neq x'$, mit $h_a(x) = h_a(x') \pmod{2^m}$. Wir werden versuchen, Pseudo-Kollisionen zu finden.

Weshalb suchen wir nach Kollisionen? Um eine lange Nachricht M durch eine kurze, digitale Unterschrift zu versehen, wendet man in der Kryptographie die Hashfunktion h auf die Nachricht an und erhält einen im Vergleich zur Nachricht kleinen Wert. Nur $h(M)$ wird digital unterschrieben. Der Teilnehmer veröffentlicht M und seine digitale Unterschrift von $h(M)$. Falls wir eine andere Nachricht M' mit $h(M) = h(M')$ finden, können wir die digitale Unterschrift für M einfach übernehmen. Wir haben eine Nachricht mit digitaler Unterschrift eines fremden Teilnehmers.

Jedem Vektor $\overline{x} = (\overline{x}_1, \ldots, \overline{x}_n) \in \{\pm 1, 0\}^n \setminus \{0\}$ mit

$$\sum_{i=1}^{n} a_i \cdot \overline{x}_i = 0 \pmod{2^m}$$

entspricht eine Pseudo-Kollision x, x' gemäß

$$x_i := \begin{cases} 1 & \text{falls } \overline{x}_i = 1 \\ 0 & \text{sonst} \end{cases} \qquad x'_i := \begin{cases} 1 & \text{falls } \overline{x}_i = -1 \\ 0 & \text{sonst} \end{cases}$$

und umgekehrt. Wir wählen als Basis:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \\ b_{n+1} \end{bmatrix} := \begin{bmatrix} 1 & 0 & \cdots & 0 & a_1 n \\ 0 & 1 & & 0 & a_2 n \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & & 1 & a_n n \\ 0 & 0 & \cdots & 0 & 2^m n \end{bmatrix} \tag{10.4}$$

Wir bezeichnen:

$$\text{P-Kollision} := \left\{ (x_1, \ldots, x_{n+1}) \in \{\pm 1, 0\}^{n+1} \;\middle|\; \begin{array}{l} x_{n+1} = 0 \text{ und } (x_1, \ldots, x_n) \\ \text{entspricht Pseudo-Kollision} \end{array} \right\}$$

Es gilt offenbar: P-Kollision $\subseteq L(b_1, \ldots, b_{n+1})$. Wir versuchen durch Gitterreduktion, einen kurzen Gittervektor in der Euklidischen Norm zu finden. Was ist das Minimum der Menge

$$\{\|x\|_2 \,:\, x \in \text{P-Kollision}\},$$

also die Länge des kürzesten Gittervektors, der einer Pseudo-Kollision entspricht? Wir führen eine probabilistische Analyse zu $a \in_{\mathrm{R}} [1, 2^m - 1]^n$ und festem x durch. Zu $\alpha \in \left[0, \frac{1}{2}\right]$ mit $\alpha n \in \mathbb{N}$ sei:

$$\mathcal{N}_\alpha := \left\{ (x_1, \ldots, x_n) \in \{\pm 1, 0\}^n \;\middle|\; \sum_{i=1}^{n} |x_i| = \alpha n \right\}$$

Für $x \in \mathcal{N}_\alpha$ ist $\|x\|_2 = \sqrt{\alpha n}$, da $x \in \{\pm 1, 0\}^n$. Es gilt:

$$N_\alpha := |\mathcal{N}_\alpha| = \binom{n}{\alpha n} \cdot 2^{\alpha n} \tag{10.5}$$

Denn wir können die αn Einträge ungleich 0 beliebig auf die n Positionen verteilen und als Wert jeweils $+1$ oder -1 setzen. Es gilt

$$N_\alpha \approx 2^{(H(\alpha, 1-\alpha) + \alpha) \cdot n}, \tag{10.6}$$

wobei H die Shannon'sche Entropie-Funktion ist:

$$H(\alpha, 1-\alpha) = -\alpha \cdot \log_2 \alpha - (1-\alpha) \cdot \log_2 (1-\alpha)$$

Wir möchten bezüglich $a \in_{\mathrm{R}} [1, 2^m - 1]^n$ die Wahrscheinlichkeit berechnen, mit der in $\mathcal{N}_\alpha$ ein Vektor aus P-Kollision liegt. Dazu definieren wir zu a und festem $x \in \mathcal{N}_\alpha$ die Zufallsvariable:

$$\xi_x := \begin{cases} 1 & \text{falls } \sum\limits_{i=1}^{n} a_i x_i = 0 \pmod{2^m} \\ 0 & \text{sonst} \end{cases}$$

Offenbar ist

$$\mathrm{E}_a[\xi_x] = 2^{-m} \tag{10.7}$$

Wir definieren die Zufallsvariable $\overline{\xi}_x := \xi_x - 2^{-m}$, so daß:

$$\mathrm{E}_a\left[\overline{\xi}_x\right] = 0 \tag{10.8}$$

$$\mathrm{E}_a\left[\overline{\xi}_x^2\right] = \mathrm{E}_a\left[\xi_x^2\right] - 2\cdot 2^{-m}\cdot \mathrm{E}_a\left[\xi_x\right] + 2^{-2m} \leq 2\cdot 2^{-m} \tag{10.9}$$

Beachte, daß für die Indikatorvariable ξ_i gilt $\mathrm{Ws}_a[\xi_i = 1] = \mathrm{Ws}_a\left[\xi_i^2 = 1\right]$. Wir verwenden aus der Stochastik (siehe u.a. [Feller68]) für eine Zufallsvariable X:

$$\begin{aligned} \mathrm{Var}[X] &= \mathrm{E}\left[X^2\right] - \mathrm{E}[X]^2 && \text{(Definition Varianz)} \\ \mathrm{Var}[cX] &= c^2 \cdot \mathrm{Var}[X] && (c > 0 \text{ konstant}) \\ \mathrm{Ws}[|X - \mathrm{E}[X]| \geq \epsilon] &\leq \frac{1}{\epsilon^2}\cdot \mathrm{Var}[X] && \text{(Tschebycheff-Ungleichung)} \end{aligned}$$

Wir wenden die Tschebycheff-Ungleichung auf $\frac{1}{N_\alpha}\cdot\sum_{x\in\mathcal{N}_\alpha}\xi_x$ an und erhalten wegen der Erwartungswerte (10.8) und (10.9):

$$\begin{aligned} \mathrm{Ws}_a\left[\left|\frac{1}{N_\alpha}\cdot\sum_{x\in\mathcal{N}_\alpha}\xi_x - 2^{-m}\right| \geq \epsilon\right] &\leq \frac{1}{\epsilon^2}\cdot\mathrm{Var}\left[\frac{1}{N_\alpha}\cdot\sum_{x\in\mathcal{N}_\alpha}\xi_x\right] \\ &= \frac{1}{\epsilon^2\cdot N_\alpha^2}\cdot\sum_{x\in\mathcal{N}_\alpha}\sum_{y\in\mathcal{N}_\alpha}\mathrm{E}_a\left[\overline{\xi}_x\cdot\overline{\xi}_y\right] \end{aligned}$$

Wegen des Erwartungswerts (10.9) ist:

$$\begin{aligned} \sum_{x\in\mathcal{N}_\alpha}\sum_{y\in\mathcal{N}_\alpha}\mathrm{E}_a\left[\overline{\xi}_x\cdot\overline{\xi}_y\right] &= \sum_{x\in\mathcal{N}_\alpha}\mathrm{E}_a\left[\overline{\xi}_x^2\right] + \sum_{\substack{x,y\in\mathcal{N}_\alpha\\ x\neq y}}\mathrm{E}_a\left[\overline{\xi}_x\right]\cdot\mathrm{E}_a\left[\overline{\xi}_y\right] \\ &= \sum_{x\in\mathcal{N}_\alpha}\mathrm{E}_a\left[\overline{\xi}_x^2\right] \\ &= N_\alpha\cdot\mathrm{E}_a\left[\overline{\xi}_x^2\right] \end{aligned} \tag{10.10}$$

Aus Abschätzung (10.10) und dem Erwartungswert (10.8) folgt:

$$\mathrm{Ws}_a\left[\left|\frac{1}{N_\alpha}\cdot\sum_{x\in\mathcal{N}_\alpha}\xi_x - 2^{-m}\right| \geq \epsilon\right] \leq \frac{1}{\epsilon^2\cdot N_\alpha}\cdot\mathrm{E}_a\left[\overline{\xi}_x^2\right] \leq \frac{2}{\epsilon^2\cdot N_\alpha\cdot 2^m}$$

Für $\epsilon = 2^{-m}$ erhalten wir

$$\mathrm{Ws}_a\left[\sum_{x\in\mathcal{N}_\alpha}\xi_x = 0\right] \leq \frac{2^{m+1}}{N_\alpha} \tag{10.11}$$

und für $\epsilon = 2^{-m-l}$:

$$\mathrm{Ws}_a\left[\sum_{x\in\mathcal{N}_\alpha}\xi_x \leq N_\alpha\cdot\left(2^{-m} - 2^{-m-l}\right)\right] \leq \frac{2^{m+1+2l}}{N_\alpha} \tag{10.12}$$

Aus (10.11) folgt unmittelbar:

Satz 10.2.1
Es gilt:

a) Für $m \leq \log_2 N_\alpha - 2 \approx (H(\alpha, 1-\alpha) + \alpha) \cdot n$ gibt es bezüglich $a \in_{\mathrm{R}} [1, 2^m - 1]^n$ mit Wahrscheinlichkeit mindestens $\frac{1}{2}$ Pseudo-Kollisionen in $\mathcal{N}_\alpha$.

b) Für $m \leq \log_2 N_\alpha - 4 \approx (H(\alpha, 1-\alpha) + \alpha) \cdot n$ gibt es bezüglich $a \in_{\mathrm{R}} [1, 2^m - 1]^n$ mit Wahrscheinlichkeit mindestens $\frac{1}{2}$ mindestens $N_\alpha \cdot 2^{-m-1}$ Pseudo-Kollisionen in $\mathcal{N}_\alpha$.

Beweis. Die Aussage a) folgt aus (10.11), die Aussage b) folgt aus (10.12) mit $l = 1$. ■

Im nächsten Schritt möchten wir $N_\alpha = |\mathcal{N}_\alpha|$ maximieren: Aus dem Ansatz

$$\frac{\partial N_\alpha}{\partial \alpha} = 0$$

mit (10.6) erhalten wir:

$$-\log_2 2 \approx \frac{\partial\left(-\alpha \cdot \log_2 \alpha - (1-\alpha) \cdot \log_2(1-\alpha)\right)}{\partial \alpha}$$

Dazu äquivalent:

$$\log_2 \alpha + \log_2(1-\alpha) \approx -\log_2 2$$

Wegen $-\log_2 2 = -1$ und $-1 + \log_2 \alpha = \log_2 \frac{1}{\alpha}$ erhalten wir den Anzatz $\alpha = \frac{k-1}{k}$

$$-\log_2 \tfrac{k-1}{k} + \log_2 \tfrac{1}{k} = \log_2(k-1) \approx -\log_2 2$$

und somit $k - 1 = 2$ bzw. $k = 3$, also $\alpha = \frac{2}{3}$ als ungefähre Maximalsstelle von N_α.

Satz 10.2.2
Bezüglich $a \in_{\mathrm{R}} [1, 2^m - 1]^n$ gibt es mit Wahrscheinlichkeit mindestens $\frac{1}{2}$ Pseudo-Kollisionen, wenn $N_{2/3} \geq 2^{m-1}$ oder äquivalent $n \geq \frac{m-1}{\log_2 3}$ ist.

Beweis. Aus (10.7) wissen wir, daß:

$$\mathrm{E}_a\left[\,\text{Anzahl Pseudo-Kollisionen in } \mathcal{N}_\alpha\right] = N_\alpha \cdot 2^{-m}$$

Wegen $N_{2/3} \geq 2^{m-1}$ folgt:

$$\mathrm{Ws}_a\left[\text{Anzahl Pseudo-Kollisionen in } \mathcal{N}_{2/3}\right] \geq \tfrac{1}{2}$$

Damit $N_{2/3} \geq 2^{m-1}$ ist, muß wegen

$$\begin{aligned}
\log_2 N_{2/3} &= n \cdot \left[-\tfrac{2}{3} \cdot \log_2 \tfrac{2}{3} - \tfrac{1}{3} \cdot \log_2 \tfrac{1}{3} + \tfrac{2}{3} \cdot \log_2 2\right] \\
&= n \cdot \left[-\tfrac{2}{3} \cdot (-\log_2 3 + \log_2) - \tfrac{1}{3} \cdot (-\log_2 3) + \tfrac{2}{3}\right] \\
&= n \cdot \left[+\tfrac{2}{3} \cdot \log_2 3 - \tfrac{2}{3} + \tfrac{1}{3} \cdot \log_2 3 + \tfrac{2}{3}\right] \\
&= n \cdot \log_2 3
\end{aligned}$$

gelten $n \cdot \log_2 3 \geq m - 1$ oder äquivalent $n \geq \frac{m-1}{\log_2 3}$. ■

Betrachten wir die Situation bei den von I.B. Dåmgard vorgeschlagenen Parametern:

- Für $m = 120$ gibt es Pseudo-Kollisionen, falls $n \geq 77$.
- Für $m = 120$ und $n = 100$ gibt es im Mittel $N_{2/3} \cdot 2^{-m} \approx 3,8 \cdot 10^{11}$ Pseudo-Kollisionen.

Betrachten wir die Anzahl der kurzen Gittervektoren:

$$\left|\left\{ z \in L(b_1, \ldots, b_{n+1}) \,:\, \|z\|_2^2 \leq \alpha n \right\}\right| \approx \frac{N(0,n,\alpha)}{2^m}$$

J.E.Mazo und A.M.Odlyzko haben in [MaOd90] die Funktion

$$N(z,n,\alpha) := \left|\left\{ x \in \mathbb{Z}^n \,:\, \|x - z\|^2 \leq \alpha \cdot n \right\}\right|$$

untersucht. Als Vektoren z kommen nur Vektoren in Frage, deren letzter Eintrag 0 ist. Der Anteil der Vektoren $(x_1, \ldots, x_n)$ mit $\sum_{i=1}^n a_i x_i = 0 \pmod{2^m}$ ist 2^{-m}. Es gilt:

$$\left|\left\{ z \in L(b_1, \ldots, b_{n+1}) \,:\, \|z\|_2^2 \leq \alpha n \right\}\right| \approx \frac{(2e\pi\alpha)^{\frac{n}{2}}}{2^m}$$

Wir wählen m und α derart, daß in etwa gilt

$$\mathrm{E}_a\,[\,\text{Anzahl Pseudo-Kollisionen in } \mathcal{N}_\alpha] \approx 1,$$

Also wegen (10.5) und (10.6):

$$m = n \cdot [H(\alpha, 1-\alpha) + \alpha] \qquad \text{bzw.} \qquad N_\alpha = \binom{n}{\alpha n} \cdot 2^{\alpha n} = 2^m$$

Gibt es zur Länge $\sqrt{\alpha n}$ kürzere, nicht-triviale Gittervektoren, die keiner Pseudo-Kollision entsprechen? Wir würden bei der Gitter-Reduktion unter Umständen diese kürzeren Vektoren anstatt der gewünschten erhalten. Für $m = 120$ und $n = 100$ ist $\frac{(2e\pi\alpha)^{\frac{n}{2}}}{2^m} \approx 2^{0{,}0039n}$, d.h. die sog. parasitären, kurzen Gittervektoren sind leicht in der Überzahl.

10.3 Faktorisieren ganzer Zahlen mit Hilfe Diophantischer Approximationen

Sei $N \in \mathbb{Z}$ das Produkt mindestens zweier verschiedener Primzahlen und $p_1, p_2, \ldots$ die Folge der Primzahlen. C.P. Schnorr [Schnorr91b, Schnorr93] hat das Problem der Faktorisierung von N auf das Finden von $t+2$ Lösungen $(e_1, \ldots, e_t) \in \mathbb{Z}^t$ der Ungleichungen ($c > 1$ fest)

$$\begin{aligned} &\left| \sum_{i=1}^t e_i \ln p_i - \ln N \right| \leq N^{-c} \cdot p_t^{\mathrm{o}(1)} \\ &\sum_{i=1}^t |e_i \ln p_i| \leq (2c-1) \cdot \log_2 N + 2 \cdot \ln p_t \end{aligned} \tag{10.14}$$

reduziert. Wir möchten in diesem Kapitel die Idee und den Algorithmus vorstellen. Für eine ausführliche Betrachtung verweisen wir auf die Originalarbeit.

Wir assoziieren mit den Primzahlen $p_1, \ldots, p_t$ ein Gitter im $\mathbb{R}^{t+1}$ und mit N einen Punkt $\vec{N}$ im $\mathbb{R}^{t+1}$. Das Problem der Diophantischen Approximation (10.14) reduzieren wir auf die Bestimmung eines in der ℓ_1-Norm hinreichend nahen Gitterpunktes.

Sei $p_1, \ldots, p_t$ die Folge der ersten Primzahlen, also $2, 3, 5, \ldots$. Wir definieren zu N und festem $c > 1$ das Gitter $L_{\alpha,c} \subseteq \mathbb{R}^{t+1}$, welches von den Zeilenvektoren $b_1, \ldots, b_t, \vec{N}$ aufgespannt wird:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_t \\ \vec{N} \end{bmatrix} := \begin{bmatrix} \ln p_1 & 0 & \cdots & 0 & N^c \cdot \ln p_1 \\ 0 & \ln p_2 & & 0 & N^c \cdot \ln p_2 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & & \ln p_n & N^c \cdot \ln p_t \\ 0 & 0 & \cdots & 0 & N^c \cdot \ln N \end{bmatrix} \tag{10.15}$$

Die reellen Vektoren kann man durch rationale Vektoren approximieren. In der Praxis genügen sogar ganzzahlige Vektoren.

Betrachten wir Algorithmus 10.3.1. Da N das Produkt mindestens zweier verschiedener Primzahlen ist, hat x^2 mindestens 4 Wurzeln modulo N, wobei sich zwei nur im Vorzeichen unterscheiden.

$$x^2 - y^2 = (x-y)(x+y) = 0 \pmod N$$

Im Fall $x \neq \pm y \pmod N$ sind $0 < x - y < N$ und $0 < x + y < N$, also $1 < x \pm y < N$, wobei $x \pm y$ modulo N reduziert sei. Dann liefert $\mathrm{ggT}(x \pm y, N)$ nicht-triviale Teiler von N. Falls x und y sich wie unabhängige Zufallsvariable verhalten, hat Schritt 7 Erfolgswahrscheinlichkeit mindestens $\frac{1}{2}$.

Der Schritt 4 erfordert, daß $|u_i - v_i N|$ über der Basis P_t faktorisiert werden kann. Satz 10.3.2 zeigt, daß für Punkte $z \in L_{\alpha,c}$, die „nahe" bei $\vec{N}$ liegen, diese Voraussetzung mit hoher Wahrscheinlichkeit erfüllt ist.

Satz 10.3.1
Sei $c > 1$, $\beta, \delta \geq 0$ fest und $p_t < N$. Falls $(e_1, \ldots, e_t) \in \mathbb{Z}^t$ das Ungleichungssystem

$$\left| \sum_{i=1}^{t} a_i \ln p_i - \ln N \right| \leq N^{-c} \cdot p_t^{o(1)}$$
$$\sum_{i=1}^{t} |a_i \ln p_i| \leq (2c-1) \cdot \log_2 N + 2 \cdot \ln p_t$$

löst, gilt für das in Schritt 3 konstruierte Paar (u_i, v_i) mit

$$u_i := \prod_{a_{i,j} > 0} p_j^{a_{ij}} \qquad \text{und} \qquad v_i := \prod_{a_{i,j} < 0} p_j^{|a_{i,j}|} \tag{10.16}$$

daß:

$$|u_i - v_i N| \leq p_t^{\beta + \delta + o(1)}$$

Beweis. Siehe [Schnorr93, Theorem 1]. ■

Falls $(e_1, \ldots, e_t) \in \mathbb{Z}^t$ die Ungleichungen (10.16) erfüllt mit $\beta + \delta \leq 1$ und N hinreichend groß ist, erfüllt das Paar (u_i, v_i) mit hoher Wahrscheinlichkeit die zur Faktorisierung in Schritt 4 nötigen Eigenschaften:

$$u_i = \prod_{a_{i,j} > 0} p_j^{a_{ij}} \qquad \text{und} \qquad |u_i - v_i N| \leq p_t$$

Dies ist nur mit vernachlässigbarer Wahrscheinlichkeit nicht der Fall [Schnorr93, Theorem 4].

Satz 10.3.2
Sei $\alpha > 1$, $c > 1$, $\delta \geq 0$ und $p_t = (\ln N)^{\alpha} < N$. Falls $z \in L_{\alpha,c}$ die Ungleichung

$$\|z - N\|_1 \leq (2c-1) \cdot \ln N + 2\delta \cdot \ln p_t$$

erfüllt, gilt für die in Schritt 3 konstruierten Paare (u_i, v_i):

$$|u_i - v_i N| \leq p_t^{\frac{1}{\alpha} + \beta + o(1)}$$

Beweis. Siehe [Schnorr93, Theorem 2]. ■

Aus den beiden Sätzen 10.3.1 und 10.3.2 folgt, daß es zum Faktorisieren von N genügt, hinreichend viele Gittervektoren $z \in L_{\alpha,c}$ zu finden, die in der ℓ_1-Norm nahe bei $\vec{N}$ liegen. Diese Gitterpunkte findet man in der Praxis durch Anwenden mächtiger Reduktionsalgorithmen auf die Vektoren $b_1, \ldots, b_n, \vec{N}$ in der ℓ_2-Norm. Die reduzierte Basis enthält im allgemeinen dann Vektoren, die bezüglich der ℓ_1-Norm kurz sind. Man kann erreichen, daß diese Vektoren die Form

$$\sum_{i=1}^{t} e_i b_i - \vec{N}$$

haben ($e_1, \ldots, e_n \in \mathbb{Z}$) und wählen $z := \sum_{i=1}^{t} e_i b_i$ für Satz 10.3.2.

Algorithmus 10.3.1 Faktorisieren einer ganzen Zahl

EINGABE: ▷ $N \in \mathbb{Z}$ (Produkt mindestens zweier verschiedener Primzahlen)
▷ α und $c \in \mathbb{Q}$ mit $c \geq 1$

1. Bilde Liste $p_1, \ldots, p_t$ der ersten Primzahlen, $p_t = (\ln N)^\alpha$. Sei $P_t := \{p_1, \ldots, p_t\}$.

2. Reduziere mit „geeignetem" Reduktionsalgorithmus das Gitter $L_{\alpha,c} \subseteq \mathbb{R}^{t+1}$ (siehe Basismatrix (10.15)).

3. Bilde für Vektoren $z^{(i)} := \sum_{j=1}^{t} a_{i,j} b_j \in L$ mit kleiner l_1-Norm $\left\| z - \vec{N} \right\|_1$ mit Hilfe von P_t und den ganzzahligen Koeffizienten $(a_{i,1}, a_{i,2}, \ldots, a_{i,t})$ $m \geq t+2$ Tupel $(u_i, v_i) \in \mathbb{N}^2$:

$$u_i := \prod_{a_{i,j}>0} p_j^{a_{ij}}$$
$$v_i := \prod_{a_{i,j}<0} p_j^{|a_{i,j}|}$$

4. FOR $i = 1, \ldots, m$ DO

Faktorisiere $u_i - v_i N$ über P_t und $p_0 := -1$:

$$u_i - v_i N := \prod_{j=0}^{t} p_j^{b_{i,j}}$$

Setze $a_{i,0} := 0$. Bezeichne:

$$a_i := (a_{i,0}, a_{i,1}, \ldots, a_{i,t})$$
$$b_i := (b_{i,0}, b_{i,1}, \ldots, b_{i,t})$$

END for

5. Finde eine $\{0,1\}$-Lösung $(c_1, \ldots, c_m) \neq 0$ zu:

$$\sum_{i=1}^{m} c_i(a_i + b_i) = 0 \pmod 2 \tag{10.13}$$

6. Bilde (Division durch 2 wegen (10.13) möglich):

$$x := \prod_{j=0}^{t} p_j^{\sum_{i=1}^{m} c_i(a_{i,j}+b_{i,j})/2} \pmod N$$
$$y := \prod_{j=0}^{t} p_j^{\sum_{i=1}^{m} c_i b_{i,j}} \pmod N$$

Es gilt $x^2 = y^2 \pmod N$.

7. IF $x = \pm y \pmod N$ THEN GOTO 5 und berechne neue Lösung

AUSGABE: Zwei nicht-triviale Faktoren $\mathrm{ggT}(x+y, N)$ und $\mathrm{ggT}(x-y, N)$

Grundlagen

Notation

Mit $M_{m,n}(S)$ bezeichnen wir die Menge aller $m \times n$-Matrizen mit Einträgen aus der Menge S. Zum Beispiel ist $M_{m,n}(\mathbb{Z})$ die Menge aller ganzzahligen $m \times n$-Matrizen. Zur Matrix B bezeichne B^T die transponierte Matrix. Die Elemente aus $\mathbb{Z}^n$, $\mathbb{R}^n$, etc. schreiben wir, sofern nicht anders angegeben, als Spaltenvektoren.

Zur reellen Zahl r bezeichne $\lceil r \rfloor := \left\lceil r - \frac{1}{2} \right\rceil$ die nächste ganze Zahl. Wir schreiben $\mathbb{R}^+ := \{ x \in \mathbb{R} \mid x > 0 \}$ für die Menge der positiven, reellen Zahlen.

Skalarprodukt

Der Vektorraum $\mathbb{R}^n$ sei mit einem beliebigen Skalarprodukt $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ ausgestattet (*Euklidischer Vektorraum*). Das *Skalarprodukt* hat die folgenden Eigenschaften: Für alle $u, v, w \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$ gilt:

- $\langle \cdot, \cdot \rangle$ ist bilinear:
$$\begin{aligned} \langle u + w, v \rangle &= \langle u, v \rangle + \langle w, v \rangle \\ \langle \lambda u, v \rangle &= \lambda \langle u, v \rangle \\ \langle u, v + w \rangle &= \langle u, v \rangle + \langle u, w \rangle \\ \langle u, \lambda v \rangle &= \lambda \langle u, v \rangle \end{aligned}$$
- $\langle \cdot, \cdot \rangle$ ist symmetrisch:
$$\langle u, v \rangle = \langle v, u \rangle$$
- $\langle \cdot, \cdot \rangle$ ist positiv definit:
$$\langle u, u \rangle > 0 \qquad \text{für } u \neq 0$$

Für $u = 0$ folgt aus der Linearität in jeder Komponente $\langle u, u \rangle = 0$. Das *Standard-Skalarprodukt* ist definiert als:

$$\left\langle (u_1, \ldots, u_n)^\mathsf{T}, (v_1, \ldots, v_n)^\mathsf{T} \right\rangle := \sum_{i=1}^{n} u_i v_i$$

Den meisten Anwendungen liegt das Standard-Skalarprodukt zugrunde. Jedes Skalarprodukt $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ läßt sich schreiben als:

$$\langle u, v \rangle := u^\mathsf{T} S v$$

mit symmetrischer Matrix $S \in M_{n,n}(\mathbb{R})$. Im Fall des Standard-Skalarprodukts ist die Matrix S die Identität.

Normen

Eine Abbildung $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}$ heißt *Norm*, falls für alle $u, v \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$ gilt:

$$\begin{aligned} \|\lambda v\| &= |\lambda| \cdot \|v\| && \text{(positive Homogenität)} \\ \|u + v\| &\leq \|u\| + \|v\| && \text{(Dreiecksungleichung)} \\ \|u\| &\geq 0 \qquad \text{für } u \neq 0 && \text{(positive Definitheit)} \end{aligned}$$

Die reelle Zahl $\|u\|$ heißt *Norm* (oder *Länge*) des Vektors $u = (u_1, \ldots, u_n)$. Aus einem Skalarprodukt erhält man die *Euklidische Norm* durch:

$$\|u\| := \sqrt{\langle u, u \rangle}$$

Die ℓ_1*-Norm* oder auch *Betragsnorm* ist:

$$\left\| (u_1, \ldots, u_n)^\mathsf{T} \right\|_1 := \sum_{i=1}^{n} |u_i|$$

Die ℓ_2*-Norm* erhält man aus dem Standard-Skalarprodukt:

$$\left\| (u_1, \ldots, u_n)^\mathsf{T} \right\|_2 := \sqrt{\langle u, u \rangle} = \left(\sum_{i=1}^{n} u_i^2 \right)^{\frac{1}{2}}$$

Allgemein: Die ℓ_p*-Norm* ist:

$$\left\| (u_1, \ldots, u_n)^\mathsf{T} \right\|_p := \left(\sum_{i=1}^{n} |u_i|^p \right)^{\frac{1}{p}}$$

Die *sup-Norm*, *Maximums-Norm* oder auch ℓ_∞*-Norm* ist:

$$\left\| (u_1, \ldots, u_n)^\mathsf{T} \right\|_\infty := \max_{i=1,\ldots,n} |u_i|$$

Ungleichungen

Für die sup-, Betrags- und 2-Norm eines Vektors $u \in \mathbb{R}^n$ gelten die folgenden Beziehungen:

$$\begin{aligned} \|u\|_2 \leq \|u\|_1 \leq \sqrt{n} \cdot \|u\|_2 \\ \|u\|_\infty \leq \|u\|_2 \leq n \cdot \|u\|_\infty \end{aligned}$$

Für die Beziehung Skalarprodukt und zugehörige Norm $\|u\| := \sqrt{\langle u, u \rangle}$ gilt die *Cauchy-Schwarz-Ungleichung* (seien $u, v \in \mathbb{R}^n$):

$$|\langle u, v \rangle| \leq \|u\| \cdot \|v\|$$

Die Gleichheit gilt genau dann, wenn beide Vektoren linear abhängig sind. Seien $b_1, \ldots, b_n \in \mathbb{R}^n$ die Spaltenvektoren (oder Zeilenvektoren) der Matrix $B \in M_{n,n}(\mathbb{R})$. Die *Hadamard'sche Ungleichung* besagt:

$$\det B \leq \prod_{i=1}^{n} \|b_i\|_2$$

Sind die Vektoren $b_1, \ldots, b_n$ orthogonal, gilt die Gleichheit.

Kapitel 11

Komplexität, $\mathcal{NP}$-Vollständigkeit

Wir fassen mit Hinblick auf die Gittertheorie die Grundbegriffe der Komplexitätstheorie, speziell die $\mathcal{NP}$-Vollständigkeit, zusammen.

11.1 $\mathcal{NP}$-Vollständigkeit

Wir definieren die Bitlänge endlicher Objekte (das Vorzeichen speichern wir getrennt):

- $\ell(0) := 1$
- $\ell(n) := \lceil \log_2(n+1) \rceil$ für $n \in \mathbb{N}$
- $\ell\left(\frac{p}{q}\right) := \ell(p) + \ell(q)$ mit $p, q \in \mathbb{N}$ und $\mathrm{ggT}(p,q) = 1$
- $\ell(A) = \sum_{i,j} \ell(a_{ij})$ für $A = [a_{ij}] \in M_{m,n}(\mathbb{Q})$

Wir setzen die Laufzeit des Algorithmus' in Beziehung zur Eingabelänge. Wir interessieren uns für Polynomialzeit-Verfahren:

Definition 11.1.1 (Polynomialzeit)
Ein Algorithmus ist in Polynomialzeit, falls die Schrittzahl (Turing-Maschine oder Anzahl Bit-Operationen) polynomiell in der Länge der Eingabe beschränkt ist:

$$\textit{Schrittzahl(Eingabe)} = \mathrm{poly}\left(\ell(\textit{Eingabe})\right)$$

In der theoretischen Informatik betrachtet man die Polynomialzeit-Algorithmen als effizient.

Definition 11.1.2 (Charakteristische Funktion)
Zu einer Menge $A \subseteq \{0,1\}^*$ ist die charakteristische Funktion $\chi_A : \{0,1\}^* \to \{0,1\}$ definiert durch: $\chi_A(a) = 1$ genau dann, wenn $a \in A$ ist.

Wir definieren mit charakteristischen Funktionen die Klasse der Polynomialzeit-Sprachen:

Definition 11.1.3 (Klasse $\mathcal{P}$ der Polynomialzeit-Sprachen)
Die Klasse $\mathcal{P}$ der Polynomialzeit-Sprachen besteht genau aus den Sprachen $A \subseteq \{0,1\}^*$, für welche die charakteristische Funktion χ_A in Polynomialzeit berechenbar ist.

Die Klasse $\mathcal{NP}$ umfaßt die Sprache, so daß es genau für jedes Wort aus der Sprache einen Bitstring gibt, anhand dessen wir effizient überpüfen können, daß dieses Wort in der Sprache liegt.

Definition 11.1.4 (Klasse $\mathcal{NP}$)
Die Klasse $\mathcal{NP}$ der nichtdeterministischen Polynomialzeit-Sprachen $A \subseteq \{0,1\}^*$ ist erklärt durch:

$$A \in \mathcal{NP} \quad \Longleftrightarrow \quad \begin{array}{l} \exists B \in \{0,1\}^* \times \{0,1\}^*, B \in \mathcal{P}: \\ A = \left\{ x \in \{0,1\}^* \;\middle|\; \exists y \in \{0,1\}^{\mathrm{poly}(\ell(x))} \text{ mit } (x,y) \in B \right\} \end{array}$$

Sei $(x,y) \in B$. Dann heißt y Zeuge für $x \in A$.

Die Cook'sche Hypothese ist $\mathcal{P} \neq \mathcal{NP}$, d.h. es gibt Sprachen in der Klasse $\mathcal{NP}$, für die wir nicht in Polynomialzeit einen Zeugen finden können.

Definition 11.1.5 (Cook-Karp-Reduktion)
Seien $A, B \subseteq \{0,1\}^*$:

$$A \leq_{pol} B \quad \Longleftrightarrow \quad \begin{array}{l} \exists \text{ Polynomialzeit-Abbildung } h \text{ mit:} \\ \forall x \in \{0,1\}^* : x \in A \Leftrightarrow h(x) \in B \end{array}$$

Aus $A \leq_{\mathrm{pol}} B$ und $B \leq_{\mathrm{pol}} C$ folgt $A \leq_{\mathrm{pol}} C$. Es gilt $A \leq_{\mathrm{pol}} B$, wenn man $x \in A$ in Polynomialzeit mit einmaliger Anwendung eines Orakels für B entscheiden kann.

Definition 11.1.6 ($\mathcal{NP}$-vollständig)
$A \subseteq \{0,1\}^*$ heißt $\mathcal{NP}$-vollständig, wenn:

1. $A \in \mathcal{NP}$
2. $\forall B \in \mathcal{NP} : B \leq_{pol} A$

Falls wir einen Polynomialzeit-Algorithmus zu einem $\mathcal{NP}$-vollständigen Problem finden, folgt $\mathcal{P} = \mathcal{NP}$. Dies würde der Cook'schen Hypothese widersprechen. Daher gelten die $\mathcal{NP}$-vollständigen Probleme als die schwierigsten in $\mathcal{NP}$.

11.2 Schwierige, algorithmische Gitterprobleme

Wir lernen in diesem Abschnitt mit der Gittertheorie verbundene Probleme kennen, die $\mathcal{NP}$-vollständig sind oder für die bisher keine effizienten Algorithmen bekannt sind. Ein solches Problem ist die ganzzahlige, lineare Programmierung (Integer Programming):

Definition 11.2.1 (Ganzzahlige, lineare Programmierung)
Das Problem der ganzzahligen, linearen Programmierung lautet:

- *Gegeben: $m, n \in \mathbb{N}$, $A \in M_{m,n}(\mathbb{Z})$ und $b \in \mathbb{Z}^m$*
- *Finde $x \in \mathbb{Z}^n$ mit $Ax \leq b$ oder zeige, daß kein solcher Vektor existiert.*

Die ganzzahlige, lineare Programmierung ist „schwierig“. Wir werden in Satz 11.2.5 sehen, daß das zugehörige Entscheidungsproblem $\mathcal{NP}$-vollständig ist:

Definition 11.2.2 (Entscheidungsproblem der ganzzahligen, linearen Programmierung)
Das Problem der ganzzahligen, linearen Programmierung lautet:

- *Gegeben:* $m, n \in \mathbb{N}$, $A \in M_{m,n}(\mathbb{Z})$ *und* $b \in \mathbb{Z}^m$
- *Entscheide, ob ein* $x \in \mathbb{Z}^n$ *mit* $Ax \leq b$ *existiert.*

Falls $\mathcal{P} \neq \mathcal{NP}$, gibt es keinen Lösungsalgorithmus in Polynomialzeit. Dagegen gibt es zum analogen Problem der rationalen, linearen Programmierung Polynomialzeit-Verfahren:

Definition 11.2.3 (Rationale, lineare Programmierung)
Das Problem der rationalen, linearen Programmierung lautet:

- *Gegeben:* $m, n \in \mathbb{N}$, $A \in M_{m,n}(\mathbb{Z})$ *und* $b \in \mathbb{Q}^m$
- *Finde* $x \in \mathbb{Q}^n$ *mit* $Ax \leq b$ *oder zeige, daß kein solcher Vektor existiert.*

Das erste Polynomialzeit-Verfahren für die lineare Programmierung ist die Ellipsoid-Methode von L.G. Khachiyan [Khach79, Khach80]. Diese Methode ist aber nicht praktikabel. Ein bekannter Polynomialzeit-Algorithmus stammt von M. Karmarkars [Karma84]. Dieser hat zur Entwicklung der Interior-Point-Methoden für die lineare Programmierung geführt. Ein bekannter Interior-Point-Algorithmus stammt von Y. Ye [Ye91]. Ein einfaches, praktisches Verfahren ist der Simplex-Algorithmus [Dantzig63, Schrijver86] von G.B. Dantzig, der allerdings im Wortcase exponentielle Laufzeit haben kann. Weitere Probleme, die man in Polynomialzeit lösen kann, sind:

Satz 11.2.4 (Sieveking 1976)
Folgende Probleme sind zu gegebenen $m, n \in \mathbb{N}$, $A \in M_{m,n}(\mathbb{Z})$ *und* $b \in M_{m,1}(\mathbb{Z})$ *in Polynomialzeit lösbar:*

a) *Löse* $Ax = b$, $x \in \mathbb{Z}^n$ *oder weise Unlösbarkeit nach.*

b) *Finde eine* $\mathbb{Z}$*-Basis* $b_1, \ldots, b_k$ *von* $\{x \in \mathbb{Z}^n \mid Ax = 0\}$, *dem* $\mathbb{Z}$*-Kern. Eine* $\mathbb{Z}$*-Basis besteht aus linear unabhängigen Vektoren* $b_1, \ldots, b_k$, *so daß:*

$$\{x \in \mathbb{Z}^n \mid Ax = 0\} = \left\{ \sum_{i=1}^{k} t_i b_i \;\middle|\; t_1, \ldots, t_k \in \mathbb{Z} \right\}$$

Beweis. Modifikation des Gauß-Eliminationsverfahrens (M. Sieveking in [SpStr76]). Alternativer Beweis in [KaBa79]. ∎

Im folgenden Satz führen wir weitere mit der Gittertheorie verbundene Aufgaben bzw. Entscheidungsprobleme auf, die $\mathcal{NP}$-vollständig sind.

Satz 11.2.5
Folgende Sprachen sind $\mathcal{NP}$*-vollständig:*

1. *Integer-Programming:*

$$\mathrm{IP} := \left\{ (m, n, A, b) \;\middle|\; \begin{array}{l} A \in M_{m,n}(\mathbb{Z}), b \in \mathbb{Z}^m, \\ \exists x \in \mathbb{Z}^n : Ax \leq b \end{array} \right\}$$

2. *Rucksack (Knapsack) oder Subsetsum:*

$$\text{SubsetSum} := \left\{ (n, a_1, \dots, a_n, b) \in \mathbb{N}^{n+2} \;\middle|\; \exists x \in \{0,1\}^n : \sum_{i=1}^{n} a_i x_i = b \right\}$$

3. $\{0,1\}$*-Integer-Programming:*

$$\{0,1\}\text{-IP} := \left\{ (m, n, A, b) \;\middle|\; \begin{array}{c} A \in M_{n,m}(\mathbb{Z}), b \in \mathbb{Z}^m, \\ \exists x \in \{0,1\}^n : Ax \leq b \end{array} \right\}$$

4. *Schwache Zerlegung:*

$$\left\{ (n, a_1, \dots, a_n) \in \mathbb{N}^{n+1} \;\middle|\; \exists\, (x_1, \dots, x_n) \in \{0, \pm 1\}^n \setminus \{0^n\} : \sum_{i=1}^{n} a_i x_i = 0 \right\}$$

Beweis. Für 1,2,3 siehe [GaJo79, SpStr76], für 4 siehe [EmBoas81]. Den Nachweis, daß es für die Sprache Integer-Programming polynomiell lange Zeugen gibt, also IP $\in \mathcal{NP}$, werden wir in Satz 11.2.6 führen. ■

Satz 11.2.6 (von zur Gathen, Sieveking 1978)
IP $\in \mathcal{NP}$.

Beweis. Wir wählen als Zeugen für $(m, n, A, b) \in$ IP ein geeignetes $x \in \mathbb{Z}^n$ mit $Ax \leq b$. Offenbar existiert x genau dann, wenn $(m, n, A, b) \in$ IP. Wir müssen noch zeigen, daß der Zeuge polynomielle Länge hat.
Sei $A =: (a_{ij})_{ij}$ und $b =: (b_1, \dots, b_m)^{\mathsf{T}}$. Setze $M := \max_{i,j} \{|a_{ij}|, |b_i|\}$. Nach [GaSi78] gilt:

$$(\exists x \in \mathbb{Z}^n : Ax \leq b) \quad \Longleftrightarrow \quad \left(\exists x \in \mathbb{Z}^n : Ax \leq b,\ \|x\|_\infty \leq (n+1) n^{\frac{n}{2}} M^n\right)$$

Die obere Schranke von $\|x\|_\infty$ impliziert, daß die Länge des Zeugen x polynomiell in der Länge von A und b beschränkt ist. Wegen $\ell(m, n, A, b) \geq nm + \log_2 M$ gilt:

$$\ell(x) = \mathcal{O}\left(n^2 (\log n + \log M\right) = \mathcal{O}\left(\ell(m, n, A, b)^3\right)$$

■

Wir definieren die Begriffe, die elementar für die weiteren Kapitel sind:

Definition 11.2.7 (Gitter, Basis, Dimension, Rang)
Seien $b_1, \dots, b_n \in \mathbb{R}^m$ linear unabhängige Vektoren. Wir nennen die additive Untergruppe

$$L(b_1, \dots, b_n) := \sum_{i=1}^{n} b_i \mathbb{Z} = \left\{ \sum_{i=1}^{n} t_i b_i \;\middle|\; t_1, \dots, t_m \in \mathbb{Z} \right\}$$

des $\mathbb{R}^m$ ein Gitter mit der Basis $b_1, \dots, b_n$. Ist die Reihenfolge der Basisvektoren fest, sprechen wir von einer geordneten Basis. Der Rang oder auch die Dimension des Gitters ist $\mathrm{Rang}(L) := n$.

Betrachten wir ein Beispiel:

Beispiel 11.2.8 (Gitter)
$\mathbb{Z}^m$ ist ein Gitter vom Rang m, die Einheitsvektoren bilden eine Basis. Zur Matrix $A \in M_{m,n}(\mathbb{Z})$ ist $\{x \in \mathbb{Z}^n \mid Ax = 0\}$ ein Gitter vom Rang $n - \mathrm{Rang}(A)$; nach Satz 11.2.4 können wir in Polynomialzeit eine Basis konstruieren. ◇

Wir versuchen, durch Gitterreduktion einen kürzesten, nicht-trivialen Gittervektor zu finden. Im Fall der sup-Norm ist dies unter der Annahme $\mathcal{P} \neq \mathcal{NP}$ nicht immer effizient möglich:

Korollar 11.2.9
Das Problem $\|\cdot\|_\infty$-kürzester Gittervektor

$$L_\infty\text{-SVP} := \left\{ (m, n, b_1, \ldots, b_n) \;\middle|\; \begin{array}{l} m, n \in \mathbb{N}, b_1, \ldots, b_n \in \mathbb{Z}^m, \\ \exists x \in L(b_1, \ldots, b_n) : \ \|x\|_\infty = 1 \end{array} \right\}$$

ist $\mathcal{NP}$-vollständig.

Beweis. Das Problem $\|\cdot\|_\infty$-kürzester Gittervektor liegt in $\mathcal{NP}$: Als Zeugen wählt man einen Vektor $x \in L(b_1, \ldots, b_n) \setminus \{0\}$ mit $\|x\|_\infty = 1$. Das $\mathcal{NP}$-vollständige Problem „schwache Zerlegung" aus Satz 11.2.5 kann in Polynomialzeit auf $\|\cdot\|_\infty$-kürzester Gittervektor reduziert werden. ■

Beim Problem des kürzesten Gittervektors in der ℓ_2-Norm soll man zu gegebener Gitterbasis $b_1, \ldots, b_n$ und k entscheiden, ob es einen Gittervektor $z \in L(b_1, \ldots, b_n)$ gibt mit $z \neq 0$ und $\|z\|_2 \leq \sqrt{k}$.

Definition 11.2.10 (Shortest Vector Problem SVP)
Die Sprache zum kürzesten Gittervektorproblem (Shortest Vector Problem) für die ℓ_2-Norm lautet:

$$L_2\text{-SVP} := \left\{ (k, m, n, b_1, \ldots, b_n) \;\middle|\; \begin{array}{l} k, m, n, \in \mathbb{N}, b_1, \ldots, b_n \in \mathbb{Z}^m, \\ \exists x \in L(b_1, \ldots, b_n) \setminus \{0\} : \ \|x\|_2^2 \leq k \end{array} \right\}$$

Der Status dieses Problems ist offen. Anstrengungen, die Vermutung, daß L_2-SVP $\mathcal{NP}$-hart ist, nachzuweisen, sind im Gegensatz zur sup-Norm (siehe Korollar 11.2.9) bislang fehlgeschlagen (vergleiche [Kannan87]).

Das Problem des kürzesten Gittervektors ist der homogene Spezialfall des Problems nächster Gittervektor, von dem man aber weiß, daß es (auch) in der ℓ_2-Norm $\mathcal{NP}$-vollständig ist:

Satz 11.2.11 (Closest Vector Problem CVP)
Das Problem ℓ_2-nächster Gittervektor

$$L_2\text{-CVP} := \left\{ (k, m, n, b_1, \ldots, b_n, z) \;\middle|\; \begin{array}{l} k, m, n, \in \mathbb{N}, b_1, \ldots, b_n, z \in \mathbb{Z}^m, \\ \exists x \in L(b_1, \ldots, b_n) : \ \|z - x\|_2^2 \leq k \end{array} \right\}$$

ist $\mathcal{NP}$-vollständig.

Beweis. Siehe [Kannan87, Theorem6.2]. ■

Wir fassen zusammen: Zu gegebener Gitterbasis $b_1, \ldots, b_n \in \mathbb{Z}^m$ sind folgende Aufgaben nach heutigem Stand schwierige, algorithmische Gitterprobleme:

- Finde kurze Gittervektoren ungleich dem Nullvektor.
- Finde eine Basis bestehend aus kurzen Gittervektoren.
- Finde zu gegebenem $z \in \text{span}(b_1, \ldots, b_n)$ einen möglichst nahen Gittervektor.

Dagegen kann man in Polynomialzeit zu einem gegebenen Erzeugendensystem $b_1, \ldots, b_n \in \mathbb{Z}^m$ des Gitters L, $n \geq \text{Rang}(L)$, eine Gitterbasis konstruieren.

Algorithmenverzeichnis

Index

Literaturverzeichnis

[Babai86] L. Babai (1986): **On Lovász' Lattice Reduction and the nearest Lattice Point Problem**, Combinatorica, Band 6, Seiten 1–13.

[Barnes59] E.S. Barnes (1959): **The Contruction of perfect and extreme Forms II**, Acta Arithmetica, Band 5, Seiten 205-222.

[BaKa84] A. Bachem und R. Kannan (1984): **Lattices and the Basis Reduction Algorithm**, Technischer Report, Carnegie-Mellon-Universität (USA).

[BeWe93] Th. Becker und V. Weispfennig (1993): **Gröbner Bases — a computational Approach to commutative Algebra**, Graduate Texts in Mathematics, Band 141, Springer-Verlag, Berlin/Heidelberg.

[Blich14] H.F. Blichfeldt (1914): **A new Principle in the Geometry of Numbers with some Applications**, Transaction of the American Mathematical Society, Band 15, Seiten 227–235.

[Blich29] H.F. Blichfeldt (1929): **The Minimum Value of quadratic Forms and the closet Packing of Sphere**, Mathematische Annalen, Band 101, Seiten 366-389.

[Blich35] H.F. Blichfeldt (1935): **The minimum Value of positive Quadratic Forms in six, seven and eight Variables**, Mathematische Zeitschrift, Band 39, Seiten 1–15.

[Bb65] B. Buchenberger (1965): **Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal**, Dissertation, Fachbereich Mathematik, Universität Insbruck (Österreich).

[Cassels71] J.W.S. Cassels (1971): **An Introduction to the Geometry of Numbers**, Springer-Verlag, Berlin/Heidelberg.

[Cohen93] H. Cohen (1993): **A Course in Computational Algebraic Number Theory**, Graduate Texts in Mathematics, Band 138, Springer-Verlag, Berlin/Heidelberg.

[CoSl88] J.H. Conway und N.J. Sloane (1988): **Sphere Packings, Lattices and Groups**, Springer-Verlag, New York.

[CJLOSS92] M.J. Coster, A. Joux, B.A. LaMacchina, A.M. Odlyzko, C.P. Schnorr und J. Stern (1992): **An improved low-density Subset Sum Algorithm**, Computational Complexity, Band 2, Seiten 111–128.

[CR88] B. Chor und R.L. Rivest (1988): **A Knapsack type Public Key Cryptosystem based on Arithmetic in finite Fields**, IEEE Transaction Information Theory, Band IT-34, Seiten 901–909.

[Di1842] G.L. Dirichlet (1842): **Verallgemeinerung eines Satzes aus der Lehrere von Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen**, Bericht über die zur Bekanntmachung geeigneter Verhandlungen der Königlich Preussischen Akademie der Wissenschaften zu Berlin, Seiten 93–95.

[Dåmgard89] I.B. Dåmgard (1989): **A Design Principle for Hash Functions**, Advances in Cryptology — Proceedings EuroCrypt '89, Lecture Notes in Computer Science, Band 435 (1990), Springer-Verlag, Berlin/Heidelberg, Seiten 416–427.

[Dantzig63] G.B. Dantzig (1963): **Linear Programming and Extensions**, Princeton University Press, Princeton, New Jersey (dt. Übersetzung „Lineare Programmierung und Erweiterungen“ 1966 im Springer-Verlag, Berlin/Heidelberg, erschienen).

[DKT87] P.D. Domich, R. Kannan und L.E. Trotter (1987): **Hermite normal Form Computation using modulo Determinant Arithmetic**, Mathematics of Operation Research, Band 12, Nr. 1 (Februar), Seiten 50–59.

[EmBoas81] P. van Emde Boas (1981): **Another $\mathcal{NP}$-complete Partition Problem and the Complexity of Computing short Vectors in a Lattice**, Technischer Report 81-04, Fachbereich Mathematik der Universität Amsterdam.

[Euchner91] M. Euchner (1991): **Praktische Algorithmen zur Gitterreduktion und Faktorisierung**, Diplomarbeit, Fachbereich Informatik der Johann-Wolfgang-Goethe-Universität, Frankfurt/Main.

[Feller68] W. Feller (1968): **An Introduction to Probability Theory and its Application**, Band I, 3. Auflage, John Wiley & Sons, New York.

[Frieze86] A.M. Frieze (1986): **On the Lagarias-Odlyzko Algorithm for the Subset Sum Problem**, SIAM Journal on Computing, Band 15, Nr. 2, Seiten 536–539.

[GaSi78] J. von zur Gathen und M. Sieveking (1978): **A Bound on Solution of linear Integer Equations and Inequations**, Proceedings of the American Mathematical Society, Band 72, Seiten 155–158.

[GaJo79] M.R. Garey und D.S. Johnson (1979): **Computer and Intractability: A Guide to the Theory of $\mathcal{NP}$-Completness**, W.H. Freeman and Company, San Francisco.

[Gauß1801] C.F. Gauß (1801): **Disquisitiones Arithmeticae**, Gerhard Fleischer, Leipzig. Deutsche Übersetzung (1889): „Untersuchung über höhere Arithmetik“, Springer-Verlag, Berlin/Heidelberg.

[GrLek87] M. Gruber und C.G. Lekkerkerker (1987): **Geometry of Numbers**, 2. Auflage, North-Holland, Amsterdam.

[GLLS88] M. Grötschel, L. Lovász und A. Schrijver (1988): **Geometric Algorithms and combinatorial Optimization**, Algorithms and Combinatorics, Band 2, Springer-Verlag, Berlin/Heidelberg.

[HaMcC91] J. Hafner und K. McCurley (1991): **Asymptotic Fast Triangulation of Matrices over Ring**, SIAM Journal on Computing, Band 20, Nr. 6, Seiten 1068–1083.

[HJLS89] J. Håstad, B. Just, J.C. Lagarias und C.P. Schnorr (1989): **Polynomial Time Algorithms for Finding Integer Relations among real Numbers**, SIAM Journal on Computing, Band 18, Nr. 5, Seiten 859–881.

[Helfrich85] B. Helfrich (1985): **Algorithms to construct Minkowski reduced and Hermite reduced Lattice Bases**, Theoretical Computer Science, Band 41, Seiten 125–139.

[Hermite1850] C. Hermite (1850): **Extraits de lettres de M. Ch. Hermite à M. Jacobi sur differents objets de la théorie des nombres, Deuxième lettre**, Reine Angewandte Mathematik, Band 40, Seiten 279–290.

[Hlawka44] E. Hlawka (1944): **Zur Geometrie der Zahlen**, Mathematische Zeitschrift, Band 49, Seiten 285–312.

[Hörner94] H.H. Hörner (1994): **Verbesserte Gitterbasenreduktion; getestet am Chor-Rivest-Kryptosystem und an allgemeinen Rucksackproblemen**, Diplomarbeit, Fachbereich Mathematik der Johann-Wolfgang-Goethe-Universität, Frankfurt/Main.

[John48] F. John (1948): **Extremum Problems with Inequalities as subsidiary Conditions**, in K.O. Friedrichs, O.E. Neugebauer und J.J. Stoker (Ed.): „Studies and Essays presented to R. Courant on his 60th Birthday Januar 8, 1948“, Interscience Publisher, New York, Seiten 187–204.

[JoSt94] A. Joux und J. Stern (1994): **Lattice Reduction: A Toolbox for the Cryptanalyst**, Technischer Report, DGA/CELAR, Bruz (Frankreich). Eingereicht bei Journal of Cryptology.

[KaLe78] G.A. Kabatiansky und V.I. Levenshtein (1978): **Bounds for Packings on a Sphere and in Space**, Problems of Information Transmission, Band 14, Seiten 1–17.

[Kaib91] M. Kaib (1991): **The Gauß Lattice Basis Reduction succeeds with any Norm**, Proceedings of Fundamentals of Computation Theory (FCT '91), Springer Lecture Notes in Computer Science, Band 591, Seiten 275–286.

[Kaib94] M. Kaib (1994): **Gitterbasenreduktion für beliebige Normen**, Dissertation, Fachbereich Mathematik der Johann-Wolfgang-Goethe-Universität, Frankfurt/Main.

[KaSchn96] M. Kaib und C.P. Schnorr (1996): **The Generalized Gauss Reduction Algorithm**, Journal of Algorithms, Band 21, Nr. 3 (November), Seiten 565–578.

[KaBa79] R. Kannan und A. Bachem (1979): **Polynomial Algorithm for Computing the Smith and the Hermite Normal Form of an Integer Matrix**, SIAM Journal on Computing, Band 8, Seiten 499–507.

[Kannan87] R. Kannan (1987): **Minkowski's Convex Body Theorem and Integer Programming**, Mathematics of Operation Research, Band 12, Nr. 3 (August), Seiten 415–440.

[Karma84] M. Karmarkar (1984): **A new Polynomial-Time Algorithm for Linear Programming**, Combinatorica, Band 4, Seiten 373–395.

[Khach79] L.G. Khachiyan (1979): **A Polynomial Algorithm in Linear Programming**, Soviet Mathmatics Doklady, Band 20, Seiten 191–194.

[Khach80] L.G. Khachiyan (1980): **Polynomial Algorithms in Linear Programming**, U.S.S.R. Computational Mathematics and Mathematical Physics, Band 20, Seiten 53–72.

[KoZo1872] A. Korkine und G. Zolotareff (1872): **Sur les formes quadratique positive quaternaires**, Mathematische Annalen, Band 5, Seiten 366-389.

[KoZo1873] A. Korkine und G. Zolotareff (1873): **Sur les formes quadratique**, Mathematische Annalen, Band 6, Seiten 366–389.

[KoZo1877] A. Korkine und G. Zolotareff (1877): **Sur les formes quadratique positive**, Mathematische Annalen, Band 11, Seiten 242–292.

[Knuth71] D.E. Knuth (1971): **The Art of Computer Programming**, Fundamental Algorithms, Band I, Addison-Wesley, Reading.

[LARIFARI] M. Kaib, R. Mirwald, C. Rössner, H.H. Hörner, H. Ritter (1994): **Programmieranleitung für LARIFARI — Version 13.07.1994**, Fachbereiche Mathematik und Informatik der Johann-Wolfgang-Goethe-Universität, Frankfurt/Main.

[La1773] J.L. Lagrange (1773): **Recherches d'arithmétique**, Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres, Berlin, Seiten 265–312.

[Lang93] S. Lang (1993): **Algebra**, 3. Auflage, Addison-Wesley, Reading.

[LLS90] J.C. Lagarias, H.W. Lenstra und C.P. Schnorr (1990): **Korkin-Zolotarev Bases and successive Minima of a Lattice and its reciprocal lattice**, Combinatorica, Band 10, Seiten 333–348.

[LaOd85] J.C. Lagarias und A.M. Odlyzko (1985): **Solving low-density Subset Sum Problems**, Journal of ACM, Band 32, Nr. 1, Seiten 229–246.

[LLL82] A.K. Lenstra, H.W. Lenstra und L. Lovász (1982): **Factoring Polynomials with Rational Coefficients**, Springer Mathematische Annalen, Band 261, Seiten 515–534.

[Lenstra83] H.W. Lenstra (1983): **Integer Programming in a fixed Number of Variables**, Mathematics of Operation Research, Band 8, Nr. 4 (November), Seiten 538–548

[Lováz86] L. Lovász (1986): **An algorithmic Theory of Numbers, Graphs and Convexity**, CBMS-NSF Regional Conference Series in Applied Mathematics, Band 50, SIAM Publications, Philadelphia.

[LoSc92] L. Lovász und H. Scarf (1992): **The Generalized Basis Reduction Algorithm**, Mathematics of Operation Research, Band 17, Nr. 3 (August), Seiten 751–764.

[MaOd90] J.E. Mazo und A.M. Odlyzko (1990): **Lattice Points in high-dimensional Sphere**, Monatsheft Mathematik, Band 110, Seiten 47–61.

[Mink1896] H. Minkowski (1896): **Geometrie der Zahlen**, erste Auflage, Teubner-Verlag, Leipzig.

[Mink1911] H. Minkowski (1911): **Gesammelte Abhandlungen**, Band I und II, Teubner-Verlag, Leipzig.

[Mishra93] B. Mishra (1993): **Algorithmic Algebra**, Texts and Monographs in Computer Science, Springer-Verlag, New-York.

[Orton1994] G. Orton (1994): **A multiple-iterated Trapdoor for dense compact Knapsacks**, Advances in Cryptology — Proceedings EuroCrypt '94, Lecture Notes in Computer Science, Band 950 (1995), Springer-Verlag, Berlin/Heidelberg, Seiten 112–130.

[PaSchn87] A. Paz und C.P. Schnorr (1987): **Approximating Integer Lattices by Lattices with cyclic Factor Group**, 14.th International Colloquium on Automata, Languages and Programming (ICALP), Lecture Notes in Computer Science, Band 267, Springer-Verlag, Berlin/Heidelberg, Seiten 386–393.

[Rieger78] G.J. Rieger (1978): **über die mittlere Schrittzahl bei Divisionsalgorithmen**, Mathematische Nachrichten, Band 82, Seiten 157–180.

[Ritter96] H. Ritter (1996): **Breaking Knapsack Cryptosystems by ℓ_∞-norm Enumeration**, Proceedings of the 1.st International Conference on the Theory and Applications of Cryptography — PragoCrypt '96, CTU Publishing House, Prag, Seiten 480–492.

[Ritter97] H. Ritter (1997): **Aufzählung kurzer Gittervektoren in allgemeiner Norm**, Dissertation, Fachbereich Mathematik der Johann-Wolfgang-Goethe-Universität, Frankfurt/Main.

[Rogers64] C.A. Rogers (1964): **Packing and Covering**, Cambridge University Press, Cambridge.

[Schnorr87] C.P. Schnorr (1987): **A Hierarchy of polynomial time Lattice Basis Reduction Algorithms**, Theoretical Computer Science, Band 53, Seiten 201–224.

[Schnorr88] C.P. Schnorr (1988): **A more efficient Algorithm for Lattice Basis Reduction**, Journal of Algorithms, Band 9, Seiten 47–62.

[Schnorr91a] C.P. Schnorr (1991): **Gittertheorie und ganzzahlige Optimierung**, Skript zur Vorlesung, Johann-Wolfgang-Goethe-Universität, Frankfurt/Main.

[Schnorr91b] C.P. Schnorr (1991): **Factoring Integers and Computing Discrete Logarithms via Diophantine Approximation**, Advances in Cryptology – Proceedings EuroCrypt '91, Lecture Notes in Computer Science, Band 547, Springer-Verlag, Berlin/Heidelberg, Seiten 171–181.

[SchnEu91] C.P. Schnorr und M. Euchner (1991): **Lattice Basis Reduction: improved Algorithms and solving Subset Sum Problems**, Proceedings of Fundamentals of Computation Theory (FCT '91), Lecture Notes in Computer Science, Band 591, Springer-Verlag, Berlin/Heidelberg, Seiten 68–85.

[Schnorr93] C.P. Schnorr (1993): **Factoring Integers and Computing Discrete Logarithms via Diophantine Approximation**, Advances in Computational Complexity, Ed. Jim-Yi Cai, AMS DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Band 13, Seiten 171–182.

[Schnorr94a] C.P. Schnorr (1994): **Block Reduced Lattice Bases and Successive Minima**, Combinatorics, Probability and Computing, Band 3, Seiten 507–522.

[Schnorr94b] C.P. Schnorr (1994): **Gittertheorie und Kryptographie**, Ausarbeitung, Johann-Wolfgang-Goethe-Universität, Frankfurt/Main.

[SchnHö95] C.P. Schnorr und H.H. Hörner (1995): **Attacking the Chor-Rivest Cryptosystem by improved Lattice Reduction**, Advances in Cryptology — Proceedings EuroCrypt '95, Lecture Notes in Computer Science, Band 921, Springer-Verlag, Berlin/Heidelberg, Seiten 1–12.

[Schrijver86] A. Schrijver (1986): **Theory of Linear and Integer Programming**, Wiley-Interscience Series in discrete Mathematics and Optimization, John Wiley & Son Ltd.

[Seysen93] M. Seysen (1993): **Simultaneous Reduction of a Lattice and its reciprocal Basis**, Combinatorica, Band 13, Seiten 363–376.

[Siegel89] C.L. Siegel (1989): **Lectures on the Geometry of Numbers**, Springer-Verlag, Berlin/Heidelberg.

[Smith1861] H.J.S. Smith (1861): **On Systems of linear indeterminate Equations and Congruences**, Philosophical Transaction of the Royal Society of London, Band 151, Seiten 293–326.

[SpStr76] E. Specker und V. Strassen (1976): **Komplexität von Entscheidungsproblemem**, Lecture Notes in Computer Science, Band 43, Springer-Verlag, Berlin/Heidelberg.

[Vetchin82] N.M. Vetchinkin (1982): **Uniqueness of Classes of positive quadratic Forms on which Values of the Hermite Constants are attained for** $6 \leq n \leq 8$, Proceedings of the Steklov Institute of Mathematics, Nr. 3, Seiten 37–95.

[Watson66] G.L. Watson (1966): **On the Minimum of a positiv Quadratic Form in** n **(**$n \leq 8$**) Variables (Verification of Blichfeldt's Calculations)**, Proceeedings of the Cambrigde Philosophical Society (Mathematical and Physical Science), Band 62, Seite 719.

[Ye91] Y. Ye (1991): **Potential Reduction Algorithm for Linear Programming**, Mathematical Programming, Band 51, Seiten 239–258.