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

Gitter und Kryptographie

an der Johann Wolfgang Goethe-Universität Frankfurt/Main
im Sommersemester 2014

β_5-Version

12. April 2016

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 $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{R}^{m \times n}$ die Matrix mit Spaltenvektoren $\mathbf{b}_1, \ldots, \mathbf{b}_n$. Dann bezeichnet

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

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 $\mathcal{L}(\mathbf{B})$ ein *Gitter* mit *Basis* $\mathbf{b}_1, ..., \mathbf{b}_n$ bzw. $\mathbf{B}$ und *Dimension* oder *Rang* $\dim(\mathcal{L}) =_{\text{def}} \text{rang}(\mathbf{B})$. Der vom Gitter $\mathcal{L} = \mathcal{L}(\mathbf{B})$ aufgespannte lineare Raum ist $\text{span}(\mathcal{L}) =_{\text{def}} \{\mathbf{Bz} | \mathbf{z} \in \mathbb{R}^n\} = \sum_{i=1}^{n} \mathbf{b}_i \mathbb{R}$. Alle Basen $\mathbf{B}$ 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 $\mathbf{U} \in GL_n(\mathbb{Z})$ heißen *unimodular*. Die Basen $\bar{\mathbf{B}}$ eines Gitters sind die transformierten einer beliebigen Basis $\mathbf{B} \in \mathbb{R}^{m \times n}$, transformiert durch unimodulare Matrizen.

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

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

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

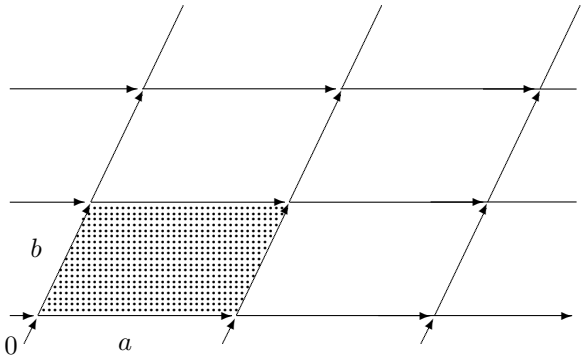

Abbildung 1.1.1: Grundmasche des Gitters mit Basis $\mathbf{a}, \mathbf{b} \in \mathbb{R}^2$

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

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

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 $\mathbf{b} + \mathcal{P}$ mit $\mathbf{b} \in \mathcal{L}$ und es gilt $\mathrm{span}(\mathcal{L}) = \bigcup_{\mathbf{b}\in\mathcal{L}} \mathbf{b} + \mathcal{P} = \mathcal{P} + \mathcal{L}$. Die *Gram-Matrix* zur Basis $\mathbf{B}$ ist die $n \times n$-Matrix $\mathbf{B}^t\mathbf{B} = [\langle \mathbf{b}_i, \mathbf{b}_j \rangle]_{1\leq i,j\leq n}$ bestehend aus den Skalarprodukten der Basisvektoren.

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

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

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

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

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

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

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

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

Da $\mathbf{b} + \mathcal{P}(\mathbf{B})$ nur den Gitterpunkt $\mathbf{b}$ enthält, gibt es pro $\det \mathcal{L}$ Volumeneinheiten genau einen Gitterpunkt. Diejenigen Gitterpunkte $\mathbf{b}$, deren Maschen $\mathbf{b} + \mathcal{P}(\mathbf{B})$ die Kugel $\mathcal{B}_n(\mathbf{0}, r)$ echt schneiden, können entweder in $\mathcal{L} \cap \mathcal{B}_n(\mathbf{0}, r)$ oder im Komplement liegen. Dies führt in der Gleichung $|\,\mathcal{L} \cap \mathcal{B}_n(\mathbf{0}, r)\,| / \mathrm{vol}\,\mathcal{B}_n(\mathbf{0}, r) = 1/\det \mathcal{L}(\mathbf{B}) + O(\frac{n}{r})$ zu einem Fehler $O(\frac{n}{r})$, der proportional zum Verhältnis Oberfläche zu Volumen von $\mathcal{B}_n(\mathbf{0}, r)$ 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 $\triangle(\mathcal{L}) = (\lambda_1/2)^n V_n / \det \mathcal{L}$, dabei ist $V_n = \operatorname{vol} \mathcal{B}_n(\mathbf{0}, 1)$ das Volumen der n-dim. Einheitskugel: $V_n = \pi^{n/2}/(n/2)! \approx \left(\frac{2\,e\,\pi}{n}\right)^{n/2}/\sqrt{\pi n}$ und $(n/2)! = \Gamma(1 + n/2)$ für die Gammafunktion Γ. Das Gitter

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

für $n = 1, 2, ...$ hat die Basis

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

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

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

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

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

Das folgende Gitter $\mathbb{E}_n$ ist für $n = 0 \bmod 4$ Untergitter von $\mathbb{D}_n$:

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

Es hat die Basen

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

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

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 $\mathbf{Q} \in \mathbb{R}^{m\times n}$, $m \ge n$, heißt *isometrisch*, bzw.*Isometrie*, wenn die Abbildung $\mathbf{x} \mapsto \mathbf{Q}\mathbf{x}$ isometrisch ist. Damit ist $\mathbf{Q} \in \mathbb{R}^{m\times n}$ genau dann isometrisch, wenn $\mathbf{Q}^t\mathbf{Q} = I_n$ die Einheitsmatrix $I_n \in \mathbb{R}^{n\times n}$ ist. Das Produkt von isometrischen Matrizen ist isometrisch. Eine isometrische Quadratmatrix $\mathbf{Q} \in \mathbb{R}^{n\times n}$ bezeichnet man als *orthogonale Matrix*. $\mathbf{Q}$ ist orthogonal genau dann, wenn $\mathbf{Q}^{-1} = \mathbf{Q}^t$. Mit $\mathbf{Q}$ ist auch $\mathbf{Q}^t$

orthogonal. Damit ist $\mathbf{Q} \in \mathbb{R}^{m\times n}$ genau dann isometrisch, wenn $\mathbf{Q}$ 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 $\operatorname{span}(\mathcal{L})$ gibt mit $T(\mathcal{L}) = \bar{\mathcal{L}}$. Zwei Basen $\mathbf{B}, \bar{\mathbf{B}}$ heißen *isometrisch*, wenn es eine isometrische Matrix $\mathbf{Q}$ gibt mit $\bar{\mathbf{B}} = \mathbf{QB}$. Offenbar sind $\bar{\mathbf{B}}, \mathbf{B}$ genau dann isometrisch, wenn $\mathbf{B}^t\mathbf{B} = \bar{\mathbf{B}}^t\bar{\mathbf{B}}$. Isometrische Basen $\mathbf{B}, \bar{\mathbf{B}}$ erzeugen isometrische Gitter $\mathcal{L}(\mathbf{B}), \mathcal{L}(\bar{\mathbf{B}})$. 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. Es gilt $\mathbb{D}_3 \cong \mathbb{A}_3$. Folgende Basen sind isometrisch:

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

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 $\pi_i : \mathbb{R}^m \to \operatorname{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^\perp$ die orthogonale Projektion, derart dass für alle $\mathbf{b} \in \mathbb{R}^m$

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

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

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

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

$$[\mathbf{b}_1, \ldots, \mathbf{b}_n] = [\, \widehat{\mathbf{b}}_1, \ldots, \widehat{\mathbf{b}}_n\,] \, [\mu_{i,j}]_{1\le i,j\le n}^t.$$

***QR*-Zerlegung und geometrische Normalform (GNF).** Die QR-Zerlegung $\mathbf{B} = \mathbf{QR}$ der Basis $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{R}^{m\times n}$ ist die eindeutige Zerlegung $\mathbf{B} = \mathbf{QR}$, so dass $\mathbf{Q} \in \mathbb{R}^{m\times n}$ isometrisch ist und $\mathbf{R} \in \mathbb{R}^{n\times n}$ obere Dreiecksmatrix mit positiven Diagonalelementen. Wir nennen $\mathbf{R}$ die *geometrische Normalform* (GNF) der Basis, Bez.: $\mathbf{R} = GNF(\mathbf{B})$. Es gilt $\mathbf{Q} := [\widehat{\mathbf{b}}_1/\|\widehat{\mathbf{b}}_1\|, ..., \widehat{\mathbf{b}}_n/\|\widehat{\mathbf{b}}_n\|] \in \mathbb{R}^{m\times n}$ und für $\mathbf{R} = [r_{i,j}]_{1\le i,j\le n}$ gilt $r_{i,i} = \|\widehat{\mathbf{b}}_i\|$, $\mu_{j,i} = r_{i,j}/r_{i,i}$,

$$\mathbf{R} := \begin{bmatrix} \|\widehat{\mathbf{b}}_1\| & 0 & \cdots & \cdots & 0 \\ 0 & \|\widehat{\mathbf{b}}_2\| & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \|\widehat{\mathbf{b}}_{n-1}\| & 0 \\ 0 & \cdots & \cdots & 0 & \|\widehat{\mathbf{b}}_n\| \end{bmatrix} \cdot \begin{bmatrix} 1 & \mu_{2,1} & \mu_{3,1} & \cdots & \mu_{n,1} \\ 0 & 1 & \mu_{3,2} & & \mu_{n,2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & \mu_{n,n-1} \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}.$$

Lemma 1.1.3

1. *Zwei Basen* $\mathbf{B}$, $\bar{\mathbf{B}}$ *sind genau dann isometrisch, wenn* $GNF(\mathbf{B}) = GNF(\bar{\mathbf{B}})$*, und damit wenn* $\mathbf{B}^t\mathbf{B} = \bar{\mathbf{B}}^t\bar{\mathbf{B}}$*. Die Basen* $\mathbf{B}$ *einer Isomorphieklasse haben dieselbe GNF* $GNF(\mathbf{B})$*. bestimmt.*
2. $\mathcal{L}(\mathbf{B})$ *ist isometrisch zum vollständigen Gitter* $\mathcal{L}(\mathbf{R})$ *mit* $\mathbf{R} = GNF(\mathbf{B})$*.*

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

Für beliebige Basen $\mathbf{B} = \mathbf{Q}\mathbf{R}$ gilt $\det(\mathbf{B}^t\mathbf{B}) = \det(\mathbf{R}^t\mathbf{R}) = \prod_{i=1}^n \|\widehat{\mathbf{b}}_i\|^2$. Insbesondere bleibt $\det\mathcal{L}(\mathbf{B}) = (\det\mathbf{B}^t\mathbf{B})^{\frac{1}{2}}$, 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 1.3.2 zu einer Basis von $\mathbb{Z}^n$ ergänzbar. Es gibt ein $\mathbf{b}_1 \in \mathbb{Z}^n$ 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 $\mathcal{P}(\mathbf{B})$ 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 $(\mathbf{A}^{-1})^t = (\mathbf{A}^t)^{-1}$ für $\mathbf{A} \in \mathbb{R}^{n\times n}$, kürzen wir ab $\mathbf{A}^{-t} := (\mathbf{A}^{-1})^t$. Es gilt $(\mathbf{A}\mathbf{B})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1}$, $(\mathbf{A}\mathbf{B})^t = \mathbf{B}^t\mathbf{A}^t$ und somit $(\mathbf{A}\mathbf{B})^{-t} = \mathbf{A}^{-t}\mathbf{B}^{-t}$.

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

Die Basis $\mathbf{B}$ ist genau dann invertierbar, wenn $\mathcal{L}(\mathbf{B})$ vollständig ist. Für invertierbare $\mathbf{B}$ gilt offenbar $\mathcal{L}(\mathbf{B})^* = \mathcal{L}(\mathbf{B}^{-t})$ und ferner $(\mathbf{B}^t\mathbf{B})^{-1} = \mathbf{B}^{-1}\mathbf{B}^{-t}$.

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

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

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

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

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 $\mathbf{B} = \mathbf{QR}$ liefert die duale Basis $\mathbf{B}^* = \mathbf{Q}\,\mathbf{R}^{-t}\mathbf{U}_n$. Die Umkehrmatrix $\mathbf{U}_n =_{\text{def}} \begin{bmatrix} & & 1 \\ & \cdot & \\ 1 & & \end{bmatrix} \in \mathbb{R}^{n\times n}$, ist die Matrix mit Einsen in der Gegendiagonalen.

Die QR-Zerlegung der dualen Basis $\mathbf{B}^*$ zu $\mathbf{B} = \mathbf{QR}$ ist $\mathbf{B}^* = (\mathbf{QU}_n)\,(\mathbf{U}_n\mathbf{R}^{-t}\mathbf{U}_n)$.
Denn zur QR-Zerlegung $\mathbf{B} = \mathbf{QR}$ ist $\mathbf{R}^{-t}$ untere Dreiecksmatrix und $\mathbf{U}_n\mathbf{R}^{-t}\mathbf{U}_n$ obere Dreiecksmatrix. Der Übergang von $\mathbf{R}^{-t}$ nach $\mathbf{U}_n\mathbf{R}^{-t}\mathbf{U}_n$ invertiert die Spalten- und die Zeilenreihenfolge in $\mathbf{R}^{-t}$. Wegen $\mathbf{U}_n^t = \mathbf{U}_n = \mathbf{U}_n^{-1}$ ist $\mathbf{QU}_n$ 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 $\langle \widehat{\mathbf{b}}_i, \widehat{\mathbf{b}}_j \rangle \, \|\widehat{\mathbf{b}}_j\|^2 = \delta_{i,j}$ 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 $\mathcal{L} = \mathcal{L}(\mathbf{B})$ mit QR-Zerlegung $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m\times n}$ und sei $T : \mathbf{x} \mapsto \bar{\mathbf{Q}}\mathbf{x}$ eine Isometrie. Weil $\mathbf{QR}^{-t}$ Basis von $\mathcal{L}^*$ ist, gilt nach Satz 1.2.1

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

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

Selbstduale und ganze Gitter. Ein Gitter $\mathcal{L}$ heißt *selbstdual* oder *unimodular*, wenn $\mathcal{L} = \mathcal{L}^*$. Offenbar gilt $\mathcal{L} = \mathcal{L}^*$ gdw die Gram-Matrix $\mathbf{B}^t\mathbf{B}$ unimodular ist, d.h., $\mathbf{B}^t\mathbf{B}$ ist ganzzahlig und $\det \mathbf{B}^t\mathbf{B} = 1$. Die Gitter $\mathbb{Z}^n$ und die geschichteten Gitter $\Lambda_8 \cong \mathbb{E}_8, \sqrt{2}\Lambda_{24}$ sind selbstdual.

Ein Gitter $\mathcal{L}$ heißt *ganz* (*integral*), wenn $\mathbf{B}^t\mathbf{B}$ ganzzahlig ist. Ein Gitter $\mathcal{L}$ ist also genau dann ganz, wenn $\mathcal{L} \subset \mathcal{L}^*$.

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 Häufungspunkt 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 $\mathcal{L}(\mathbf{b}_1) = \mathcal{L} \cap \mathrm{span}\,(\mathbf{b}_1)$. Betrachte die orthogonale Projektion $\pi : \mathbb{R}^m \to \mathrm{span}\,(\mathbf{b}_1)^\perp$ 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 $\bar{\mathbf{y}}^{(i)} := \mathbf{y}^{(i)} - \left\lceil \langle \mathbf{y}^{(i)}, \mathbf{b}_1 \rangle \,/\, \langle \mathbf{b}_1, \mathbf{b}_1 \rangle \right\rfloor \mathbf{b}_1$. Dabei bezeichnet $\lceil r \rfloor := \lceil r - \frac{1}{2} \rfloor$ 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 $\lim\limits_{i \to \infty} \|\pi(\bar{\mathbf{y}}^{(i)})\| = 0$ 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 $\mathbf{b} - \bar{\mathbf{b}} \in \mathrm{span}\,(\mathbf{b}_1)$. Nach Wahl von $\mathbf{b}_1$ gilt $\mathcal{L}(\mathbf{b}_1) = \mathcal{L} \cap \mathrm{span}\,(\mathbf{b}_1)$ 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. $\mathrm{span}\,(\mathbf{b}_1, \ldots, \mathbf{b}_k) \cap \mathcal{L} = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_k)$.

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 $k \in \mathbb{Z} \setminus \{\mathbf{0}\}$.

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 $\pi : \mathrm{span}\,(\mathcal{L}) \to \mathrm{span}\,(\mathbf{b}_1, \ldots, \mathbf{b}_k)^\perp$ 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 $\mathbf{b}_1, ..., \mathbf{b}_n$ 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 $\mathbf{b} - \bar{\mathbf{b}} \in \mathrm{span}\,(\mathbf{b}_1, \ldots, \mathbf{b}_k)$. 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 zur ℓ_2-Norm $||\ ||$

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 $|\mu_{i,j}| \leq \frac{1}{2}$

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

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

Definition 1.4.2
Die Vektoren $\mathbf{b}_1, \ldots, \mathbf{b}_{\bar{n}} \in \mathbb{R}^n \setminus \{\mathbf{0}\}$ *nennen wir* paarweise reduziert, *wenn*

1. $\frac{|\langle \mathbf{b}_i, \mathbf{b}_j \rangle|}{\|\mathbf{b}_j\|^2} \leq \frac{1}{2}$ *für* $1 \leq j < i \leq \bar{n}$, **2.** $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \cdots \leq \|\mathbf{b}_{\bar{n}}\|$.

Die Eigenschaft 1. bezieht sich *nicht* auf den Gram-Schmidt-Koeffizienten $\mu_{i,j} = \frac{\langle \mathbf{b}_i, \widehat{\mathbf{b}}_j \rangle}{\|\widehat{\mathbf{b}}_j\|^2}$. Sie ist äquivalent zu $\|\mathbf{b}_i\| \leq \|\mathbf{b}_i \pm \mathbf{b}_j\|$ für $1 \leq j < i \leq \bar{n}$, 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: Vektoren $\mathbf{b}_1, \ldots, \mathbf{b}_{\bar{n}} \in \mathbb{Z}^m$ (möglicherweise linear abhängig)

1. Ordne $\mathbf{b}_1, \ldots, \mathbf{b}_{\bar{n}}$ so, dass $1 \leq \|\mathbf{b}_1\| \leq \cdots \leq \|\mathbf{b}_{\bar{n}}\|$

2. `FOR` $i = 1, \ldots, \bar{n}$ 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` $\mathbf{b}_i := \mathbf{b}_i - \lceil r \rfloor \mathbf{b}_j$

`IF` $\mathbf{b}_i = \mathbf{0}$ `THEN` [entferne $\mathbf{b}_i$, $\bar{n} := \bar{n} - 1$, `GO TO` **1.**]

AUSGABE: paarweise reduzierte Vektoren $\mathbf{b}_1, \ldots, \mathbf{b}_{\bar{n}}$ $(\sum_{i=1}^{\bar{n}} \mathbf{b}_i \mathbb{Z}$ bleibt erhalten)

Korrektheit. Algorithmus 1.4.2 terminiert und bei Abbruch des Verfahrens sind die Vektoren paarweise reduziert. Bei jedem Reduktionsschritt wird nämlich der Vektor $\mathbf{b}_i$ echt kleiner, und die übrigen Vektoren bleiben unverändert. Somit hat jedes Gitter eine paarweise reduzierte Basis.

Die Laufzeit der paarweisen Reduktion ist nicht polynomial. Aber es gibt höchstens polynomial viele Schritte $\mathbf{b}_i := \mathbf{b}_i - \lceil r \rfloor \mathbf{b}_j$, welche $\|\mathbf{b}_i\|$ um mindestens $\varepsilon\|\mathbf{b}_i\|$ für festes $\varepsilon > 0$ erniedrigen.

Satz 1.4.3
Algorithmus 1.4.2 sichert nach höchstens $\log_{1/(1-\varepsilon)}(\prod_{i=1}^{\bar{n}} \|\mathbf{b}_i\|) \leq n \log_{1/(1-\varepsilon)} M$ *Schritten* $\mathbf{b}_i := \mathbf{b}_i - \lceil r \rfloor \mathbf{b}_j$ *mit* $\|\mathbf{b}_i\|_{\text{neu}} \leq \|\mathbf{b}_i\|(1-\varepsilon)$ *dass* $\|\mathbf{b}_i\|(1-\varepsilon) \leq \|\mathbf{b}_i \pm \mathbf{b}_j\|$ *für* $1 \leq j < i \leq \bar{n}$.

1.5 Hermite Normalform, Untergitter

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 $\mathbf{T} \in \mathbb{Z}^{n\times n}$ kann man $\det \mathcal{L}(\mathbf{B}) / \det \mathcal{L}(\mathbf{BT}) = |\det \mathbf{T}|$ ablesen.

Definition 1.5.1
Eine Matrix $\mathbf{A} = [a_{ij}] \in \mathbb{R}^{m\times n}$ *mit* $n \leq m$ *ist in* Hermite-Normalform *(kurz HNF), wenn*

1. $a_{ij} = 0$ *für* $j > i$, *d.h.* $\mathbf{A}$ *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 $\mathbf{A} = [a_{ij}] = [\mathbf{a}_1, ..., \mathbf{a}_n]$ 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 [PS87] 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 [He1850] gilt folgender Satz.

Satz 1.5.2 (Hermite 1850)
Zu jeder Matrix $\mathbf{A} \in \mathbb{Q}^{m\times n}$ *mit* $\text{Rang}(A) = n$ *gibt es genau eine HNF* $\mathbf{A}\,\mathbf{U}$ *mit* $\mathbf{U} \in GL_n(\mathbb{Z})$.

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

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

Weil $\mathbf{A}$ 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 $\mathcal{L}(\mathbf{A})$. $\mathbf{a}' := [\mathbf{a}'_1, ..., \mathbf{a}'_n]$ 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

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

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

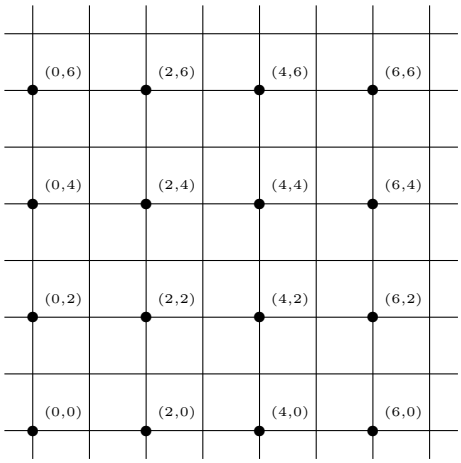

Abbildung 1.5.1: Untergitter $\mathcal{L}(\mathbf{A})$ von $\mathbb{Z}^2$

Lemma 1.5.3
Sei $\mathcal{L} = \mathcal{L}(\mathbf{B})$ Gitter und $\mathcal{L}' = \mathcal{L}(\mathbf{BT})$ Untergitter von $\mathcal{L}$ mit $\mathbf{T} \in \mathbb{Z}^{n\times n}$. Dann gilt
$\det \mathcal{L}' = \det \mathcal{L} \cdot |\det \mathbf{T}|$.

Index des Untergitters. Die ganze Zahl $|\det \mathbf{T}| = \frac{\det \mathcal{L}'}{\det \mathcal{L}}$ aus Lemma 1.5.3 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 $\mathcal{L}' = \mathcal{L}(\mathbf{BT})$ Untergitter von $\mathcal{L} = \mathcal{L}(\mathbf{B})$ und $\mathbf{T} = [t_{ij}] \in \mathbb{Z}^{n\times n}$ eine obere (bzw. untere) Dreiecksmatrix. Dann gilt

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

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

Korollar 1.5.4
Zu $\mathbf{a} = (a_1, \ldots, a_n)^t \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$, $b \in \mathbb{N}$ *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 1.5.5
Sei $\mathcal{L}'$ *ein Untergitter von* $\mathcal{L} = \mathcal{L}(\mathbf{B})$. *Dann gibt es eine untere (bzw. obere) Dreiecksmatrix* $\mathbf{T} \in \mathbb{Z}^{n\times n}$ *mit* $\mathcal{L}' = \mathcal{L}(\mathbf{BT})$. *Umgekehrt gibt es zu jeder Basis* $\mathbf{B}'$ *von* $\mathcal{L}'$ *eine Basis* $\bar{\mathbf{B}}$ *von* $\mathcal{L}$ *und eine untere (bzw. obere) Dreiecksmatrix* $\mathbf{T} \in \mathbb{Z}^{n\times n}$ *mit* $\mathbf{B}' = \bar{\mathbf{B}}\,\mathbf{T}$.

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

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

Kapitel 2

Minkowski-Sätze, Hermite-Konstante

Die sukzessiven Minima $\lambda_1 \leq ... \leq \lambda_n$ eines Gitters der Dimension n sind wichtige geometrische Invarianten. Eine Gitterbasis $\mathbf{b}_1, ..., \mathbf{b}_n$ gilt als "stark reduziert", wenn $\|\mathbf{b}_i\|$ nicht viel grösser ist als $\lambda_i\sqrt{i}$. Für Gitter $\mathcal{L}$ der Dimension n gilt $\lambda_1^2 \leq \gamma_n \det(\mathcal{L})^{2/n}$, dabei ist γ_n die Hermite-Konstante.

2.1 Sukzessive Minima und erster Satz von Minkowski

Sukzessive Minima. Eine allgemeine Norm $\|\cdot\| : \mathbb{R}^m \to \mathbb{R}_{\geq 0}$ ist durch ihren *Eichkörper* $K = \{\mathbf{x} \in \mathbb{R}^m \mid \|\mathbf{x}\| \leq 1\}$ definiert. $K \subset \mathbb{R}^m$ ist eine beliebige kompakte, konvexe, nullsymmetrische Menge. Es gilt $\|\mathbf{x}\| = \min\{r \in \mathbb{R}_{\geq 0} \mid \mathbf{x} \in rK\}$. Der Eichkörper der ℓ_2-Norm ist die Einheitskugel $\mathcal{B}_m(\mathbf{0}, 1)$ der Dimension m, der Eichkörper der sup-Norm $\ell_\infty = \| \ |_\infty$ ist der Würfel mit Seitenlängen 2.

Die sukzessiven Minima $\lambda_1, \ldots, \lambda_n$ des Gitters $\mathcal{L} \subset \mathbb{R}^m$ der $\dim \mathcal{L} = n$ zur Norm $\|\cdot\|$ sind

$$\lambda_i = \lambda_i(\mathcal{L}) := \inf\left\{ r > 0 \;\middle|\; \begin{array}{l} \exists \text{ linear unabhängige } \mathbf{a}_1, \ldots, \mathbf{a}_i \in \mathcal{L} \\ \text{mit } \|\mathbf{a}_1\|, ..., \|\mathbf{a}_i\| \leq r. \end{array} \right\}.$$

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 $\|\mathbf{x}\|_\infty \leq \|\mathbf{x}\| \leq \sqrt{m}\, \|\mathbf{x}\|_\infty$.

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 $i = 1, \ldots, n$. Für das Gitter $\mathcal{L} := \mathbb{Z}^n + \mathbb{Z}\,(\frac{1}{2}, \ldots, \frac{1}{2})^t$ gilt offenbar $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 1$ für $n \geq 4$. Für $n \geq 5$ gibt es aber keine Basis bestehend aus Vektoren der Länge 1.

Lemma 2.1.1 (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 $\left(1 + \frac{1}{i}\right) S + \mathbf{b}$ mit $\mathbf{b} \in \mathcal{L}$ nicht paarweise disjunkt, weil das Volumen von $\left(1 + \frac{1}{i}\right) S$ das der Grundmasche übersteigt. Zu jedem i gibt es ein $\mathbf{b}_i \in \mathcal{L} \setminus \{\mathbf{0}\}$, so dass der folgende Durchschnitt nicht leer ist und somit ein $\mathbf{y}_i$ enthält:

$$\mathbf{y}_i \in \left(1+\tfrac{1}{i}\right) S \cap \left[\left(1+\tfrac{1}{i}\right) S + \mathbf{b}_i\right]$$

Da S kompakt ist, hat die Folge $(\mathbf{y}_i)_{i\in\mathbb{N}}$ einen Häufungspunkt $\mathbf{y} \in S$. Für jede Teilfolge $\left(\mathbf{y}_{\alpha(i)}\right)_{i\in\mathbb{N}}$ die gegen $\mathbf{y}$ konvergiert ist die Folge $\left(\mathbf{b}_{\alpha(i)}\right)_{i\in\mathbb{N}} \subset \mathcal{L}$ beschränkt und hat einen Häufungspunkt $\mathbf{b} \in \mathcal{L} \setminus \{\mathbf{0}\}$. Es folgt: $\mathbf{y} \in S \cap (S+\mathbf{b})$. □

Satz 2.1.2 (Minkowski's Convex Body Theorem)
Sei $\mathcal{L} \subset \mathbb{R}^n$ Gitter der $\dim \mathcal{L} = n$ und $S \subset \operatorname{span}(\mathcal{L})$ konvex, kompakt und nullsymmetrisch. Wenn $\operatorname{vol}(S) \geq 2^n \det(\mathcal{L})$ dann gilt $|S \cap \mathcal{L}| \geq 3$.

Beweis. Für $S' := \frac{1}{2}S$ gilt $\operatorname{vol}(S') = 2^{-n} \operatorname{vol}(S) \geq \det \mathcal{L}$. Nach Lemma 2.1.1 gibt es $\mathbf{x}, \mathbf{y} \in S'$, $\mathbf{x} \neq \mathbf{y}$ so dass $\mathbf{x}-\mathbf{y} \in \mathcal{L}$. Somit gilt $2\mathbf{x}, 2\mathbf{y} \in S$ und $-2\mathbf{x} \in S$ weil S nullsymmetrisch ist. Weil S konvex ist folgt $\pm(2\mathbf{x}-2\mathbf{y})/2 = \pm(\mathbf{x}-\mathbf{y}) \in S$. □

Satz 2.1.3
Sei $\mathcal{L} \subset \mathbb{R}^n$ Gitter der $\dim \mathcal{L} = n$ und $K \subset \mathbb{R}^n$ Eichkörper einer beliebigen Norm $\| \ \|$. Dann gilt

$$\lambda_{1,\| \ \|}(\mathcal{L}) \leq 2 \operatorname{vol}(K)^{-1/n} \det \mathcal{L}^{1/n}.$$

Beweis. $S := (\det \mathcal{L}/\operatorname{vol}(K))^{1/n} K$ ist konvex und nullsymmetrisch mit $\operatorname{vol}(S) = \det \mathcal{L}$. Nach Lemma 2.1.1 gibt es ein $\mathbf{b} \in \mathcal{L} \setminus \{\mathbf{0}\}$ mit $S \cap (S+\mathbf{b}) \neq \emptyset$. Sei $\mathbf{y}$ im Durchschnitt, also $\mathbf{y}, \mathbf{b}-\mathbf{y} \in S$. Die Dreiecksungleichung liefert $\|\mathbf{b}\| \leq \|\mathbf{b}-\mathbf{y}\| + \|\mathbf{y}\| \leq 2\,(\det \mathcal{L}/\operatorname{vol}(K))^{1/n}$. □

Das Volumen V_n der n-dimensionalen Einheitskugel $\mathcal{B}_n(\mathbf{b}, 1) = \{\mathbf{x} \in \mathbb{R}^n \ : \ \|\mathbf{x}-\mathbf{b}\| \leq 1\}$ ist

$$V_n \ := \ \pi^{\frac{n}{2}} / \Gamma(1+\tfrac{n}{2}) \ = \ (\tfrac{2e\pi}{n})^{\frac{n}{2}} (\tfrac{1}{\pi n})^{1/2} (1 - \Theta(\tfrac{1}{n})). \tag{2.1}$$

Dabei gilt $\Gamma(1+\frac{n}{2}) = (\frac{n}{2})!$, $\Gamma(1+x) = x\,\Gamma(x)$, $(\frac{1}{2})! = \sqrt{\pi}/2$ für $n \in \mathbb{N}$, $x \in \mathbb{R}$. Für $x \in \mathbb{R}_{>0}$ gilt nach Stirling $\Gamma(1+x) = \sqrt{2\pi x}\ (\frac{x}{e})^x\,(1 + \frac{1}{12x} + \Theta(\frac{1}{x^2}))$ [Knuth 71, Sektion 1.2.5, 1.2.11.2].

Nach Satz 2.1.3 gilt damit für Gitter der Dimension n dass $\lambda_1^2(\mathcal{L}) \leq \frac{2n+o(n)}{e\pi} (\det \mathcal{L})^{2/n}$.

Im Falle der Norm ℓ_∞ mit Eichkörper K_∞ gilt in Satz 2.1.3 dass $\operatorname{vol}(K_\infty) = 2^n$. Damit liefert Satz 2.1.3 die scharfe Schranke $\lambda_{1,\infty}(\mathcal{L}) \leq (\det \mathcal{L})^{\frac{1}{n}}$. Es gilt $\lambda_{1,\infty}(\mathbb{Z}^n) = 1 = (\det \mathbb{Z}^n)^{\frac{1}{n}}$.

Satz 2.1.4 (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. Eine Lösung $(p_1, ..., p_n, q)$ findet man durch Konstruktion eines kürzesten Vektors in der sup-Norm ℓ_∞ zum Gitter $\mathcal{L}(\mathbf{B})$ mit folgender Gitterbasis

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

Wegen $\det \mathbf{B} = \epsilon^{n+1}$ gilt nach Satz 2.1.3 $\lambda_{1,\infty}(\mathcal{L}(\mathbf{B})) \leq (\det \mathbf{B})^{\frac{1}{n+1}} = \epsilon$. Für den $\| \ \|_\infty$-kürzesten Gittervektor $\mathbf{B}(p_1, ..., p_n, -q)^t$ gilt also $|p_i - \alpha_i q\,| \leq \epsilon$ und $|q\epsilon^{n+1}| \leq \epsilon$ und somit $|q| \leq \epsilon^{-n}$. □

Dirichlet bewies Satz 2.1.4 inkonstruktiv mit dem Schubfachprinzip.

Satz 2.1.5
Sei $\mathcal{L}$ Gitter der Dimension n und $\bar{\mathbf{b}}_1, ..., \bar{\mathbf{b}}_n \in \mathcal{L}$ linear unabhängig mit $||\bar{\mathbf{b}}_i|| = \lambda_i$ für $i = 1, ..., n$. Dann gibt es eine Basis $\mathbf{b}_1, ..., \mathbf{b}_n$ von $\mathcal{L}$ so dass für $i = 1, ..., n$

1. $\mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_i) = \text{span}(\bar{\mathbf{b}}_1, ..., \bar{\mathbf{b}}_i) \cap \mathcal{L}$,
2. $\big(\ \mathbf{b}_i = \bar{\mathbf{b}}_i \ \ \textit{oder} \ \ ||\pi_i(\mathbf{b}_i)|| \leq \frac{1}{2}\lambda_i\ \big) \ \ \textit{und} \ \ ||\mathbf{b}_i||^2 \leq \max(1, \frac{i}{4})\lambda_i^2$.

Damit hat jedes Gitter $\mathcal{L}$ eine Basis $\mathbf{b}_1, ..., \mathbf{b}_n$ so dass $||\mathbf{b}_i|| \leq \lambda_i\sqrt{i/4}$ für $i = 4, .., n$. Insbesondere gilt $||\mathbf{b}_i|| = \lambda_i$ für $i = 1, .., 4$ und die Schranke $||\mathbf{b}_i|| \leq \lambda_i\sqrt{i/4}$ ist scharf für $i > 4$.

Beweis durch Induktion nach n. Die Induktionsannahme für $n-1$ sei für $\mathbf{b}_1, ..., \mathbf{b}_{n-1} \in \mathcal{L}$ erfüllt. Wir konstruieren $\mathbf{b}_n$. Im Fall

$$\mathcal{L} \cap \mathcal{P}(\mathbf{b}_1, ..., \mathbf{b}_{n-1}, \bar{\mathbf{b}}_n) = \{\mathbf{0}\}$$

gilt $\mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_{n-1}, \bar{\mathbf{b}}_n) = \mathcal{L}$ und damit gilt die Induktionsbehauptung für $\mathbf{b}_n := \bar{\mathbf{b}}_n$. Andernfalls wählt man für $\mathbf{b}_n$ eine Minimalstelle von

$$||\pi_n(\mathbf{b})|| \neq 0 \text{ für } \mathbf{b} \in \mathcal{L} \cap \mathcal{P}(\mathbf{b}_1, ..., \mathbf{b}_{n-1}, \bar{\mathbf{b}}_n).$$

Diese Wahl von $\mathbf{b}_n$ minimiert $\text{vol}\,\mathcal{P}(\mathbf{b}_1, ..., \mathbf{b}_{n-1}, \mathbf{b}_n)$ sowie $\det \mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_n)$. Somit sichert sie dass $\mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_n) = \mathcal{L}$, denn für echte Untergitter $\bar{\mathcal{L}} \subset \mathcal{L}$ gilt $\det \bar{\mathcal{L}} > \det \mathcal{L}$.

Weil $||\pi_n(\mathbf{b}_n)||$ minimal ist mit $||\pi_n(\mathbf{b}_n)|| \neq 0$ folgt

$$||\pi_n(\mathbf{b}_n)|| \leq \tfrac{1}{2}||\bar{\mathbf{b}}_n|| = \tfrac{1}{2}\lambda_n.$$

Schliesslich reduzieren wir $\mathbf{b}_n \mod \bar{\mathbf{b}}_i$ für $i = n-1, ..., 1$ so dass $||\bar{\pi}_i(\mathbf{b}_n)|| \leq \frac{1}{2}||\bar{\mathbf{b}}_i||$ für die orthogonale Projektion $\bar{\pi}_i : \text{span}(\bar{\mathbf{b}}_1, ..., \bar{\mathbf{b}}_i) \to \text{span}(\bar{\mathbf{b}}_1, ..., \bar{\mathbf{b}}_{i-1})^\perp$. Im Fall $\mathbf{b}_i = \bar{\mathbf{b}}_i$ sichert dies $\bar{\pi}_{i+1}(\mathbf{b}_n) = \pi_i(\bar{\mathbf{b}}_n)$. Es folgt

$$||\mathbf{b}_n||^2 \leq \textstyle\sum_{i=1}^n ||\bar{\pi}_i(\mathbf{b}_n) - \bar{\pi}_{i+1}(\mathbf{b}_n)||^2 \leq \frac{1}{4}\sum_{i=1}^n ||\bar{\mathbf{b}}_i||^2 = \frac{1}{4}\sum_{i=1}^n \lambda_i^2 \leq \frac{n}{4}\lambda_n^2.$$

Dabei ist $\bar{\pi}_i(\mathbf{b}_n) - \bar{\pi}_{i+1}(\mathbf{b}_n)$ der Orthogonalanteil von $\mathbf{b}_n$ in $\text{span}(\bar{\mathbf{b}}_1, ..., \bar{\mathbf{b}}_i) \cap \text{span}(\bar{\mathbf{b}}_1, ..., \bar{\mathbf{b}}_{i-1})^\perp$. Im Fall $\mathbf{b}_i = \bar{\mathbf{b}}_i$ ist dieser Anteil $\mathbf{0}$. Diese Anteile sind für alle i paarweise orthogonal. □

2.2 Packungsdichte, Hermite-Konstante, kritische Gitter

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

Dichte des Gitters. Die (Packungs-)Dichte $\triangle(\mathcal{L})$ des Gitters $\mathcal{L}$ ist der Volumenanteil der Kugelpackung $\bigcup_{\mathbf{b}\in\mathcal{L}} \mathcal{B}_n(\mathbf{b}, \lambda_1/2)$ von $\text{span}\,(\mathcal{L})$ und $\triangle_n$ das Supremum für alle $\mathcal{L}$ mit $\dim \mathcal{L} = n$:

$$\triangle(\mathcal{L}) =_{\text{def}} \lambda_1^n 2^{-n} V_n / \det \mathcal{L}, \qquad \triangle_n =_{\text{def}} \sup\{\triangle(\mathcal{L}) \mid \dim \mathcal{L} = n\}.$$

$\triangle(\mathcal{L})$ ist invariant gegen Äquivalenz, bleibt also bei Isometrie und Skalierung von $\mathcal{L}$ erhalten. Die **relative Dichte** des Gitters $\mathcal{L}$ ist $rd(\mathcal{L}) = \triangle(\mathcal{L})/\triangle_n$.

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 $\mathbf{e} \in \text{span}\,(\mathcal{L})$ 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 $\mathbf{b} + \mathbf{e}$. Mit der Dichte $\triangle(\mathcal{L})$ von $\mathcal{L}$ wächst also das Korrekturpotential des analogen Kodes.

Hermite-Konstante, Hermite-Invariante. Die *Hermite-Invariante* des Gitters $\mathcal{L}$ der Dimension n ist $\gamma(\mathcal{L}) := \lambda_1(\mathcal{L})^2/(\det \mathcal{L})^{\frac{2}{n}}$ Die *Hermite-Konstante* γ_n der Dimension n ist

$$\gamma_n =_{\text{def}} \sup\{\gamma_n(\mathcal{L}) |\ \dim \mathcal{L} = n\} = 4\,(\triangle_n/V_n)^{2/n}.$$

Es genügt das Supremum über die vollständigen Gitter $\mathcal{L}$ zu nehmen, denn $\gamma(\mathcal{L})$ ist gegen Äquivalenz invariant. Weil beschränkte Basen dieser Gitter über einen kompakten Bereich des $\mathbb{R}^{n\times n}$ variieren, ist das Supremum ein Maximum.

Global extreme, kritische Gitter. Ein Gitter $\mathcal{L}$ mit $\dim(\mathcal{L}) = n$ heißt *global extrem* oder *kritisch*, wenn $\triangle(\mathcal{L}) = \triangle_n$, also wenn $rd(\mathcal{L}) = 1$ und $\lambda_1^2(\mathcal{L}) = \gamma_n(\det \mathcal{L})^{2/n}$.

Extreme Gitter. Ein Gitter $\mathcal{L}$ heißt *extrem*, wenn $\triangle(\mathcal{L})$ 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 die Umkehrung gilt nicht.

Satz 2.2.1

$$\gamma_n = 4\,(\triangle_n/V_n)^{2/n} < \tfrac{4}{\pi}\,\Gamma\left(1+\tfrac{n}{2}\right)^{\frac{2}{n}} < \tfrac{2}{e\pi}(n+\ln(\pi n)) \quad \textit{für } n > n_0.$$

Beweis. Sei $\mathcal{L}$ Gitter mit $\dim(\mathcal{L}) = n$ und $\gamma(\mathcal{L}) = \gamma_n$, $\triangle(\mathcal{L}) = \triangle_n$ sowie $\det \mathcal{L} = 1$. Nach Abbildung 2.2.1 ergeben die 2^n Kugelteile in der Grundmasche des Gitters zusammen gerade eine Kugel vom Radius $\lambda_1/2$. Es folgt $V_n(\lambda_1/2)^n = \triangle_n < 1$ somit $\lambda_1 = 2\,(\triangle_n/V_n)^{1/n}$. Nach Satz 2.1.3 und (2.1) gilt $\gamma_n = \lambda_1^2 \det \mathcal{L} = 4\,(\triangle_n/V_n)^{2/n} < \tfrac{4}{\pi}\,\Gamma\left(1+\tfrac{n}{2}\right)^{\frac{2}{n}} = \tfrac{2n}{e\pi}(\pi n)^{\frac{1}{n}}(1+\Theta(\tfrac{1}{n}))$. Aus $1+\varepsilon := (\pi n)^{1/n}$ erhält man $(1+\varepsilon)^n = \pi n$ und $n\ln(1+\varepsilon) = \ln(\pi n)$, also $n\varepsilon \approx \ln(\pi n)$ und somit $n(\pi n)^{\frac{1}{n}} \approx n + \ln(\pi n)$. □

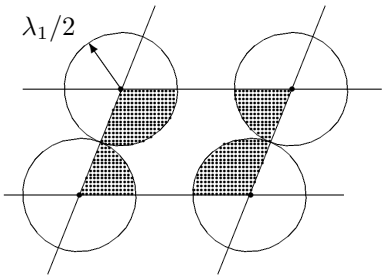

Abbildung 2.2.1: Veranschaulichung von $V_n(\lambda_1/2)^n < \det \mathcal{L}$

Der Beweis von Satz 2.2.1 benutzt nur $\triangle_n < 1$. Blichfeldt [Bli14] zeigt $\triangle_n \le (\sqrt{2} + \mathrm{o}(1))^{-n}$ und damit die bessere Schranke

$$\gamma_n \le \tfrac{2}{\pi}\,\Gamma\left(2+\tfrac{n}{2}\right)^{\frac{2}{n}} \le \tfrac{1}{e\pi}(n+\ln(\pi n)). \tag{2.2}$$

Z.B. gilt $\gamma_{10} \le \tfrac{2}{\pi}(6!)^{0,2} \approx 2,373$. Kabatiansky, Levenshtein [KaLe78] zeigen dass

$$\gamma_n \le \tfrac{1,744}{2e\pi}\,n \quad \text{für } n \ge n_0.$$

Satz 2.2.2 (Minkowski, Hlawka)

$$\triangle_n \ge \textstyle\sum_{k=1}^{\infty} k^{-n}2^{-n+1} > 2^{-n+1} \quad \textit{und} \quad \gamma_n \ge \tfrac{n}{2e\pi}(1+\Omega(\tfrac{1}{n})).$$

Minkowski bewies 1905 inkonstruktiv dass $\triangle_n > 2^{-n+1}$, siehe auch [Hlawka, 44].
Explizite Gitter mit Dichte $\triangle(\mathcal{L}) > 2^{-n+1}$ sind nur für wenige Dimensionen $n < 200$ bekannt. Aus $\triangle_n > 2^{-n+1}$ folgt nach (2.1)

$$\gamma_n = 4(\triangle_n/V_n)^{2/n} > 2^{2/n}/V_n^{2/n} = \frac{n}{2e\pi}(\pi n)^{1/n}(1+\Theta(n^{-2})) = \frac{n}{2e\pi}(1+\Omega(\frac{1}{n})) \tag{2.3}$$

Umgekehrt zeigt die Gauß'sche Volumen-Heuristik dass $\gamma_n \lesssim V_n^{-2/n} \approx \frac{n}{2e\pi}$. Für Gitter $\mathcal{L} \subset \mathbb{R}^n$ mit $\dim \mathcal{L} = n$, $\det \mathcal{L} = 1$ und zufällige $\mathbf{t} \in \mathbb{R}^n$ gilt nämlich:

$$\mathbf{E}[|\mathcal{L} \cap \mathcal{B}_n(\mathbf{t}, (2/V_n)^{1/n})|] = V_n(2/V_n)^{n/n} = 2.$$

Verhält sich $\mathbf{t} = \mathbf{0}$ wie ein zufälliges $\mathbf{t}$ dann gilt $\lambda_1(\mathcal{L}) \leq (2/V_n)^{1/n}$, also $\gamma_n \lesssim (2/V_n)^{2/n} \approx \frac{n}{2e\pi}(e\pi)^{1/n}$.

Vermutlich gilt also $\gamma_n \approx \frac{n}{2e\pi}(4e\pi)^{1/n}$ und somit $\triangle_n = 2^{-n} n^{O(1)}$. 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.

n	2	3	4	5	6	7	8	24
γ_n^n	$\frac{4}{3}$	2	4	8	$2^6/3$	2^6	2^8	2^{48}
$\triangle_n$	0,907	0,740	0,617	0,465	0,373	0,295	0,254	$V_{24} \approx 0.002$
$\delta = \triangle_n/V_n$	$1/2\sqrt{3}$	$1/4\sqrt{2}$	1/8	$1/8\sqrt{2}$	$1/8\sqrt{3}$	1/16	1/16	1
krit. Gitter	$\mathbb{A}_2$	$\mathbb{A}_3 \cong \mathbb{D}_3$	$\mathbb{D}_4$	$\mathbb{D}_5$	$\mathbb{E}_6$	$\mathbb{E}_7$	$\mathbb{E}_8$	Leech G. Λ_{24}

Tabelle 2.2.2

Die bekannten Hermite-Konstanten. Die Hermite-Konstanten $\gamma_3, \gamma_4, \gamma_5$ wurden von Gauß (γ_3) sowie Korkine und Zolotareff (γ_4, γ_5) [KZ1872, KZ1873, KZ1877] bestimmt. Blichfeldt [Bli35] hat $\gamma_6, \gamma_7, \gamma_8$ ermittelt. Blichfeldts Beweis ist kompliziert und wurde von Watson [W66] und Vetchinkin [V82] bestätigt. Für Dimension $n \leq 8$ sind die kritischen Gitter bis auf Äquivalenz (Isometrie und Skalierung) eindeutig bestimmt. Dies wurde von Barnes [Bar59] und Vetchinkin [V82] bewiesen. Cohn hat 2005 gezeigt, dass das Leech Gitter Λ_{24} kritisch und bis aud Äquivalenz eindeutig ist, siehe [CK09]. Die Tabelle 2.2.2 zeigt die bewiesenen γ_n^n, die gerundeten maximalen Dichten $\triangle_n$, sowie kritische Gitter. Zu $\mathbb{A}_n, \mathbb{D}_n, \mathbb{E}_n$ siehe Seite 7.

Einfache GNF's und Gram-Matrizen der kritischen Gitter. Betrachte die GNF

$$\mathbf{R}_8 := \sqrt{2}\begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ 0 & \sqrt{\frac{3}{4}} & \frac{1}{\sqrt{12}} & \sqrt{\frac{1}{3}} & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{\frac{2}{3}} & \sqrt{\frac{1}{6}} & \sqrt{\frac{3}{8}} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \sqrt{\frac{3}{8}} & \frac{1}{\sqrt{6}} & \sqrt{\frac{2}{3}} \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{12}} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{bmatrix}, \qquad \det \mathbf{R}_8 = 1.$$

Die Teilmatrix $\mathbf{R}_n$ der ersten $n \leq 8$ Zeilen und Spalten von $\mathbf{R}_8$ liefert für $n \leq 8$ das kritische Gitter $\mathcal{L}(\mathbf{B}_n)$ skaliert zu $\lambda_1^2 = 2$. Für die Gram-Matrizen $\mathbf{R}_n^t \mathbf{R}_n = [\langle \mathbf{r}_i, \mathbf{r}_j \rangle]_{1 \leq i,j \leq n}$ gilt :

$$\langle \mathbf{r}_i, \mathbf{r}_j \rangle = \begin{cases} 2 & \text{für } i = j \\ 1 & \text{für } 1 \leq |i-j| \leq 2 \text{ und } 1 \leq i,j \leq n \\ 0 & \text{sonst} \end{cases} \tag{2.4}$$

$$\mathbf{R}_8^t\mathbf{R}_8 := \begin{bmatrix} 2 & 1 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 1 & 2 & 1 & \ddots & \ddots & & & \vdots \\ 1 & 1 & 2 & \ddots & & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & & & \ddots & \vdots \\ \vdots & \ddots & & & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & & \ddots & 2 & 1 & 1 \\ \vdots & & & \ddots & \ddots & 1 & 2 & 1 \\ 0 & \cdots & \cdots & \cdots & 0 & 1 & 1 & 2 \end{bmatrix} \in \mathbb{Z}^{8\times 8}. \qquad \det \mathbf{R}_8 = 1$$

Nach Lemma 2.2.3 gilt $\lambda_1(\mathbf{R}_n) = \sqrt{2}$. Die δ-Werte von $\mathcal{L}(\mathbf{R}_n)$ stimmen für $n \leq 8$ mit den δ-Werten der Tabelle 2.2.2 überein. Die Gitter $\mathcal{L}(\mathbf{R}_n)$ für $n = 1, ..., 8$ sind kritisch und äquivalent zu $\mathbb{A}_2, \mathbb{A}_3 \cong \mathbb{D}_3, \mathbb{D}_4, \mathbb{D}_5, \mathbb{E}_6, \mathbb{E}_7, \mathbb{E}_8$. $\Lambda_n := \mathcal{L}(\mathbf{R}_n)$. Sie realisieren die Hermite-Konstanten γ_n.

Das Gitter $\mathcal{L}(\mathbf{R}_8)$ ist wegen $\det \mathbf{R}_8 = 1$ selbstdual, $\mathcal{L}(\mathbf{R}_8) = \mathcal{L}(\mathbf{R}_8)^*$. Damit ist jeder Vektor $\mathbf{b} \in \operatorname{span}(\mathcal{L}(\mathbf{R}_8))$ mit $\langle \mathbf{r}_i, \mathbf{b}\rangle \in \mathbb{Z}$ für $i = 1, ..., 8$ bereits in $\mathcal{L}(\mathbf{R}_8)$. Die Gitter $\mathbf{R}_i$ für $i = 1, ..., 8$ sind geschichtet nach Def. 2.2.3 und sind durch Schichtung fortsetzbar in Dimension $n > 8$, siehe [CoSl88, chapter 6]. Für $n = 11, 12, 13$ und $n > 24$ gibt es mehrere Isometrieklassen geschichteter Gitter verschiedener Dichte $\triangle$, siehe [CoSl88, Figur 6.1]. $\mathbf{R}_{24}$ ist äquivalent zum Leech Gitter.

Das Leech Gitter. Das Leech Gitter $\mathcal{L}(\mathbf{B}_{24})$ ist bis auf $\ddot{A}$quivalenz das einzige Gitter maximaler Dichte der Dimension 24, siehe H. Cohn, A. Kumar [CK09]. Seine Basis $\mathbf{B}_{24}$ ist delbstdual.

$$\mathbf{B}_{24} = \frac{1}{\sqrt{8}} \left[\begin{array}{cccc|cccc|cccc|cccc|cccc|cccc} 8&4&4&4&4&4&4&2&4&4&4&2&4&2&2&2&4&2&2&2&0&0&0&-3 \\ 0&4&0&0&0&0&0&2&0&0&0&2&0&2&0&0&0&0&0&2&2&0&0&1 \\ 0&0&4&0&0&0&0&2&0&0&0&2&0&0&2&0&0&2&0&0&2&0&0&1 \\ 0&0&0&4&0&0&0&2&0&0&0&2&0&0&0&2&0&0&2&0&2&0&0&1 \\ \hline 0&0&0&0&4&0&0&2&0&0&0&0&0&2&2&2&0&2&2&2&2&0&0&1 \\ 0&0&0&0&0&4&0&2&0&0&0&0&0&2&0&0&0&0&2&0&0&0&0&1 \\ 0&0&0&0&0&0&4&2&0&0&0&0&0&0&2&0&0&0&0&2&0&0&0&1 \\ 0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&2&0&2&0&0&0&0&0&1 \\ \hline 0&0&0&0&0&0&0&0&4&0&0&2&0&2&2&2&0&2&2&2&2&2&2&1 \\ 0&0&0&0&0&0&0&0&0&4&0&2&0&2&0&0&0&2&0&0&0&2&0&1 \\ 0&0&0&0&0&0&0&0&0&0&4&2&0&0&2&0&0&0&2&0&0&0&2&1 \\ 0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&2&0&0&0&2&0&0&0&1 \\ \hline 0&0&0&0&0&0&0&0&0&0&0&0&4&2&2&2&0&0&0&0&2&2&2&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&2&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&2&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&1 \\ \hline 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&2&2&2&2&2&2&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&2&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&2&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&1 \\ \hline 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&2&2&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \end{array}\right]$$

GNF-Basis $\mathbf{B}_{24} = \mathrm{GNF}(\mathbf{B}_{24})$ des Leech Gitters Λ_{24}, skaliert zu $\lambda_1 = 2$, $\det \mathbf{B}_{24} = 1$.

Lemma 2.2.3
Sei $\mathbf{B}^t\mathbf{B} \in k\,\mathbb{Z}^{n\times n}$, $k \in \mathbb{N}$ *mit* $\|\mathbf{b}_1\|^2, \cdots, \|\mathbf{b}_n\|^2 \in 2k\,\mathbb{N}$, *dann gilt* $\lambda_1^2(\mathcal{L}(\mathbf{B})) \in 2k\,\mathbb{N}$.

Beweis. Offenbar folgt für $t_i, t_j \in \mathbb{Z}$

$$\|\sum_{i=1}^n t_i\mathbf{b}_i\|^2 = \sum_{1\le i,j\le n} t_it_j\,\langle \mathbf{b}_i, \mathbf{b}_j\rangle = \sum_{i=1}^n t_i^2||\mathbf{b}_i||^2 + 2\sum_{j<i} t_it_j\,\langle \mathbf{b}_i, \mathbf{b}_j\rangle \in 2k\,\mathbb{Z}. \qquad \square$$

Es bezeichne $\mathbf{B}_n$ die Matrix der ersten $n \le 8$ Zeilen und Spalten von $\mathbf{B}_{24}$ und $\Lambda_n = \mathcal{L}(\mathbf{B}_n)$.

Fakt. Es gilt $\lambda_1^2 = 4$ für $\Lambda_n = \mathcal{L}(\mathbf{B}_n)$, $n = 2, ..., 24$.

Beweis. Sei $\mathbf{B}_n = [\mathbf{b}_1, ..., \mathbf{b}_n]$. Dann gilt $\mathbf{B}_{24}^t\mathbf{B}_{24} \in 2\,\mathbb{Z}$, $||\mathbf{b}_2||^2 = 4$ und $\|\mathbf{b}_1\|^2, \cdots, \|\mathbf{b}_{24}\|^2 \in 4\,\mathbb{N}$. Nach Lemma 2.2.3 folgt $\lambda_1^2 = 4$ für Λ_n, $n = 2, ..., 24$. $\square$

Definition 2.2.4
Der Punkt $\mathbf{z} \in \mathrm{span}(\mathcal{L})$ *heißt* **tiefes Loch** *des Gitters* $\mathcal{L}$, *wenn*

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

Der Abstand $\rho = \|\mathbf{z} - \mathcal{L}\| = \min\{\|\mathbf{z} - \mathbf{y}\| \,:\, \mathbf{y} \in \mathcal{L}\}$ *zum tiefen Loch* $\mathbf{z}$ *ist der* Überdeckungsradius *(covering radius) von* $\mathcal{L}$. *Die Kugeln* $\mathcal{B}_n(\mathbf{b}, \rho)$ *mit* $\mathbf{b} \in \mathcal{L}$ *überdecken* $\mathrm{span}(\mathcal{L})$.

Die Menge S der tiefen Löcher von $\mathcal{L}$ ist $S = \mathbf{b} + \mathcal{L}$ für jedes $\mathbf{b} \in S$. Zum tiefen Loch $\mathbf{z}$ von $\mathcal{L}$ der Dimension n gibt es $n+1$ Vektoren $\mathbf{b}_i \in \mathcal{L}$ mit $\|\mathbf{z} - \mathbf{b}_i\| = \|\mathbf{z} - \mathcal{L}\|$ für $i = 1, ..., n+1$ so dass $\mathrm{span}(\mathbf{b}_1, ..., \mathbf{b}_{n+1}) = \mathrm{span}(\mathcal{L})$.

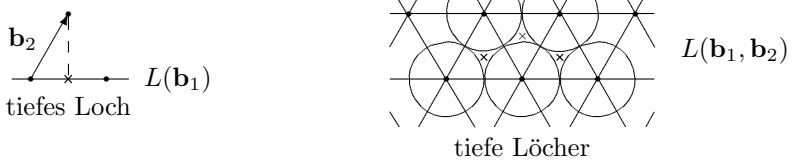

Abbildung 2.2.2: Tiefe Löcher in Λ_1 und Λ_2

Definition 2.2.5
Das Gitter $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ *ist* geschichtet (laminated) *zum Gitter* $\mathcal{L}_{n-1} = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$ *wenn* $\mathbf{b}_n - \widehat{\mathbf{b}}_n \in \mathrm{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$ *tiefes Loch des Gitters* $\mathcal{L}_{n-1}$ *ist und* $\|\mathbf{b}_n\| = \lambda_1(\mathcal{L}_{n-1})$. *Es bezeichne* Λ_n *ein ab der Dimension 1 iterativ geschichtetes Gitter der Dimension* n.

Die Anzahl der Gittervektoren $\mathbf{b} \in \mathcal{L}$ mit $\|\mathbf{b}\| = \lambda_1$ ist die **kissing number** der Kugelpackung zu $\mathcal{L}$ mit Kugelradius $\lambda_1/2$. Dies ist die Anzahl der Berührungspunkte einer Kugel der Kugelpackung mit anderen Kugeln.

Die Gitter Λ_n, für $n = 2, ..., 24$ sind geschichtet und sind durch die Schichtung bis auf Isomorphie eindeutig. Sie sind kritisch für $n = 2, ..., 8, 24$. Die K_i sind Gitter über den komplexen Zahlen $\mathbb{C}$. Es wird $\mathbb{Z}$ ersetzt durch den Ring der Eisenstein ganzen Zahlen $\mathbb{Z} + \omega\mathbb{Z}$ mit $\omega = (-1 + i\sqrt{3})/2 = (-1)^{1/3} \in \mathbb{C}$.

Die Gitter K_i haben für $i = 11, 12, 13$ grössere Dichte als Λ_i. Das Coxeter-Todd Gitter K_{12} hat Dichte $V_{12}/27$, aber Λ_{12} hat nur Dichte $V_{12}/32$. K_{12} besteht aus den Vektoren $\mathbf{z} = \mathbf{B}_{24}\mathbf{x}$ des Leech Gitters so dass für $\mathbf{z} = (z_1, ..., z_{24})^t$ gilt dass $z_i = z_{i+1} = z_{i+2}$ für $i = 4j + 1$ und $j = 0, ..., 5$. Auch K_{11}, K_{13} sind Sektionen des Leech Gitters. Zu weiteren Informationen siehe [CoSl88], [Mar03].

Es ist offen, ob die Gitter Λ_9, Λ_{10} kritisch sind. Die kissing number der Gitter Λ_n, $2 \le n \le 24$ und die kürzesten Gittervektoren kann man leicht aus $\mathbf{B}_{24}$ ablesen. Z.B. hat das Gitter Λ_8 kissing number 240.

2.3 Zweiter Satz von Minkowski.

Satz 2.3.1
Für jedes Gitter $\mathcal{L} \subset \mathbb{R}^m$ mit $\dim \mathcal{L} = n$ gilt für die ℓ_2-Norm $\prod_{i=1}^n \lambda_i(\mathcal{L}) \leq \gamma_n^{n/2} \det \mathcal{L}$.

Satz 2.3.1 verschärft die Ungleichung $\lambda_1^2 \leq \gamma_n (\det \mathcal{L})^{2/n}$. Für kritische Gitter $\mathcal{L}$ gilt $\lambda_1^n = \gamma_n^{n/2} \det \mathcal{L}$ und 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 $\|\mathbf{a}_i\| = \lambda_i$ für $i = 1, \ldots, n$. $\mathcal{L}(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ ist ein Untergitter von $\mathcal{L}$. Wähle die Basis $\mathbf{b}_1, ..., \mathbf{b}_n$ von $\mathcal{L}$ so dass mit einer oberen Dreiecksmatrix $\mathbf{T} \in \mathbb{Z}^{n \times n}$ nach Satz 1.5.5 gilt $[\mathbf{b}_1, \ldots, \mathbf{b}_n]\, \mathbf{T} = [\mathbf{a}_1, \ldots, \mathbf{a}_n]$. Es gilt dann

$$\mathbf{b} \in \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n) \setminus \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{s-1}) \quad \Longrightarrow \quad \|\mathbf{b}\| \geq \lambda_s \ \text{ für } s = 2, ..., n, \tag{2.5}$$

weil $\mathbf{b} \notin \operatorname{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{s-1}) = \operatorname{span}(\mathbf{a}_1, \ldots, \mathbf{a}_{s-1})$.

Wir setzen $\bar{\mathbf{b}}_i := \sum_{j=1}^i \mu_{i,j} \widehat{\mathbf{b}}_j / \lambda_j$ für $1 \leq i \leq n$, $\bar{\mathcal{L}} := \mathcal{L}\left(\bar{\mathbf{b}}_1, \ldots, \bar{\mathbf{b}}_n\right)$ und 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, $t_s \neq 0$ und $\mathbf{b} := \sum_{i=1}^s t_i \mathbf{b}_i$. Dann gilt

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

so dass wegen (2.5) 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

$$1 \leq \lambda_1(\bar{\mathcal{L}})^2 \leq \gamma_n \, (\det \bar{\mathcal{L}})^{2/n} = \gamma_n \, (\det \mathcal{L})^{2/n} (\textstyle\prod_{i=1}^n \lambda_i)^{-2/n}.$$

Diese Ungleichung potenziert mit $n/2$ und multipliziert mit $\prod_{i=1}^n \lambda_i$ liefert die Behauptung. □

Lemma 2.3.2
Für jedes Gitter $\mathcal{L}$ mit $\dim \mathcal{L} = n$ gilt für die ℓ_2-Norm $\prod_{i=1}^n \lambda_i \geq \det \mathcal{L}$.

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 $\det \mathcal{L}(a_1, \ldots, a_n) \geq \det \mathcal{L}$. Ferner liefert die Ungleichung von Hadamard $\prod_{i=1}^n \lambda_i = \prod_{i=1}^n \|a_i\| \geq \det \mathcal{L}(a_1, \ldots, a_n)$. Es folgt die Behauptung. □

Satz 2.3.3 verallgemeinert Satz 2.3.1 auf eine allgemeine Norm mit Eichkörper K. Der Satz stammt von Minkowski 1907, siehe Paragraph 9.1, Kapitel 2, [GrLek87].

Satz 2.3.3
Seien $\lambda_1, \ldots, \lambda_n$ die sukzessiven Minima des Gitters $\mathcal{L} \subset \mathbb{R}^m$ mit $\dim \mathcal{L} = n$ bezüglich einer beliebigen Norm mit Eichkörper K, dann gilt $\det \mathcal{L}/n! \leq \operatorname{vol}(K \cap \operatorname{span}(\mathcal{L}))\, 2^{-n} \prod_{i=1}^n \lambda_i \leq \det \mathcal{L}$.

Im Fall der sup-Norm ℓ_∞ gilt $\operatorname{vol}(K \cap \mathcal{L}) \geq 2^n$ und somit $\prod_{i=1}^n \lambda_{i,\infty} \leq \det \mathcal{L}$. Diese Schranke ist scharf, denn für $\mathcal{L} = \mathbb{Z}^n$ gilt $\lambda_{i,\infty} = 1$ und $\det \mathcal{L} = 1$.

Kapitel 3

Gauß-Reduktion

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

3.1 Reduzierte Basis

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

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

Satz 3.1.1
Für jede reduzierte Basis $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$ ist $\mathbf{a}$ ein kürzester Gittervektor $\neq 0$ und $\mathbf{b}$ ein dazu linear unabhängiger kürzester Gittervektor.

Beweis. Zu zeigen ist für allgemeine Norm

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

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

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

Für eine allgemeine Norm und $c > 0$ ist der Bereich der Vektoren $K_c = \{x \,|\, \|x\| \leq c\}$ konvex. Wegen dieser Konvexität hat die Norm auf jeder der vier Grenzgeraden von $\mathcal{P}$, den Geraden $\pm\mathbf{a} + t\mathbf{b}$, $\pm\mathbf{b} + t\mathbf{a}$ 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 $\pm\mathbf{a} \pm \mathbf{b}$ an. Daher sind $\mathbf{a}, \mathbf{b}$ offenbar zwei kleinste, linear unabhängige Gitterpunkte. □

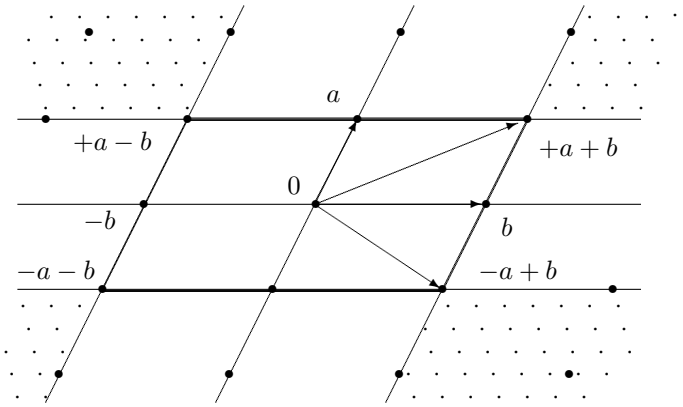

Abbildung 3.1.1: Reduzierte Basis $\mathbf{a}, \mathbf{b}$

3.2 Reduktionsverfahren für die Euklidische Norm

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

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

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

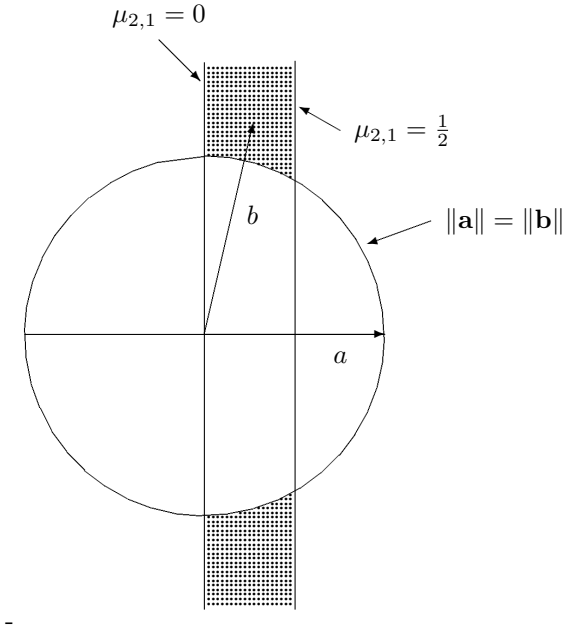

Abbildung 3.2.1: Bereich der reduzierten Basen $\mathbf{a}, \mathbf{b}$ mit $\mu_{2,1} \geq 0$

Abbildung 3.2.1 zeigt zu festem $\mathbf{a}$ den gepunkteten Bereich der Vektoren $\mathbf{b}$ der reduzierten Basen $\mathbf{a}, \mathbf{b}$ mit $\mu_{2,1} \geq 0$. Sei $\phi = \angle(\mathbf{a}, \mathbf{b})$ der Winkel zwischen den Gittervektoren $\mathbf{a}, \mathbf{b}$, $\cos\phi = \frac{\mathbf{a}^t\mathbf{b}}{\|\mathbf{a}\|\cdot\|\mathbf{b}\|}$. Für reduzierte Basen $\mathbf{a}, \mathbf{b}$ gilt $60° \leq \phi \leq 90°$.

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

Algorithmus 3.2.1 Gauß-Reduktionsverfahren für die Euklidische Norm

EINGABE: Gitterbasis $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{R}^n$ mit $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$

WHILE $|\mu_{2,1}| > \frac{1}{2}$ DO $\quad /* \ \mu_{2,1} = r_{1,2}/r_{1,1} \ */$

1. $\mathbf{b}_2 := \mathbf{b}_2 \cdot \text{sign}(\mu_{2,1}) \quad /* \text{ wir erreichen } \mu_{2,1} \geq 0 \ */$

2. $\mathbf{b}_2 := \mathbf{b}_2 - \lceil \mu_{2,1} \rfloor \mathbf{b}_1$

3. IF $\|\mathbf{b}_1\| > \|\mathbf{b}_2\|$ THEN vertausche $\mathbf{b}_1$ und $\mathbf{b}_2$

AUSGABE: Reduzierte Basis $\mathbf{b}_1, \mathbf{b}_2$

Eine *Runde* der Schritte **1. 2. 3.** sichert in Schritt **1.** durch Vorzeichenwahl von $\mathbf{b}_2$ dass $\mu_{2,1} \geq 0$, reduziert in Schritt **2.** gemäß $\mathbf{b}_2 := \mathbf{b}_2 - \lceil \mu_{2,1} \rfloor \mathbf{b}_1$ und vertauscht in Schritt **3.** sofern nicht schon $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$ gilt. Nach Schritt **1.** gilt stets $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$ und $\mu_{2,1} \geq 0$. Die Schritte **2. 3.** lauten bei Vertauschung in Matrizenschreibweise

$$[\mathbf{b}_1, \mathbf{b}_2] := [\mathbf{b}_1, \mathbf{b}_2] \begin{bmatrix} -\lceil \mu_{2,1} \rfloor & 1 \\ 1 & 0 \end{bmatrix}.$$

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

Zu gegebener reduzierten Ausgabebasis $\mathbf{b}_1, \mathbf{b}_2$ und Rundenzahl k der Gauß-Reduktion identifizieren wir eine *minimale* Eingabebasis, welche in k Runden auf $\mathbf{b}_1, \mathbf{b}_2$ reduziert wird. Die Minimalität der Basis bedeutet, dass ihre Vektoren minimale Länge haben. Eine solche Eingabebasis heißt eine *minimale k-te Vorgängerbasis* zu $\mathbf{b}_1, \mathbf{b}_2$.

Satz 3.2.1

1. *Zur reduzierten Basis* $\mathbf{b}_1, \mathbf{b}_2$ *und Rundenzahl* k *ist* $[\mathbf{b}_1, \mathbf{b}_2]\, A_k$ *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 3.2.1 macht zur Eingabe* $\mathbf{b}_1, \mathbf{b}_2$ *höchstens* $\log_{1+\sqrt{2}}(\|\mathbf{b}_1\| / \lambda_2) + 2.54$ *Runden.*

Wohlgeordnete Basis. Eine Basis $\mathbf{b}_1, \mathbf{b}_2$ heißt *wohlgeordnet* wenn $\|\mathbf{b}_1\| \leq \|\mathbf{b}_1 - \mathbf{b}_2\| < \|\mathbf{b}_2\|$. Dies ist für die Euklidischen Norm äquivalent zu $\frac{1}{2} < \mu_{2,1} \leq 1$, $\|\mathbf{b}_1\| < \|\mathbf{b}_2\|$. In Schritt **2.** wird also eine wohlgeordnete Basis erzeugt, es sei denn die Basis ist schon reduziert. Offenbar gelten folgende Aussagen.

Lemma 3.2.2

Für jede nicht reduzierte Basis mit $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$ *ist genau eine der Basen* $\mathbf{b}_1, \pm\mathbf{b}_2$ *wohlgeordnet.*

Lemma 3.2.3

Wendet man die Schritte **2. 3.** *an auf zwei equivalente Basen* $\mathbf{b}_1, \mathbf{b}_2$ *und* $\mathbf{b}'_1, \mathbf{b}'_2$*, so bleibt die Äquivalenz erhalten.*

Wegen Lemma 3.2.3 gibt es zu gegebener reduzierten Basis eine minimale k-te Vorgängerbasis, bei deren Reduktion das Vorzeichen von $\mathbf{b}_2$ 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 $(\mathbf{b}_{k+1}, \mathbf{b}_{k+2})$, $(\mathbf{b}_k, \mathbf{b}_{k+1}), \ldots, (\mathbf{b}_2, \mathbf{b}_3)$ und schließlich die reduzierte Basis $(\mathbf{b}_1, \mathbf{b}_2)$. Bleibt das Vor-

zeichen von $\mathbf{b}_2$ in Schritt **1.** stets unverändert, und wird in der letzten Runde in Schritt **3.** getauscht, dann ist die k-te Vorgängerbasis $(\mathbf{b}_{k+1}, \mathbf{b}_{k+2})$ zur reduzierten Basis $(\mathbf{b}_1, \mathbf{b}_2)$ von der Form

$$[\mathbf{b}_k, \mathbf{b}_{k+1}] = [\mathbf{b}_1, \mathbf{b}_2] \prod_{i=1,\ldots,k} \begin{bmatrix} 0 & 1 \\ 1 & \mu^{(i)} \end{bmatrix}.$$

Dabei ist $\mu^{(i)} = \lceil \mu_{2,1} \rfloor$ der ganzzahlige Reduktionskoeffizient der i-ten Runde. Die behauptete Form von $(\mathbf{b}_{k+1}, \mathbf{b}_{k+2})$ 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 3.2.4
Sei $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{R}^n$ wohlgeordnete Basis, welche durch die Schritte **2. 3.** *in die wohlgeordnete Basis $\mathbf{b}'_1 = \mathbf{b}_2 - \lceil \mu_{2,1} \rfloor \mathbf{b}_1,\ \mathbf{b}'_2 = \mathbf{b}_1$ transformiert wird. Im Fall $\angle(\mathbf{b}_1, \mathbf{b}'_1) < 30^o$ gilt $\mu'_{2,1} > \frac{3}{2}$.*
Im Fall $\angle(\mathbf{b}_1, \mathbf{b}'_1) \geq 30^o$ gibt es eine reduzierte Basis bestehend aus den Vektoren $\mathbf{b}'_1, \mathbf{b}'_2, \mathbf{b}'_2 - \mathbf{b}'_1$.

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 $\langle \mathbf{b}_1, \mathbf{b}'_1 \rangle \|\mathbf{b}_1\|^{-2} = \frac{1}{2}$, weil dann $\|\mathbf{b}'_1\| / \|\mathbf{b}_1\|$ maximal ist.

Abbildung 3.1: Der Fall $\angle(\mathbf{b}_1, \mathbf{b}'_1) = 30$, $\langle \mathbf{b}_1, \mathbf{b}'_1 \rangle \|\mathbf{b}_1\|^{-2} = \frac{1}{2}$

Im Fall $\angle(\mathbf{b}_1, \mathbf{b}'_1) = 30^o$ gilt $\frac{3}{4}\|\mathbf{b}'_1\|^2 = \frac{1}{4}\|\mathbf{b}_1\|^2$. Daher gilt im Falle $\angle(\mathbf{b}_1, \mathbf{b}'_1) < 30^o$ offenbar $\|\mathbf{b}_1\|^2 < 3\,\|\mathbf{b}'_1\|^2$. Es folgt die Behauptung

$$\mu'_{2,1} = \langle \mathbf{b}_1, \mathbf{b}'_1 \rangle \|\mathbf{b}'_1\|^{-2} \geq 3\,\langle \mathbf{b}_1, \mathbf{b}'_1 \rangle \|\mathbf{b}_1\|^{-2} > \tfrac{3}{2}.$$

Im Falle $\angle(\mathbf{b}_1, \mathbf{b}'_1) > 30^o$ gilt $\frac{1}{2} < \mu'_{2,1} < \frac{3}{2}$. Sofern die Basis $\mathbf{b}'_1, \mathbf{b}'_2$ nicht schon reduziert ist, wird in der nächsten Runde $\mathbf{b}'_2 - \mathbf{b}'_1$ gebildet und die Reduktion bricht ab. □

Beweis von Satz 3.2.1. Betrachte nun den Fall dass $(\mathbf{b}_2, \mathbf{b}_3) = (\mathbf{b}'_1, \mathbf{b}'_2)$ direkte Vorgängerbasis ist zur reduzierten Basis $\mathbf{b}_1, \mathbf{b}_2$ gemäß Lemma 3.2.4. Es sei also $\mathbf{b}_1, \mathbf{b}_2$ eine Auswahl von $\mathbf{b}'_1, \mathbf{b}'_2, \mathbf{b}'_2 - \mathbf{b}'_1$. Dann ist

$$[\mathbf{b}_{k+1}, \mathbf{b}_{k+2}] = [\mathbf{b}_1, \mathbf{b}_2] \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}^{k-2} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

eine minimale k-te Vorgängerbasis $(\mathbf{b}_{k+1}, \mathbf{b}_{k+2})$ zur reduzierten Basis $(\mathbf{b}_1, \mathbf{b}_2)$. Wegen Lemma 3.2.4 gilt nämlich $\mu^{(i)} \geq 2$ für die ganzzahligen Reduktionskoeffizienten mit $1 < i < k$ und $\mu^{(1)} = \mu^{(k)} = 1$. Offenbar wird $\mathbf{b}_{k+1}, \mathbf{b}_{k+2}$ 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

$$[\mathbf{b}_{k+1}, \mathbf{b}_{k+2}]\,[\mathbf{b}_{k+1}, \mathbf{b}_{k+2}]^t = A_k\ [\mathbf{b}_1, \mathbf{b}_2]^t [\mathbf{b}_1, \mathbf{b}_2] A_k^t$$

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 $\langle \mathbf{b}_1, \mathbf{b}_2 \rangle \geq 0$ folgt

$$\|\mathbf{b}_{k+1}\| \geq (a_{k-4} + 2a_{k-3} + a_{k-2}) \|\mathbf{b}_2\| \geq 1.5\,(1+\sqrt{2})^{k-3}\,\lambda_2.$$

Algorithmus 3.2.2 Gauß-Reduktionsverfahren für beliebige Norm

EINGABE: Wohlgeordnete Gitterbasis $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{R}^n$ mit $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$

WHILE $\|\mathbf{b}_2\| > \|\mathbf{b}_1 - \mathbf{b}_2\|$ DO

1. $\mathbf{b}_2 := \mathbf{b}_2 - \mu\mathbf{b}_1$ mit $\mu \in \mathbb{Z}$ derart, dass $\|\mathbf{b}_2 - \mu\mathbf{b}_1\|$ minimal ist

2. IF $\|\mathbf{b}_1 + \mathbf{b}_2\| < \|\mathbf{b}_1 - \mathbf{b}_2\|$ THEN $\mathbf{b}_2 := -\mathbf{b}_2$

3. vertausche $\mathbf{b}_1$ und $\mathbf{b}_2$

AUSGABE: Reduzierte Basis $\mathbf{b}_1, \mathbf{b}_2$

Somit gilt $k \leq 2.54 + \log_{1+\sqrt{2}}(\|\mathbf{b}_{k+1}\|/\lambda_2)$, weil $2.54 > 3 - \log 1.5/\log(1+\sqrt{2})$. □

Korrektheit. Nach Schritt **1.** gilt $\|\|\mathbf{b}_2\|\| \leq \|\mathbf{b}_1 \pm \mathbf{b}_2\|$, nach Schritt **2.** gilt $\|\mathbf{b}_2\| \leq \|\mathbf{b}_1 - \mathbf{b}_2\| \leq \|\mathbf{b}_1 + \mathbf{b}_2\|$ und nach Schritt **3.** gilt $\|\mathbf{b}_1\| \leq \|\mathbf{b}_1 - \mathbf{b}_2\| \leq \|\mathbf{b}_1 + \mathbf{b}_2\|$. Falls nach Schritt **3.** $\|\mathbf{b}_2\| \leq \|\mathbf{b}_1 - \mathbf{b}_2\|$ gilt, dann gilt auch $\|\mathbf{b}_1\|, \|\mathbf{b}_2\| \leq \|\mathbf{b}_1 \pm \mathbf{b}_2\|$.

Die Rundenzahl für dieses Verfahren ist beschränkt durch $\log_{1+\sqrt{2}}(\|\mathbf{b}_1\|/\lambda_{2,\|\ \|}) + O(1)$. Dabei ist $\lambda_{2,\|\ \|}$ das zweite sukzessive Minimum zur Norm $\|\ \|$. Eine ausführliche Analyse findet sich in [KS96] sowie in [Ka94]. Dort werden effiziente Algorithmen für den Schritt **1.** in der l_1- und sup-Norm vorgestellt.

Kapitel 4

LLL-reduzierte Gitterbasen

LLL-reduzierte Gitterbasen $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ beliebigen Ranges n wurde 1982 von A.K. Lenstra, H.W. Lenstra und L. Lovász [LLL82] eingeführt. Der LLL-Algorithmus ist das erste Reduktionsverfahren für ganzzahlige Gitterbasen mit einer polynomiellen Laufzeit und Approximationsfaktor $\|\mathbf{b}_i\|^2/\lambda_i^2 \leq 2^n$. Es iteriert die Gauß-Reduktion in Dimension $n = 2$.

4.1 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. Sei $[\mathbf{b}_1, ..., \mathbf{b}_n] = \mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m\times n}$ Gitterbasis mit $\mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n\times n}$.

Definition 4.1.1 (LLL-reduzierte Basis)
Eine Gitterbasis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m\times n}$ *heißt* LLL-reduziert *(oder LLL-Basis) mit* δ, $\frac{1}{4} < \delta \leq 1$, *wenn*

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

Basen mit *1.* sind *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. Die Eigenschaft 'LLL-Basis' zu sein bleibt bei Isometrie erhalten : $\mathbf{B} = \mathbf{QR}$ ist LLL-Basis gdw $\mathbf{R}$ LLL-Basis ist.

Die LLL-Basen mit $\delta = 1$ und $n = 2$ sind genau die Gauß-reduzierten Basen. $\mathbf{B}$ ist LLL-Basis mit δ gdw die Matrizen $\begin{bmatrix} r_{k-1,k-1} & r_{k-1,k} \\ 0 & r_{k,,k} \end{bmatrix} \in \mathbb{R}^{2\times 2}$ für $k = 2, ..., n$ LLL-Basen mit δ sind.

Lemma 4.1.2
Für jede LLL-Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m\times n}$ *mit* δ *und* $\alpha = (\delta - \frac{1}{4})^{-1}$ *gilt*

$$r_{i,i}^2 \leq \alpha^{j-i}\, r_{j,j}^2 \quad \textit{für } 1 \leq i \leq j \leq n.$$

Für $\delta = \frac{3}{4}$, $\alpha = 2$, $i = 1$ gilt $\|\mathbf{b}_1\|^2 = r_{1,1}^2 \leq 2^{j-1}\, r_{j,j}^2$, so dass die $\|\widehat{\mathbf{b}}_j\|^2 = r_{j,j}^2$ für große j nicht beliebig klein werden.

Beweis. Die Eigenschaften einer LLL-Basis implizieren

$$\delta\, r_{k-1,k-1}^2 \leq r_{k-1,k}^2 + r_{k,k}^2 \leq \tfrac{1}{4}\, r_{k-1,k-1}^2 + r_{k,k}^2$$

und somit $\left(\delta - \frac{1}{4}\right) r_{k-1,k-1}^2 \leq r_{k,k}^2$. Durch Induktion über $j - i$ folgt $r_{i,i}^2 \leq \alpha^{j-i}\, r_{j,j}^2$. □

Lemma 4.1.3
Für jede Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *des Gitters* $\mathcal{L}$ *gilt* $\lambda_j(\mathcal{L}) \geq \min\{r_{j,j}, \ldots, r_{n,n}\}$ *für* $j = 1, ..., n$.

Beweis. Es seien $\mathbf{a}_1, \ldots, \mathbf{a}_n \in \mathcal{L}$ linear unabhängig , so dass $\|\mathbf{a}_j\| = \lambda_j(\mathcal{L})$ für $j = 1, \ldots, n$. Sei

$$\mathbf{a}_k = \sum_{i=1}^n t_{i,k}\mathbf{b}_i = \sum_{i=1}^n \bar{t}_{i,k}\widehat{\mathbf{b}}_i \quad \text{für } k = 1, \ldots, n.$$

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

Wegen $\mathbf{b}_i = \sum_{j=1}^i \mu_{i,j}\widehat{\mathbf{b}}_j$ und $\mu_{i,i} = 1$, ist $\bar{t}_{\mu(k),k} = t_{\mu(k),k}$ ganzzahlig. Wegen der linearen Unabhängigkeit der Vektoren $\mathbf{a}_1, \ldots, \mathbf{a}_j$ 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 $\mathbf{a}_1, \ldots, \mathbf{a}_j \in \operatorname{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{j-1})$, so dass $\mathbf{a}_1, \ldots, \mathbf{a}_j$ linear abhängig sind — Widerspruch. Aus $k \leq j$, $\mu(k) \geq j$ folgt

$$\lambda_j^2 \;\geq\; \lambda_k^2 \;=\; \|\mathbf{a_k}\|^2 \;\geq\; \bar{t}_{\mu(k),k}^2\, r_{\mu(k),\mu(k)}^2 \geq r_{\mu(k),\mu(k)}^2 \geq \min\{r_{j,j}^2, ..., r_{n,n}^2\}$$ □

Die untere Schranke zu λ_j in Lemma 4.1.3 gilt für beliebige Basen. Für LLL-reduzierten Basen ist $\|\mathbf{b}_j\|$ grobe Approximation zu λ_j, es gilt nämlich

Satz 4.1.4 (Lenstra, Lenstra, Lovász 1982)
Jede LLL-Basis $\mathbf{b}_1, ..., \mathbf{b}_n$ *mit* δ *des Gitters* $\mathcal{L}$ *erfüllt mit* $\alpha = (\delta - \frac{1}{4})^{-1}$

1. $\alpha^{1-j} \leq r_{j,j}^2/\lambda_j(\mathcal{L})^2$ *für* $j = 1, \ldots, n$,
2. $\|\mathbf{b}_j\|^2/\lambda_j(\mathcal{L})^2 \leq \alpha^{n-1}$ *für* $j = 1, \ldots, n$,
3. $\|\mathbf{b}_k\|^2 \leq \alpha^{j-1}\, r_{j,j}^2$ *für* $k \leq j$.

Beweis. Wir zeigen *1.* und *3.* : Offenbar gibt es ein $k \leq j$ so dass $\lambda_j \leq \|\mathbf{b}_k\|$. Es folgt

$$\begin{aligned}
\lambda_j^2 \leq \|\mathbf{b}_k\|^2 &\leq r_{k,k}^2 + \tfrac{1}{4}\textstyle\sum_{i=1}^{k-1} r_{i,i}^2 \\
&\leq r_{j,j}^2(\alpha^{j-k} + \tfrac{1}{4}\textstyle\sum_{i=1}^{k-1}\alpha^{j-i}) && \text{(nach Lemma 4.1.2)} \\
&= r_{j,j}^2\alpha^{j-1}(\alpha^{1-k} + \tfrac{1}{4}\textstyle\sum_{i=1}^{k-1}\alpha^{1-i}).
\end{aligned}$$

Damit gilt *3.* für alle $k \leq j$ mit $\lambda_j \leq \|\mathbf{b}_k\|$ und somit auch für die $k' \leq j$ mit $\|\mathbf{b}'_k\| \leq \lambda_j$ wegen $\|\mathbf{b}_{k'}\|^2 \leq \|\mathbf{b}_k\|^2 \leq r_{j,j}^2\alpha^{j-1}$. 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

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

Damit sind *1.* und *3.* gezeigt. Nach Lemma 4.1.3 gibt es ein $k \geq j$, so dass $\lambda_j \geq r_{k,k}$. Es folgt

$$\begin{aligned}
\lambda_j^2 \geq r_{k,k}^2 &\geq \alpha^{-k+j}\, r_{j,j}^2 && \text{(wegen Lemma 4.1.2)} \\
&\geq \alpha^{-k+1}\, \|\mathbf{b}_j\|^2 && \text{(wegen 3. Aussage des Satzes mit } k = j) \\
&\geq \alpha^{-n+1}\, \|\mathbf{b}_j\|^2 && \text{(wegen } k \leq n \text{ und } \alpha \geq 1
\end{aligned}$$ □

Korollar 4.1.5
Jede LLL-Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *mit* δ *erfüllt*

1. $\|\mathbf{b}_1\|^2 \leq \alpha^{\frac{n-1}{2}} (\det \mathcal{L})^{\frac{2}{n}}$, *2.* $\prod_{i=1}^n \|\mathbf{b}_i\|^2 \leq \alpha^{\binom{n}{2}} (\det \mathcal{L})^2$.

Beweis. Aus $\prod_{i=1}^n r_{i,i}^2 = (\det \mathcal{L})^2$ und $\|\mathbf{b}_1\|^2 \leq r_{i,i}^2 \, \alpha^{i-1}$ (Lemma 4.1.2) folgt

$$\|\mathbf{b}_1\|^{2n} \leq \alpha^1 \alpha^2 \cdots \alpha^{n-1} \prod_{i=1}^n r_{i,i}^2 = \alpha^{\binom{n}{2}} (\det \mathcal{L})^2$$

und somit $$\|\mathbf{b}_1\|^2 \leq \alpha^{\frac{n-1}{2}} (\det \mathcal{L})^{\frac{2}{n}}.$$

2. folgt aus $\prod_{i=1}^n r_{i,i}^2 = (\det \mathcal{L})^2$ und $\|\mathbf{b}_i\|^2 \leq r_{i,i}^2 \, \alpha^{i-1}$, Satz 4.1.4, *3.* für $k = j = i$. □

Die *relative Dichte* $rd(\mathcal{L})$ des Gitters $\mathcal{L}$ ist definiert durch $\lambda_1^2 = rd(\mathcal{L})^2 \, \gamma_n \, (\det \mathcal{L})^{2/n}$. Aus Satz 4.1.4 und Korollar 4.1.5 folgt

$$\|\mathbf{b}_1\|^2 / \lambda_1^2 \leq \alpha^{\frac{n-1}{2}} / (rd(\mathcal{L})^2 \gamma_n). \tag{4.0}$$

Diese obere Schranke für LLL-Basen ist für $rd(\mathcal{L}) > (\frac{1}{n})^{O(1)}$ deutlich besser als *2.* von Satz 4.1.4.

4.2 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.

4.2.1 LLL-Verfahren

Algorithmus 4.2.1 transformiert eine ganzzahlige Gitterbasis in eine LLL-Basis mit δ desselben Gitters. Der Algorithmus reduziert sukzessive einen möglichst großen Anfangsabschnitt $\mathbf{b}_1, ..., \mathbf{b}_{k-1}$ der Basis. Bei Eintritt in Stufe k ist die Teilbasis $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$ stets LLL-Basis mit δ. Am Ende ist $k = n + 1$ und die gesamte Basis $\mathbf{b}_1, ..., \mathbf{b}_n$ ist LLL-Basis.

Das Verfahren operiert auf Stufe k mit den rationalen Zahlen $\mu_{i,j}$, $r_{i,i}^2$ für $1 \leq i, j \leq k$ und den ganzzahligen Vektoren $\mathbf{b}_1, ..., \mathbf{b}_k$, siehe Lemma 4.2.2. Die Längenreduktion von $\mathbf{b}_k$ 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 $\mu_{k,j}$, $r_{k,k}^2$, siehe Satz 4.2.6. Es bezeichne

$$M := \max(\|\mathbf{b}_1\|^2, ..., \|\mathbf{b}_n\|^2),$$

$$D_i := \det \mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_i)^2 = \det \left[\langle \mathbf{b}_s, \mathbf{b}_t \rangle \right]_{1 \leq s,t \leq i} = \prod_{j=1}^i r_{j,j}^2 \in \mathbb{N}, \tag{4.1}$$

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

Die Gram-Determinante D_i ist die Determinante der Gram-Matrix der Teilbasis $\mathbf{b}_1, ..., \mathbf{b}_i$. 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 $\mathbf{b}_1, ..., \mathbf{b}_{k-1}$ stets LLL-Basist. Dies folgt durch Induktion über die Abfolge der Iterationen. Eine *Iteration* ist die Abfolge der Schritte der WHILE-Schleife bis zur Aktualisierung von k.

Algorithmus 4.2.1 zur LLL-Reduktion in $\mathbb{Z}$-Arithmetik

EINGABE: Basis $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{Z}^{m \times n}$, δ mit $\frac{1}{4} < \delta < 1$

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

2. WHILE $k \leq n$ DO /* $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$ ist stets LLL-reduziert */

berechne $\mu_{k,j} = r_{j,k}/r_{j,j}$ für $j = 1, \ldots, k$ und $r_{k,k}^2$ gemäß Lemma 4.2.2

Längenreduziere $\mathbf{b}_k$, aktualisiere $\mu_{k,1}, \ldots, \mu_{k,k-1}$

IF $\delta\, r_{k-1,k-1}^2 > r_{k-1,k}^2 + r_{k,k}^2$

THEN vertausche $\mathbf{b}_{k-1}$ und $\mathbf{b}_k$ /* *kurz* $\mathbf{b}_{k-1} \leftrightarrow \mathbf{b}_k$ */

IF $k = 2$ THEN aktualisiere $r_{1,1}^2 = \|\mathbf{b}_1\|^2$

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

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

AUSGABE: LLL-Basis $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n]$.

Lemma 4.2.1
Die LLL-Reduktion führt zu gegebener ganzzahligen Basis $\mathbf{b}_1, ..., \mathbf{b}_n \in \mathbb{Z}^m$ höchstens $\log_{1/\delta}\left(D^{Start}\right) \leq n \log_{1/\delta} \overline{M}$ Austausche $\mathbf{b}_{k-1} \leftrightarrow \mathbf{b}_k$ durch.

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

$$D^{\text{Start}} \geq D^{\text{Ende}}\, (1/\delta)^{\#\text{Austausche}} \geq (1/\delta)^{\#\text{Austausche}}. \tag{4.2}$$

Die Gitter $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_i)$ mit $i \neq k-1$ werden beim Austausch $\mathbf{b}_{k-1} \leftrightarrow \mathbf{b}_k$ nicht verändert. Die Determinanten D_i mit $i \neq k-1$ bleiben erhalten. Im LLL-Verfahren wird nur ausgetauscht wenn

$$\delta\, r_{k-1,k-1}^2 \;>\; r_{k-1,k}^2 + r_{k,k}^2.$$

Wegen $D_{k-1} = \prod_{i=1}^{k-1} r_{i,i}^2$ bewirkt der Austausch $\mathbf{b}_{k-1} \leftrightarrow \mathbf{b}_k$, dass

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

Nach (4.2) 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 $\#\text{Austausche} \leq (n-1) \log_{1/\delta} \overline{M}$. □

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

Lemma 4.2.2
Die Berechnung von $\mu_{k,1}, ..., \mu_{k,k}$ und $r_{k,k}^2$, sowie die Längenreduktion von $\mathbf{b}_k$ auf Stufe k gehen in $\mathcal{O}(k\, m)$ arithmetischen Schritten.

Beweis. Die $\mu_{k,j} = r_{j,k}/r_{j,j}$ für $j = 1, ..., k$ und $r_{k,k}^2$ werden durch folgende $\mathcal{O}(k\, m)$ Schritte berechnet

FOR $j = 1, \ldots, k-1$ DO $\mu_{k,j} := (\langle \mathbf{b}_k, \mathbf{b}_j \rangle - \sum_{i=1}^{j-1} \mu_{k,i}\, \mu_{j,i}\, r_{i,i}^2)/r_{j,j}^2$,

$\mu_{k,k} := 1, \qquad r_{k,k}^2 := \langle \mathbf{b}_k, \mathbf{b}_k \rangle - \sum_{j=1}^{k-1} \mu_{k,j}^2 r_{j,j}^2$.

Die Längenreduktion von $\mathbf{b}_k$ geht mit folgenden $\mathcal{O}(k\,m)$ Schritten

FOR $j = k-1, ..., 1$ DO $\quad \mathbf{b}_k := \mathbf{b}_k - \lceil \mu_{k,j} \rfloor \mathbf{b}_j, \quad \mu_{k,i} := \mu_{k,i} - \lceil \mu_{k,j} \rfloor \mu_{j,i} \quad$ für $i = 1, ..., k$. $\quad \square$

Aufgrund von Lemma 4.2.1 und 4.2.2 führt das LLL-Verfahren höchstens $\mathcal{O}(n^2 m \log_{1/\delta} \overline{M})$ arithmetischen Schritte aus, siehe Satz 4.2.6. 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 $\mu_{j,i},\ r_{i,i}^2$ während der LLL-Reduktion ab.

Lemma 4.2.3
Für jede ganzzahlige Eingabebasis $\mathbf{b}_1, ..., \mathbf{b}_n \in \mathbb{Z}^m$ gilt 1. $D_{i-1}\,\widehat{\mathbf{b}}_i \in \mathbb{Z}^m$, 2. $D_j\,\mu_{i,j} \in \mathbb{Z}$.

Beweis. 1. Aus $[\mathbf{b}_1, ..., \mathbf{b}_n] = [\widehat{\mathbf{b}}_1, \ldots, \widehat{\mathbf{b}}_n]_{1 \le i,j \le n}\ [\mu_{i,j}]^{\mathsf{T}}_{1 \le i,j \le n}$ folgt für $[\nu_{i,j}] := [\mu_{i,j}]^{-1}$: dass

$$[\widehat{\mathbf{b}}_1, \ldots, \widehat{\mathbf{b}}_n] \ = \ [\mathbf{b}_1, ..., \mathbf{b}_n]\,[\nu_{i,j}]^{\mathsf{T}}_{1 \le k,j \le n}.$$

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

$$-\langle \mathbf{b}_i, \mathbf{b}_j \rangle = \sum_{t=1}^{i-1} \nu_{i,t}\,\langle \mathbf{b}_t, \mathbf{b}_j \rangle \qquad\qquad \text{für } j = 1, 2, \ldots, i-1.$$

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

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

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

2. Wegen $D_j = \prod_{i=1}^{j} r_{i,i}^2$ gilt

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

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

Lemma 4.2.4
Auf Stufe k des LLL-Verfahrens gilt stets

1. $\|\mathbf{b}_i\|^2 \le \frac{i+3}{4}\,M$ *für $i = 1, \ldots, k$,*
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 $\mathbf{b}_k$ auf Stufe k die Längen der Basisvektoren unverändert. Nach der Längenreduktion von $\mathbf{b}_k$ gilt

$$\|\mathbf{b}_k\|^2 = \textstyle\sum_{j=1}^{k} \mu_{k,j}^2 r_{j,j}^2 \le r_{k,k}^2 + \frac{k-1}{4} \max(\, r_{1,1}^2, ..., r_{k-1,k-1}^2\,) \le \frac{k+3}{4}\ M.$$

Denn im LLL-Verfahren gilt stets $\max_i r_{i,i}^2 \le M := \max(\, \|\mathbf{b}_1\|^2, ..., \|\mathbf{b}_n\|^2\,)$. Für jeden Austausch $\mathbf{b}_{k-1} \leftrightarrow \mathbf{b}_k$ gilt nämlich $(r_{k-1,k-1}^{\text{neu}})^2 \le \delta\,(r_{k-1,k-1}^{\text{alt}})^2, \quad (r_{k,k}^{\text{neu}})^2 \le (r_{k-1,k-1}^{\text{alt}})^2$.

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

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

Weil $\mathbf{b}_1, ..., \mathbf{b}_{k-1}$ LLL-reduziert ist, gilt

$$\begin{aligned} |\mu_{i,j}|^2 &\le \tfrac{i+3}{4}\, M\, r_{j,j}^{-2} && \text{(wegen } \|\mathbf{b}_i\|^2 \le \tfrac{i+3}{4} M\text{)} \\ &\le \tfrac{i+3}{4}\, M\, \alpha^{j-1}\, r_{1,1}^{-2} && \text{(nach Lemma 4.1.2)} \\ &\le \tfrac{i+3}{4}\, M\, \alpha^{j-1} && \text{(weil } \|\mathbf{b}_1\|^2 = r_{1,1}^2 \in \mathbb{Z}\text{).} \end{aligned}$$

□

Lemma 4.2.5
Während der Längenreduktion von $\mathbf{b}_k$ 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

$$\mathbf{b}_k := \mathbf{b}_k - \lceil \mu_{k,i} \rfloor \, \mathbf{b}_i \qquad \text{für } i < k$$

der Längenreduktion wird begleitet von

$$\mu_{k,j} := \mu_{k,j} - \lceil \mu_{k,i} \rfloor \underbrace{\mu_{i,j}}_{|\mu_{i,j}| \le 1/2} \qquad \text{für } j = 1, 2, ..., k-1. \tag{4.3}$$

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

$$M_k^{\text{neu}} \le M_k^{\text{alt}} + \tfrac{1}{2}\left(M_k^{\text{alt}} + \tfrac{1}{2}\right) \le \tfrac{3}{2}\, M_k^{\text{alt}} + \tfrac{1}{4} \tag{4.4}$$

Nach Lemma 4.2.4 gilt vor der Längenreduktion von $\mathbf{b}_k$ dass

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

Wegen (4.4) erhöht sich die Größe M_k während der Längenreduktion von $\mathbf{b}_k$ 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 4.2.6
Zu gegebener ganzzahliger Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Z}^m$ liefert Algorithmus 4.2.1 eine LLL-Basis. Mit $\overline{M} := \max_i(\|\mathbf{b}_i\|^2, D_i)$ macht der Algorithmus höchstens $\mathcal{O}(n^2 m \log_{1/\delta} \overline{M})$ arithmetische Schritte auf den Koordinaten der $\mathbf{b}_i$ und den rationalen Zahlen $\mu_{i,j}, r_{i,i}^2$. Die Bitlänge der auftretenden ganzen Zahlen, insbesondere der Zähler und Nenner von $\mu_{i,j}, r_{i,i}^2$ ist höchstens $\mathcal{O}(n + \log_2 \overline{M})$.

Beweis. Nach Lemma 4.2.1 gilt

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

Die LLL-Reduktion beginnt mit Stufe $k = 2$ und endet mit Stufe $k = n+1$. Jeder Austausch erniedrigt die Stufe k gemäß $k := \min(k-1, 2)$. Jede Stufenerniedrigung wird durch eine Stufenerhöhung ohne Austausch ausgeglichen. Es folgt

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

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 4.2.3, 4.2.4 und 4.2.5 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 $r_{j,j}^2 = \frac{D_j}{D_{j-1}}$ 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 $\mathbf{b}_{k-1} \leftrightarrow \mathbf{b}_k$ kann man die Gram-Schmidt-Koeffizienten $\mu_{k-1,1}, ..., \mu_{k-1,k-2}$, sowie $r_{k-1,k-1}^2$ schnell aktualisieren. Dies erfordert nur $\mathcal{O}(1)$ Rechenschritte und $\mathcal{O}(k)$ Datentransporte während die Neuberechnung nach Lemma 4.2.2 $\mathcal{O}(k\,m)$ Rechenschritte erfordert.

Lemma 4.2.7
Der Austausch $\mathbf{b}_{k-1} \leftrightarrow \mathbf{b}_k$ *bewirkt mit* $\mu := \mu_{k,k-1}$ *dass*

1. $\mu_{\text{neu}} \;=\; \mu\, \dfrac{r_{k-1,k-1}^2}{(r_{k-1,k-1}^{\text{neu}})^2} \qquad \textit{mit } (r_{k-1,k-1}^{\text{neu}})^2 = \mu^2 r_{k-1,k-1}^2 + r_{k,k}^2,$

2. $[\mu_{k,i}^{\text{neu}}\,,\, \mu_{k-1,i}^{\text{neu}}] \;=\; [\mu_{k-1,i}\,,\, \mu_{k,i}] \quad \textit{für } i = 1, \ldots, k-2.$

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

4.3 LLL-Reduktion ganzzahliger Erzeugendensysteme

Wir erweitern die LLL-Reduktion auf ganzzahlige Erzeugendensysteme $\mathbf{b}_1, ..., \mathbf{b}_n \in \mathbb{Z}^m \setminus 0$. Es genügt, die im LLL-Verfahren entstehenden Nullvektoren zu eliminieren. Der Nullvektor kann nur durch Längenreduktion von $\mathbf{b}_k$ auf Stufe k entstehen.

Korrektheit. Algorithmus 4.3.1 operiert auf Stufe k mit den rationalen Zahlen $\mu_{i,j}, r_{i,i}^2$ für $i, j \leq k$ und den ganzzahligen Basisvektoren. Das Verfahren ist korrekt, weil die Vektoren $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$ auf Stufe k stets linear unabhängig und somit LLL-reduziert sind. Sind nämlich nach der Längereduktion von $\mathbf{b}_k$ die Vektoren $\mathbf{b}_1, \ldots, \mathbf{b}_k$ erstmals linear abhängig, so gilt $\mathbf{b}_k \in \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{k-1})$. Die Längenreduktion von $\mathbf{b}_k$ erzeugt den Nullvektor. Dieser wird sofort entfernt.

Algorithmus 4.3.1 LLL-Reduktion von ganzzahligen Erzeugendensystemen

EINGABE: Erzeugendensystem $\mathbf{b}_1, ..., \mathbf{b}_n \in \mathbb{Z}^m \setminus \{0\}$, δ mit $\frac{1}{4} < \delta < 1$
/* $\mathcal{L} := \sum_{i=1}^{n} \mathbf{b}_i\mathbb{Z}$ ist ein Gitter */

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

2. WHILE $k \leq n$ DO

/* $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$ ist LLL-reduziert */

berechne $\mu_{k,j}$ für $j = 1, \ldots, k$ und $r_{k,k}^2$ gemäß Lemma 4.2.2

Längenreduziere $\mathbf{b}_k$, aktualisiere $\mu_{k,1}, \ldots, \mu_{k,k-1}$

IF $\mathbf{b}_k = \mathbf{0}$ THEN entferne $\mathbf{b}_k$ aus dem Erzeugendensystem, $n := n - 1$ RETURN

IF $\delta\, r_{k-1,k-1}^2 > r_{k-1,k}^2 + r_{k,k}^2$

THEN vertausche $\mathbf{b}_{k-1}$ und $\mathbf{b}_k$ /* *kurz* $\mathbf{b}_{k-1} \leftrightarrow \mathbf{b}_k$ */

IF $k = 2$ THEN aktualisiere $r_{1,1}^2$

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

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

AUSGABE: LLL-Basis $\mathbf{b}_1, ..., \mathbf{b}_n$ des Gitters $\mathcal{L}$.

Laufzeitanalyse. Zu den Teilgittern $\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_i) = \sum_{j=1}^{i} \mathbf{b}_j\mathbf{Z}$ und den Gram-Determinanten $D_i = (\det \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_i))^2$ setzt man wieder

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

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

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 4.2.6. Insbesondere gelten die Zahlen-Schranken von Lemma 4.2.3 4.2.4 und 4.2.5 auch für die Werte im Verlauf von Algorithmus 4.3.1. Somit gilt der

Satz 4.3.1
Zu gegebenen ganzzahligen Vektoren $\mathbf{b}_1, ..., \mathbf{b}_n \in \mathbb{Z}^m \setminus 0$ liefert Algorithmus 4.3.1 eine LLL-reduzierte Basis des von $\mathbf{b}_1, ..., \mathbf{b}_n$ erzeugten Gitters. Mit $\overline{M} := \max_i(\|\mathbf{b}\|^2, D_i)$ macht das LLL-Verfahren höchstens $\mathcal{O}(n^2 m \log_{1/\delta} \overline{M})$ arithmetische Schritte auf den Koordinaten der $\mathbf{b}_i$ und den rationalen Zahlen $\mu_{i,j}, r_{i,i}^2$. Die Bitlänge der auftretenden ganzen Zahlen, insbesondere der Zähler und Nenner von $\mu_{i,j}, r_{i,i}^2$ ist höchstens $\mathcal{O}(n + \log_2 \overline{M})$.

4.4 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 $\mathbf{b}_1, \ldots, \mathbf{b}_n$ wird in exakter Arithmetik durchgeführt. Für die Rechnung auf den rationalen Zahlen $\mu_{i,j}, r_{i,i}^2$ für $i, j \leq k$ genügen dagegen gute Näherungen in Gleitkomma-Arithmetik.

Definition 4.4.1 (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 4.2.1 für den Fall, dass alle rationalen Zahlen $\mu_{i,j}, r_{j,j}^2$ mit relativem Fehler ε berechnet werden. Dann führt die Längenreduktion des Vektors $\mathbf{b}_k$ 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 4.4.2
Haben bei der LLL-Reduktion mit δ die rationalen Zahlen $\|\pi_{k-1}(\mathbf{b}_{k-1})\|^2, \|\pi_{k-1}(\mathbf{b}_k)\|^2$ bei der Entscheidung über den Austausch $\mathbf{b}_{k-1} \leftrightarrow \mathbf{b}_k$ stets relativen Fehler $\leq \varepsilon$, dann ist die Ausgabebasis LLL-reduziert mit $\delta_- := \delta(1-\varepsilon)/(1+\varepsilon)$. Die Anzahl der Austausche $\mathbf{b}_{k-1} \leftrightarrow \mathbf{b}_k$ 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 $\mathbf{b}_{k-1} \leftrightarrow \mathbf{b}_k$. Dann gilt $\delta_- \|\pi_{k-1}(\mathbf{b}_{k-1})\|^2 > \|\pi_{k-1}(\mathbf{b}_k)\|^2$. Für die Näherungen mit relativem Fehler $\leq \varepsilon$ folgt — es bezeichnet stets f' eine Näherung zu f:

$$\delta_-(1+\varepsilon)\|\pi_{k-1}\mathbf{b}\|'^2 > \|\pi_{k-1}(\mathbf{b}_k)\|'^2(1-\varepsilon).$$

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

Wir zeigen, dass die LLL-Reduktion mit Näherungen abbricht sofern $\delta_+ := \delta(1+\varepsilon)/(1-\varepsilon) < 1$. Es folgt nämlich ein Austausch $b_{k-1} \leftrightarrow b_k$ mit δ und Näherungen, dann gilt

$$\delta\|\pi_{k-1}(\mathbf{b}_{k-1})\|'^2 > \|\pi_{k-1}(\mathbf{b}_k)\|'^2$$

und somit $\delta(1+\varepsilon)\|\pi_{k-1}(\mathbf{b}_{k-1})\|^2 > \|\pi_{k-1}(\mathbf{b}_k)\|^2(1-\varepsilon)$. Dann wird D_{k-1} beim Austausch $\mathbf{b}_{k-1} \leftrightarrow \mathbf{b}_k$ 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 4.4.2 gilt es bei der LLL-Reduktion mit Gleitkomma-Zahlen $\mu_{i,j}, r_{j,j}$ den relativen Fehler zu begrenzen. Wichtigste Punkte dabei sind

1. War vor der Längenreduktion von $\mathbf{b}_k$ 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 4.2.2.

2. Bei der Neuberechnung von $\mu_{k,j}$ gemäß Lemma 4.2.2 rechnet man $\langle \mathbf{b}'_k, \mathbf{b}'_j \rangle$ in Gleitkomma. Im Falle dass $|\mathbf{b}_k, \mathbf{b}_j\rangle| \approx 2^{-m}\|\mathbf{b}_k\|\|\mathbf{b}_j\|$, gehen dabei m Präzisionsbits verloren. Ist m zu groß, rechnet man besser $\langle \mathbf{b}_k, \mathbf{b}_j \rangle$ exakt.

Mit diesen Maßnahmen haben Schnorr, Euchner [SE94] 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 4.2.4 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 $\mu_{i,j}$, $r_{j,j}^2$ mit $1 \leq j \leq i \leq k$ nach den Formeln von Lemma 4.2.2. Diese sind geeignet für das Rechnen mit

[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.

Gleitkommazahlen $\mu_{i,j}, r^2_{j,j}$. Weil die Basis $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$ stets LLL-reduziert ist, gilt nach Lemma 4.1.2

$$r^2_{j,j} \geq \|/mathbf{b}_1\|^2 \, \alpha^{1-j} \qquad \text{für } j = 1, \ldots, k-1.$$

Die Divisoren $r^2_{j,j}$ bei der Berechnung von $\mu_{k,j}$ gemäß Lemma 4.2.2 sind daher nicht beliebig klein. Dies ist wichtig für die Begrenzung von Gleitkommafehlern.

4.5 LLL-Reduktion mit ganzzahliger Gram-Matrix

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

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

$$\begin{aligned} \langle \mathbf{b}_k, \mathbf{b}_i \rangle &:= \langle \mathbf{b}_k, \mathbf{b}_i \rangle - \mu \langle \mathbf{b}_j, \mathbf{b}_i \rangle \quad \text{für } i = 1, \ldots, n, i \neq k \\ \langle \mathbf{b}_k, \mathbf{b}_k \rangle &:= \langle \mathbf{b}_k, \mathbf{b}_k \rangle - 2\mu \langle \mathbf{b}_k, \mathbf{b}_j \rangle + \mu^2 \langle \mathbf{b}_j, \mathbf{b}_j \rangle \end{aligned}$$

Die Aktualisierung von $\mathbf{B}^\top\mathbf{B}$ bei der Längenreduktion von $\mathbf{b}_k$ geht in $O(kn)$ arithmetischen Schritten.

Aktualisierung von T. Die Aktualisierung von $\mathbf{T} = [t_{i,j}]_{1 \leq i,j \in n}$ beim Schritt $\mathbf{b}_k := \mathbf{b}_k - \mu\,\mathbf{b}_j$ 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 $\mathbf{T}$ bei der Längenreduktion von $\mathbf{b}_k$ in $\mathcal{O}(kn)$ arithmetischen Schritten. Beim Austausch $\mathbf{b}_{k-1} \leftrightarrow \mathbf{b}_k$ werden $\mathbf{B}^\top\mathbf{B}$ und $\mathbf{T}$ durch $\mathcal{O}(n)$ Datentransporte aktualisiert, indem $\mathcal{O}(n)$ Einträge in $\mathbf{B}^\top\mathbf{B}$ und $\mathbf{T}$ getauscht werden. Damit kostet eine Iteration der LLL-Reduktion $\mathcal{O}(n^2)$ Schritte und es folgt der

Satz 4.5.1
Zu gegebener ganzzahliger Gram-Matrix $\mathbf{B}^\top\mathbf{B} \in \mathbb{Z}^{n \times n}$ geht die LLL-Reduktion gemäß Alg. 4.2.1 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 $\mathbf{B} \in \mathbb{Z}^{m \times n}$ mit $m >> n$ ist es wegen Satz 4.5.1 günstig, vorweg $\mathbf{B}^\top\mathbf{B}$ 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 4.2.1.

4.6 LLL-Basen mit großem Approximationsfaktor

Wir konstruieren LLL-Basen mit großem Approximationsfaktor $\|\mathbf{b}_1\| / \lambda_1$, vergleiche Satz 4.1.4.

Satz 4.6.1
Jede Gitterbasis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ mit $|\mu_{i,j}| = |r_{j,i}/r_{i,i}| \leq \frac{1}{2}$ und $|\mu_{i+1,i}|^2 \geq \frac{1}{12}$ für $1 \leq i < j \leq n$ und

$$r^2_{i+1.i+1} = r^2_{i,i} \cdot (1 - \mu^2_{i+1,i}) \qquad \textit{für } i = 1, \ldots, n-1 \tag{4.5}$$

ist eine LLL-Basis mit $\gamma_n \|\mathbf{b}_1\|^2 \geq \lambda_1^2 \left(\frac{12}{11}\right)^{\frac{n-1}{2}}$.

Beweis. Die Basis ist LLL-reduziert mit $\delta = 1$, weil nach (4.5):

$$r_{i,i}^2 = r_{i+1,i+1}^2 + \mu_{i+1,i}^2 r_{i,i}^2$$

Es folgt: $\lambda_1^2 \leq \gamma_n (\det \mathcal{L})^{\frac{2}{n}} = \gamma_n \prod_{i=1}^n r_{i,i}^{\frac{2}{n}} = \gamma_n \|\mathbf{b}_1\|^2 \prod_{i=1}^{n-1} (1 - \mu_{i+1,i}^2)^{\frac{n-i}{n}}$

und somit für $|\mu_{i+1,i}|^2 \geq 1/12$:

$$\|\mathbf{b}_1\|^2 / \lambda_1^2 \geq \left(\tfrac{12}{11}\right)^{\frac{1}{n}\sum_{i=1}^{n-1} i} / \gamma_n \geq \left(\tfrac{12}{11}\right)^{\frac{1}{n}\binom{n}{2}} / \gamma_n = \left(\tfrac{12}{11}\right)^{\frac{n-1}{2}} / \gamma_n.$$

■

Beachte, für zufällige $\mu_{i+1,i} \in_R [-\frac{1}{2}, +\frac{1}{2}]$ ist der Erwartungswert von $\mu_{i+1,i}^2$ gerade $\frac{1}{12}$. Damit ist der Approximationsfaktor $\|\mathbf{b}_1\| / \lambda_1$ für zufällige LLL-Basen im Mittel $\Theta(\frac{12}{11}^{\frac{n-1}{2}} / n)$.

Kapitel 5

Lösen von Subsetsum-Problemen durch kurze Gittervektoren

Wir lösen fast alle Subsetsum-Probleme kleiner Dichte d durch Vektoren der Länge λ_1 des Lagarias-Odlyzko-Gitters und dann des CJLOSS-Gitter. Im CJLOSS-Gitter entsprechen Lösungen des Subsetsum-Problems besonders kurzen Gittervektoren. Die Lösung gelingt für fast alle Subsetsum-Probleme der Dichte kleiner 0.9408 und für Dimension $n \leq 80$ in der Praxis sogar effektiv durch LLL-Reduktion. Fast alle CJLOSS-Gitter für Subsetsum-Probleme der Dichte $d < 0.9408$ haben eine Packungsdichte $\triangle$ mit $\frac{1}{n}\log_2 \triangle \geq -1.0158$ für hinreichend grosse Dimension n.

5.1 Das Subsetsum-Problem

Definition 5.1.1 (Subsetsum-Problem, oder Knapsack- bzw. Rucksack-Problem.)

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

Nach Satz 12.2.5 auf Seite 105 ist das Subsetsum-Entscheidungsproblem $\mathcal{NP}$-vollständig, sogar für beliebig kleine Dichte d.

Annahmen. Der Gewichtsvektor $(a_1, \ldots, a_n)$ variiere über $[1, A]^n \subset \mathbb{N}^n$ für ein beliebiges $A \in \mathbb{N}$. Es wird die Existenz einer Lösung $\mathbf{e} = (e_1, \ldots, e_n) \in \{0,1\}^n$ vorausgesetzt.

Die Wahrscheinlichkeiten und die „fast alle"-Aussagen in diesem Kapitel beziehen sich auf zufällig gewählte $(a_1, \ldots, a_n) \in_R [1, A]^n$.

Definition 5.1.2 (Inverses Subsetsum-Problem)
Im inversen Problem wird s *durch* $\overline{s} := t - s$ *mit* $t = \sum_{i=1}^{n} a_i$ *ersetzt.*

Jede Lösung $\mathbf{e}$ des Ausgangsproblems liefert eine Lösung $\overline{\mathbf{e}}$ des inversen Problems und umgekehrt:

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

Eine der beiden Lösungen $\mathbf{e}$, bzw $\overline{\mathbf{e}}$ hat höchstens $n/2$ Einsen.

Wir lösen das Subsetsum-Problem durch ein **SVP**-Orakel welches zur Basis des Gitters $\mathcal{L}$ einen Gittervektor der Länge λ_1 in Euklidischer Norm liefert. Wir zeigen, daß das **SVP**-Orakel für fast alle $(a_1, ..., a_n) \in [1, A]^n$entweder das gegebene Subsetsum-Problem oder sein inverses löst. Die Wahrscheinlichkeit eines Misserfolgs wird für zufällige $(a_1, ..., a_n) \in [1, A]^n$ mit wachsendem n

beliebig klein, wenn nur die Dichte d hinreichend klein ist.

Dichte d des Subsetsum-Problems

$$d := \frac{n}{\log_2(\max\limits_{i=1,\ldots,n} a_i)} \quad \text{und somit} \quad \max_{i=1,\ldots,n} a_i = 2^{n/d}.$$

Für Dichte $d \gg 1$ gibt es bei zufälliger Wahl der Gewichte $a_1, \ldots, a_n$ "in der Regel" viele Lösungen. Am schwierigsten gelten zufällige Subsetsum-Probleme mit Dichte nahe bei 1.

In kleiner Dimension n findet man einen kürzesten Gittervektor durch Gitterbasenreduktion siehe [SH95, SE94]. Dies führt zu Angriffen auf Krypto-Schemata, die auf Subsetsum-Problemen basieren. C.P. Schnorr und H.H. Hörner [SH95] haben das Chor-Rivest-System [CR88] mittels Gitterreduktion angegriffen.

5.2 Die Lagarias-Odlyzko-Gitterbasis

J.C. Lagarias und A.M. Odlyzko [LaOd85] schlagen die folgende Gitterbasis $\mathbf{B}$ vor um das Subsetsum-Problem durch ein **SVP**-Orakel zu $\mathcal{L}(\mathbf{B})$ zu lösen. Die letzte Zeile von $\mathbf{B}$ wird von uns zur Beweisvereinfachung hinzugefügt. Wir überarbeiten die Darstellung von [CJLOSS92].

$$\mathbf{B} = [\mathbf{b}_1, \cdots, \mathbf{b}_{n+1}] := \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & & 1 & 0 \\ Na_1 & Na_2 & \cdots & Na_n & Ns \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \in \mathbb{Z}^{(n+2)\times(n+1)} \tag{5.1}$$

und $\mathcal{L}(\mathbf{B}) = \mathcal{L}_{LO}$ sei das zugehörige Gitter. Die Lösung $\mathbf{e} \in \{0,1\}^n$ von $\sum_{i=1}^n x_i e_i = s$ liefert den Lösungsvektor

$$\widehat{\mathbf{e}} := \left(\sum_{i=1}^n e_i \mathbf{b}_i\right) - \mathbf{b}_{n+1} = (e_1, \ldots, e_n, 0, -1)^t \in \mathcal{L}_{\mathrm{LO}}. \tag{5.2}$$

Entweder $\mathbf{e}$ oder $\overline{\mathbf{e}} = \mathbf{1} - \mathbf{e}$, die Lösung zum inversen Subsetsum-Problem, hat höchstens $n/2$ Einsen und liefert damit einen Lösungsvektor in $\mathcal{L}_{\mathrm{LO}}$ der Länge $\leq \sqrt{n/2+1}$. Für jeden Vektor $\widehat{\mathbf{x}} = (x_1, ..., x_{n+1}, -y) \in \mathcal{L}_{LO}$ mit $\|\widehat{\mathbf{x}}\| = \lambda_1$ gilt somit für $N \geq \sqrt{n/2}$: $\sum_{i\neq n+1} |x_i| \geq 2,\ x_{n+1} = 0$.

Satz 5.2.1
Für $n > n_0$ und $N \geq \sqrt{n/2}$ werden fast alle lösbare Subsetsum-Probleme zu $(a_1, \ldots, a_n) \in [1, A]^n$ der Dichte $d < 0.6463$ durch jeden Vektor der Länge λ_1 von $\mathcal{L}_{LO}$ für s oder $\overline{s} = t - s$ gelöst.

Beweis. Sei $\|\mathbf{e}\|^2 \leq n/2$. Das **SVP**-Orakel liefere den Gittervektor $\widehat{\mathbf{x}} := \sum_{i-1}^n x_i \mathbf{b}_i - y\mathbf{b}_{n+1}$ der Länge λ_1 mit $y \geq 0$. Löst $\widehat{\mathbf{x}}$ das Subsetsum-Problem nicht so gilt

$$\|\widehat{\mathbf{x}}\| = \lambda_1 \leq \sqrt{n/2+1}, \qquad \widehat{\mathbf{x}} \neq \widehat{\mathbf{e}}. \tag{5.3}$$

Wir analysieren die Wahrscheinlichkeit des Misserfolgs

$$P(n) := \mathrm{Ws}[\text{Es existiert ein } \widehat{\mathbf{x}} \in \mathcal{L}_{CJLOSS} \text{ mit (5.3)}]$$

bezüglich zufälliger $(a_1, \ldots, a_n) \in_R [1, A]^n$. Für $N \geq \sqrt{n/2}$ wurde oben gezeigt dass $x_{n+1} = 0$ und somit $\sum_{i=1}^n a_i x_i = ys$. Offenbar gilt $0 \leq y < \lambda_1 \leq \sqrt{n/2+1}$. Wir setzen $\mathbf{x} := (x_1, ..., x_n)$. Dann gilt

$$P(n) \leq \mathrm{Ws}\left[\begin{array}{l} \exists \mathbf{x} \in \mathbb{Z}^n,\ \mathbf{x} \notin \{\mathbf{0}, \pm\mathbf{e}\},\ \|\mathbf{x}\| \leq \|\mathbf{e}\| \\ \exists y \in \mathbb{Z} :\ 0 \leq y < \sqrt{n/2+1}, \quad \sum_{i=1}^n a_i(x_i - e_i y) = 0 \end{array}\right]$$

$$\leq \overbrace{\mathrm{Ws}\left[\sum_{i=1}^n a_i(x_i - e_i y) = 0 \ \text{ für feste } \mathbf{e},\ \mathbf{x}, y \text{ mit } \|\mathbf{x}\| \leq \|\mathbf{e}\|,\ \mathbf{x} \neq \mathbf{e},\ 0 \leq y < \sqrt{n/2+1}\right]}^{\text{Faktor 1}}$$
$$\cdot \underbrace{\left|\left\{\mathbf{x} \in \mathbb{Z}^n \ :\ \|\mathbf{x}\| \leq \sqrt{n/2}\right\}\right|}_{\text{Faktor 2}} \cdot \underbrace{\left|\left\{y \in \mathbb{Z} \ :\ 0 \leq y < \sqrt{n/2+1}\right\}\right|}_{\text{Faktor 3}}$$

Wir schätzen die drei Faktoren nach oben ab:

1. Für feste $e_1, ..., e_n, x_1, ..., x_n, y$ ist die Gleichung $\sum_{i=1}^{n} a_i(x_i - e_i y) = 0$ höchstens mit Wahrscheinlichkeit n/A erfüllt, denn falls $x_i \neq e_i y$ ist a_i durch die a_j mit $j \neq i$ bestimmt.

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

$$\left|\left\{\mathbf{x} \in \mathbb{Z}^n \ : \ \|\mathbf{x}\| \leq \sqrt{n/2}\ \right\}\right| \leq 2^{c_0 n} \qquad \text{mit } c_0 = 1.54725$$

3. Es gilt: $\left|\left\{y \in \mathbb{Z} \ : \ 0 \leq y < \sqrt{n/2+1}\ \right\}\right| \leq \sqrt{n/2+1}.$

Damit folgt $P(n) \leq \frac{2^{c_0 n}}{A}\, n\, \sqrt{n/2+1}.$ Wegen $1/d > 1.547269 > c_0$ und $\max_{i=1,...,n} a_i = 2^{n/d}$ gilt $A \geq \max\limits_{i=1,...,n} a_i \geq 2^{n/d}$ und somit $\lim\limits_{n\to\infty} P(n) = 0$ für $d < 0.6463$. ■

5.3 Das CJLOSS-Gitter

M.J. Coster, A. Joux, B.A. LaMacchina, A.M. Odlyzko, C.P. Schnorr und J. Stern [CJLOSS92] ersetzen den Vektor $\mathbf{b}_{n+1}$ der Basis (5.1) durch $\mathbf{b}'_{n+1} := (\frac{1}{2}, \ldots, \frac{1}{2}, Ns, 1)^t$ und erhöhen damit die Grenzdichte von $0,6463$ auf $0,9408$. Die CJLOSS-Basis ist

$$\mathbf{B}' = [\mathbf{b}_1, \cdots, \mathbf{b}_n, \mathbf{b}'_{n+1}] := \begin{bmatrix} 1 & 0 & \cdots & 0 & \frac{1}{2} \\ 0 & 1 & & 0 & \frac{1}{2} \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & & 1 & \frac{1}{2} \\ Na_1 & Na_2 & \cdots & Na_n & Ns \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \in \tfrac{1}{2}\,\mathbb{Z}^{(n+2)\times(n+1)} \tag{5.4}$$

und $\mathcal{L}_{\text{CJLOSS}} = \mathcal{L}(\mathbf{B}')$ sei das zugehörige Gitter. Die letzte Zeile von $\mathbf{B}'$ dient der Beweisvereinfachung. Die Lösung $\mathbf{e} \in \{0,1\}^n$ des Subsetsum-Problems liefert den Lösungsvektor

$$\widehat{\mathbf{e}}' := \textstyle\sum_{i=1}^{n} e_i \mathbf{b}_i - \mathbf{b}'_{n+1} = (e_1 - \frac{1}{2}, e_2 - \frac{1}{2}, \ldots, e_n - \frac{1}{2}, 0, -1)^t \in \mathcal{L}_{CJLOSS} \tag{5.5}$$

Offenbar gilt $\|\widehat{\mathbf{e}}'\| = \sqrt{n/4+1}$ und damit ist der Lösungsvektor $\widehat{\mathbf{e}}'$ der CJLOSS-Basis bis zu einem Faktor $\sqrt{2}$ kleiner als der Lösungsvektor $\widehat{\mathbf{e}}$ der Lagarias-Odlyzko-Basis.

Satz 5.3.1
Für $n > n_0$ und $N \geq \sqrt{n/4}$ werden fast alle lösbare Subsetsum-Probleme zu $(a_1, \ldots, a_n)^t \in [1, A]^n$ der Dichte $d < 0.9408$ durch jeden Vektor der Länge λ_1 von $\mathcal{L}_{CJLOSS}$ gelöst.

Beweis. Das **SVP**-Orakel liefere $\widehat{\mathbf{x}}' = \sum_{i=1}^{n} y_i \mathbf{b}_i - y\mathbf{b}'_{n+1} = (x_1, ..., x_{n+2})^t \in \mathcal{L}_{\text{CJLOSS}}$ mit $y \geq 0$. Bei Misserfolg gilt

$$\|\widehat{\mathbf{x}}'\| = \lambda_1 \leq \|\widehat{\mathbf{e}}'\| = \sqrt{n/4+1}, \qquad \widehat{\mathbf{x}}' \neq \widehat{\mathbf{e}}', \qquad 0 \leq y < \lambda_1 \tag{5.6}$$

Beh.: $x_{n+1} = N(\sum_{i=1}^{n} a_i y_i - ys) = 0$.
Denn aus $x_{n+1} \neq 0$ und $N \geq \sqrt{n/4}$ und weil offenbar $x_i \neq 0$ für zwei $i \neq n+1$ folgt $\|\widehat{\mathbf{x}}'\|^2 > \frac{n}{4} + 1$, ein Widerspruch. Ferner gilt:

$$x_i = y_i - \tfrac{1}{2} y \qquad \text{für } i = 1, \ldots, n \tag{5.7}$$

$$\textstyle\sum_{i=1}^{n} a_i(y_i - y e_i) = 0 \tag{5.8}$$

Es bezeichne $P'(n) := \text{Ws}[\ \exists \widehat{\mathbf{x}}' \in \mathcal{L}_{CJLOSS}$ mit (5.6), (5.7), (5.8) $]$ die Wahrscheinlichkeit des Misserfolgs für zufällige $(a_1, \ldots, a_n)^t \in_R [1, A]^n$, ferner $\mathbf{1/2} := (\frac{1}{2}, ..., \frac{1}{2})^t$, $\mathbf{x} := (x_1, ..., x_n)^t \in \mathbb{Z}^n - \mathbf{1/2} \cdot \{0, 1\}$. Offenbar gilt $\widehat{\mathbf{x}}' \neq \widehat{\mathbf{e}}'$ gdw $\exists j : y_j \neq y e_j$. Zwar hängen $\mathbf{x}, y$ von den

a_i ab, werden aber in der Ws-Analyse fixiert. Es folgt

$$P'(n) \le \overbrace{\mathrm{Ws}\left[\begin{array}{l}\text{für feste } \mathbf{e}\in\{0,1\}^n,\ \mathbf{x}\in\mathbb{Z}^n-\mathbf{1/2}\cdot\{0,1\},\ y\in\mathbb{Z},\ 0\le y<\sqrt{n/4+1},\\ \exists j: y_j\neq ye_j,\ \|\mathbf{x}\|\le\sqrt{n/4},\ \sum_{i=1}^n a_i(y_i-ye_i)=0\end{array}\right]}^{\text{Faktor 1}}$$
$$\cdot\underbrace{\left|\left\{\mathbf{x}\in\mathbb{Z}^n-\mathbf{1/2}\cdot\{0,1\}\ :\ \|\mathbf{x}\|\le\sqrt{n/4}\right\}\right|}_{\text{Faktor 2}}\cdot\underbrace{\left|\left\{y\in\mathbb{Z}\ :\ 0\le y<\sqrt{n/4+1}\right\}\right|}_{\text{Faktor 3}}$$

Wir schätzen die drei Faktoren nach oben ab:

1. Für festes j mit $y_j\neq ye_j$ ist die Gleichung $\sum_{i=1}^n a_i(y_i-ye_i)=0$ mit Wahrscheinlichkeit $\le 1/A$ erfüllt, denn a_j ist durch die a_i mit $i\neq j$ bestimmt. Somit für alle j: Faktor $1\le n/A$.

2 J.E. Mazo und A.M. Odlyzko [MaOd90] beweisen für hinreichend grosses n und alle $u\ge 0$

$$\left|\left\{\mathbf{x}\in\mathbb{Z}^n+\mathbf{1/2}\cdot\{0,1\}\ :\ \|\mathbf{x}\|\le\sqrt{n/4}\right\}\right|\le e^{\delta(u)n}+2^n\quad\text{für }\delta(u)=u/4+\ln\theta(e^{-u}),$$

$\theta(z):=1+2\sum_{k=1}^\infty z^{k^2}$. Für $u_o=1.8132$ gilt $\delta\approx 0.7367$ und $e^{\delta(u_o)n}\le 2^{c'_o n}$ mit $c'_o=1.0629\cdots$.

3. Offenbar gilt Faktor 3 $\le 1+\sqrt{n/4+1}$.

Somit gilt $P'(n)\le(1+\sqrt{n/4+1})\,2^{c'_0 n}\ n/A$ und wegen $1/d>1.0628\cdots>c'_0$ und $A\ge\max_{i=1,\ldots,n}a_i\ge 2^{n/d}$ folgt die Behauptung $\lim_{n\to\infty}P'(n)=0$. ■

Towards NP-hardness of SVP. Die Menge der lösbaren Subsetsum-Probleme der Dichte $d<0.9408$ ist **NP**-vollständig. Satz 5.3.1 liefert eine polynomialzeit Transformation von Subsetsumproblemen mit $d<0.9408$ auf **SVP**, mit Ausnahme der Misserfolge. Wir eliminieren die Misserfolge für lösbare Subsetsumprobleme mit höchstens $c(\mathbf{a},s)=O(1)$ linear unabhängigen Vektoren $\mathbf{b}=\sum_{i=1}^n y_i\mathbf{b}_i-y\mathbf{b}'_{n+1}\neq\pm\widehat{\mathbf{e}}'$ in $\mathcal{L}=\mathcal{L}_{CJLOSS}$ der Länge $\|\mathbf{b}\|^2\le\frac{n}{4}+1$.

Für $c=c(\mathbf{a},s)$ gibt es $1\le i_1<\cdots<i_c\le n$ so dass die Teilvektoren $\sum_{k=1}^c y_{i_k}\mathbf{b}_{i_k}$ für c viele der $\mathbf{b}$ linear unabhängig von $\sum_{k=1}^c e_{i_k}\mathbf{b}_{i_k}$ sind. Wir erraten $i_1,\ldots,i_c$ und $e_{i_1},\ldots,e_{i_c}\in\{0,1\}$. Wir beschränken die Basisvektoren auf die Zeilen $i\in[1,n]_{red}:=[1,n]-\{i_1,\ldots,i_c\}$ und projizieren so $\mathcal{L}$ auf ein Gitter $\mathcal{L}_{red}$ der Dimension $n-c$ und das Subsetsumproblem auf

$$\textstyle\sum_{i\in[1,n]_{red}}a_ie_i=s_{red},\qquad s_{red}:=s-\sum_{k=1}^c a_{i_k}e_{i_k}$$

einem Subsetsumproblem der Dimension $n-c$. In $\mathcal{L}_{red}$ ist $\mathbf{b}'_{n+1}$ durch $\mathbf{b}'^{red}_{n+1}$ mit s_{red} ersetzt. Das **SVP**-Orakel liefert zum Gitter $\mathcal{L}_{red}$ den Vektor $\widehat{\mathbf{e}}'_{red}=\sum_{i\in[1,n]_{red}}a_ie_i-\mathbf{b}'^{red}_{n+1}$ der Länge $\sqrt{(n-c)/4+1}$. Entscheidend ist, dass die störenden kurzen Vektoren $\mathbf{b}\neq\pm\widehat{\mathbf{e}}'$ von $\mathcal{L}$ durch die Reduktion eliminiert werden. Dies beweist für $c=c(\mathbf{a},s)$ Teil **1.** von

Satz 5.3.2

1. *Durch $2^c\binom{n}{c}$ Aufrufe des* **SVP***-Orakels auf die Gitter $\mathcal{L}_{red}$ zu $\mathcal{L}=\mathcal{L}_{CJLOSS}$ mit $1\le i_1<\cdots<i_c\le n$ und $e_{i_1},\ldots,e_{i_c}\in\{0,1\}$ werden alle Subsetsumprobleme mit $c(\mathbf{a},s)\le c$ für alle d gelöst.*

2. *Der Anteil der Subsetsumprobleme mit $c(\mathbf{a},s)>c$ unter den $(\mathbf{a},s)\in[1,A]^n[1,\frac{n}{2}A]$, $A\ge 2\cdot 2^{n/d}$ ist höchstens $P'(n)^c$.*

Beweis. 2. Wir schätzen den Anteil der $(\mathbf{a},s)\in[1,A]^n[1,\frac{n}{2}A]$ mit $c(\mathbf{a},s)>c$ ab, analog zur oberen Schranke von $P'(n)$ im Beweis von Satz 5.3.1. Es gibt $c(\mathbf{a},s)$ linear unabhängige $(y_{1,j},\ldots,y_{n,j},y_j)^t\in\mathbb{Z}^{n+1}$ für $j=1,\ldots,c$ mit $\mathbf{b}_j=\sum_{i=1}^n y_{i,j}\mathbf{b}_i-y_j\mathbf{b}'_{n+1}\neq\pm\widehat{\mathbf{e}}'$ und $\|\mathbf{b}_j\|^2\le\frac{n}{4}+1$. Für diese c Vektoren $\mathbf{b}_j\in\mathcal{L}$ gilt $\sum_{i=1}^n a_iy_{i,j}=y_js$ und somit

$$\textstyle\sum_{i=1}^n a_i(y_{i,j}-y_je_i)=0\quad\text{für } j=1,\ldots,c \tag{5.8}$$

Diese Gleichungen bestimmen c der $a_1,\ldots,a_n$ durch die übrigen $n-c$ der a_i. Der Anteil der $(a_1,\ldots,a_n)\in[1,A]^n$ der Dichte $d<0.9408$, der diese c Gleichungen (5.8) erfüllt, ist dem Beweis von Satz 5.3.1 folgend kleiner gleich $P'(n)^c$ mit $\lim_{n\to\infty}P'(n)=0$. ■

Fakt. Nach Satz 5.3.2 löst das **SVP**-Orakel alle Subsetsumprobleme mit konstantem $c(\mathbf{a}, s)$ durch polynomial viele Aufrufe. Dies macht den Anteil der Misserfolge bei der Reduktion von Subsetsum mit $d < 0.9408$ auf **SVP** vernachlässigbar klein, kleiner als jeder polynomiale Bruchteil.

Satz 5.3.3
Lösbare Subsetsum-Probleme werden für $n \geq n_o$ und $N \geq 1.163^{n-1}\sqrt{n/4+1}$ für fast alle $(a_1, \ldots, a_n)^t \in [1, A]^n$ der Dichte $d < 4.8/n$ durch den ersten Vektor jeder LLL-Basis zu $\delta = 0.99$ von $\mathcal{L}_{CJLLOSS}$ gelöst, und zwar in Polynomialzeit.

Beweis. (Bezeichnungen wie im Beweis von Satz 5.3.1, $\mathbf{B}' = [\mathbf{b}_1 ..... \mathbf{b}'_{n+1}]$ ist die Basis (5.4)) Für den ersten Vektor $\mathbf{b}$ einer LLL-Basis von $\mathcal{L}_{CJLOSS}$ gilt $\|\mathbf{b}\|^2 \leq \lambda_1^2/(\delta - 1/4)^{n-1}$ nach Satz 4.1.4 und somit für $\delta = 0.99$ dass $\|\mathbf{b}\| \leq 1.163^{n-1}\lambda_1 \leq 1.163^{n-1}\sqrt{n/4+1}$. Sei $\mathbf{b} = \sum_{i=1}^n y_i \mathbf{b}_i - y\mathbf{b}'_{n+1}$ mit $y \geq 0$. Aus $N \geq 1.163^{n-1}\sqrt{n/4+1}$ folgt $\sum_{i=1}^n a_i y_i = ys$ und somit gilt (5.8). Das $\mathbf{x}$ von (5.7) erfüllt $\|\mathbf{x}\| < \sqrt{n/4+1} \cdot 1.163^n$.

J.C. Lagarias und A.M. Odlyzko [LaOd85] zeigen im Anschluss an Theorem 3.5 für das Gitter $\mathcal{L}_{LO}$: der Anteil der $(a_1, \ldots, a_n)^t \in [1, A]^n$ der Dichte $d < 4.8/n$ mit $\mathbf{b} \neq \widehat{\mathbf{e}}$ für den Lösungsvektor $\widehat{\mathbf{e}} \in \mathcal{L}_{LO}$ wird für $n \to \infty$ beliebig klein. Damit gilt für fast alle $(a_1, ..., a_n) \in [1, A]^n$ dass $\mathbf{b} = \widehat{\mathbf{e}}$. Die Grenzdichte $4.8/n$ erhöht sich weiter durch stärkere Reduktion als LLL. ■

Für $n \leq 80$ gilt Satz 5.3.2 in der Praxis schon für $N = 16$ und $d < 0,9408$ für den Hauptfall dass $\sum_{i=1}^n e_i = n/2$. Hierzu ersetzt man die LLL-Reduktion durch die stärkere BKZ-Reduktion mit Blockweite 32 und erweitert $\mathbf{B}'$ durch die $(n+3)$-te Zeile $(N, ..., N, N\frac{1}{2})$. Siehe [SS12].

5.4 Gitter mit großer Packungsdichte

Zu $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ bezeichne $\mathcal{L}_\mathbf{a} = \mathcal{L}(\mathbf{B}_\mathbf{a}) \subset \mathbb{R}^{n+1}$ das Gitter mit Basismatrix

$$\mathcal{L}_\mathbf{a} := \mathcal{L}(\mathbf{B}_\mathbf{a}). \quad \mathbf{B}_\mathbf{a} = \begin{bmatrix} 1 & & & \\ & \ddots & O & \\ & O & 1 & \\ Na_1 & \cdots & Na_n & \end{bmatrix} \in \mathbb{R}^{(n+1)n}, \quad \det \mathbf{B}_\mathbf{a}^t \mathbf{B}_\mathbf{a} = 1 + N^2 \sum_{i=1}^n a_i^2$$

Korollar 5.4.1
Für $n \geq n_0$ und $N \geq \sqrt{n/4}$ gilt $\lambda_1(\mathcal{L}_\mathbf{a}) \geq \sqrt{n/4}$ für fast alle $\mathbf{a} \in [1, A]^n$ der Dichte $d < 0,9408$.

Beweis. Obiges $\mathbf{B}_\mathbf{a} = [\mathbf{b}_1, ..., \mathbf{b}_n]$ ist die Basis (5.4) ohne die letzte Zeile und letzte Spalte. Ergänze $\mathbf{B}_\mathbf{a}$ zu einer CJLOSS-Basis $\mathbf{B}'_\mathbf{a}$ (ohne letzte Zeile) zu gegebener Subsetsum-Lösung $\mathbf{e}$. Im Fall $\lambda_1(\mathcal{L}_\mathbf{a}) < \sqrt{n/4}$ gibt es einen Gittervektor in $\mathcal{L}(\mathbf{B}'_\mathbf{a})$ der Länge $\leq \lambda_1$, der nicht zur Lösung $\mathbf{e}$ gehört. Dies ist nach Satz 5.3.1 für fast alle $\mathbf{a} \in [1, A]^n$ mit Dichte $d < 0,9408$ ausgeschlossen.
Satz 5.3.1 gilt auch ohne die letzte Zeile der Basismatrix (5.4). Der Beweis in [CJLOSS92] kommt ohne diese letzte Zeile aus. Dann gilt für den Lösungsvektor $\widehat{\mathbf{e}}' \in \mathcal{L}_{\text{CJLOSS}}$ dass $\|\widehat{\mathbf{e}}'\|^2 = n/4$. ■

Satz 5.4.2
Für $n \geq n_0$, $N^2 = \frac{n}{4}$ haben fast alle $\mathbf{a} \in [1, 2 \cdot 2^{n/0,9408}]^n$ Dichte $d < 0,9408$ und $\mathcal{L}_\mathbf{a}$ hat Packungsdichte $\triangle$ mit $\frac{1}{n}\log_2 \triangle \geq -1,01583$.

Beweis. Für fast alle $\mathbf{a} \in [1, 2 \cdot 2^{n/0,9408}]^n$ gilt $d = \frac{n}{\log_2(\max\limits_{i=1,\ldots,n} a_i)} < 0,9408$. Nach Kor. 5.4.1 gilt $\lambda_1^2 \geq n/4$ für fast alle $\mathbf{a} \in [1, A]^n$. Wegen $4N^2 n = n^2$ sowie $n^{1/n} = 1 + o(1)$ und

$$(\det \mathcal{L}_\mathbf{a})^2 = 2^{2n}(1 + N^2 \textstyle\sum_{i=1}^n a_i^2) \leq 2^{2n}(1 + 4N^2 n 2^{2n/d})$$

folgt für $n \geq n_0$ dass $\lambda_1^2/(\det(\mathcal{L}_\mathbf{a})^{2/n} \geq n\, 2^{-2-2/0,9408}(1 - o(1))$ und somit

$$\triangle(\mathcal{L}_\mathbf{a}) = 2^{-n}\lambda_1^n\, V_n / \det \mathcal{L}_\mathbf{a} > (n\, 2^{-2-2/0,9408}(1 - o(1))\tfrac{e\pi}{2n} n)^{n/2} > 0.4945438^n > 2^{-1.01583\ n}.$$ ■

Vergleich mit expliziten Konstruktionen dichter Gitter. Die unendlichen Klassenkörpertürme von Gold, Shafarevitch, Martinet, liefern eine unendliche Folge von Gittern mit

$$\tfrac{1}{n}\log_2 \triangle \geq -2,218,$$

siehe [CoSl88, Kap. 8, Sektion 7.4]. Eine praktische Methode zum Auffinden solcher Gitter ist nicht bekannt. Explizite Konstruktionen von Gittern gibt es [CoSl88], so dass

$$\tfrac{1}{n}\ \log_2 \triangle \geq -1,2454 \quad \text{für } n \leq 98328,$$

$$\tfrac{1}{n}\ \log_2 \triangle \geq -2,0006 \quad \text{für } n \leq 10^{51}.$$

Verglichen damit kann man nach Satz 5.4.2 die grössere Dichte

$$\tfrac{1}{n}\ \log_2 \triangle \geq -1,0158$$

für beliebige n und fast alle $\mathbf{a} = (a_1, \ldots, a_n) \in [0, A]^n$ der Dichte $d < 0,9408$ leicht erreichen. Man wählt $\mathbf{a}$ zufällig und verifiziert dass $\lambda_1(\mathcal{L}_\mathbf{a}) = n/4$.

Dichteste bekannte Gitterpackung. J.A. Rush [R89] zeigt die Existenz von Gitterpackungen der Dimension $n = p^2$ mit p prim und Packungsdichte

$$\frac{1}{n}\log_2(\triangle) \geq -1 - 2(\log_2 e)/e^{2\pi^2}) \gtrsim -1,000000007719...$$

Dies gilt für die Konstruktion A von [CoSl88] angewandt auf fehlerkorrigierende $[n, k, d, p, \mathcal{H}]$-Codes. Das Ergebnis ist nicht konstruktiv aber der Suchraum für geeignete Codes ist erheblich kleiner als beim Beweis der Minkowski-Schranke $\frac{1}{n}\log_2 \triangle \geq -1$.

Die obere Schranke für $\mathbf{P'(n)}$ ist scharf und die Grenzdichte $\mathbf{d = 0,9408...}$ maximal. Angenommen der kürzeste Gittervektor $\widehat{\mathbf{x}}' = \sum_{i=1}^n y_i \mathbf{b}_i - y\mathbf{b}'_{n+1} = (x_1, ..., x_{n+2})^t$ von $\mathcal{L}_{\text{CJLOSS}}$ löst das Subsetsum-Problem zu $\mathbf{a} = (a_1, ..., a_n), s$ nicht. Dann gilt $x_{n+1} = 0$ und der Lösungsvektor $\widehat{\mathbf{e}}' := \sum_{i=1}^n e_i \mathbf{b}_i - \mathbf{b}'_{n+1} \in \mathcal{L}_{CJLOSS}$ erfüllt (5.6).

Satz 5.3.1 schätzt die Anzahl der Lösungen $(x_1, ..., x_n, y) \in \frac{1}{2}\mathbb{Z}^{n+1}$ mit $(\sqrt{n/4}+1)2^{c'_0 n}$ ab. Ferner ist für $x_i = y_i - \frac{y}{2}$ die Wahrscheinlichkeit für $\sum_{i=1}^n a_i(y_i - ye_i) = 0$ höchstens n/A. Wegen $\sum_{i=1}^n a_i(y_i - ye_i) = 0$ schränken die Bedingungen

$$a_j = -\sum_{i=1, i\neq j}^{n} a_i \frac{y_i - ye_i}{y_j - ye_j} \in [1, A] \cap \mathbb{N} \ \text{ für alle } \ j \text{ mit } y_j \neq ye_j$$

die Anzahl der $(x_1, ..., x_n, y)$ weiter ein. Für die Varianz $V(X) = \mathbf{E}[(X - \mathbf{E}(X))^2]$ von $X = -\sum_{i=1, i\neq j}^n a_i \frac{y_i - ye_i}{y_j - ye_j}$ gilt $V(X) = O(A^2\sqrt{n})$. Daraus folgt $\text{Ws}[X \in [1, A]] \geq \Theta(1/\sqrt{n})$. Damit ist $\text{Ws}[X \in [1, A] \cap \mathbb{N}]$ so groß dass dies c'_0 nicht erniedrigt. Somit ist die Grenzdichte $d = 0,9408...$ maximal.

Kapitel 6

HKZ- und Block-Reduktion von Gitterbasen

Die LLL-Reduktion in Kapitel 4 liefert in Polynomialzeit LLL-Basen $\mathbf{b}_1, ..., \mathbf{b}_n$ mit exponentiellen Approximationsfaktoren $\|\mathbf{b}_i^2\|/\lambda_i^2 \leq \alpha^n$ für $i = 1, ..., n$. Die HKZ-Reduktion nach Hermite und Korkine-Zolotareff liefert dagegen in Exponentialzeit HKZ-Basen $\mathbf{b}_1, ..., \mathbf{b}_n$ mit polynomialen Approximationsfaktoren $\|\mathbf{b}_i\|^2/\lambda_i^2 \leq \frac{i+3}{4}$ für $i = 1, ..., n$. Schnorr [S87] entwickelt eine Hierarchie von Block-Reduktionsverfahren, welche LLL- und HKZ-Reduktion überbrückt, derart dass höhere Laufzeit die Approximationsfaktoren erniedrigt.

6.1 HKZ-Basen

Zur Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ des Gitters $\mathcal{L}$ sind die projizierten Gitter $\mathcal{L}_i$ für $i = 1, \ldots, n$ erklärt durch

$$\mathcal{L}_i = \pi_i(\mathcal{L}) \in \text{span}(\mathbf{b}_1, ..., \mathbf{b}_{i-1})^{\perp}.$$

Insbesondere gilt für jede GNF $\mathbf{B} = \mathbf{R} \in \mathbb{R}^{n \times n}$ dass

$$\pi_i : (r_1, ..., r_n)^t \mapsto (0, ..., 0, r_i, ..., r_n)^t \in 0^{i-1}\mathbb{R}^{n-i+1}.$$

C. Hermite [He1850] sowie unabhängig A. Korkine und G. Zolotareff [KZ1873, KZ1877] definierten HKZ-Basen in der Sprache quadratischer Formen.

Definition 6.1.1 (HKZ-Basis)
Eine LLL-Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m \times n}$ *ist HKZ-Basis, wenn für* $\mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n \times n}$ *gilt:*

$$r_{i,i} = \lambda_1(\mathcal{L}_i(\mathbf{B})) \quad \textit{für } i = 1, \ldots, n.$$

Für jede HKZ-Basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n] = \mathbf{B} = \mathbf{QR}$ sind auch $\pi_j\{\mathbf{b}_j, \ldots, \mathbf{b}_n\}$ und $[r_{i,\ell}]_{j \leq k, \ell \leq n}$ für $1 \leq j \leq n$ HKZ-Basen. Es gilt $\lambda_1(\mathcal{L}_i(\mathbf{B})) = \lambda_1(\mathcal{L}_i(\mathbf{R}))$. Jede -Basis approximiert λ_i^2 mit Approximationsfaktor $\frac{i+3}{4}$ (fast so gut wie der Approximationsfaktor $\max(1, i/4)$ von Satz 2.1.5):

Satz 6.1.2
Für jede HKZ-Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *von* $\mathcal{L}$ *gilt* $\frac{4}{i+3} \leq \|\mathbf{b}_i\|^2 / \lambda_i(\mathcal{L})^2 \leq \frac{i+3}{4}$ *für* $i = 1, \ldots, n$.

Dagegen gilt für LLL-Basen $\mathbf{b}_1, \ldots, \mathbf{b}_n$ nach Satz 4.1.4 mit $\alpha = \frac{1}{\delta - 1/4}$

$$\alpha^{1-i} \leq \|\widehat{\mathbf{b}}_i\|^2/\lambda_i(\mathcal{L})^2 \leq \|\mathbf{b}_i\|^2/\lambda_i(\mathcal{L})^2 \leq \alpha^{n-1}.$$

Beweis. *Obere Schranke* $\frac{\|\mathbf{b}_i\|^2}{\lambda_i(\mathcal{L})^2} \leq \frac{i+3}{4}$: Für das Gitter $\mathcal{L}_i = \pi_i(\mathcal{L})$ gilt

$$\|\widehat{\mathbf{b}}_i\| = r_{i,i} = \lambda_1(\mathcal{L}_i) \leq \lambda_i(\mathcal{L}), \tag{6.1}$$

denn es gibt linear unabhängige Gittervektoren $\mathbf{a}_1, \ldots, \mathbf{a}_i \in \mathcal{L}$ mit $\|\mathbf{a}_1\| \leq \cdots \leq \|\mathbf{a}_i\| \leq \lambda_i(\mathcal{L})$. Daher gilt $\pi_i(\mathbf{a}_j) \neq 0$ für ein $j \leq i$, also $\pi_i(\mathbf{a}_j) \in \mathcal{L}_i \setminus \{0\}$ und somit $\lambda_1(\mathcal{L}_i) \leq \|\pi_i(\mathbf{a}_j)\| \leq \lambda_i(\mathcal{L})$. Für die HKZ-Basis $\mathbf{R} = [\mathbf{r}_1, \ldots, \mathbf{r}_n]$ gilt nach (6.1) dass

$$\|\mathbf{b}_i\|^2 = \|\mathbf{r}_i\|^2 = \sum_{j=1}^{i} r_{j,i}^2 \leq r_{i,i}^2 + \tfrac{1}{4}\sum_{j=1}^{i-1} r_{j,j}^2 \leq \tfrac{i+3}{4}\,\lambda_i(\mathcal{L})^2.$$

Untere Schranke $\frac{4}{i+1} \leq \frac{\|\mathbf{b}_i\|^2}{\lambda_i(\mathcal{L})^2}$: Nach Definition der HKZ-Basis gilt für $j \leq i$:

$$r_{j,j}^2 = \lambda_1(\mathcal{L}_j)^2 \leq \|\pi_j(\mathbf{b}_i)\|^2 \leq \|\mathbf{b}_i\|^2.$$

Somit $\|\mathbf{b}_j\|^2 = \sum_{\ell=1}^{j} r_{\ell,j}^2 \leq r_{j,j}^2 + \frac{1}{4}\sum_{\ell=1}^{j-1} r_{\ell,\ell}^2 \leq \frac{j+3}{4}\|\mathbf{b}_i\|^2$.

Es folgt die Behauptung $\lambda_i(\mathcal{L})^2 \leq \max_{j=1,\ldots,i}\|\mathbf{b}_j\|^2 \leq \frac{i+3}{4}\|\mathbf{b}_i\|^2$. ■

Zu HKZ-Basen siehe auch [LLS90] von J.C. Lagarias, H.W. Lenstra und C.P. Schnorr. Kannan's Algorithm für HKZ -Reduction [K87] hat Laufzeit $n^{n/2e+o(n)}$ nach Hanrot, Stehlé, Proc. CRYPTO 2007.

6.2 Semi Block 2k-Reduktion

Block-reduzierte Gitterbasen bilden eine Brücke, die HKZ-Basen und LLL-Basen verbindet, siehe C.P. Schnorr [S87] [S94]. Während die Algorithmen zur HKZ-Reduktion in Dimension n expontielle Laufzeit in n haben, ist die Block-Reduktion für Blockweite 20 ähnlich effizient wie die schwächere LLL-Reduktion. Die Variante der Semi-Block-$2k$-Reduktion hat polynomielle Laufzeit für $k = O(\log n/\log\log n)$. [S87].

Einer GNF $\mathbf{R} \in \mathbb{R}^{n\times n}$ mit $n = hk$ ordnen wir die Untermatrizen $\mathbf{R}_\ell = [r_{i,j}]_{\ell k-k<i,j\leq \ell k} \in \mathbb{R}^{k\times k}$ der Blockweite k zu für $\ell = 1, ..., h$. Ferner sei $\mathbf{R}_{\ell,\ell+1} = [r_{i,j}]_{\ell k-k<i,j\leq \ell k+k} \in \mathbb{R}^{2k\times 2k}$ die $2k \times 2k$-Untermatrix von $\mathbf{R}$ die $\mathbf{R}_\ell$ und $\mathbf{R}_{\ell+1}$ umfasst. Es bezeichnet $\mathcal{D}_\ell := (\det \mathbf{R}_\ell)^2$ und $\mathbf{B}_\ell := [\mathbf{b}_{k\ell-k+1}, ..., \mathbf{b}_{k\ell}]$ ist der ℓ-te Block von $\mathbf{B}$.

Definition 6.2.1 (Semi Block 2k-Basis)
Eine Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m\times n}$, $n = hk$ *ist eine Semi Block-*$2k$*-Basis zu* $1 \geq \delta_B > 0$ *wenn*

1. $\mathbf{R}_1, ..., \mathbf{R}_h$ *von* $\mathbf{R}$ HKZ*-Basen sind und* $\mathbf{B}$ *ist längenreduziert.*
2. $\delta_B^k\,(\mathcal{D}_\ell/\mathcal{D}_{\ell+1})^{1/k} \leq \beta_k$ *für* $\ell = 1, ..., h-1$ *und das* β_k *von Def. 6.2.2.*

Gilt $\delta_B^k\,(\mathcal{D}_\ell/\mathcal{D}_{\ell+1})^{1/k} > \beta_k$ dann führt *HKZ*-Reduktion von $\mathbf{R}_{\ell,\ell+1}$ zu $\mathcal{D}_\ell^{neu} \leq \delta_B^{k^2}\,\mathcal{D}_\ell^{alt}$.

Definition 6.2.2

$$\alpha_k := \max r_{1,1}^2/r_{k,k}^2 \quad \textit{maximiert über alle HKZ-GNF } \mathbf{R} \in \mathbb{R}^{k\times k}$$
$$\beta_k := \max\left(\mathcal{D}_1/\mathcal{D}_2\right)^{1/k} \quad \textit{maximiert über alle HKZ-GNF } \mathbf{R} \in \mathbb{R}^{2k\times 2k}.$$

Für das $\alpha = \frac{4}{3} = 1/(\delta_L - 1/4)$ der LLL-Basen mit $\delta_L = 1$ gilt offenbar $\alpha_2 = \beta_1 = \frac{4}{3}$. Ferner gilt

$$\alpha_k \leq k^{1+\ln k} \qquad \text{[S87]}$$

$$k/12 \leq \beta_k \leq (1 + k/2)^{2\ln 2 + 1/k}. \qquad \text{[GHKN06]}$$

Damit gilt $\beta_k^{1/k} \to 1$ für $k \to \infty$.

Satz 6.2.3
Für jede Semi Block $2k$-Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m\times n}$, $n = hk$ zu $\delta_B > 0$ von $\mathcal{L}$ gilt

$$\|\mathbf{b}_1\|^2 \le \gamma_k(\beta_k/\delta_B^k)^{\frac{h-1}{2}}(\det\mathcal{L})^{2/n} = \gamma_k/\gamma_n\,(\beta_k/\delta_B^k)^{\frac{h-1}{2}} rd(\mathcal{L})^{-2}\lambda_1^2.$$

Im Vergleich gilt für LLL-Basen $\|\mathbf{b}_1\|^2 \le \alpha^{\frac{n-1}{2}}(\det\mathcal{L})^{2/n} = \gamma_n^{-1}\alpha^{\frac{n-1}{2}} rd(\mathcal{L})^{-2}\lambda_1^2$.
Das α von LLL-Basen ersetzt durch $\beta_k^{1/k}/\delta_B = 1/\delta_B + o(1)$ für $k\to\infty$.

Beweis. Sei $\mathcal{D}_\ell := (\det\mathbf{R}_\ell)^2$. Für die HKZ-Basis $\mathbf{R}_1 \in \mathbb{R}^{k\times k}$ gilt $\|\mathbf{b}_1\|^2 \le \gamma_k\mathcal{D}_1^{1/k}$.
Nach Definition von β_k und Definition 6.2.1, Teil **2** gilt $\mathcal{D}_\ell \le (\beta_k/\delta_B^k)^k\mathcal{D}_{\ell+1}$.
Es folgt durch Induktion über ℓ für $\ell = 1,...,h = n/k$

$$\|\mathbf{b}_1\|^2 \le \gamma_k\mathcal{D}_1^{1/k} \le \gamma_k(\beta_k/\delta_B^k)^{\ell-1}\mathcal{D}_\ell^{1/k}. \tag{6.2}$$

Wir ziehen aus dem Produkt dieser h Ungleichungen die h-te Wurzel. Dies liefert die Behauptung:

$$\|\mathbf{b}_1\|^2 \le \gamma_k(\beta_k/\delta_B^k)^{\binom{h}{2}\frac{1}{h}}(\det\mathcal{L})^{\frac{1}{hk}} = \gamma_k(\beta_k/\delta_B^k)^{\frac{h-1}{2}}(\det\mathcal{L})^{2/n}.$$

Wir kombinieren dies mit der Gleichung $\lambda_1^2 = \gamma_n rd(\mathcal{L})^2\det(\mathcal{L})^{2/n}$. ■

Algorithmus 6.2.1, Semi Block 2k-Reduktion

`EINGABE` LLL-Basis $\mathbf{B}\in\mathbb{Z}^{m\times n}$ zu δ, α, $n = hk$ und δ_B mit $0 < \delta_B < 1$.

1. HKZ-reduziere $\mathbf{B}_1 = [\mathbf{b}_1,...,\mathbf{b}_k]$ und $\mathbf{R}_1$, $\ell := 1$

2. HKZ-reduziere $\mathbf{R}_{\ell+1}$ zu $\mathbf{R}_{\ell+1}\mathbf{T}_k$ mit $\mathbf{T}_k \in \mathrm{GL}_k(\mathbb{Z})$.
$\mathbf{B}_{\ell+1} := \mathbf{B}_{\ell+1}\mathbf{T}_k$, längenreduziere $\mathbf{B}_{\ell+1}$, erneuere $\mathbf{R}_{\ell,\ell+1}$.

3. HKZ-reduziere $\mathbf{R}_{\ell,\ell+1}$ zu $\mathbf{R}_{\ell,\ell+1}\mathbf{T}_{2k}$ mit $\mathbf{T}_{2k}\in\mathrm{GL}_{2k}(\mathbb{Z})$.
`IF` $\mathcal{D}_\ell^{neu} \le \delta_B^{k^2}\,\mathcal{D}_\ell^{alt}$
`THEN` $[\mathbf{B}_\ell,\mathbf{B}_{\ell+1}] := [\mathbf{B}_\ell,\mathbf{B}_{\ell+1}]\mathbf{T}_{2k}$, längenreduziere $\mathbf{B}_\ell,\mathbf{B}_{\ell+1}$, $\ell := \max(\ell-1,1)$
`ELSE` $\ell := \ell+1$.
`IF` $\ell < h$ `THEN GO TO` **2**

`AUSGABE` Semi Block $2k$-Basis $\mathbf{B}$.

Korrektheit. Nach Schritt 3 ist $\mathbf{b}_1,...,\mathbf{b}_{k\ell}$ eine Semi Block $2k$-Basis.

Satz 6.2.4
1. *Alg. 6.2.1 macht höchstens $(\frac{2h^2}{k}+h)\log_{1/\delta_B} M$ Iterationen für den Wert $M := \max(\|\mathbf{b}_1\|,...,\|\mathbf{b}_n\|)$ der Eingabebasis. Eine Iteration geht in $(2k)^{k/e+o(k)}\,n^{O(1)}$ arithmetischen Schritten nach [HS07].*

2. *Alg. 6.2.1 macht höchstens $\frac{h^3}{12}\log_{1/\delta_B}\alpha$ Iterationen bis $\mathcal{D}_B \le 1$ erreicht ist.*

Beweis. **1.** Jeder Schritt **3** mit $\ell := \max(\ell-1,1)$ erniedrigt die Lovász Invariante zu k

$$\mathcal{D} := \mathcal{D}_1^{h-1}\mathcal{D}_2^{h-2}\cdots\mathcal{D}_{h-1}^1 \qquad \text{so dass} \qquad \mathcal{D}_{neu} \le \delta_B^{k^2}\mathcal{D}_{alt}.$$

Die Eingabebasis hat den $\mathcal{D}$-Wert $\mathcal{D}^{Ein} \le M^{n(h-1)}$ und für die Ausgabebasis gilt $\mathcal{D}^{Aus} \ge 1$.
Damit ist die Anzahl $\#\mathbf{It}^-$der Schritte **3** mit $\ell := \max(\ell-1,1)$ beschränkt durch

$$\#\mathbf{It}^- \le \tfrac{n(h-1)}{k^2}\log_{1/\delta_B} M = \tfrac{h}{k}(h-1)\log_{1/\delta_B} M.$$

Für die Gesamtzahl #**It** der Schritte **3** folgt die Behauptung

$$\#\mathbf{It} = h - 1 + 2\#\mathbf{It}^- \leq (\tfrac{2h^2}{k} + h)\log_{1/\delta_B} M.$$

Die HKZ-Reduktion von $\mathbf{R}_{\ell,\ell+1} \in \mathbb{R}^{2k\times 2k}$ geht in $(2k)^{k/4+o(k)}$ arithmetischen Schritten.

2. Wir ersetzen die Lovász Invariante $\mathcal{D}$ durch die folgende Invariante

$$\mathcal{D}_B := \textstyle\prod_{\ell=1}^{h-1}(\mathcal{D}_\ell/\mathcal{D}_{\ell+1})^{h^2/4-(h/2-\ell)^2}.$$

Der Exponent $h^2/4-(h/2-\ell)^2$ ist maximal bei $\ell = h/2$, er ist null für $\ell = 0$ und $\ell = h$ und ist symmetrisch zu $\ell = h/2$. Für die LLL-Eingabebasis gilt $\mathcal{D}_\ell \leq \alpha^{k^2}\mathcal{D}_{\ell+1}$ und somit gilt für ihren $\mathcal{D}_B$-Wert $\mathcal{D}_B^{Ein}$ dass $\mathcal{D}_B^{Ein} \leq \alpha^{k^2 s}$ für $s =_{def} \sum_{\ell=1}^{h-1} h^2/4-(h/2-\ell)^2$.

Die bekannte Summe $\bar{s} := \sum_{\ell=1}^{h-1}\ell^2 = h(h-1)(h-1/2)/3$ liefert

$$\textstyle\sum_{\ell=1}^{h-1}(h/2-\ell)^2 = -h^2(h-1)/4 + \bar{s} = h(h-1)(h-2)/12$$

und somit $s = (h+1)h(h-1)/6 = (h^3-h)/6$.

Es folgt $\mathcal{D}_B^{Ein} \leq \alpha^{k^2(h^3-h)/6}$. Ein aktiver Schritt **3** ändert von $\mathcal{D}_B$ nur den Faktor

$$\prod_{t=\ell-1,\ell,\ell+1}(\mathcal{D}_t/\mathcal{D}_{t+1})^{t(h-t)} = \mathcal{D}_{\ell-1}^{(\ell-1)(h-\ell+1)}(\mathcal{D}_\ell\mathcal{D}_{\ell+1})^{h-2\ell-1}\mathcal{D}_\ell^2.$$

Ein aktiver Schritt **3** lässt $\mathcal{D}_{\ell-1}$ und $\mathcal{D}_\ell\mathcal{D}_{\ell+1}$ unverändert und bewirkt somit $\mathcal{D}_B^{neu} \leq \delta_B^{2k^2}\mathcal{D}_B^{alt}$. Für die Anzahl der Iterationen zum Erreichen von $\mathcal{D}_B \leq 1$ folgt

$$\#\mathbf{It} \leq \log_{1/\delta_B^{2k^2}}\mathcal{D}_B^{Ein} \leq \tfrac{k^2h^3}{6}\tfrac{1}{2k^2}\log_{\delta_B}\alpha = \tfrac{h^3}{12}\log_{\delta_B}\alpha. \qquad \blacksquare$$

Nach [HS07] ist die arithmetische Schrittzahl für die HKZ-Reduktion von $\mathbf{R}_{\ell,\ell+1} \in \mathbb{R}^{2k\times 2k}$ höchstens $(2k)^{k/e+o(k))}n^{O(1)}$, jeder arithmetische Schritt hat $O((\log M)^2)$ Bitoperationen.

Alternativer Beweis zu **2. Beh.:** #**It** $\leq \frac{h^3(1+o(1))}{2}\log_{1/\delta_B}\alpha$ — auch für $\mathcal{D}_B^{Aus} \ll 1$. Für die LLL-Eingabebasis gilt $r_{j,j}^2 \leq \alpha^{n-1}\lambda_j^2$. Damit gilt für den Startwert $\mathcal{D}^{Ein}$ der Lovász Invariante $\mathcal{D}$ der Eingabebasis

$$\mathcal{D}^{Ein} = \mathcal{D}_1^{h-1}\mathcal{D}_2^{h-2}\cdots\mathcal{D}_{h-1}^1$$

$$\leq (\lambda_1^{2(h-1}\cdots\lambda_k^{2(h-1)})\,(\lambda_{k+1}^{2(h-2)}\cdots\lambda_{2k}^{2(h-2)})\cdot\cdots\cdot(\lambda_{kh-2k+1}^2\cdots\lambda_{kh-k}^2)\,\alpha^{(n-1)n\frac{h-1}{2}}.$$

Andererseits gilt für HKZ-Basen dass $r_{1,1}^2/r_{j,j}^2 \leq \alpha_j < j^{1+\ln j}$ [S87] und somit

$$\mathcal{D} \geq (\lambda_1^{2(h-1)}\cdots\lambda_k^{2(h-1)})\,(\lambda_{k+1}^{2(h-2)}\cdots\lambda_{2k}^{2(h-2)})\cdot\cdots\cdot(\lambda_{kh-2k+1}^2\cdots\lambda_{kh-k}^2)\,/n^{(1+\ln n)n(h-1)/2}$$

Der $\mathcal{D}$-Wert der Ausgabebasis ist nicht kleiner als der einer HKZ-Basis, daher folgt

$$\#\mathbf{It} \leq \log_{1/{\delta_B}^{k^2}}(\mathcal{D}^{Ein}/\mathcal{D}^{Aus})$$

$$\leq \tfrac{1}{k^2}\tfrac{(n-1)n(h-1)}{2}\log_{1/\delta_B}\alpha + \tfrac{n(h-1)}{2k^2}\log_{1/\delta_B} n^{1+\ln n}$$

$$\leq \tfrac{h^3(1+o(1))}{2}\log_{1/\delta_B}\alpha \qquad \text{sofern } \log_{1/\delta_B} n^{1+\ln n} = o(n).$$

Demgegenüber liefert der Beweis zu Satz 6.2.4, Teil **2** eine obere Schranke für #**It**, die um den Faktor $\frac{1}{6}$ kleiner ist, aber die Voraussetzung $\min_\ell \mathcal{D}_\ell/\mathcal{D}_{\ell+1} \geq 1$ gilt mit wenigen Ausnahmen.

Algorithmus 6.2.2, Beschleunigte Semi Block 2k-Reduktion

`EINGABE` LLL-Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{Z}^{m\times n}$ zu (δ_L, α), $n = hk$; δ_B mit $0 < \delta_B < 1$.

1. Wähle ℓ, $1 \le \ell < n$ so dass $\mathcal{D}_\ell/\mathcal{D}_{\ell+1}$ maximal ist.
HKZ-reduziere $\mathbf{R}_\ell$ zu $\mathbf{R}_\ell\mathbf{T}_k$ mit $\mathbf{T}_k \in \mathrm{GL}_k(\mathbb{Z})$, $\mathbf{B}_\ell := \mathbf{B}_\ell\mathbf{T}_k$.

2. HKZ-reduziere $\mathbf{R}_{\ell+1}$ zu $\mathbf{R}_{\ell+1}\mathbf{T}_k$ mit $\mathbf{T}_k \in \mathrm{GL}_k(\mathbb{Z})$,
$\mathbf{B}_{\ell+1} := \mathbf{B}_{\ell+1}\mathbf{T}_k$, längenreduziere $\mathbf{B}_\ell, \mathbf{B}_{\ell+1}$, erneuere $\mathbf{R}_{\ell,\ell+1}$.

3. HKZ-reduziere $\mathbf{R}_{\ell,\ell+1}$ zu $\mathbf{R}_{\ell,\ell+1}\mathbf{T}_{2k}$ mit $\mathbf{T}_{2k} \in \mathrm{GL}_{2k}(\mathbb{Z})$.
`IF` $\mathcal{D}_\ell^{neu} \le \delta_B^{k^2}\mathcal{D}_\ell^{alt}$ `THEN` $[\mathbf{B}_\ell, \mathbf{B}_{\ell+1}] := [\mathbf{B}_\ell, \mathbf{B}_{\ell+1}]\mathbf{T}_{2k}$, längenreduziere $\mathbf{B}_\ell, \mathbf{B}_{\ell+1}$, `GO TO 1`
HKZ-`reduziere alle` $\mathbf{R}_\ell$ zu $\mathbf{R}_\ell\mathbf{T}_k$, $\mathbf{B}_\ell := \mathbf{B}_\ell\mathbf{T}_k$, `und längenreduziere` $\mathbf{B}$.

`AUSGABE` Semi Block $2k$-Basis $\mathbf{B}$.

Satz 6.2.5 (zu Alg. 6.2.2)

1. *Bei der Wahl von ℓ ist $\mathbf{B}$ Semi Block $2k$-Basis für δ_B mit $\delta_B^k(\mathcal{D}_\ell/\mathcal{D}_{\ell+1})^{1/k} = \beta_k$.*

2. *Sobald $\max_\ell(\mathcal{D}_\ell/\mathcal{D}_{\ell+1}) \le \alpha^{k^2/2^t}\beta_k^k$ erreicht ist, erreicht Alg. 6.2.2 mit höchstens $h^3/12$ Iterationen und $\delta_B = \alpha^{-1/2^t}$ dass $\mathcal{D}_B \le 1$ und damit dass im Mittel der ℓ : $\mathcal{D}_\ell/\mathcal{D}_{\ell+1} \le \beta_k^k$.*

Beweis. 2. Wir folgen dem Beweis zu Satz 6.2.4, Teil **2**. Wie für die Schranke von $\mathcal{D}_B^{Ein}$ gilt beim Erreichen von $\max_\ell \mathcal{D}_\ell/\mathcal{D}_{\ell+1} \le \alpha^{k^2/2^t}\beta_k^k$ dass $\mathcal{D}_B \le (\alpha^{k^2/2^t}\beta_k^k)^s \le (\alpha^{k^2/2^t}\beta_k^k)^{h^3/6}$. Danach führt jeder Schritt **3** mit $\delta_B = \alpha^{-1/2^t}$ zu $\mathcal{D}_B^{neu} \le \delta_B^{2k^2}\mathcal{D}^{alt} = \alpha^{-k^2/2^t}\mathcal{D}^{alt}$. Nach $\frac{h^3}{12}\log_{1/\delta_B}\alpha$ solchen Iterationen gilt $\mathcal{D}_B^{neu} \le \beta_k^{ks} \le \beta_k^{k\,h^3/6}$ und somit im Mittel $\mathcal{D}_\ell/\mathcal{D}_{\ell+1} \le \beta_k^k$. ■

Folgerungen. Wenn für die Ausgabebasis von Alg. 6.2.2 mit $\delta_B := \alpha^{-1/2^t}$ gilt dass $\mathcal{D}_\ell/\mathcal{D}_{\ell+1} \gtrsim \beta_k^k$ für alle ℓ dann folgt $\#It \lesssim \frac{h^3}{12}$. Offen bleibt, wie sich die $\mathcal{D}_\ell^{neu}/\mathcal{D}_\ell^{alt}$ -Werte der Schritte 3 verteilen, welche $\mathcal{D}_\ell/\mathcal{D}_{\ell+1}$ weiter zu $\mathcal{D}_\ell/\mathcal{D}_{\ell+1} \ll \beta_k^k$ erniedrigen. Wenn auch hier kleine Werte $\mathcal{D}_\ell^{neu}/\mathcal{D}_\ell^{alt}$ ähnlich häufig sind, dann macht Alg. 6.2.2 mit wachsendem $\delta_B = \alpha^{-1/2^j}$ für $j = 1, ..., t$ $\delta_B = \alpha^{-1/2^t} \to 1$ für $t \to \infty$ nur $O(h^3 t)$ Iterationen, während Alg. 6.2.1 nach Satz 6.2.4 bis zu $O(h^3 2^t)$ Iterationen ausführt. Dies ermöglicht einen exponentiellen Speed-up durch Alg. 6.2.2.

6.3 Primal-Duale Reduktion

Koy's primal-duale Reduktion [Ko05] erniedrigt $\mathcal{D}_\ell = (\det \mathbf{R}_\ell)^2$ wie folgt durch HKZ-Reduktion in Dimension k: Maximiere $r_{k\ell,k\ell}$ über alle GNF von $\mathbf{R}_\ell\mathbf{T}$ mit $\mathbf{T} \in \mathrm{GL}_k(\mathbb{Z})$ zu $\max_T r_{k\ell,k\ell}$ durch HKZ-Reduktion der dualen Basis $\mathbf{R}_\ell^*$. Minimiere $r_{k\ell+1,k\ell+1}$ durch HKZ-Reduktion von $\mathbf{R}_{\ell+1}$. Danach LLL-reduziert man $\mathbf{R}_{\ell,\ell+1}$, wenn dies $r_{k\ell,k\ell}$ und damit $\mathcal{D}_\ell$ erniedrigt.

Für Gitter der Dimension $n = hk$ wird mit polynomial vielen HKZ-Reduktionen der Dimension k die Schranke $\|\mathbf{b}_1\|^2 \le \gamma_k(\alpha\gamma^2)^{\frac{h-1}{2}}(\det\mathcal{L})^{2/n}$ erreicht. Damit wird β_k/δ_B^k in Satz 6.2.3 ersetzt durch $\alpha\gamma_k^2$. Die primal-duale Reduktion iteriert HKZ-Reduktion in Dimension k, während Semi Block $2k$-Reduktion auf der HKZ-Reduktion in Dimension $2k$ aufbaut. Primal-duale Reduktion mit Blockbreite $2k$ ersetzt β_k/δ_B^k in Satz 6.2.3 durch die wohl kleinere Konstante $\sqrt{\alpha}\,\gamma_{2k} = \Theta(k)$.

Definition 6.3.1
Eine Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m\times hk}$ ist primal-duale Basis mit Blockweite k wenn

1. *$\mathbf{R}_1, ..., \mathbf{R}_h \subset \mathbf{R}$ HKZ-Basen sind und $\mathbf{B}$ längenreduziert ist,*

2. *$\max_T r_{k\ell,k\ell}^2 \le \alpha\, r_{k\ell+1,k\ell+1}^2$ für $\ell = 1, ..., h-1$, dabei wird $r_{k\ell,k\ell}^2$ von $\mathrm{GNF}(\mathbf{R}_\ell\mathbf{T})$ maximiert über alle $\mathbf{T} \in \mathrm{GL}_k(\mathbb{Z})$.*

Satz 6.3.2 (Ko04, GHKN06)
Für jede primal-duale Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m\times n}$, $n = hk$, *des Gitters* $\mathcal{L}$ *gilt:*

1. $\|\mathbf{b}_1\|^2 \le \gamma_k(\alpha\gamma_k^2)^{\frac{h-1}{2}}(\det\mathcal{L})^{2/n}$,

2. $\|\mathbf{b}_1\|^2 \le \gamma_k^2(\alpha\gamma_k^2)^{h-1}\lambda_1^2$.

Beweis. 1. Nach Def. 6.3.1 gilt für $[r_{i,j}] = R$ dass $\max_T r_{k\ell,k\ell}^2 \le \alpha\, r_{k\ell+1,k\ell+1}^2$. Die Hermite Ungleichung $\lambda_1^2(\mathcal{L}(\mathbf{R}_\ell^*)) \le \gamma_k\mathcal{D}_\ell^{-1/k}$ für $\mathcal{L}(\mathbf{R}_\ell^*)$ und die HKZ-Reduktion von $\mathbf{R}_\ell^*$ sichern dass

$$\mathcal{D}_\ell^{1/k} \le \gamma_k \max_T r_{k\ell,k\ell}^2 = \gamma_k/\lambda_1^2(\mathcal{L}(\mathbf{R}_\ell^*)).$$

Für die HKZ-Basis $\mathbf{R}_{\ell+1}$ gilt $\lambda_1^2(\mathcal{L}(\mathbf{R}_{\ell+1})) = r_{k\ell+1,k\ell+1}^2 \le \gamma_k\mathcal{D}_{\ell+1}^{1/k}$.
Die Kombination dieser beiden Ungleichungen führt mit Def. 6.3.1, **2** zu

$$\mathcal{D}_\ell^{1/k} \le \gamma_k \max_T r_{k\ell,k\ell}^2 \le \alpha\gamma_k r_{k\ell+1,k\ell+1}^2 \le \alpha\gamma_k^2\,\mathcal{D}_{\ell+1}^{1/k}. \tag{6.3}$$

Mit der HKZ-Basis $\mathbf{R}_1$ folgt durch Induktion über ℓ dass

$$\|\mathbf{b}_1\|^2 \le \gamma_k\mathcal{D}_1^{1/k} \le \gamma_k(\alpha\gamma_k^2)^\ell\mathcal{D}_{\ell+1}^{1/k} \text{ für } \ell = 0,...,h-1.$$

Die h-te Wurzel des Produkts dieser h Ungleichungen ergibt die Behauptung.
2. Die Ungleichung (6.3) gilt auch in dualer Form für $\mathcal{D}_\ell^* = (\det\mathbf{R}_\ell^*)^2$. Daher gilt auch das duale $\mathbf{1}^*$ zu Satz 6.3.2, Teil **1** :

$$\mathbf{1}^*. \quad \max_T r_{k\ell,k\ell}^2 \ge \gamma_k^{-1}(\alpha\gamma_k^2)^{\frac{-h+1}{2}}(\det\mathcal{L})^{2/n}$$

$$\text{mit } r_{k\ell,k\ell}^2 \text{ maximiert über die GNF von } \mathbf{R}_\ell\mathbf{T} \text{ mit } \mathbf{T} \in \mathrm{GL}_k(\mathbb{Z})$$

1 und $\mathbf{1}^*$ ergeben zusammen $\|\mathbf{b}_1\|^2 \le \gamma_k^2(\alpha\gamma_k^2)^{\ell-1}\max_T r_{k\ell,k\ell}^2$. Somit liefert Def. 6.3.1 Teil **2.**

$$\|\mathbf{b}_1\|^2 \le \gamma_k^2(\alpha\gamma_k^2)^{\ell-1}\max_T r_{k\ell,k\ell}^2$$
$$\le (\alpha\gamma_k^2)^\ell r_{k\ell+1,k\ell+1}^2 \text{ für } \ell = 0,...,h-1.$$

Es folgt die Behauptung, denn es gilt für $\mathbf{b} = \sum_{j=1}^{\bar n} u_j\mathbf{b}_j \in \mathcal{L}$, $u_{\bar n} \ne \mathbf{0}$ mit $norm\mathbf{b}_1 = \lambda_1$ O.B.d.A. dass $\bar n > n-k$ und folglich $r_{n-k+1,n-k+1} \le \|\pi_{n-k+1}(\mathbf{b})\| \le \lambda_1$. ■

Erläuterungen zu Alg. 6.3.1.
1. Schritt 2 maximiert den letzten Diagonaleintrag $r_{k,k}$ von $\mathrm{GNF}(\mathbf{R}_\ell\mathbf{T}) \in \mathbb{R}^{k\times k}$ über alle $\mathbf{T} \in \mathrm{GL}_k(\mathbb{Z})$ wie folgt: HKZ-reduziere $\mathbf{R}_\ell^* = \mathbf{U}_k\mathbf{R}_\ell^{-t}\mathbf{U}_k$ zu $\mathbf{R}_\ell^*\mathbf{T}_*$ mit $\mathbf{T}_* \in \mathrm{GL}_k(\mathbb{Z})$. Diese HKZ-Reduktion minimiert den ersten Diagonaleintrag $r_{1,1}$ von $\mathrm{GNF}(\mathbf{R}_\ell^*\mathbf{T}_*)$ und $1/r_{1,1}$ ist der letzte Diagonaleintrag von $\mathrm{GNF}(\mathbf{R}_\ell\mathbf{U}_k\mathbf{T}_*^{-t}\mathbf{U}_k)$. Die Transformation $\mathbf{T}_*$ von $\mathbf{R}_\ell^*$ wird als Transformation $\mathbf{U}_k\mathbf{T}_*^{-t}\mathbf{U}_k$ auf $\mathbf{R}_\ell$ übertragen.
2. Bei der LLL-Reduktion von $\mathbf{R}_{\ell,\ell+1}$ in Schritt **3** sind nur Austausche der Spalten k und $k+1$ von $\mathbf{R}_{\ell,\ell+1}$ möglich. Denn das letzte Diagonalement $r_{k,k}$ von $\mathbf{R}_\ell$ ist maximal und $r_{k-i,k-i}$ ist maximal bei festen $r_{k-i_1,k-i+1},...,r_{k,k}$. Ebenso sind die Diagonalemente von $\mathbf{R}_{\ell+1}$ nininimal wenn alle vorangehenden Diagonalelemente von $\mathbf{R}_{\ell+1}$ festgehalten werden.

Algorithmus 6.3.1, Primal-Duale Reduktion

EINGABE LLL-Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{Z}^{m\times n}$, $n = hk$, zu δ, α.

0. $\ell := 1$

1. HKZ-reduziere $\mathbf{R}_{\ell+1}$ zu $\mathbf{R}_{\ell+1}\mathbf{T}_k$ mit $\mathbf{T}_k \in \mathrm{GL}_k(\mathbb{Z})$, $\mathbf{B}_{\ell+1} := \mathbf{B}_{\ell+1}\mathbf{T}_k$

2. HKZ-reduziere $\mathbf{R}_\ell^*$ zu $\mathbf{R}_\ell^*\mathbf{T}_\star$ mit $\mathbf{T}_\star \in \mathrm{GL}_k(\mathbb{Z})$, $\mathbf{B}_\ell := \mathbf{B}_\ell\mathbf{U}_k\mathbf{T}_\star^{-t}\mathbf{U}_k$,
längenreduziere $\mathbf{B}_\ell, \mathbf{B}_{\ell+1}$, erneuere $\mathbf{R}_{\ell,\ell+1}$, LLL-reduziere $\mathbf{R}_{\ell,\ell+1}$ mit δ zu $\mathbf{R}_{\ell,\ell+1}\mathbf{T}_{2k}$

3. IF in Schritt **2** erfolgte ein LLL-Austausch der Spalten k und $k+1$ von $\mathbf{R}_{\ell,\ell+1}$
THEN $[\mathbf{B}_\ell, \mathbf{B}_{\ell+1}] := [\mathbf{B}_\ell, \mathbf{B}_{\ell+1}]\mathbf{T}_{2k}$, längenreduziere $\mathbf{B}_\ell, \mathbf{B}_{\ell+1}$, $\ell := \max(\ell-1, 1)$
ELSE $\ell := \ell + 1$

4. IF $\ell < h$ THEN GO TO **1**

AUSGABE primal-duale Basis $\mathbf{B}$

Satz 6.3.3

1. *Alg. 6.3.1 macht höchstens* $2nh\log_{1/\delta} M$ *Iterationen für den Wert* $M := \max(\|\mathbf{b}_1\|, ..., \|\mathbf{b}_n\|)$ *der Eingabebasis. Eine Iteration geht in* $k^{\frac{k}{2e}+o(k))}n^{O(1)}$ *arithmetischen Schritten mit jeweils* $O((\log M)^2)$ *Bitoperationen..*

2. *Alg. 6.3.1 macht höchstens* $\frac{n^2h}{12}\log_{1/\delta}\alpha$ *Iterationen bis* $\mathcal{D}_B \le 1$ *erreicht ist.*

Beweis. **1.** Jeder Schritt **3** mit $\ell := \max(\ell-1, 1)$ erniedrigt $\mathcal{D} := \mathcal{D}_1^{h-1}\mathcal{D}_2^{h-2}\cdots\mathcal{D}_{h-1}^1$ so dass $\mathcal{D}^{neu} \le \delta\,\mathcal{D}^{alt}$ für das $\delta < 1$ der LLL-Reduktion und $\mathcal{D}_\ell = (\det\mathbf{R}_\ell)^2$.

Die Eingabebasis hat den $\mathcal{D}_B$-Wert $\mathcal{D}^{Ein} \le M^{n(h-1)}$ und für die Ausgabebasis gilt $\mathcal{D}^{Aus} \ge 1$. Dies beschränkt die Anzahl $\#It^-$ der Schritte **3** mit $\ell := \max(\ell-1, 1)$ zu

$$\#\mathbf{It}^- \le \log_{1/\delta}\mathcal{D}^{Ein} \le n(h-1)\log_{1/\delta} M.$$

Die Gesamtzahl $\#\mathbf{It}$ der Schritte **3** ist $\#\mathbf{It} = h - 1 + 2\#\mathbf{It}^- \le 2nh\log_{1/\delta} M$.

2. Wir folgen dem Beweis von Satz 6.2.4, Teil **2**. Jede Iteration mit $\mathcal{D}_\ell^{neu} \le \delta\,\mathcal{D}_\ell^{alt}$ erniedrigt wie gezeigt $\mathcal{D}_B$ zu $\mathcal{D}_B^{\text{neu}} \le \delta^2\mathcal{D}_B^{alt}$. Für die Anzahl $\#\mathbf{It}$ der Iterationen bis zum Erreichen von $\mathcal{D}_B \le 1$ folgt mit $s = \sum_{\ell=1}^{h}(h^2/4 - (h/2-\ell)^2) = (h^3-h)/6$

$$\#\mathbf{It} \le \tfrac{1}{2}\log_{1/\delta}\mathcal{D}_B^{Ein} \le \tfrac{1}{2}\log_{1/\delta}\alpha^{k^2 s} \le \tfrac{k^2h^3}{12}\log_{1/\delta}\alpha = \tfrac{n^2h}{12}\log_{1/\delta}\alpha.$$

Die Schranken für die Anzahl der Iterationen $\#\mathbf{It}$ der Algorithmen 6.3.1 und 6.2.1 fallen für $\delta = \delta_B^{k^2}$ zusammen. ∎

Die Klausel **2.** von Def. 6.3.1 wurde von Gama, Nguyen [GN08b] verschärft zu

$\mathbf{2}^+$. $\max_{\mathbf{R}'_\ell\mathbf{T}} r_{k\ell+1,k\ell+1} \le (1+\varepsilon)\,r_{k\ell+1,k\ell+1}$ für $\ell = 1, ..., h-1$. (*slide-reduction* [GN08b])

Es bezeichne $\mathbf{R}'_\ell := [r_{i,j}]_{k\ell-k+2\le i,j\le k\ell+1} \in \mathbb{R}^{k\times k}$ das um eine Einheit nach rechts verschobene Segment $\mathbf{R}_\ell$ von $\mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n\times n}$. Es bezeichnet $\max_{\mathbf{R}'_\ell\mathbf{T}} r^2_{k\ell+1,k\ell+1}$ das Maximum über $\bar{r}^2_{k\ell+1,k\ell+1}$ von $[\bar{r}_{i,j}] = \mathrm{GNF}(\mathbf{R}'_\ell\mathbf{T})$ über alle $\mathbf{T} \in \mathrm{GL}_k(\mathbb{Z})$. Ferner sei $\mathbf{B}'_\ell = [\mathbf{b}_{k\ell-k+2}, ..., \mathbf{b}_{k\ell+1}]$ der um eine Einheit nach rechts verschobenen Block $\mathbf{B}_\ell$.

Definition 6.3.4

Eine längenreduzierte Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m\times n}$ *mit* $n = hk$ *ist* streng primal-dual*, wenn* $\mathbf{R}_1, ..., \mathbf{R}_h$ *HKZ-Basen sind und wenn* $\mathbf{2}^+$ *für ein* $\ell = \ell_{max}$ *gilt, welches* $\mathcal{D}_\ell/\mathcal{D}_{\ell+1}$ *maximiert.*

Satz 6.3.5 (GN08b)
Für jede streng primal-duale Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m\times n}$, $n = hk$ *und* $\varepsilon > 0$, *des Gitters* $\mathcal{L}$ *gilt:*

1. $\|\mathbf{b}_1\| < ((1+\varepsilon)\,\gamma_k)^{\frac{1}{2}\frac{n-1}{k-1}}(\det\mathcal{L})^{1/n}$,

2. $\|\mathbf{b}_1\| < ((1+\varepsilon)\,\gamma_k)^{\frac{1}{2}\frac{n-1}{k-1}}/(\sqrt{\gamma_n}\det\mathcal{L})\lambda_1 \quad$ *wegen* $\lambda_1^2 = \gamma_n rd(\mathcal{L})\det(\mathcal{L})^{2/n}$.

Beweis. Nach Hermite gilt für die HKZ-Basis $\mathbf{R}_\ell$ dass $r^{2k}_{k\ell-k+1,k\ell-k+1} \le \gamma_k^k\,\mathcal{D}_\ell$. Das duale dieser Ungleichung ergibt für $\mathcal{D}'_\ell := (\det R'_\ell)^2$ dass $\max\limits_{\mathbf{R}'_\ell\mathbf{T}} r^{2k}_{k\ell+1,k\ell+1} \ge \mathcal{D}'_\ell/\gamma_k^k$ für $\mathbf{T}\in\mathrm{GL}_k(\mathbb{Z})$.
Für $\ell = \ell_{max}$ folgt damit aus $\mathbf{2}^+$ für jede streng primal-duale Basis dass

$$\mathcal{D}'_\ell \le (1+\varepsilon)^{2k}\gamma_k^k\, r^{2k}_{k\ell+1,k\ell+1}. \tag{6.4}$$

Kombination von (6.4) mit $r^{2k}_{k\ell-k+1,k\ell-k+1} \le \gamma_k^k\,\mathcal{D}_\ell$ und $\mathcal{D}'_\ell/r^2_{k\ell+1,k\ell+1} = \mathcal{D}_\ell/r^2_{k\ell-k+1,k\ell-k+1}$ liefert

$$r_{k\ell-k+1,k\ell-k+1} \le ((1+\varepsilon)\,\gamma_k)^{\frac{k}{k-1}} r_{k\ell+1,k\ell+1} \quad \text{für } \ell = \ell_{max} \text{ und } \ell = h-1. \tag{6.5}$$

Für $\ell = \ell_{max}$ folgt aus (6.4) und $r^{2k}_{k\ell-k+1,k\ell-k+1} \le \gamma_k^k\,\mathcal{D}_\ell$ dass
$\mathcal{D}'_\ell \le (1+\varepsilon)^{2k}\gamma_k^k r^{2k}_{k\ell+1,k\ell+1} \le (1+\varepsilon)^{2k}\gamma_k^{2k}\mathcal{D}_{\ell+1}$. Aus (6.5) folgt

$$\mathcal{D}_\ell = r^2_{k\ell-k+1,k\ell-k+1}\mathcal{D}'_\ell/r^2_{k\ell+1,k\ell+1} \le ((1+\varepsilon)\,\gamma_k)^{\frac{2k}{k-1}}\mathcal{D}'_\ell. \tag{6.6}$$

Die Kombination der beiden vorangehenden Ungleichungen liefert für $\ell = \ell_{max}$

$$\mathcal{D}_\ell \le ((1+\varepsilon)\,\gamma_k)^{\frac{2k}{k-1}+2k}\mathcal{D}_{\ell+1} \le ((1+\varepsilon)\,\gamma_k)^{\frac{2k^2}{k-1}}\mathcal{D}_{\ell+1}. \tag{6.7}$$

Somit gilt für ℓ_{max} und damit auch für alle $\ell = 1,...,h-1$ dass $\mathcal{D}_\ell \le ((1+\varepsilon)\,\gamma_k)^{\frac{2k^2}{k-1}}\mathcal{D}_{\ell+1}$.

1. Für die HKZ-Basis $\mathbf{R}_1$ folgt somit für $\ell = 1,...,h$ dass

$$\|\mathbf{b}_1\|^2 \le \gamma_k\mathcal{D}_1^{1/k} \le \gamma_k((1+\varepsilon)\,\gamma_k)^{\frac{2k(\ell-1)}{k-1}}\mathcal{D}_\ell^{1/k}.$$

Multiplikation dieser h Ungleichungen und $\sum_{\ell=1}^h(\ell-1) = \frac{h(h-1)}{2}$ liefert

$$\|\mathbf{b}_1\|^{2h} \le \gamma_k^h((1+\varepsilon)\,\gamma_k)^{\frac{kh(h-1)}{k-1}}(\det\mathcal{L})^{2/k.}$$

Es folgt die Behauptung

$$\|\mathbf{b}_1\|^2 \le \gamma_k((1+\varepsilon)\,\gamma_k)^{\frac{n-k}{k-1}}(\det\mathcal{L})^{2/n} < ((1+\varepsilon)\,\gamma_k)^{\frac{n-1}{k-1}}(\det\mathcal{L})^{2/n}. \qquad \blacksquare$$

Algorithmus 6.3.2, Beschleunigte, Streng Primal-Duale Reduktion

`EINGABE` LLL-Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{Z}^{m\times n}$, $n = hk$, $\varepsilon > 0$.

1. Wähle ℓ, $1 \le \ell < n$ so dass $\mathcal{D}_\ell/\mathcal{D}_{\ell+1}$ maximal ist.

2. HKZ-reduziere $\mathbf{R}_{\ell+1}$ zu $\mathbf{R}_{\ell+1}\mathbf{T}$ mit $\mathbf{T}\in\mathrm{GL}_k(\mathbb{Z})$, $\mathbf{B}_{\ell+1} := \mathbf{B}_{\ell+1}\mathbf{T}$, längenreduziere $\mathbf{B}_{\ell+1}$, erneuere $\mathbf{R}_{\ell+1}$. HKZ-reduziere $(\mathbf{R}'_\ell)^*$ zu $(\mathbf{R}'_\ell)^*\mathbf{T}_\star$ mit $\mathbf{T}_\star\in\mathrm{GL}_k(\mathbb{Z})$, $[r^{neu}_{k\ell+i,k\ell+j}]_{2\le i,j\le 1+k} := \mathrm{GNF}(\mathbf{R}'_\ell\mathbf{T}_\star^{-1}\mathbf{U}_k)$,

3. `IF` $r^{neu}_{k\ell+1,k\ell+1} > (1+\varepsilon)\,r^{alt}_{k\ell+1,k\ell+1}$ `THEN` $\mathbf{B}'_\ell := \mathbf{B}'_\ell T_\star^{-1}\mathbf{U}_k$, längenreduziere $\mathbf{B}'_\ell$, erneuere $\mathbf{R}_{\ell,\ell+1}$, `GO TO 1`

`AUSGABE` streng primal-duale Basis $\mathbf{B}$.

Satz 6.3.6
Alg. 6.3.2 führt höchstens $\frac{n^2h}{24}\log_{1+\varepsilon}\alpha$ *Iterationen durch bis* $\mathcal{D}_B \le 1$ *erreicht ist.*

Beweis. Ein aktiver Schritt **3** bewirkt $\mathcal{D}_\ell^{neu} \le \mathcal{D}_\ell^{alt}/(1+\varepsilon)^2$, somit $\mathcal{D}_B^{neu} \le \mathcal{D}'^{alt}_B/(1+\varepsilon)^4$. Für die LLL-basis $\mathbf{B}$ der Eingabe gilt $\mathcal{D}_B^{Ein} \le \alpha^{k^2 \frac{h^3-h}{6}}$. Es folgt $\#It \le \frac{k^2h^3}{24} \log_{1+\varepsilon} \alpha$ bis $\mathcal{D}_B \le 1$. ■

[GN08b] fordert für slide-reduzierte Basen dass $\mathbf{2}^+$, mit $(1+\varepsilon)$ ersetzt durch $\sqrt{1+\varepsilon}$, für alle $\ell \le h-1$ gilt; es wird in etwa Satz 6.3.4 für slide reduzierte Basen gezeigt. Weil wir die Bedingung $\mathbf{2}^+$ nur für ℓ_{max} fordern, macht Alg. 6.3.2 zur streng primal-dualen Reduktion höchstens 2 HKZ-Reduktionen der Dim. k pro Iteration und ist damit deutlich schneller als die slide Reduktion von [GN08b].

6.4 Block-Korkine Zolotareff Reduktion, BKZ

Definition 6.4.1 (k-reduzierte Basis)
Eine Basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n] = \mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m \times n}$ *ist* k-reduziert, *wenn*

1. $|r_{i,j}| \le \frac{1}{2} r_{i,i}$ *für* $1 \le i < j \le n$

2. *Die Basen* $[r_{i,j}]_{\ell < i,j \le \ell+k} \in \mathbb{R}^{k \times k}$ *für* $\ell = 0, ..., n-k$ *sind* HKZ-*Basen.*

Jede k-reduzierte Basis ist $(k-1)$-reduziert. Es sei stets $k \ge 2$ sonst ist die Eigenschaft **2.** leer.

Satz 6.4.2
Die 2-reduzierten Basen sind genau die LLL-Basen zu $\delta = 1$.

Beweis. Sei $\mathbf{b}_1, \ldots, \mathbf{b}_n$ eine 2-reduzierte Basis. Dann gilt für $i = 1, \ldots, n-1$:

$$\lambda_1\big(\pi_i \mathcal{L}(\mathbf{b}_i, \mathbf{b}_{i+1})\big)^2 = r_{i,i}^2 \le r_{i,i+1}^2 + r_{i+1,i+1}^2.$$

Für $\delta = 1$ ist dies die zweite LLL-Eigenschaft. Ferner ist $\mathbf{b}_1, \ldots, \mathbf{b}_n$ längenreduziert und somit LLL-Basis.

Umgekehrt ist offenbar jede LLL-Basis für $\delta = 1$ auch 2-reduziert. ■

Die Approximationsfaktoren von k-reduzierten Basen sind wie folgt durch die Hermite-Konstante γ_k nach oben und unten beschränkt.

Satz 6.4.3 (S94)
Für jede k*-reduzierte Basis* $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *des Gitters* $\mathcal{L}$ *gilt mit der Hermite-Konstanten* γ_k

1. $\|\widehat{\mathbf{b}}_i\|^2/\lambda_i(\mathcal{L})^2 \le \gamma_k^{2\frac{n-i}{k-1}}$ *für* $i = 1, \ldots, n$,

2. $\|\mathbf{b}_i\|^2/\lambda_i(\mathcal{L})^2 \le \gamma_k^{2\frac{n-i}{k-1}\frac{i+3}{4}}$ *für* $i = 1, \ldots, n$.

Verdoppelung der Blockweite k reduziert somit den Approximationsfaktor $\gamma_k^{2\frac{n-i}{k-1}}$ annähernd auf die Quadratwurzel multiplixiert mit $2^{2/k}$.

Wie für LLL- und HKZ-Basen sind die oberen Schranken zu $\frac{\|\mathbf{b}_i\|^2}{\lambda_i(\mathcal{L})^2}$ und $\frac{\lambda_i(\mathcal{L})^2}{\|\mathbf{b}_i\|^2}$ fast gleich.

Satz 6.4.4
Für jede k*-reduzierte Basis* $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *des Gitters* $\mathcal{L}$ *gilt*

$$\lambda_i(\mathcal{L})^2/\|\mathbf{b}_i\|^2 \le \gamma_k^{2\frac{i-1}{k-1}\frac{i+3}{4}} \qquad \text{für } i = 1, \ldots, n.$$

Die Werte $\gamma_k^{\frac{2}{k-1}}$ sind bekannt für $k = 2, 3, \ldots, 8, 24$:

k	2	3	4	5	6	7	8	24
$\gamma_k^{\frac{2}{k-1}}$	$\frac{4}{3}$	$2^{1/3}$	$2^{1/3}$	$2^{3/10}$	$2^{2/5}/3^{15}$	$2^{2/7}$	$2^{2/7}$	$2^{4/23}$
$\approx$	1,333	1,260	1,260	1,231	1,226	1,219	1,219	1.128

Ajtai [Aj03] zeigt, dass die Schranken von Satz 6.4.3 bis auf einen konstanten Faktor im Exponenten von γ_k optimal sind. Dagegen sind die minimalen oberen Schranken $C_{k,n}$ zum Satz 6.4.3 nicht bekannt Die Schranke aus Satz 6.4.3 ist für $n \geq 3$ nicht scharf. Es gilt dass $C_{2,n} = \left(\frac{4}{3}\right)^{n-1}$ [BaKa84] und $C_{3,n} = \left(\sqrt{3/2}\right)^{n-3}$ für ungerade $n \geq 3$ [S94].

Lemma 6.4.5
Für jede k-reduzierte Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ *gilt* $\|\mathbf{b}_1\| \leq \gamma_k^{\frac{n-1}{k-1}} M$ *mit*
$M := \max\left(\|\widehat{\mathbf{b}}_{n-k+2}\|, \ldots, \|\widehat{\mathbf{b}}_n\|\right)$.

Beweis. Wir erweitern die Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ durch $k-2$ linear unabhängige Vektoren zu

$$\mathbf{b}_{-k+3}, \ldots, \mathbf{b}_{-1}, \mathbf{b}_0, \mathbf{b}_1, \ldots, \mathbf{b}_n \tag{6.8}$$

so, dass gilt

$$\|\mathbf{b}_i\| = \|\mathbf{b}_1\| \qquad \text{für } i \leq 0 \tag{6.9}$$
$$\langle \mathbf{b}_i, \mathbf{b}_j \rangle = 0 \qquad \text{für } i \leq 0,\ i\ < j \text{ und } j = -k+3, \ldots, n. \tag{6.10}$$

Dazu betten wir die Basis in den $\mathbb{R}^{m+k-2}$ ein: Wir wählen $\mathbf{b}_{-k+3}, \mathbf{b}_{-k+4}, \ldots, \mathbf{b}_{-1}, \mathbf{b}_0$ als $\|\mathbf{b}_1\|$-Vielfaches der kanonischen Einheitsvektoren in die zusätzlichen $k-2$ Richtungen. Die Gitterbasis (6.8) ist k-reduziert. Für jedes i mit $-k+3 \leq i \leq n-k+1$ bilden die Vektoren

$$\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_{i+k-1})$$

eine HKZ-reduzierte Basis. Nach Definition der Hermite-Konstanten γ_k gilt

$$\|\widehat{\mathbf{b}}_i\|^k \leq \gamma_k^{\frac{k}{2}} \prod_{s=0}^{k-1} \|\widehat{\mathbf{b}}_{i+s}\| \text{ für } i = -k+3, \ldots, n-k+1.$$

Durch Multiplikation dieser $n-1$ Ungleichungen erhalten wir

$$\prod_{i=-k+3}^{n-k+1} \|\widehat{\mathbf{b}}_i\|^k \leq (\gamma_k)^{\frac{k(n-1)}{2}} \|\widehat{\mathbf{b}}_{-k+3}\|^1 \|\widehat{\mathbf{b}}_{-k+4}\|^2 \cdots \|\widehat{\mathbf{b}}_1\|^{k-1}$$

$$\cdot \|\widehat{\mathbf{b}}_2\|^k \|\widehat{\mathbf{b}}_3\|^k \cdots \|\widehat{\mathbf{b}}_{n-k+1}\|^k \quad \|\widehat{\mathbf{b}}_{n-k+2}\|^{k-1} \cdots \|\widehat{\mathbf{b}}_{n-1}\|^2 \|\widehat{\mathbf{b}}_n\|^1.$$

Durch Kürzen folgt

$$\|\widehat{\mathbf{b}}_{-k+3}\|^{k-1} \cdots \|\widehat{\mathbf{b}}_0\|^2 \|\widehat{\mathbf{b}}_1\|^1 \leq (\gamma_k)^{\frac{k(n-1)}{2}} \|\widehat{\mathbf{b}}_{n-k+2}\|^{k-1} \|\widehat{\mathbf{b}}_{n-k+2}\|^{k-1} \cdots \|\widehat{\mathbf{b}}_{n-1}\|^2 \cdot \|\widehat{\mathbf{b}}_n\|^1.$$

Nach Konstruktion gilt $\|\widehat{\mathbf{b}}_i\| = \|\mathbf{b}_1\|$ für $i \leq 0$ und es folgt

$$\|\mathbf{b}_1\|^{\binom{k}{2}} \leq (\gamma_k)^{\frac{k(n-1)}{2}} \cdot M^{\binom{k}{2}} \text{ und somit } \|\mathbf{b}_1\| \leq \gamma_k^{\frac{n-1}{k-1}} M. \qquad \blacksquare$$

Korollar 6.4.6
Für jede k-reduzierte Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *des Gitters* $\mathcal{L}$ *gilt* $\|\mathbf{b}_1\| \leq \gamma_k^{\frac{n-1}{k-1}} \lambda_1(\mathcal{L})$.

Die Schranke von Korollar 6.4.6 ist suboptimal für $k \approx n$ denn für $k = n$ gilt $\|\mathbf{b}_1\| = \lambda_1$. Sie ist besser als die in Theorem 2.6 [S87] für den Fall $k|n$ bewiesene Schranke $\|\mathbf{b}_1\| \leq \gamma_{k/2}^{1/2} (2k)^{\frac{n}{k}-1} \lambda_1$.

Beweis. Induktion über n: Für $n = k$ ist $\mathbf{b}_1, \ldots, \mathbf{b}_n$ eine HKZ-Basis mit $\|\mathbf{b}_1\| = \lambda_1(\mathcal{L})$ und somit gilt die Behauptung.

Sei $n > k$ und $\mathbf{v} \neq 0$ ein kürzester Gittervektoren. O.B.d.A. sei $\mathbf{v} \notin \mathcal{L}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{n-1})$, denn sonst folgt die Behauptung aus der Induktionsannahme für $n-1$. Wegen $\mathbf{v} \notin \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$ gilt $\pi_i(\mathbf{v}) \neq 0$ für $i = n-k+1, \ldots, n-1$. Wir erhalten mit $\mathcal{L}_i = \pi_i(\mathcal{L})$ für $i = n-k+1, \ldots, n$:

$$\lambda_1(\mathcal{L}) = \|\mathbf{v}\| \geq \lambda_1(\mathcal{L}_i) = \|\widehat{\mathbf{b}}_i\|.$$

Die Gleichheit $\lambda_1(\mathcal{L}_i) = \|\widehat{\mathbf{b}}_i\|$ gilt, weil $\pi_{n-k+1}(\mathbf{b}_i)$, für $i = n-k+1, \ldots, n$ HKZ-Basis ist. Für das M von Lemma 6.4.5 gilt $\lambda_1(\mathcal{L}) \geq \max\left\{\|\widehat{\mathbf{b}}_i\| : i = n-k+1, \ldots, n\right\} = M$. Somit folgt die Behauptung aus Lemma 6.4.5: $\|\mathbf{b}_1\| \leq (\gamma_k)^{\frac{n-1}{k-1}} \cdot M \leq (\gamma_k)^{\frac{n-1}{k-1}} \cdot \lambda_1(\mathcal{L})$. ■

Beweis (zu Satz 6.4.3). . Korollar 6.4.6 liefert für die Gitter $\mathcal{L}_i = \pi_i(\mathcal{L})$ mit $i = 1, \ldots, n$:

$$\|\widehat{\mathbf{b}}_i\| \leq \gamma_k^{\frac{n-i}{k-1}} \lambda_1(\mathcal{L}_i) \tag{6.11}$$

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

Wir erhalten die erste Behauptung, daß für $i = 1, \ldots, n$ gilt: $\frac{\|\widehat{\mathbf{b}}_i\|^2}{\lambda_i(\mathcal{L})^2} \leq \gamma_k^{2 \cdot \frac{n-i}{k-1}}$.

Aus (6.11), $\mu_{i,j}^2 \leq \frac{1}{4}$ (die Basis ist längenreduziert) und $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_j$ folgt:

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

Wir schätzen die Summanden durch $\gamma_k^{2 \cdot \frac{-1}{k-1}}$ nach oben ab und erhalten:

$$\begin{aligned}
\|\mathbf{b}_i\|^2 &\leq \gamma_k^{2 \cdot \frac{n}{k-1}} \cdot \gamma_k^{2 \cdot \frac{-1}{k-1}} \cdot \left(1 + \frac{i-1}{4}\right) \cdot \lambda_i(\mathcal{L})^2 \\
&\leq \gamma_k^{2 \cdot \frac{n-1}{k-1}} \cdot \frac{i+3}{4} \cdot \lambda_i(\mathcal{L})^2
\end{aligned}$$

Damit haben wir die zweite Behauptung auch gezeigt. ■

Beweis (zu Satz 6.4.4). Nach Definition der sukzessiven Minima gilt $\lambda_i^2 \leq \max_{j=1,\ldots,i} \|\mathbf{b}_j\|^2$. Für $B = QR$, $R = [r_{i,j}] \in \mathbb{R}^{n \times n}$ gilt $\|\mathbf{b}_i\|^2 = \sum_{j=1}^{i} r_{j,i}^2 \leq \frac{1}{4} \sum_{j=1}^{n} r_{j,j}^2$ und somit

$$\lambda_i^2 \leq \tfrac{i+3}{4} \cdot \max_{j=1,\ldots,i} \|\widehat{\mathbf{b}}_j\|^2 \tag{6.12}$$

Lemma 6.4.5 angewandt auf die k-reduzierte Basis $\pi_j(\mathbf{b}_j), \ldots, \pi_j(\mathbf{b}_i)$ liefert für $1 \leq j \leq i-k+1$:

$$\|\widehat{\mathbf{b}}_j\| \leq \gamma_k^{\frac{i-j}{k-1}} \max(\|\widehat{\mathbf{b}}_{i-k+2}\|, \ldots, \|\widehat{\mathbf{b}}_i\|). \tag{6.13}$$

Andererseits gilt für $i-k+2 \leq j \leq i$

$$\|\widehat{\mathbf{b}}_j\| \leq \|\pi_j(\mathbf{b}_j)\| \leq \|\mathbf{b}_i\| \tag{6.14}$$

Aus (6.13) und (6.14) erhalten wir für $1 \leq j \leq i$: $\|\widehat{\mathbf{b}}_j\| \leq \gamma_k^{\frac{i-j}{k-1}} \|\mathbf{b}_i\|$. Diese Ungleichung liefert mit (6.12) die Behauptung, daß für $i = 1, \ldots, n$ gilt:

$$\lambda_i(\mathcal{L})^2 / \|\mathbf{b}_i\|^2 \leq \gamma_k^{2\frac{i-1}{k-1}\,\frac{i+3}{4}}.$$ ■

6.5 BKZ-Algorithmus

Definition 6.5.1 ((k,δ)-reduzierte Basis)
Eine Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m \times n}$ ist (k,δ)-reduziert zu $2 \leq k \leq n$ und $\frac{1}{4} < \delta < 1$ wenn

1. $|r_{i,j}| \leq \frac{1}{2} r_{i,i}$ *für* $1 \leq i < j \leq n$,

2. $\delta\, r_{j,j}^2 \leq \lambda_1 \left(\pi_j\, \mathcal{L}(\mathbf{b}_j, \ldots, \mathbf{b}_{j+k-1}) \right)^2$ *für* $j = 1, \ldots, n-k+1$.

Algorithmus 6.5.1, BKZ-Algorithmus

`EINGABE`: LLL-Basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n] = \mathbf{B} = \mathbf{QR} \in \mathbb{Z}^{m \times n}$, $2 \leq k \leq n$, $\frac{1}{4} < \delta < 1$.

`FOR` $j = 1, ..., n-1$ `DO`

$\bar{j} := \min(j+k-1, n)$

`ENUM`$(j, \bar{j})$: Find minimal point $(u_j, \ldots, u_{\bar{j}}) \in \mathbb{Z}^k \setminus \{\mathbf{0}\}$ of:

$c_j(u_j, \ldots, u_{\bar{j}}) := \sum_{i=j}^{\bar{j}} \sum_{s=j}^{i} (u_i r_{s,i})^2 = \|\pi_j(\sum_{i=j}^{\bar{j}} u_i \mathbf{b}_i)\|^2$,

$\mathbf{b}_j^{\text{neu}} := \sum_{s=j}^{\bar{j}} u_s \mathbf{b}_s, \quad \bar{c}_j := c_j(u_j, \ldots, u_{\bar{j}})$.

`IF` $\delta c_j > \bar{c}_j$ `THEN` $L^3FP(\mathbf{b}_1, \ldots, \mathbf{b}_{j-1}, \mathbf{b}_j^{\text{neu}}, \mathbf{b}_j, \ldots, \mathbf{b}_{j+k}, \delta)$

`ELSE` $L^3FP(\mathbf{b}_1, \ldots, \mathbf{b}_{j+k}, \delta)$

`IF some` $\mathbf{b}_j$ `has been changed THEN repeat with the new basis` B `ELSE` terminate

`AUSGABE` (k,δ)-reduzierte Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$.

Der Algorithmus 6.5.1 aus [SE94] transformiert eine gegebene Basis in eine (k,δ)-reduzierte Basis des gleichen Gitters. Die Routine L^3FP aus Kapitel 4.4 macht LLL-Reduktion mit Gleitkommazahlen; Sie transformiert linear abhängige Eingabevektoren in eine Basis mit vorangehenden Nullvektoren. Die Routine ENUM$(j, \bar{j})$ minimiert $c_j(u_j, \ldots, u_{\bar{j}})$, siehe Algorithmus 8.1.1 und GAUSS-ENUM in Kapitel 8.

Offenbar ist eine Ausgabebasis (k,δ)-reduziert. Die Variable j wird zyklisch durch die Zahlen $1, \ldots, n-k+1$ geschoben. Durch LLL-Reduktion wird die Ausgabebasis längenreduziert. In der Praxis [SE94, GN08a] ist der Algorithmus für $k \leq 20$ recht schnell. Zu experimentell erreichten Approximationsfaktoren $\|\mathbf{b}_1\|/\lambda_1$ und Laufzeiten siehe [GN08a].

6.6 Kritische k-reduzierte Basen für $k = 2, 3$

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

Definition 6.6.1 (kritische k-reduzierte Basis)
Eine k-reduzierte Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ des Gitters $\mathcal{L}$ heißt kritisch für n und k, falls $\frac{\|\mathbf{b}_1\|}{\lambda_1(\mathcal{L})}$ maximal für alle k-reduzierten Basen vom Rang n ist.

Für $k = 2$ konstruieren wir die Basismatrix $\mathbf{A}_n := [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in M_{n,n}(\mathbb{R})$ wie folgt. Sei $\rho := \sqrt{\frac{3}{4}}$:

$$\mathbf{A}_n := \begin{bmatrix} 1 & \frac{1}{2} & 0 & \cdots & \cdots & 0 \\ 0 & \rho & \frac{1}{2}\rho & \ddots & 0 & \vdots \\ \vdots & 0 & \rho^2 & \frac{1}{2}\rho^2 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ \vdots & & & \ddots & \rho^{n-2} & \frac{1}{2}\rho^{n-2} \\ 0 & \cdots & \cdots & \cdots & 0 & \rho^{n-1} \end{bmatrix} \tag{6.15}$$

Es gilt für $n \geq 2$

$$\mathbf{A}_2 := \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \sqrt{\frac{3}{4}} \end{bmatrix} \qquad \mathbf{A}_n := \begin{bmatrix} 1 & \frac{1}{2} & 0 & \cdots & 0 \\ 0 & & & & \\ \vdots & & & \rho \cdot A_{n-1} & \\ 0 & & & & \end{bmatrix}$$

Satz 6.6.2
Für die Basismatrix $\mathbf{A}_n = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$, des Gitters $\mathcal{L} = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ und $\rho = \sqrt{\frac{3}{4}}$ gilt

1. $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *ist eine kritische, 2-reduzierte Basis,*
2. $\dfrac{\|\mathbf{b}_1\|}{\lambda_1(\mathcal{L})} = \dfrac{1}{\rho^{n-2}} = \rho^{-n+2}$,
3. $\lambda_1(\mathcal{L}) = \rho^{2(n+2)} \left(\frac{1}{4} + \rho^2\right) = \rho^{2(n+2)}$.

Beweis. Siehe [S94, Theorem 9]. ■

Für $k = 3$ definieren wir die Basismatrix $\mathbf{B}_n := [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in M_{n,n}(\mathbb{R})$ wie folgt (zur Konstruktion siehe [S94]):

$$\mathbf{B}_4 := \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{\sqrt{3}}{2} & \frac{-1}{2\sqrt{3}} & \frac{1}{2\sqrt{3}} \\ 0 & 0 & \sqrt{\frac{2}{3}} & \frac{1}{2}\sqrt{\frac{2}{3}} \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} \tag{6.16}$$

Die Matrizen $\mathbf{B}_2, \mathbf{B}_3$ seien die 2×2- bzw. 3×3-Matrizen in der linken, oberen Ecke von $\mathbf{B}_4$. Für $n \geq 4$ definieren wir die Basismatrix $\mathbf{B}_n$ rekursiv:

$$\mathbf{B}_n := \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & \cdots & 0 \\ 0 & \frac{\sqrt{3}}{2} & \frac{-1}{2\sqrt{3}} & \frac{1}{2\sqrt{3}} & 0 & \cdots & 0 \\ 0 & 0 & & & & & \\ \vdots & \vdots & & \sqrt{\frac{2}{3}} \cdot \mathbf{B}_{n-2} & & & \\ 0 & 0 & & & & & \end{bmatrix} \tag{6.17}$$

Satz 6.6.3
Die Basismatrix $\mathbf{B}_{2k+1} = [\mathbf{b}_1, \ldots, \mathbf{b}_{2k+1}]$ *aus* (6.17) *bzw.* (6.16) *ist für* $k = 1, 2, \ldots$ *eine kritische,* 3*-reduzierte Basis.*

Beweis. Siehe [S94, Theorem 14]. ■

Kapitel 7

$\mathcal{NP}$-vollständige Gitterprobleme

7.1 $\mathcal{NP}$-Vollständigkeit von Rucksack.

Sei Σ endl. Alphabet, o.B.d.A. $\Sigma = \{0,1\}$. Es bezeichne $\mathcal{P}$ die Klasse der polynomial-Zeit entscheidbaren Sprachen $L \subset \Sigma^*$, d.h.

$L \in \mathcal{P}$ gdw $\exists$ Turing Maschine M, welche $x \mapsto \chi_L(x)$ in $|x|^{O(1)}$ Turingschritten berechnet. D.h. $\exists c > 0$, so dass die Schrittzahl der Berechnung $x \mapsto \chi_L(x)$ höchstens $c|x|^c$ ist. Dabei ist $|x|$ die Länge von $x \in \Sigma^*$.

Die Klasse $\mathcal{NP}$ der nichtdeterministischen polynomial-Zeit Sprachen:

$L \in \mathcal{NP}$ gdw $\exists c > 0 \ : \ \exists R \subset \Sigma^* \times \Sigma^*$ polynomial-Zeit entscheidbar so dass

$L = \{x \in \Sigma^* \mid \exists y : |y| \leq |x|^c, \ (x,y) \in R\}$ (y ist *Zeuge* für $x \in L$).

Offenbar gilt $\mathcal{P} \subset \mathcal{NP}$.

Karp-Reduktion. Sei $A, B \subset \Sigma^*$. A ist *Karp-reduzierbar* auf B, Bez.: $A \leq_{\text{pol}} B$, wenn $\exists$ polynomial Zeit berechenbares $f : \Sigma^* \to \Sigma^*$, so dass $x \in A \iff f(x) \in B$ für alle $x \in \Sigma^*$.

Fakt $A \leq_{\text{pol}} B, \quad B \in \mathcal{P} \ \Rightarrow \ A \in \mathcal{P}$
$A \leq_{\text{pol}} B \leq_{\text{pol}} C \ \Rightarrow \ A \leq_{\text{pol}} C.$

Definition 7.1.1
$L \in \mathcal{NP}$ ist $\mathcal{NP}$-vollständig, wenn $A \leq_{\text{pol}} L$ für alle $A \in \mathcal{NP}$.

Fakt Sei $A \leq_{\text{pol}} B$ und A $\mathcal{L}$-vollständig, dann ist B $\mathcal{NP}$-vollständig.

Satz 7.1.2 (Cook, Levin 1973)
Für jedes $\mathcal{NP}$-vollständige L gilt $L \in \mathcal{P}$ gdw $\mathcal{P} = \mathcal{NP}$.

Cook'sche Hypothese. $\mathcal{P} \neq \mathcal{NP}$.

Begründung: Schwierige $\mathcal{NP}$-Probleme sind seit Jahrhunderten bekannt, z.B. Entscheide zu gegebenen $n, s \in \mathbb{N}$: $\exists$ Primzahl $p \leq s$ mit p teilt n.

Satz 7.1.3 (Cook, Karp 1973)

$$\textit{Rucksack} := \left\{ (a_1, \ldots, a_n, b) \in \mathbb{N}^{n+1} \;\middle|\; \begin{array}{l} \exists x_1, \ldots, x_n \in \{0,1\} : \\ \Sigma_{i=1}^n a_i x_i = b, \ n \in \mathbb{N} \end{array} \right\} \textit{ ist } \mathcal{NP}\textit{-vollständig.}$$

Cook zeigte : SAT ist $\mathcal{NP}$-vollständig, Karp zeigte: SAT $\leq_{\text{pol}}$ Rucksack.

7.2 $\mathcal{NP}$-Vollständigkeit von $\text{SVP}_{\ell_\infty}, \text{CVP}_{\ell_\infty}, \text{CVP}_{\ell_2}$.

Siehe Micciancio, Goldwasser, Complexity of Lattice Problems, KAP 2002 [MG02], Kapitel 3, 4.

Wir formulieren $\text{SVP}_{\|\,\|}, \text{CVP}_{\|\,\|}$ als Sprachen

$$\text{CVP}_{\|\,\|} = \{(B, \mathbf{y}, t) \in \mathbb{Z}^{m\times n+m+1} \,|\, \exists \mathbf{x} \in \mathbb{Z}^n : \ \|B\mathbf{x} - \mathbf{y}\| \leq t\}$$

$$\text{SVP}_{\|\,\|} = \{(B, t) \in \mathbb{Z}^{m\times n+1} \,|\, \exists \mathbf{x} \in \mathbb{Z}^n \backslash \{\mathbf{0}\} : \ \|B\mathbf{x}\| \leq t\}.$$

Satz 7.2.1
$\text{SVP}_{\ell_\infty}, \text{CVP}_{\ell_\infty}$ *sind $\mathcal{NP}$-vollständig.*

Beweis. **I.** Rucksack $\leq_{\text{pol}} \text{SVP}_{\|\,\|_\infty}$. Reduziere gemäß $f : (a_1, \ldots, a_n, b) \mapsto (B, 1)$ mit

$$B = [\mathbf{b}_1, \ldots, \mathbf{b}_{n+1}] = \begin{bmatrix} 2 & & & 1 \\ & \ddots & O & \vdots \\ & O & 2 & 1 \\ 2a_1 & \cdots & 2a_n & 2b \\ 0 & \cdots & 0 & 1 \end{bmatrix} \in \mathbb{Z}^{(n+2)(n+1)}.$$

Beh.: $(a_1, \ldots, a_n, b) \in$ Rucksack $\Leftrightarrow \lambda_{1,\infty}(\mathcal{L}(B)) = 1$.

Bew.: " $\Rightarrow$" (trivial) Sei $(x_1, \ldots, x_n) \in \{0,1\}^n$ Rucksacklösung, $\Sigma_{i=1}^n a_i x_i = b$. Dann gilt für $\mathbf{x} := (x_1, \ldots, x_n, -1)^t$, dass

$$B\mathbf{x} = \Sigma_{i=1}^n \mathbf{b}_i x_i - \mathbf{b}_{n+1}, \ \|B\mathbf{x}\|_\infty = 1 \ ,$$

denn $|2x_i - 1| = 1$ für $x_i \in \{0,1\}$ und $2(\Sigma_{i=1}^n a_i x_i - b) = 0$.
" $\Leftarrow$" Ang. $\|\Sigma_{i=1}^{n+1} x_i \mathbf{b}_i\|_\infty = 1$. Wir zeigen **1.** $x_1, \ldots, x_n \in \{0,1\}$, **2.** $\Sigma_{i=1}^n a_i x_i = b$.
1. Offenbar gilt $|2x_i - 1| \leq 1$ für $i = 1, \ldots, n$. Aus $2x_i - 1 = 0$ folgt der Widerspruch $x_i = \frac{1}{2}$. Somit gilt $2x_i - 1 = \pm 1$ und $x_i \in \{1, 0\}$ für $i = 1, \ldots, n$. Offenbar sichert die letzte Zeile von B, dass $|x_{n+1}| = 1$.
2. O.B.d.A. sei $x_{n+1} = -1$. Wegen $|x_{n+1}| \leq 1$, $x_{n+1} \neq 0$ liefert die Multiplikation von $\mathbf{x}$ mit $-\text{sign}(x_{n+1})$ dass $x_{n+1} = -1$. Aus $2 \,|\, \sum_{i=1}^n a_i x_i - b| \leq 1$ folgt $\sum_{i=1}^n a_i x_i = b$.

II. Rucksack $\leq_{\text{pol}} \text{CVP}_{\ell_\infty}$: Reduziere gemäß $f : (a_1, \ldots, a_n, b) \mapsto (B', \mathbf{y}, 1)$ mit

$$[B', \mathbf{y}] \ = \ \begin{bmatrix} 2 & & & 1 \\ & \ddots & O & \vdots \\ & O & 2 & 1 \\ 2a_1 & \cdots & 2a_n & 2b \end{bmatrix} \in \mathbb{Z}^{(n+1)^2} \ .$$

Wir zeigen: $(a_1, ..., a_n, b) \in$ Rucksack $\Leftrightarrow (B', \mathbf{y}, 1) \in$ CVP.
"$\Rightarrow$" trivial. "$\Leftarrow$" Aus $\|B'\mathbf{x} - \mathbf{y}\|_\infty = 1$ folgt $(a_1, \ldots, a_n, b) \in$ Rucksack nach Teil I des Beweises. ■

Satz 7.2.1 wurde von VAN EMDE BOAS [EmBoas 81] bewiesen. Er ist wichtig für den Fall, dass man Quantencomputer bauen kann. Für Quantencomputer sind Faktorisieren ganzer Zahlen, Brechen von RSA, Diskreter Logarithmus in pol.-Zeit. Aber $\mathcal{P} \neq \mathcal{NP}$, d.h. $\mathcal{P}^{\text{Qu}} \neq \mathcal{NP}^{\text{Qu}}$ gilt wohl weiter.

Satz 7.2.2
CVP_{ℓ_2} *ist $\mathcal{NP}$-vollständig,($\ell_2 = \|\ \|$).*

Beweis. Wir zeigen Rucksack $\leq_{\text{pol}}$ CVP_{ℓ_2} und reduzieren gemäß $f : (a_1, \ldots, a_n, b) \mapsto (B', \mathbf{y}, \sqrt{n})$ mit

$$[B', \mathbf{y}] \;=\; \begin{bmatrix} 2 & & & 1 \\ & \ddots & O & \vdots \\ & O & 2 & 1 \\ 2a_1 & \cdots & 2a_n & 2b \end{bmatrix} \in \mathbb{Z}^{(n+1)^2}.$$

Zu zeigen: $(a_1, \ldots, a_n, b) \in$ Rucksack $\Leftrightarrow (B', \mathbf{y}, \sqrt{n}) \in \text{CVP}_{\ell_2}$.
"$\Rightarrow$" Sei $(a_1, \ldots, a_n, b) \in$ Rucksack und $\Sigma_{i=1}^n a_i x_i = b$, $x_i \in \{0, 1\}$ Rucksacklösung. Es folgt

$$\| \textstyle\sum_{i=1}^n \mathbf{b}_i x_i - \mathbf{b}_{n+1} \| = \|(\pm 1, \ldots, \pm 1, 0)\| = \sqrt{n}.$$

"$\Leftarrow$" Ang. $\|\Sigma_{i=1}^n \mathbf{b}_i x_i - \mathbf{y}\|_2 \leq \sqrt{n}$ für $x_1, \ldots, x_n \in \mathbb{Z}$. Es folgt $\|\Sigma_{i=1}^n \mathbf{b}_i x_i - \mathbf{y}\| = \sqrt{n}$ und $x_i \in \{0, 1\}$, somit $\Sigma_{i=1}^n a_i x_i = b$. ■

Vergleich CVP, SVP für die ℓ_2-Norm. SVP ist nicht schwieriger als CVP, es gilt SVP $\leq_{\text{pol,multi}}$ CVP, d.h. SVP $\leq_{\text{Cook}}$ CVP, siehe [MG02, Sektion 4]. Wir vereinfachen SVP und CVP zu GAP-SVP_γ und GAP-SVP_γ mit $\gamma \geq 1$.

GAP-SVP_γ-Problem. Gesucht ist ein deterministischer Algorithmus, der alle Ja-Instanzen akzeptiert und alle Nein-Instanzen ablehnt und beliebig reagiert, falls die Eingabe weder Ja- noch Nein-Instanz ist.

Ja-Instanzen sind Paare $(B, t) \in \mathbb{Z}^{m \times n+1}$, so dass $\exists \mathbf{x} \in \mathbb{Z}^n \backslash \{\mathbf{0}\} : \|B\mathbf{x}\| \leq t$.

Nein-Instanzen sind Paare $(B, t) \in \mathbb{Z}^{m \times n+1}$, so dass $\forall \mathbf{x} \in \mathbb{Z}^n \backslash \{\mathbf{0}\} : \|B\mathbf{x}\| \geq \gamma t$.

GAP-CVP_γ-Problem. Gesucht ist ein deterministischer Algorithmus, der alle Ja-Instanzen akzeptiert und alle Nein-Instanzen ablehnt und beliebig reagiert, falls die Eingabe weder Ja- noch Nein-Instanz ist.

Ja-Instanzen sind Tripel $(B, \mathbf{y}, t) \in \mathbb{Z}^{m \times n+m+1}$ mit $\exists \mathbf{x} \in \mathbb{Z}^n : \|B\mathbf{x} - \mathbf{y}\| \leq t$.

Nein-Instanzen sind Tripel $(B, \mathbf{y}, t) \in \mathbb{Z}^{m \times n+m+1}$ mit $\forall \mathbf{x} \in \mathbb{Z}^n : \|B\mathbf{x} - \mathbf{y}\| \geq \gamma t$.

Satz 7.2.3
GAP-$\text{CVP}_{\sqrt{1+8/n}}$ *ist $\mathcal{NP}$-hart.*

Beweis. Wir zeigen Rucksack $\leq_{\text{pol}}$ GAP-$\text{CVP}_{\sqrt{1+8/n}}$, es folgt $\mathcal{NP} \leq_{\text{pol}}$ GAP-$\text{CVP}_{\sqrt{1+8/n}}$. Wir reduzieren gemäß $f : (a_1, \ldots, a_n, b) \mapsto (B', \mathbf{y}, \sqrt{n})$ mit

$$[B'|\mathbf{y}] \;:=\; \begin{bmatrix} 2 & & & 1 \\ & \ddots & O & \vdots \\ & O & 2 & 1 \\ 3\,a_1 & \cdots & 3\,a_n & 3\,b \end{bmatrix} \in \mathbb{Z}^{(n+1)^2}.$$

Korrektheit der Reduktion.

$(a_1, \ldots, a_n, b) \in$ Rucksack $\Rightarrow$ $(B', \mathbf{y}, \sqrt{n})$ Ja-Instanz, d.h. $\exists \mathbf{x} \in \{0, 1\}^n : \|B'\mathbf{x} - \mathbf{y}\| \leq \sqrt{n}$.
$(a_1, \ldots, a_n, b) \notin$ Rucksack $\Rightarrow$ $(B', \mathbf{y}, \sqrt{n})$ Nein-Instanz. (wird wie folgt gezeigt)

Im Fall $(a_1, \ldots, a_n, b) \notin$ Rucksack gilt für $\mathbf{x} \in \mathbb{Z}^n$ entweder $\exists i : x_i \notin \{0, 1\}$, somit $|2x_i - 1| \geq 3$, $|2x_i - 1|^2 \geq 9 = 1 + 8$, oder $\sum_{i=1}^n a_i x_i \neq b$, somit $9(\Sigma_{i=1}^n a_i x_i - b)^2 \geq 9$. Wegen $|2x_i - 1| \geq 1$ für $x_i \in \mathbb{Z}$ folgt $\forall \mathbf{x} \in \mathbb{Z}^n : \|B'\mathbf{x} - \mathbf{y}\| \geq \sqrt{n+8}$. Somit ist $(B', \mathbf{y}, \sqrt{n})$ Nein-Instanz. ■

Satz 7.2.4 (DKRS03)
GAP-CVP_γ *und* CVP_γ *sind $\mathcal{NP}$-hart für* $\gamma = n^{1/\log\log n}$.

Satz 7.2.5 (Ajtai 1998, Micciancio 2001, MG02, Sektion 4)
GAP-SVP$_\gamma$ *ist für* $\gamma < \sqrt{2}$ $\mathcal{NP}$*-hart bzgl. probabilistischen Karp-Reduktionen.*

Satz 7.2.6 (Khot 2005)
GAP-SVP$_\gamma$ *ist für beliebige, konstante* $\gamma > 1$ $\mathcal{NP}$*-hart bzgl. probabilistischen Karp-Reduktionen.*

Die probabilistischen Karp-Reduktionen von Khot erzeugen recht große Zahlen polynomialer Länge.

Probabilistische Karp-Reduktionen werden erklärt wie $\leq_{\text{pol}}$, aber die pol. Zeit Transformation $f = f(x, w)$ benutzt einen Münzwurf w. Der Satz von Ajtai-Micciancio zeigt

$$\text{Rucksack}, \ \mathcal{NP} \leq_{\text{pol,prob.}} \text{SVP}_{\ell_2}.$$

Die Reduktion Rucksack $\leq_{\text{pol}}$ SVP konnte bisher nur für probabilistische Karp-Reduktionen gezeigt werden. Man reduziert Rucksack auf das CVP-Problem eines Gitters $\mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_{n+1})$ und benötigt für die Korrektheit, dass $\lambda_1(\mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_n)) > \sqrt{2n}$. Diese Bedingung kann man nur probabilistisch sichern. Wir geben die Reduktion ohne diese nicht triviale Bedingung zu sichern. Wir reduzieren Rucksack auf SVP durch die Reduktion

$$f : (a_1, \ldots, a_n, b) \mapsto (B, \sqrt{n}) \text{ mit}$$

$$B = [\mathbf{b}_1, \ldots, \mathbf{b}_{n+1}] \ = \ \begin{bmatrix} 2 & & & 1 \\ & \ddots & O & \vdots \\ & O & 2 & 1 \\ \sqrt{n}\, a_1 & \cdots & \sqrt{n}\, a_n & \sqrt{n}\, b \\ 0 & \cdots & 0 & \sqrt{n} \end{bmatrix} \in \mathbb{R}^{(n+2)\times(n+1)}.$$

Satz 7.2.7
Rucksack $\leq_{\text{pol}}$ SVP *falls für* $(a_1, ..., a_n, b) \in$ *Rucksack und* $f(a_1, ..., a_n, b) := ([\mathbf{b}_1, ..., \mathbf{b}_{n+1}]$ *gilt dass* $\lambda_1(\mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_n)) > \sqrt{2n}$.

Beweis. $(a_1, \ldots, a_n, b) \in$ Rucksack impliziert $(B, \sqrt{2n}) \in$ SVP, denn für jede Rucksack-Lösung $\Sigma_{i=1}^n a_i x_i = b$, $x_i \in \{0, 1\}$ gilt $|2x_i - 1| = 1$ und

$$\|\Sigma_{i=1}^n \mathbf{b}_i x_i - \mathbf{b}_{n+1}\| = \|(\pm 1, \ldots, \pm 1, 0, \sqrt{n})\| = \sqrt{2n}.$$

Umgekehrt sichert $\lambda_1(\mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_n)) > \sqrt{2n}$ dass $(B, \sqrt{2n}) \in$ SVP $\Rightarrow (a_1, \ldots, a_n, b) \in$ Rucksack: Angenommen $\|\Sigma_{i=1}^n \mathbf{b}_i x_i + \mathbf{b}_{n+1} x_{n+1}\| \leq \sqrt{2}n$. Wegen $\lambda_1(\mathcal{L}(\mathbf{b}_1, ..., \mathbf{b}_n)) > \sqrt{2n}$ gilt $\sum_{i=1}^n a_i x_i + x_{n+1} b = 0$ mit $x_{n+1} \neq 0$, dabei gilt $|x_{n+1}| \leq 1$, denn andernfalls wäre $\|\Sigma_{i=1}^n \mathbf{b}_i x_i + \mathbf{b}_{n+1} x_{n+1}\| \geq 2\sqrt{n} > \sqrt{2n}$.

Sei O.B.d.A. $x_{n+1} = -1$. Es folgt $|2x_i - 1| = 1$ für $i = 1, \ldots, n$, somit $x_i \in \{0, 1\}$. Also $(a_1, \ldots, a_n, b) \in$ Rucksack. ■

Kapitel 8

Konstruktion eines kürzesten Gittervektors

Die Algorithmen zur Blockreduktion benötigen einen kürzesten Gittervektor ungleich $\mathbf{0}$. Alg. 8.1.1 ENUM [SE94, SH95] findet einen kürzesten Gittervektor durch vollständige Aufzählung kurzer Gittervektoren. Die Laufzeit von ENUM ist im worst case exponentiell $n^{n/2+o(n)}$. NEW ENUM's Laufzeit ist unter GSA und der Volumen Heuristik polynomiell für Gitter $\mathcal{L}$ kleiner Dichte, so dass $\|\mathbf{b}_1\|\ e\pi\sqrt{n} \leq \gamma_n^{1/2}(\det \mathcal{L})^{1/n}$ zu gegebenem $\mathbf{b}_1$ [S10]. NEW ENUM führt die Stufen $(u_t, ..., u_n)$ geordnet nach aufsteigendem t und zu festem t mit absteigender Erfolgsquote β_t durch.

8.1 Algorithmus mit vollständiger Aufzählung

Gegeben sei eine Basis $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] = \mathbf{QR} \in \mathbb{Z}^{m \times n}$. Wir berechnen ein $\mathbf{b} \in \mathcal{L}(\mathbf{B})$ mit $\|\mathbf{b}\| = \ell_2(\mathbf{b}) = \lambda_1(\mathcal{L})$. Sei $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ die Basis mit zugehörigem Orthogonalsystem $\widehat{\mathbf{b}}_1, \ldots, \widehat{\mathbf{b}}_n$ und Gram-Schmidt-Koeffizienten $\mu_{i,j}$, also $\mathbf{b}_i = \sum_{j=1}^{i} \mu_{i,j}\widehat{\mathbf{b}}_j = \sum_{j=1}^{i} r_{i,j}/r_{i,i}\widehat{\mathbf{b}}_j$ für $i = 1, \ldots, n$.

Zur orthogonalen Projektion $\pi_i : \mathbb{R}^m \to \operatorname{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^{\perp}$ bezeichne:

$$c_t(u_t, \ldots, u_n) := \|\pi_t(\textstyle\sum_{i=t}^{n} u_i \mathbf{b}_i)\|^2 = \sum_{i=t}^{n}(\sum_{j=t}^{i} u_i r_{j,i})^2.$$

Die Funktion $u' := \operatorname{next}(u, r)$ liefert zu $u \in \mathbb{Z}$ und $r \in \mathbb{R}$ die in der Reihenfolge nach u betragsmäßig nächste, ganze Zahl zur reellen Zahl r (siehe Grafik 8.1.1). Es gilt:

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

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 $|u - r| = |u' - r|$ folgt $u < r < u'$.

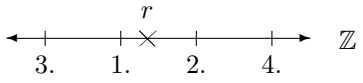

Abbildung 8.1.1: Reihenfolge der Approximationen bei der Iteration $u' := \operatorname{next}(u\,, r)$

Algorithmus 8.1.1, Enum [SE94], Finden eines kürzesten Gittervektors

EINGABE: $\mathbf{B} = \mathbf{QR} \in \mathbb{Z}^{m\times n}$, $R = [r_{i,j}]_{1\le i,j\le n} \in \mathbb{R}^{n\times n}$.

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

2. $t := 1,\ \tilde{u}_1 := u_1 := 1,\ c_1^{\min} := \tilde{c}_1 := r_{1,1}^2$. $\qquad$ /⋆ stets ist $\tilde{c}_t = c_t(\tilde{u}_t,\ldots,\tilde{u}_n)$ und $c_1^{\min} = c_1(u_1,...,u_t)$ ist aktuelles Minimum von c_1 ⋆/

3. WHILE $t \le n$ DO

3.1 $\tilde{c}_t := \tilde{c}_{t+1} + (y_t + \tilde{u}_t)^2 r_{t,t}^2$

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

IF $t > 1$ THEN $\ t := t-1,\ y_t := \sum_{i=t+1}^{n} \tilde{u}_i\, r_{t,i}/r_{t,t},\ \tilde{u}_t := \lfloor -y_t \rceil$

ELSE $\ c_1^{\min} = \tilde{c}_1,\ $ FOR $i = 1,\ldots,n\ $ DO $\ u_i := \tilde{u}_i$

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

/⋆ $t_{\max}$ bezeichne das bisher maximale t vor der Erhöhung ⋆/

AUSGABE: Minimalstelle $(u_1,\ldots,u_n) \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ von $c_1$und Minimalwert $c_1^{\min} = \lambda_1^2$ für Funktion c_1

Die Korrektheit von Alg. 8.1.1 folgt aus den folgenden Beobachtungen:

- Stets gilt: $\tilde{c}_t = c_t(\tilde{u}_t,,\ldots,\tilde{u}_n)$. Beweis durch Induktion über Anzahl der Iterationen. Durch die Zuweisungen im ersten Schritt gelten die Behauptungen vor der ersten Iteration (Induktionsverankerung). Induktionsschluß: Es gilt für $\ y_1 := \sum_{i=t+1}^{n} \tilde{u}_i\, r_{t,i}/r_{t,t}$ dass

$$c_t(\tilde{u}_t,\ldots,\tilde{u}_n) = \underbrace{c_{t+1}(\tilde{u}_{t+1},\ldots,\tilde{u}_n)}_{\text{nach Ind.Ann. } = \tilde{c}_{t+1}} + \big(\textstyle\sum_{i=t}^{n} \tilde{u}_i r_{t,i}\big)^2 = \tilde{c}_{t+1} + (y_t + \tilde{u}_t)^2\, r_{t,t}^2.$$

- Der Algorithmus zählt in Depth-First-Order alle Vektoren $(\tilde{u}_t,\ldots,\tilde{u}_n) \in \mathbb{Z}^{n-t+1} \setminus \{\mathbf{0}\}$ für $t = 1,\ldots,n$ auf mit $c_t(\tilde{u}_t,\ldots,\tilde{u}_n) < c_1^{\min}$ ($c_1^{\min}$ ist das aktuelle Minimum der Funktion c_1). Es werden nur Vektoren aufgezählt so dass $\tilde{u}_i > 0$ für das größte i mit $\tilde{u}_i \neq \mathbf{0}$.
- Für feste $\tilde{u}_{t+1},\ldots,\tilde{u}_n$ liefert die Folge der $\tilde{u}_t$-Werte, erzeugt durch $\text{next}(\tilde{u}_t, -y_t)$ monoton wachsende Werte $|y_t + \tilde{u}_t|$, $c_t(\tilde{u}_t,\ldots,\tilde{u}_n)$. Wenn $\tilde{c}_t \ge c_1^{\min}$ für den aktuellen Vektor $(\tilde{u}_t,\ldots,\tilde{u}_n)$, dann kann die Aufzählung der weiteren $\tilde{u}_t$ -Werte entfallen.

8.2 Algorithmus mit geschnittener Aufzählung

Wir schneiden die Aufzählung an der Stelle $(\tilde{u}_t,...,\tilde{u}_n)$ ab, wenn nach der Vol. Heur. ein kürzerer Vektor $\sum_{i=1}^{n} \tilde{u}_i \mathbf{b}_i$ nur mit Wahrscheinlichkeit $< 2^{-s}$ zu gegebenem s zu erwarten ist, siehe [SH95].

8.2.1 Volumen-Heuristik und Gauß-ENUM

Folgendes Lemma geht auf C.F. Gauß zurück. Für nicht zufällige $\mathbf{z}$ ist es die Volumen-Heuristik.

Lemma 8.2.1 (Volumen-Heuristik)
Sei $S \subseteq \text{span}(\mathcal{L})$ Jordan-meßbar, $\mathbf{z} \in_R \text{span}(\mathcal{L}) \mod \mathcal{L}$ zufällig, dann gilt:

$$\mathrm{E}_{\mathbf{z}}[\,|(\mathbf{z}+S)\cap\mathcal{L}|] = \text{vol}(S) \,/\, \det\mathcal{L}.$$

Beweis. Denn $\dfrac{1}{\det \mathcal{L}} = \dfrac{\text{Anzahl Gitterpunkte}}{\text{Volumen Grundmasche}} = \dfrac{\text{Anzahl Gitterpunkte}}{\text{Volumeneinheit}}$. ■

Angenommen, wir halten $(\tilde{u}_t, \ldots, \tilde{u}_n) \in \mathbb{Z}^{n-t+1} \setminus \{\mathbf{0}\}$ 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 $\mathcal{L}_t := \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{t-1})$
Wir addieren zum gegebenem Gittervektor $\mathbf{b} = \sum_{i=t}^{n} \tilde{u}_i \mathbf{b}_i$ einen Vektor $\overline{\mathbf{b}} = \sum_{i=1}^{t-1} \tilde{u}_i \mathbf{b}_i \in \mathcal{L}_t$ so daß $\left\|\mathbf{b} + \overline{\mathbf{b}}\right\|^2 < c_1^{\min}$. Wir zerlegen $\mathbf{b}$ in orthogonale Anteile (es sei $Q = [\mathbf{q}_1, ..., \mathbf{q}_n]$ mit $B = QR$):

$$\mathbf{b} = \underbrace{\sum_{j=1}^{t-1} \sum_{i=1}^{n} \tilde{u}_i r_{j,i}\, \mathbf{q}_j}_{-\mathbf{z} \in \operatorname{span}(\mathcal{L}_t)} + \underbrace{\sum_{j=t}^{n} \sum_{i=t}^{n} \tilde{u}_i r_{j,i}\, \mathbf{q}_j}_{\mathbf{y} \in \operatorname{span}(\mathcal{L}_t)^{\perp}} = -\mathbf{z} + \mathbf{y} \tag{8.1}$$

Wir suchen einen Punkt in $(\mathbf{b} + \mathcal{L}_t) \cap \mathcal{B}_{t-1}(\mathbf{y}, \rho_t)$ in der Kugel $\mathcal{B}_{t-1}(\mathbf{y}, \rho_t)$ der Dimension $t-1$ mit Mittelpunkt $\mathbf{y}$ und Radius $\rho_t = \sqrt{c_1^{\min} - \tilde{c}_t}$. Es gilt für $\mathbf{b} = -\mathbf{z} + \mathbf{y}$:

$$\big|\big(\mathbf{b} + \mathcal{L}_t\big) \cap \mathcal{B}_{t-1}\big(\mathbf{y}, \rho_t\big)\big| = \big|\mathcal{L}_t \cap \mathcal{B}_{t-1}(\mathbf{z}, \rho_t)\big|.$$

Die Grafik 8.2.1 verdeutlicht diese Aufgabe, hier ist $S(\sqrt{c_1^{\min} - \tilde{c}_t}, y) = \mathcal{B}_{t-1}\big(\mathbf{y}, \rho_t\big)$, $\overline{L} = \mathcal{L}_t$.

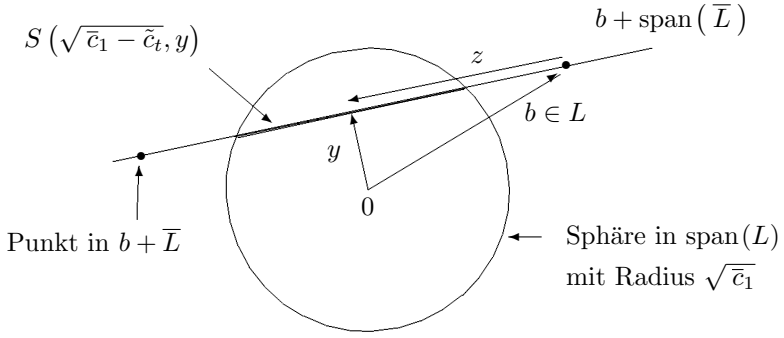

Abbildung 8.2.1: Volumenheuristik bei Gauß-ENUM

Wir wenden die Volumen-Heuristik an auf das Gitter $\mathcal{L}_t$ und die Kugel $\mathcal{B}_{t-1}(\mathbf{0}, \rho_t)$ und erhalten für zufällige $\mathbf{z} \in \operatorname{span}(\mathcal{L}_t)$ die Erfolgsquote β_t:

$$\beta_t = \mathrm{E}_{\mathbf{z}}\left[\,\left|\left\{(\tilde{u}_1, \ldots, \tilde{u}_{t-1}) \in \mathbb{Z}^{t-1} \;:\; c_1(\tilde{u}_1, \ldots, \tilde{u}_{t-1}) < c_1^{\min}\right\}\right|\right] = V_{t-1}\, \rho_t^{t-1} / \det \mathcal{L}_t$$

Wir schneiden die weitere Aufzählung an der Stelle $(\tilde{u}_1, \ldots, \tilde{u}_{t-1})$ ab, falls $\beta_t < 2^{-s}$. Je größer s, desto umfangreicher die Aufzählung. Für $s = \infty$ erhalten wir die vollständige Aufzählung.

Ersetzen von Schritt **3.2** in Alg. 8.1.1 durch

IF $\beta_t > 2^{-s}$ THEN

liefert Alg. 8.2.1 genannt Gauß-ENUM [SH95].

Algorithmus 8.2.1, Kürzester Gittervektor durch geschnittene Aufzählung

EINGABE: Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{Z}^{m\times n}$, $\mathbf{R} = [r_{i,j}]_{1\le i,j\le n} \in \mathbb{R}^{n\times n}$

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

2. $\tilde{u}_1 := u_1 := 1,\ t := 1,\ c_1^{\min} := \tilde{c}_1 := \|\mathbf{b}_1\|^2$ /⋆ stets ist $\tilde{c}_t = c_t(\tilde{u}_t,\ldots,\tilde{u}_n)$ und $c_1^{\min} = c_1(u_1,...,u_t)$ ist aktuelles Minimum von c_1 ⋆/

3. WHILE $t \le n$ DO

3.1 $\tilde{c}_t := \tilde{c}_{t+1} + (y_t + \tilde{u}_t)^2 r_{t,t}^2$

3.2 IF $\beta_t \ge 2^{-s}$ THEN

IF $t > 1$ THEN $t := t-1,\ y_t := \sum_{i=t+1}^{n} \tilde{u}_i\, r_{t,i}/r_{t,t},\ \tilde{u}_t := \lfloor -y_t \rceil$

ELSE $c_1^{\min} = \tilde{c}_1$ FOR $i = 1,\ldots,n$ DO $u_i := \tilde{u}_i$

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

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

AUSGABE: Wahrscheinliche Minimalstelle $(u_1,\ldots,u_n)$ und Minimalwert $c_1^{\min}$ von c_1

Die Volumen Heuristik nimmt an, dass die orthogonale Projektion von $\mathbf{b} = \sum_{i=t}^{n} \tilde{u}_i \mathbf{b}_i$ in $\mathcal{L}_t = \mathcal{L}(\mathbf{b}_1,...,\mathbf{b}_{t-1})$ modulo —$\mathcal{L}_t$ zufällig ist. Wenn aber $(\tilde{u}_t,...,\tilde{u}_n)$ mit den Koordinaten eines kürzesten Gittervektors übereinstimmt, dann ist diese orthogonale Projektion von $\mathbf{b}$ nach Längenreduktion gegen $\mathbf{b}_1,...,\mathbf{b}_{t-1}$ oft sehr klein und die Volumen Heuristik damit eher inkorrekt.

Aufzählung mit Zurücklegen, New Enum. In der Neufassung New Enum von [S10] wird $(\tilde{u}_t,...,\tilde{u}_n)$ im Falle $\beta_t < 2^{-s}$ nicht verworfen, sondern in eine Liste zur späteren Bearbeitung zurückgelegt. Nach Ende der Bearbeitung mit dem Wert s wird s erhöht auf $s := s+1$ und der Aufzählungsprozess wird ausgehend von allen zurückgelegten $(\tilde{u}_t,...,\tilde{u}_n)$ mit dem erhöhten s neu initiiert und zwar in der Reihenfolge mit aufsteigendem t und bei festem t mit absteigendem β_t.

Das Zurücklegen der $(\tilde{u}_t,...,\tilde{u}_n)$ mit $\beta_t < 2^{-s}$ erfordert einen Speicherplatz der im allgemeinen exponentiell in n ist. Diesen grossen Speicherbedarf kann man dadurch reduzieren, dass man das Abspeichern der $(\tilde{u}_t,...,\tilde{u}_n)$ unterlässt und nach Erhöhung von s den Algorithmus neu initiiert. Dabei werden die schon behandelten Werte $(\tilde{u}_t,...,\tilde{u}_n)$ nochmals behandelt. Diese Wiederholung erhöht die Laufzeit höchstens um den Faktor s des letzten s-Wertes. Dieser grösste s-Wert ist aber höchstens $O(n \ln n)$ so dass die Laufzeit nur um einen polynomiellen Faktor wächst.

Ein einfache Abschneid-Methode (pruning) ersetzt die Bedingung IF $\beta_t \ge 2^{-s}$ THEN von Schritt 3.2 durch

IF $c_t \le \frac{n-t+1}{n} c_1^{\min}$ THEN

Diese Bedingung wurde in [SE94] initiiert und in [NR10] analysiert. Nguyen und Regev zeigen in [NR10], dass Modifizierung von Schritt 3.2 in

IF $c_t \le \frac{n-t+1}{n} \lambda_1^2$ THEN

ein kürzester Gittervektor von zufälligen Gittern mit Wahrscheinlichkeit $1/n$ gefunden wird. Für dieses Abschneiden muss man entweder λ_1 kennen oder eine hinreichend gute Approximation von λ_1 erraten.

In [SE94] wird Schritt 3.2 angewandt in der modifizierten Form

IF $c_t \le 1.05\, \frac{n-t+1}{n} c_1^{min}$ THEN

Mit diesem pruning wurden Subsetsum Probleme der Dimension ≤ 66 und fast aller Dichten durch Konstruktion kürzester Vektoren des CJLOSS-Gitters fast immer gelöst [SE94]. Diese hohe Erfolgswahrscheinlichkeit beim Finden eines kürzesten Gittervektors mit diesem pruning ist beweisbar unter GSA und der Volumen-Heuristik, die Methode ist effektiv für Dimension $n \le 250$, nach B. Lange, Februar 2011.

Kapitel 9

Factoring Integers

9.1 Factoring Integers by CVP Algorithms for the Prime Number Lattice [S13]

Let N be a positive integer that is not a prime power, with all prime factors larger than p_n the n-th smallest prime. A classical method factors N via $n + O(1)$ modular equations $\prod_{i=1}^n p_i^{e_i} = \pm \prod_{i=1}^n p_i^{e_i'} \mod N$. We construct such modular equations from **CVP** solutions for the prime number lattice $\mathcal{L}(\mathbf{B}_{n,c})$ with basis $\mathbf{B}_{n,c} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{R}^{(n+1)\times n}$ and target vector $\mathbf{N}_c \in \mathbb{R}^{n+1}$ for some $c > 0$:

$$\mathbf{B}_{n,c} = \begin{bmatrix} \sqrt{\ln p_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sqrt{\ln p_n} \\ N^c \ln p_1 & \cdots & N^c \ln p_n \end{bmatrix}, \qquad \mathbf{N}_c = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ N^c \ln N \end{bmatrix}, \tag{9.1}$$

$$\big(\det \mathcal{L}(\mathbf{B}_{n,c})\big)^2 = \big(\prod_{i=1}^n \ln p_i\big)\ (1 + N^{2c} \sum_{i=1}^n \ln p_i),$$

$$\big(\det \mathcal{L}(\mathbf{B}_{n,c})\big)^{2/n} = \ln p_n \cdot (1 \pm o(1)) \cdot N^{2c/n}$$

as the prime number theorem implies $\prod_{i=1}^n \ln p_i^{1/n} / \ln p_n = 1 - o(1)$ for $n \to \infty$. We use that $o(1) \to 0$ for $n, N \to \infty$.

Outline of the factoring method. We compute vectors $\mathbf{b} = \sum_{i=1}^n e_i \mathbf{b}_i \in \mathcal{L}(\mathbf{B}_{n,c})$ close to $\mathbf{N}_c$ such that $|u - vN| \le p_n^{O(1)}$ factorizes as $|u - vN| = \prod_{i=1}^n p_i^{e_i'}$. This yields a non-trivial relation

$$u = \prod_{e_i > 0} p_i^{e_i} = \pm \prod_{i=1}^n p_i^{e_i'} \mod N. \tag{9.2}$$

We write $n+1$ such relations with $p_0 = -1$ as $\prod_{i=0}^n p_i^{e_{i,j} - e_{i,j}'} = 1 \mod N$ for $j = 1, ..., n+1$. Any solution $t_1, ..., t_{n+1} \in \{0, 1\}$ of the equations

$$\sum_{j=1}^{n+1} t_j (e_{i,j} - e_{i,j}') = 0 \mod 2 \quad \text{for } i = 0, ..., n \tag{9.3}$$

solves $X^2 = 1 \mod N$ by $X = \prod_{i=0}^n p_i^{\frac{1}{2} \sum_{j=1}^{n+1} t_j (e_{i,j} - e_{i,j}')} \mod N$. In case that $X \neq \pm 1 \mod N$ this yields two non-trivial factors $\gcd(X \pm 1, N) \notin \{1, N\}$ of N.

The linear equations (9.3) can be solved within $O(n^3)$ bit operations. We neglect this minor part of the work load of factoring N. This reduces factoring N to finding about n vectors $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ for which $|u - vN|$ factorizes over $p_1, ..., p_n$. This factoring method goes back to Morrison & Brillhart [MB75] and let to the first factoring algorithm in subexponetial time by J. Dixon [D81].

We identify each vector $\mathbf{b} = \sum_{i=1}^n e_i \mathbf{b}_i \in \mathcal{L}(\mathbf{B}_{n,c})$ with the pair (u, v) of relative prime integers

$$u = \prod_{e_i>0} p_i^{e_i},\ \ v = \prod_{e_i<0} p_i^{-e_i} \in \mathbb{N}.$$

Clearly uv is square-free if and only if $e_1, ..., e_n \in \{0, \pm 1\}$. Let $\widehat{z}_{\mathbf{b}} := N^c \ln \frac{u}{v}$, $\widehat{z}_{\mathbf{b}-\mathbf{N}_c} := N^c \ln \frac{u}{vN}$ denote the last coordinates of $\mathbf{b}$ and $\mathbf{b} - \mathbf{N}_c$. As a factor $p_i^{e_i}$ of uv contributes $e_i \ln p_i$ to $\ln uv$ and $e_i^2 \ln p_i$ to $\|\mathbf{b}\|^2$ we have $\|\mathbf{b}\|^2 \geq \ln uv + \widehat{z}_{\mathbf{b}}^2$ with equality if and only if uv is square-free. Similarly

Lemma 9.1.1
$\|\mathbf{b} - \mathbf{N_c}\|^2 \geq \ln uv + \widehat{z}^2_{\mathbf{b}-\mathbf{N}_c}$ holds for all u, v of $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ with equality iff uv is square-free.

In practice $\|\mathcal{L}(\mathbf{B}_{n,c}) - \mathbf{N}_c\|^2$ is close to the minimum of $\ln uv + \widehat{z}^2_{\mathbf{b}-\mathbf{N}_c}$ for square-free uv.

Lemma 9.1.2
Let $(u, v) \sim \mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ satisfy $\frac{1}{2}N^\delta \leq v \leq N^\delta$ and $|u - vN| = o(vN)$. Then
1. $\|\mathbf{b} - \mathbf{N}_c\|^2 \geq (2\delta + 1) \ln N \pm o(1) + \widehat{z}^2_{\mathbf{b}-\mathbf{N}_c}$ **2.** $|u - vN| = N^{\delta+1-c}|\widehat{z}_{\mathbf{b}-\mathbf{N}_c}|(1 \pm o(1))$.

Proof. Clearly $|u-vN| = o(vN)$ and $\frac{1}{2}N^\delta \leq v \leq N^\delta$ implies $|\frac{u-vN}{vN}| = o(1)$ and $\frac{1}{2}N^{1+\delta}(1-o(1)) \leq u \leq N^{1+\delta}(1 + o(1))$. Hence $\ln uv = (2\delta + 1) \ln N \pm o(1)$ proving **1** by Fact 1. The upper bound **1** is sharp if uv is square-free. Moreover $\ln(1 + \frac{u-vN}{vN}) = \frac{u-vN}{vN}(1 \pm o(1)) = \pm o(1)$ and thus $|\widehat{z}_{\mathbf{b}-\mathbf{N}_c}| = N^c \frac{|u-vN|}{vN}(1 \pm o(1)) = N^{c-1-\delta}|u - vN|(1 \pm o(1))$ which proves **2.** □

Lemma 5.3 of [MG02] proves that $\lambda_1^2 > 2c \ln N$ holds if the prime 2 is excluded from the prime basis. Lemma 2 extends this proof to include the prime 2 and increases the lower bound by $1-o(1)$.

Lemma 9.1.3
$\lambda_1^2 > 2c \ln N + 1 - \frac{1}{2}N^{-c} \pm \Theta(N^{-2c})$ holds for the lattice $\mathcal{L}(\mathbf{B}_{n,c})$ for $N^c \geq 10^3$.

Proof. Let $\mathbf{b} = \mathbf{B}_{n,c}\mathbf{u} \neq \mathbf{0}$ be a shortest vector of $\mathcal{L}(\mathbf{B}_{n,c})$, corresponding to (u, v). Let $u > v$, otherwise change $\mathbf{u}$ into $-\mathbf{u}$. Then $\ln \frac{u}{v}$ minimizes for $u \geq v + 1$. Hence

$$\begin{aligned}
&\ln \tfrac{u}{v} \geq \ln(1 + 1/v) > \ln(1 + 1/\sqrt{uv}) && \text{since } u \geq v+1 \text{ and} \sqrt{uv} > v \\
&> \tfrac{1}{\sqrt{uv}} - \tfrac{1}{2}\tfrac{1}{uv} = \tfrac{1}{\sqrt{uv}}(1 - \tfrac{1}{2}\tfrac{1}{\sqrt{uv}}) && \text{since } \ln(1+x) = \textstyle\sum_{i=1}^{\infty}(-1)^{i+1}x^i/i \text{ for } |x| < 1.
\end{aligned}$$

Hence $\lambda_1^2 \geq \ln uv + N^{2c} \ln^2(\frac{u}{v}) > \ln uv + N^{2c}\frac{1}{uv}(1 - \frac{1}{2\sqrt{uv}})^2 =: f(\sqrt{uv})^2$ where $N^c \ln \frac{u}{v} = \widehat{z}_{\mathbf{b}}$ is the last coordinate of $\mathbf{b}$. We abbreviate $h := \sqrt{uv}$. The derivative $\frac{\vartheta f(h)}{\vartheta h} = h^{-5}[2h^4 + N^{2c}[-2h^2 + 3h - 1]\ ]$ is zero for some h with $N^c - 0.751 < h < N^c - 0.75$ and this h determines the minimal value $f(h)$ of f. Then the Lemma follows from

$$\begin{aligned}
&f(N^c - \varepsilon) = \ln(N^c - \varepsilon)^2 + \tfrac{N^{2c}}{(N^c-\varepsilon)^2}(1 - \tfrac{1}{2(N^c-\varepsilon)}) \\
&= 2c \ln N + 2\ln(1 - \varepsilon/N^c) + 1 + \tfrac{2\varepsilon N^c - \varepsilon^2}{(N^c-\varepsilon)^2} - \tfrac{N^{2c}}{2(N^c-\varepsilon)^3} \\
&\geq 2c \ln N + 1 - \tfrac{1}{2}N^{-c} \pm \Theta(N^{-2c}) \text{ for } |\varepsilon - 0.7505| \leq 10^{-3} \text{ by an easy proof.}
\end{aligned}$$

□

An integer is called *y-smooth*, if it has no prime factor larger than y. If p_n-smooth u, v exist such that $u = v+1$, $u = O(N^c)$, uv is square-free then $\lambda_1^2 = 2c \ln N + O(1)$. Otherwise λ_1^2 increases by the minimum of $\widehat{z}_{\mathbf{b}}^2 \geq N^{2c} \ln^2(\frac{u}{v})$ for p_n-smooth $v < u$ of order $u = O(N^c)$. Let $\Psi(X, y)$ denote the number of integers in $[1, X]$ that are y-smooth. Dickman [D30] has shown for any fixed $z > 0$

$$\lim_{y\to\infty} \Psi(y^z, y)y^{-z} = \rho(z). \tag{9.5}$$

$\rho(z)$ is known as Dickman's de Bruijn ρ-function, see [G08] for a recent surview. It is known that

$$\rho(z) = 1 - \ln z \ \text{ for } \ 1 \leq z \leq 2$$

$$\rho(z) = \big(\tfrac{e\pm o(1)}{z\ln z}\big)^z = 1/z^{z+o(z)} \text{ for } z\to\infty \tag{9.6}$$

HILDEBRAND [H84] extended (9.5) to a wide finite range of y and z. For any fixed $\varepsilon > 0$

$$\Psi(y^z, y)y^{-z} = \rho(z)\big(1 + O\big(\tfrac{\ln(z+1)}{\ln y}\big)\big) \tag{9.7}$$

holds uniformly for $1 \le z \le y^{1/2-\varepsilon}$, $y \ge 2$ if and only if the Riemann Hypothesis is true.

Let $\Phi(N, p_n, \sigma)$ denote the number of triples $(u, v, |u - vN|) \in \mathbb{N}^3$ that are p_n–smooth and bounded as $v, |u - vN| \le p_n^\sigma$. We conclude from (9.7) that

$$\Phi(N, p_n, \sigma) = O(2p_n^{2\,\sigma}\,\rho\big(\tfrac{\ln(Np_n^\sigma)}{\ln p_n}\big)\rho^2(\sigma)) \tag{9.8}$$

uniformly holds for $\frac{\ln N}{\ln p_n} + \sigma \le p_n^{1/2-\varepsilon}$ if the p_n-smoothness events of $u, v, |u - vN|$ are nearly statistically independent. We will use (9.8) in a range where $\frac{\ln N}{\ln p_n} + \sigma < p_n^{0.4}$ and we will neglect the $O(1)$-factor of (9.8).

Proof of (9.8). There are $2p_n^{2\sigma}$ pairs of integers u, v such that $0 < v, |u - vN| \le p_n^\sigma$. Clearly $u \le Np_n^\sigma + p_n^\sigma \le p_n^z$ holds for $z = \frac{\ln(N+1)}{\ln p_n} + \sigma$. Then (9.7) for $y^z = p_n^z = (N+1)p_n^\sigma$ shows that the fraction of u that are p_n-smooth is $\rho(z)\big(1 + O\big(\frac{\ln(z+1)}{\ln p_n}\big)\big)$ if $\frac{\ln N}{\ln p_n} + \sigma \le p_n^{0.4}$.

Moreover (9.7) for $y = p_n$, $z = \sigma$ shows that the fraction of $0 < v \le p_n^\sigma$ that are p_n-smooth is $\rho(\sigma)\big(1 + O\big(\frac{\ln(\sigma+1)}{\ln p_n}\big)\big)$ if $\sigma \le p_n^{1/2-\varepsilon}$. Therefore the statistical independence of the p_n-smoothness events of $u, v, |u - vN|$ implies (9.8) if $\ln(z + 1) = O(\ln p_n)$ holds in both cases. The latter holds due to $\frac{\ln N}{\ln p_n} + \sigma \le p_n^{0.4}$.

Example factoring. Let $N = 100000980001501 \approx 10^{14}$ and $n = 90$, $p_{90} = 463$. (9.8) shows that there are $\Theta(6.4 \cdot 10^5)$ relations (9.2) such that $v, |u - vN| \le 463^3$ are p_n-smooth. Here we use the values $\rho(8.25) \approx 1.38 \cdot 10^{-8}$ and $\rho(3) \approx 4.86 \cdot 10^{-2}$ from [G08, table 1]. M. Charlet has constructed several hundreds such relations (9.2) for the above N. For this N the following program is particular efficient for $N^c = 10^{10}$, $c \approx 5/7$ and pruned to stages with success rate $\ddot{\beta}_t \ge 2^{-14}$. For the first time this recommends to use $c < 1$ as well as relatively small prime bases and to use extreme pruning.

A program for finding relations (9.2) efficiently. Initially the given basis $\mathbf{B}_{n,c}$ gets strongly BKZ-reduced with block size 32 and the target vector $\mathbf{N}_c$ is shifted modulo lattice vectors into the ground mesh of the reduced basis. The initial value $\ddot{A}$, the upper bound on $\|\mathbf{N}_c - \mathcal{L}(\mathbf{B}_{n,c})\|^2$ is set to $\frac{1}{5}\frac{1}{4}\sum_{i=1}^n r_{i,i}^2$ which is $\frac{1}{5}$ the standard upper bound.

LOOP. In each round the vectors of the reduced basis of $\mathcal{L}(\mathbf{B}_{n,c})$ and the shifted $\mathbf{N}_c$ are randomly scaled as follows. For $i = 1, ..., n$ with probabiliy 1/2 all i-th coordinates of the basis vectors and the shifted target vector are multiplied by 2. (This nearly excludes the ßcaledprimes p_i to appear as factors of uv in relations (9.2) resulting from **CVP**-solutions.) The scaled basis gets slightly reduced by BKZ-reduction of block size 20. Then NEW ENUM for **CVP** is called to search for lattice vectors that are close to the shifted target vector $\mathbf{N}_c$. NEW ENUM always decreases $\ddot{A}$ to the square distance to $\mathbf{N}_c$ of the closest found lattice vector. But whenever a relation (9.2) has been found NEW ENUM stops further decreasing $\ddot{A}$ for this round. Whenever a new closer lattice vector is found it is checked whether it yields a relation (9.2). The scaling per rround makes sure that the algorithm produces distinct relations (9.2). This program has been implemented by M. Charlet.

Performance. The program of Charlet found in 2012 in one run of 15 minutes and 350 rounds 136 relations. On average it found a relation every 6.6 seconds. This amounts to a factoring time of 10 minutes. Here are the first 10 of these example relations, they mostly satisfy $|u - vN| \le p_{90}^3$.

round	u	v	$\lvert u - vN\rvert$

6	$19 \cdot 29^2 \cdot 31 \cdot 73 \cdot 109 \cdot 139 \cdot 211 \cdot 359$	415	$2^2 \cdot 11 \cdot 37 \cdot 439$
6	$29 \cdot 37 \cdot 83 \cdot 139 \cdot 191 \cdot 269 \cdot 307 \cdot 443$	865	$2 \cdot 11 \cdot 239 \cdot 383$
12	$2 \cdot 3 \cdot 17^2 \cdot 103 \cdot 263 \cdot 317 \cdot 379 \cdot 443$	25	$13 \cdot 173$
14	$2 \cdot 5 \cdot 47 \cdot 83 \cdot 157 \cdot 179 \cdot 307 \cdot 331 \cdot 421$	469	$19 \cdot 43 \cdot 373$
19	$7^2 \cdot 13 \cdot 41 \cdot 43 \cdot 107 \cdot 109 \cdot 113 \cdot 131 \cdot 409 \cdot 461$	365571	$2^4 \cdot 5 \cdot 11^2 \cdot 197 \cdot 433$
19	$2 \cdot 7 \cdot 13 \cdot 31 \cdot 107 \cdot 127 \cdot 149 \cdot 179 \cdot 383 \cdot 397 \cdot 4391364927$		$3 \cdot 5 \cdot 11 \cdot 61 \cdot 337 \cdot 419$
21	$43 \cdot 131 \cdot 139 \cdot 193 \cdot 307 \cdot 353 \cdot 401 \cdot 439$	28829	$2 \cdot 3^2 \cdot 5^2 \cdot 13 \cdot 41 \cdot 107$
30	$19 \cdot 31 \cdot 53 \cdot 61 \cdot 67 \cdot 131 \cdot 163 \cdot 241 \cdot 313$	2055	$2^2 \cdot 59 \cdot 71 \cdot 89$
31	$13^2 \cdot 17 \cdot 101 \cdot 137 \cdot 199 \cdot 229 \cdot 277 \cdot 331$	1661	$2^6 \cdot 3 \cdot 19 \cdot 233$
33	$19 \cdot 101 \cdot 107 \cdot 127 \cdot 131 \cdot 179 \cdot 191 \cdot 211 \cdot 379$	93398	$3^3 \cdot 13 \cdot 29 \cdot 109 \cdot 167$

Note that $|u - vN|$ increases with v proportionally to $\sqrt{v}$, $|u - vN| \sim \sqrt{v}$.

M. Charlet's program, improved in 2014 by A. Schickedan, found for $N = 100000980001501 \approx 10^{14}$, $n = 90$, $p_{90} = 463$, $c = 1/2$ and pruned to stages with $\ddot{\beta}_t \geq 2^{-14}t$ 99 relations (9.2) in 32 seconds. This factors $N \approx 10^{14}$ in 32 seconds. However for $N \approx 10^{20}$ this program took for $n = 150$, $c = 1/2$ about 34.5 seconds per relation (9.2).and factors N in 86 minutes.

Extending the search of relations (9.2) to large v. This is necessary for factoring $N \gg 10^{14}$ because the $\Phi(N, n, \sigma)$ values get to small for $\sigma = 3$. Let $rel_{N,n,\delta}$ denote the set of relations (9.2) consisting of p_n-smooth $u, v, |u - vN|$ such that $|u - vN| \leq p_n^3$ and $\frac{1}{2}N^\delta \leq v \leq N^\delta$ and let $\#_{N,n,\delta} = card(rel_{N,n,\delta})$. Using (9.7) we neglect the $O(\frac{\ln z+1}{\ln y})$-term of (9.7). The number of p_n-smooth $v \in [\frac{1}{2}N^\delta, N^\delta]$ is $\Psi(N^\delta, p_n) - \Psi(N^\delta/2, p_n) \approx N^\delta\big(\rho(z_v) - \frac{1}{2}\rho(z'_v)\big)$ for $z_v = \frac{\delta \ln N}{\ln p_n}$ $z'_v = z_v - \frac{\ln 2}{\ln p_n}$. Similarly the number of p_n-smooth $u \in [\frac{1}{2}N^{1+\delta}, N^{1+\delta}]$ is $\Psi(N^{1+\delta}, p_n) - \Psi(N^{1+\delta}/2, p_n) \approx N^{1+\delta}\big(\rho(z_u) - \frac{1}{2}\rho(z'_u)\big)$ for $z_u = \frac{(1+\delta)\ln N}{\ln p_n}$, $z'_u = z_u - \ln 2/\ln p_n$. Hence random $v \in_R [\frac{1}{2}N^\delta, N^\delta]$ is p_n-smooth with probability close to $2(\rho(z_v) - \frac{1}{2}\rho(z'_v))$, and random $u \in_R [\frac{1}{2}N^{\delta+1}, N^{\delta+1}]$ is p_n-smooth with probability close to $2(\rho(z_u) - \frac{1}{2}\rho(z'_u))$. $\#_{N,n,\delta}$ is the product of the probabilities of p_n-smoothness for random $v, u, |u - vN|$ with $\frac{1}{2}N^\delta$, the number of $v \in [\frac{1}{2}N^\delta, N^\delta]$ and $2p_n^3$ the number of non zero $u - vN \in [-p_n^3, p_n^3]$. We have 3 factors 2 and one factor 1/2. This yields

$$\#_{N,n,\delta} \approx 4\, N^\delta p_n^3\, \rho(3)\big(\rho(z_u) - \tfrac{1}{2}\rho(z'_u)\big)\big(\rho(z_v) - \tfrac{1}{2}\rho(z'_v)\big) \tag{9.9}$$

assuming that for random u, v, $\frac{1}{2}N^\delta \leq v \leq N^\delta$ and $u \in [\frac{1}{2}N^{1+\delta}, N^{1+\delta}]$ such that $|u - vN| \leq p_n^3$ the p_n-smoothness events for u, v and $|u - vN|$ are nearly statistically independent. Hahn has computed the $\rho(z)$ values for $z = 2, .., 200$ via [Sage] and we interpolate these values for arbitrary z_u, z_v.

For the following statstic we have chosen n, δ for N so that $\#_{N,n,\delta} \gg n$ and $\#_{N,n,\delta}$ is nearly maximal for the given N, n.

$N \approx$	10^{14}	10^{20}	2^{100}	2^{200}	2^{400}	2^{800}
n	90	150	300	1500	8200	42000
p_n	463	863	1987	12553	84127	506131
δ	0.75	0.78	0.8	1.15	1.65	2.095
$\#_{N,n,\delta}$	$1.55 \cdot 10^5$	$6.4 \cdot 10^4$	$9 \cdot 10^3$	$1.46 \cdot 10^4$	$5 \cdot 10^4$	$8.2\, n$

Our prime base is much smaller than the prime base for the quadratic sieve QS. QS requires for $N \approx 2^{400}$ that $p_n \geq e^{1/2\sqrt{lnNlnlnN}} \approx 2 \cdot 10^8$ whereas our $p_{8200} = 84127$.

Corollary 9.1.1 Let $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$, $\mathbf{b} \sim (u,v) \in rel_{N,n,\delta}$, uv squarefree and $p_n^3 = o(N)$. Then we have for $c = \delta + 1 - \frac{3\ln p_n}{\ln N}$ that $||\mathbf{b} - \mathbf{N}_c||^2 = (2\delta+1)\ln N + 1 \pm o(1)$.

Proof. Lemma 1 part **1** shows $||\mathbf{b} - \mathbf{N}_c||^2 = (2\delta+1)\ln N \pm o(1) + \widehat{z}^2_{\mathbf{b}-\mathbf{N}_c}$ Moreover Lemma 1, part **2** shows that $|\widehat{z}_{\mathbf{b}-\mathbf{N}_c}| = N^{c-1-\delta}|u - vN|(1 \pm o(1))$
$\leq N^{c-1-\delta}p_n^3(1 \pm o(1)) = N^0(1 \pm o(1)) = 1 \pm o(1)$
for $c = \delta + 1 - \frac{3\ln p_n}{\ln N}$ which proves the claim. □

Consequences. Cor. 9.1.1 shows that we can enumerate the square-free $(u,v) \in rel_{N,n,\delta}$ by applying the **CVP** algorithm to an unscaled **BKZ**-reduced basis of $\mathcal{L}(\mathbf{B}_{n,c})$ and the target vector $\mathbf{N}_c$, setting $c := \delta+1-\frac{3\ln p_n}{\ln N}$, and fixing the upper bound A of $||\mathbf{b}-\mathbf{N}_c||^2$ to $A := (2\delta+1)\ln N+1$. This way the enumeration also covers many $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ of non square-free $(u,v) \in rel_{N,n,\delta_-}$ for the $\delta_- < \delta$.

Theorem 9.1.2 proves for $p_n = (\ln N)^\alpha$, $\alpha > 2$ that $rd(\mathcal{L}(\mathbf{B}_{n,c}) = o(n^{-1/4})$. Hence Prop. 1 shows that **CVP** runs under heuristic assumptions, including the volume heuristics, in polynomial time. Fixing the initial A increases the running time but preserves the pol. time bound of Prop. 1.

Outline of the CVP-algorithm without scaling. Let $\mathbf{B} = \mathbf{QR} = \mathbf{B}_{n,c}\mathbf{T} = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{Z}^{(n+1)\times n}$ be a BKZ-basis of $\mathcal{L}(\mathbf{B}_{n,c})$, $|\det(\mathbf{T})| = 1$. For $\mathbf{u} = (u_1, ..., u_n)^t \in \mathbb{Z}^n$ we denote $\mathbf{u'} = (u'_1, ..., u'_n)^t = \mathbf{Tu}$ so that $\mathbf{b} := \mathbf{B}_{n,c}\mathbf{u'} = \mathbf{Bu} \sim (u,v)$, with p_n-smooth $u = \prod_{u'_i>0} p_i^{u'_i}$, $v = \prod_{u'_i<0} p_i^{-u'_i} \in \mathbb{N}$. We replace the input $\mathbf{N}_c$ by its projection $\tau(\mathbf{N}_c) = \sum_{i=1}^n \tau_i \mathbf{b}_i \in \mathrm{span}(\mathcal{L})$, where $\tau : \mathbb{R}^{n+1} \to \mathrm{span}\,(\mathcal{L})$ satisfies $\mathbf{N}_c - \tau(\mathbf{N}_c) \in \mathcal{L}^\perp$. Then $\tau(\mathbf{N}_c) = d\,\mathbf{B}_{n,c}\mathbf{1} = d\,\mathbf{B}\,\mathbf{T}^{-1}\mathbf{1}$ holds for $d := \ln N/(N^{-2c} + \sum_{i=1}^n \ln p_i)$, $\mathbf{1} := (1, ..., 1)^t \in \mathbb{Z}^n$.

Starting at $t = n$ the algorithm tries to satisfy (9.10) as t decreases to 1.

$$||\pi_t(\,\mathbf{b} - \tau(\mathbf{N}_c))\,||^2 \leq \tfrac{n-t+1}{n}(2c-1)\ln N + \widehat{z}^2_{\mathbf{b}-\tau(\mathbf{N}_c)} \quad \text{for } \mathbf{b} = \mathbf{Bu} \sim (u,v) \tag{9.10}$$

(9.10) clearly holds for $t = n+1$. If (9.10) holds at $t = 1$ then $||\,\mathbf{b}-\tau(\mathbf{N}_c)||$ and $|u-vN|$ are so small that they can provide a relation (9.2). We denote $\ddot{c}_t = c_t(\tau_t - u_t, ..., \tau_n - u_n) = ||\pi_t(\tau(\mathbf{N}_c) - \mathbf{Bu})||^2$ and $c_t(u_t, ..., u_n) := ||\pi_t(\sum_{i=t}^n u_i\mathbf{b}_i)||^2$.

New Enum for CVP of the prime number lattice creating relations (9.2)
`INPUT` $\mathbf{B}$, $\mathbf{R} = [r_{i,j}] \in \mathbb{R}^{n\times n}$, $\mathbf{B}_{n,c}$, c, $\mathbf{T}$, $\tau_1, ..., \tau_n$, $\ddot{A} \in \mathbb{Q}$ s.t. $||\mathcal{L} - \mathbf{N}_c||^2 < \ddot{A}$, s_{max}.
`OUTPUT` A sequence of $\mathbf{b} = \sum_{i=1}^n u_i\mathbf{b}_i \in \mathcal{L}$ where $\|\mathbf{b} - \mathbf{N}_c\|$ decreases to $||\mathcal{L} - \mathbf{N}_c||$.

1. $s := 10$, $t := n$, $L := \emptyset$, $y_n := \tau_n$, $u_n := \lceil y_n \rfloor$, $\ddot{c}_{n+1} := 0$,
   # $\ddot{c}_t = c_t(\tau_t - u_t, ..., \tau_n - u_n)$ *always holds for the current* $t, u_t, ..., u_n$
   $\mathbf{u} := (0, ..., 0, u_n)^t \in \mathbb{Z}^n$, $\mathbf{b} := \mathbf{B} \cdot \mathbf{u}$, $\mathbf{u'} := \mathbf{T} \cdot \mathbf{u}$.
2. `WHILE` $t \leq n$ #*perform stage* $(t, u_t, ..., u_n, ..., y_t)$:
   [[$\ddot{c}_t := \ddot{c}_{t+1} + (u_t - y_t)^2 r_{t,t}^2$,
   `IF` $\ddot{c}_t \geq \ddot{A}$ `THEN GO TO` 2.1 # *this cuts the present stage*
   $\ddot{\rho}_t := (\ddot{A} - \ddot{c}_t)^{1/2}$, $\ddot{\beta}_t := V_{t-1}\ddot{\rho}_t^{t-1}/(r_{1,1}\cdots r_{t-1,t-1})$,
   `IF` $t = 1$ `THEN` [output $\mathbf{b}$, $\ddot{A} := \ddot{c}_1 = \|\mathbf{b} - \tau(\mathbf{N}_c)\|^2$, `GO TO 2.1`]
   `IF` $\ddot{\beta}_t < 2^{-s}t$ `THEN` [store the current stage in L `GO TO 2.1`]
   [$t := t-1$, $y_t := \tau_t + \sum_{i=t+1}^n (\tau_i - u_i)r_{t,i}/r_{t,t}$, $\sigma_t := sign(u_t - y_t)$
   $u_t := \lceil y_t \rfloor$, $\nu_t := 1$, $u'_i := u'_i + t_{i,t}u_i$ for $i = 1, ..., n$, GO TO 2.]
2.1. `IF` $t < n$ `THEN` $t := t+1$, $u_t := \lceil y_t \rfloor + \lceil \nu_t/2 \rceil \sigma_t, \nu_t := \nu_t + 1, \sigma_t := -\sigma_t$.]]
3. perform and eliminate all undone stages of L on level s; hereby update $\ddot{A}$, delay all new stages with $2^{-s_{max}}t' \leq \ddot{\beta}_{t'} < 2^{-s}t'$, $t' \leq t$ and store them in L.
4. `IF` $s < s_{max}$ `THEN` $s := s+1$ `GO TO 3`

Recall that $\ddot{\beta}_t := V_{t-1}\ddot{\rho}_t^{t-1}/(r_{1,1}\cdots r_{t-1,t-1})$ for $\ddot{\rho}_t := (\ddot{A} - \ddot{c}_t)^{1/2}$ where $\ddot{A} \geq ||\mathcal{L} - \tau(\mathbf{N}_c)||^2$. The success rate $\ddot{\beta}_t$ increases as $\ddot{c}_t$ decreases, The stored stages with small success rate $\ddot{\beta}_t$ will be done after all stages with higher success rate $\ddot{\beta}_t$. They can be cut off if $\ddot{\beta}_t$ is extremely small or if to many stages with higher success rate $\ddot{\beta}_t$ have been stored and the algorithm runs out of storage space.

For the corresponding **SVP**- algorithm we initially replace $\mathbf{B}_{n,c}$ by $[\mathbf{N}_c, \mathbf{B}n, c]$. Note that **BKZ** reduction and `New Enum` can easily be iterated by iteratively increasing c.

Improving New Enum by continued fractions. A. Schickedanz has extended the New Enum algorithm for **CVP** by continued fractions (CF). At stage $(t, u_t, ..., u_n)|$ with $t = 1$ take $\mathbf{b} = \sum_{j=1}^{n} u_j \mathbf{b}_j \in \mathcal{L}(\mathbf{B}_{n,c})$ and the corresponding $(u, v) \sim \mathbf{b}$, $u = \prod_{u_j>0} p_j^{u_j}$ and compute all CF $\frac{h_i}{k_i}$ of $|\delta| := |\frac{u}{N} - \lceil \frac{u}{N} \rfloor|$ with denominators $k_i \lesssim p_n^3$.

The CF-algorithm starts with $\alpha_1 = 1/|\delta|$ and iterates $\alpha_{i+1} := 1/(\alpha_i - \lfloor \alpha_i \rfloor)$ for $i \geq 1$ as long as $\alpha_i > \lfloor \alpha_i \rfloor$. Then $\frac{h_i}{k_i}$ is given by $h_i = \lfloor \alpha_i \rfloor h_{i-1} + h_{i-2}$ and $k_i = \lfloor \alpha_i \rfloor k_{i-1} + k_{i-2}$ where $(h_{-1}, k_{-1}, h_0, k_0) = (1, 0, 0, 1)$ and $h_1 = 1$, $k_1 = \lfloor \alpha_1 \rfloor$. Hence $k_i \geq \prod_{j=1}^{i} \lfloor \alpha_j \rfloor$ and thus each $k_1, ..., k_i$ increases with $\alpha_1 = 1/|\delta|$. Each $\frac{h_i}{k_i}$ is a best approximation under all rational approximations $\frac{h_i'}{k_i}$ of $\delta|$ with denominators $k_i' \leq k_i$. Lagrange has proved that $||\delta| - \frac{h_i}{k_i}| \leq \frac{1}{k_i k_{i+1}}$, where equality holds if and only if $|\delta| = \frac{h_{i+1}}{k_{i+1}}$. This implies

Lemma 9.1.4
$|u_i - v_i N| \leq N/k_{i+1}$ holds for $u_i := uk_i$ and $v_i := \lceil \frac{u}{N} \rfloor k_i + sign(\delta) h_i$

Proof.
$$\begin{aligned} &|u_i - v_i N| = |(u - \lceil \tfrac{u}{N} \rfloor N)k_i - \text{sign}(\delta) h_i N|| \\ &= |(\tfrac{u}{N} - \lceil \tfrac{u}{N} \rfloor - \text{sign}(\delta)\tfrac{h_i}{k_i}) N k_i| = |(\delta - \text{sign}(\delta)\tfrac{h_i}{k_i}) N k_i| \\ &\leq N/k_{i+1} \qquad \text{since } ||\delta| - \tfrac{h_i}{k_i}| \leq \tfrac{1}{k_i k_{i+1}} \quad \text{due to Lagrange's inequality.} \end{aligned}$$ □

Note that $|u_i - v_i N|$ yields a relation (9.2) if k_i and $|u_i - v_i N|$ are p_n-smooth. This way CF improves the **CVP**- minimization of $||\mathcal{L}(\mathbf{B}_{n,c}) - \mathbf{N}_c||$ towards smaller values $|u_i - v_i N|$. CF's provide relations (9.2) with extremely large v_i that need not be p_n-smooth. The number of such relations with possibly p_n-unsmooth v_i increases rapidly with the bit length of v_i.

For $N \approx 10^{14}$ and $c = 1.4$ his program found 14.000 relations (9.2) in 966 seconds, i.e. it took 0.067 seconds per relation. This yields a factoring time for $N \approx 10^{14}$ of 6.8 seconds. These 14.000 relations have been found for one fixed scaling. We present the first 10 of the 14.000 relations. These example relations for $N \approx 10^{14}$ have extremely large $v \gtrsim N^2$ and thus

$$||\mathbf{b} - \mathbf{N}_c||^2 \geq \ln(v^2 N) > 5 \ln N \quad \text{holds for } \mathbf{b} \sim (u, v).$$

The first 10 of the 14.000 relations found for $\mathbf{N \approx 10^{14}}$ via continued fractions for just one scaling

$u = 29 \cdot 89 \cdot 101 \cdot 103 \cdot 109 \cdot 127 \cdot 163 \cdot 167 \cdot 179 \cdot 227 \cdot 257 \cdot 337 \cdot 401 \cdot 409 \cdot 431 \cdot 449 \cdot 457 \cdot 461^2 \cdot 463$
$v = 508169841688914466658429687834 2775$
$|u - vN| = 2^6 \cdot 13 \cdot 157$

$u = 3 \cdot 5^2 \cdot 31 \cdot 101 \cdot 109 \cdot 157^2 \cdot 167^2 \cdot 229^2 \cdot 257 \cdot 263 \cdot 347 \cdot 349 \cdot 383 \cdot 389 \cdot 409 \cdot 439 \cdot 449 \cdot 457 \cdot 461 \cdot 463$
$v = 884490004923637711487480829355666391349$
$|u - vN| = 2 \cdot 19 \cdot 79 \cdot 113$

$u = 3 \cdot 5 \cdot 11 \cdot 23 \cdot 37^2 \cdot 43 \cdot 47 \cdot 73 \cdot 101 \cdot 157 \cdot 163 \cdot 211 \cdot 257 \cdot 263 \cdot 277 \cdot 293 \cdot 313 \cdot 347 \cdot 409 \cdot 431^2 \cdot 449 \cdot 463$
$v = 39337475528468020686337374289751504$
$|u - vN| = 41 \cdot 53 \cdot 383$

$u = 3 \cdot 43 \cdot 47^2 \cdot 73^2 \cdot 101 \cdot 131 \cdot 157 \cdot 163^2 \cdot 167 \cdot 257 \cdot 263 \cdot 269^2 \cdot 409 \cdot 431 \cdot 449 \cdot 457 \cdot 461 \cdot 463$
$v = 39337475528468020686337374289751504$
$|u - vN| = 13 \cdot 199$

$u = 3^2 \cdot 23 \cdot 37 \cdot 43 \cdot 59 \cdot 107 \cdot 157 \cdot 163 \cdot 167 \cdot 179 \cdot 197 \cdot 229 \cdot 257 \cdot 313 \cdot 331 \cdot 379 \cdot 389 \cdot 409 \cdot 431 \cdot 449 \cdot 463$
$v = 113217349317428292671717081216913$
$|u - vN| = 2 \cdot 227 \cdot 311 \cdot 461$

$u = 2^2 \cdot 5^2 \cdot 43 \cdot 47 \cdot 67 \cdot 109 \cdot 137 \cdot 163 \cdot 167 \cdot 229 \cdot 257 \cdot 331 \cdot 389^2 \cdot 409 \cdot 439 \cdot 449 \cdot 457 \cdot 463$
$v = 113197926367550036524784704897 3$
$|u - vN| = 83 \cdot 157 \cdot 317$

$u = 2^5 \cdot 519^2 \cdot 61 \cdot 101 \cdot 103 \cdot 107 \cdot 157^2 \cdot 163 \cdot 257 \cdot 281 \cdot 313 \cdot 331^2 \cdot 389 \cdot 409 \cdot 449 \cdot 457 \cdot 463$
$v = 589845483936124751832121304 5467$
$|u - vN| = 7 \cdot 13^3 \cdot 53$

$u = 2 \cdot 5^3 \cdot 7 \cdot 19^2 \cdot 59 \cdot b79^2 \cdot 89 \cdot 113 \cdot 137 \cdot 197 \cdot 263 \cdot 313 \cdot 313 \cdot 389^2 \cdot 431 \cdot 439 \cdot 449 \cdot 457 \cdot 463$
$v = 467966793632373069227028762631303$
$|u - vN| = 11 \cdot 97 \cdot 359$

$u = 5^2 \cdot 13 \cdot 19^2 \cdot 59 \cdot 101^2 \cdot 197 \cdot 293 \cdot 313 \cdot 331 \cdot 347 \cdot 389 \cdot 409 \cdot 439 \cdot 449 \cdot 457 \cdot 461 \cdot 463$
$v = 448227610967303970415277 1836$
$|u - vN| = 3^2 \cdot 7^3 \cdot 71 \cdot 307$

$u = 17 \cdot 19^2 \cdot 43 \cdot 47 \cdot 73 \cdot 103 \cdot 109 \cdot 113 \cdot 257 \cdot 263 \cdot 281 \cdot 313 \cdot 317 \cdot 347^2 \cdot 431 \cdot 449 \cdot 457 \cdot 463$
$v = 113457285559875139699227627406$
$|u - vN| = 3 \cdot 5^2 \cdot 13^2 \cdot 23 \cdot 89 \cdot 199$

The **CVP** - algorithm has been used for $c = 1.4$. Large c increase the distance $||\mathcal{L}(\mathbf{B}_{n,c}) - \mathbf{N}_c||$ and also increase v of $\mathbf{b} \sim (u, v)$ because $||\mathcal{L}(\mathbf{B}_{n,c}) - \mathbf{N}_c||^2 \approx 2\ln(v^2 N)$. In fact CF extremely decreases $\widehat{z}_{\mathbf{b}-\mathbf{N}_c}$. Note that $|u - vN|$ no more increases with v, the CF stopped this former increase. Interestingly the **CVP**-algorithm only found 78 relations at $t = 1$ before the CF-initiations.

A. Schickedanz uses the following hardware and software.
Hardware: Prozessor AMD Phenom II X4 965 (3.41 GHz), storage: : 16 GB
Software operating system Windows 7 (64 Bit Version), Compiler: GCC 5.2.0 (Mingw-w64 Toolchain)
NTL: 9.6.2 (-02 -m64) Compiler Flags: -std=c++11 -O3 -m64

Comparison with [S93]. Our new results show an enormous progress compared to the previous approach of [S93]. [S93] reports on experiments for $N = 2131438662079 \approx 2.1 \cdot 10^{12}$, $N^c = 10^{25}$, $c \approx 2.0278$ and the prime number basis of dimension $n = 125$ with diagonal entries $\ln p_i$ for $i = 1, ..., n$ instead of $\sqrt{\ln p_i}$. The larger diagonal entries $\ln p_i$ require a larger c and more time for the construction of relations (9.2). The latter took 10 hours per found relation on a PC of 1993.

9.2 Exponentially many of factoring relations with large v

Now let $p_n = (\ln N)^\alpha$ for a small $\alpha > 2$ and a large N. Then p_n and n are larger than for the factoring experiments reported in section 5. Theorem 2 shows for the larger n that there are exponentially many p_n-smooth u, v such that $|u - vN| = 1$, $\frac{1}{2}N^\delta \le v \le N^\delta$. Theorem 3 shows under the assumptions of Theorem 2 and Prop. 1 that vectors $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ closest to $\mathbf{N}_c$ can be found in pol. time. The proof combines the results of Theorem 2, Prop. 1, Lemma 1, Lemma 2 and Cor. 3. We denote for $\delta > 0$

$$M_{N,n,\delta} = \left\{ (u, v) \in \mathbb{N}^2 \;\middle|\; \begin{array}{l} |u - vN| = 1,\ \frac{1}{2}N^\delta \le v \le N^\delta \\ u, v \text{ are } p_n\text{−smooth} \end{array} \right\}.$$

Clearly every $(u,v) \in M_{N,n,\delta}$ yields a relation (9.2) because $|u - vN| = 1$ and uv is p_n-smooth. Theorem 9.1.1 shows that $\#M_{N,n,\delta} \geq N^{\varepsilon} = 2^{\varepsilon k}$, it is exponential in the bit length k of N.

Theorem 9.2.1
Let $\alpha \geq 1.01\frac{2\delta+1}{\delta-\varepsilon}$ and $0 < \varepsilon < \delta < \alpha \ln\ln N$. Assume the events that u, resp. v is p_n-smooth are nearly statistically independent for random v, $\frac{1}{2}N^{\delta} \leq v \leq N^{\delta}$ under the equation $|u - vN| = 1$ then $\#M_{N,n,\delta} \geq N^{\varepsilon}$ holds for sufficiently large N.

Proof. (9.7) shows for $y^z = N$, $y = (\ln N)^{\alpha} = p_n = N^{1/z}$, $z = \ln N/\alpha \ln\ln N$ that

$$\Psi(N, p_n)/N = \big(\tfrac{e+o(1)}{z \ln z}\big)^z = z^{-z-o(z)} \quad \text{holds for } z \to \infty.$$

Extending this equation from N to N^{δ} and $N^{1+\delta}$ our assumption shows for large N :

$$\#M_N, n, \delta \geq N^{\delta}(z\delta)^{-z\delta-o(1)}(z\delta+z)^{-z\delta-z-o(z)},$$
$$\ln \#M_{N,n,\delta} \geq \delta \ln N - z\delta \ln(z\delta) - (z\delta+z)\ln(z\delta+z)\,(1+o(1)).$$

Here N^{δ} counts twice the number of integers v, $\frac{1}{2}N^{\delta} \leq v \leq N^{\delta}$. For every such v there are two $u = vN \pm 1$; $(z\delta)^{-z\delta-o(z)}$ and $(z\delta+z)^{-z\delta-z-o(z)}$ lower bound the portions of these v and u that are p_n-smooth. We assume that the p_n-smoothness events for u and v are nearly statistical independent of the equation $|u - vN| = 1$. Hence we get for $z = \ln N/\alpha \ln\ln N$ that

$$\begin{aligned}
&\ln \#M_{N,n,\delta} > \delta \ln N - \tfrac{(2\delta+1)\ln N \ln(z\delta)}{\alpha \ln\ln N}(1+o(1)) \\
&(\text{ since } \ln(z\delta+z) = \ln(z\delta)(1+o(1)) \text{ for large } z \text{ and constant } \delta\ ) \\
&> \delta \ln N - \tfrac{(2\delta+1)\ln N\,(\ln\ln N - \ln(\alpha\ln\ln N) + \ln\delta)}{\alpha \ln\ln N}(1+o(1)) \qquad (\text{ since } \delta < \alpha \ln\ln N\ ) \\
&\geq \ln N\big(\delta - \tfrac{2\delta+1}{\alpha}1.01\big) \qquad (\text{ for large } N\ ) \\
&> \varepsilon \ln N \qquad \text{since } \alpha > 1.01\tfrac{2\delta+1}{\delta-\varepsilon}. \qquad \text{Hence } \#M_{N,n,\delta} \geq N^{\varepsilon}. \qquad \square
\end{aligned}$$

Theorem 9.2.2
Let $1 < c < (\ln N)^{\alpha/2-1}$. Assume the events that u, resp. v is p_n-smooth are nearly statistically independent for random v, $\frac{1}{2}N^{c} \leq v \leq N^{c}$ under the equation $|u - v| = 1$. Then $\lambda_1^2 = 2c \ln N(1 + o(1))$ and $rd(\mathcal{L}) = o(n^{-1/4})$. If a reduced version of the basis $\mathbf{B}_{n,c}$ is given that satisfies **GSA** *and $\|\mathbf{b}_1\|^2 = O(2c \ln N)$ and if some vector $\ddot{\mathbf{b}} \in \mathcal{L}(\mathbf{B}_{n,c})$ closest to $\mathbf{N}_c$ of (9.2) satisfies* **CA** *then* **New Enum** *finds $\ddot{\mathbf{b}}$ under the volume heuristics in pol. time.*

Remarks. Theorem 9.1.2 shows that $rd(\mathcal{L}) = o(n^{-1/4})$ is as small as required for Prop. 1 and Cor. 3.

Without the volume heuristics the time bound of Theorem 3 increases to $n^{O(1)}(R_{\mathcal{L}}/\lambda_1)^n$ where $R_{\mathcal{L}} = \max_{\mathbf{u} \in \mathrm{span}(\mathcal{L})} \|\mathcal{L} - \mathbf{u}\|$ is the covering radius of $\mathcal{L}$. The factor $(R_{\mathcal{L}}/\lambda_1)^n$ overestimates **New Enum**'s running time since **New Enum** essentially enumerates only lattice points in a ball of radius $\|\mathcal{L} - \mathbf{N}_c\| < \lambda_1 < R_{\mathcal{L}}$.

Proof. We first prove that $\lambda_1^2 = 2c \ln N\ (1 + o(1))$ for $\mathcal{L} := \mathcal{L}(\mathbf{B}_{n,c})$ and $N \to \infty$. We denote

$$\widetilde{M}_{N,n,c} =_{def} \Big\{(u,v) \in \mathbb{N}^2 \;\Big|\; \begin{array}{c} |u-v| = 1,\ \frac{1}{2}N^c \leq v \leq N^c \\ uv\ p_n - \text{smooth} \end{array} \Big\}.$$

Following the proof of Theorem 2 for $\delta = c$ we see that $\#\widetilde{M}_{N,n,c} \geq N^c(zc)^{-2zc-o(z)}$ holds for $z = \frac{\ln N}{\alpha \ln\ln N}$. Recall that $(u,v) \in \widetilde{M}_N, n, c$ defines a vector $\mathbf{b} \sim (u,v)$ in $\mathcal{L}$. Hence

$$\ln \#\widetilde{M}_{N,n,c} \geq \ln N\big(c - \tfrac{2c}{\alpha}(1+o(1))\big) = \Theta(\ln N),$$

since $\alpha > 2$ due to $1 < (\ln N)^{\alpha/2-1}$. Let $\mathcal{L}(\mathbf{B}_{n,c}) \ni \mathbf{b} \sim (u,v) \in \widetilde{M}_{N,n,c}$ and let uv be essentially square-free except for a few small primes. We see from $\frac{1}{2}N^c \le v \le N^c$ and $u = v \pm 1$ that

$$\|\mathbf{b}\|^2 = \ln uv\ (1+o(1)) + \widehat{z}_{\mathbf{b}}^2 \le 2c \ln N\ (1+o(1)) + \widehat{z}_{\mathbf{b}}^2,$$

where $c \ln N - \ln 2 \le \ln v \le c \ln N$. Moreover $\widehat{z}_{\mathbf{b}}^2 = N^{2c} \ln^2(u/v)$ where $|\ln(u/v)| = |\ln(1+\frac{u-v}{v})| \le \frac{1}{v}(1+o(1)) \le 2N^{-c}(1+o(1))$ holds for large N. Hence $\widehat{z}_{\mathbf{b}}^2 \le 4(1+o(1))$ and thus $\lambda_1^2 \le 2c \ln N\ (1+o(1))$. On the other hand $\lambda_1^2 \ge 2c \ln N$ holds by Lemma 2 and thus $\|\mathbf{b}\|^2/\lambda_1^2 = 1 + o(1)$.

Next we bound $rd(\mathcal{L})$ for $\mathcal{L} = \mathcal{L}(\mathbf{B}_{n,c})$. Using $\gamma_n \ge \frac{n}{2e\pi}$ we get

$$\gamma_n (\det \mathcal{L})^{\frac{2}{n}} \ge \tfrac{n}{2e\pi}(\ln p_n \pm o(1)) \cdot N^{2c/n}, \text{ and thus}$$

$$rd(\mathcal{L}) = \lambda_1/(\sqrt{\gamma_n}(\det \mathcal{L})^{\frac{1}{n}}) = \left(\tfrac{2e\pi\, 2c \ln N}{n \ln p_n}\right)^{\frac{1}{2}} / N^{c/n}(1 \pm o(1)).$$

Moreover $c \le (\ln N)^{\alpha/2-1} = \sqrt{p_n}/\ln N$ implies $N^{c/n} = e^{\sqrt{p_n}/n} = e^{o(1)}$ and $N^{c/n} = 1 + o(1)$. Hence

$$\begin{aligned} rd(\mathcal{L}) &= (\tfrac{4e\pi c \ln N}{n \ln p_n})^{1/2}(1+o(1)) = O(\tfrac{\ln N}{p_n})^{1/2} \\ &= O(p_n^{\alpha/2-1})^{1/2} = O(p_n^{-1/4}) = o(n^{-1/4}). \end{aligned}$$

since $p_n = O(n \ln p_n)$ and $c < (\ln N)^{\alpha/2-1}$ and $\ln N = p_n^{1/\alpha}$ and $\alpha > 2$.

Following the proof of [Prop. 1, Cor. 3 of S13] **New Enum** for **CVP** finds for $p_n = (\ln N)^\alpha$ some $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ that minimizes $\|\mathbf{b} - \mathbf{N}_c\|$ in polynomial time, without proving correctness of the minimization. This proves the polynomial time bound. □

Towards factoring integers in pol. time. Theorem 3 shows that we can minimize $||\mathbf{b} - \mathbf{N}_c||$ for $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$ under the vol. heuristics and other reasonable assumptions in pol. time. In order to obtain n relations by the **CVP** algorithm we choose δ to maximize $\#_{N,n,\delta}$ forgiven N, n. In fact n must be so large that $\max_\delta \#_{N,n,\delta} > n$.

Kapitel 10

Weitere Anwendungen

In Kapitel 5 (Seite 43 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 [Ri96], in der er mit Hilfe der Gitterreduktion G. Ortons 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 $z \in L$:*

$$\begin{array}{l} \textit{Es existiert eine erfüllende Belegung} \\ y \in \{0,1\}^n \textit{ zu } \gamma(y) \textit{ mit } z = \pm b(y) \end{array} \quad \Longleftrightarrow \quad \|z\|_\infty = 1$$

Beweis. Wir zeigen beide Richtungen:

„⇒“ Wegen $b(y) \in \{\pm 1, 0\}^{n+m+1}$ gilt $\|z\|_\infty = 1$.

„⇐“ 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 12.2.9 von Seite 106 kennengelernt: Das Problem $\|\cdot\|_\infty$-kürzester Gittervektor ist $\mathcal{NP}$-vollständig.

10.2 Angriff auf Dåmgards Hashfunktion

I.B. Dåmgard [Då89] 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:

$$\begin{array}{rcccl} h_a & : & \{0,1\}^n & \to & \mathbb{N} \\ & & (x_1, \ldots, x_n) & \mapsto & \sum_{i=1}^{n} a_i x_i \end{array}$$

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:

$$\mathrm{E}_a\left[\,\overline{\xi}_x\right] = 0 \tag{10.8}$$

$$\mathrm{E}_a\left[\,\overline{\xi}_x^2\right] = \mathrm{E}_a\left[\,\xi_x^2\right] - 2 \cdot 2^{-m} \cdot \mathrm{E}_a[\,\xi_x] + 2^{-2m} \leq 2 \cdot 2^{-m} \tag{10.9}$$

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. [Fe68]) für eine Zufallsvariable X:

$$\mathrm{Var}[\,X] = \mathrm{E}\left[\,X^2\right] - \mathrm{E}[\,X]^2 \qquad \text{(Definition Varianz)}$$

$$\mathrm{Var}[\,cX] = c^2 \cdot \mathrm{Var}[\,X] \qquad (c > 0 \text{ konstant})$$

$$\mathrm{Ws}[\,|X - \mathrm{E}[\,X]| \geq \epsilon] \leq \frac{1}{\epsilon^2} \cdot \mathrm{Var}[\,X] \qquad \text{(Tschebycheff-Ungleichung)}$$

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.

Kapitel 11

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 9). Bis auf den Gauß-Reduktionsalgorithmus aus Kapitel 3 für aus zwei Vektoren bestehende Basen ist die Reduktion in beliebiger Norm in der Praxis „schwierig“.

11.1 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 $\mu \in \mathbb{R}$:

$$\begin{aligned} \|\mu v\| &= |\mu| \cdot \|v\| && \text{(positive Homogenität)} \\ \|u + v\| &\le \|u\| + \|v\| && \text{(Dreiecksungleichung)} \\ \|u\| &\ge 0 \qquad \text{für } u \neq 0 && \text{(positive Definitheit)} \end{aligned}$$

Wir definieren zu einer gegebenen fest geordneten Gitterbasis Abstandsfunktionen:

Definition 11.1.1 (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 $1 \le i \le n$

$$F_i : \operatorname{span}(b_1, \ldots, b_n) \to \mathbb{R}$$

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

$$V_i := \mathrm{vol} \underbrace{\{x \in \mathrm{span}\,(b_1, \ldots, b_i) \ : \ \|x\| \leq 1\}}_{=\mathrm{span}(b_1,\ldots,b_i) \cap S_{\|\cdot\|}(1)} \qquad i = 1, \ldots, n \tag{11.1}$$

Man beachte, daß sich Volumen stets auf die Euklidische Metrik bezieht.

Lemma 11.1.2
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 11.1.3
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 11.1.2). Wir zeigen durch Induktion über n:

$$\frac{2^n}{n!} \cdot \prod_{i=1}^{n} \frac{\|\widehat{b}_i\|_2}{F_i(b_i)} \leq V_n \leq 2^n \cdot \prod_{i=1}^{n} \frac{\|\widehat{b}_i\|_2}{F_i(b_i)}$$

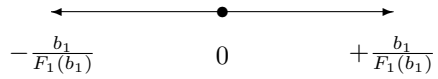

Abbildung 11.1.1: Induktionsverankerung im Beweis zu Lemma 11.1.2

- Induktionsverankerung $n = 1$: Es gilt (vergleiche Abbildung 11.1.1):

$$V_1 = 2 \cdot \frac{\|b_1\|_2}{\|b_1\|} = 2 \cdot \frac{\|\widehat{b}_1\|_2}{F_1(b_1)}$$

- 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 11.1.2). Man erhält eine obere Schranke für V_n durch:

$$V_n \leq 2 \cdot V_{n-1} \cdot \frac{\|\widehat{b}_n\|_2}{F_n(b_n)}$$

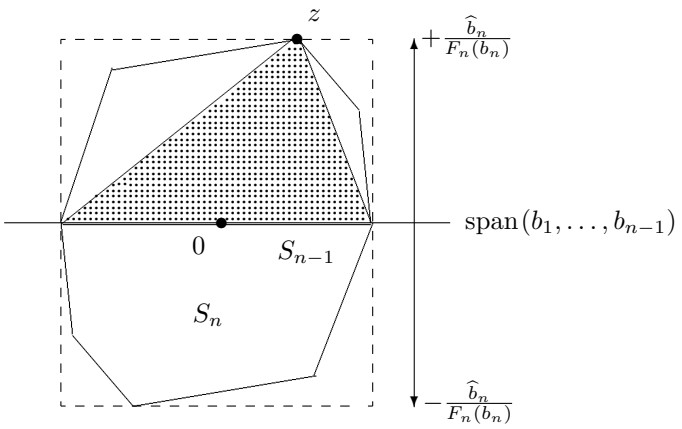

Abbildung 11.1.2: Induktionsschluß im Beweis zu Lemma 11.1.2

Die konvexe Hülle von S_{n-1} und z (gepunktetes Gebiet in Abbildung 11.1.2) 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 11.1.2), 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 11.1.4 (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 2.3.1 (Seite 24), 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 11.1.4). 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 [Mi1896] folgt wegen $\lambda_{1,\|\cdot\|} \leq \lambda_{2,\|\cdot\|} \leq \cdots \leq \lambda_{n,\|\cdot\|}$:

  $$V_n \cdot \lambda_{1,\|\cdot\|}^n \leq 2^n \cdot \det L \tag{11.2}$$

  Aus Lemma 11.1.2 wissen wir:

  $$\frac{n!}{2^n} \cdot \prod_{i=1}^{n} \frac{F_i(b_i)}{\|\widehat{b}_i\|_2} \geq \frac{1}{V_n} \tag{11.3}$$

  Aus $\det L = \prod_{i=1}^{n} \|\widehat{b}_i\|_2$ erhalten wir:

  $$\begin{aligned}
  \lambda_{1,\|\cdot\|}^n &\leq 2^n \cdot V_n^{-1} \cdot \prod_{i=1}^{n} \|\widehat{b}_i\|_2 && \text{(wegen (11.2))} \\
  &\leq 2^n \cdot \left(\frac{n!}{2^n} \cdot \prod_{i=1}^{n} \frac{F_i(b_i)}{\|\widehat{b}_i\|_2} \right) \cdot \left(\prod_{i=1}^{n} \|\widehat{b}_i\|_2 \right) && \text{(wegen (11.3))} \\
  &= n! \cdot \prod_{i=1}^{n} F_i(b_i)
  \end{aligned}$$

■

Es gilt für das Produkt der sukzessiven Minima:

Satz 11.1.5
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 2.3.1 auf Seite 24, besagt:

$$\prod_{i=1}^{n} \lambda_{i,\ell_2} \leq (\gamma_n)^{\frac{n}{2}} \cdot \det L$$

Beweis (zu Satz 11.1.5). Die Behauptung folgt aus dem Beweis zu Satz 11.1.4 durch Anwenden des zweiten Satzes von Minkowski:

$$\frac{\det L}{n!} \leq \frac{V_n}{2^n} \cdot \prod_{i=1}^{n} \lambda_{i,\|\cdot\|} \leq \det L$$

■

11.2 Reduzierte Basen zur Norm $\|\cdot\|$

Analog zur Euklidischen Norm führen wir Reduktionsbegriffe ein und versuchen, Eigenschaften reduzierter Basen zu beweisen.

11.2.1 Definitionen

Wir übertragen die Reduktionsbegriffe auf den Fall einer beliebig vorgegebenen Norm:

Definition 11.2.1 (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 11.2.2 (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.

11.2.2 Eigenschaften 2-reduzierter Gitterbasen

Wir untersuchen die Eigenschaften 2-reduzierter Basen und vergleichen die Resultate mit denen im Spezialfall der ℓ_2-Norm (LLL-reduziert) aus Kapitel 3.

Satz 11.2.3
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 4.1.2 auf Seite 31 $\|\widehat{b}_i\|_2^2 \leq 2 \cdot \|\widehat{b}_{i+1}\|_2^2$, also:

$$\|\widehat{b}_{i+1}\|_2 \geq \sqrt{\tfrac{1}{2}} \cdot \|\widehat{b}_i\|_2$$

Beweis (zu Satz 11.2.3). 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 11.2.4
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 4.1.4 auf Seite 32:

$$\|b_1\|_2 \leq \left(\tfrac{4}{3}\right)^{\frac{n-1}{2}} \cdot \lambda_{1,\ell_2}$$

Beweis. Sei $b = \sum_{i=1}^{n} t_i b_i$ $\|\cdot\|$-minimaler Vektor in $L = (b_1, \ldots, b_n) \setminus \{0\}$. O.B.d.A. sei $t_n \in \mathbb{Z} \setminus \{0\}$. Es gilt:

$$\begin{aligned}
\|b\| &\geq F_n(b) \\
&= \min_{t_1,\ldots,t_{n-1}\in\mathbb{R}} \left\| b - \sum\nolimits_{j=1}^{n-1} t_j b_j \right\| && \text{(Definition)} \\
&= F_n(t_n b_n) \\
&= |t_n| \cdot F_n(b_n) && \text{(Linearität der Norm } F_n\text{)} \\
&\geq F_n(b_n) && \text{(wegen } t_n \in \mathbb{Z} \setminus \{0\}\text{)} \\
&\geq 2^{-n+1} \cdot F_1(b_1) && \text{(induktiv aus Satz 11.2.3)} \\
&= \|b_1\| \cdot 2^{-n+1} && \text{(wegen } F_1(b_i) = \|b_i\| \text{ und } \widehat{b}_1 = b_1\text{)}
\end{aligned}$$

Wegen $\lambda_{1,\|\cdot\|} = \|b\|$ folgt die Behauptung. ■

11.2.3 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 6.1 (Seite 49 und folgende) bewiesen haben. Es gilt für HKZ-reduzierte Basen zur Norm $\|\cdot\|$:

Satz 11.2.5 (Lovász, Scarf 1992)
Sei $b_1, \ldots, b_n$ eine HKZ-reduzierte Basis zu $\|\cdot\|$ des Gitters L. Es gilt für $i = 1, \ldots, n$:

$$\frac{2}{i+1} \cdot \|b_i\| \leq \lambda_{i,\|\cdot\|} \leq \frac{i+1}{2} \cdot F_i(b_i) \leq \frac{i+1}{2} \cdot \|b_i\|$$

Zum Vergleich: Für die ℓ_2-Norm wissen wir aus Satz 6.2.3 auf Seite 51, daß für $i = 1, \ldots, n$ gilt:

$$\frac{i+3}{4} \cdot \|b_i\| \leq \lambda_{i,\ell_2} \leq \frac{i+1}{4} \|b_i\|$$

Beweis (zu Satz 11.2.5). Wir zeigen die untere und obere Schranke:

- Wir zeigen $\frac{2}{i+1} \cdot \|b_i\| \leq \lambda_{i,\|\cdot\|}$ für $i = 1, \ldots, n$. Angenommen, $h_1, \ldots, h_n \in L$ realisieren die sukzessiven Minima $\lambda_1, \ldots, \lambda_n$, d.h. es ist $\|h_i\| = \lambda_{i,\|\cdot\|}$ für $i = 1, \ldots, n$, und die Vektoren $h_1, \ldots, h_n$ sind linear unabhängig. Es gilt

  $$\max_{j \leq i} F_i(h_j) \geq F_i(b_i), \tag{11.4}$$

  weil:

  - wegen $\dim(\operatorname{span}(h_1, \ldots, h_i)) = i$ ist $\max_{j \leq i} F_i(h_j) \neq 0$ und
  - $b_1, \ldots, b_n$ eine HKZ-reduzierte Basis ist, also

    $$F_i(b_i) = \min\{F_i(b) \mid b \in L(b_i, \ldots, b_n) \setminus \{0\}\}$$

    gilt.

  Wir erhalten aus (11.4) und $\lambda_{1,\|\cdot\|} \leq \lambda_{2,\|\cdot\|} \leq \cdots \leq \lambda_{n,\|\cdot\|}$:

  $$\lambda_{i,\|\cdot\|} = \|h_i\| = \max_{j \leq i} \|h_i\| \geq F_i(b_i) \tag{11.5}$$

Wir wenden aus Beweis zu Satz 11.2.3 die Ungleichung

$$\min_{\mu\in\mathbb{Z}} F_j(x+\mu\cdot b_j) \le F_{j+1}(x) + \tfrac{1}{2}\cdot F_j(b_j)$$

rekursiv beginnend mit $x := b_i$ und $j = i-1$ an:

$$\begin{aligned} F_{i-1}(b_i) &\le F_{i-1}(b_i + \mu_{i,i-1}\cdot b_{i-1}) && \text{für alle } \mu_{i,i-1}\in\mathbb{Z} \\ &\le F_i(b_i) + \tfrac{1}{2}\cdot F_{i-1}(b_{i-1}) && \text{für Minimalstelle } \mu_{i,i-1}\in\mathbb{Z} \end{aligned}$$

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 (11.5) die Behauptung:

$$\|b_i\| = F_1(b_i) \le F_1\left(b_i + \sum_{j=1}^{i-1}\mu_{i,j}\cdot b_j\right) \le \frac{i+1}{2}\cdot\lambda_{i,\|\cdot\|} \tag{11.6}$$

- Wir zeigen für $i = 1,\ldots,n$:

$$\lambda_{i,\|\cdot\|} \le \frac{i+1}{2}\cdot F_i(b_i) \le \frac{i+1}{2}\cdot\|b_i\|$$

Es gilt:

$$\begin{aligned} \lambda_{i,\|\cdot\|} &\le \max_{j\le i} F_1(b_j) && \text{(wegen } F_1(b) = \|b\|) \\ &\le \max_{j\le i}\left\{F_j(b_j) + \tfrac{1}{2}\cdot\sum_{t=1}^{j-1}F_t(b_t)\right\} && \text{(wegen (11.6))} \\ &\le \max_{j\le i}\left\{\tfrac{j+1}{2}\cdot F_j(b_j)\right\} && \text{(wegen (11.6))} \\ &\le \tfrac{i+1}{2}\cdot F_1(b_i) && \text{(wegen } F_t(b_t)\le F_1(b_j) \text{ für } t<j) \\ &\le \tfrac{i+1}{2}\cdot\|b_i\| && \text{(wegen } F_1(b_i) = \|\widehat{b}_i\| \le \|b\|) \end{aligned}$$

■

11.2.4 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 6.4 (Seite 57 und folgende) bewiesen haben. Wir definieren:

Definition 11.2.6 (α_β)
Wir setzen:

$$\alpha_\beta := \sup\left\{\frac{\|b_1\|}{F_\beta(b_\beta)} \;\middle|\; \begin{array}{l} b_1,\ldots,b_n \textit{ HKZ-reduzierte} \\ \textit{Basis und } \|\cdot\| \textit{ Norm}\end{array}\right\}$$

Satz 11.2.7
Für jede β-reduzierte Basis $b_1,\ldots,b_n$ zu $\|\cdot\|$ gilt:

$$\|b_1\| \le \alpha_\beta^{\left\lceil\frac{n-1}{\beta-1}\right\rceil}\cdot\lambda_{1,\|\cdot\|}$$

Beweis. Sei $h_i := F_i(b_i)$. Bestimme Index μ mit minimalem h_μ. Nach Satz 11.1.4 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:

$$h_i \leq \alpha_\beta \cdot h_{i+j} \tag{11.7}$$

Wir erhalten durch wiederholtes Anwenden von (11.7):

$$h_1 \leq \alpha_\beta \cdot h_{1+1(\beta-1)} \leq \alpha_\beta^2 \cdot h_{1+2(\beta-1)} \leq \alpha_\beta^3 \cdot h_{1+3(\beta-1)} \leq \ldots \leq \alpha_\beta^{\left\lfloor \frac{\mu-1}{\beta-1} \right\rfloor} \cdot h_{1+\left\lfloor \frac{\mu-1}{\beta-1} \right\rfloor(\beta-1)}$$

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 [S87, Korollar 2.5], daß für

$$\alpha_{\beta,\ell_2} := \sup \left\{ \frac{\|b_1\|_2}{\|\widehat{b}_\beta\|} \ : \ b_1, \ldots, b_n \text{ HKZ-reduzierte Basis} \right\} \tag{11.8}$$

gilt, wobei α_{β,ℓ_2} als Quadrat von (11.8) 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 11.2.8
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 6.4.3 auf Seite 57:

$$\sqrt{\frac{4}{i+3}} \cdot \gamma_\beta^{-\frac{i-1}{\beta-1}} \leq \frac{\|b_i\|}{\lambda_{i,\ell_2}} \leq \sqrt{\frac{i+3}{4}} \cdot \gamma_\beta^{\frac{n-1}{\beta-1}}$$

Der Beweis zu Satz 11.2.8 ist im wesentlichen analog zum Beweis zur ℓ_2-Norm. Wichtiger „Baustein“ ist folgendes Analogon zu Lemma 6.4.5 auf Seite 58: Für jede β-reduzierte Basis $b_1, \ldots, b_n$ gilt:

$$\|b_1\| \leq {\gamma'_\beta}^{\frac{m-\beta/2}{\beta-1}} \cdot M \qquad \text{mit} \quad M := \max_{n-\beta+2 \leq i \leq n} F_i(b_i)$$

11.3 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 $i = 1, \ldots, n$ 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 $b_1, \ldots, b_{i-1}$ festgelegt haben. Es gilt genau dann $F_i(b) \neq 0$, wenn $b \notin \operatorname{span}(b_1, \ldots, b_{i-1})$. Die Vektoren $b_1, \ldots, b_n$ bilden eine Basis von L: Falls dies nicht der Fall ist, existiert ein minimales i, so daß $b_1, \ldots, b_i$ kein primitives System ist:

   $$L \cap \operatorname{span}(b_1, \ldots, b_{i-1}) = L(b_1, \ldots, b_{i-1}) \tag{11.9}$$
   $$L \cap \operatorname{span}(b_1, \ldots, b_i) \supsetneq L(b_1, \ldots, b_i) \tag{11.10}$$

   Wegen 11.10 existiert ein $b \in L \cap \operatorname{span}(b_1, \ldots, b_i) \setminus L(b_1, \ldots, b_i)$ mit:

   $$b = \sum_{j=1}^{i-1} t_j b_j + t_i b_i \qquad \text{mit } t_1, \ldots, t_{i-1} \in \mathbb{Z} \text{ und } t_i \notin \mathbb{Z}$$

   Sei $k > 1$ der Index der additiven Untergruppe $L(b_1, \ldots, b_i)$ in $\operatorname{span}(b_1, \ldots, b_i) \cap L$. Wegen (11.9) 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:

   $$F_i(t_1 b_1 + t_2 b_2 + \cdots + t' b_i) = F_i(t' b_i) = |t'| \cdot F_i(b_i) < F_i(b_i).$$

2. Längenreduktion: Für $i = 1, \ldots, n$, für $j = i-1, i-2, \ldots, 1$ wähle $\mu_{i,j} \in \mathbb{Z}$, so daß:

   $$F_j(b_i + \mu_{i,i-1} b_{i-1} + \mu_{i,i-2} b_{i-2} + \cdots + \mu_{i,j} b_j)$$

   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 11.3.1
Obige Konstruktion liefert eine HKZ-reduzierte Basis $b_1, \ldots, b_n$ des Gitters L.

Beweis. Nachrechnen! ■

11.4 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 [J48] 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 6.4.3:

$$\tfrac{1}{n} \cdot \sqrt{\tfrac{4}{i+3}} \cdot \gamma_\beta^{-\frac{i-1}{\beta-1}} \leq \frac{\|b_i\|}{\lambda_{i,\|\cdot\|}} \leq n \cdot \sqrt{\tfrac{i+3}{4}} \cdot \gamma_\beta^{\frac{n-1}{\beta-1}} \tag{11.11}$$

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 (11.11) schärfer als Satz 11.2.8, weil $\gamma'_\beta = \Theta\left(\gamma_\beta^2\right)$. Für große Blockweiten $\beta \approx n$ ist Satz 11.2.8 schärfer. Für $\beta = n$ sind die Schranken für HKZ-reduzierte Basen zu $\|\cdot\|$ um den Faktor $\sqrt{n}$ besser als die Schranken (11.11).

11.5 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 [Ri96] gibt eine Übersicht über die Aufzählung kürzester Gittervektoren in der sup-Norm.

11.5.1 ENUM-Algorithmus für beliebige Norm

Wir verallgemeinern Algorithmus **??** von Seite **??**. 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

$$\left| F_t\left(u \cdot b_t + \sum_{i=t}^{n} \tilde{u}_i b_i\right) - F_t\left(u' \cdot b_t + \sum_{i=t}^{n} \tilde{u}_i b_i\right) \right| \tag{11.12}$$

und mit $\mathrm{next}_{F_t}(\tilde{u}_t, u)$ die nächste, ganzzahlige Nullstelle von (11.12) 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.

11.5.2 Gauß-ENUM-Algorithmus für beliebige Norm

Betrachten wir Schritt 2 des Algorithmus' 11.5.1. 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 11.5.1 $\|\cdot\|$-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 $F_t\left(ub_t + \sum_{i=t+1}^{n} \tilde{u}_i b_i\right)$

$\tilde{u}_t := \mathrm{next}_{F_t}(u)$

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 */

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

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:

$$\begin{aligned} \left|\overline{L} \cap \left[S_{\|\cdot\|}(\, c_1^{\min}) + z\right]\right| &\approx \frac{\mathrm{vol}_{t-1}\left(\mathrm{span}\left(\,\overline{L}\,\right) \cap \left[S_{\|\cdot\|}(\, c_1^{\min}) + z\right]\right)}{\det \overline{L}} \\ &= \frac{\mathrm{vol}_{t-1}\left(\,\left[w + \mathrm{span}\left(\,\overline{L}\,\right)\right] \cap S_{\|\cdot\|}(\, c_1^{\min})\right)}{\det \overline{L}} \end{aligned}$$

Wann gilt die Volumen-Heuristik streng? Hinreichende Voraussetzung: Bei festem y ist z uniformly distributed modulo $\overline{L}$ (vergleiche Definition **??** auf Seite **??**):

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

Die Menge $\left(b + \operatorname{span}\left(\overline{L}\right)\right) \cap S_{\|\cdot\|}(c_1^{\min})$ hängt nur von z, aber nicht von y ab. Es folgt aus der Volumenheuristik Lemma 8.2.1 (Seite 68):

Lemma 11.5.1
Angenommen, z ist uniformly distributed modulo $\overline{L}$ und unabhängig von y. Dann gilt

$$\mathrm{E}\left[\left|\left[w + \overline{L}\right] \cap S_{\|\cdot\|}(c_1^{\min})\right|\right] = \frac{\mathrm{vol}_{t-1}\left(\left[y + \operatorname{span}\left(\overline{L}\right)\right] \cap S_{\|\cdot\|}(c_1^{\min})\right)}{\det \overline{L}},$$

wobei $y + \operatorname{span}\left(\overline{L}\right) = b + \operatorname{span}\left(\overline{L}\right)$.

Wir erhalten analog zu Satz **??**:

Satz 11.5.2
Angenommen, $(\{\mu_{i,j}\} : 1 \le j < i \le n)$ ist gleichverteilt in $[0,1[^{\binom{n}{2}}$. Dann gilt in Algorithmus 11.5.1 $\|\cdot\|$-ENUM stets:

- *z ist uniformly distributed modulo $\overline{L}$ und unabhängig von y.*
- $\mathrm{E}\left[\left|\left[w + \overline{L}\right] \cap S_{\|\cdot\|}(c_1^{\min})\right|\right] = \dfrac{\mathrm{vol}_{t-1}\left(\left[y + \operatorname{span}\left(\overline{L}\right)\right] \cap S_{\|\cdot\|}(c_1^{\min})\right)}{\det \overline{L}}$

Wir erhalten Gauß-$\|\cdot\|$-ENUM aus Algorithmus' 11.5.1, indem wir Schritt 2 ersetzen durch:

$$\text{IF } \frac{\mathrm{vol}_{t-1}\left(\left[y + \operatorname{span}\left(\overline{L}\right)\right] \cap S_{\|\cdot\|}(c_1^{\min})\right)}{\det \overline{L}} \ge 2^{-p}$$

Kapitel 12

Komplexität, $\mathcal{NP}$-Vollständigkeit

Wir fassen mit Hinblick auf die Gittertheorie die Grundbegriffe der Komplexitätstheorie, speziell die $\mathcal{NP}$-Vollständigkeit, zusammen.

12.1 $\mathcal{NP}$-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 $A = [a_{ij}] \in \mathbb{Q}^{m \times n}$

Wir setzen die Laufzeit des Algorithmus' in Beziehung zur Eingabelänge. Wir interessieren uns für Polynomialzeit-Verfahren:

Definition 12.1.1 (Polynomialzeit)
Ein Algorithmus ist in Polynomialzeit, falls die Schrittzahl (Turing-Maschine oder Anzahl Bit-Operationen) polynomiell in der Länge der Eingabe beschränkt ist:

$$\textit{Schrittzahl(Eingabe)} = \mathrm{poly}(\ell(\textit{Eingabe}))$$

In der theoretischen Informatik betrachtet man die Polynomialzeit-Algorithmen als effizient.

Definition 12.1.2 (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 12.1.3 (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 12.1.4 (Klasse $\mathcal{NP}$)
Die Klasse $\mathcal{NP}$ der nichtdeterministischen Polynomialzeit-Sprachen $A \subseteq \{0,1\}^*$ ist erklärt durch:

$$A \in \mathcal{NP} \iff \begin{array}{l} \exists B \in \{0,1\}^* \times \{0,1\}^*, B \in \mathcal{P} : \\ A = \left\{ x \in \{0,1\}^* \;\middle|\; \exists y \in \{0,1\}^{\mathrm{poly}(\ell(x))} \text{ mit } (x,y) \in B \right\} \end{array}$$

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 12.1.5 (Karp-Reduktion)
Seien $A, B \subseteq \{0,1\}^*$:

$$A \leq_{pol} B \iff \begin{array}{l} \exists \text{ Polynomialzeit-Abbildung } h \text{ mit:} \\ \forall x \in \{0,1\}^* : x \in A \Leftrightarrow h(x) \in B \end{array}$$

Aus $A \leq_{\mathrm{pol}} B$ und $B \leq_{\mathrm{pol}} C$ folgt $A \leq_{\mathrm{pol}} C$.

Definition 12.1.6 ($\mathcal{NP}$-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 $\mathcal{NP}$.

12.2 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 12.2.1 (Ganzzahlige, lineare Programmierung)
Das Problem der ganzzahligen, linearen Programmierung lautet:

- *Gegeben: $m, n \in \mathbb{N}$, $A \in (\mathbb{Z})^{m \times n}$ 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 12.2.5 sehen, daß das zugehörige Entscheidungsproblem $\mathcal{NP}$-vollständig ist:

Definition 12.2.2 (Entscheidungsproblem der ganzzahligen, linearen Programmierung)
Das Problem der ganzzahligen, linearen Programmierung lautet:

- *Gegeben: $m, n \in \mathbb{N}$, $A \in \mathbb{Z}^{m \times n}$ 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 12.2.3 (Rationale, lineare Programmierung)
Das Problem der rationalen, linearen Programmierung lautet:

- *Gegeben: $m, n \in \mathbb{N}$, $A \in \mathbb{Z}^{m \times n}$ 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 [Kh79, Kh80]. Diese Methode ist aber nicht praktikabel. Ein bekannter Polynomialzeit-Algorithmus stammt von M. Karmarkars [Ka84]. 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 [Da63, Schr86] von G.B. Dantzig, der allerdings im Wortcase exponentielle Laufzeit haben kann. Weitere Probleme, die man in Polynomialzeit lösen kann, sind:

Satz 12.2.4 (Sieveking 1976)
Folgende Probleme sind zu gegebenen $m, n \in \mathbb{N}$, $A \in \mathbb{Z}^{m \times n}$ und $b \in (\mathbb{Z})$ 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 [SS76]). Alternativer Beweis in [KaBa79]. ■

Im folgenden Satz führen wir weitere mit der Gittertheorie verbundene Aufgaben bzw. Entscheidungsprobleme auf, die $\mathcal{NP}$-vollständig sind.

Satz 12.2.5
Folgende Sprachen sind $\mathcal{NP}$-vollständig:

1. *Integer-Programming:*

$$\text{IP} := \left\{ (m, n, A, b) \;\middle|\; \begin{array}{l} A \in \mathbb{Z}^{m \times n}, b \in \mathbb{Z}^m, \\ \exists x \in \mathbb{Z}^n : Ax \leq b \end{array} \right\}$$

2. *Rucksack (Knapsack) oder Subsetsum:*

$$\text{SubsetSum} := \left\{ (n, a_1, \ldots, a_n, b) \in \mathbb{N}^{n+2} \;\middle|\; \exists x \in \{0,1\}^n : \sum_{i=1}^{n} a_i x_i = b \right\}$$

3. *$\{0,1\}$-Integer-Programming:*

$$\{0,1\}\text{-IP} := \left\{ (m, n, A, b) \;\middle|\; \begin{array}{l} A \in \mathbb{Z}^{m \times n}, b \in \mathbb{Z}^m, \\ \exists x \in \{0,1\}^n : Ax \leq b \end{array} \right\}$$

4. Schwache Zerlegung:

$$\left\{ (n, a_1, \ldots, a_n) \in \mathbb{N}^{n+1} \;\middle|\; \exists\, (x_1, \ldots, x_n) \in \{0, \pm 1\}^n \setminus \{0^n\} : \sum_{i=1}^{n} a_i x_i = 0 \right\}$$

Beweis. Für 1,2,3 siehe [GaJo79][SS76], für 4 siehe [EB81]. Den Nachweis, daß es für die Sprache Integer-Programming polynomiell lange Zeugen gibt, also IP $\in \mathcal{NP}$, werden wir in Satz 12.2.6 führen. ■

Satz 12.2.6 (von zur Gathen, Sieveking 1978)
IP $\in \mathcal{NP}$.

Beweis. Wir wählen als Zeugen für $(m, n, A, b) \in \text{IP}$ ein geeignetes $x \in \mathbb{Z}^n$ mit $Ax \leq b$. Offenbar existiert x genau dann, wenn $(m, n, A, b) \in \text{IP}$. Wir müssen noch zeigen, daß der Zeuge polynomielle Länge hat.

Sei $A =: (a_{ij})_{ij}$ und $b =: (b_1, \ldots, b_m)^{\mathsf{T}}$. 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 12.2.7 (Gitter, Basis, Dimension, Rang)
Seien $b_1, \ldots, b_n \in \mathbb{R}^m$ linear unabhängige Vektoren. Wir nennen die additive Untergruppe

$$L(b_1, \ldots, b_n) := \sum_{i=1}^{n} b_i \mathbb{Z} = \left\{ \sum_{i=1}^{n} t_i b_i \;\middle|\; t_1, \ldots, t_m \in \mathbb{Z} \right\}$$

des $\mathbb{R}^m$ ein Gitter mit der Basis $b_1, \ldots, b_n$. Ist die Reihenfolge der Basisvektoren fest, sprechen wir von einer geordneten Basis. Der Rang oder auch die Dimension des Gitters ist $\text{Rang}(L) := n$.

Betrachten wir ein Beispiel:

Beispiel 12.2.8 (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 $n - \text{Rang}(A)$; nach Satz 12.2.4 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 12.2.9
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 12.2.5 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 12.2.10 (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 12.2.9) bislang fehlgeschlagen (vergleiche [K87]).

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 12.2.11 (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 KANNAN [K87]. ■

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 $z \in \operatorname{span}(b_1, \ldots, b_n)$ 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, $n \geq \operatorname{Rang}(L)$, eine Gitterbasis konstruieren.

.

Kapitel 13

Grundlagen

13.1 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:

$$\langle u, u \rangle > 0 \qquad \text{für } u \neq 0$$

Die meisten Anwendungen beziehen sich auf das *Standard-Skalarprodukt*:

$$\langle (u_1, \ldots, u_n), (v_1, \ldots, v_n) \rangle := \sum_{i=1}^{n} u_i v_i$$

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 $S \in \mathbb{R}^{n \times n}$. 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: $\| (u_1, \ldots, u_n) \|_1 := \sum_{i=1}^n |u_i|$
Die ℓ_2-*Norm* zum Standard-Skalarprodukt ist: $\| (u_1, \ldots, u_n) \|_2 := \sqrt{\langle u, u \rangle} = \left(\sum_{i=1}^n u_i^2 \right)^{\frac{1}{2}}$.
Die ℓ_p-*Norm* ist: $\| (u_1, \ldots, u_n) \|_p := \left(\sum_{i=1}^n |u_i|^p \right)^{\frac{1}{p}}$.
Die *sup-Norm*, *Maximums-Norm* oder auch ℓ_∞-*Norm* ist: $\| (u_1, \ldots, u_n) \|_\infty := \max_{i=1,\ldots,n} |u_i|$.

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.

Algorithmenverzeichnis

Literaturverzeichnis

[Aj98] *M. Ajtai*, The Shortest Vector Problem in L_2 is NP-hard for Randomized Reductions. Proc. 30th STOC, pp. 10–19, 1998.

[Aj03] *M. Ajtai*, The Worst-case Behavior of Schnorr's Algorithm Approximating the Shortest Nonzero Vector in a Lattice. Proc. 35th STOC, pp. 396–406 2003.

[AKS01] *M. Ajtai, R. Kumar, and D. Sivakumar*, A Sieve Algorithm for the Shortest Lattice Vector Problem. Proc. 33th STOC, pp. 601–610, 2001.

[Ak02] *A. Akhavi*, Random Lattices, Threshold Phenomena and Efficient Reduction Algorithms. *Theoret. Comput. Sci.*, **287**, pp. 359–385, 2002.

[Ba86] *L. Babai* , On Lovász' Lattice Reduction and the nearest Lattice Point Problem, Combinatorica, Band 6, Seiten 1–13, 1986.

[Bar59] *E.S. Barnes* , The Contruction of perfect and extreme Forms II, Acta Arithmetica, Band 5, Seiten 205-222, 1959.

[BaKa84] *A. Bachem und R. Kannan* , Lattices and the Basis Reduction Algorithm, Technischer Report, Carnegie-Mellon-Universität (USA), (1984).

[BeWe93] *Th. Becker und V. Weispfennig*, Gröbner Bases — a computational Approach to commutative Algebra, Graduate Texts in Mathematics, Band 141, Springer-Verlag, Berlin/Heidelberg, 1993.

[Bli14] *H.F. Blichfeldt*, A new Principle in the Geometry of Numbers with some Applications, Transaction of the American Mathematical Society, Band 15, Seiten 227–235, 1914.

[Bli29] *H.F. Blichfeldt* , The Minimum Value of quadratic Forms and the closet Packing of Sphere, Mathematische Annalen, Band 101, Seiten 366-389, 1929.

[Bli35] *H.F. Blichfeldt*, The minimum Value of positive Quadratic Forms in six, seven and eight Variables, Mathematische Zeitschrift, Band 39, Seiten 1–15, 1935.

[Be80] *G. Bergman*, Notes on Ferguson and Forcade's Generalized Euclidean Algorithm. TR. Dep. of Mathematics, University of Berkeley, CA, 1980.

[BM03] *J. Blömer and A. May* New Partial Key Exposure Attacks on RSA. Proc. Crypto'2003, Lecture Notes in Comp.Sci., 2729, Springer, New York, pp. 27 - 43, 2003.

[BS99] *J. Blömer and J.P. Seifert*, On the Complexity of Computing Short Linearly Independent Vectors and Short Bases in a Lattice. Proc. 31th STOC, pp. 711–720, 1999.

[Bo00] *D. Boneh*, Finding Smooth Integers in Small Intervals Using CRT Decoding. Proc. 32th STOC, pp. 265-272, 2000.

[Bb65] *B. Buchenberger 1965*, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal, Dissertation, Fachbereich Mathematik, Universität Insbruck (Österreich), 1965.

[Ca00] *J. Cai*, The Complexity of some Lattice Problems. Algorithmic Number Theory, Lecture Notes in Comput. Sci., 1838, Springer, New York, pp. 1-32, 2000.

[Co97] *D. Coppersmith*, Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities. *J. Cryptology*, **10**, pp. 233-260, 1997.

[Co01] *D. Coppersmith*, Finding Small Solutions to Small Degree Polynomials. Cryptography and Lattices, Lecture Notes in Comput. Sci., Springer, New York, 2146, pp. 20-31, 2001.

[Ca71] *J.W.S. Cassels* , An Introduction to the Geometry of Numbers, Springer-Verlag, Berlin/Heidelberg, 1971.

[CK09] *H. Cohn and A. Kumar*, Optimality and Uniqueness of the Leech Lattice among Lattices, Annals of Mathematics **170** (3), pp. 1003 – 1050, 2009.

[Co93] *H. Cohen* , A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics, Band 138, Springer-Verlag, Berlin/Heidelberg, 1993.

[CoSl88] *J.H. Conway und N.J. Sloane* , Sphere Packings, Lattices and Groups, Springer-Verlag, New York, 1988.

[CJLOSS92] *M.J. Coster, A. Joux, B.A. LaMacchina, A.M. Odlyzko, C.P. Schnorr und J. Stern*, An improved low-density Subset Sum Algorithm, Computational Complexity, Band 2, Seiten 111–128, 1992.

[CR88] *B. Chor und R.L. Rivest*, A Knapsack type Public Key Cryptosystem based on Arithmetic in finite Fields, IEEE Transaction Information Theory, Band IT-34, Seiten 901–909, 1988.

[Då89] *I.B. Dåmgard*, 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, 1989.

[Da63] *G.B. Dantzig* , Linear Programming and Extensions, Princeton University Press, Princeton, New Jersey (dt. Übersetzung „Lineare Programmierung und Erweiterungen“ 1966 im Springer-Verlag, Berlin/Heidelberg, erschienen), 1963.

[DV94] *H. Daudé and B. Vallée*, An Upper Bound on the Average Number of Iterations of the LLL algorithm, *Theoret. Comput. Sci.*, **123**, pp. 395–115, 1994.

[D30] *K. Dickman*, On the frequency of numbers containing prime factors of a certain relative magnitude. *Ark. Math. Astr. Fys.* **22**, pp. 1–14, 1930.

[DKRS03] I. Dinur, G. Kindler, R.Raz, S.Safra, Approximating CVP to within polynomial factors is NP-hard, *Combinatorica* **23** (2), pp. 205–243, 2003.

[Di1842] *G.L. Dirichlet*, 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, 1842.

[D81] *J.D. Dixon*, Asymptotically Fast Factorization of Integers. *Mathematics of Computation* **36**(153), pp. 255–260, 1981.

[DKT87] *P.D. Domich, R. Kannan und L.E. Trotter*, Hermite normal Form Computation using modulo Determinant Arithmetic, Mathematics of Operation Research, Band 12, Nr. 1 (Februar), Seiten 50–59, 1987.

[EB81] *P. van Emde Boas*, 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, 1981.

[E91] *M. Euchner* , Praktische Algorithmen zur Gitterreduktion und Faktorisierung, Diplomarbeit, Fachbereich Informatik der Johann-Wolfgang-Goethe-Universität, Frankfurt/Main, 1991.

[Fe68] *W. Feller*, An Introduction to Probability Theory and its Application, Band I, 3. Auflage, John Wiley & Sons, New York, 1968.

[Fr86] *A.M. Frieze* , On the Lagarias-Odlyzko Algorithm for the Subset Sum Problem, SIAM Journal on Computing, Band 15, Nr. 2, Seiten 536–539, 1986.

[GaSi78] *J. von zur Gathen und M. Sieveking* , A Bound on Solution of linear Integer Equations and Inequations, Proceedings of the American Mathematical Society, Band 72, Seiten 155–158, 1978.

[GaJo79] *M.R. Garey, D.S. Johnson*, Computer and Intractability: A Guide to the Theory of $\mathcal{NP}$-Completness, W.H. Freeman and Company, San Francisco, 1979.

[G1801] *C.F. Gauß* , Disquisitiones Arithmeticae, Gerhard Fleischer, Leipzig. Deutsche Übersetzung (1889): „Untersuchung über höhere Arithmetik“, Springer-Verlag, Berlin/Heidelberg, 1801.

[GrLek87] *M. Gruber und C.G. Lekkerkerker*, Geometry of Numbers, 2. Auflage, North-Holland, Amsterdam, 1987.

[GLLS88] *M. Grötschel, L. Lovász and A. Schrijver*, Geometric Algorithms and combinatorial Optimization, Algorithms and Combinatorics, Band 2, Springer-Verlag, Berlin/Heidelberg, 1988.

[GHKN06] *N. Gama, N. How-Grave-Graham, H. Koy and P. Nguyen*, Rankin's Constant and Blockwise Lattice Reduction, In Proc. CRYPTO 2006, LNCS 4117, Springer-Verlag, Berlin/Heidelberg, pp. 112–139, 2006.

[GN08a] *N. Gama and P. Nguyen*, Predicting Lattice Reduction. In Proc. EUROCRYPT 2008, LNCS 4965, Springer-Verlag, Berlin/Heidelberg, pp. 31–51, 2008.

[GN08b] *N. Gama and P. Nguyen*, Finding Short Lattice Vectors within Mordell.s Inequality, In Proc. of the 2008 ACM Symposium on Theory of Computing, pp. 208–216, 2008.

[GNR10] *N. Gama, P.Q. Nguyen and O. Regev*, Lattice enumeration using extreme pruning, Proc. EUROCRYPT 2010, LNCS 6110, Springer-Verlarg, pp. 257–278, 2010, final version to be published.

[HS07] *G. Hanrot and D. Stehlé*, Improved Analysis of Kannan's Shortest Lattice Vector Algorithm (Extended Abstract), Proc. CRYPTO 2007, LNCS 4622, Springer-Verlarg, pp. 170–186, 2007.

[HaMcC91] *J. Hafner und K. McCurley* , Asymptotic Fast Triangulation of Matrices over Ring, SIAM Journal on Computing, Band 20, Nr. 6, Seiten 1068–1083, 1991.

[HJLS89] *J. Håstad, B. Just, J.C. Lagarias und C.P. Schnorr* , Polynomial Time Algorithms for Finding Integer Relations among real Numbers, SIAM Journal on Computing, Band 18, Nr. 5, Seiten 859–881, 1989.

[HT98] *C. Heckler and L. Thiele* Complexity Analysis of a Parallel Lattice Basis Algorithm. *Siam J. Comput.* **27**(5), pp. 1295–1302, 1998.

[He85] *B. Helfrich 1985*, Algorithms to construct Minkowski reduced and Hermite reduced Lattice Bases, Theoretical Computer Science, Band 41, Seiten 125–139, 1985.

[He1850] *C. Hermite*, 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, 1850.

[H84] *A. Hildebrand*, Integers free of large prime factors and the Riemann hypothesis. *Mathematika* **31**, pp. 258–271, 1984.

[Hl44] *E. Hlawka* , Zur Geometrie der Zahlen, Mathematische Zeitschrift, Band 49, Seiten 285–312, 1944.

[J48] *F. John* , 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, 1948.

[JoSt94] *A. Joux und J. Stern* , Lattice Reduction: A Toolbox for the Cryptanalyst, Technischer Report, DGA/CELAR, Bruz (Frankreich). Eingereicht bei Journal of Cryptology, 1994.

[KaLe78] *G.A. Kabatiansky und V.I. Levenshtein* , Bounds for Packings on a Sphere and in Space, Problems of Information Transmission, Band 14, Seiten 1–17, 1978.

[Ka91] *M. Kaib* , 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, 1991.

[Ka94] *M. Kaib* , Gitterbasenreduktion für beliebige Normen, Dissertation, Fachbereich Mathematik der Johann-Wolfgang-Goethe-Universität, Frankfurt/Main, 1994.

[KS96] *M. Kaib und C.P. Schnorr*, The Generalized Gauss Reduction Algorithm, Journal of Algorithms, Band 21, Nr. 3 (November), Seiten 565–578, 1996.

[KaBa79] *R. Kannan und A. Bachem*, Polynomial Algorithm for Computing the Smith and the Hermite Normal Form of an Integer Matrix, SIAM Journal on Computing, Band 8, Seiten 499–507, 1979.

[K87] *R. Kannan*, Minkowski's Convex Body Theorem and Integer Programming. Math. Oper. Res., **12**, pp. 415–440, 1987.

[Ka01] *H. Koy*, Notes of a Lecture. Frankfurt 2004., //www.mi.informatik.uni-frankfurt.de/index.html#publications

[Ka84] *M. Karmarkar*, A new Polynomial-Time Algorithm for Linear Programming, Combinatorica, Band 4, Seiten 373–395, 1984.

[Kh79] *L.G. Khachiyan*, A Polynomial Algorithm in Linear Programming, Soviet Mathmatics Doklady, Band 20, Seiten 191–194, 1979.

[Kh80] *L.G. Khachiyan*, Polynomial Algorithms in Linear Programming, U.S.S.R. Computational Mathematics and Mathematical Physics, Band 20, Seiten 53–72, 1980

[Kh05] *S. Khot*, Hardness of Approximating the Shortest Vector Problem in Lattices, Journal of the ACM, Vol. 52, No. 5, Seiten 789–803, 2005.

[Kh71] *D.E. Knuth*, The Art of Computer Programming, Fundamental Algorithms, Band I, Addison-Wesley, Reading, 2001.

[Ko04] *H. Koy*, Primal/duale Segmentreduktion von Gitterbasen, Vortrag 7. Mai 2004, //www.mi.informatik.uni-frankfurt.de/research/papers.html

[KZ1872] *A. Korkine und G. Zolotareff*, Sur les formes quadratique positive quaternaires, Mathematische Annalen, Band 5, Seiten 366-389, 1872.

[KZ1873] *A. Korkine und G. Zolotareff*, Sur les formes quadratique, Mathematische Annalen, Band 6, Seiten 366–389, 1873

[KZ1877] *A. Korkine und G. Zolotareff*, Sur les formes quadratique positive, Mathematische Annalen, Band 11, Seiten 242–292, 1877.

[KS01a] *H. Koy and C.P. Schnorr*, Segment LLL-Reduction. Cryptography and Lattices, Lecture Notes in Comput. Sci., 2146, Springer, New York, pp.67–80, 2001. //www.mi.informatik.uni-frankfurt.de/research/papers.html

[KS01b] *H. Koy and C.P. Schnorr*, Segment LLL-Reduction with Floating Point Orthogonalization. Cryptography and Lattices, Lecture Notes in Comput. Sci., 2146, Springer, New York, pp. 81–96, 2001. //www.mi.informatik.uni-frankfurt.de/research/papers.html

[KS02] *H. Koy and C.P. Schnorr*, Segment and Strong Segment LLL-Reduction of Lattice Bases. TR Universität Franfurt, April 2002, //www.mi.informatik.uni-frankfurt.de/research/papers.html

[Ko04] *H. Koy*, Files of a lecture, Frankfurt, May 2004, //www.math.uni-frankfurt.de/ dmst/, see publications.

[LA] 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*, Recherches d'arithmétique, Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres, Berlin, Seiten 265–312,1773.

[Lang93] *S. Lang*, Algebra, 3. Auflage, Addison-Wesley, Reading, 1993

[LLS90] *J.C. Lagarias, H.W. Lenstra und C.P. Schnorr*, Korkin-Zolotarev Bases and successive Minima of a Lattice and its reciprocal lattice, Combinatorica, Band 10, Seiten 333–348, 1998.

[LaOd85] *J.C. Lagarias und A.M. Odlyzko*, Solving low-density Subset Sum Problems, Journal of ACM, Band 32, Nr. 1, Seiten 229–246, 1985.

[LLL82] *A.K. Lenstra, H.W. Lenstra und L. Lovász*, Factoring Polynomials with Rational Coefficients, Springer Mathematische Annalen, Band 261, Seiten 515–534, 1982.

[Lenstra83] *H.W. Lenstra*, Integer Programming in a fixed Number of Variables, Mathematics of Operation Research, Band 8, Nr. 4 (November), Seiten 538–548, 1983.

[Lováz86] *L. Lovász*, An algorithmic Theory of Numbers, Graphs and Convexity, CBMS-NSF Regional Conference Series in Applied Mathematics, Band 50, SIAM Publications, Philadelphia, 1986

[LoSc92] *L. Lovász und H. Scarf*, The Generalized Basis Reduction Algorithm, Mathematics of Operation Research, Band 17, Nr. 3 (August), Seiten 751–764, 1992

[MaOd90] *J.E. Mazo und A.M. Odlyzko*, Lattice Points in high-dimensional Sphere, Monatsheft Mathematik, Band 110, Seiten 47–61, 1930.

[Mar03] *J. Martinet*, Perfect Lattices in Euclidean Spaces. Springer-Verlag 2003.

[Ma03] *A. May*, New RSA Vulnerabilities Using Lattice Reduction Methods. Dissertation Thesis, University of Paderborn, October 2003.

[ML01] *S. Mehrotra and Z. Li*, Reduction of Lattice Bases Using Modular Arithmetic. TR. Dept. of Industrial Engeneering and Management Sciences, Northwestern University, Evanston, Il. Oct 2001, mehrotra, zhifeng@iems.nwu.edu.

[MH78] *R.C. Merkle and M.E. Hellman*, Hiding Information and Signatures in Trapdoor Knapsacks, IEEE Trans. Inform. Theory, vol, IT-30, 594–601, 1984.

[MG02] *D. Micciancio and S. Goldwasser*, Complexity of Lattice Problems: A Cryptographic Perspective. Kluwer Academic Publishers, Boston, London, 2002.

[Mi1896] *H. Minkowski*, Geometrie der Zahlen, erste Auflage, Teubner-Verlag, Leipzig, 1896.

[Mi1911] *H. Minkowski*, Gesammelte Abhandlungen, Band I und II, Teubner-Verlag, Leipzig, 1911.

[Mis93] *B. Mishra*, Algorithmic Algebra, Texts and Monographs in Computer Science, Springer-Verlag, New-York, 1993.

[MB75] *M.A. Morrison and J. Brillhart*: *A Method of Factoring and the Factorization of* F_7, Mathematics of Computation **29**(129), pp. 183 –205, 1975.

[NS06] *P. Nguyen and D. Stehlé*, LLL on the average. In Proc. ANTS-VII, LNCS 4076, Springer-Verlag, Berlin New York, pp. 238–356, 2006.

[O90] *A. M. Odlyzko*, The rise and fall of knapsack cryptosystems. In Cryptology and Computational Number Theory, C. Pomerance ed., Proc. Symp. Appl. Math. **12** Amer. Math, Soc, Providence, 1990, 75–88,

[PS87] *A. Paz and C.P.Schnorr*, Approximating integer lattices by lattices with cyclic factor groups. Proceedings 14th International Colloquium on Automata, Languages and Programming (ICALP), LNCS 267, Springer-Verlag, Berlin New York, pp. 386–393, 1987.

[R89] *J.A. Rush*, A lower bound on packing spheres. Invent. math., **98**, pp. 499–509, 1989.

[Ri96] H. Ritter: Breaking Knapsack Cryptosystems by ℓ_∞-norm enumeration. Proceedings of 1st International Conference on the Theory and Applications of Cryptography–PragoCrypt '96, CTU Publishing House, Prag, Seiten 480–492, 1996.

[S87] *C.P.Schnorr*, A Hierarchy of polynomial time lattice basis reduction algorithms. Theoretical Computer Science, **53**, pp. 201–224, 1987.

[S93] *C.P.Schnorr*, Factoring integers and computing discrete logarithms via Diophantine approximation. In *Advances in Computational Complexity*, AMS, *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, **13**, pp. 171–182, 1993. Preliminary version in Proc. EUROCRYPT'91, LNCS 547, Springer-Verlag, Berlin New York, pp. 281–293, 1991. //www.mi.informatik.uni-frankfurt.de.

[S94] *C.P.Schnorr*, Block reduced lattice bases and successive minima. *Comb. Prob. and Comp.* **3**, pp. 507–522, 1994.

[SE94] *C.P. Schnorr and M. Euchner*, Lattce basis reduction: Improved practical algorithms and solving subset sum problems. Mathematical Programming **66**, pp. 181–199, 1994. Preliminary version in Proc. FCT'91, LNCS 591, Springer-Verlag, Berlin New York, pp. 68–85, 1991. //www.mi.informatik.uni-frankfurt.de.

[SH95] *C.P. Schnorr and H.H. Hörner*, Attacking the Chor–Rivest cryptosystem by improved lattice reduction. In Proc. EUROCRYPT'95, LNCS 921, Springer-Verlag, Berlin New York, pp. 1–12, 1995. //www.mi.informatik.uni-frankfurt.de.

[S03] *C.P. Schnorr*, Lattice reduction by sampling and birthday methods. Proc. STACS 2003: 20th Annual Symposium on Theoretical Aspects of Computer Science, LNCS 2007, Springer-Verlag, Berlin New York, pp. 146–156, 2003. //www.mi.informatik.uni-frankfurt.de

[S06] *C.P. Schnorr*, Fast LLL-type lattice reduction. Information and Computation, **204**, pp. 1–25, 2006. //www.mi.informatik.uni-frankfurt.de

[S07] *C.P. Schnorr*, Progress on LLL and lattice reduction, Proceedings LLL+25, Caen, France, June 29–July 1, 2007, Final version to appear by Springer-Verlag, 2009. //www.mi.informatik.uni-frankfurt.de

[S10] *C.P. Schnorr*, Average Time Fast SVP und CVP Algorithms for Low Density Lattices and the Factorization of Integers. Technical Report, University Frankfurt, Sepember 2010. //www.mi.informatik.uni-frankfurt.de

[SS12] *C.P. Schnorr und T. Shevchenko*, Solving Subset Sum Problems of Density close to 1 by randomized"BKZ-reduction. Cryptology ePrint Archiv: Report 2013/620,

[S13] *C.P. Schnorr*, Factoring integers by CVP Algorithms, Proceedings Number Theory and Cryptography, LNCS 8260, Springer-Verlag, Nov. 2013, pp. 73–93, this is an early version of the most recent version in //www.mi.informatik.uni-frankfurt.de/ Publications 2013

[Sc84] *A. Schönhage*, Factorization of Univariate Integer Polynomials by Diophantine Approximation and Improved Lattice Basis Reduction Algorithm. *Proc. 11-th Coll. Automata, Languages and Programming, Antwerpen 1984*, Lecture Notes in Comput. Sci., 172, Springer, New York, pp. 436–447, 1984.

[Schr86] *A. Schrijver*, Theory of Linear and Integer Programming, Wiley-Interscience Series in discrete Mathematics and Optimization, John Wiley & Son Ltd, 1986.

[Se93] *M. Seysen*, Simultaneous Reduction of a Lattice and its reciprocal Basis, Combinatorica, Band 13, Seiten 363–376, 1993.

[Si89] *C.L. Siegel*, Lectures on the Geometry of Numbers, Springer-Verlag, Berlin/Heidelberg, 1989.

[Sm1861] *H.J.S. Smith*, On Systems of linear indeterminate Equations and Congruences, Philosophical Transaction of the Royal Society of London, Band 151, Seiten 293–326, 1861.

[SS76] *E. Specker und V. Strassen*, Komplexität von Entscheidungsproblemem, Lecture Notes in Computer Science, Band 43, Springer-Verlag, Berlin/Heidelberg, 1976.

[St96] *A. Storjohann*, Faster Algorithms for Integer Lattice Basis Reduction.
TR 249, Swiss Federal Institute of Technology, ETH-Zurich, Department of Computer Science, Zurich, Switzerland, July 1996.
//www.inf.ethz.ch/research/publications/html.

[V82] *N.M. Vetchinkin*, 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, 1982.

[W66] *G.L. Watson*, 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, 1966.

[Ye91] *Y. Ye*, Potential Reduction Algorithm for Linear Programming, Mathematical Programming, Band 51, Seiten 239–258, 1991.