Gitter und LLL Basisreduktion

Vorlesung Kryptographie WS2007/8

F. Heß

7. Februar 2008

In diesem Text behandeln wir die theoretischen Grundlagen von Gittern und Algorithmen für Gitter im Hinblick auf die Kryptographie. Gitter finden darüberhinaus in vielen Bereichen der Mathematik, zum Beispiel der algebraischen Zahlentheorie, aber auch in der Physik, Chemie und Informationstheorie Anwendung (siehe zum Beispiel Conway und Sloane: „Sphere Packings, Lattices and Groups“, Springer 1988). Darauf gehen wir hier nicht weiter ein und versuchen darüberhinaus, die Darstellung möglichst kurz zu halten.

Gitter im $\mathbb{R}^n$

Im folgenden bezeichnet $\mathbb{R}^n$ den euklidischen $\mathbb{R}$-Vektorraum der Dimension n mit dem Skalarprodukt $\langle\cdot,\cdot\rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, $(b, b') \mapsto b^{tr}b'$. Dieses ist eine symmetrische, positiv definite Bilinearform. Aufgrund des Skalarprodukts haben wir auf $\mathbb{R}^n$ einen translationsinvarianten Volumenbegriff $\mathrm{vol}(\cdot)$ (also ein Haarsches Maß). Die euklidische Norm wird durch $||b|| = \langle b, b\rangle^{1/2}$ gegeben.

Für $\mathbb{R}$-linear unabhängige Vektoren $b_1, \ldots, b_m \in \mathbb{R}^n$ definieren wir das zugehörige Parallelotop $\Pi(b_1, \ldots, b_m) = \{\sum_i \lambda_i b_i \,|\, 0 \leq \lambda_i < 1\}$. Das Volumen des Parallelotops ist $\mathrm{vol}(\Pi(b_1, \ldots, b_m)) = |\det((\langle b_i, b_j\rangle)_{i,j})|^{1/2}$. Es gilt $\mathrm{vol}(\Pi(b_1, \ldots, b_m)) \leq ||b_1|| \cdot \cdots \cdot ||b_m||$ nach der Hadamard Schranke. Für $m = n$ ergibt sich auch $\mathrm{vol}(\Pi(b_1, \ldots, b_m)) = |\det((b_1, \ldots, b_n))|$.

1 Definition. Ein Gitter im $\mathbb{R}^n$ ist ein $\mathbb{Z}$-Untermodul von $\mathbb{R}^n$ von der Form

$$\Lambda = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_m$$

mit $\mathbb{R}$-linear unabhängigen Vektoren $b_i \in \mathbb{R}^n$. Die Dimension des Gitters ist m. Das Gitter Λ heißt vollständig, wenn $m = n$ ist. Das Parallelotop $\Pi(b_1, \ldots, b_m)$ nennt man auch ein Fundamentalparallelotop von Λ.

Der Rang von Λ ist auch gleich der Dimension des $\mathbb{R}$-Spanns $\mathbb{R}\Lambda = \{rx \,|\, r \in \mathbb{R},\, x \in \Lambda\}$. Die b_i bilden eine Basis von Λ. Durch beliebige unimodulare Transformation erhalten wir alle anderen Basen in der Form $b'_j = \sum_i u_{i,j} b_i$, wobei $U = (u_{i,j}) \in \mathbb{Z}^{m\times m}$ und $\det(U) = \pm 1$.

2 Beispiel. $\mathbb{Z}^n$ ist ein Gitter im $\mathbb{R}^n$. Eine Basis von $\mathbb{Z}^n$ ist durch die Einheitsvektoren gegeben. Man mache sich auch den Fall $n = 1$ klar.

Sind irgendwelche $\mathbb{R}$-linear unabhängigen Vektoren $b_1, \ldots, b_m$ aus $\mathbb{R}^n$ gegeben, so kann man das von ihnen erzeugte Gitter $\Lambda = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_m$ betrachten.

Seien $b_1 = 1$ und $b_2 = \sqrt{2}$. Wir definieren $\Lambda = \mathbb{Z}b_1 + \mathbb{Z}b_2$. Dann gilt $\Lambda \subseteq \mathbb{R}$ und Λ ist frei vom Rang 2, da b_1 und b_2 über $\mathbb{Z}$ linear unabhängig sind. Da b_1 und b_2 aber über $\mathbb{R}$ linear abhängig sind, ist Λ kein Gitter.

3 Lemma. *Es gilt* $\mathrm{vol}(\Pi(b_1, \ldots, b_m)) = \mathrm{vol}(\Pi(b'_1, \ldots, b'_m))$.

Beweis. Folgt aus $(\langle b'_i, b'_j\rangle)_{i,j} = U^{tr}(\langle b_i, b_j\rangle)_{i,j}U$, wenn U die unimodulare Transformationsmatrix der b'_i und b_i ist, der Multiplikativität von $\det(\cdot)$ und $|\det(U)| = 1$. □

4 Definition. Die Gitterdiskriminante $d(\Lambda)$ von Λ wird als

$$d(\Lambda) = \mathrm{vol}(\Pi(b_1, \ldots, b_m))$$

für eine Basis $b_1, \ldots, b_m$ von Λ definiert. Dies hängt nicht von der Wahl der Basis ab.

5 Lemma. *Es gilt* $d(\Lambda) \leq ||b_1|| \cdot \cdots \cdot ||b_m||$.

Beweis. Hadamard Ungleichung. □

6 Definition. Ein Teilgitter Λ' von Λ im $\mathbb{R}^n$ ist ein Gitter von $\mathbb{R}^n$ mit $\Lambda' \subseteq \Lambda$. Der Index von Λ' in Λ ist der Index abelscher Gruppen $(\Lambda : \Lambda_1)$.

7 Lemma. *Ist Λ' ein Teilgitter von Λ und haben Λ und Λ' den gleichen Rang, so gilt* $(\Lambda : \Lambda') = d(\Lambda')/d(\Lambda)$.

Beweis. Sei m der Rang von Λ. Sind b'_i eine Basis von Λ' und b_i eine Basis von Λ, so gibt es eine Matrix $T = (t_{i,j}) \in \mathbb{Z}^{m\times m}$ mit $b'_j = \sum_i t_{i,j} b_j$. Dann gilt wieder $(\langle b'_i, b'_j\rangle)_{i,j} = T^{tr}(\langle b_i, b_j\rangle)_{i,j}T$, und folglich $d(\Lambda')/d(\Lambda) = |\det(T)|$. Wir können ohne Einschränkung annehmen, daß T diagonal ist (Smith Normalform), da dies einer speziellen Wahl der b'_j und b_i entspricht. Dies zeigt $(\Lambda' : \Lambda) = |\det(T)| = d(\Lambda')/d(\Lambda)$. □

Diskretheit

Ein $\mathbb{Z}$-Modul Λ in $\mathbb{R}^n$ heißt diskret, wenn $\#\Lambda \cap C < \infty$ für alle beschränkten Mengen $C \subseteq \mathbb{R}^n$. Insbesondere besitzt jedes Element eines solchen Λ eine Umgebung im $\mathbb{R}^n$, in der kein weiteres Element von Λ liegt.

8 Satz. *Sei Λ ein $\mathbb{Z}$-Modul in $\mathbb{R}^n$. Dann ist Λ genau dann ein Gitter, wenn Λ diskret ist.*

Beweis. Sei Λ ein Gitter, und $b_1, \ldots, b_m$ eine Basis. Wir können diese zu einer Basis $b_1, \ldots, b_n$ von $\mathbb{R}^n$ ergänzen. Für eine beschränkte Menge C sind die Koordinaten der Elemente von C bezüglich dieser Basis ebenfalls beschränkt. Daher gibt es nur endlich viele ganzzahlige Koordinaten, und es folgt, daß Λ diskret ist.

Sei Λ diskret in $\mathbb{R}^n$. Sei $V = \mathbb{R}\Lambda$ und $m = \dim(V)$. Sei $a_1, \ldots, a_m$ eine in Λ gelegene Basis von V und $\Lambda_0 = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_m$. Wir zeigen, daß Λ_0 endlichen Index in Λ hat. Sei dazu $\{r_i \mid i \in I\} \subseteq \Lambda$ ein Repräsentantensystem von Λ/Λ_0. Wegen $V = \cup_{s \in \Lambda_0}(s + \Pi(a_1, \ldots, a_m))$ gibt es $s_i \in \Lambda_0$ und $t_i \in \Pi(a_1, \ldots, a_m)$ mit $r_i = s_i + t_i$ für alle $i \in I$. Es gilt aber auch $t_i = r_i - s_i \in \Lambda$ und $t_i \neq t_j$ für $i \neq j$, da sonst $r_i - r_j = s_j - s_i \in \Lambda_0$, was nach Annahme über die r_i nicht möglich ist. Wegen der Diskretheit von Λ kann es nur endliche viele t_i in der beschränkten Menge $\Pi(a_1, \ldots, a_m)$ geben. Also $\#I = (\Lambda : \Lambda_0) < \infty$. Mit $d = (\Lambda : \Lambda_0)$ gilt nun $d\Lambda \subseteq \Lambda_0$, also $\Lambda \subseteq (1/d)\Lambda_0 = \mathbb{Z}(a_1/d) + \cdots + \mathbb{Z}(a_m/d)$. Also ist Λ ein Untermodul eines freien Moduls über $\mathbb{Z}$ vom Rang m. Daher besitzt Λ eine Basis $b_1, \ldots, b_r$ mit $r \leq m$. Wegen $\mathbb{R}\Lambda = V$ folgt $r = m$ und die b_i sind $\mathbb{R}$-linear unabhängig. $\square$

Gitter mit anderen Skalarprodukten und quadratische Formen

Im vorigen Abschnitt haben wir Gitter Λ stets eingebettet in einen $\mathbb{R}^n$ betrachtet. Das Skalarprodukt auf $\mathbb{R}^n$ ergibt hierbei ein Skalarprodukt auf Λ. Eine andere, im wesentlichen äquivalente Definition von Gitter betrachtet diese Einbettung in $\mathbb{R}^n$ nicht, sondern benutzt nur ein vorgegebenes Skalarprodukt.

9 Definition. Ein Gitter ist ein freier $\mathbb{Z}$-Modul Λ vom Rang m zusammen mit einem Skalarprodukt $\langle \cdot, \cdot \rangle : \Lambda \times \Lambda \to \mathbb{R}$, so daß $A = (\langle b_i, b_j \rangle)_{i,j} \in \mathbb{R}^{m \times m}$ für eine Basis $b_1, \ldots, b_m$ von Λ positiv definit ist.

Wir schreiben auch $\langle \cdot, \cdot \rangle_\Lambda$, falls in einem Kontext Skalarprodukte verschiedener Gitter auftreten. Die Matrix $A = (\langle b_i, b_j \rangle)_{i,j}$ aus der Definition heißt

die Grammatrix von Λ bezüglich der b_i. Für $x = \sum_i \lambda_i b_i$ und $y = \sum_i \mu_i b_i$ gilt $\langle x, y\rangle = (\lambda_i)_i^{tr} A(\mu_i)_i$, wobei $(\lambda_i)_i, (\mu_i)_i$ als Spaltenvektoren aufgefaßt werden.

Wir zeigen im folgenden, daß diese Definition im wesentlichen das gleiche liefert wie die erste Definition. Darüberhinaus kann man zeigen, daß die positive Definitheit von A äquivalent zur Diskretheit von Λ ist.

10 Definition. Seien Λ_1, Λ_2 Gitter. Eine Isometrie $\phi : \Lambda_1 \to \Lambda_2$ ist ein $\mathbb{Z}$-Modulisomorphismus $\Lambda_1 \to \Lambda_2$ mit $\langle \phi(x), \phi(y)\rangle_{\Lambda_2} = \langle x, y\rangle_{\Lambda_1}$.

Zwei isometrische Gitter können als für gitterrelevante Fragen gleich angesehen werden. Jedoch werden Eigenschaften einer Einbettung (zum Beispiel in den $\mathbb{R}^n$ oder $\mathbb{Z}^n$) nicht erhalten.

Ist Λ_1 ein Gitter und A die Grammatrix zur Basis $b_1, \ldots, b_m$, so erhalten wir ein isometrisches Gitter Λ_2 durch $\Lambda_2 = \mathbb{Z}^n$ mit dem durch A definierten Skalarprodukt auf $\mathbb{Z}^n$.

11 Satz. *(Cholesky Zerlegung) Eine symmetrische, positiv definite Matrix $A \in \mathbb{R}^{m\times m}$ kann geschrieben werden als $A = B^{tr}B$, wobei $B \in \mathbb{R}^{m\times m}$ eine obere Dreiecksmatrix ist.*

Beweis. Siehe lineare Algebra oder Numerik, die Cholesky Zerlegung ist äquivalent zur Gram-Schmidt Orthonormalisierung: Sei $A = (a_{i,j})_{i,j}$. Wähle einen $\mathbb{R}$-Vektorraum V mit Basis $b_1, \ldots, b_m$ und definiere ein Skalarprodukt $\langle \cdot, \cdot\rangle$ auf V durch $\langle b_i, b_j\rangle = a_{i,j}$. Die Gram-Schmidt orthogonalisierten Vektoren b_j^* erfüllen $b_j^* = b_j - \sum_{i<j} \mu_{i,j} b_i^*$ und $\mu_{i,j} = \langle b_j, b_i^*\rangle / \langle b_i^*, b_i^*\rangle$. Mit $T = I_m + (\mu_{i,j})_{i<j}$ gilt also $(b_j)_j = (b_j^*)T$, und T ist eine obere Dreiecksmatrix in $\mathbb{R}^{m\times m}$. Da die b_j^* orthogonal sind, folgt, daß $(T^{-1})^{tr} A T^{-1} = \langle b_i^*, b_j^*\rangle$ diagonal mit positiven Einträgen ist. Indem man noch mit den Wurzeln, also den $||b_i^*||$, normalisiert, ergibt sich die Aussage: Schreibe $(T^{-1})^{tr} A T^{-1} = D^2$ mit einer Diagonalmatrix D. Durch Umstellen folgt $((DT)^{-1})^{tr} A (DT)^{-1} = I_m$, also leistet $B = DT$ das Gewünschte. □

12 Korollar. *Sei Λ ein Gitter mit Basis $b_1, \ldots, b_m$ und Grammatrix $A = B^{tr}B$, wobei B eine obere Dreiecksmatrix ist. Sei Λ' das vollständige Gitter im $\mathbb{R}^m$, welches von den Spalten B_i von B erzeugt wird. Sei $\phi : \Lambda \to \Lambda'$ der durch $\sum_i \lambda_i b_i \mapsto \sum_i \lambda_i B_i$ definierte $\mathbb{Z}$-Modulisomorphismus. Dann ist ϕ eine Isometrie.*

Beweis. Folgt aus $\langle b_i, b_j\rangle_\Lambda = a_{i,j} = B_i^{tr} B_j = \langle B_i, B_j\rangle_{\Lambda'}$. □

Das Korollar zeigt, daß beide Definitionen von Gitter im wesentlichen gleich sind. Man kann sich also ein Gitter in einen $\mathbb{R}^n$ eingebettet vorstellen, zusammen mit dem euklidischen Skalarprodukt auf $\mathbb{R}^n$, oder als $\mathbb{Z}^n$ mit einem

Skalarprodukt, welches durch eine positiv definite Grammatrix A gegeben wird.

Wir wollen schließlich noch auf einen weiteren Sprachgebrauch hinweisen. Eine quadratische Form in den Variablen $x_1, \ldots, x_n$ wird durch

$$Q(x_1, \ldots, x_n) = \sum_{1 \leq i < j \leq n} q_{i,j} x_i x_j$$

mit $q_{i,j} \in \mathbb{R}$ gegeben. Sie heißt positiv definit, wenn $Q(x_1, \ldots, x_n) \geq 0$ für alle $x_i \in \mathbb{R}$ und $Q(x_1, \ldots, x_n) = 0$ genau dann gilt, wenn alle $x_i = 0$ sind.

Sei $A \in \mathbb{R}^{n \times n}$ symmetrisch und positiv definit. Dann erhalten wir eine positiv definite quadratische Form durch $Q(x_1, \ldots, x_n) = (x_i)_i^{tr} A (x_i)_i$. Ist umgekehrt eine quadratische Form gegeben, so erhalten wir eine symmetrische, positiv definite Matrix A wie folgt: A hat die $q_{i,i}$ auf der Diagonalen und $q_{i,j}/2$ über der Diagonalen. Die Werte unter der Diagonalen sind per Symmetrie festgelegt. Man stellt leicht fest, daß diese Zuordnungen $A \mapsto Q(x_1, \ldots, x_n)$ und $Q(x_1, \ldots, x_n) \mapsto A$ invers zueinander sind. Dies zeigt auch, daß die Matrix A, die man aus $Q(x_1, \ldots, x_n)$ erhält, positiv definit ist.

Bezüglich dieser Zuordnungen sind ein Gitter Λ und eine ausgezeichnete Basis bis auf Isometrie „äquivalent“ zu einer quadratischen Form. Zwei quadratische Formen $Q_1(x_1, \ldots, x_n)$ und $Q_2(y_1, \ldots, y_n)$ heißen kongruent, wenn man die eine aus der anderen durch unimodulare Transformation der Variablen $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)T$ erhalten kann, wenn also $Q_1(\sum_i t_{i,1} y_i, \ldots, \sum_i t_{i,n} y_i) = Q_2(y_1, \cdots y_n)$ für $T = (t_{i,j})_{i,j}$ gilt. Dies entspricht einem Basiswechsel auf der Gitterseite.

Im allgemeinen ist es einfacher, mit Gittern an Stelle von quadratischen Formen zu arbeiten, da man bei Gittern auf geometrische Intuition zurückgreifen kann und keinen speziellen Bezug zu Basen haben muß. Die Betrachtung von Kongruenzklassen von quadratischen Formen käme der Betrachtung von Gittern gleich.

Auszählen von Gittervektoren

Sei Λ ein Gitter im $\mathbb{R}^n$ und $v \in \mathbb{R}^n$. Wir beschäftigen uns jetzt mit der Frage, wie alle Vektoren aus Λ eines vorgegebenen Höchstabstands von v berechnet werden können.

Ohne Einschränkung nehmen wir an, daß Λ vollständig ist. Ansonsten können wir nämlich statt v die orthogonale Projektion von v auf $\mathbb{R}\Lambda$ und eine Isometrie $\mathbb{R}\Lambda \to \mathbb{R}^m$ verwenden.

Sei $b_1, \ldots, b_n$ eine Basis von Λ (und von $\mathbb{R}^n$) und $b_1^*, \ldots, b_n^*$ die zugehörige Gram-Schmidt orthogonalisierte Basis von $\mathbb{R}^n$. Mit $\mu_{i,j} = \langle b_j, b_i^* \rangle / \langle b_i^*, b_i^* \rangle$ gilt

dann $b_j = b_j^* + \sum_{i<j} \mu_{i,j} b_i^*$.

Sei $d > 0$ der gewünschte Höchstabstand und $w \in \Lambda$ mit $||w - v||^2 \leq d$. Wir drücken $w = \sum_j \lambda_j b_j$ mit $\lambda_j \in \mathbb{Z}$ und v als Kombination der b_j^* aus, also

$$w = \sum_j \lambda_j (b_j^* + \sum_{i<j} \mu_{i,j} b_i^*) = \sum_i (\lambda_i + \sum_{i<j} \mu_{i,j} \lambda_j) b_i^*$$

und $v = \sum_i \gamma_i b_i^*$. Dann gilt unter Benutzung der Orthogonalität der b_i^*

$$\begin{aligned} ||w - v||^2 &= || \sum_i (\lambda_i - \gamma_i + \sum_{i<j} \mu_{i,j} \lambda_j) b_i^* ||^2 \\ &= \sum_i ||b_i^*||^2 (\lambda_i - \gamma_i + \sum_{i<j} \mu_{i,j} \lambda_j)^2 \leq d. \end{aligned}$$

Auf der rechten Seite steht eine Summe voller Quadrate. Man kann nun die Möglichkeiten für $\lambda_i \in \mathbb{Z}$ rekursiv aufzählen. Angenommen, wir haben eine Menge möglicher Lösungsvektoren $(\lambda_n, \lambda_{n-1}, \ldots, \lambda_{s+1})$ bereits bestimmt, dann erweitern wir diese zu möglichen Lösungsvektoren $(\lambda_n, \ldots, \lambda_s)$ durch Wahl von λ_s derart, daß

$$\sum_{i=s}^{n} ||b_i^*||^2 (\lambda_i - \gamma_i + \sum_{i<j} \mu_{i,j} \lambda_j)^2 \leq d$$

gilt. Es kann hierbei auch der Fall eintreten, daß es kein geeignetes λ_s gibt.

Auf diese Weise erhält man alle $w \in \Lambda$ mit $||w - v||^2 \leq d$. Man sieht so auch noch einmal, daß Λ diskret ist.

Es ist relativ klar, daß diese Prozedur im allgemeinen exponentiell in n ist, unabhängig davon, wieviel Lösungen im Endeffekt existieren. Im Prinzip durchläuft man einen Suchbaum, dessen Kanten mit den möglichen Werten von λ_s bezeichnet werden. Von der Wurzel gehen so viele Kanten ab, wie es Möglichkeiten für λ_n gibt. Von jeder dieser Kante gehen wiederum so viele Kanten ab, wie es Möglichkeiten für λ_{n-1} bei der jeweiligen Wahl von λ_n gibt, etc. Auf dem Weg zu den Blättern, also den Ecken nach den Kanten zu λ_1, kann es Sackgassen geben. Dies veranschaulicht: Es kann exponentiell viele Lösungen geben. Gibt es nur wenige Lösungen, so kann es exponentiell viele Sackgassen geben, und das Aufsuchen der Lösungen benötigt exponentiellen Aufwand.

Besonders viele Sackgassen treten auf, wenn die Ausgangsbasis b_i „wenig orthogonal“ ist. Dies stellt die Frage, wie man möglichst orthogonale Basen im Gitter finden kann und führt auf die Gitterbasenreduktion. Dazu kommen wir später.

Kürzeste Gittervektoren

Sei Λ ein Gitter im $\mathbb{R}^n$. Beschränkte Kugeln um den Ursprung enthalten nur endlich viele Gittervektoren. Daher gibt es in Λ ein Element kleinster Norm ungleich Null. Dieses heißt ein kürzester Vektor von Λ. Die Norm ist eine Invariante von Λ und wird mit $\lambda_1(\Lambda)$ bezeichnet. Zum Beispiel sind die Einheitsvektoren kürzeste Vektoren von $\mathbb{Z}^n$ und $\lambda_1(\mathbb{Z}^n) = 1$.

Üblicherweise ist man an oberen Schranken für die Norm kürzester Vektoren interessiert, und an Verfahren, einen oder alle kürzeste Vektoren möglichst effizient zu bestimmen. Das Problem, kürzeste Vektoren zu berechnen, wird mit SVP (Shortest Vector Problem) abgekürzt. Die Auszählmethode des vorigen Abschnitts ist im allgemeinen exponentiell in der Dimension. Es stellt sich in der Tat heraus, daß das SVP NP-hart ist, so daß es vermutlich keinen Polynomzeitalgorithmus hierfür gibt. Es gibt Kryptosysteme, welche auf dem SVP basieren.

13 Satz. *(Blichfeldt) Sei Λ ein vollständiges Gitter im $\mathbb{R}^n$ und $S \subseteq \mathbb{R}^n$ eine Menge. Gilt $\mathrm{vol}(S) > d(\Lambda)$, oder $\mathrm{vol}(S) = d(\Lambda)$ und S ist kompakt, dann gibt es $z_1, z_2 \in S$ mit $z_1 \neq z_2$ und $z_1 - z_2 \in \Lambda$.*

Beweis. Sei Π ein Fundamentalparallelotop von Λ. Wir definieren $S_x = S \cap (x + \Pi)$ für $x \in \Lambda$. Da Λ vollständig ist, gilt $S = \cup_{x\in\Lambda} S_x$, und diese Vereiningung ist disjunkt. Daher gilt auch $\mathrm{vol}(S) = \sum_{x\in\Lambda} \mathrm{vol}(S_x)$. Weiter haben wir $\mathrm{vol}(S_x) = \mathrm{vol}(S_x - x)$ und $S_x - x \subseteq \Pi$. Unter der ersten Annahme erhalten wir

$$\mathrm{vol}(\Pi) < \mathrm{vol}(S) = \sum_{x\in\Lambda} \mathrm{vol}(S_x - x).$$

Wären die $S_x - x$ alle disjunkt, so ergäbe sich wegen $\sum_{x\in\Lambda} \mathrm{vol}(S_x - x) \leq \mathrm{vol}(\Pi)$ ein Widerspruch. Daher gibt es $x_1, x_2 \in \Lambda$, $x_1 \neq x_2$ mit $(S_{x_1} - x_1) \cap (S_{x_2} - x_2) \neq \emptyset$. Sei $z \in (S_{x_1} - x_1) \cap (S_{x_2} - x_2)$. Wir definieren $z_1 = x_1 + z$ und $z_2 = x_2 + z$. Dann gilt $z_1, z_2 \in S$, $z_1 \neq z_2$ und $z_1 - z_2 = x_1 - x_2 \in \Lambda$.

Der Beweis unter der zweiten Annahme an S ist eine Übungsaufgabe.

□

Eine Menge $S \subseteq \mathbb{R}^n$ heißt zentralsymmetrisch, wenn $S = -S$ gilt. Eine Menge S heißt konvex, wenn für alle $x, y \in S$ die Strecke $\{\lambda x + (1-\lambda)y \mid 0 \leq \lambda \leq 1\}$ in S enthalten ist.

14 Satz. *(Minkowskischer Gitterpunktsatz) Sei Λ ein vollständiges Gitter im $\mathbb{R}^n$ und $S \subseteq \mathbb{R}^n$ eine Menge. Ist S zentralsymmetrisch und konvex mit $\mathrm{vol}(S) > 2^n d(\Lambda)$, oder ist $\mathrm{vol}(S) = 2^n d(\Lambda)$ und S kompakt, dann gibt es mindestens ein $x \in \Lambda \cap S$ mit $x \neq 0$.*

n	1	2	3	4	5	6	7	8
γ_n^n	1	4/3	2	4	8	64/3	64	256

Tabelle 1: Hermite Konstanten

Beweis. Wir wenden Blichfeldt auf $S/2$ an. Dies ist möglich, da wir aufgrund der Annahmen $\mathrm{vol}(S/2) = 2^{-n}\mathrm{vol}(S) > d(\Lambda)$, oder $\mathrm{vol}(S/2) = d(\Lambda)$ und $S/2$ kompakt haben. Dann gibt es $z_1, z_2 \in S/2$ mit $z_1 - z_2 \in \Lambda\backslash\{0\}$. Da S zentralsymmetrisch und konvex ist, folgt $z_1 - z_2 = (2z_1 + (-2z_2))/2 \in S$. Also leistet $x = z_1 - z_2$ das Gewünschte. □

15 Korollar. *Sei Λ ein vollständiges Gitter im $\mathbb{R}^n$. Dann gibt es ein $x \in \Lambda\backslash\{0\}$ mit*

$$||x|| \leq n^{1/2} d(\Lambda)^{1/n}.$$

Beweis. Der Würfel $S = [-d(\Lambda)^{1/n}, d(\Lambda)^{1/n}]^n$ im $\mathbb{R}^n$ hat Volumen $\mathrm{vol}(S) = 2^n d(\Lambda)$. Nach dem Satz gibt es also ein $x \in \Lambda \cap S$ mit $x \neq 0$. Dann gilt $||x||^2 \leq n d(\Lambda)^{2/n}$. □

Der Minkowskische Gitterpunktsatz gilt für alle zentralsymmetrischen, konvexen Teilmengen S. Es sei bemerkt, daß man mit spezielleren Argumenten für Kugeln um den Ursprung eine bessere Schranke für die Norm eines kürzesten Vektors erhalten kann. Der Minkowskische Gitterpunktsatz ergibt kein konstruktives Verfahren zur Bestimmung kürzester Vektoren.

16 Definition. Die Hermite Konstante γ_n ist

$$\gamma_n = \sup\{(\lambda_1(\Lambda)/d(\Lambda)^{1/n})^2 \mid \Lambda \text{ vollständiges Gitter im } \mathbb{R}^n\}.$$

Das Quadrat in der Definition ist eigentlich nur Konvention. Ob man quadriert oder nicht hängt davon ab, ob man lieber Normenquadrate oder nur Normen betrachtet. Wir benutzen hier vornehmlich nur Normen, aber γ_n wird traditionell für Normenquadrate definiert.

Mit der Definition gilt also

$$\lambda_1(\Lambda) \leq \gamma_n^{1/2} d(\Lambda)^{1/n}. \tag{17}$$

Anhand von $\mathbb{Z}^n$ und Korollar 15 ersehen wir $1 \leq \gamma_n \leq n$. Tabelle 1 enthält die Werte von γ_n^n bis $n = 8$. Die genauen Werte für $n \geq 9$ sind meines Wissens unbekannt. Für alle n gilt

$$(1/\pi)^n \Gamma(1 + n/2)^2 \leq \gamma_n^n \leq (2/\pi)^n \Gamma(2 + n/2)^2,$$

wobei Γ die Gammafunktion bezeichnet, und asymptotisch für $n \to \infty$

$$1/(2\pi e) + o(1) \leq \gamma_n/n \leq 1.744/(2\pi e) + o(1).$$

Das folgende Lemma gibt eine untere Schranke für die Norm kürzester Vektoren an, welche in Berechnungen hilfreich sein kann.

18 Lemma. *Für jede Basis $b_1, \ldots, b_m$ des Gitters Λ im $\mathbb{R}^n$ und die zugehörige Gram-Schmidt orthogonalisierte Basis $b_1^*, \ldots, b_m^*$ von $\mathbb{R}\Lambda$ und jedes $x \in \Lambda \backslash \{0\}$ gilt $||x|| \geq \min_i ||b_i^*||$.*

Beweis. Beweisen wir in Lemma 24 in allgemeinerer Form. □

Die Abschätzung wird besser, wenn man reduzierte Basen $b_1, \ldots, b_m$ betrachtet. Siehe später.

Sukzessive Minima

Im allgemeinen sind wir an Basen eines Gitters Λ interessiert, welches aus möglichst kurzen Vektoren besteht. Dies ist gleichbedeutend damit, daß die Vektoren möglichst orthogonal sind. Man kann auch sagen, daß die Basisvektoren „wenigstens grob“ die im folgenden definierten sukzessiven Minima realisieren sollten. Anstelle von Gitterbasen betrachten wir zunächst nur möglichst kurze, linear unabhängige Vektoren.

19 Definition. Sei Λ ein Gitter im $\mathbb{R}^n$ der Dimension m. Für $1 \leq i \leq m$ werden die sukzessiven Minima $\lambda_i(\Lambda)$ wie folgt definiert:

$$\lambda_i(\Lambda) = \inf \left\{ \max_{1 \leq j \leq i} ||v_j|| \,|\, v_1, \ldots, v_i \in \Lambda \text{ linear unabhängig} \right\}.$$

Dies ist eine Erweiterung der bisherigen Definition von $\lambda_1(\Lambda)$. Es gilt $\lambda_1(\Lambda) \leq \lambda_2(\Lambda) \leq \cdots \leq \lambda_m(\Lambda)$. Aufgrund der Diskretheit von Λ gibt es also für jedes i Vektoren $v_1, \ldots, v_i \in \Lambda$ mit $\lambda_i(\Lambda) = \max_{1 \leq j \leq i} ||v_j||$. Es läßt sich sogar zeigen, daß es Vektoren $v_1, \ldots, v_n \in \Lambda$ mit $\lambda_i(\Lambda) = ||v_i||$ gibt. Man sagt dann, daß die v_i die sukzessiven Minima realisieren.

20 Lemma. *(i) Seien $v_1, \ldots, v_j \in \Lambda$ linear unabhängig mit $||v_i|| = \lambda_i(\Lambda)$ für $1 \leq i \leq j-1$. Dann gilt $||v_j|| \geq \lambda_j(\Lambda)$.*

(ii) Es gibt linear unabhängige Vektoren $v_1, \ldots, v_m \in \Lambda$, welche die sukzessiven Minima realisieren, also mit $\lambda_i(\Lambda) = ||v_i||$ für $1 \leq i \leq m$.

Beweis. (i): Wir nehmen $||v_j|| < \lambda_j(\Lambda)$ an. Sei $1 \leq r \leq j$ minimal mit $||v_j|| < \lambda_r(\Lambda)$. Dann gilt $||v_j|| \geq \lambda_i(\Lambda) = ||v_i||$ für $1 \leq i \leq r-1$ und $\max\{||v_1||, \ldots, ||v_{r-1}||, ||v_j||\} < \lambda_r(\Lambda)$, was nicht möglich ist, da die $v_1, \ldots, v_{r-1}, v_j$ linear unabhängig sind. Also muß $||v_j|| \geq \lambda_j(\Lambda)$ gelten.

(ii): Per Induktion. Seien $v_1, \ldots, v_{j-1} \in \Lambda$ linear unabhängig mit $\lambda_i(\Lambda) = ||v_i||$ für $1 \leq i \leq j-1$. Seien $w_1, \ldots, w_j \in \Lambda$ linear unabhängig mit $\lambda_j(\Lambda) = \max_i ||w_i||$. Dann ist eines der w_i aus Dimensionsgründen linear unabhängig von $v_1, \ldots, v_{j-1}$. Durch Hinzunahme dieses w_i erhalten wir v_j mit $||v_j|| \leq \lambda_j(\Lambda)$. Hier gilt wegen (i) Gleichheit. □

Manchmal werden die sukzessiven Minima über die Normquadrate definiert, das ist aber nur eine Normierungsfrage.

21 Beispiel. Seien $b_i = e_i$ (die Einheitsvektoren) für $1 \leq i \leq 4$ und $b_5 = (1/2)\sum_{i=1}^{5} e_i$ in $\mathbb{R}^5$. Wir betrachten das von den $b_1, \ldots, b_5$ aufgespannte, vollständige Gitter Λ im $\mathbb{R}^5$. Es gilt $\lambda_i(\Lambda) = 1$ für $1 \leq i \leq 5$, wie man an $b_1, \ldots, b_4, 2b_5 - \sum_{i=1}^{4} b_i$ sehen kann. Es gibt jedoch keine Basis von Λ, welche die sukzessiven Minima realisiert. Eine solche Basis müßte nämlich einen Vektor enthalten, dessen Koordinaten sämtlich ungleich Null sind und Nenner 2 haben. Solche Vektoren haben aber Norm $\geq \sqrt{5/4} > 1$. Grund: Die Basisvektoren sind Linearkombinationen von $b_1, \ldots, b_5$, und bei mindestens einem Basisvektor müßte der Koeffizient von b_5 ungerade sein (sonst hätte die zugehörige Basistransformationsmatrix durch 2 teilbare Determinante und wäre nicht unimodular).

Das Beispiel zeigt, daß es im allgemeinen keine Basis bestehend aus linear unabhängigen, kürzesten Vektoren geben kann.

22 Satz. *Sei Λ ein m-dimensionales Gitter im $\mathbb{R}^n$.*

- (i) *Realisieren $b_1, \ldots, b_r$ die ersten r sukzessiven Minima und gilt $r \leq 3$, so lassen sich $b_1, \ldots, b_r$ zu einer Basis von Λ ergänzen.*
- (ii) *Λ besitzt stets eine Basis $b_1, \ldots, b_m$ mit $||b_j|| = \lambda_j(\Lambda)$ für $1 \leq j \leq \min\{m, 4\}$.*

Beweis. Lassen wir aus (siehe zum Beispiel Pohst und Zassenhaus, „Algorithmic Algebraic Number Theory“, S. 196). □

23 Satz. *Sei Λ ein m-dimensionales Gitter im $\mathbb{R}^n$. Dann gilt*

$$d(\Lambda) \leq \prod_{i=1}^{m} \lambda_i(\Lambda) \leq \gamma_m^{m/2} d(\Lambda).$$

Beweis. Seien $v_1, \dots v_m$ linear unabhängige Vektoren, welche die sukzessiven Minima realisieren.

Die untere Schranke ergibt sich wie folgt. Sei $\Lambda' \subseteq \Lambda$ das von den v_i erzeugte Teilgitter. Dann gilt $d(\Lambda) \leq d(\Lambda') \leq \prod_i ||v_i|| = \prod_i \lambda_i(\Lambda)$, weil Λ' ein Teilgitter ist und wegen der Hadamard Ungleichung.

Die obere Schranke ergibt sich wie folgt. Sei $b_1, \dots, b_m$ eine Basis von Λ derart, daß $(v_1, \dots, v_m) = (b_1, \dots, b_m)T$ mit einer oberen Dreiecksmatrix $T \in \mathbb{Z}^{m \times m}$. Solche b_i existieren, da wir T zeilenweise in Hermite Normalform bringen können und dies einem Basiswechsel entspricht. Für $x \in \Lambda$ folgt aus $x \notin \mathbb{Z}b_1 + \dots + \mathbb{Z}b_{s-1}$ dann $x \notin \mathbb{R}v_1 + \dots + \mathbb{R}v_{s-1}$, also $v_1, \dots, v_{s-1}, x$ linear unabhängig und daher $||x|| \geq \lambda_s(\Lambda)$ nach Lemma 20, (i).

Sei $b_1^*, \dots, b_m^*$ die Gram-Schmidt Orthogonalisierung mit $b_j = \sum_{i=1}^j \mu_{i,j} b_i^*$ mit $\mu_{i,i} = 1$. Sei ferner $b_j' = \sum_{i=1}^j \mu_{i,j} b_i^* / \lambda_i(\Lambda)$ und Λ' das von den b_j' erzeugte Gitter. Da $\det((\mu_{i,j})_{i,j}) = 1$ folgt $d(\Lambda') = d(\Lambda) \prod_{i=1}^m \lambda_i(\Lambda)^{-1}$. Wir zeigen jetzt $\lambda_1(\Lambda') \geq 1$. Sei dazu $x \in \Lambda'$ mit $x = \sum_{j=1}^m x_j b_j' \neq 0$ beliebig. Sei $s \geq 1$ der größte Index mit $x_s \neq 0$ und $x_j = 0$ für alle $j > s$. Dann gilt

$$\begin{aligned} ||x||^2 &= ||\sum_{j=1}^s x_j b_j'||^2 = ||\sum_{j=1}^s \sum_{i=1}^j x_j \mu_{i,j} b_i^* / \lambda_i(\Lambda)||^2 \\ &\geq \lambda_s(\Lambda)^{-2} ||\sum_{j=1}^s \sum_{i=1}^j x_j \mu_{i,j} b_i^*||^2 = \lambda_s(\Lambda)^{-2} ||\sum_{j=1}^s x_j b_j||^2 \geq 1, \end{aligned}$$

wobei die erste Ungleichung die Orthogonalität der b_j^* benutzt und die letzte Ungleichung aus obigen Bemerkungen und $x_s \neq 0$ folgt. Damit ist $\lambda_1(\Lambda') \geq 1$ gezeigt. Nach (17) angewendet auf Λ' erhalten wir

$$1 \leq \lambda_1(\Lambda')^m \leq \gamma_m^{m/2} d(\Lambda') = \gamma_m^{m/2} d(\Lambda) \prod_{i=1}^m \lambda_i(\Lambda)^{-1},$$

woraus die Behauptung folgt. □

Für die sukzessiven Minima erhalten wir eine analoge Abschätzung von unten wie für die Norm eines kürzesten Vektors.

24 Lemma. *Für jede Basis $b_1, \dots, b_m$ des Gitters Λ im $\mathbb{R}^n$ und die zugehörige Gram-Schmidt orthogonalisierte Basis $b_1^*, \dots, b_m^*$ von $\mathbb{R}\Lambda$ gilt*

$$\lambda_j(\Lambda) \geq \min_{j \leq i \leq m} ||b_i^*||.$$

Beweis. Seien $v_1, \dots, v_m \in \Lambda$ linear unabhängig mit $||v_j|| = \lambda_j(\Lambda)$. Seien $\mu_{i,j} \in \mathbb{R}$ mit $b_i = \sum_{j=1}^i \mu_{i,j} b_j^*$. Wir wissen $\mu_{i,i} = 1$. Seien $\lambda_{k,j} \in \mathbb{Z}$, $\lambda_{k,j}^* \in \mathbb{R}$ mit $v_k = \sum_{j=1}^m \lambda_{k,j} b_j = \sum_{j=1}^m \lambda_{k,j}^* b_j^*$ für $1 \leq k \leq m$. Sei $s_k = \max\{j \mid \lambda_{k,j} \neq 0\}$.

Es gilt $v_k = \sum_{i=1}^m \lambda_{k,i} b_i = \sum_{i=1}^m \lambda_{k,i} \sum_{j=1}^i \mu_{i,j} b_j^* = \sum_{j=1}^m (\sum_{i=j}^m \lambda_{k,i}\mu_{i,j}) b_j^*$, daher $\lambda_{k,j}^* = \sum_{i=j}^m \lambda_{k,i}\mu_{i,j}$. Wegen $\mu_{i,i} = 1$ gilt $\lambda_{k,s_k}^* = \lambda_{k,s_k}$ nach Definition von s_k und daher $\lambda_{k,s_k}^* \in \mathbb{Z}\backslash\{0\}$. Zu jedem j gibt es wegen der linearen Unabhängigkeit der $v_1, \ldots, v_j$ ein $k \leq j$ mit $s_k \geq j$, denn sonst wären die $v_1, \ldots, v_j$ im Spann der $b_1, \ldots, b_{j-1}$. Für ein solches k folgt aus $j \geq k$, $s_k \geq j$ und $\lambda_{k,s_k}^* \in \mathbb{Z}\backslash\{0\}$:

$$\lambda_j(\Lambda)^2 \;\geq\; \lambda_k(\Lambda)^2 \;\geq\; ||v_k||^2 \;\geq\; \lambda_{k,s_k}^2 ||b_{s_k}^*||^2 \;\geq\; ||b_{s_k}^*||^2 \;\geq\; \min_{j \leq i \leq m} ||b_i^*||^2.$$

□

Die Abschätzung wird besser, wenn man reduzierte Basen $b_1, \ldots, b_m$ betrachtet. Siehe die folgenden Abschnitte.

Basisreduktion

Wir kommen nun zu der angekündigten Basisreduktion. Basisreduktion bedeutet, daß man zu einer vorgelegten Basis eines Gitters eine neue Basis mit kürzeren bzw. möglichst orthogonalen Vektoren mittels eines Algorithmus bestimmt. Solche Basen nennt man dann reduziert. Speziell gibt es eine ganze Reihe von Reduziertheitsbegriffen. Je nach „Qualität“ der Reduziertheit benötigen die zugehörigen Reduktionsverfahren in der Dimension polynomielle oder exponentielle Laufzeit.

Im folgenden bezeichnet Λ ein Gitter im $\mathbb{R}^n$ der Dimension m. Wir betrachten Vektoren $v_1, \ldots, v_r \in \Lambda$ und bezeichnen die zugehörigen Gram-Schmidt orthogonalisierten Vektoren mit $v_1^*, \ldots, v_r^*$. Diese liegen in $\mathbb{R}\Lambda$. Sollten einige der v_j^* Null sein, so verwenden wir diese im Gram-Schmidt Orthogonalisierungsprozeß nicht weiter. Die zugehörige Gram-Schmidt Transformationsmatrix mit $(v_1, \ldots, v_r) = (v_1^*, \ldots, v_r^*)T$ ist dann $T = (\mu_{i,j})_{i,j}$ mit

$$\mu_{i,j} = \begin{cases} 0 & \text{für } 1 \leq j < i \leq r, \\ 1 & \text{für } 1 \leq i = j \leq r, \\ \langle v_j, v_i^* \rangle / \langle v_i^*, v_i^* \rangle & \text{für } 1 \leq i < j \leq r \text{ und } v_i^* \neq 0, \\ 0 & \text{für } 1 \leq i < j \leq r \text{ und } v_i^* = 0. \end{cases}$$

Die Gram-Schmidt Transformationsmatrix ist also eine obere Dreicksmatrix mit Einsen auf der Diagonalen. Die $v_1^*, \ldots, v_r^*$ sind orthogonal und v_j^* hängt nur vom Unterraum $\mathbb{R}v_1 + \cdots + \mathbb{R}v_{j-1}$ und der Nebenklasse $v_j + \mathbb{R}v_1 + \cdots + \mathbb{R}v_{j-1}$ ab.

Längenreduktion

25 Definition. Die Vektoren $v_1, \ldots, v_r \in \Lambda$ heißen längenreduziert, wenn die Gram-Schmidt-Transformationsmatrix T oberhalb der Diagonalen Einträge $> -1/2$ und $\leq 1/2$ hat.

Zur Berechnung längenreduzierter Vektoren aus gegebenen $v_1, \ldots, v_r$ mittels unimodularer Transformation geht man ähnlich wie gegen Ende einer Hermite Normalformberechnung vor, reduziert die Einträge rechts von der Diagonalen in T modulo 1 und führt die entsprechenden unimodularen Spaltenoperationen auf $(v_1, \ldots, v_r)$ aus. Man muß allerdings etwas aufpassen, da die v_j^* von den v_j abhängen und eine Transformation der v_j im allgemeinen auch eine Transformation der v_j^* bewirkt. Daher arbeiten wir von links nach rechts in T und addieren entsprechend nur Vielfache von v_i zu v_j für $i < j$.

26 Algorithmus. *(Längenreduktion)*

Eingabe: *Vektoren* $v_1, \ldots, v_r \in \Lambda$.

Ausgabe: *Längenreduzierte Vektoren* $w_1, \ldots, w_r \in \Lambda$ *und die unimodulare Transformationsmatrix* $U \in \mathbb{Z}^{r \times r}$ *mit* $(w_1, \ldots, w_r) = (v_1, \ldots, v_r)U$.

1. *Setze* $U = I_r$.
2. *Führe die Schritte 3 bis 7 für* $j = 1, \ldots, r$ *aus.*
3. *Berechne* $\mu_{i,j} := \langle v_j, v_i^* \rangle / ||v_i^*||^2$ *für* $1 \leq i \leq j-1$. *Für* $v_i^* = 0$ *sei* $\mu_{i,j} := \delta_{i,j}$ *(Kronecker Delta).*
4. *Berechne* $v_j^* := v_j - \sum_{i=1}^{j-1} \mu_{i,j} v_i^*$.
5. *Führe die Schritte 6 und 7 für* $i = j-1, \ldots, 1$ *aus.*
6. *Berechne* $v_j := v_j - \lceil \mu_{i,j} \rfloor v_i$, $\mu_{k,j} := \mu_{k,j} - \lceil \mu_{i,j} \rfloor \mu_{k,i}$ *für* $1 \leq k \leq i$.
7. *Subtrahiere das* $\lceil \mu_{i,j} \rfloor$*-fache der* i*-ten Spalte von* U *von der* j*-ten Spalte von* U.
8. *Ausgabe von* $v_1, \ldots, v_r$ *und* U.

Im Algorithmus wird mit $\lceil x \rfloor$ diejenige ganze Zahl bezeichnet, für die $-1/2 < x - \lceil x \rfloor \leq 1/2$ gilt. Wir nennen die von Algorithmus 26 berechneten Vektoren $w_1, \ldots, w_r$ die längenreduzierten Vektoren der $v_1, \ldots, v_r$.

Der Spann der $w_1, \ldots, w_j$ ist also gleich dem Spann der $v_1, \ldots, v_j$ für $0 \leq j \leq r$. Aus der obigen Bemerkung über die Abhängigkeit der v_j^* von den

v_j ersehen wir daher $w_j^* = v_j^*$. Die Gram-Schmidt-Transformationsmatrix der w_j ensteht folglich aus der Gram-Schmidt-Transformationsmatrix der v_j durch dieselben Spaltentransformationen U wie die w_j aus den v_j und hat daher tatsächlich Koeffizienten oberhalb der Diagonalen $> 1/2$ und $\leq 1/2$, so daß die w_j längenreduziert sind.

Paarreduktion

Die Idee bei der Paarreduktion ist leicht erklärt. Die Vektoren $v_1, \ldots, v_r \in \Lambda$ heißen paarweise reduziert, wenn kein v_i durch Addition eines geeigneten ganzzahligen Vielfachen eines v_j mit $j \neq i$ kürzer gemacht werden kann. Entsprechend ergibt sich der Reduktionsalgorithmus zur Paarreduktion.

27 Definition. Sei $0 < \delta \leq 1$. Die Vektoren $v_1, \ldots, v_r \in \Lambda$ heißen paarweise reduziert für δ, wenn $\delta||v_i|| \leq \min_{\lambda \in \mathbb{Z}} ||v_i + \lambda v_j||$ für $1 \leq i, j \leq r$ und $i \neq j$ gilt.

Es ist günstig, sich das folgende Lemma geometrisch zu verdeutlichen.

28 Lemma. *Seien $v, w \in \Lambda$. Dann sind äquivalent:*

(i) $||v|| = \min_{\lambda \in \mathbb{Z}} ||v + \lambda w||$,

(ii) $||v|| \leq ||v \pm w||$,

(iii) $2|\langle v, w\rangle| \leq ||w||^2$.

Für $||w|| \neq 0$ und $\mu = \lceil \langle v, w\rangle / ||w||^2 \rfloor$ gilt $||v - \mu w|| = \min_{\lambda \in \mathbb{Z}} ||v + \lambda w||$.

Beweis. $(i) \Rightarrow (ii)$. Klar. $(ii) \Rightarrow (iii)$: Es gilt $||v||^2 \leq ||v \pm w||^2 = \langle v \pm w, v \pm w\rangle = ||v||^2 \pm 2\langle v, w\rangle + ||w||^2$, also $\pm 2\langle v, w\rangle + ||w||^2 \geq 0$. $(iii) \Rightarrow (i)$: Es gilt $||v + \lambda w||^2 \geq ||v||^2 + 2\lambda\langle v, w\rangle + \lambda^2 ||w||^2 \geq ||v||^2$, da $\lambda \in \mathbb{Z}$.

Die zweite Aussage folgt unter Benutzung von $(iii) \Leftrightarrow (i)$ aus $|\langle v - \mu w, w\rangle| / ||w||^2 = |\langle v, w\rangle / ||w||^2 - \mu| \leq 1/2$. □

Ein einfacher Algorithmus zur paarweisen Reduktion liegt damit auf der Hand. Man überprüft mit Hilfe von Lemma 28 paarweise $\delta||v_i|| \leq \min_{\lambda \in \mathbb{Z}} ||v_i + \lambda v_j||$. Gilt dies nicht, ersetzt man v_i durch $v_i - \mu v_j$ und fängt wieder von vorne an.

Das Verfahren ist endlich, da in jedem Schritt v_i durch ein echt kürzeres v_i ersetzt wird und Λ diskret ist. Innerhalb eines Balls gibt es nämlich nur endlich viele Vektoren, daher nur endlich viele Möglichkeiten für $v_1, \ldots, v_r$, aber in jedem Schritt der Paarreduktion wird eine von den bisherigen Kombinationen verschiedene, neue Kombination $v_1, \ldots, v_r$ erzeugt. Es ergibt sich der folgende Satz.

29 Satz. *Sei $0 < \delta \leq 1$. Aus den Vektoren $v_1, \ldots, v_r \in \Lambda$ kann man durch unimodulare Transformation Vektoren $w_1, \ldots, w_r \in \Lambda$ erhalten, welche paarweise reduziert für δ sind.*

Für $\delta < 1$ und Basen $v_1, \ldots, v_m$ von Λ ist das Verfahren im allgemeinen polynomiell in m. Nach der Hadamard Schranke muß nach t Schritten nämlich $d(\Lambda) < \delta^t \prod_{i=1}^m ||v_i||$ gelten. Dies liefert eine obere Schranke für t, welche linear von m, $\log(d(\Lambda))$ und $\log(\max_i ||v_i||)$ abhängt.

Gaußreduktion

Die Gaußreduktion beschäftigt sich mit den speziellen Verhältnissen bei der Paarreduktion für $r = 2$, also für zweidimensionale Gitter Λ. Wir wollen hier nicht im Detail darauf eingehen. Von Interesse ist für uns nur der folgende Satz.

30 Satz. *Sei $v_1, v_2 \in \Lambda$ mit $||v_1|| \leq ||v_2||$. Dann sind äquivalent:*

(i) *v_1, v_2 sind eine paarweise reduzierte Basis von Λ für $\delta = 1$.*

(ii) *v_1, v_2 oder $v_1, -v_2$ ist eine längenreduzierte Basis von Λ.*

(iii) *v_1, v_2 realisieren die sukzessiven Minima.*

Beweis. *(i)* $\Rightarrow$ *(iii)*: Seien v_1, v_2 paarweise reduziert und $||v_1|| \leq ||v_2||$. Nach Lemma 28 gilt $2|\langle v_1, v_2\rangle| \leq ||v_1||^2$ und für $s, r \in \mathbb{Z}$ weiter

$$\begin{aligned} ||sv_1 + rv_2||^2 &= s^2||v_1||^2 + r^2||v_2||^2 + 2sr\langle v_1, v_2\rangle \\ &\geq s^2||v_1||^2 + r^2||v_2||^2 - sr||v_1||^2 \\ &\geq \begin{cases} ||v_1||^2 & \text{für } sr \neq 0, \\ ||v_2||^2 & \text{für } r \neq 0. \end{cases} \end{aligned}$$

durch Fallunterscheidung. Daraus folgt $||v_1|| = \lambda_1(\Lambda)$ und $||v_2|| = \lambda_2(\Lambda)$.

(iii) $\Rightarrow$ *(ii)*: Wenn v_1, v_2 die sukzessiven Minima realisieren, dann müssen v_1, v_2 auch längenreduziert sein (mit Gram-Schmidt Koeffizienten im Intervall $\geq -1/2$ und $\leq 1/2$), denn sonst könnte man v_2 durch einen zu v_1 linear unabhängigen, kürzeren Vektor aus Λ ersetzen. Das $\pm$ ist erforderlich, um den Gram-Schmidt Koeffizienten in das Intervall $> -1/2$ und $\leq 1/2$ zu bekommen.

(ii) $\Rightarrow$ *(i)*: Aufgrund der Annahme läßt sich v_2 nicht durch v_1 verkleinern, also $|\langle v_1, v_2\rangle|/||v_1||^2 \leq 1/2$. Wegen $||v_1|| \leq ||v_2||$ gilt auch $|\langle v_1, v_2\rangle|/||v_2||^2 \leq 1/2$, also sind v_1, v_2 paarweise reduziert für $\delta = 1$. $\square$

LLL Reduktion

Die LLL Reduktion wurde von A. K. Lenstra, H. W. Lenstra Jr. und L. Lovasz 1982 erfunden, und zwar um zu zeigen, daß normierte Polynome in $\mathbb{Z}[x]$ in Polynomzeit im Grad und der Länge der Koeffizienten faktorisiert werden können. Mitterweile spielt die LLL Reduktion eine sehr wichtige Rolle in vielen anderen Bereichen der diskreten, algorithmischen Mathematik.

Wir bezeichnen mit π_j die orthogonale Projektion von $\mathbb{R}^n$ auf das orthogonale Komplement von $\sum_{i=1}^{j-1} \mathbb{R}v_i$. Es gilt also speziell $v_i^* = \pi_i(v_i)$ und $\pi_i(v_j) = 0$ für $1 \leq j < i$. Für das folgende bemerken wir auch, daß $\langle \pi_i(v_{i+1}), v_i^* \rangle = \langle v_{i+1}, v_i^* \rangle$ gilt.

31 Definition. Sei $1/4 < \delta \leq 1$. Die Vektoren $v_1, \ldots, v_r \in \Lambda$ heißen LLL reduziert für δ, wenn die folgenden zwei Bedingungen gelten.

(LLL1) die $v_1, \ldots, v_r$ sind längenreduziert,

(LLL2) $\delta ||\pi_i(v_i)||^2 \leq ||\pi_i(v_{i+1})||^2$ für $1 \leq i \leq r-1$.

32 Lemma. *Die Bedingung* (LLL2*) aus der Definition ist äquivalent zur Bedingung*

(LLL2') $(\delta - \mu_{i,i+1}^2)||v_i^*||^2 \leq ||v_{i+1}^*||^2$ *für* $1 \leq i \leq r-1$

Beweis. Es gilt

$$\pi_i(v_{i+1}) = \pi_{i+1}(v_{i+1}) + \mu_{i,i+1}\pi_i(v_i) = v_{i+1}^* + \mu_{i,i+1}v_i^*$$

mit $\mu_{i,i+1} = \langle v_{i+1}, v_i^* \rangle / ||v_i^*||^2 = \langle \pi_i(v_{i+1}), v_i^* \rangle / ||v_i^*||^2$, $|\mu_{i,i+1}| \leq 1/2$ oder $\mu_{i,i+1} = 0$ für $v_i^* = 0$. Einsetzen in (LLL2), Anwendung von $|| \cdot ||^2$, der Satz des Pythagoras und Umstellen liefern (LLL2'). □

Aus (LLL2') ergibt sich sinnvollerweise $\delta > 1/4$, da (LLL2') bzw. (LLL2) sonst keine echte Anforderung darstellen könnten. Die obere Schranke $\delta \leq 1$ ergibt sich daraus, daß man ein endliches Verfahren zur Bestimmung LLL reduzierter Vektoren bzw. eine Existenzaussage für LLL reduzierte Basen von Gittern haben möchte (siehe später). Die obere und untere Schranke für δ wird im Satz 33 über die Eigenschaften einer LLL reduzierten Basis verwendet.

Für $\delta = 1$ und linear unabhängige v_i, v_{i+1} wird durch (LLL1) und (LLL2) nach Satz 30 und der Bemerkung vor der Definition gefordert, daß $\pi_i(v_i)$ und $\pi_i(v_{i+1})$ paarweise reduziert sind. Insbesondere gilt daher im Fall $\delta = 1$, daß $||\pi_i(v_i)|| = \lambda_1(\Lambda_i^*)$ und $||\pi_i(v_{i+1})|| = \lambda_2(\Lambda_i^*)$ für $\Lambda_i^* = \mathbb{Z}\pi_i(v_i) + \mathbb{Z}\pi_i(v_{i+1})$ ist.

33 Satz. *(Eigenschaften von LLL reduzierten Vektoren) Seien $v_1, \ldots, v_r \in \Lambda$ LLL reduziert für δ und $\alpha = (\delta - 1/4)^{-1} \geq 4/3$. Dann gilt:*

(*i*) *Es gibt s mit $1 \leq s \leq r+1$, so daß $v_j = 0$ für $1 \leq j \leq s-1$ und $v_s, \ldots, v_r$ linear unabhängig sind,*

(*ii*) $||v_i^*||^2 \leq \alpha^{j-i}||v_j^*||^2$ *für* $1 \leq i \leq j \leq r$.

Sind die $v_1, \ldots, v_r$ zusätzlich eine Basis des Gitters Λ, so gilt:

(*iii*) $\lambda_j(\Lambda)^2 \leq \alpha^{j-1}||v_j^*||^2$ *für* $1 \leq j \leq r$,

(*iv*) $||v_k||^2 \leq \alpha^{j-1}||v_j^*||^2$ *für* $1 \leq k \leq j$,

(*v*) $||v_j||^2 \leq \alpha^{r-1}\lambda_j(\Lambda)^2$ *für* $1 \leq j \leq r$.

Speziell ergibt sich dann:

(*vi*) $||v_1|| \leq \alpha^{(r-1)/4}d(\Lambda)^{1/r}$,

(*vii*) $\prod_{i=1}^r ||v_i|| \leq \alpha^{r(r-1)/4}d(\Lambda)$.

Beweis. (*i*): Die Aussage ist richtig, wenn alle $v_j = 0$ sind. Sei $1 \leq s \leq r$ minimal mit $v_s \neq 0$. Dann gilt $v_s^* = v_s \neq 0$, und aufgrund von (LLL2) folgt induktiv unter Verwendung von $\delta > 1/4$, daß $v_i^* \neq 0$ für $i \geq s$. Daher sind $v_s, \ldots, v_r$ linear unabhängig.

(*ii*): Folgt induktiv aus (LLL2').

(*iii*) und (*iv*): Es gibt ein k mit $1 \leq k \leq j$ und $\lambda_j(\Lambda) \leq ||v_k||$. Dann folgt aus der Längenreduziertheit und (*ii*):

$$\begin{aligned}\lambda_j(\Lambda)^2 \leq ||v_k||^2 \leq ||v_k^*||^2 + (1/4)\sum_{i=1}^{k-1}||v_i^*||^2 \leq ||v_j^*||^2(\alpha^{j-k} + (1/4)\sum_{i=1}^{k-1}\alpha^{j-i}) \\ = ||v_j^*||^2\alpha^{j-1}(\alpha^{1-k} + (1/4)\sum_{i=1}^{k-1}\alpha^{1-i}) \leq ||v_j^*||^2\alpha^{j-1}.\end{aligned}$$

Daraus ergibt sich (*iii*) und (*iv*). Wir zeigen noch $\alpha^{1-k}+(1/4)\sum_{i=1}^{k-1}\alpha^{1-i} \leq 1$. Dies gilt für $k = 1$. Für $k \geq 2$ ergibt sich mit $\alpha^{-1} \leq 3/4$ wegen $\delta \leq 1$, daß

$$\begin{aligned}\alpha^{1-k} + (1/4)\sum_{i=1}^{k-1}\alpha^{1-i} &\leq (3/4)^{k-1} + (1/4)(1-(3/4)^{k-1})/(1-3/4) \\ &= (1/4)/(1-3/4) = 1.\end{aligned}$$

(v): Nach Lemma 24 gibt es ein $k \geq j$ mit $\lambda_j(\Lambda) \geq ||v_k^*||$. Daraus ergibt sich mit $\alpha \geq 1$: $\lambda_j(\Lambda)^2 \geq ||v_k^*||^2 \geq \alpha^{-k+j}||v_j^*||^2 \geq \alpha^{-k+1}||v_j||^2 \geq \alpha^{-r+1}||v_j||^2$.

(vi) und (vii): Aus $\prod_{i=1}^r ||v_i^*|| = d(\Lambda)$ und $||v_1||^2 \leq ||v_i^*||^2\alpha^{i-1}$ nach (iv) für $k = 1$ und $j = i$ folgt

$$||v_1||^{2r} \leq \alpha^{1+\cdots+(r-1)} \prod_{i=1}^r ||v_i^*||^2 = \alpha^{r(r-1)/2} d(\Lambda)^2,$$

also (vi). Aus $\prod_{i=1}^r ||v_i^*|| = d(\Lambda)$ und $||v_i||^2 \leq ||v_i^*||^2\alpha^{i-1}$ nach (iv) für $k = i = j$ folgt

$$\prod_{i=1}^r ||v_i||^2 \leq \alpha^{1+\cdots+(r-1)} \prod_{i=1}^r ||v_i^*||^2 = \alpha^{r(r-1)/2} d(\Lambda)^2,$$

also (vii). □

Zur konzeptuellen Interpretation der Aussagen von Satz 33 können wir folgendes festhalten.

- Die Bedingungen (v) und (vi) besagen, daß v_1 approximativ ein kürzester Vektor in Λ ist, mit in der Dimension r exponentiellem Fehlerfaktor.
- Die Bedingungen (v) und (vii) besagen weiter, daß die v_j die sukzessiven Minimal approximativ realisieren, mit in der Dimension r exponentiellem Fehlerfaktor.
- Die Bedingungen (LLL2'), (iv) und (vii) besagen, daß die v_j approximativ orthogonal sind.

Man vergleiche auch die Aussagen (vi) und (vii) mit (17), $\lambda_1(\Lambda) \leq \gamma_r^{1/2} d(\Lambda)^{1/r}$, und Satz 23, $\prod_{i=1}^r \lambda_i(\Lambda) \leq \gamma_r^{r/2} d(\Lambda)$.

Zusätzlich zur oberen Abschätzung (iii) aus Satz 33 gilt die untere Abschätzung aus Lemma 24, welche günstigerweise nur auf LLL reduzierte Vektoren angewendet werden sollte.

Wir kommen nun zum LLL Reduktionsverfahren bzw. LLL Algorithmus.

34 Algorithmus. *(LLL Reduktionsverfahren)*

Eingabe: *Vektoren* $v_1, \ldots, v_r \in \Lambda$, δ *mit* $1/4 < \delta \leq 1$.

Ausgabe: *LLL reduzierte Vektoren* $w_1, \ldots, w_r \in \Lambda$ *bezüglich* δ, *die unimodulare Transformationsmatrix* $T \in \mathbb{Z}^{r\times r}$ *mit* $(w_1, \ldots, w_r) = (v_1, \ldots, v_r)T$.

1. *$j := 1$, $v_1^* := v_1$, $T := I_r$, $\mu_{1,1} := 1$.*

2. *Hier gilt stets, daß die $v_1, \ldots, v_j$ LLL reduziert sind und T die unimodulare Transformationsmatrix ist, welche die Eingabebasis in die gegenwärtigen $v_1, \ldots, v_r$ transformiert. Darüberhinaus sind Gram-Schmidt orthogonalisierte Vektoren $v_1^*, \ldots, v_j^* \in \mathbb{R}\Lambda$ und die zugehörigen Gram-Schmidt Koeffizienten $\mu_{i,k}$ für $1 \leq i \leq k \leq j$ bekannt.*

3. *Wenn $j \geq r$ dann Ausgabe von $v_1, \ldots, v_r$, T. Terminiere.*

4. *Berechne die Gram-Schmidt Koeffizienten $\mu_{i,j+1}$ von v_{j+1} bezüglich der v_i^* für $1 \leq i \leq j$, $\mu_{j+1,j+1} := 1$ und v_{j+1}^* wie eingangs erläutert.*

5. *Längenreduziere v_{j+1} bezüglich der v_i für $1 \leq i \leq j$ mit Hilfe der $\mu_{i,k}$ für $1 \leq i \leq k \leq j+1$ und passe T entsprechend an. Nun sind die $v_1, \ldots, v_{j+1}$ längenreduziert und* (LLL1) *gilt entsprechend bis $j+1$ anstatt r.*

6. *Wenn* (LLL2) *für $i = j$ gilt, wenn also $(\delta - \mu_{i,i+1}^2)||v_i^*||^2 \leq ||v_{i+1}^*||^2$ für $i = j$ gilt, dann gilt* (LLL2) *hier für alle $1 \leq i \leq j$, und wir setzen $j := j+1$ und gehen zu Schritt 2.*

7. *Vertausche v_j und v_{j+1} und passe T entsprechend an (also die j-te Spalte mit der $j+1$-ten Spalte von T vertauschen). Ebenfalls anzupassen ist v_j^* und die $\mu_{i,j}$ für $1 \leq i \leq j$. Setze $j := \max\{j-1, 1\}$ und gehe zu Schritt 2.*

35 Satz. *Für $1/4 < \delta \leq 1$ terminiert der LLL Algorithmus in einer endlichen Anzahl von Schritten mit LLL reduzierten Vektoren.*

Genauere Abschätzungen für die Anzahl der Iterationen von Schritt 7 im Fall $1/4 < \delta < 1$ ergeben sich wie folgt. Mit $\Lambda = \sum_{i=1}^r \mathbb{Z}v_i$ setze $n = \dim(\Lambda)$, $M = \max_{1 \leq i \leq r, v_i \neq 0} ||v_i||^2$, $M = 1$ wenn alle $v_i = 0$, und $T(\Lambda) = \inf\{\, d(\Lambda')^2 \,|\, \Lambda'$ Teilgitter von $\Lambda \,\}$. Es gilt $T(\Lambda) > 0$. Die Anzahl m der Iterationen von Schritt 7 ist dann nach oben beschränkt durch

$$m \leq n \log_{1/\delta}(M^n/T(\Lambda)) + (r-n)n.$$

Beweis. Wenn der Algorithmus terminiert, so ist die Ausgabe korrekt aufgrund der Schleifeninvariante in Schritt 2. Man kann sich leicht klar machen, daß die Anpassungen in den beiden letzten Schritten gerade zur Erhaltung der Schleifeninvarianten dienen.

Angenommen nun, der LLL Algorithmus würde unter Eingabe der Vektoren $v_1, \ldots, v_r$ nicht terminieren. Dann wird Schritt 7 unendlich oft ausgeführt. Sei s der minimale Index j, welcher im Schritt 7 unendlich oft vorkommt. Wir betrachten einen Zeitpunkt in der Ausführung des LLL Algorithmus, ab dem $j < s$ in Schritt 7 nicht mehr vorkommt. Ab diesem Zeitpunkt bleiben die $v_1, \ldots, v_{s-1}$ und damit die Projektion π_s unverändert. Sei $\Lambda' = \pi_s(\Lambda) = \mathbb{Z}\pi_s(v_s) + \cdots + \mathbb{Z}\pi_s(v_r)$. Dann ist Λ' ein Gitter: Sei $\pi_s(x_i)$ eine Folge in $\Lambda' \backslash \{0\}$ mit $x_i \in \Lambda$ und $\lim_{i\to\infty} \pi_s(x_i) = 0$. Dann gibt es $y_i \in \mathbb{R}\Lambda''$ mit $\Lambda'' = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_{s-1}$ und $\pi_s(x_i) = x_i - y_i$. Aufgrund der Annahme sind Λ und Λ'' Gitter. Durch Translation der x_i und y_i mit geeigneten Vektoren aus Λ'' können wir $y_i \in \Pi$ für ein Fundamentalparallelotop Π von Λ'' annehmen. Eine Teilfolge der y_i konvergiert im Abschluß von Π gegen $y \in \Pi \subseteq \mathbb{R}\Lambda''$, da Π kompakt ist. Wegen $x_i = \pi_s(x_i) + y_i$ mit $\lim_{i\to\infty} \pi_s(x_i) = 0$ liegen daher in jeder Umgebung von y in $\mathbb{R}\Lambda$ unendlich viele x_i mit $x_i \neq y$ wegen $x_i \notin \mathbb{R}\Lambda''$, da $\pi_s(x_i) \neq 0$. Dies ist ein Widerspruch zur Diskretheit von Λ, und somit ist Λ' in der Tat ein Gitter. Die Elemente $\pi_s(v_s), \ldots, \pi_s(v_r)$ sind unabhängig von einer Längenreduktion der $v_s, \ldots, v_r$ bezüglich der $v_1, \ldots, v_{s-1}$ wie in Schritt 5. Die Folge ist, daß speziell $\pi_s(v_s)$ sich nur in Schritt 7 für $j = s$ ändern kann. Da Schritt 7 unendlich oft für $j = s$ durchlaufen wird, erhalten wir wegen der Nichtgültigkeit von (LLL2) eine unendliche Folge von Elementen $\pi_s(v_s)$ von Λ' mit echt absteigenden Längen (ungleich Null), im Widerspruch zur Diskretheit von Λ'.

Sei nun $\delta < 1$. In Schritt 2 betrachten wir die wie folgt definierten Teilgitter von Λ: $\Lambda_j = \sum_{1\leq i\leq j} \mathbb{Z}v_i$ und $\Lambda'_{k(j)} = \sum_{1\leq i\leq j, v_i^* \neq 0} \mathbb{Z}v_i$ der Dimension $k(j)$. Es gilt $\{k(j) \,|\, 1 \leq j \leq r\} = \{1, \ldots, n\}$ und $d(\Lambda'_{k(j)}) = \prod_{1\leq i\leq j, v_i^* \neq 0} ||v_i^*||$. Ohne Beschränkung der Allgemeinheit können wir $M \geq 1$ annehmen. Nach der Hadamard Schranke gilt dann $d(\Lambda'_k)^2 \leq M^n$, wobei wir $d(\{0\}) = 1$ definieren. Eine untere Schranke > 0 für $T(\Lambda)$ ist wie folgt gegeben. Für $\Lambda = \{0\}$ gilt $T(\Lambda) = 1$. Andernfalls sei $\Lambda' \subseteq \Lambda$ mit $\dim(\Lambda') = i$ und $i \geq 1$. Es gilt $\lambda_1(\Lambda) \leq \lambda_1(\Lambda') \leq \gamma_i^{1/2} d(\Lambda')^{1/i}$, also $d(\Lambda') \geq \gamma_i^{-i/2} \lambda_1(\Lambda)^i$, also gilt $T(\Lambda) \geq \min\{1, \min_i \gamma_i^{-i} \lambda_1(\Lambda)^{2/i}\} > 0$.

Wir nehmen zunächst den Fall an, daß die Eingabevektoren $v_1, \ldots, v_r$ linear unabhängig sind, also $n = r$, $k(j) = j$ und $\Lambda_j = \Lambda'_{k(j)}$ gilt. Für die Gitterdiskriminanten folgt $d(\Lambda_j) = \prod_{1\leq i\leq j} ||v_i^*||$. Beim Tausch für den Index j in Schritt 7 verringert sich dann $d(\Lambda_j)^2$ wegen (LLL2) um den Mindestfaktor δ, während die übrigen Λ_i für $i \neq j$ unverändert bleiben. In jedem Schritt 7 wird dann $\prod_{i=1}^{n-1} d(\Lambda_i)^2$ um den Mindestfaktor δ kleiner. Wegen $T(\Lambda)^{n-1} \leq \prod_{i=1}^{n-1} d(\Lambda_i)^2 \leq M^{n(n-1)}$ folgt $\delta^m M^{n(n-1)} \geq T(\Lambda)^{n-1}$ und daraus die Aussage.

Zum Beweis für den linear abhängigen Fall ist eine genauere Betrachtung der Fälle in Schritt 7 erforderlich. Vor Schritt 7 ist aufgrund von Schritt 2

und Satz 33, (i) folgendes der Fall. Es gibt s, j mit $0 \leq s \leq j \leq r-1$, so daß $v_1, \ldots, v_s$ Null und $v_{s+1}, \ldots, v_j$ linear unabhängig und LLL reduziert sind. Dann gilt $\pi_i(v_i) \neq 0$ für $s+1 \leq i \leq j$. Wir nehmen an, wir befinden uns in Schritt 7 für dieses $j \geq s$.

1. Fall $\pi_{j+1}(v_{j+1}) \neq 0$: Hier sind $v_{s+1}, \ldots, v_{j+1}$ linear unabhängig und wir befinden uns (lokal) in der oben bereits betrachteten Situation.

2. Fall $\pi_{j+1}(v_{j+1}) = 0$ und $j = s$: Hier folgt $v_{j+1} = 0$ und der LLL Algorithmus geht ohne Tausch von j zu $j+1$ über. Dieser Fall kommt in Schritt 7 also gar nicht vor.

3. Fall $\pi_{j+1}(v_{j+1}) = 0$ und $j > s$. Hier findet wegen $\pi_j(v_j) \neq 0$ nach (LLL2') auf jeden Fall ein Tausch statt. Vor dem Tausch gilt $v_{j+1} \notin \mathbb{R}\Lambda_{j-1}$ oder $v_{j+1} \in \mathbb{R}\Lambda_{j-1}$.

3.1. Im ersten Fall $v_{j+1} \notin \mathbb{R}\Lambda_{j-1}$ in 3. erhalten wir nach dem Tausch wieder $\pi_j(v_j) \neq 0$ und $\pi_{j+1}(v_{j+1}) = 0$.

3.2. Im zweiten Fall $v_{j+1} \in \mathbb{R}\Lambda_{j-1}$ in 3. gilt nach dem Tausch $\pi_j(v_j) = 0$ und das neue $\pi_{j+1}(v_{j+1})$ ist gleich dem alten $\pi_j(v_j)$, insbesondere $\neq 0$. Dieser zweite Fall unterteilt sich in zwei Unterfälle. Entweder es gilt vor dem Tausch $v_{j+1} \notin \Lambda_{j-1}$ oder $v_{j+1} \in \Lambda_{j-1}$.

3.2.1. In der ersten Situation $v_{j+1} \notin \Lambda_{j-1}$ in 3.2. gilt also nach dem Tausch $d(\Lambda_j) \leq d(\Lambda_{j-1})/2$.

3.2.2. In der zweiten Situation $v_{j+1} \in \Lambda_{j-1}$ in 3.2. gilt aufgrund der vorangegangenen Längenreduktion vor dem Tausch $v_{j+1} = 0$, und nach dem Tausch $v_j = 0$ und $d(\Lambda_j) = d(\Lambda_{j-1})$.

Nach Ausführung von Schritt 7 gilt die obige Annahme für $v_1, \ldots, v_{\max\{j-1,1\}}$ und der LLL Algorithmus fährt mit $\max\{j-1, 1\}$ als neuem j fort. Linear abhängige Vektoren werden also der Reihe nach mit etwaigen Zwischenreduktionsschritten für kleinere j nach vorne sortiert, wo sie dann „Null werden müssen“.

Wir wollen jetzt untersuchen, wie sich die Gitterdiskriminanten der Λ'_k und $D = \prod_{k=1}^{n} d(\Lambda'_k)^2$ in den einzelnen Fällen ändern. Die v_i^* können sich in Schritt 7 nur für $i = j$ und $i = j+1$ ändern. Daher bleiben die $\Lambda'_{k(i)}$ für $i < j$ gleich. Im Fall 1 und 3.1 verringert sich $d(\Lambda'_{k(j)})^2$ um den Mindestfaktor δ. Im Fall 1 bleiben auch die $\Lambda'_{k(i)}$ für $i > j$ gleich, während sich im Fall 3.1 ihre Diskriminantenquadrate um den gleichen Faktor wie bei $\Lambda'_{k(j)}$ verringern. In beiden Fällen bleiben die $k(i)$ gleich. Im Fall 3.2 bleiben alle Λ'_k für $1 \leq k \leq n$ gleich, $k(j)$ verringert sich allerdings um eins, die anderen $k(i)$ bleiben gleich.

Es gilt $T(\Lambda) \leq d(\Lambda'_k) \leq M^k$ beziehungsweise $T(\Lambda)^n \leq D \leq M^{n^2}$ zu jedem Zeitpunkt. Bezeichnet m_0 die Anzahl der Fälle 1 oder 3.1 in den Ausführungen von Schritt 7 und m_1 die Anzahl der Fälle 3.2, so gilt folglich $\delta^{m_0} M^{n^2} \geq T(\Lambda)^n$ und $m_1 \leq (r-n)n$ („Anzahl der abhängigen Vektoren" mal „Anzahl möglicher Tausche für einen abhängigen Vektor"). Daraus ergibt sich die Aussage. □

36 Korollar. *Jedes Gitter besitzt LLL reduzierte Basen für beliebige δ mit $1/4 < \delta \leq 1$.*

Wir bemerken, daß die Annahme $v_1, \ldots, v_r \in \Lambda$ für ein *Gitter* Λ für die endliche Laufzeit des LLL Algorithmus wesentlich ist. Beispielsweise besitzt $\mathbb{Z} + \pi\mathbb{Z}$ keine $\mathbb{R}$-linear unabhängige Basis, insbesondere auch keine LLL reduzierte Basis. Wir bemerken außerdem, daß eine LLL reduzierte Basis eines Gitters Λ nicht eindeutig nur durch Λ bestimmt wird.

Für $\Lambda \subseteq \mathbb{Z}^n$ gilt $T(\Lambda) \geq 1$ wegen $d(\Lambda)^2 \in \mathbb{Z}^{\geq 1}$, so daß sich die Abschätzung aus Satz 35 entsprechend vereinfacht.

37 Satz. *Mit den Bezeichnungen von Satz 35 gelte $\Lambda \subseteq \mathbb{Z}^n$. Der LLL Algorithmus ohne Mitführen von T benötigt eine Laufzeit von $O((m+r)r^2)$ arithmetischen Operationen mit ganzen Zahlen der Größe $O(r \log(M))$ und $m \leq n^2 \log_{1/\delta}(M) + (r-n)n$.*

Speziell ergibt sich für $r = n$ eine Laufzeit von $O(n^4 \log_{1/\delta}(M))$ arithmetischen Operationen mit ganzen Zahlen der Größe $O(n \log(M))$.

Beweis. Schritt 2 wird $O(m+r)$ mal durchlaufen. Schritt 1, Schritt 4 und Schritt 5 benötigen $O(r^2)$ Operationen. Schritt 6 und Schritt 7 benötigen $O(r)$ Operationen. Daraus ergeben sich insgesamt $O((m+r)r^2)$ Operationen. Die Aussage über die Größe der Koeffizienten beweisen wir nicht. □

In vielen praktischen Fällen (für $\delta < 1$) sind die exponentiellen Fehlerfaktoren in Satz 33 wesentlich zu pessimistisch, und man erhält aus dem LLL Algorithmus unter Eingabe einer Gitterbasis mit w_1 beispielsweise wirklich einen kürzesten Vektor des Gitters. Auf der anderen Seite lassen sich die exponentiellen Fehlerfaktoren im allgemeinen (worst case) für ein Polynomzeitverfahren vermutlich nicht verringern. Gibt man beispielsweise in der Dimension konstante Fehlerfaktoren vor, so sind nur Basisreduktionsverfahren bekannt, welche von der Dimension exponentiell abhängen.