Johann Wolfgang Goethe-Universität
Frankfurt/Main
Fachbereich Mathematik

Diplomarbeit

Gitterreduktion, elementare Algorithmen und Faktorisierung ganzer Zahlen [1]

Gerold Jäger
Ackermannstraße 68
60326 Frankfurt/Main
Tel. 069/7391200

Frankfurt/Main, den 17. März 1998

Betreuer: Professor Dr. C.P. Schnorr
Vertreter: Professor Dr. M. Sieveking

[1] nach Arbeiten von M. Seysen:
"A Measure for the Non-Orthogonality of a Lattice Basis"
und M. Ajtai:
"The Shortest Vector Problem in L_2 is NP-hard for Randomized Reductions"

Inhaltsverzeichnis

Einleitung

Gitter sind diskrete, additive Untergruppen des $\mathbb{R}^m$, ein linear unabhängiges Erzeugendensystem eines Gitters heißt Gitterbasis. Die Anzahl der Basisvektoren eines Gitters ist eindeutig bestimmt und heißt Rang des Gitters. Zu jedem Gitter vom Rang n gibt es mehrere Gitterbasen, die man alle erhält, indem man eine Basismatrix $B = [b_1, \cdots, b_n]$ von rechts mit allen Matrizen aus der Gruppe $GL_n(\mathbb{Z})$ multipliziert.
Eine wichtige Fragestellung der Gittertheorie ist es, zu einem gegebenen Gitter einen kürzesten, vom Nullvektor verschiedenen Gittervektor zu finden. Dieses Problem heißt das "kürzeste Gittervektorproblem". Ein dazu verwandtes Problem ist das "nächste Gittervektorproblem", das zu einem beliebigen Vektor x aus $\mathbb{R}^m$ einen Gittervektor sucht, dessen Abstand zu x minimal ist.
Aus dem "kürzesten Gittervektorproblem" entwickelte sich die Gitterbasenreduktion, deren Ziel es ist, eine gegebene Gitterbasis in eine Gitterbasis zu transformieren, deren Vektoren bzgl. der Euklidischen Norm kurz und möglichst orthogonal zueinander sind. Wichtig für die Güte einer Reduktion ist der Begriff der sukzessiven Minima $\lambda_1(L), \cdots, \lambda_n(L)$ eines Gitters L. Dabei ist $\lambda_i(L)$ die kleinste reelle Zahl $r > 0$, für die es i linear unabhängige Vektoren $c_j \in L$ gibt mit $\|c_j\| \leq r$ für $j = 1, \cdots, i$. Man versucht, für ein Gitter L eine Gitterbasis $b_1, \cdots, b_n$ zu finden, bei der die Größe $\|b_i\| \,/\, \lambda_i(L)$ für $i = 1, \cdots, n$ möglichst klein ist. Für Gitter vom Rang 2 liefert das Gauß'sche Reduktionsverfahren eine Gitterbasis mit $\|b_i\| = \lambda_i(L)$ für $i = 1, 2$. Eine Verallgemeinerung der Gauß-Reduktion auf Gitter mit beliebigem Rang ist die im Jahre 1982 von Lenstra, Lenstra, Lovász vorgeschlagene L^3-Reduktion einer Gitterbasis, deren Laufzeit polynomiell in der Bitlänge der Eingabe ist. L^3-reduzierte Gitterbasen approximieren die sukzessiven Minima bis auf einen (im Rang des Gitters) exponentiellen Faktor.
Die vorliegende Arbeit besteht aus zwei Teilen. Im ersten Teil (Kapitel 1-6) wird ein neues Reduktionskonzept von M. Seysen aus der Arbeit "A Measure for the Non-Orthogonality of a Lattice Basis" [13] behandelt und im zweiten Teil (Kapitel 7) ein aktuelles Ergebnis von M. Ajtai über die Faktorisierung ganzer Zahlen aus "The Shortest Vector Problem in L_2 is NP-hard for Randomized Reductions" [2].
Seysen führte in [13] zu einer gegebenen Gitterbasis $b_1, \cdots, b_n$ die Größe $\sigma(A)$ ein, die nur von den Einträgen der zugehörigen Gram-Matrix $A = [b_1, \cdots, b_n]^T \cdot [b_1, \cdots, b_n]$ und der Inversen A^{-1} abhängt. Sie hat die Eigenschaft, daß für jede Gitterbasis $b_1, \cdots, b_n$ mit Gram-Matrix A gilt, daß $\sigma(A) \geq 1$, wobei die Gleichheit genau dann gilt, wenn $b_1, \cdots, b_n$ orthogonal ist. Aus dieser Defintion ergibt sich folgender Reduktionsbegriff: Eine Gitterbasis $b_1, \cdots, b_n$ mit Gram-Matrix A heißt genau dann τ-reduziert, wenn $\sigma(A)$ minimal für alle Basen des Gitters ist. Der wesentliche Unterschied der τ-Reduktion zur L^3-Reduktion ist, daß die Größe $\sigma(A)$ unabhängig von der Reihenfolge der Basisvektoren ist, so daß eine

τ-reduzierte Gitterbasis bei beliebiger Permutation der Basisvektoren τ-reduziert bleibt. Die τ-Reduktion reduziert also im Gegensatz zur L^3-Reduktion die Basisvektoren gleichmäßig. Seysen zeigte, daß man zu jedem Gitter vom Rang n eine Gitterbasis mit Gram-Matrix A findet, so daß $\sigma(A)$ durch $e^{O((\ln n)^2)}$ beschränkt ist. Daraus läßt sich ableiten, daß τ-reduzierte Gitterbasen eines Gitters vom Rang n die sukzessiven Minima bis auf den Faktor $e^{O((\ln n)^2)}$ approximieren. Da es sich bei der τ-Reduktion um einen sehr starken Reduktionsbegriff handelt, für den es schwer ist, einen effizienten Algorithmus zu finden, definiert man folgenden schwächeren Reduktionsbegriff: $b_1, \cdots, b_n$ heißt genau dann τ_2-reduziert, wenn keine Basistransformation der Form $b_j := b_j + k \cdot b_i$ mit $1 \leq i \neq j \leq n$ und $k \in \mathbb{Z}$ die Größe $\sigma(A)$ erniedrigt. Für $n = 2$ entspricht die τ-Reduktion sowohl der τ_2-Reduktion als auch der Gauß-Reduktion. Für die τ_2-Reduktion findet man einen effizienten Algorithmus. Wendet man diesen Algorithmus auf Rucksackprobleme an, so ergibt sich, daß durch einen Algorithmus, bestehend aus τ_2-Reduktion und anschließender L^3-Reduktion, bei großer Dichte und bei kleiner Dimension wesentlich mehr Rucksackprobleme gelöst werden als durch den L^3-Algorithmus.

Die Faktorisierung großer ganzer Zahlen ist ein fundamentales Problem mit großer kryptographischer Bedeutung. Schnorr stellte in [11] erstmals einen Zusammenhang zwischen Gitterbasenreduktion und Faktorisierung her, indem er das Faktorisieren ganzer Zahlen auf das "nächste Gittervektorproblem in der Eins-Norm" zurückführte. Adleman führte in [1] das Faktorisieren ganzer Zahlen sogar auf das "kürzeste Gittervektorproblem in der Euklidischen Norm" zurück, allerdings unter zahlentheoretischen Annahmen. In [2] stellte Ajtai ein neues Ergebnis vor, in dem er das Faktorisieren ganzer Zahlen auf das "kürzeste Gittervektorproblem in der Euklidischen Norm" ohne zusätzliche Annahmen zurückführte.

Für die intensive Betreuung meiner Diplomarbeit möchte ich mich bei Prof. Dr. Claus Peter Schnorr bedanken. Weiterhin danke ich Dr. Harald Ritter und Jean-Pierre Seifert für viele nützliche Anregungen und Verbesserungsvorschläge zu dieser Arbeit.

Kapitel 1

Grundlagen

Wir führen in Abschnitt 1.1 die in dieser Arbeit benötigten Notationen ein und fassen in Abschnitt 1.2 wichtige Begriffe und elementare Sätze der Gittertheorie zusammen.

1.1 Notationen

Sei $\mathbb{N}$ die Menge der natürlichen Zahlen und $\mathbb{N}_0$ die Menge der natürlichen Zahlen einschließlich der 0. Es bezeichne $\mathbb{Z}$ bzw. $\mathbb{Q}$ die Menge der ganzen bzw. rationalen Zahlen. $\mathbb{R}$ steht für die Menge der reellen Zahlen und $\mathbb{R}_+$ für die Menge der positiven reellen Zahlen. Sei $\mathbb{Z}^n$ bzw. $\mathbb{R}^n$ die Menge der n-dimensionalen ganzzahligen bzw. reellen Vektoren. $\mathbb{R}^n$ ist ein n-dimensionaler Vektorraum mit dem Standardskalarprodukt $< \cdot, \cdot >$, der zugehörigen Euklidischen Norm $\|y\| := < y, y >^{1/2}$, der Maximums-Norm $\|y\|_\infty := \max_{1 \le i \le n}\{|y_i|\}$ und der Eins-Norm $\|y\|_1 := \sum_{i=1}^n |y_i|$. Es gilt die Cauchy-Schwarz'sche Ungleichung:

$$| < x, y > | \quad \le \quad \|x\| \cdot \|y\| \tag{1.1}$$

vol_n sei das n-dimensionale Volumen einer Teilmenge von $\mathbb{R}^n$. Eine Teilmenge aus $\mathbb{R}^n$ heißt diskret, wenn sie keinen Häufungspunkt besitzt. Es bezeichne $\mathrm{span}(y_1, \cdots, y_n)$ die lineare Hülle der Vektoren $y_1, \cdots, y_n$.
Sei $\mathbb{Z}^{m,n}$ bzw. $\mathbb{R}^{m,n}$ die Menge aller $m \times n$-Matrizen mit Einträgen aus $\mathbb{Z}$ bzw. $\mathbb{R}$. Für Matrizen $C = (c_{s,t})_{1 \le s \le m, 1 \le t \le n}$ sei $\|C\| := \left(\sum_{1 \le s \le m, 1 \le t \le n} c_{s,t}^2\right)^{1/2}$ die Euklidische Norm und $\|C\|_\infty := \max_{1 \le s \le m, 1 \le t \le n}\{|c_{s,t}|\}$ die Maximums-Norm.
Es gilt für $C \in \mathbb{R}^{m,n}, D \in \mathbb{R}^{n,r}$:

$$\|C \cdot D\| \quad \le \quad \|C\| \cdot \|D\| \tag{1.2}$$

Wir betrachten – wenn nicht anders erwähnt – immer die Euklidische Norm.
Es sei C^T die Transponierte einer beliebigen Matrix C, C^{-1} die Inverse einer

regulären Matrix C und $\det(C)$ die Determinante einer quadratischen Matrix C. Für eine quadratische Matrix C sei $\mathrm{tr}(C)$ die Spur von C, sie ist gleich der Summe der Diagonalelemente von C. Eine quadratische Matrix heißt Diagonalmatrix, wenn sie nur in der Diagonalen Einträge ungleich Null hat. Die Inverse einer regulären Matrix $C \in \mathbb{R}^{n,n}$ läßt sich als

$$C^{-1} = \Big((-1)^{s+t} \cdot \frac{\det C'_{t,s}}{\det C}\Big)_{1 \le s,t \le n} \tag{1.3}$$

schreiben, wobei $C'_{t,s}$ die Matrix ist, die durch Streichen der t-ten Zeile und der s-ten Spalte aus C entsteht.
Sei $GL_n(\mathbb{R})$ die Gruppe aller invertierbaren Matrizen aus $\mathbb{R}^{n,n}$ und $GL_n(\mathbb{Z})$ die Gruppe aller Matrizen aus $\mathbb{Z}^{n,n}$ mit Determinante ± 1. Die Elemente aus $GL_n(\mathbb{Z})$ heißen auch unimodulare Matrizen. Schließlich bezeichnet $[y_1, \cdots, y_n]$ die Matrix, die aus den Spaltenvektoren $y_1, \cdots, y_n$ besteht.
$[a, b]$ steht für das abgeschlossene Intervall von a bis b . Für $x \in \mathbb{R}$ bezeichne $\lceil x \rfloor$ die nächste ganze Zahl zu x, wobei bei halbzahligen Werten abgerundet wird.
Seien O und o die Landau'schen Symbole und $\delta_{i,j}$ das Kronecker-Symbol mit $\delta_{i,j} = 1$, falls $i = j$, und $\delta_{i,j} = 0$ sonst.
Zwei ganze Zahlen a, b heißen kongruent modulo c ($a \equiv b \,(\mathrm{mod}\, c)$), wenn $c \,|\, (b-a)$.
Ein Verfahren heißt Polynomialzeit-Algorithmus, wenn die Anzahl der arithmetischen Operationen polynomiell in der Bitlänge der Eingabe beschränkt ist.

1.2 Einführung in die Gittertheorie

Für linear unabhängige Vektoren $b_1, \cdots, b_n \in \mathbb{R}^m$ heißt die Menge

$$L(b_1, \cdots, b_n) := \left\{ \sum_{i=1}^{n} t_i \cdot b_i \,\Big|\, t_i \in \mathbb{Z} \right\} \subset \mathbb{R}^m$$

ein *Gitter* mit *Gitterbasis* $b_1, \cdots, b_n$ und *Rang* n. Zur Gitterbasis $b_1, \cdots, b_n \in \mathbb{R}^m$ ist $B = [b_1, \cdots, b_n] \in \mathbb{R}^{m,n}$ die zugehörige *Basismatrix* und $A = B^T \cdot B \ \in \mathbb{R}^{n,n}$ die zugehörige *Gram-Matrix*. Eine Gram-Matrix ist symmetrisch und hat positive Diagonalelemente. Das Gitter heißt *vollständig*, wenn $n = m$ ist, und *ganzzahlig*, wenn es in $\mathbb{Z}^m$ enthalten ist. Die Gitterbasis $b_1, \cdots, b_n$ heißt *orthogonal*, falls $< b_i, b_j >= 0$ für $1 \le i \ne j \le n$ gilt. Zu einem Gitter $L(b_1, \cdots, b_n)$ heißt $\mathrm{span}(L\,(b_1, \cdots, b_n)\,) = \mathrm{span}(b_1, \cdots, b_n)$ die lineare Hülle von $L(b_1, \cdots, b_n)$ und

$$P(b_1, \cdots, b_n) := \left\{ \sum_{i=1}^{n} x_i \cdot b_i \,\Big|\, 0 \le x_i < 1 \right\}$$

die *Grundmasche* zur Gitterbasis $b_1, \cdots, b_n$.

Gitter lassen sich folgendermaßen charakterisieren:

Satz 1.1 [6] *Die Gitter in $\mathbb{R}^m$ sind genau die diskreten, additiven Untergruppen des $\mathbb{R}^m$.*

Die Basis eines Gitters ist nicht eindeutig bestimmt. Eine wichtige Aussage über die Mengen aller Basen eines Gitters liefert der folgende Satz:

Satz 1.2 [6] *Sei $L = L(b_1, \cdots, b_n)$ ein Gitter in $\mathbb{R}^m$ und $\bar{b}_1, \cdots, \bar{b}_n \in \mathbb{R}^m$. Dann ist $\bar{b}_1, \cdots, \bar{b}_n$ genau dann eine Gitterbasis von L, wenn es eine Matrix $T \in GL_n(\mathbb{Z})$ gibt mit $[\bar{b}_1, \cdots, \bar{b}_n] = [b_1, \cdots, b_n] \cdot T$.*

Sei B eine Basismatrix eines Gitters mit Gram-Matrix A und $\bar{B}$ eine Basismatrix desselben Gitters mit $\bar{B} = B \cdot T$. Die Gram-Matrix von $\bar{B}$ erhält man durch

$$\bar{A} = (B \cdot T)^T \cdot B \cdot T = T^T \cdot A \cdot T.$$

Definition 1.3 *Die Determinante eines Gitters $L(b_1, \cdots, b_n)$ ist das n-dimensionale Volumen der Grundmasche, d.h.*

$$\det L := vol_n\Big(P(b_1, \cdots, b_n)\Big).$$

Die Gitterdeterminante kann wie folgt berechnet werden:

Satz 1.4 [6] *Sei L ein Gitter mit Gitterbasis $b_1, \cdots, b_n$ und zugehöriger Gram-Matrix A. Dann gilt:*

$$\det L = \sqrt{\det A}.$$

Die Determinante eines Gitters L hängt nicht von der Wahl der Gitterbasis ab, denn für Gram-Matrizen A und $\bar{A} = T^T \cdot A \cdot T$ verschiedener Gitterbasen gilt:

$$\det \bar{A} = \det(T^T \cdot A \cdot T) = \det^2 T \cdot \det A = \det A.$$

Definition 1.5 *Sei L ein Gitter. Das zu L duale Gitter ist definiert durch*

$$L^* := \{x \in span(L) \mid \forall\, y \in L : < x, y > \in \mathbb{Z}\}.$$

Satz 1.6 [6] *Sei L ein Gitter mit Gitterbasis $b_1, \cdots, b_n$ und zugehöriger Gram-Matrix A. Dann gilt:*

a) *Es gibt genau eine Gitterbasis $b_1^*, \cdots, b_n^*$ von L^* mit*

$$< b_i, b_j^* > = \delta_{i,j} \quad \text{für } 1 \leq i, j \leq n,$$

b) *A^{-1} ist die Gram-Matrix von $b_1^*, \cdots, b_n^*$.*

Bemerkung 1.7 *Man nennt die Gitterbasis $b_1^*, \cdots, b_n^*$ die zu $b_1, \cdots, b_n$ duale Gitterbasis.*

Kapitel 2

Gitterbasenreduktion

Ziel der Gitterbasenreduktion ist es, zu einem gegebenen Gitter eine Gitterbasis zu finden, deren Vektoren bzgl. der Euklidischen Norm kurz und möglichst orthogonal zueinander sind. In Abschnitt 2.1 werden wichtige Begriffe der Gitterbasenreduktion eingeführt, und es wird beschrieben, wann eine Gitterbasis gut reduziert ist. In den Abschnitten 2.2, 2.3 und 2.4 werden elementare Reduktionsbegriffe mit den zugehörigen Algorithmen vorgestellt.

2.1 Einführung

Die Gitterbasenreduktion versucht, eine Gitterbasis in eine andere mit kürzeren Vektoren zu transformieren. Nach Satz 1.2 erfolgt dies durch Multiplikation der Basismatrix mit unimodularen Matrizen. Folgende Basistransformationen werden durch unimodulare Matrizen beschrieben:

- Multiplikation eines Basisvektors mit -1,
- Vertauschen von zwei Basisvektoren,
- Addition des k-fachen ($k \in \mathbb{Z}$) eines Basisvektors zu einem anderen Basisvektor.

Wichtig für die Reduktion einer Gitterbasis $b_1, \cdots, b_n$ sind das zugehörige *Orthogonalsystem* $\hat{b}_1, \cdots, \hat{b}_n$ und die zugehörigen *Gram-Schmidt-Koeffizienten*

$$\mu_{i,j} := \frac{< b_i, \hat{b}_j >}{\|\hat{b}_j\|^2} \quad \text{für } 1 \leq i, j \leq n,$$

die wie folgt berechnet werden:

Algorithmus 2.1 **(Gram-Schmidt-Verfahren)**

INPUT *Gitterbasis* $b_1, \cdots, b_n \in \mathbb{R}^m$

1 $\hat{b}_1 = b_1$

2 *FOR* $i = 2, \cdots, n$

$$\mu_{i,j} = \frac{< b_i, \hat{b}_j >}{\|\hat{b}_j\|^2} \quad \textit{für } \; j < i,$$

$$\hat{b}_i \; = b_i - \sum_{j=1}^{i-1} \mu_{i,j} \cdot \hat{b}_j.$$

OUTPUT $\hat{b}_1, \cdots, \hat{b}_n \; \in \mathbb{R}^m, \; \mu_{i,j}$ *für* $1 \leq j < i \leq n$

Die Vektoren $\hat{b}_1, \cdots, \hat{b}_n$ sind linear unabhängig und paarweise orthogonal zueinander. Sie entsprechen den Höhen der zugehörigen Gitterbasis. Außerdem gilt:

$$\det L = \prod_{i=1}^{n} \|\hat{b}_i\|.$$

Für die übrigen Gram-Schmidt-Koeffizienten gilt:

$$\mu_{i,j} = \begin{cases} 1 & \text{für } i = j \\ 0 & \text{für } 1 \leq i < j \leq n \end{cases}$$

Ein Maß für die Reduziertheit einer Gitterbasis sind die sogenannten sukzessiven Minima:

Definition 2.2 *Sei L ein Gitter vom Rang n. Für $i = 1, \cdots, n$ ist das i-te sukzessive Minimum von L definiert als*

$$\lambda_i(L) := \min_{\substack{c_1, \cdots, c_i \in L \\ lin.unabh.}} \Big\{ \max \{ \, \|c_1\|, \cdots, \|c_i\| \, \} \Big\}$$

$\lambda_i(L)$ ist die kleinste reelle Zahl $r > 0$, für die es i linear unabhängige Vektoren $c_j \in L$ gibt mit $\|c_j\| \leq r$ für $j = 1, \cdots, i$. Insbesondere ist $\lambda_1(L)$ die Länge des kürzesten, vom Nullvektor verschiedenen Gittervektors. Das Problem, zu einem gegebenen Gitter einen kürzesten, vom Nullvektor verschiedenen Gittervektor zu bestimmen, heißt das "kürzeste Gittervektorproblem". Das Problem, zu einem gegebenen Vektor einen nächsten Gittervektor zu bestimmen, heißt das "nächste Gittervektorproblem".
Gibt es eine Gitterbasis von L mit Vektoren, deren Längen gleich den sukzessiven Minima von L sind, so ist dies die am besten reduzierte Gitterbasis von L. Für $n = 2$ kann man immer eine solche Gitterbasis finden (siehe Satz 2.5). Da es für $n > 2$ i.a. keine solche Gitterbasis gibt, ist in diesem Fall das Ziel, eine Gitterbasis $b_1, \cdots, b_n$ zu finden, bei der die Größe $\|b_i\| \, / \, \lambda_i(L)$ für $i = 1, \cdots, n$ möglichst klein ist.

2.2 Gauß-Reduktion

Gitter vom Rang 2 wurden bereits von Gauß [5] untersucht. Er führte folgenden Reduktionsbegriff ein:

Definition 2.3 *Eine Gitterbasis b_1, b_2 heißt Gauß-reduziert, wenn gilt:*

a) $0 \leq \mu_{2,1} \leq \frac{1}{2}$,

b) $\|b_1\| \leq \|b_2\|$.

Man hat folgende alternative Definition der Gauß-Reduktion:

Bemerkung 2.4 *Eine Gitterbasis b_1, b_2 ist Gauß-reduziert*

$$\Leftrightarrow \|b_1\| \leq \|b_2\| \leq \|b_1 - b_2\| \leq \|b_1 + b_2\|.$$

Satz 2.5 [5] *Sei b_1, b_2 eine Gauß-reduzierte Basis eines Gitters L. Dann gilt:*

$$\|b_i\| = \lambda_i(L) \quad \textit{für } i = 1, 2.$$

Für Gitter vom Rang 2 ist also die Gauß-Reduktion die bestmögliche Reduktion.

Algorithmus 2.6 (Gauß'sches Reduktionsverfahren)

INPUT *Gitterbasis* $b_1, b_2 \in \mathbb{R}^m$

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

2 *IF* $\mu_{2,1} < 0$

THEN $b_2 := -b_2$

3 *IF* $\|b_1\| > \|b_2\|$

THEN Vertausche b_1, b_2

GOTO 1

OUTPUT *Gauß-reduzierte Gitterbasis* $b_1, b_2 \in \mathbb{R}^m$

Korrektheit: Nach Schritt 1 gilt:

$$|\mu_{2,1}^{neu}| \leq \tfrac{1}{2}.$$

Durch Schritt 1 wird im Fall $|\mu_{2,1}^{alt}| > \frac{1}{2}$ ein Basisvektor echt verkleinert, während der andere unverändert bleibt.
Nach Schritt 2 gilt:

$$0 \leq \mu_{2,1}^{neu} \leq \tfrac{1}{2}.$$

Nach Schritt 3 gilt:

$$\|b_1\| \leq \|b_2\|.$$

Falls in Schritt 3 b_1 und b_2 nicht ausgetauscht wurden, gilt auch:

$$0 \leq \mu_{2,1}^{neu} \leq \tfrac{1}{2}.$$

Somit ist die Ausgabebasis Gauß-reduziert. $\square$

Dieser Algorithmus ist eine Verallgemeinerung des zentrierten Euklidischen Algorithmus. Da er nach [14] ein Polynomialzeit-Algorithmus ist, kann man für Gitter vom Rang 2 die sukzessiven Minima in polynomialer Zeit berechnen.

2.3 Längenreduktion

Definition 2.7 *Eine Gitterbasis $b_1, \cdots, b_n$ heißt längenreduziert, wenn für die zugehörigen Gram-Schmidt-Koeffizienten gilt:*

$$|\mu_{i,j}| \leq \tfrac{1}{2} \quad \textit{für } 1 \leq j < i \leq n.$$

Für Rang 2 sind Gauß-reduzierte Gitterbasen längenreduziert.

Algorithmus 2.8 **(zur Längenreduktion)**

INPUT *Gitterbasis* $b_1, \cdots, b_n \in \mathbb{R}^m$

FOR $i = 2, \cdots, n$ *DO*

  FOR $j = i-1, \cdots, 1$ *DO*

    $b_i = b_i - \lceil \mu_{i,j} \rfloor \cdot b_j$

OUTPUT *längenreduzierte Gitterbasis* $b_1, \cdots, b_n \in \mathbb{R}^m$

Korrektheit: Nach jedem Reduktionsschritt gilt:

$$\mu_{i,l}^{neu} = \mu_{i,l}^{alt} - \lceil \mu_{i,j}^{alt} \rfloor \cdot \mu_{j,l} \quad \text{für } l = 1, \cdots, i-1.$$

Daraus folgt:

- $|\mu_{i,j}^{neu}| \leq \frac{1}{2}$,
- $\mu_{i,l}$ mit $l > j$ bleiben unverändert.

Am Ende des Verfahrens gilt somit für alle Gram-Schmidt-Koeffizienten:

$$|\mu_{i,j}| \leq \tfrac{1}{2} \quad \text{für } 1 \leq j < i \leq n. \quad \square$$

Bemerkung 2.9 *Bei einer Längenreduktion verändert sich das Orthogonalsystem $\hat{b}_1, \cdots, \hat{b}_n$ nicht.*

Da die Gittervektoren während der Reduktion nicht permutiert werden, wird der Vektor b_1 $(= \hat{b}_1)$ nicht verändert. Da auch die Höhen der Basisvektoren erhalten bleiben, ist die Längenreduktion ein schwacher Reduktionsbegriff.

2.4 L^3-Reduktion

1982 führten Lenstra, Lenstra, Lovász eine neue Reduktion ein, die L^3-Reduktion [8]. Außerdem entwickelten sie einen zugehörigen Polynomialzeit-Algorithmus. Dieser ist eine natürliche Erweiterung des Gauß'schen Reduktionsverfahrens 2.6 auf beliebigen Rang, da er Gauß-Reduktionsschritte auf zwei aufeinanderfolgenden Basisvektoren durchführt.

Definition 2.10 *Eine Gitterbasis $b_1, \cdots, b_n$ heißt L^3-reduziert (nach Lenstra, Lenstra und Lovász) mit δ ($\frac{1}{4} < \delta \leq 1$), wenn gilt:*

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

b) $\delta \cdot \|\hat{b}_{k-1}\|^2 \leq \|\hat{b}_k\|^2 + \mu_{k,k-1}^2 \cdot \|\hat{b}_{k-1}\|^2$ *für* $k = 2, \cdots, n$.

Bemerkung 2.11 **a)** *Je größer δ ist, desto stärker ist die L^3-Reduktion.*
b) *Für $k = 2$ ist Bedingung b) äquivalent zu $\delta \cdot \|b_1\|^2 \leq \|b_2\|^2$.*

Satz 2.12 [8] *(Lenstra, Lenstra, Lovász) Sei $b_1, \cdots, b_n$ eine Basis eines Gitters L, die L^3-reduziert mit δ ($\frac{1}{4} < \delta \leq 1$) ist. Dann gilt für $\alpha = \frac{1}{\delta - \frac{1}{4}}$:*

$$\frac{\|b_i\|}{\lambda_i(L)} \leq \alpha^{\frac{n-1}{2}} \quad \text{für } i = 1, \cdots, n.$$

Algorithmus 2.13 **(zur L^3-Reduktion)**

INPUT *Gitterbasis $b_1, \cdots, b_n \in \mathbb{R}^m$, δ mit $\frac{1}{4} < \delta < 1$*

1 $k = 2$ *(k ist die Stufe)*
Berechne $\mu_{i,j}$ für $1 \leq j < i \leq n$, $\|\hat{b}_i\|^2$ für $i = 1, \cdots, n$

2 *WHILE $k \leq n$ DO*
Längenreduziere b_k und korrigiere $\mu_{k,j}$ für $j = 1, \cdots, k-1$
IF $\delta \cdot \|\hat{b}_{k-1}\|^2 > \|\hat{b}_k\|^2 + \mu_{k,k-1}^2 \cdot \|\hat{b}_{k-1}\|^2$
THEN Vertausche b_{k-1}, b_k
$k = \max\{k-1, 2\}$
ELSE $k = k + 1$

OUTPUT *mit δ L^3-reduzierte Gitterbasis $b_1, \cdots, b_n \in \mathbb{R}^m$*

Korrektheit: Beim Eintritt in Stufe k ist die Gitterbasis $b_1, \cdots, b_{k-1}$ L^3-reduziert mit δ. Am Ende ist $k = n + 1$ und damit die gesamte Gitterbasis $b_1, \cdots, b_n$ L^3-reduziert mit δ. $\square$

Kommentare: 1. Nach jedem der $k - 1$ Reduktionsschritte $b_k = b_k - \lceil \mu_{k,j}^{alt} \rfloor \cdot b_j$ müssen die $\mu_{k,i}$ mit $i \leq j$ neu berechnet werden gemäß

$$\mu_{k,i}^{neu} = \mu_{k,i}^{alt} - \lceil \mu_{k,j}^{alt} \rfloor \cdot \mu_{j,i}$$

(siehe Korrektheitsbeweis zur Längenreduktion).

2. Bei einem Austausch $b_{k-1} \leftrightarrow b_k$ bleiben die $\hat{b}_i$ für $i \neq k-1,\ k$ unverändert, und somit müssen nur die $\|\hat{b}_{k-1}\|^2, \|\hat{b}_k\|^2,\ \mu_{i,l}$ für $l = k-1,\ k\,;\ i > l$ und $\mu_{l,i}$ für $l = k-1,\ k\,;\ i < l$ neu berechnet werden.

Der L^3-Algorithmus ist nach [8] ein Polynomialzeit-Algorithmus und approximiert somit die sukzessiven Minima in polynomialer Zeit bis auf einen (im Rang des Gitters) exponentiellen Faktor.

Kapitel 3

Ergebnisse von Seysen

In [13] wird ein neuer Reduktionsbegriff für Gitterbasen, die τ-Reduktion, eingeführt. Dieser Begriff ist über die Größe $\sigma(A)$ definiert, die sowohl von der Gram-Matrix der Gitterbasis als auch von der Gram-Matrix der dazu dualen Basis, also der inversen Gram-Matrix, abhängt. Im Gegensatz zur L^3-Reduktion ist die τ-Reduktion aber nicht algorithmisch motiviert, und es ist auch kein effizienter Algorithmus zur τ-Reduktion bekannt. In Abschnitt 3.1 fassen wir die Hauptergebnisse Seysens über die τ-Reduktion zusammmen. In Abschnitt 3.2 stellen wir eine geometrische Anwendung Seysens vor, die es ermöglicht, zwei für die Gittertheorie wichtige Teilmengen von span(L), die Voronoi-Zelle eines Gitters und die Basiszelle einer Gitterbasis, zu vergleichen.

3.1 Hauptergebnisse

Definition 3.1 *Sei* $A = (a_{s,t})_{1\le s,t\le n} \in GL_n(\mathbb{R})$ *und* $A^{-1} = (a^*_{s,t})_{1\le s,t\le n}$.

a) $\tau_s(A) := \sum_{t=1}^{n} |a_{s,t} \cdot a^*_{t,t}|$,

b) $\tau(A) := \max_{1\le s\le n} \{\tau_s(A)\}$,

c) $\sigma(A) := \tau(A) \cdot \tau(A^{-1})$.

Es gilt:

$$\begin{aligned} \sigma(A) &\geq 0, \\ \sigma(E_n) &= 1. \end{aligned}$$

In Satz 3.6 zeigen wir, daß für Gram-Matrizen von Gitterbasen gilt:

$$\sigma(A) \geq 1$$

und daß für Gram-Matrizen orthogonaler Gitterbasen gilt:

$$\sigma(A) = 1.$$

Definition 3.2 *Sei $b_1, \cdots, b_n$ eine Basis eines Gitters L mit Gram-Matrix A. $b_1, \cdots, b_n$ heißt τ-reduziert genau dann, wenn $\sigma(A)$ minimal für alle Gitterbasen von L ist.*

Bemerkung 3.3 *In [12] hatte Seysen bereits den Begriff der S-Reduktion eingeführt, der sich von der τ-Reduktion dadurch unterscheidet, daß $\sigma(A)$ durch die Größe*

$$S(A) := \sum_{i=1}^{n} a_{i,i} \cdot a_{i,i}^*$$

ersetzt wird. Viele der folgenden Ergebnisse und Beweistechniken sind von der S-Reduktion übertragen worden.

Aus der Diskretheit eines Gitters erhält man:

Fakt 3.4 *Jedes Gitter besitzt eine τ-reduzierte Gitterbasis.*

Für jede Gram-Matrix A gilt:

$$\sigma(A) = \tau(A) \cdot \tau(A^{-1}) = \tau(A^{-1}) \cdot \tau(A) = \sigma(A^{-1}).$$

Aus Satz 1.6b) schließt man:

Fakt 3.5 *Eine Gitterbasis ist genau dann τ-reduziert, wenn die dazu duale Basis τ-reduziert ist.*

Daß der Begriff der τ-Reduktion sinnvoll ist, zeigt folgender Satz:

Satz 3.6 *Sei $b_1, \cdots, b_n$ eine Gitterbasis mit Gram-Matrix A. Dann gilt:*

a) $\tau(A) = 1 \Leftrightarrow b_1, \cdots, b_n$ *ist orthogonal,*

b) $\tau(A^{-1}) = 1 \Leftrightarrow b_1, \cdots, b_n$ *ist orthogonal,*

c) $\tau(A), \tau(A^{-1}) \geq 1$.

Beweis: Seien A $= (a_{s,t})_{1 \leq s,t \leq n}$ und $A^{-1} = (a_{s,t}^*)_{1 \leq s,t \leq n}$, und sei $b_1^*, \cdots, b_n^*$ die duale Gitterbasis zu $b_1, \cdots, b_n$.

zu **a)** „$\Rightarrow$“: Sei $\tau(A) = 1$.

Annahme: $b_1, \cdots, b_n$ ist nicht orthogonal.

Dann gibt es i, j mit $1 \leq i \neq j \leq n$ und $< b_i, b_j > \neq 0$.

Sei $\epsilon_1 := | < b_i, b_j > | > 0$ und $\epsilon_2 := | < b_j^*, b_j^* > | > 0$.

Nach der Cauchy-Schwarz'schen Ungleichung (1.1) und Satz 1.6a),b) gilt:

$$\begin{aligned}\tau(A) &\geq \tau_i(A) \geq |a_{i,i} \cdot a^*_{i,i}| + |a_{i,j} \cdot a^*_{j,j}| \\ &= \|b_i\|^2 \cdot \|b_i^*\|^2 + | < b_i, b_j > | \cdot | < b_j^*, b_j^* > | \\ &\geq | < b_i, b_i^* > |^2 + \epsilon_1 \cdot \epsilon_2 = 1 + \epsilon_1 \cdot \epsilon_2 > 1 \quad \lightning \quad \text{zu } \tau(A) = 1\end{aligned}$$

Somit ist $b_1, \cdots, b_n$ orthogonal.

„$\Leftarrow$“: Sei $b_1, \cdots, b_n$ orthogonal. Dann gilt für $1 \leq s, t \leq n$:

$$a_{s,t} = < b_s, b_t > = \delta_{s,t} \cdot \|b_s\|^2$$

und damit

$$a^*_{s,t} = \delta_{s,t} \cdot \|b_s\|^{-2}.$$

Somit gilt:

$$\tau(A) = \max_{1 \leq s \leq n} \left\{ \sum_{t=1}^{n} |a_{s,t} \cdot a^*_{t,t}| \right\} = \max_{1 \leq s \leq n} \left\{ \sum_{t=1}^{n} |\delta_{s,t} \cdot \|b_s\|^2 \cdot \|b_t\|^{-2}| \right\} = 1.$$

zu **b)** Wendet man a) auf die duale Gitterbasis an, so ergibt sich:

$$\tau(A^{-1}) = 1 \Leftrightarrow b_1^*, \cdots, b_n^* \text{ ist orthogonal.}$$

Die Behauptung ergibt sich mit der Äquivalenz

$$b_1, \cdots, b_n \text{ ist orthogonal } \Leftrightarrow b_1^*, \cdots, b_n^* \text{ ist orthogonal,}$$

die daraus folgt, daß die Gram-Matrizen orthogonaler Gitterbasen immer Diagonalmatrizen sind und das Inverse einer Diagonalmatrix ebenfalls eine Diagonalmatrix ist.

zu **c)** Für $s = 1, \cdots, n$ gilt:

$$\tau(A) \geq \tau_s(A) \geq \|b_s\|^2 \cdot \|b_s^*\|^2 \geq 1,$$

$$\tau(A^{-1}) \geq \tau_s(A^{-1}) \geq \|b_s^*\|^2 \cdot \|b_s\|^2 \geq 1. \quad \square$$

$\sigma(A)$ ist also immer größer gleich Eins und gleich Eins genau dann, wenn die Gitterbasis orthogonal ist, so daß orthogonale Gitterbasen immer τ-reduziert sind. Daß die Größe $\sigma(A)$ dennoch kein Maß für die Orthogonalität einer Gitterbasis sein kann, zeigt folgendes Beispiel:

Beispiel 3.7 *Man betrachte die Gitterbasen*

$$b_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \quad b_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \quad b_3 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

und

$$b_1^{'} \;=\; b_1 \;=\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix},\;\; b_2^{'} \;=\; b_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix},\;\; b_3^{'} \;=\; b_3 - b_1 \;=\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

desselben Gitters. Die Gram-Matrizen zur ersten Gitterbasis sind:

$$A \;=\; \begin{pmatrix} 2 & -1 & 1 \\ -1 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix},\;\; A^{-1} \;=\; \frac{1}{4}\cdot\begin{pmatrix} 4 & 2 & -2 \\ 2 & 3 & -1 \\ -2 & -1 & 3 \end{pmatrix}.$$

Es folgt:

$$\sigma(A) \;=\; \tau(A)\cdot\tau(A^{-1}) \;=\; 3.5\cdot 4 \;=\; 14.$$

Die Gram-Matrizen zur zweiten Gitterbasis sind:

$$A^{'} \;=\; \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & 1 \\ -1 & 1 & 2 \end{pmatrix},\;\; A^{'-1} \;=\; \frac{1}{4}\cdot\begin{pmatrix} 3 & 1 & 1 \\ 1 & 3 & -1 \\ 1 & -1 & 3 \end{pmatrix}.$$

Es ergibt sich:

$$\sigma(A^{'}) \;=\; \tau(A^{'})\cdot\tau(A^{'-1}) \;=\; 3\cdot 2.5 \;=\; 7.5.$$

Somit gilt:

$$\sigma(A) \;>\; \sigma(A^{'}).$$

Andererseits erhält man:

$$\begin{aligned} |<b_1,b_2>| &= |<b_1^{'},b_2^{'}>|, \\ |<b_1,b_3>| &= |<b_1^{'},b_3^{'}>|, \\ |<b_2,b_3>| &< |<b_2^{'},b_3^{'}>|. \end{aligned}$$

Das folgende Theorem ist das Hauptergebnis der Arbeit [13].

Theorem 3.8 [13] *Zu jedem Gitter L gibt es eine Gitterbasis $b_1,\cdots,b_n$ mit dualer Gitterbasis $b_1^*,\cdots,b_n^*$, so daß gilt:*

$$|<b_i,b_j>|\cdot|<b_j^*,b_k^*>| = e^{O((\ln n)^2)} \quad \textit{für } 1\le i,j,k\le n.$$

Wir benötigen später folgendes Korollar, das besagt, daß man in jedem Gitter Basen mit kleinem $\sigma(A)$ finden kann.

Korollar 3.9 *Zu jedem Gitter L gibt es eine Gitterbasis $b_1, \cdots, b_n$ mit Gram-Matrix A, so daß gilt:*

$$\sigma(A) = e^{O((\ln n)^2)}.$$

Beweis: Sei $b_1, \cdots, b_n$ die Gitterbasis aus Theorem 3.8 und $b_1^*, \cdots, b_n^*$ die zugehörige duale Gitterbasis. Seien $A = (a_{s,t})_{1 \le s,t \le n}$ und $A^{-1} = (a_{s,t}^*)_{1 \le s,t \le n}$. Dann gilt nach Theorem 3.8:

$$\begin{aligned} \tau_s(A) &= \sum_{t=1}^{n} | \, a_{s,t} \cdot a_{t,t}^* | \\ &= \sum_{t=1}^{n} | < b_s, b_t > | \cdot | < b_t^*, b_t^* > | \\ &= e^{O((\ln n)^2)} \quad \text{für} \;\; s = 1, \cdots, n. \end{aligned}$$

Analog gilt:

$$\tau_s(A^{-1}) = e^{O((\ln n)^2)} \quad \text{für} \;\; s = 1, \cdots, n.$$

Nach Definition von $\tau(A)$ und $\tau(A^{-1})$ folgt:

$$\tau(A), \tau(A^{-1}) = e^{O((\ln n)^2)}.$$

Aus $\sigma(A) = \tau(A) \cdot \tau(A^{-1})$ folgt:

$$\sigma(A) = e^{O((\ln n)^2)}. \quad \square$$

Für die Einträge einer Transformationsmatrix aus $GL_n(\mathbb{Z})$, die eine gegebene Gitterbasis in eine andere gegebene Gitterbasis transformiert, ergeben sich folgende Schranken:

Theorem 3.10 [13] Seien $B = [b_1, \cdots, b_n]$ und $\bar{B} = [\bar{b}_1, \cdots, \bar{b}_n]$ zwei Basismatrizen desselben Gitters L, und sei $\bar{B} = B \cdot T$ für ein $T \in GL_n(\mathbb{Z})$. Seien $A, \bar{A} = (\bar{a}_{s,t})_{1 \le s,t \le n}$ die entsprechenden Gram-Matrizen, $A^{-1} = (a_{s,t}^*)_{1 \le s,t \le n}$ und $T = (t_{i,j})_{1 \le i,j \le n}$. Dann gilt für $1 \le i, j \le n$:

a) $t_{i,j}^2 \le a_{i,i}^* \cdot \bar{a}_{j,j}$,

b) $|t_{i,j}| \le \tau_i(A^{-1}) \cdot \tau_j(\bar{A})$.

3.2 Geometrische Bedeutung der τ-Reduktion

Definition 3.11 *Sei L ein Gitter mit Basismatrix $B = [b_1, \cdots, b_n]$.*

a) $V(L) := \left\{ x \in span(L) \;\middle|\; \forall\, y \in L : \|x\| \leq \|x - y\| \right\}$ *heißt Voronoi-Zelle von L,*

b) $C(B) := \left\{ \sum_{i=1}^{n} x_i \cdot b_i \;\middle|\; |x_i| \leq \frac{1}{2}\,, i = 1, \cdots, n \right\}$ *heißt Basiszelle der Gitterbasis $b_1, \cdots, b_n$.*

$V(L)$ enthält die Punkte aus span(L), die nicht weiter entfernt vom Nullpunkt als von jedem anderen Gitterpunkt liegen, und $C(B)$ ist die um $-\frac{1}{2} \cdot \sum_{i=1}^{n} b_i$ verschobene Grundmasche zur Gitterbasis $b_1, \cdots, b_n$. Während $V(L)$ nur vom Gitter L abhängt, hängt $C(B)$ von der speziellen Gitterbasis $b_1, \cdots, b_n$ ab. Die Gemeinsamkeit von Voronoi-Zelle und Basiszelle ist, daß für ein Gitter L mit Basismatrix B sowohl $\{y + V(L) \,|\, y \in L\}$ als auch $\{y + C(B) \,|\, y \in L\}$ die Menge span(L) ganz abdecken. Für ein Gitter L mit Basismatrix $B = [b_1, \cdots, b_n]$ zeigt man leicht folgende Äquivalenz:

$$b_1, \cdots, b_n \text{ ist orthogonal } \Leftrightarrow\; V(L) = C(B) \tag{3.1}$$

Mit Hilfe von $\tau(A)$ bzw. $\tau(A^{-1})$ kann man folgenden Zusammenhang zwischen der Basiszelle einer Gitterbasis und der Voronoi-Zelle des entsprechenden Gitters herstellen:

Theorem 3.12 [13] *Sei L ein Gitter mit Basismatrix B und zugehöriger Gram-Matrix A. Dann gilt:*

$$\frac{C(B)}{n \cdot \tau(A)} \;\subseteq\; V(L) \;\subseteq\; \tau(A^{-1}) \cdot C(B).$$

Beispiel 3.13 *Zur Veranschaulichung von Theorem 3.12 betrachte man das Gitter $L = L(b_1, b_2)$ mit*

$$b_1 \;= \begin{pmatrix} 3 \\ 0 \end{pmatrix}, \quad b_2 \;= \begin{pmatrix} 1 \\ 4 \end{pmatrix}.$$

Die Gram-Matrix zu dieser Gitterbasis ist:

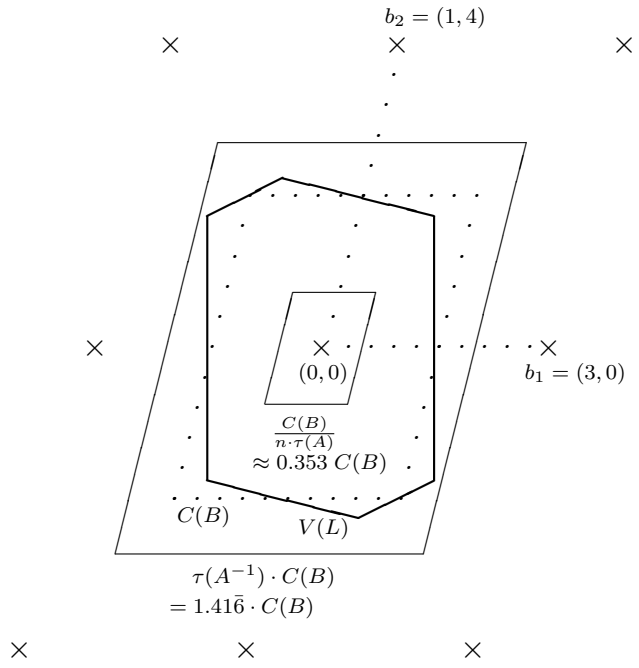
$$A \;=\; \begin{pmatrix} 9 & 3 \\ 3 & 17 \end{pmatrix}.$$

Mit

$$\det L \;=\; \sqrt{\det A} \;=\; 12$$

folgt:

$$\tau(A) \;=\; \tau(A^{-1}) \;=\; 1.41\bar{6} \text{ (vgl. Satz 5.5).}$$



$\sigma(A)$ ist somit ein Maß dafür, wie sehr Voronoi-Zelle und Basiszelle einer Gitterbasis voneinander abweichen. Nach (3.1) und Satz 3.6 stimmen im Fall $\sigma(A) = 1$ sogar Voronoi-Zelle und Basiszelle einer Gitterbasis überein, und nach Korollar 3.9 gibt es zu jedem Gitter eine Basis, bei der Voronoi-Zelle und Basiszelle höchstens um den Faktor

$$n \cdot \sigma(A) \;=\; e^{O((\ln n)^2)} \cdot e^{O((\ln n)^2)} \;=\; e^{O((\ln n)^2)}$$

voneinander abweichen.

Kapitel 4

τ-Reduktion für beliebigen Rang

In Abschnitt 4.1 zeigen wir, daß die τ-Reduziertheit einer Gitterbasis nicht von der Reihenfolge und den Vorzeichen der Basisvektoren abhängt. Diese Eigenschaft, die weder für Gauß-reduzierte noch für längenreduzierte noch für L^3-reduzierte Gitterbasen gilt, erlaubt es, die Basisvektoren während einer Reduktion beliebig zu permutieren. In Abschnitt 4.2 zeigen wir, daß τ-reduzierte Gitterbasen die sukzessiven Minima bis auf einen Faktor $e^{O((\ln n)^2)}$ approximieren. Abschließend geben wir in Abschnitt 4.3 (sehr ineffiziente) Algorithmen an, die eine Gitterbasis τ-reduzieren. Dabei benutzen wir Eigenschaften von Transformationsmatrizen aus $GL_n(\mathbb{Z})$, die eine gegebene Gitterbasis in eine τ-reduzierte transformieren. Zusätzlich geben wir eine obere Schranke für die Anzahl der notwendigen unimodularen Basistransformationen an.

4.1 Elementare Eigenschaften der τ-Reduktion

Für eine τ-Reduktion ist wichtig, wie sich die Größe $\sigma(A)$ bei den einfachsten unimodularen Basistransformationen, der Multiplikation eines Basisvektors mit -1 und dem Vertauschen zweier Basisvektoren, verhält. Nach folgendem Satz ist die Größe $\sigma(A)$ unabhängig von der Reihenfolge und den Vorzeichen der Basisvektoren.

Satz 4.1 *Sei $b_1, \cdots, b_n$ eine Gitterbasis mit Gram-Matrix A. Dann wird durch folgende Basistransformationen die Größe $\sigma(A)$ nicht verändert:*

- **a)** *Multiplikation des i-ten Basisvektors mit -1 für $1 \leq i \leq n$,*
- **b)** *Vertauschen des i-ten und des j-ten Basisvektors für $1 \leq i \neq j \leq n$.*

Beweis: Sei $b_1^*, \cdots, b_n^*$ die duale Basis zu $b_1, \cdots, b_n$, und seien $A = (a_{s,t})_{1 \leq s,t \leq n}$ und $A^{-1} = (a_{s,t}^*)_{1 \leq s,t \leq n}$.
zu **a)** Sei $\bar{B}$ die neue Basismatrix. Dann gilt:

$$\bar{B} = [b_1, \cdots, b_{i-1}, -b_i, b_{i+1}, \cdots, b_n].$$

Nach Satz 1.6a) folgt für die neue duale Basismatrix:

$$\bar{B}^* = [b_1^*, \cdots, b_{i-1}^*, -b_i^*, b_{i+1}^*, \cdots, b_n^*].$$

Für die neuen Gram-Matrizen $\bar{A} = (\bar{a}_{s,t})_{1\le s,t\le n}$ bzw. $\bar{A}^{-1} = (\bar{a}^*_{s,t})_{1\le s,t\le n}$ gilt somit:

$$|\bar{a}_{s,t}| = |a_{s,t}| \text{ bzw. } |\bar{a}^*_{s,t}| = |a^*_{s,t}| \text{ für } 1 \le s,t \le n.$$

Da in die Größe $\sigma(A)$ nur die Beträge der Einträge von A und A^{-1} eingehen, folgt:

$$\sigma(A) = \sigma(\bar{A}).$$

zu **b)** Sei $\tilde{B}$ die neue Basismatrix. Dann gilt:

$$\tilde{B} = [b_1, \cdots, b_{i-1}, b_j, b_{i+1}, \cdots, b_{j-1}, b_i, b_{j+1}, \cdots, b_n].$$

Nach Satz 1.6a) folgt für die neue duale Basismatrix:

$$\tilde{B}^* = [b_1^*, \cdots, b_{i-1}^*, b_j^*, b_{i+1}^*, \cdots, b_{j-1}^*, b_i^*, b_{j+1}^*, \cdots, b_n^*].$$

Sei $\pi : \{1, \cdots, n\} \to \{1, \cdots, n\}$ die Transposition (i, j), d.h.

$$\pi(s) := \begin{cases} i & \text{für } s = j \\ j & \text{für } s = i \\ s & \text{sonst} \end{cases}$$

Für die neuen Gram-Matrizen $\tilde{A} = (\tilde{a}_{s,t})_{1\le s,t\le n}$ bzw. $\tilde{A}^{-1} = (\tilde{a}^*_{s,t})_{1\le s,t\le n}$ ergibt sich:

$$\tilde{a}_{s,t} = a_{\pi(s),\pi(t)} \text{ bzw. } \tilde{a}^*_{s,t} = a^*_{\pi(s),\pi(t)} \text{ für } 1 \le s,t \le n.$$

Es folgt:

$$\tau_s(\tilde{A}) = \tau_{\pi(s)}(A) \text{ bzw. } \tau_s(\tilde{A}^{-1}) = \tau_{\pi(s)}(A^{-1}) \text{ für } 1 \le s \le n.$$

Somit erhält man:

$$\begin{aligned} \sigma(A) &= \max_{1\le s\le n}\{\tau_s(A)\} \cdot \max_{1\le s\le n}\{\tau_s(A^{-1})\} \\ &= \max_{1\le s\le n}\{\tau_s(\tilde{A})\} \cdot \max_{1\le s\le n}\{\tau_s(\tilde{A}^{-1})\} \\ &= \sigma(\tilde{A}). \quad \square \end{aligned}$$

Untersucht man die Größe $\sigma(A)$, kann man somit die Basisvektoren beliebig permutieren und z.B. bzgl. der Euklidischen Norm ordnen. Dies stellt einen großen

Unterschied zur L^3-Reduktion dar, bei der der erste Basisvektor i.a. wesentlich kürzer als der letzte ist. Dies legt die Vermutung nahe, daß die τ-Reduktion hilfreicher ist, wenn man eine Gitterbasis sucht, die aus kurzen Vektoren besteht, während die L^3-Reduktion bei der Suche nach einem kürzesten Gittervektor besser ist. Zur Berechnung eines kürzesten Gittervektors kann man die τ-Reduktion als Vorreduktion der L^3-Reduktion benutzen, da sie die Basisvektoren gleichmäßig reduziert (vgl. Abschnitt 6.4).

4.2 Approximation der sukzessiven Minima

Um den Begriff der τ-Reduktion mit anderen Reduktionsbegriffen vergleichen zu können, untersuchen wir, wie gut die sukzessiven Minima durch eine τ-reduzierte Gitterbasis approximiert werden.
Einen Zusammenhang zwischen den sukzessiven Minima eines Gitters und des dazu dualen Gitters stellt folgendes Lemma her.

Lemma 4.2 [6] *Sei L ein Gitter und L^* das dazu duale Gitter. Dann gilt:*

$$1 \leq \lambda_i(L) \cdot \lambda_{n+1-i}(L^*) \quad \textit{für } i = 1, \cdots, n.$$

Für eine beliebige Gitterbasis und deren duale Gitterbasis ergeben sich folgende obere und untere Schranken, abhängig von den sukzessiven Minima des Gitters.

Satz 4.3 *Sei L ein Gitter mit Gitterbasis $b_1, \cdots, b_n$ und zugehöriger Gram-Matrix A, und sei $L^* = L(b_1^*, \cdots, b_n^*)$ das dazu duale Gitter. Außerdem gelte: $\|b_j\| \geq \|b_i\|$ für $j \geq i$. Sei $\xi := \min\{\tau(A), \tau(A^{-1})\}$. Dann gilt für $i = 1, \cdots, n$:*

a) $\lambda_i(L) \leq \|b_i\|$,

b) $\|b_i\| \leq \xi \cdot \lambda_i(L)$,

c) $\dfrac{1}{\sqrt{\xi} \cdot \lambda_i(L)} \leq \|b_i^*\|$,

d) $\|b_i^*\| \leq \dfrac{\sqrt{\xi}}{\lambda_i(L)}$.

Beweis: In [12] wurde ein ähnliches Resultat für die Größe $S(A)$ gezeigt, dessen Beweis man hierauf übertragen kann.
Seien $A = (a_{s,t})_{1 \leq s,t \leq n}$ und $A^{-1} = (a^*_{s,t})_{1 \leq s,t \leq n}$. Für $i = 1, \cdots, n$ gilt:

$$\tau(A) \geq \tau_i(A) \geq |a_{i,i} \cdot a^*_{i,i}| = |b_i\|^2 \cdot \|b_i^*\|^2 \tag{4.1}$$

Analog gilt für $i = 1, \cdots, n$:

$$\tau(A^{-1}) \geq \|b_i\|^2 \cdot \|b_i^*\|^2 \tag{4.2}$$

zu **a)** Gilt wegen $\|b_j\| \geq \|b_i\|$ für $j \geq i$ und nach Definition der sukzessiven Minima.

zu **d)** Nach (4.1), (4.2) gilt:

$$\|b_i^*\| \;\leq\; \frac{\sqrt{\xi}}{\|b_i\|} \;\overset{a)}{\leq}\; \frac{\sqrt{\xi}}{\lambda_i(L)} \quad \text{für } i = 1, \cdots, n.$$

zu **c)** Es gilt:

$$\max_{i \leq j \leq n} \left\{ \|b_j^*\|^2 \right\} \;\leq\; \max_{i \leq j \leq n} \left\{ \frac{\xi}{\|b_j\|^2} \right\} \;\leq\; \frac{\xi}{\|b_i\|^2} \;\overset{(1.1)}{\leq}\; \xi \cdot \|b_i^*\|^2 \quad \text{für } i = 1, \cdots, n.$$

Somit ergibt sich:

$$\|b_i^*\| \;\geq\; \frac{\max\limits_{i \leq j \leq n} \left\{ \|b_j^*\| \right\}}{\sqrt{\xi}} \;\geq\; \frac{\lambda_{n+1-i}(L^*)}{\sqrt{\xi}} \;\overset{L\,4.2}{\geq}\; \frac{1}{\sqrt{\xi} \cdot \lambda_i(L)} \quad \text{für } i = 1, \cdots, n.$$

zu **b)** Es gilt:

$$\|b_i\| \;\leq\; \frac{\sqrt{\xi}}{\|b_i^*\|} \;\overset{c)}{\leq}\; \lambda_i(L) \cdot \sqrt{\xi}^2 \;=\; \xi \cdot \lambda_i(L) \quad \text{für } i = 1, \cdots, n. \quad \square$$

Wendet man Satz 4.3 auf die duale Gitterbasis an, so erhält man obere und untere Schranken, abhängig von den sukzessiven Minima des dualen Gitters. Da A^{-1} die Gram-Matrix der dualen Gitterbasis ist, erhält man diese Schranken, indem man in den Aussagen a), b), c), d) $\lambda_i(L)$ durch $\lambda_i(L^*)$, b_i durch b_i^* und b_i^* durch b_i ersetzt.

Für die Approximation der sukzessiven Minima einer τ-reduzierten Gitterbasis gilt:

Korollar 4.4 *Sei $b_1, \cdots, b_n$ eine τ-reduzierte Basis eines Gitters L, wobei $\|b_j\| \geq \|b_i\|$ für $j \geq i$. Dann gilt:*

$$\frac{\|b_i\|}{\lambda_i(L)} = e^{O((\ln n)^2)} \quad \textit{für } i = 1, \cdots, n.$$

Beweis: Nach Korollar 3.9 gibt es eine Basis $\bar{b}_1, \cdots, \bar{b}_n$ von L mit Gram-Matrix $\bar{A}$, so daß gilt:

$$\sigma(\bar{A}) = e^{O((\ln n)^2)}.$$

Sei A die Gram-Matrix zu $b_1, \cdots, b_n$. Dann folgt:

$$\frac{\|b_i\|}{\lambda_i(L)} \;\overset{S\,4.3b)}{\leq}\; \tau(A) \;\leq\; \sigma(A) \;\overset{Vor.}{\leq}\; \sigma(\bar{A}) \;=\; e^{O((\ln n)^2)} \quad \text{für } i = 1, \cdots, n. \quad \square$$

Man sieht, daß τ-reduzierte Gitterbasen eine schärfere Worst-Case-Schranke für die Approximation der sukzessiven Minima liefern als L^3-reduzierte Gitterbasen (vgl. Satz 2.12):

	L^3-reduziert mit δ	τ-reduziert
$b_i/\lambda_i(L)$	$\left(\frac{1}{\delta-\frac{1}{4}}\right)^{\frac{n-1}{2}}$	$e^{O((\ln n)^2)}$

Zur τ-Reduktion sind allerdings bis jetzt keine Polynomialzeit-Algorithmen bekannt. Im nächsten Abschnitt stellen wir Algorithmen zur τ-Reduktion vor, deren Laufzeit exponentiell in der Bitlänge der Eingabe ist.

4.3 Algorithmen zur τ-Reduktion

Um einen Algorithmus zur τ-Reduktion zu erhalten, zeigt man zunächst, daß es zu einem vorgegebenen Gitter nur endlich viele Gitterbasen gibt, deren Größe $\sigma(A)$ unter einer festen Schranke $x \in \mathbb{R}_+$ liegt. Dazu wird folgendes Lemma benötigt:

Lemma 4.5 *Sei $A \in \mathbb{R}^{n,n}$ Gram-Matrix einer Gitterbasis $b_1, \cdots, b_n \in \mathbb{R}^m$ und $T \in \mathbb{R}^{n,n}$. Dann gilt:*

$$tr(T^T \cdot A \cdot T) \cdot tr(A^{-1}) \;\geq\; \|T\|^2.$$

Beweis: Sei $B = [b_1, \cdots, b_n] \in \mathbb{R}^{m,n}$.
Man braucht folgende Beziehung, die für beliebige Matrizen $C = (c_{s,t})_{1\leq s\leq m,\, 1\leq t\leq n}$ gilt:

$$\mathrm{tr}(C^T \cdot C) \;=\; \sum_{t=1}^{n} \Big(\sum_{s=1}^{m} c_{s,t}^2 \Big) \;=\; \|C\|^2.$$

Daraus folgt:

$$\begin{aligned}
\mathrm{tr}(T^T \cdot A \cdot T) \cdot \mathrm{tr}(A^{-1}) &= \mathrm{tr}((B\cdot T)^T \cdot B \cdot T) \cdot \mathrm{tr}((B \cdot A^{-1})^T \cdot B \cdot A^{-1}) \\
&= \|B \cdot T\|^2 \cdot \|B \cdot A^{-1}\|^2 \\
&= (\, \|(A^{-1})^T \cdot B^T\| \cdot \|B \cdot T\| \,)^2 \\
&\overset{(1.2)}{\geq} \|A^{-1} \cdot A \cdot T\|^2 \\
&= \|T\|^2. \quad \square
\end{aligned}$$

Satz 4.6 *Sei L ein Gitter, und sei $x \in \mathbb{R}_+$ beliebig. Dann wird jede der drei folgenden Bedingungen nur von endlich vielen Basismatrizen $\bar{B}$ von L mit Gram-Matrix $\bar{A}$ erfüllt:*

a) $\tau(\bar{A}) \leq x$,

b) $\tau(\bar{A}^{-1}) \leq x$,

c) $\sigma(\bar{A}) \leq x$.

Beweis: Die Beweisidee stammt wiederum aus [12].

zu **c)** Folgt mit $\sigma(\bar{A}) = \tau(\bar{A}) \cdot \tau(\bar{A}^{-1})$ aus a) und b).

zu **a)** bzw. **b)** Sei $b_1, \cdots, b_n$ eine beliebige Gitterbasis von L und $B = [b_1, \cdots, b_n]$. Sei $L^* = L(b_1^*, \cdots, b_n^*)$ das zu L duale Gitter und A und $A^{-1} = (a^*_{s,t})_{1 \leq s,t \leq n}$ die zugehörigen Gram-Matrizen. Wegen Satz 4.1b) kann man $b_1, \cdots, b_n$ o.B.d.A. so wählen, daß $\|b_j\| \geq \|b_i\|$ für $j \geq i$ gilt.
Sei $T \in GL_n(\mathbb{Z})$ fest, so daß für die Basismatrix $\bar{B} := B \cdot T = [\bar{b}_1, \cdots, \bar{b}_n]$ mit Gram-Matrix $\bar{A} = (\bar{a}_{s,t})_{1 \leq s,t \leq n}$ gilt:

$$\tau(\bar{A}) \leq x \text{ bzw. } \tau(\bar{A}^{-1}) \leq x.$$

Es folgt:

$$\begin{aligned}
|T\|^2 &\overset{L\,4.5}{\leq} \operatorname{tr}(T^T \cdot A \cdot T) \cdot \operatorname{tr}(A^{-1}) \\
&= \sum_{s=1}^{n} \bar{a}_{s,s} \cdot \sum_{s=1}^{n} a^*_{s,s} \\
&= \sum_{s=1}^{n} \|\bar{b}_s\|^2 \cdot \sum_{s=1}^{n} \|b_s^*\|^2 \\
&\overset{S\,4.3\,b),\,d)}{\leq} \sum_{s=1}^{n} \min\left\{\tau(\bar{A})^2, \tau(\bar{A}^{-1})^2\right\} \cdot \lambda_s(L)^2 \cdot \sum_{s=1}^{n} \min\left\{\tau(A), \tau(A^{-1})\right\} \cdot \frac{1}{\lambda_s(L)^2} \\
&\leq \min\left\{\tau(\bar{A})^2, \tau(\bar{A}^{-1})^2\right\} \cdot \min\left\{\tau(A), \tau(A^{-1})\right\} \cdot \sum_{s=1}^{n} \lambda_n(L)^2 \cdot \sum_{s=1}^{n} \frac{1}{\lambda_1(L)^2}.
\end{aligned}$$

Daraus erhält man:

$$|T\| \leq \min\left\{\tau(\bar{A}), \tau(\bar{A}^{-1})\right\} \cdot \sqrt{\min\left\{\tau(A), \tau(A^{-1})\right\}} \cdot n \cdot \frac{\lambda_n(L)}{\lambda_1(L)}.$$

Mit den Abschätzungen

$$\begin{aligned}
\lambda_n(L) &\leq \sqrt{\max_{1 \leq s \leq n}\{a_{s,s}\}}, \\
\frac{1}{\lambda_1(L)} &\overset{L\,4.2}{\leq} \lambda_n(L^*) \leq \sqrt{\max_{1 \leq s \leq n}\{a^*_{s,s}\}}
\end{aligned}$$

erhält man:

$$\|T\| \;\leq\; \min\left\{\tau(\bar{A}), \tau(\bar{A}^{-1})\right\} \cdot n \cdot \sqrt{\min\{\tau(A), \tau(A^{-1})\} \cdot \max_{1\leq s\leq n}\{a_{s,s}\} \cdot \max_{1\leq s\leq n}\{a^*_{s,s}\}} \tag{4.3}$$

Nach Voraussetzung folgt mit

$$c_A := n \cdot \sqrt{\min\{\tau(A), \tau(A^{-1})\} \cdot \max_{1\leq s\leq n}\{a_{s,s}\} \cdot \max_{1\leq s\leq n}\{a^*_{s,s}\}}:$$

$$\|T\| \;\leq\; c_A \cdot x.$$

Die Einträge von $T \in GL_n(\mathbb{Z})$ können somit in **a)** bzw. **b)** nur endlich viele Werte annehmen, d.h. es gibt nur endlich viele Gitterbasen, die **a)** bzw. **b)** erfüllen. □

Aus Theorem 3.10b) und dem Beweis zu Satz 4.6 ergeben sich Schranken für die Einträge von Transformationsmatrizen aus $GL_n(\mathbb{Z})$, die eine gegebene Gitterbasis in eine τ-reduzierte transformieren.

Satz 4.7 *Sei L ein Gitter mit Basismatrix $B = [b_1, \cdots, b_n]$, zugehöriger Gram-Matrix $A = (a_{s,t})_{1\leq s,t\leq n}$ und $A^{-1} = (a^*_{s,t})_{1\leq s,t\leq n}$. Sei $T \in GL_n(\mathbb{Z})$, so daß für $\bar{B} := B \cdot T$ mit Gram-Matrix $\bar{A}$ gilt:*

$$\sigma(\bar{A}) \leq \sigma(A).$$

Dann folgt:

a) $\|T\|_\infty \;\leq\; \tau(A^{-1}) \cdot \sigma(A)$,

b) $\|T\|_\infty \;\leq\; \|T\| \;\leq\; n \cdot \sqrt{\sigma(A) \cdot \min\{\tau(A), \tau(A^{-1})\} \cdot \max_{1\leq s\leq n}\{a_{s,s}\} \cdot \max_{1\leq s\leq n}\{a^*_{s,s}\}}$.

Insbesondere gelten a) und b) für Matrizen $T \in GL_n(\mathbb{Z})$, so daß $\bar{B} := B \cdot T$ τ-reduziert ist.

Beweis: zu **a)** Nach Theorem 3.10b) gilt für $T = (t_{i,j})_{1\leq i,j\leq n}$:

$$\begin{aligned} |t_{i,j}| &\leq \tau_i(A^{-1}) \cdot \tau_j(\bar{A}) \\ &\leq \tau(A^{-1}) \cdot \tau(\bar{A}) \\ &\leq \tau(A^{-1}) \cdot \sigma(\bar{A}) \\ &\leq \tau(A^{-1}) \cdot \sigma(A) \quad \text{für } 1 \leq i,j \leq n. \end{aligned}$$

Es folgt:

$$\|T\|_\infty \;\leq\; \tau(A^{-1}) \cdot \sigma(A).$$

zu **b)** Offensichtlich gilt:

$$\|T\|_\infty \leq \|T\|.$$

Weiter gilt nach (4.3):

$$\|T\| \;\leq\; \min\left\{\tau(\bar{A}), \tau(\bar{A}^{-1})\right\} \cdot n \cdot \sqrt{\min\{\tau(A), \tau(A^{-1})\} \cdot \max_{1\leq s\leq n}\{a_{s,s}\} \cdot \max_{1\leq s\leq n}\{a^*_{s,s}\}}.$$

Mit der Abschätzung

$$\min\left\{\tau(\bar{A}), \tau(\bar{A}^{-1})\right\} \;\leq\; \sqrt{\sigma(\bar{A})} \;\leq\; \sqrt{\sigma(A)}$$

erhält man:

$$\|T\| \;\leq\; n \cdot \sqrt{\sigma(A) \cdot \min\{\tau(A), \tau(A^{-1})\} \cdot \max_{1\leq s\leq n}\{a_{s,s}\} \cdot \max_{1\leq s\leq n}\{a^*_{s,s}\}}. \quad \square$$

Bemerkung 4.8 *Aus Satz 4.7a) bzw. 4.7b) ergeben sich direkt Algorithmen zur τ-Reduktion, indem man jeweils die endlich vielen Transformationsmatrizen, die die Bedingungen aus Satz 4.7a) bzw. 4.7b) erfüllen, von rechts mit der gegebenen Gitterbasis multipliziert und somit eine τ-reduzierte Gitterbasis erhält.*

Eine obere Schranke für die Schritte, die zu einer τ-reduzierten Gitterbasis führen, ergibt sich aus folgendem Korollar:

Korollar 4.9 *Sei L ein Gitter mit Gitterbasis $b_1, \cdots, b_n$ und zugehöriger Gram-Matrix A. Dann findet man nach höchstens*

$$\Big(\frac{n! \cdot \|A\|^n_\infty}{\det A}\Big)^{2n^2} \cdot \min\Big\{n^{\frac{1}{2}n^2}, \Big(\frac{n! \cdot \|A\|^n_\infty}{\det A}\Big)^{n^2}\Big\}$$

unimodularen Basistransformationen eine τ-reduzierte Gitterbasis (für ganzzahlige Gitter kann man $\det A$ *durch 1 abschätzen).*

Beweis: Seien $B = [b_1, \cdots, b_n], A = (a_{s,t})_{1\leq s,t\leq n}$ und $A^{-1} = (a^*_{s,t})_{1\leq s,t\leq n}$. Dann gilt:

$$\tau(A) \;=\; \max_{1\leq s\leq n}\Big\{\sum_{t=1}^{n} |a_{s,t} \cdot a^*_{t,t}|\Big\} \;\leq\; n \cdot \|A\|_\infty \cdot \|A^{-1}\|_\infty \tag{4.4}$$

Analog gilt:

$$\tau(A^{-1}) \;\leq\; n \cdot \|A\|_\infty \cdot \|A^{-1}\|_\infty \tag{4.5}$$

Nach (1.3) gilt:

$$A^{-1} = \Big((-1)^{s+t} \cdot \frac{\det A'_{t,s}}{\det A}\Big)_{1\leq s,t\leq n}.$$

Da $\det A'_{t,s}$ nach Definition der Determinante aus $(n-1)!$ Summanden besteht, die jeweils aus $n-1$ Faktoren $a_{s,t}$ bestehen, folgt:

$$\|A^{-1}\|_\infty \leq \frac{(n-1)! \cdot \|A\|_\infty^{n-1}}{\det A} \tag{4.6}$$

Für eine Matrix T $\in GL_n(\mathbb{Z})$, so daß $\bar{B} := B \cdot T$ τ-reduziert ist, gilt nach Satz 4.7a) bzw. b):

$$\|T\|_\infty \leq \tau(A^{-1}) \cdot \sigma(A)$$

bzw.

$$\|T\|_\infty \leq n \cdot \sqrt{\sigma(A) \cdot \min\{\tau(A), \tau(A^{-1})\} \cdot \max_{1 \leq s \leq n}\{a_{s,s}\} \cdot \max_{1 \leq s \leq n}\{a^*_{s,s}\}}.$$

Nach (4.4), (4.5), (4.6) folgt:

$$\|T\|_\infty \leq (n \cdot \|A\|_\infty \cdot \|A^{-1}\|_\infty)^3 \leq \left(\frac{n! \cdot \|A\|_\infty^n}{\det A}\right)^3$$

bzw.

$$\|T\|_\infty \leq n \cdot n^{\frac{3}{2}} \cdot \|A\|_\infty^2 \cdot \|A^{-1}\|_\infty^2 \leq n^{\frac{1}{2}} \cdot \left(\frac{n! \cdot \|A\|_\infty^n}{\det A}\right)^2.$$

Da T n^2 Einträge hat, folgt die Behauptung. $\square$

Kapitel 5

τ-Reduktion für Rang 2

Gitter vom Rang 2 sind ein wichtiger Spezialfall der Gittertheorie, da die Gauß-Reduktion und die L^3-Reduktion zusammenfallen. Das Hauptergebnis aus 5.1 besagt, daß in diesem wichtigen Spezialfall auch die τ-Reduktion mit zwei Reduktionsbegriffen identisch ist, nämlich der Gauß-Reduktion und der τ_2-Reduktion. Dabei ist die τ_2-Reduktion eine algorithmisch motivierte Verallgemeinerung der τ-Reduktion, die die Größe $\sigma(A)$ verkleinert, aber nicht unbedingt minimiert. Wir zeigen in Abschnitt 5.2, daß für Rang 2 der τ-Reduktionsbegriff einfacher wird. Mit Hilfe dieser Vereinfachung beweisen wir in den Abschnitten 5.3 und 5.4 das Hauptergebnis.

5.1 Hauptergebnis

Definition 5.1 *Sei $b_1, \cdots, b_n$ eine Gitterbasis mit Gram-Matrix A. $b_1, \cdots, b_n$ heißt τ_2-reduziert genau dann, wenn durch keine Basistransformation der Form $b_j := b_j + k \cdot b_i$ mit $1 \leq i \neq j \leq n$ und $k \in \mathbb{Z}$ die Größe $\sigma(A)$ erniedrigt wird.*

Wir zeigen:

Satz 5.2 *Für Gitter vom Rang 2 gilt:*

a) *Die τ-Reduktion entspricht bis auf Reihenfolge und Vorzeichen der Basisvektoren der Gauß-Reduktion,*

b) *Die τ-Reduktion entspricht der τ_2-Reduktion.*

Beide Aussagen des Satzes 5.2 sind nicht auf Rang 3 verallgemeinerbar:

Beispiel 5.3 *Daß Aussage a) für Rang 3 nicht mehr gilt, wenn die Gauß-Reduktion durch die L^3-Reduktion mit $\delta = 1$ ersetzt wird, sieht man an den Gitterbasen*

$$b_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \quad b_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \quad b_3 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

und

$$b_1' \;=\; b_1 \;=\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix},\;\; b_2' \;=\; b_2 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix},\;\; b_3' \;=\; b_3 - b_1 \;=\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

desselben Gitters (vgl. Beispiel 3.7). Man zeigt leicht, daß die erste Gitterbasis L^3-reduziert mit $\delta = 1$ ist, wobei $\sigma(A) = 14$. Für die zweite Gitterbasis gilt: $\sigma(A') = 7.5$. Somit ist die erste Gitterbasis L^3-reduziert mit $\delta = 1$, aber nicht τ-reduziert.

Beispiel 5.4 *Um Aussage b) für $n = 3$ zu widerlegen, betrachte man die Gitterbasen*

$$b_1 \;=\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix},\;\; b_2 \;=\begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix},\;\; b_3 \;=\begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$$

und

$$b_1' \;=\; b_1 \;=\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix},\;\; b_2' \;=\; b_2 \;=\begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix},\;\; b_3' \;=\; b_3 - b_1 - b_2 \;=\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

desselben Gitters. Die Gram-Matrizen zur ersten Gitterbasis sind:

$$A \;=\begin{pmatrix} 2 & -1 & 1 \\ -1 & 2 & 1 \\ 1 & 1 & 5 \end{pmatrix},\;\; A^{-1} \;=\; \frac{1}{9}\cdot\begin{pmatrix} 9 & 6 & -3 \\ 6 & 9 & -3 \\ -3 & -3 & 3 \end{pmatrix}.$$

Es folgt:

$$\sigma(A) \;=\; \tau(A)\cdot\tau(A^{-1}) \;=\; 3\tfrac{2}{3}\cdot 5 \;=\; 18\tfrac{1}{3}.$$

Die Gram-Matrizen zur zweiten Gitterbasis sind:

$$A' \;=\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix},\;\; A'^{-1} \;=\; \frac{1}{9}\cdot\begin{pmatrix} 6 & 3 & 0 \\ 3 & 6 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Man erhält:

$$\sigma(A') \;=\; \tau(A')\cdot\tau(A'^{-1}) \;=\; 2\cdot 2 \;=\; 4.$$

Mit Algorithmus 6.3 zeigt man, daß die erste Gitterbasis τ_2-reduziert ist. Wegen $\sigma(A') < \sigma(A)$ ist sie aber nicht τ-reduziert.

In Abschnitt 6.2 wird ein Algorithmus vorgestellt, der eine τ_2-Reduktion und damit für $n = 2$ eine τ-Reduktion effizient durchführt.

5.2 Vereinfachung des Reduktionsbegriffes

Im Fall $n = 2$ ergeben sich einfache Schreibweisen für die Gram-Matrix einer Gitterbasis und die inverse Gram-Matrix. Daraus ergeben sich auch einfache Schreibweisen für die Größen $\tau(A)$ und $\tau(A^{-1})$. Der nächste Satz zeigt, daß dann $\tau(A)$ und $\tau(A^{-1})$ sogar gleich sind.

Satz 5.5 *Sei L ein Gitter mit Gitterbasis b_1, b_2 und zugehöriger Gram-Matrix $A = (a_{s,t})_{1\le s,t\le 2}$. Dann gilt:*

$$\tau(A) = \tau(A^{-1}) = \frac{1}{\det^2 L} \cdot (a_{1,1} \cdot a_{2,2} + |a_{2,1}| \cdot \max\{a_{1,1}, a_{2,2}\}).$$

Beweis: Sei $A^{-1} = (a^*_{s,t})_{1\le s,t\le 2}$. Dann gilt:

$$\begin{aligned} A^{-1} &= \begin{pmatrix} a_{2,2} & -a_{2,1} \\ -a_{2,1} & a_{1,1} \end{pmatrix} \cdot \frac{1}{a_{1,1} \cdot a_{2,2} - a_{2,1}^2} \\ &\overset{S\,1.4}{=} \begin{pmatrix} a_{2,2} & -a_{2,1} \\ -a_{2,1} & a_{1,1} \end{pmatrix} \cdot \frac{1}{\det^2 L}. \end{aligned}$$

Es folgt:

$$\begin{aligned} \tau(A) &= \max\left\{|a_{1,1} \cdot a^*_{1,1}| + |a_{1,2} \cdot a^*_{2,2}|, |a_{2,1} \cdot a^*_{1,1}| + |a_{2,2} \cdot a^*_{2,2}|\right\} \\ &= \max\left\{\left|a_{1,1} \cdot \frac{a_{2,2}}{\det^2 L}\right| + \left|a_{2,1} \cdot \frac{a_{1,1}}{\det^2 L}\right|, \left|a_{2,1} \cdot \frac{a_{2,2}}{\det^2 L}\right| + \left|a_{2,2} \cdot \frac{a_{1,1}}{\det^2 L}\right|\right\} \\ &= \frac{1}{\det^2 L} \cdot (a_{1,1} \cdot a_{2,2} + |a_{2,1}| \cdot \max\{a_{1,1}, a_{2,2}\}). \end{aligned}$$

Analog folgt:

$$\tau(A^{-1}) = \frac{1}{\det^2 L} \cdot (a_{1,1} \cdot a_{2,2} + |a_{2,1}| \cdot \max\{a_{1,1}, a_{2,2}\}). \quad \square$$

Der Begriff der τ-Reduktion vereinfacht sich für $n = 2$:

Korollar 5.6 *Sei L ein Gitter mit Gitterbasis b_1, b_2 und zugehöriger Gram-Matrix A. Dann ist b_1, b_2 genau dann τ-reduziert, wenn $\tau(A)$ minimal für alle Gitterbasen von L ist.*

Beweis: Folgt aus der Definition der τ-Reduktion und aus Satz 5.5. $\square$

Würde $\tau(A) = \tau(A^{-1})$ für alle $n \in \mathbb{N}$ gelten, dann könnte man den Begriff der τ-Reduktion statt über die Größe $\sigma(A)$ auch über die Größe $\tau(A)$ definieren und den Reduktionsbegriff vereinfachen. Für $n > 2$ ist aber i.a. $\tau(A) \neq \tau(A^{-1})$, wie man an den beiden Gitterbasen aus Beispiel 3.7 sieht.

5.3 Beweis von Satz 5.2a)

Folgendes Lemma zeigt, daß im Fall $n = 2$ τ-reduzierte Gitterbasen ebenso wie Gauß-reduzierte aus Vektoren bestehen, deren Längen gleich den sukzessiven Minima des Gitters sind.

Lemma 5.7 *Für ein Gitter $L = L(b_1, b_2)$ ist b_1, b_2 genau dann τ-reduziert, wenn die Längen von b_1, b_2 gleich den sukzessiven Minima $\lambda_1(L)$ und $\lambda_2(L)$ sind.*

Mit Satz 4.1 folgt daraus Satz 5.2a).

Beweis: Sei im folgenden $\mu_{2,1}(b_1, b_2)$ der Gram-Schmidt-Koeffizient $\mu_{2,1}$, in Abhängigkeit von der Gitterbasis b_1, b_2. Nach Satz 4.1b) können wir o.B.d.A. $\|b_1\| \leq \|b_2\|$ voraussetzen. Der Beweis basiert auf den 2 Hilfsbehauptungen:

Beh.1: Sei L = $L(b_1, b_2) = L(d_1, d_2)$ ein Gitter mit $\|b_1\| = \|d_1\|$ und $\|b_2\| = \|d_2\|$.

Dann gilt: $|\,\mu_{2,1}(b_1, b_2)| = |\,\mu_{2,1}(d_1, d_2)|$.

Bew.: Folgt aus

$$\det^2 L \;=\; \|b_1\|^2 \cdot \|b_2\|^2 - < b_1, b_2 >^2 = \; \|d_1\|^2 \cdot \|d_2\|^2 - < d_1, d_2 >^2 .$$

Beh.2: Für ein Gitter $L = L(b_1, b_2)$ ist b_1, b_2 genau dann τ-reduziert, wenn

$$\|b_1\|^2 \cdot \|b_2\|^2 \cdot \Big(1 + \max\Big\{|\,\mu_{2,1}(b_1, b_2)|\,,\; |\,\mu_{2,1}(b_2, b_1)|\Big\}\Big)$$

minimal für alle Gitterbasen von L ist.

Bew.: Ergibt sich aus $\mu_{2,1}(b_1, b_2) = \frac{a_{2,1}}{a_{1,1}}$ und $\mu_{2,1}(b_2, b_1) = \frac{a_{2,1}}{a_{2,2}}$ mit Satz 5.5 und Korollar 5.6.

„⇒": Sei b_1, b_2 τ-reduziert. Sei d_1, d_2 eine Gauß-reduzierte Gitterbasis von L. Wegen $\|b_1\| \leq \|b_2\|$ und $\|d_1\| \leq \|d_2\|$ folgt aus Beh.2:

$$\|b_1\|^2 \cdot \|b_2\|^2 \cdot (1 + |\,\mu_{2,1}(b_1, b_2)|\,) \;\leq\; \|d_1\|^2 \cdot \|d_2\|^2 \cdot (1 + |\,\mu_{2,1}(d_1, d_2)|\,).$$

Wegen $\|d_1\| \cdot \|d_2\| \leq \|b_1\| \cdot \|b_2\|$ gilt:

$$|\,\mu_{2,1}(b_1, b_2)| \;\leq\; |\,\mu_{2,1}(d_1, d_2)| \;\leq\; \tfrac{1}{2}.$$

Aus $|\,\mu_{2,1}(b_1, b_2)| \leq \frac{1}{2}$ und $\|b_1\| \leq \|b_2\|$ folgt, daß entweder b_1, b_2 oder $b_1, -b_2$ Gauß-reduziert sind. Mit Satz 2.5 erhält man:

$$\|b_1\| \;=\; \lambda_1(L), \;\; \|b_2\| \;=\; \|\pm b_2\| \;=\; \lambda_2(L).$$

„⇐": Sei b_1, b_2 mit $\|b_1\| = \lambda_1(L)$ und $\|b_2\| = \lambda_2(L)$. Sei d_1, d_2 eine τ-reduzierte Gitterbasis von L mit o.B.d.A. $\|d_1\| \leq \|d_2\|$. Nach „⇒" gilt:

$$\|d_1\| = \lambda_1(L) = \|b_1\|, \;\; \|d_2\| = \lambda_2(L) = \|b_2\|.$$

Aus Beh.1 ergibt sich:

$$|\,\mu_{2,1}(b_1,b_2)|\;=\;|\,\mu_{2,1}(d_1,d_2)|\,,\;|\,\mu_{2,1}(b_2,b_1)|\;=\;|\,\mu_{2,1}(d_2,d_1)|.$$

Wegen Beh.2 ist b_1, b_2 τ-reduziert. $\square$

5.4 Beweis von Satz 5.2b)

Offensichtlich sind τ-reduzierte Gitterbasen τ_2-reduziert. Wir zeigen, daß im Fall $n = 2$ auch die Umkehrung gilt. Daraus folgt Satz 5.2b).

Lemma 5.8 *Sei b_1, b_2 eine τ_2-reduzierte Gitterbasis. Dann ist b_1, b_2 τ-reduziert.*

Beweis: Sei $A = (a_{s,t})_{1\le s,t\le 2}$ die Gram-Matrix zu b_1, b_2, und für $k \in \mathbb{Z}$ sei $\bar{A}(k) = (\bar{a}_{s,t}(k))_{1\le s,t\le 2}$ die Gram-Matrix zu $b_1, b_2 + k \cdot b_1$. Dann gilt:

$$\bar{A}(k) \;=\; \begin{pmatrix} a_{1,1} & k\cdot a_{1,1}+a_{2,1} \\ k\cdot a_{1,1}+a_{2,1} & k^2\cdot a_{1,1}+2\cdot k\cdot a_{2,1}+a_{2,2} \end{pmatrix}$$

Die Funktionen

$$f_1(k) := |k \cdot a_{1,1} + a_{2,1}|$$

und

$$f_2(k) := k^2 \cdot a_{1,1} + 2 \cdot k \cdot a_{2,1} + a_{2,2}$$

haben die gleiche ganzzahlige Minimalstelle $\lceil -\frac{a_{2,1}}{a_{1,1}} \rfloor$. Nach Satz 5.5 und Korollar 5.6 wird $\sigma(\bar{A}(k))$ genau dann minimal, wenn die Größe

$$\bar{a}_{1,1}(k) \cdot \bar{a}_{2,2}(k) + |\bar{a}_{2,1}(k)| \cdot \max\{\bar{a}_{1,1}(k), \bar{a}_{2,2}(k)\}$$

minimal wird, also genau dann, wenn $f_1(k)$ und $f_2(k)$ ihre gemeinsame ganzzahlige Minimalstelle $\lceil -\frac{a_{2,1}}{a_{1,1}} \rfloor$ annehmen. Da b_1, b_2 τ_2-reduziert ist, folgt:

$$-\frac{1}{2} \;\le\; -\frac{a_{2,1}}{a_{1,1}} \;=\; -\frac{< b_1, b_2 >}{\|b_1\|^2} \;\le\; \frac{1}{2}.$$

Es ergibt sich somit:

$$-\tfrac{1}{2} \;\le\; \mu_{2,1}(b_1,b_2) \;\le\; \tfrac{1}{2}.$$

Da auch b_2, b_1 τ_2-reduziert ist, ergibt sich analog:

$$-\tfrac{1}{2} \;\le\; \mu_{2,1}(b_2,b_1) \;\le\; \tfrac{1}{2}.$$

1. Fall: $\|b_1\| \le \|b_2\|$.

Wegen $-\frac{1}{2} \le \mu_{2,1}(b_1,b_2) \le \frac{1}{2}$ sind b_1, b_2 oder $b_1, -b_2$ Gauß-reduziert.

2. Fall: $\|b_1\| > \|b_2\|$.

Wegen $-\frac{1}{2} \leq \mu_{2,1}(b_2, b_1) \leq \frac{1}{2}$ sind b_2, b_1 oder $b_2, -b_1$ Gauß-reduziert.

Nach Satz 2.5 sind die Längen von b_1, b_2 gleich den sukzessiven Minima $\lambda_1(L)$ und $\lambda_2(L)$ von $L = L(b_1, b_2)$. Nach Lemma 5.7 ist b_1, b_2 τ-reduziert. $\square$

Kapitel 6

Praktische τ_2-Reduktion

Da für die τ-Reduktion keine effizienten Algorithmen bekannt sind, versucht man, zumindest für die τ_2-Reduktion solche Algorithmen zu finden. Um für eine Gitterbasis $b_1, \cdots, b_n$ mit Gram-Matrix A einen Schritt der τ_2-Reduktion $b_j := b_j + k \cdot b_i$ durchzuführen, muß man k so wählen, daß für die neue Gram-Matrix $\bar{A}(k)$ gilt: $\sigma(\bar{A}(k)) \leq \sigma(A)$. In Abschnitt 6.1 wird zu gegebenen A, i, j ein Intervall konstruiert, in dem alle k mit dieser Eigenschaft liegen. Daraus ergibt sich ein Algorithmus zur τ_2-Reduktion, indem man in dem Intervall aus Abschnitt 6.1 nacheinander für alle $1 \leq i \neq j \leq n$ ein k sucht, das die Größe $\sigma(A)$ verkleinert, und jeweils die Gitterbasis durch $b_j := b_j + k \cdot b_i$ reduziert. Dies geschieht solange, bis die Größe $\sigma(A)$ durch solche Schritte nicht mehr verkleinerbar ist. Dieser Algorithmus wird in Abschnitt 6.2 vorgestellt. In Abschnitt 6.3 wird gezeigt, wie die Laufzeit dieses Algorithmus' verringert werden kann. In Abschnitt 6.4 testen wir am Beispiel eines Rucksackgitters, ob wir duch den neuen Algorithmus eine Verbesserung bei der Suche nach kurzen Gittervektoren gegenüber dem L^3-Algorithmus erhalten.

6.1 Grundlagen zur τ_2-Reduktion

Sei $\bar{A}(k)$ die Gram-Matrix, die aus der Gram-Matrix A durch die Basistransformation $b_j := b_j + k \cdot b_i$ entsteht. Für einen Schritt der τ_2-Reduktion sucht man zu gegebenen A, i, j ein $\bar{k} \in \mathbb{Z}$ mit:

$$\sigma(\bar{A}(\bar{k})) \leq \sigma(A).$$

Insbesondere gilt diese Gleichung für eine ganzzahlige Minimalstelle $\bar{k}$ von $\sigma(\bar{A}(k))$. Dabei gilt trivialerweise:

$$\sigma(\bar{A}(0)) = \sigma(A).$$

Ziel ist es, ein möglichst kleines Intervall zu finden, in dem alle $\bar{k}$ mit der geforderten Eigenschaft liegen. Eine Möglichkeit wäre, die Schranken aus Satz 4.7 zu

benutzen. Diese liefern aber sehr große Intervalle und sind deshalb für einen effizienten Algorithmus ungeeignet. Es wird ein anderer Ansatz vorgestellt, kurze Intervalle zu erhalten. Dieser benutzt die Einträge der Matrizen $\bar{A}(k)$ und $(\bar{A}(k))^{-1}$, in denen k vorkommt. Für die neue Gram-Matrix $\bar{A}(k) = (\bar{a}_{s,t}(k))_{1\leq s,t\leq n}$ nach der Basistransformation $b_j := b_j + k \cdot b_i$ ergibt sich:

$$\bar{a}_{s,t}(k) \;=\; \begin{cases} k^2 \cdot a_{i,i} + 2 \cdot k \cdot a_{i,j} + a_{j,j} & \text{für } (s,t) = (j,j), \\ k \cdot a_{i,l} + a_{j,l} & \text{für } (s,t) = (l,j) \text{ oder} \\ & (s,t) = (j,l) \text{ mit } l \neq j \\ a_{s,t} & \text{sonst} \end{cases} \tag{6.1}$$

Da die Gitterbasen $b_1, \cdots, b_{j-1}, b_j + k \cdot b_i, b_{j+1}, \cdots, b_n$ und $b_1^*, \cdots, b_{i-1}^*, b_i^* - k \cdot b_j^*$, $b_{i+1}^*, \cdots, b_n^*$ zueinander dual sind, entspricht die Basistransformation $b_j := b_j + k \cdot b_i$ der Basistransformation $b_i^* := b_i^* - k \cdot b_j^*$ der dualen Basis. Somit ergibt sich für $\bar{A}(k)^{-1} = (\bar{a}_{s,t}^*(k))_{1\leq s,t\leq n}$:

$$\bar{a}_{s,t}^*(k) \;=\; \begin{cases} k^2 \cdot a_{j,j}^* - 2 \cdot k \cdot a_{i,j}^* + a_{i,i}^* & \text{für } (s,t) = (i,i), \\ a_{i,l}^* - k \cdot a_{j,l}^* & \text{für } (s,t) = (l,i) \text{ oder} \\ & (s,t) = (i,l) \text{ mit } l \neq i \\ a_{s,t}^* & \text{sonst} \end{cases} \tag{6.2}$$

Aus $\sigma(\bar{A}(\bar{k})) \leq \sigma(A)$ ergibt sich:

$$\tau(\bar{A}(\bar{k})) \;\leq\; \tau(A) \;\vee\; \tau(\bar{A}(\bar{k})^{-1}) \;\leq\; \tau(A^{-1}).$$

1.Fall: $\tau(\bar{A}(\bar{k})) \;\leq\; \tau(A)$

Es folgt:

$$\tau_l(\bar{A}(\bar{k})) \;\leq\; \tau(A) \quad \text{für } \; l \neq j \;,\; a_{l,i} \neq 0$$

und damit:

$$\sum_{p=1}^{n} |\bar{a}_{l,p}(\bar{k})| \cdot \bar{a}_{p,p}^*(\bar{k}) \;\;\leq\;\; \tau(A) \quad \text{für } \; l \neq j \;,\; a_{l,i} \neq 0 \tag{6.3}$$

Ebenso folgt:

$$\tau_j(\bar{A}(\bar{k})) \;\leq\; \tau(A)$$

und damit:

$$\sum_{p=1}^{n} |\bar{a}_{j,p}(\bar{k})| \cdot \bar{a}_{p,p}^*(\bar{k}) \;\;\leq\;\; \tau(A) \tag{6.4}$$

Sei $d_1(l) := \tau(A) - \sum\limits_{\substack{p=1 \\ p\neq i,j}}^{n} |a_{l,p}| \cdot a^*_{p,p}$ für $l = 1, \cdots, n$.

Dann erhält man folgende Bedingungen für $\bar{k}$:

a) Aus (6.3) folgt:

$$\sum_{\substack{p=1 \\ p\neq i}}^{n} |\bar{a}_{l,p}(\bar{k})| \cdot \bar{a}^*_{p,p}(\bar{k}) \;\leq\; \tau(A) \quad \text{für } l \neq j\ ,\ a_{l,i} \neq 0.$$

Mit (6.1) und (6.2) ergibt sich:

$$\sum_{\substack{p=1 \\ p\neq i,j}}^{n} |a_{l,p}| \cdot a^*_{p,p} + |\bar{k} \cdot\ a_{i,l} + a_{j,l}| \cdot a^*_{j,j} \;\leq\; \tau(A) \quad \text{für } l \neq j\ ,\ a_{l,i} \neq 0.$$

Durch Auflösen nach $\bar{k}$ erhält man:

$$\min\left\{\frac{\pm d_1(l) - a_{l,j} \cdot a^*_{j,j}}{a_{l,i} \cdot a^*_{j,j}}\right\} \;\leq\; \bar{k} \;\leq\; \max\left\{\frac{\pm d_1(l) - a_{l,j} \cdot a^*_{j,j}}{a_{l,i} \cdot a^*_{j,j}}\right\}$$

$$\text{für } l \neq j\ ,\ a_{l,i} \neq 0 \tag{6.5}$$

b) Aus (6.3) folgt:

$$\sum_{\substack{p=1 \\ p\neq j}}^{n} |\bar{a}_{l,p}(\bar{k})| \cdot \bar{a}^*_{p,p}(\bar{k}) \;\leq\; \tau(A) \quad \text{für } l \neq j\ ,\ a_{l,i} \neq 0.$$

Mit (6.1) und (6.2) ergibt sich:

$$\sum_{\substack{p=1 \\ p\neq i,j}}^{n} |a_{l,p}| \cdot a^*_{p,p} + |a_{l,i}| \cdot (\bar{k}^2 \cdot\ a^*_{j,j} - 2 \cdot \bar{k} \cdot\ a^*_{i,j} + a^*_{i,i}) \;\leq\; \tau(A) \quad \text{für } l \neq j\ ,\ a_{l,i} \neq 0.$$

Durch Auflösen nach $\bar{k}$ erhält man:

$$\frac{a^*_{i,j}}{a^*_{j,j}} - \sqrt{\frac{d_1(l)}{|a_{l,i}| \cdot a^*_{j,j}} - \frac{a^*_{i,i}}{a^*_{j,j}} + \left(\frac{a^*_{i,j}}{a^*_{j,j}}\right)^2} \;\leq\; \bar{k} \;\leq\; \frac{a^*_{i,j}}{a^*_{j,j}} + \sqrt{\frac{d_1(l)}{|a_{l,i}| \cdot a^*_{j,j}} - \frac{a^*_{i,i}}{a^*_{j,j}} + \left(\frac{a^*_{i,j}}{a^*_{j,j}}\right)^2}$$

$$\text{für } l \neq j\ ,\ a_{l,i} \neq 0 \tag{6.6}$$

c) Aus (6.4) folgt:

$$|\bar{a}_{j,l}(\bar{k})| \cdot \bar{a}^*_{l,l}(\bar{k}) \;\leq\; \tau(A) \quad \text{für } l \neq i, j\ ,\ a_{l,i} \neq 0.$$

Mit (6.1) und (6.2) ergibt sich:

$$|\bar{k} \cdot a_{i,l} + a_{j,l}| \cdot a^*_{l,l} \;\leq\; \tau(A) \quad \text{für } l \neq i,j \;,\; a_{l,i} \neq 0.$$

Durch Auflösen nach $\bar{k}$ erhält man:

$$\min\left\{\frac{\pm\tau(A) - a_{l,j} \cdot a^*_{l,l}}{a_{l,i} \cdot a^*_{l,l}}\right\} \;\leq\; \bar{k} \;\leq\; \max\left\{\frac{\pm\tau(A) - a_{l,j} \cdot a^*_{l,l}}{a_{l,i} \cdot a^*_{l,l}}\right\}$$

$$\text{für } l \neq i,j \;,\; a_{l,i} \neq 0 \tag{6.7}$$

d) Aus (6.4) folgt:

$$\bar{a}_{j,j}(\bar{k}) \cdot \bar{a}^*_{j,j}(\bar{k}) \;\leq\; \tau(A).$$

Mit (6.1) und (6.2) ergibt sich:

$$(\bar{k}^2 \cdot a_{i,i} + 2 \cdot \bar{k} \cdot a_{i,j} + a_{j,j}) \cdot a^*_{j,j} \;\leq\; \tau(A).$$

Durch Auflösen nach $\bar{k}$ erhält man:

$$-\frac{a_{i,j}}{a_{i,i}} - \sqrt{\frac{\tau(A)}{a_{i,i} \cdot a^*_{j,j}} - \frac{a_{j,j}}{a_{i,i}} + \left(\frac{a_{i,j}}{a_{i,i}}\right)^2} \;\leq\; \bar{k} \;\leq\; -\frac{a_{i,j}}{a_{i,i}} + \sqrt{\frac{\tau(A)}{a_{i,i} \cdot a^*_{j,j}} - \frac{a_{j,j}}{a_{i,i}} + \left(\frac{a_{i,j}}{a_{i,i}}\right)^2}$$

$$\tag{6.8}$$

2.Fall: $\tau(\bar{A}(\bar{k})^{-1}) \;\leq\; \tau(A^{-1})$

Sei $d_2(l) := \tau(A^{-1}) - \sum\limits_{\substack{p=1 \\ p \neq i,j}}^{n} |a^*_{l,p}| \cdot a_{p,p}$ für $l = 1, \cdots, n$.

Dann ergeben sich analog zu Fall 1 folgende Bedingungen für $\bar{k}$:

a) $$\min\left\{\frac{\pm d_2(l) + a^*_{l,i} \cdot a_{i,i}}{a^*_{l,j} \cdot a_{i,i}}\right\} \;\leq\; \bar{k} \;\leq\; \max\left\{\frac{\pm d_2(l) + a^*_{l,i} \cdot a_{i,i}}{a^*_{l,j} \cdot a_{i,i}}\right\}$$

$$\text{für } l \neq i \;,\; a^*_{l,j} \neq 0 \tag{6.9}$$

b) $$-\frac{a_{i,j}}{a_{i,i}} - \sqrt{\frac{d_2(l)}{|a^*_{l,j}| \cdot a_{i,i}} - \frac{a_{j,j}}{a_{i,i}} + \left(\frac{a_{i,j}}{a_{i,i}}\right)^2} \leq \bar{k} \leq -\frac{a_{i,j}}{a_{i,i}} + \sqrt{\frac{d_2(l)}{|a^*_{l,j}| \cdot a_{i,i}} - \frac{a_{j,j}}{a_{i,i}} + \left(\frac{a_{i,j}}{a_{i,i}}\right)^2}$$

$$\text{für } l \neq i \;,\; a^*_{l,j} \neq 0 \tag{6.10}$$

c) $$\min\left\{\frac{\pm\tau(A^{-1})+a^*_{l,i}\cdot a_{l,l}}{a^*_{l,j}\cdot a_{l,l}}\right\} \;\le\; \bar{k} \;\le\; \max\left\{\frac{\pm\tau(A^{-1})+a^*_{l,i}\cdot a_{l,l}}{a^*_{l,j}\cdot a_{l,l}}\right\}$$

$$\text{für } l\neq i,j\ ,\ a^*_{l,j}\neq 0 \tag{6.11}$$

d) $$\frac{a^*_{i,j}}{a^*_{j,j}}-\sqrt{\frac{\tau(A^{-1})}{a_{i,i}\cdot a^*_{j,j}}-\frac{a^*_{i,i}}{a^*_{j,j}}+\left(\frac{a^*_{i,j}}{a^*_{j,j}}\right)^2} \;\le\; \bar{k} \;\le\; \frac{a^*_{i,j}}{a^*_{j,j}}+\sqrt{\frac{\tau(A^{-1})}{a_{i,i}\cdot a^*_{j,j}}-\frac{a^*_{i,i}}{a^*_{j,j}}+\left(\frac{a^*_{i,j}}{a^*_{j,j}}\right)^2}$$

(6.12)

Aus den beiden Fällen ergibt sich:

Satz 6.1 *Sei $b_1,\cdots,b_n$ eine Gitterbasis mit Gram-Matrix $A=(a_{s,t})_{1\le s,t\le n}$ und $A^{-1}=(a^*_{s,t})_{1\le s,t\le n}$. Seien i,j fest mit $1\le i\neq j\le n$ und $\bar{k}\in\mathbb{Z}$ mit $\sigma(\bar{A}(\bar{k}))\le\sigma(A)$. Dann erfüllt $\bar{k}$ die Bedingungen (6.5), (6.6), (6.7), (6.8) oder die Bedingungen (6.9), (6.10), (6.11), (6.12). Insbesondere gilt dies für eine ganzzahlige Minimalstelle $\bar{k}$ von $\sigma(\bar{A}(k))$.*

Bemerkung 6.2 *Satz 6.1 liefert für eine ganzzahlige Minimalstelle $\bar{k}$ von $\sigma(\bar{A}(k))$ Zahlen $a,b\in\mathbb{Z}$ mit $0,\bar{k}\in[a,b]$.*

6.2 Algorithmus zur τ_2-Reduktion

Im nachfolgenden Algorithmus zur τ_2-Reduktion werden sukzessive τ_2-Reduktionsschritte durchgeführt, bis die Größe $\sigma(A)$ durch solche Schritte nicht mehr verkleinerbar ist. Für feste A,i,j suchen wir k, so daß nach dem Reduktionsschritt $b_j=b_j+k\cdot b_i$ die neue Größe $\sigma(\bar{A}(k))$ minimal ist. Das gesuchte k ist in dem Intervall, das man aus Satz 6.1 erhält.

Algorithmus 6.3 **(zur τ_2-Reduktion)**

INPUT *Gitterbasis* $b_1, \cdots, b_n \in \mathbb{R}^m$

1 *Berechne* $A = [b_1, \cdots, b_n]^T \cdot [b_1, \cdots, b_n]$, A^{-1} *und* $\sigma = \sigma(A)$

2 *FOR* $i = 1, \cdots, n$ *DO*

FOR $j = 1, \cdots, n$, $j \neq i$ *DO*

a) *Berechne die Intervallgrenzen* l, r (A, i, j) *aus Satz 6.1*

b) *FOR* $k = l, \cdots, r$, $k \neq 0$ *DO*

Berechne $\bar{A}(k), (\bar{A}(k))^{-1}$ *und* $\sigma(\bar{A}(k))$

IF $(\, \sigma(\bar{A}(k)) < \sigma \,)$

THEN $b_j = b_j + k \cdot b_i$

$A = \bar{A}(k)$

$A^{-1} = (\bar{A}(k))^{-1}$

$\sigma = \sigma(\bar{A}(k))$

GOTO 2

OUTPUT τ_2*-reduzierte Gitterbasis* $b_1, \cdots, b_n \in \mathbb{R}^m$

Korrektheit: Algorithmus 6.3 gibt eine τ_2-reduzierte Basis aus, da nach Satz 6.1 für alle $n^2 - n$ Paare (i, j) mit $i \neq j$ und für alle $k \in \mathbb{Z}$ durch den Reduktionsschritt $b_j = b_j + k \cdot b_i$ keine Verbesserung gefunden wird.
Er endet nach endlich vielen Schritten, da nach $n^2 - n$ Durchläufen der Schritte 2a),b) eine Verbesserung gefunden wird oder der Algorithmus stoppt. Nach Satz 4.6c) gibt es nämlich nur endlich viele Gitterbasen mit Gram-Matrix A, für die gilt: $\sigma(A) \leq \sigma(A^{alt})$.
□

Die Anzahl der Schritte in 2a),b), die der Algorithmus höchstens durchläuft, kann durch

$$(n^2 - n) \cdot \Big(\frac{n! \cdot \|A\|_\infty^n}{\det A}\Big)^{2n^2} \cdot \min\Big\{n^{\frac{1}{2}n^2}, \Big(\frac{n! \cdot \|A\|_\infty^n}{\det A}\Big)^{n^2}\Big\}$$

abgeschätzt werden. Diese Schranke ergibt sich, da nach $n^2 - n$ Durchläufen der Schritte 2a),b) eine Verbesserung gefunden wird oder der Algorithmus stoppt und da wegen Korollar 4.9 nach höchstens

$$\Big(\frac{n! \cdot \|A\|_\infty^n}{\det A}\Big)^{2n^2} \cdot \min\Big\{n^{\frac{1}{2}n^2}, \Big(\frac{n! \cdot \|A\|_\infty^n}{\det A}\Big)^{n^2}\Big\}$$

unimodularen Basistransformationen eine τ-reduzierte und damit auch τ_2-reduzierte Gitterbasis vorliegt.

6.3 Beschleunigung des Algorithmus'

1. Man kann die arithmetischen Operationen, die nicht die Gitterbasis $b_1, \cdots, b_n$ und die Gram-Matrizen A und A^{-1} betreffen, statt in exakter Arithmetik in Gleitpunkt-Arithmetik durchführen, da in diesem Fall Rechenfehler das Gitter nicht verändern können.

2. In Algorithmus 6.3 wird in Schritt 2b) für jeden Punkt im Intervall neu das entsprechende $\sigma(\bar{A}(k))$ berechnet und mit σ verglichen. Dazu sind jeweils n Berechnungen von $\tau_s(\bar{A}(k))$ und $\tau_s(\bar{A}(k)^{-1})$ notwendig. Nur bei $\sigma(\bar{A}(k)) < \sigma$ wird der Wert von $\sigma(\bar{A}(k))$ im weiteren gebraucht. Somit ist es effektiver, die $\tau_s(\bar{A}(k))$ bzw. $\tau_s(\bar{A}(k)^{-1})$ Schritt für Schritt zu berechnen, den Zwischenwert von $\sigma(\bar{A}(k))$ jeweils zu aktualisieren und, sobald dieser Wert größer gleich dem bisherigen σ ist, in der FOR-Schleife in Schritt 2b) weiterzugehen.

3. Nachteilig an Algorithmus 6.3 ist noch, daß in Schritt 2b) k ein evtl. großes Intervall ganz durchlaufen muß. Dies kann man in der Praxis mit folgender Hypothese verbessern, für die wir keinen Beweis gefunden haben.

Hypothese 6.4 *Sei $b_1, \cdots, b_n$ eine Gitterbasis mit Gram-Matrix A. Seien i, j fest mit $1 \leq i \neq j \leq n$. Dann gibt es ein $k_0 \in \mathbb{Z}$, so daß $\sigma(\bar{A}(k))$ für $k \leq k_0$ streng monoton fallend und für $k \geq k_0$ streng monoton steigend ist.*

Mit Hypothese 6.4 ergibt sich, daß im Fall $\sigma(\bar{A}(-1)) > \sigma(\bar{A}(0)) = \sigma(A) < \sigma(\bar{A}(1))$ der Reduktionsschritt $b_j = b_j + k \cdot b_i$ für alle $k \in \mathbb{Z}$ keine Verbesserung bringt und ansonsten entweder $k = -1$ oder $k = 1$ eine Verbesserung bringen. Man muß in der FOR-Schleife von Schritt 2b) also nur $k = -1$ und $k = 1$ untersuchen. Um auch ohne Hypothese 6.4 sicherzustellen, daß die Reduktion abgeschlossen ist, verifiziert man am Ende mit dem ursprünglichen Algorithmus, daß die ausgegebene Gitterbasis tatsächlich τ_2-reduziert ist.

6.4 Anwendung auf Rucksackprobleme

Ein Rucksackproblem oder Subset-Sum-Problem ist folgendes Problem:

- Gegeben: $n, s \in \mathbb{N}, a_1, \cdots, a_n \in \mathbb{N}$.
- Finde $x_i \in \{0, 1\}$ mit $\sum_{i=1}^{n} a_i x_i = s$ oder zeige, daß keine solche Lösung existiert.

Dabei heißt n die Dimension des Rucksackproblems, die maximale Bitlänge b von $a_1, \cdots, a_n$ die Bitlänge des Rucksackproblems und $d := n/b$ die Dichte des Rucksackproblems.
Ein Rucksackproblem kann man auf das "kürzeste Gittervektorproblem" zurückführen. So wurde mit Hilfe einer Gitterbasis, die nur vom Rucksackproblem

$(n, a_1, \cdots, a_n, s)$ abhängt, in [7] gezeigt, daß für ein zufälliges, lösbares Rucksackproblem mit Dichte $d < 0.6463$ die Wahrscheinlichkeit, daß ein kürzester Gittervektor nicht zu einer Lösung des Rucksackproblems führt, für große n gegen Null geht. In [4] konnte durch Verwendung einer anderen Gitterbasis die obere Schranke der Dichte auf 0.9408 erhöht werden.

Wir betrachten Rucksackprobleme mit der zusätzlichen Einschränkung $\sum_{i=1}^{n} x_i = q$ für festes $q \in \mathbb{N}$ mit $1 \leq q \leq n$. Diese Rucksackprobleme lassen sich mit folgender Gitterbasis lösen:

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & q & \cdots & q & n^2 s & n^2 q \\ 0 & n & & 0 & n^2 a_1 & n^2 \\ \vdots & & \ddots & & \vdots & \vdots \\ 0 & 0 & & n & n^2 a_n & n^2 \end{pmatrix}$$

Ein Gittervektor $(z_0, z_1, \cdots, z_{n+2}) \in \mathbb{Z}^{n+3}$ liefert eine Lösung des Rucksackproblems, falls

$$z_{n+1} = z_{n+2} = 0,\ z_j = \begin{cases} z_0 q & (n-q)\text{-mal} \\ z_0(q-n) & q\text{-mal} \end{cases} \text{ für } j = 1, \cdots, n.$$

Viele Reduktionsalgorithmen, wie z.B. die L^3-Reduktion, sind schon ausgiebig an Rucksackgittern getestet worden ([4], [7]). Die folgenden Untersuchungen dienten dazu, exemplarisch an diesem Rucksackgitter zu untersuchen, inwieweit die τ_2-Reduktion in der Lage ist, kurze Gittervektoren zu finden, und ob wir durch den Algorithmus 6.3 zur τ_2-Reduktion gegenüber dem L^3-Algorithmus einen Fortschritt erreichen. Dazu haben wir diesen Algorithmus in der Programmiersprache C implementiert und einen Algorithmus zur L^3-Reduktion mit $\delta = 0.99$ benutzt. Die Untersuchungen wurden auf HP-Workstations "Apollo 9000" der Serie 780/C160 durchgeführt. Diese haben eine theoretisch erreichbare Anzahl der Floating-Point-Operationen (MFLOPs) von 140 Millionen pro Sekunde. Für die Berechnungen in exakter Arithmetik wurde die in der Arbeitsgruppe Mathematische Informatik der Universität Frankfurt entwickelte Programmbibliothek LARIFARI verwendet.

Es wurden jeweils 10 verschiedene zufällige, lösbare Rucksackprobleme mit $q = n/2$ betrachtet. Dann wurde untersucht, wieviele Probleme durch den L^3-Algorithmus und wieviele durch einen Algorithmus, bestehend aus τ_2-Reduktion und anschließender L^3-Reduktion, gelöst werden. Außerdem wurden die Laufzeiten der beiden Algorithmen verglichen. Die Dimension n und Bitlänge b des Rucksackproblems durchliefen folgende Werte:

- $n = 42 : b = 24, 28, 32, 36, 40, 44, 48, 52, 56, 60,$
- $n = 50 : b = 26, 30, 34, 38, 42, 46, 50, 54, 58, 62, 66, 70,$
- $n = 58 : b = 29, 35, 41, 47, 53, 58, 63, 69, 75, 81, 87, 93,$
- $n = 66 : b = 18, 26, 34, 42, 50, 58, 66, 72, 80, 88, 96, 104, 112.$

Es wird jeweils die Anzahl l der gelösten Probleme von 10 Problemen und die Durchschnittslaufzeit t in “Stunden : Minuten : Sekunden“ angegeben.

$n = 42$		L^3	$\tau_2 + L^3$
$b = 24$	l	6	10
	t	00:00:00	00:09:49
$b = 28$	l	4	9
	t	00:00:00	00:11:25
$b = 32$	l	2	9
	t	00:00:00	00:11:58
$b = 36$	l	1	0
	t	00:00:01	00:13:04
$b = 40$	l	1	1
	t	00:00:01	00:14:52
$b = 44$	l	2	4
	t	00:00:01	00:14:22
$b = 48$	l	4	6
	t	00:00:01	00:14:16
$b = 52$	l	8	5
	t	00:00:01	00:15:10
$b = 56$	l	6	10
	t	00:00:01	00:15:25
$b = 60$	l	10	10
	t	00:00:01	00:17:11
Durch-	l	4.4	6.4
schnitt	t	00:00:01	00:13:45

$n = 50$		L^3	$\tau_2 + L^3$
$b = 26$	l	6	9
	t	00:00:00	00:24:31
$b = 30$	l	2	9
	t	00:00:01	00:25:03
$b = 34$	l	1	3
	t	00:00:01	00:28:31
$b = 38$	l	0	2
	t	00:00:01	00:31:35
$b = 42$	l	0	0
	t	00:00:01	00:31:44
$b = 46$	l	0	0
	t	00:00:01	00:33:33
$b = 50$	l	0	0
	t	00:00:01	00:35:51
$b = 54$	l	0	1
	t	00:00:01	00:33:00
$b = 58$	l	0	0
	t	00:00:02	00:38:29
$b = 62$	l	1	1
	t	00:00:02	00:39:44
$b = 66$	l	5	1
	t	00:00:02	00:40:07
$b = 70$	l	8	7
	t	00:00:02	00:38:27
Durch-	l	1.9	2.8
schnitt	t	00:00:01	00:33:23

$n = 58$		L^3	$\tau_2 + L^3$
$b = 29$	l	6	7
	t	00:00:01	00:44:34
$b = 35$	l	1	2
	t	00:00:01	01:12:47
$b = 41$	l	0	0
	t	00:00:01	00:58:06
$b = 47$	l	0	0
	t	00:00:01	01:03:44
$b = 53$	l	0	0
	t	00:00:02	01:12:08
$b = 58$	l	0	0
	t	00:00:02	01:14:07
$b = 63$	l	0	0
	t	00:00:02	01:15:27
$b = 69$	l	1	0
	t	00:00:03	01:12:21
$b = 75$	l	0	0
	t	00:00:03	01:23:56
$b = 81$	l	3	4
	t	00:00:03	01:22:40
$b = 87$	l	2	2
	t	00:00:04	01:31:08
$b = 93$	l	3	5
	t	00:00:04	01:39:25
Durch-	l	1.3	1.7
schnitt	t	00:00:02	01:14:12

$n = 66$		L^3	$\tau_2 + L^3$
$b = 18$	l	10	9
	t	00:00:00	01:28:28
$b = 26$	l	6	7
	t	00:00:01	01:11:36
$b = 34$	l	2	2
	t	00:00:01	01:37:23
$b = 42$	l	0	0
	t	00:00:01	01:45:14
$b = 50$	l	0	0
	t	00:00:02	01:43:39
$b = 58$	l	0	0
	t	00:00:02	01:59:15
$b = 66$	l	0	0
	t	00:00:03	02:00:01
$b = 72$	l	0	0
	t	00:00:03	02:30:12
$b = 80$	l	0	0
	t	00:00:04	02:37:41
$b = 88$	l	0	2
	t	00:00:05	02:38:20
$b = 96$	l	0	0
	t	00:00:05	03:06:31
$b = 104$	l	0	0
	t	00:00:06	03:29:13
$b = 112$	l	3	1
	t	00:00:07	02:29:02
Durch-	l	1.6	1.6
schnitt	t	00:00:03	02:12:03

Ergebnisse

Man erkennt, daß bei großer Dichte und bei kleiner Dimension durch den neuen Algorithmus wesentlich mehr Rucksackprobleme gelöst werden als durch den L^3-Algorithmus. Bei kleiner Dichte und bei großer Dimension werden etwa gleich viele Rucksackprobleme gelöst. Die Verbesserung geht aber auf Kosten einer vielfach höheren Laufzeit.

Kapitel 7

Faktorisierung ganzer Zahlen

Eine andere Anwendung der Gitterreduktion ist die Faktorisierung ganzer Zahlen. Es gibt drei Ansätze, mit Hilfe von Gitterbasenreduktion ganze Zahlen zu faktorisieren, und zwar von Schnorr [11], Adleman [1] und Ajtai [2]. In Abschnitt 7.1 beschreiben wir die Bedeutung der Faktorisierung großer ganzer Zahlen und welche gemeinsame Idee den obigen Faktorisierungsansätzen zugrundeliegt. In Abschnitt 7.2 stellen wir Schnorrs Gitterbasis und in Abschnitt 7.3 Adlemans Gitterbasis vor und erläutern kurz ihre Funktion. Unser Hauptaugenmerk gilt aber dem neuen Ansatz Ajtais, der in den Abschnitten 7.4 und 7.5 ausführlich beschrieben wird.

7.1 Einleitung

Die Sicherheit vieler Public-Key-Kryptosysteme basiert auf der Annahme, daß es nicht effizient möglich ist, große ganze Zahlen in Primfaktoren zu zerlegen. Der derzeit schnellste Faktorisierungsalgorithmus ist das *Number Field Sieve* [9], das zur Faktorisierung einer Zahl N asymptotisch $O(e^{(1.92+o(1))(\ln N)^{1/3}(\ln\ln N)^{2/3}})$ arithmetische Operationen benötigt. Der erste Ansatz, große Zahlen mit Hilfe von Gitterbasenreduktion zu faktorisieren, stammt von Schnorr [11]. Er führt ein Gitter L und einen Vektor b ein und reduziert das Faktorisierungsproblem auf das Finden eines nächsten Gittervektors zu b in der Eins-Norm. Adleman [1] benutzt ein modifiziertes Gitter und reduziert das Faktorisierungsproblem auf das Finden eines kürzesten Gittervektors in der Euklidischen Norm, benötigt dazu aber zahlentheoretische Annahmen. Ajtai [2] erweitert Adlemans Gittter, so daß er ohne diese Annahmen auskommt. Allen drei Reduktionen ist folgende Idee gemeinsam:
Sei N eine hinreichend große ganze Zahl, die faktorisiert werden soll. Seien $p_0 := -1$ und $p_1, \cdots, p_t$ die ersten t Primzahlen, wobei t polynomial in $\ln N$ sei. Man

konstruiert mit Hilfe von Gitterbasenreduktion Kongruenzen der Form:

$$\prod_{i=0}^{t} p_i^{\alpha_i} \equiv \prod_{i=0}^{t} p_i^{\beta_i} \,(\mathrm{mod}\, N) \tag{7.1}$$

Hat man $t+2$ verschiedene solche Kongruenzen, dann liefert lineare Algebra über $\mathbb{Z}_2$ eine Kongruenz dieser Form mit α_i, β_i gerade für alle i. Somit liegt eine Kongruenz

$$x^2 \equiv y^2 \,(\mathrm{mod}\, N)$$

vor. Für zufällige $x, y \bmod N$, die diese Kongruenz erfüllen, gilt mit Wahrscheinlichkeit mindestens $\frac{1}{2}$:

$$x \not\equiv \pm y \,(\mathrm{mod}\, N).$$

In diesem Fall sind $(x+y, N)$ und $(x-y, N)$ nicht-triviale Teiler von N.

Für die folgenden Reduktionen benötigen wir den Glattheitsbegriff natürlicher Zahlen:

Definition 7.1 *Eine natürliche Zahl n heißt B-glatt, wenn für alle Primteiler p von n gilt: $p \leq B$.*

7.2 Schnorrs Reduktion

Seien $\alpha, c \in \mathbb{Q}$ mit $\alpha, c > 1$ und $p_t = (\ln N)^\alpha < N$. Schnorr [11] betrachtet das Gitter $L(v_1, \cdots, v_t)$ mit:

$$\begin{pmatrix} v_1 \\ \vdots \\ v_t \end{pmatrix} = \begin{pmatrix} \ln p_1 & \cdots & 0 & N^c \ln p_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & \ln p_t & N^c \ln p_t \end{pmatrix}$$

und den Vektor

$$b = (0, \cdots, 0, N^c \ln N).$$

Man definiert für einen Gittervektor $w = \sum_{i=1}^{t} \delta_i v_i$:

$$u(w) := \prod_{\substack{i=1 \\ \delta_i > 0}}^{t} p_i^{\delta_i}, \quad v(w) := \prod_{\substack{i=1 \\ \delta_i < 0}}^{t} p_i^{-\delta_i}.$$

Schnorr zeigt, daß für $\sigma > 0$ und für jeden Gittervektor w aus

$$\|w - b\|_1 \;\leq\; (2c-1) \ln N + 2\sigma \ln p_t \tag{7.2}$$

folgt, daß

$$|u(w) - v(w)N| \;\leq\; p_t^{\frac{1}{\alpha}+\sigma+o(1)}.$$

Dann gilt mit großer Wahrscheinlichkeit:

$$u(w) - v(w)N = \pm \prod_{i=1}^{t} p_i^{\gamma_i}$$

für geeignete $\gamma_i \in \mathbb{N}_0$. Somit erhält man, falls es einen Gittervektor mit (7.2) gibt, die gewünschte Kongruenz (7.1).
Schnorr zeigt weiter, daß für hinreichend großes N und $\epsilon := (c-1) - (2c-1)/\alpha$ mindestens $N^{\epsilon+o(1)}$ viele Gittervektoren (7.2) erfüllen. Dabei benutzt er die Hypothese, daß für hinreichend großes N und zufällige natürliche Zahlen u, v mit $u \leq N^c$ und $N^{c-1}/2 < v < N^{c-1}$ die Ereignisse "u, v sind p_t-glatt" und "$|u - vN| = 1$" fast unabhängig sind.

7.3 Adlemans Reduktion

Adleman [1] benutzt für seine Reduktion der Faktorisierung auf das "kürzeste Gittervektorproblem" ein ähnliches Gitter wie Schnorr. Die $\ln p_i$ werden durch $\sqrt{\ln p_i}$ ersetzt, da Adleman die Euklidische Norm statt der Eins-Norm betrachtet. Der letzte Basisvektor ist gleich dem Vektor b von Schnorr, wobei $c = 4$.
Sei p_t die größte Primzahl kleiner gleich $\ln^{20}(2n^{1.25})$. Adleman untersucht das Gitter L, dessen Basisvektoren $v_1, \cdots, v_{t+1}$ rationale Approximationen der Zeilenvektoren folgender Matrix sind:

$$\begin{pmatrix} \sqrt{\ln p_1} & \cdots & 0 & N^4 \ln p_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & \sqrt{\ln p_t} & N^4 \ln p_t \\ 0 & \cdots & 0 & N^4 \ln N \end{pmatrix}$$

Wie bei Schnorr definiert man für einen Gittervektor $w = \sum_{i=1}^{t+1} \delta_i v_i$:

$$u(w) := \prod_{\substack{i=1 \\ \delta_i > 0}}^{t} p_i^{\delta_i}, \quad v(w) := \prod_{\substack{i=1 \\ \delta_i < 0}}^{t} p_i^{-\delta_i}.$$

Sei $w = \sum_{i=1}^{t+1} \delta_i v_i$ ein kürzester Gittervektor mit o.B.d.A. $\delta_{t+1} \geq 0$. Adleman zeigt, daß $\delta_{t+1} = 1$ ist. Da die letzte Komponente klein sein muß, folgt:

$$N \cdot \frac{u(w)}{v(w)} \approx 1.$$

Daraus folgt, daß $u(w)N - v(w)$ so klein ist, daß es sich über $p_1, \cdots, p_t$ faktorisieren läßt:

$$u(w)N - v(w) = \prod_{i=1}^{t} p_i^{\gamma_i}.$$

für geeignete $\gamma_i \in \mathbb{N}_0$. Somit erhält man die gewünschte Kongruenz (7.1).
Adleman benutzt folgende zahlentheoretische Annahmen:
Sei $P = N^{1/4} + 1, \cdots, 2N^{1/4}$ und $Q = PN - 1$. Dann gilt:

- Die Wahrscheinlichkeit, daß Q quadratfrei und p_t-glatt ist, ist genauso groß wie bei einer zufälligen Zahl kleiner als $2N^{5/4}$.
- Die Wahrscheinlichkeit, daß P quadratfrei und p_t-glatt ist, ist unabhängig von der Wahrscheinlichkeit, daß Q quadratfrei und p_t-glatt ist.

7.4 Ajtais Reduktion

Ajtai [2] erweitert Adlemans Gitter, indem er folgendes Gitter $L(v_1, \cdots, v_{t+2})$ benutzt:

$$\begin{pmatrix} v_1 \\ \vdots \\ v_t \\ v_{t+1} \\ v_{t+2} \end{pmatrix} = \begin{pmatrix} \sqrt{\ln p_1} & \cdots & 0 & 0 & N^{11} \ln p_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & \sqrt{\ln p_t} & 0 & N^{11} \ln p_t \\ 0 & \cdots & 0 & 0 & N^{11} \ln b \\ 0 & \cdots & 0 & N^{-2} & N^{11} \ln(1 + \frac{N}{b}) \end{pmatrix}$$

Sei t polynomial in $\ln N$ und b eine zufällige natürliche Zahl, die folgende zwei Bedingungen erfüllt:

$$N^{10} < b < (2N)^{10} \tag{7.3}$$

$$b \equiv \prod_{i=1}^{t} p_i^{\alpha_i} \pmod{N} \quad \text{mit} \quad \alpha_i \in \{0, 1\} \tag{7.4}$$

Die Reduktion beruht auf der Voraussetzung, daß unter den Zahlen $b + lN$ mit $|l| \leq N^{1/2}$ mindestens eine ist, die p_t-glatt und quadratfrei ist. Somit hat man:

$$b + lN = \prod_{i=1}^{t} p_i^{-\gamma_i} \quad \text{mit} \quad \gamma_i \in \{0, -1\} \tag{7.5}$$

Ist die Voraussetzung erfüllt, so ist der Gittervektor $w' = \sum_{i=1}^{t} \gamma_i v_i + v_{t+1} + l v_{t+2}$ sehr kurz:

- Die ersten t Komponenten sind 0 oder $-\sqrt{\ln p_i}$.

- Die $(t+1)$-te Komponente ist klein, da $|l| \leq N^{1/2}$ ist.
- Wegen $(1+\frac{N}{b})^l \approx 1 + l\frac{N}{b}$ ist die $(t+2)$-te Komponente ungefähr gleich $N^{11} \ln\left(\prod_{i=1}^{t} p_i^{\gamma_i} \cdot b \cdot (1+l\frac{N}{b})\right) = 0$.

Ajtai zeigt genauer, daß unter obiger Voraussetzung gilt:

$$\|w'\| \;\leq\; c + \ln b,$$

wobei $c < 2\ln 2$ ist (Satz 7.3d)). Findet man durch Gitterbasenreduktion den Gittervektor w', so hat man wegen (7.4) und (7.5) eine Kongruenz der Form (7.1). In Satz 7.6 zeigen wir, daß für zufällige b mit den Bedingungen (7.3) und (7.4) diese Voraussetzung in der Tat mit Wahrscheinlichkeit mindestens $1/2$ erfüllt ist.

Weiter zeigt Ajtai, daß jeder Gittervektor w ungleich Null mit $\|w\| \leq c + \ln b$ eine Kongruenz der Form (7.1) liefert. Sei dazu $w = \sum_{i=1}^{t+2} \delta_i v_i$ mit o.B.d.A. $\delta_{t+1} \geq 0$. Im ersten Schritt wird gezeigt, daß $\delta_{t+1} = 1$ ist (Satz 7.3 a)), und im zweiten Schritt, daß $\delta_i \in \{0, -1\}$ für $i = 1, \cdots, t$ ist (Satz 7.3 b)). Die $(t+2)$-te Koordinate von w ist somit

$$N^{11} \cdot \ln \frac{b(1+\frac{N}{b})^{\delta_{t+2}}}{\prod_{i=1}^{t} p_i^{-\delta_i}}.$$

Damit $\|w\|^2 \leq c + \ln b$ ist, muß $\prod_{i=1}^{t} p_i^{-\delta_i}$ die nächste ganze Zahl zu $b(1+\frac{N}{b})^{\delta_{t+2}}$ sein. Andererseits gilt aber die Näherung $b(1+\frac{N}{b})^{\delta_{t+2}} \approx b(1+\delta_{t+2}\cdot\frac{N}{b}) = b+\delta_{t+2}N$, so daß $b + \delta_{t+2}\, N$ die nächste ganze Zahl zu $b(1+\frac{N}{b})^{\delta_{t+2}}$ ist. Somit hat man eine Kongruenz (Satz 7.3 c)):

$$\prod_{i=1}^{t} p_i^{-\delta_i} \equiv b \,(\mathrm{mod}\, N).$$

Aus (7.4) ergibt sich wiederum die Kongruenz der Form (7.1).

Bemerkung 7.2 *In der Praxis werden für dieses Gitter ebenso wie für das Gitter von Schnorr die reellzahligen Basisvektoren durch rationalzahlige approximiert. Bei Adleman ist es hingegen schon für die Theorie von großer Bedeutung, daß die Basisvektoren rational sind.*

7.5 Korrektheit von Ajtais Reduktion

Satz 7.3 *Seien* $c \in \mathbb{R}_+$, $t, b \in \mathbb{N}$ *und* $N \in \mathbb{N}$ *hinreichend groß mit: i)* $c < 2\ln 2$, *ii)* $N^{10} < b < (2N)^{10}$. *Sei* $L = L(b, N, t)$ *das Gitter mit folgenden Basisvektoren:*

$$\begin{pmatrix} v_1 \\ \vdots \\ v_t \\ v_{t+1} \\ v_{t+2} \end{pmatrix} = \begin{pmatrix} \sqrt{\ln p_1} & \cdots & 0 & 0 & N^{11}\ln p_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & \sqrt{\ln p_t} & 0 & N^{11}\ln p_t \\ 0 & \cdots & 0 & 0 & N^{11}\ln b \\ 0 & \cdots & 0 & N^{-2} & N^{11}\ln(1+\frac{N}{b}) \end{pmatrix}$$

Sei $w \in L$ *ein beliebiger Gittervektor ungleich Null mit* $w = \sum_{i=1}^{t+2} \delta_i v_i$ *und* $\delta_{t+1} \geq 0$. *Falls* $\|w\|^2 \leq c + \ln b$, *dann gilt:*

a) $\delta_{t+1} = 1$,

b) $\delta_i \in \{0, -1\}$ *für* $i = 1, \cdots, t$,

c) $\prod_{i=1}^{t} p_i^{-\delta_i} \equiv b \,(mod\, N)$.

Außerdem gilt:

d) *falls eine* p_t*-glatte, quadratfreie Zahl* g *existiert mit* $g \equiv b \,(mod\, N)$ *und* $|b - g| \leq N^{\frac{3}{2}}$, *dann gibt es einen Gittervektor* w' *mit* $\|w'\|^2 \leq c + \ln b$.

Bemerkung 7.4 *Dieser Satz und der folgende Beweis sind nicht direkt aus [2], sondern aus einer verbesserten Version von Cai/Nerurkar [3].*

Beweis: Es bezeichne $\mathrm{cord}_i(u)$ die i-te Koordinate des Vektors u. Sei wiederum

$$u(w) := \prod_{\substack{i=1 \\ \delta_i > 0}}^{t} p_i^{\delta_i}, \quad v(w) := \prod_{\substack{i=1 \\ \delta_i < 0}}^{t} p_i^{-\delta_i}.$$

Es gilt:

$$\begin{aligned} \|w\|^2 &\geq \sum_{i=1}^{t} \delta_i^2 \ln p_i \\ &= \sum_{\substack{i=1 \\ \delta_i > 0}}^{t} \delta_i^2 \ln p_i + \sum_{\substack{i=1 \\ \delta_i < 0}}^{t} \delta_i^2 \ln p_i \\ &\geq \sum_{\substack{i=1 \\ \delta_i > 0}}^{t} \delta_i \ln p_i - \sum_{\substack{i=1 \\ \delta_i < 0}}^{t} \delta_i \ln p_i \\ &= \ln u(w) + \ln v(w) \end{aligned} \tag{7.6}$$

Aus N hinreichend groß und $i), ii)$ schließt man:

$$|\delta_{t+2}\, N^{-2}| \;=\; |\mathrm{cord}_{t+1}(w)| \;\le\; \|w\| \;\le\; \sqrt{c+\ln b} \;\le\; \sqrt{12\ln 2 + 10\ln N} \;\le\; N.$$

Daraus folgt:

$$|\delta_{t+2}| \le N^3 \tag{7.7}$$

zu **a)** Nach Voraussetzung gilt: $\delta_{t+1} \ge 0$. Man führt im folgenden $\delta_{t+1} = 0$ und $\delta_{t+1} \ge 2$ zum Widerspruch und erhält dann $\delta_{t+1} = 1$.

1.Fall: $\delta_{t+1} = 0$

Es gilt:

$$\|v_{t+2}\| \;>\; N^{11}\ln\left(1+\tfrac{N}{b}\right) \;\ge\; N^{11}\cdot\tfrac{1}{2}\cdot\tfrac{N}{b} \overset{ii)}{>} \tfrac{N^2}{2^{11}} \;\ge\; \sqrt{c+\ln b} \;\ge\; \|w\|.$$

Somit ist der Vektor w kein ganzzahliges Vielfaches des Vektors v_{t+2} und wegen $\delta_{t+1} = 0$ ist eine der Zahlen $u(w), v(w) \in \mathbb{N}$ ungleich 1. Da $u(w)$ und $v(w)$ keinen gemeinsamen Primfaktor haben, gilt: $u(w) \ne v(w)$. Man definiere

$$g_{\min} := \min\{u(w), v(w)\}, \quad g_{\max} := \max\{u(w), v(w)\}.$$

Aus (7.6) folgt: $\ln g_{\min} \le \frac{1}{2}(c + \ln b)$ und mit $i)$ ist:

$$g_{\min} < 2b^{\frac{1}{2}}.$$

Daraus folgt:

$$\begin{aligned}
\left|\sum_{i=1}^{t}\delta_i \ln p_i\right| &= |\ln u(w) - \ln v(w)| \;=\; \ln g_{\max} - \ln g_{\min} \\
&\ge \ln(g_{\min}+1) - \ln g_{\min} \;=\; \ln\left(1+\tfrac{1}{g_{\min}}\right) \\
&\ge \tfrac{1}{2}\cdot\tfrac{1}{g_{\min}} > \tfrac{1}{4}\cdot b^{-\frac{1}{2}} > 2^{-7}N^{-5}
\end{aligned} \tag{7.8}$$

Aus $\delta_{t+1} = 0$ folgt:

$$\begin{aligned}
\left|N^{11}\cdot\sum_{i=1}^{t}\delta_i\ln p_i + \delta_{t+2}\cdot N^{11}\cdot\ln\left(1+\tfrac{N}{b}\right)\right| &= |\mathrm{cord}_{t+2}(w)| \\
&\le \|w\| \\
&\le \sqrt{c+\ln b}.
\end{aligned}$$

Daraus ergibt sich:

$$\begin{aligned}
|\delta_{t+2}| &\ge \frac{|N^{11}\cdot\sum_{i=1}^{t}\delta_i\ln p_i| - \sqrt{c\,+\,\ln b}}{N^{11}\cdot\ln(1+\frac{N}{b})} \\
&\overset{(7.8)}{>} \frac{N^6\cdot 2^{-7} - N}{N^{11}\cdot\frac{N}{b}} \\
&\overset{ii)}{>} \frac{N^6\cdot 2^{-7} - N}{N^{11}\cdot N^{-9}} \\
&\ge N^3 \;\lightning\; \text{zu (7.7)}
\end{aligned}$$

2.Fall: $\delta_{t+1} \geq 2$

Es gilt:

$$\left|\delta_{t+2} \cdot \ln\left(1+\tfrac{N}{b}\right)\right| \overset{(7.7)}{\leq} N^3 \cdot N^{-9} < N^{-2} \tag{7.9}$$

$$\mathrm{cord}_{t+2}(w) = N^{11} \cdot \Big(\sum_{i=1}^{t} \delta_i \ln p_i + \delta_{t+1} \cdot \ln b + \delta_{t+2} \cdot \ln\left(1+\tfrac{N}{b}\right) \Big) \tag{7.10}$$

Es folgt:

$$\begin{aligned}
\|w\|^2 &\overset{(7.6)}{\geq} \ln u(w) + \ln v(w) \;\geq\; |\ln u(w) - \ln v(w)| \;=\; \Big|\sum_{i=1}^{t} \delta_i \ln p_i\Big| \\
&\overset{(7.10)}{\geq} \delta_{t+1} \cdot \ln b - N^{-11} \cdot \mathrm{cord}_{t+2}(w) + \delta_{t+2} \cdot \ln\left(1+\tfrac{N}{b}\right) \\
&\overset{(7.9)}{\geq} 2\ln b - N^{-11} \cdot \sqrt{c+\ln b} - N^{-2} \\
&\geq \tfrac{3}{2}\ln b \;\lightning\; \text{zu } \|w\|^2 \leq c + \ln b
\end{aligned}$$

zu **b)** Wegen $\delta_{t+1} = 1$ gilt:

$$\Big|N^{11} \cdot \Big(\sum_{i=1}^{t} \delta_i \ln p_i + \ln b + \delta_{t+2} \cdot \ln\left(1+\tfrac{N}{b}\right)\Big)\Big| = |\mathrm{cord}_{t+2}(w)| \leq \sqrt{c+\ln b}.$$

Daraus folgt:

$$\begin{aligned}
|\ln u(w) - \ln v(w) + \ln b| &\leq N^{-11} \cdot \sqrt{c+\ln b} + \left|\delta_{t+2} \cdot \ln\left(1+\tfrac{N}{b}\right)\right| \\
&\overset{(7.9)}{\leq} N^{-11} \cdot N + N^{-2} < N^{-1}
\end{aligned} \tag{7.11}$$

Annahme: Es gibt ein $\delta_i > 0$ für ein $i \in \{1, \cdots, t\}$.

Es folgt: $u(w) \geq 2$ und somit:

$$\begin{aligned}
\|w\|^2 &\overset{(7.6)}{\geq} \ln u(w) + \ln v(w) \\
&\overset{(7.11)}{\geq} 2\ln u(w) + \ln b - N^{-1} \\
&\geq 2\ln 2 - N^{-1} + \ln b \\
&\overset{i)}{>} c + \ln b, \quad \text{da } N \text{ hinreichend groß ist} \\
&\lightning \quad \text{zu } \|w\|^2 \leq c + \ln b
\end{aligned}$$

Somit hat man:

$$\delta_i \leq 0 \quad \text{für} \quad i = 1, \cdots, t.$$

Annahme: Es gibt ein $|\delta_i| \geq 2$ für ein $i \in \{1, \cdots, t\}$.

Dann gilt: ${\delta_i}^2 \geq 2|\delta_i|$ und ${\delta_j}^2 \geq |\delta_j|$ für alle anderen $j \in \{1, \cdots, t\}$.

Daraus ergibt sich:

$$\|w\|^2 \;\geq\; \sum_{j=1}^{t} \delta_j^2 \ln p_j \;\geq\; |\delta_i| \ln p_i + \sum_{j=1}^{t} |\delta_j| \ln p_j \;\geq\; 2 \ln 2 + \ln v(w).$$

Mit (7.11) und $u(w) = 1$ folgt:

$$\begin{aligned} \|w\|^2 \;\geq\; \ln b + 2 \ln 2 - N^{-1} \;&>\; c + \ln b \\ &\lightning\; \text{zu } \|w\|^2 \leq c + \ln b \end{aligned}$$

Somit hat man:

$$\delta_i \in \{0, -1\} \quad \text{für} \;\; i = 1, \cdots, t.$$

zu **c)** Nach a) ist $\delta_{t+1} = 1$ und nach b) $u(w) = 1$. Daraus folgt:

$$\begin{aligned} |-\ln v(w) + \ln b + \delta_{t+2} \cdot \ln(1 + \tfrac{N}{b})| \;&=\; |N^{-11} \cdot \mathrm{cord}_{t+2}(w)| \\ &\leq\; N^{-11} \sqrt{c + \ln b} \\ &\leq\; N^{-10.5}. \end{aligned}$$

Aus (7.9) folgt:

$$|-\ln v(w) + \ln b| < N^{-2} + N^{-10.5} < c.$$

Daraus folgt:

$$v(w) \;<\; b \cdot e^c \;<\; 4b.$$

Sei $y := b(1 + \frac{N}{b})^{\delta_{t+2}}$.

Beh.: $v(w)$ ist die nächste ganze Zahl zu y.

Bew.: Folgt aus folgenden drei Ungleichungen:

$$\begin{aligned} |\ln y - \ln v(w)| \;&\leq\; N^{-10.5}, \\ |\ln(v(w) + \tfrac{1}{2}) - \ln v(w)| \;&=\; \left|\ln\left(1 + \tfrac{1}{2v(w)}\right)\right| \\ &\geq\; \tfrac{1}{4v(w)} \;>\; \tfrac{1}{16\,b} \;>\; \tfrac{1}{2^{14}} N^{-10} \\ &>\; N^{-10.5}, \\ |\ln(v(w) - \tfrac{1}{2}) - \ln v(w)| \;&=\; \left|\ln\left(1 + \tfrac{1}{2\,(\,v(w) - \frac{1}{2}\,)}\right)\right| \\ &\geq\; \tfrac{1}{4v(w) - 2} \;>\; \tfrac{1}{4v(w)} \\ &>\; N^{-10.5}. \end{aligned}$$

Andererseits gilt:

$$y \;=\; b\left(1+\tfrac{N}{b}\right)^{\delta_{t+2}} \;=\; b+\delta_{t+2}N+b\tbinom{\delta_{t+2}}{2}\left(\tfrac{N}{b}\right)^2+\cdots \;=\; b+\delta_{t+2}N+R,$$

wobei

$$|R| \;\le\; \delta_{t+2}^2\cdot\tfrac{N^2}{b} \;\overset{(7.7)}{\le}\; N^6\cdot N^2\cdot N^{-10} \;=\; N^{-2}.$$

Somit ist $b+\delta_{t+2}N$ die nächste ganze Zahl zu y und damit $v(w)=b+\delta_{t+2}N$. Man erhält:

$$\prod_{i=1}^{t} p_i^{-\delta_i} \;\overset{b)}{=}\; \prod_{\substack{i=1\\ \delta_i<0}}^{t} p_i^{-\delta_i} \;=\; v(w)\equiv b\,(\mathrm{mod}\,N).$$

zu **d)** Sei $g=b+lN=\prod_{i=1}^{t} p_i^{-\gamma_i}$, wobei $\gamma_i\in\{-1,0\}$. Sei weiterhin $\gamma_{t+1}=1$ und $\gamma_{t+2}=l$. Dann gilt für den Gittervektor $w'=\sum_{i=1}^{t+2}\gamma_i v_i\in L$:

$$\begin{aligned}
\|w'\|^2 &= \sum_{i=1}^{t}\gamma_i^2\ln p_i + l^2N^{-4} + N^{22}\cdot\Big(\sum_{i=1}^{t}\gamma_i\ln p_i+\ln b+l\ln\left(1+\tfrac{N}{b}\right)\Big)^2\\
&= \sum_{i=1}^{t}-\gamma_i\ln p_i + l^2N^{-4} + N^{22}\cdot\Big(-\ln g+\ln b+l\ln\left(1+\tfrac{N}{b}\right)\Big)^2\\
&= \ln g + l^2N^{-4} + N^{22}\cdot\Big(-\ln b-\ln\left(1+\tfrac{lN}{b}\right)+\ln b+l\ln\left(1+\tfrac{N}{b}\right)\Big)^2\\
&= \ln b+\ln\left(1+\tfrac{lN}{b}\right)+l^2N^{-4}+N^{22}\cdot\Big(-\tfrac{lN}{b}-R_1+l\tfrac{N}{b}+lR_2\Big)^2,
\end{aligned}$$

wobei

$$R_1=-\tfrac{1}{2}(\tfrac{lN}{b})^2+\tfrac{1}{3}(\tfrac{lN}{b})^3-\tfrac{1}{4}(\tfrac{lN}{b})^4+\tfrac{1}{5}(\tfrac{lN}{b})^5-\cdots$$

und

$$\begin{aligned}
R_2 &= -\tfrac{1}{2}(\tfrac{N}{b})^2+\tfrac{1}{3}(\tfrac{N}{b})^3-\tfrac{1}{4}(\tfrac{N}{b})^4+\tfrac{1}{5}(\tfrac{N}{b})^5-\cdots\\
&\le \ln b+\tfrac{lN}{b}+l^2N^{-4}+N^{22}\cdot\Big(\left(\tfrac{lN}{b}\right)^2+|l|\cdot(\tfrac{N}{b})^2\Big)^2\\
&\le \ln b+lN^{-9}+l^2N^{-4}+N^{22}\cdot 4l^4N^{-36}.
\end{aligned}$$

Aus $|b-g|\le N^{\frac{3}{2}}$ folgt: $|l|\le N^{\frac{1}{2}}$. Somit gilt:

$$\begin{aligned}
\|w'\|^2 &\le \ln b+N^{\frac{1}{2}}N^{-9}+NN^{-4}+4N^{22}N^2N^{-36}\\
&\le c+\ln b. \quad\square
\end{aligned}$$

Um zu beweisen, daß die Voraussetzung von Satz 7.3d) mit großer Wahrscheinlichkeit erfüllt ist, verwenden wir folgendes Lemma über glatte Zahlen, das auch Adleman in seiner Arbeit benutzt.

Lemma 7.5 [10] *Für alle $c \in \mathbb{N} \setminus \{1\}$ und für alle hinreichend großen natürlichen Zahlen n ist die Anzahl der $\ln^c(n)$-glatten, quadratfreien Zahlen, die kleiner als n sind, größer als $n^{1-\frac{1}{c}}$.*

Satz 7.6 *Sei $N \in \mathbb{N}$ hinreichend groß. Sei p_t die kleinste Primzahl größer als $\ln^{22}(N^{11})$, also insbesondere $t \in \mathbb{N}$ polynomial in $\ln N$. Man wähle $b \in \mathbb{N}$ zufällig mit den Bedingungen (7.3) und (7.4). Dann ist die Wahrscheinlichkeit, daß es eine p_t-glatte, quadratfreie Zahl gibt, die sowohl im Intervall $[\, b - N^{\frac{3}{2}}, b + N^{\frac{3}{2}} \,]$ als auch in der Restklasse $b \,(\mathrm{mod}\, N)$ liegt, mindestens $1/2$.*

Beweis: Sei A das Ereignis, daß es eine p_t-glatte, quadratfreie Zahl gibt, die sowohl im Intervall $[\, b - N^{\frac{3}{2}}, b + N^{\frac{3}{2}} \,]$ als auch in der Restklasse $b \,(\mathrm{mod}\, N)$ liegt. Man wendet Lemma 7.5 auf $c = 22$ und $n = N^{11}$ an. Somit ist für eine beliebige natürliche Zahl aus $[1, N^{11}]$ die Wahrscheinlichkeit, daß es eine p_t-glatte, quadratfreie Zahl ist, größer als

$$\frac{N^{11-\frac{11}{22}}}{N^{11}} = \frac{1}{N^{\frac{1}{2}}}.$$

Im Intervall $[\, b - N^{\frac{3}{2}}, b + N^{\frac{3}{2}} \,]$ liegen $2 \cdot N^{\frac{3}{2}}$ natürliche Zahlen und damit $2 \cdot N^{\frac{1}{2}}$ natürliche Zahlen, die auch in der Restklasse $b \,(\mathrm{mod}\, N)$ liegen. Somit gilt für das Gegenereignis $\bar{A}$ von A:

$$\mathrm{Ws}\,(\bar{A}) \;\leq\; \left(1 - \frac{1}{N^{1/2}}\right)^{2N^{1/2}} \;\leq\; \left(1 - \frac{1}{N^{1/2}}\right)^{N^{1/2}} \;\leq\; e^{-1}.$$

Daraus folgt:

$$\mathrm{Ws}\,(A) \;\geq\; 1 - e^{-1} \;>\; \tfrac{1}{2}. \quad \square$$

Aus Satz 7.6 folgt, daß die Voraussetzung von Satz 7.3d) mit Wahrscheinlichkeit mindestens $1/2$ erfüllt ist, so daß es mit dieser Wahrscheinlichkeit einen Gittervektor mit Euklidischem Normquadrat kleiner gleich $c + \ln b$ gibt. In diesem Fall ist gewährleistet, daß man die für die Faktorisierung nötige Kongruenz (7.1) findet.

Bemerkung 7.7 *Problematisch ist bei Ajtais Reduktion ebenso wie bei den Reduktionen von Schnorr und Adleman, sicherzustellen, daß man bei mehrfacher Anwendung der Reduktion $t + 2$ verschiedene Kongruenzen (7.1) findet.*

Index

Literaturverzeichnis

[1] L.M. Adleman: "Factoring and Lattice Reduction",
Draft, University of Southern California, CA, 1995.

[2] M. Ajtai: "The Shortest Vector Problem in L_2 is NP-hard for Randomized Reductions",
Electronic Colloquium on Computational Complexity, ECCC TR 97-047, 1997.

[3] J. Cai, A. Nerurkar: "Approximating the SVP to within a Factor $(1 + 1/\dim^{\epsilon})$ is NP-hard under Randomized Reductions",
Electronic Colloquium on Computational Complexity, ECCC TR 97-059, 1997.

[4] M.J. Coster, A. Joux, B.A. LaMacchia, A.M. Odlyzko, C.P. Schnorr, J. Stern: "Improved Low-Density Subset Sum Algorithms",
Computational Complexity 2, S. 111-128, 1992.

[5] C.F. Gauß: "Disquisitiones Arithmeticae",
Leipzig, 1801, Deutsche Übersetzung: "Untersuchungen über höhere Arithmetik", Springer-Verlag, Berlin/Heidelberg, 1889.

[6] P.M. Gruber, C.G. Lekkerkerker: "Geometry of Numbers",
North-Holland, Amsterdam, 1987.

[7] J.C. Lagarias, A.M. Odlyzko: "Solving Low-Density Subset Sum Problems",
Journal of the Association for Computing Machinery 32, S. 229-246, 1985.

[8] A.K. Lenstra, H.W. Lenstra, Jr., L. Lovász: "Factoring Polynomials with Rational Coefficients",
Mathematische Annalen 261, S. 515-534, 1982.

[9] A.K. Lenstra, H.W. Lenstra, Jr.: "The Development of the Number Field Sieve",
Springer Lecture Notes in Mathematics 1554, 1993.

[10] C. Pomerance: in Adleman [1] als persönliche Mitteilung zitiert.

[11] C.P. Schnorr: “Factoring Integers and Computing Discrete Logarithms via Diophantine Approximation“,
AMS DIMACS Series in Discrete Mathematics and Theoretical Computer Science 13, S. 171-181, 1993.

[12] M. Seysen: “Simultaneous Reduction of a Lattice Basis and its Reciprocal Basis“,
Combinatorica 13, S. 363-376, 1993.

[13] M. Seysen: “A Measure for the Non-Orthogonality of a Lattice Basis“,
Manuskript, 1994.

[14] B. Vallée : “Gauss’ Algorithm Revisited“,
Journal of Algorithms 12, S. 556-572, 1991.