UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Fakultät für Elektrotechnik, Informatik und Mathematik
Institut für Informatik

Diplomarbeit
im Studiengang Mathematik

Samplemethoden in der algorithmischen Geometrie der Zahlen

von
Stefanie Naewe

vorgelegt bei
Prof. Dr. Johannes Blömer

Betreuer
Prof. Dr. Johannes Blömer

30. März 2006

Erklärung

Ich versichere, dass ich die beiliegende Diplomarbeit ohne Hilfe Dritter und ohne anderer als der angegebenen Quellen und Hilfsmittel angefertigt und die den benutzten Quellen wörtlich oder inhaltlich entnommenden Stellen als solche kenntlich gemacht habe.

Hövelhof, den 30. März 2006

Stefanie Naewe

Danksagung

Diese Studienarbeit ist im Rahmen meines Mathematikstudiums an der Universität Paderborn entstanden. Ich möchte mich hiermit bei Prof. Dr. Johannes Blömer für die sehr gute Betreuung bedanken, sowie bei Julia Borghoff, Carmen Krogmeier, Holger Mense, Melanie Merschjohann, Sabine Naewe und Christiane Peters für das Korrekturlesen und die hilfreichen Kommentare.

Inhaltsverzeichnis

1. Einleitung

Das Forschungsgebiet „Geometrie der Zahlen", auch „geometrische Zahlentheorie" genannt, wurde von Hermann Minkowski Anfang des 19. Jahrhunderts begründet [20]. Die Geometrie der Zahlen verwendet geometrische Methoden, um zahlentheoretische Probleme zu lösen, zum Beispiel die diophantische Approximation, und verbindet auf diese Weise diskrete Elemente wie Ganzzahligkeit mit Aspekten der Geometrie. Grundlegendes Thema in der Geometrie der Zahlen ist die Fragestellung, welche Bedingungen ein konvexer Körper im euklidischen Raum erfüllen muss, damit er Punkte mit ganzzahligen Koordinaten enthält. Eine klassische Einführung in die Methodik der Geometrie der Zahlen gibt Cassels [10].

Zu Beginn der 80er Jahre begann man die Methoden der „klassischen" Geometrie der Zahlen unter einem algorithmischen und komplexitätstheoretischen Aspekt zu betrachten Im Jahr 1983 entwickelte H. W. Lenstra einen Polynomzeitalgorithmus für ganzzahlige Programmierung in fester Dimension [27]. Ausgehend von diesem Ergebnis gewann der algorithmische Aspekt der Geometrie der Zahlen in den letzten Jahrzehnten zunehmend an Bedeutung, da die Ergebnisse vielfältige Anwendungen in zahlreichen Bereichen der angewandten Mathematik fanden, unter anderem der Kodierungstheorie, Kryptographie und Optimierung.

Minkowski prägte in seiner Arbeit [20] den Begriff des Gitters beziehungsweise der quadratischen Form, obwohl bereits Gauß und Lagrange mit diesem mathematischen Objekt gearbeitet haben. Ein Gitter ist eine diskrete Untergruppe des $\mathbb{R}^n$ und wird üblicherweise durch eine Basis dargestellt. Innerhalb der Gittertheorie gibt es zwei wesentliche Probleme:

Problem des kürzesten Gittervektors: Finde zu einer Gitterbasis einen möglichst kurzen von 0 verschiedenen Gittervektor.

Problem des nächsten Gittervektors: Finde zu einem gegebenen Vektor einen möglichst nahen Gittervektor.

Diese beiden Probleme sind – zumindest unter randomisierter Reduktion – NP-hart und die meisten Anwendungen der Geometrie der Zahlen beruhen auf diesen Problemen. Eine der großen Fragen ist es, ob das Problem des nächsten Gittervektors NP-vollständig ist.

Die Bedeutung der beiden Probleme beruht unter anderem auf der Tatsache, dass man in den vergangenen Jahren Kryptosysteme entwickelt hat, deren Sicherheit auf der Schwierigkeit dieser Probleme beruht. Andererseits kann man approximative Lösungen der Probleme für Attacken auf Kryptosysteme verwenden, zum Beispiel auf RSA. Auf Grund der vielfältigen Anwendungsmöglichkeiten wurden die beiden Probleme „Problem des kürzesten Gittervektors" und „Problem des nächsten Gittervektors" in den letzten Jahren intensiv untersucht. Grundlage für die meisten Untersuchungen ist der LLL-Algorithmus von Lenstra, Lenstra und Lovász aus dem Jahr 1982, der in polynomieller Zeit das Problem des kürzesten Gittervektors mit dem Faktor $2^{\frac{n-1}{2}}$ approximiert. Eine genauere Übersicht über die Entwicklungsgeschichte dieser Probleme wird in Abschnitt 2.5 gegeben.

Da das Problem des kürzesten Gittervektors und das Problem des nächsten Gittervektors schwer zu lösen sind, verwendet man zur Lösung beziehungsweise zur Approximation häufig randomisierte Algorithmen. Die Randomisierung besteht in den meisten Fällen darin, dass man Punkte aus einem Bereich, meist einem konvexen Körper, zufällig auswählt. Solche Methoden bezeichnet man als Samplemethoden. Die erste Samplemethode zur Lösung des Problems des kürzesten Gittervektors bezüglich der ℓ_2-Norm wurde von Ajtai, Kumar und Sivakumar [2] im Jahr 2001 entwickelt. Ein Jahr später stellten sie eine Turingreduktion mit einfach exponentieller Laufzeit vom Problem des nächsten Gittervektors auf das Problem des kürzesten Gittervektors mit dem Approximationsfaktor $(1 + \epsilon)$ für ein $\epsilon > 0$ vor [3].

In dieser Diplomarbeit wird eine Samplemethode vorgestellt, die auf Ideen von Sudan und Regev beruht. Mit Hilfe der Samplemethode kann man einen Gittervektor wählen, dessen Länge kleiner als eine vorgegebene Konstante ist. Durch eine geringfügige Modifikation kann dann das Problem des kürzesten Gittervektors für jede ℓ_p-Norm mit einfach exponentieller Laufzeit gelöst werden. Unter der Voraussetzung, dass man das Problem des kürzsten Gittervektors exakt lösen kann, kann man mit Hilfe einer von Blömer entwickelten Variation dieser Samplemethode das Problem des nächsten Gittervektors mit dem Approximationsfaktor $c(1 + \epsilon)^2$ für eine Konstante c und $\epsilon > 0$ lösen. Die Reduktion verwendet im Wesentlichen die Ideen und Methoden von Ajtai, Kumar und Sivakumar in [3]. Es ist aber nicht gelungen, ebenfalls den Approximationsfaktor $(1 + \epsilon)$ zu erreichen.

Die Arbeit gliedert sich in folgende Teile:

Kapitel 2: Dieses Kapitel gibt eine grundlegende Einführung in die Theorie der Gitter sowie die Komplexität des Problems des kürzesten Gittervektors und des Problems des nächsten Gittervektors soweit sie für diese Arbeit benötigt werden.

Kapitel 3: Auf der Grundlage von Ideen von Regev und Sudan wird eine allgemeine Samplemethode beschrieben, die Gittervektoren berechnet, deren Länge bezüglich der ℓ_p-Norm kleiner als eine Konstante sind. Ein besonderer Schwerpunkt liegt in der Beschreibung der Funktionsweise, sowie allgemeinen Aussagen über die Eigenschaften dieser Methode.

Kapitel 4: In diesem Kapitel wird eine Modifikation der Samplemethode aus Kapitel 3 vorgestellt, mit der man das Problem des kürzesten Gittervektors bezüglich der ℓ_p-Norm durch einen randomisierten Algorithmus mit einfach exponentieller Laufzeit lösen kann.

Kapitel 5 Dieses Kapitel zeigt, dass man unter der Voraussetzung, dass man das Problem des kürzesten Gittervektors exakt lösen kann und unter Verwendung einer Variation der Samplemethode aus Kapitel 3, das Problem des nächsten Gittervektors in einfach exponentieller Laufzeit approximieren kann.

Das Kapitel 3 bildet die Grundlage für die Kapitel 4 und 5, wobei diese aber unabhängig voneinander gelesen werden können.

2. Einführung in die Theorie der Gitter

In diesem Kapitel soll eine kurze Einführung in die Theorie der Gitter gegeben werden. Sie beruht auf [28] und soll die Grundlagen der Gittertheorie darstellen, soweit sie für diese Arbeit benötigt werden. Eine detailliertere Einführung gibt [28].

2.1. Grundlagen

Sei $\mathbb{R}^m$ ein m-dimensionaler euklidischer Vektorraum. Ein Gitter im $\mathbb{R}^m$ ist definiert als die Menge

$$\mathcal{L}(b_1, \ldots, b_n) = \left\{ \sum_{i=1}^{n} x_i b_i | x_i \in \mathbb{Z} \right\}$$

aller ganzzahligen Linearkombinationen von n linear unabhängigen Vektoren $b_1, \ldots, b_n$. Der Rang des Gitters ist n und m ist die Dimension des Gitters. Die Menge $B = \{b_1, \ldots, b_n\}$ wird eine Gitterbasis genannt. Wenn man B als Matrix

$$B = [b_1, \ldots, b_n] \in \mathbb{R}^{m \times n}$$

betrachtet, so kann ein Gitter unter Verwendung der Matrix-Vektor-Multiplikation auch als folgende Menge definiert werden:

$$\mathcal{L}(B) = \{Bx | x \in \mathbb{Z}^n\}.$$

Ohne Bezug auf eine Basis kann man ein Gitter L auch als eine diskrete additive Untergruppe des $\mathbb{R}^m$ charakterisieren.

Im Fall $n = m$, falls also Rang und Dimension übereinstimmen, heißt $\mathcal{L}(B)$ ein volldimensionales Gitter. Das Gitter $\mathcal{L}(B)$ ist also genau dann volldimensional, wenn der von B aufgespannte Vektorraum $\text{span}(B) = \{Bx | x \in \mathbb{R}^n\}$ gleich dem Raum $\mathbb{R}^m$ ist. Der Unterschied zwischen $\mathcal{L}(B)$ und $\text{span}(B)$ besteht darin, dass bei einem Gitter nur ganzzahlige Linearkombinationen erlaubt sind. Es ist offensichtlich, dass $\text{span}(B)$ nicht von der Basis B abhängt, das heißt wenn B und B' das gleiche Gitter erzeugen, so ist $\text{span}(B) = \text{span}(B')$. Deswegen wird für jedes Gitter $L = \mathcal{L}(B)$ der aufgespannte Vektorraum unabhängig von der Basis definiert und man bezeichnet ihn allgemein mit $\text{span}(L)$. Die Menge B ist eine Basis von $\text{span}(B)$ als Vektorraum und damit ist der Rang des Gitters $\mathcal{L}(B)$ gleich der Dimension von $\text{span}(B)$. Eine beliebige Menge von n linear unabhängigen Gittervektoren $B' \in \mathcal{L}(B)$ ist eine Basis für $\text{span}(B)$, aber nicht notwendig auch eine Gitterbasis für $\mathcal{L}(B)$.

Sei $B' = \{b'_1, \ldots, b'_n\}$ eine Menge mit n linear unabhängige Gittervektoren, das heißt $b'_i \in \mathcal{L}(B)$ für $i = 1, \ldots, n$. Man definiert ein halboffenes Parallelepiped

$$\mathcal{P}(B') = \left\{ \sum_{i=1}^{n} x_i b'_i | 0 \leq x_i < 1 \right\}$$

Dann ist B' genau dann eine Gitterbasis für $\mathcal{L}(B)$, wenn $\mathcal{P}(B')$ keinen anderen Gittervektor enthält als den Ursprung. Für eine Gitterbasis B bezeichnet man $\mathcal{P}(B)$ als Fundamentalbereich des Gitters bezüglich der Basis B.

Da B' eine Menge von linear unabhängigen Vektoren ist, ist $\mathcal{L}(B')$ ein Gitter mit der Gitterbasis B'. Offensichtlich gilt $\mathcal{L}(B') \subseteq \mathcal{L}(B)$. Man bezeichnet $\mathcal{L}(B')$ auch als Untergitter von $\mathcal{L}(B)$. Falls $\mathcal{L}(B') = \mathcal{L}(B)$, so heißen die Basen B und B' äquivalent. Algebraisch sind äquivalente Basen dadurch charakterisiert, dass eine unimodulare Matrix $U \in \mathbb{Z}^{n\times n}$ existiert, das heißt eine Matrix mit ganzzahligen Einträgen und $\det(U) = \pm 1$, mit $B' = B \cdot U$.

Die Determinante eines Gitters $L = \mathcal{L}(B)$ ist das n-dimensionale Volumen des Fundamentalbereiches $\mathcal{P}(B)$, das durch die Basisvektoren aufgespannt wird. Sie ist eine Gitterinvariante, da für zwei äquivalente Basen B und B' eine unimodulare Matrix U existiert mit $B' = B \cdot U$. Am einfachsten kann man die Determinante eines Gitters mit der Gram-Schmidt-Orthogonalisierung berechnen, denn die Determinante ist gleich dem Produkt der Längen der orthogonalisierten Vektoren $b_1^*, \ldots, b_n^*$ der Basis $b_1, \ldots, b_n$:

$$\det(\mathcal{L}(B)) = \prod_{i=1}^{n} ||b_i^*||_2.$$

2.2. Sukzessive Minima und die Sätze von Minkowski

Die Sätze von Minkowski bilden die Grundlage für die gesamte Geometrie der Zahlen und insbesondere der Gittertheorie. Sie verwenden weitere Invarianten des Gitters, die sukzessiven Minima.

2.2.1. Sukzessive Minima

Im Folgenden sei L ein Gitter der Dimension m vom Rang n. Sei $B_m(0,r) = \{x \in \mathbb{R}^m | \; ||x|| < r\}$ die offene m-dimensionale Kugel vom Radius r um den Ursprung bezüglich der Norm $||.||$. Die Bezeichnung $||.||$ wird in dieser Arbeit verwendet, wenn eine beliebige Norm gemeint ist. Die ℓ_p-Norm wird mit $||.||_p$ bezeichnet, insbesondere also die ℓ_2-Norm mit $||.||_2$ und die ℓ_∞-Norm mit $||.||_\infty$. Falls die Dimension offensichtlich ist, notiert man $B(0,r)$.

Für ein Gitter L vom Rang n und $1 \leq i \leq n$ definiert man das i-te Minimum $\lambda_i(L)$ als den Radius der kleinsten Kugel um den Ursprung, die i linear unabhängige Gittervektoren enthält:

$$\lambda_i(L) = \inf\{r | \dim(\mathrm{span}(L \cap B(0,r))) \geq i\}.$$

Diese sukzessiven Minima $\lambda_1(L), \lambda_2(L), \ldots, \lambda_n(L)$ sind für jedes Gitter wichtige Konstanten. Falls eindeutig ist, welches Gitter gemeint ist, so schreibt man auch $\lambda_1, \lambda_2, \ldots, \lambda_n$. Sukzessive Minima können in Bezug auf jede Norm definiert werden. Mit $\lambda_i^{(p)}(L)$ bezeichnet man das i-te sukzessive Minimum bezüglich der ℓ_p-Norm. Wenn sich aus dem Kontext eindeutig ergibt, welche Norm verwendet wird, so schreibt man $\lambda_i(L)$. Man kann zeigen, dass für jedes Gitter die sukzessiven Minima angenommen werden können, das heißt es existieren $x_1, \ldots, x_n \in L$ mit $||x_i|| = \lambda_i(L)$. Entsprechend dieser Definition ist $\lambda_1(L)$ die Länge der kürzesten Gittervektoren ungleich 0 im Gitter L. Wenn im Folgenden von den kürzesten Gittervektoren gesprochen

wird, so sind immer die kürzesten Gittervektoren ungleich 0 gemeint. Die Länge der kürzesten Gittervektoren ist gleich dem minimalen Abstand zwischen zwei verschiedenen Gitterpunkten:

$$\lambda_1(L) = \min_{x \neq y \in L} ||x - y|| = \min_{x \in L \setminus \{0\}} ||x||.$$

Die Vektoren $x_1, \ldots, x_n \in L$ mit $||x_i|| = \lambda_i(L)$ für $i = 1, \ldots, n$ bilden nicht notwendigerweise eine Basis des Gitters L. Mit $\mathrm{bl}(L)$ bezeichnet man das Minimum r, so dass $B(0, r)$ eine Menge von Vektoren enthält, die L erzeugen. Es gilt:

$$\lambda_n(L) \leq \mathrm{bl}(L).$$

2.2.2. Das 1. Theorem von Minkowski

Das 1. Theorem von Minkowski bildet eine wichtige obere Schranke für die Länge des kürzesten Gittervektors in einem Gitter L. Es beruht auf folgendem grundlegenden Theorem:

Theorem 2.2.1 Theorem von Blichfeldt
Sei L ein beliebiges Gitter und $S \subseteq \mathrm{span}(L)$ eine messbare Menge, das heißt man kann $\mathrm{vol}(S)$ bestimmen. Falls $\mathrm{vol}(S) > \det(L)$, dann existieren zwei verschiedene Punkte $z_1, z_2 \in S$ mit $z_1 - z_2 \in L$.

Beweis: Sei L ein beliebiges Gitter, B eine Basis von L und $S \subseteq \mathrm{span}(L)$ mit $\mathrm{vol}(S) > \det(L)$. Die Menge S soll nun disjunkt in verschiedene Mengen aufgeteilt werden. Für jeden Gitterpunkt $v \in L$ definiere man

$$S_v = S \cap (\mathcal{P}(B) + v).$$

Da B eine Basis ist, bilden die Mengen S_v mit $v \in L$ eine Partition von S: $S = \bigcup_{v \in L} S_v$.
Da L abzählbar ist, gilt:

$$\mathrm{vol}(S) = \sum_{v \in L} \mathrm{vol}(S_v).$$

Man betrachte nun die verschobenen Mengen

$$S'_v = S_v - v = (S - v) \cap \mathcal{P}(B)$$

Für alle $v \in L$ gilt dann $S'_v \subseteq \mathcal{P}(B)$, das heißt $\mathrm{vol}(S'_v) \leq \mathrm{vol}(\mathcal{P}(B))$ und $\mathrm{vol}(S_v) = \mathrm{vol}(S'_v)$.

Im Folgenden soll nun gezeigt werden, dass die Mengen S'_v mit $v \in L$ nicht paarweise disjunkt sind. Dies zeigt man indirekt, das heißt man nimmt an, dass die Mengen S'_v paarweise disjunkt sind. Dann gilt:

$$\sum_{v \in L} \mathrm{vol}(S'_v) = \mathrm{vol}(\bigcup_{v \in L} S'_v) \leq \mathrm{vol}(\mathcal{P}(B)).$$

Nach Voraussetzung ist

$$\sum_{v \in L} \mathrm{vol}(S'_v) = \sum_{v \in L} \mathrm{vol}(S_v) = \mathrm{vol}(S) > \det(L)$$

und damit erhält man den Widerspruch $\det(L) < \mathrm{vol}(\mathcal{P}(B))$.
Also können die Mengen S'_v mit $v \in L$ nicht paarweise disjunkt sein.

Man betrachte zwei Vektoren $v, w \in L$ mit $S'_v \cap S'_w \neq \emptyset$. Für $z \in S'_v \cap S'_w$ gilt dann:

- Aus $z \in S'_v$ erhält man $z = z_1 - v$ mit $z_1 \in S_v \subseteq S$.
- Aus $z \in S'_w$ erhält man $z = z_2 - w$ mit $z_2 \in S_w \subseteq S$.

Da v und w verschieden sind, gilt $z_1 \neq z_2$, und damit ergibt sich

$$z_1 - z_2 = z + v - (z + w) = v - w \in L\backslash\{0\}$$

□

Als Folgerung aus diesem Theorem erhält man folgendes Theorem von Minkowski:

Theorem 2.2.2 Convex body theorem
Sei L ein beliebiges Gitter vom Rang n und $S \subseteq \text{span}(L)$ eine konvexe Menge, die symmetrisch zum Ursprung ist. Falls $\text{vol}(S) > 2^n \det(L)$, dann enthält S einen von Null verschiedenen Gitterpunkt $v \in S \cap L\backslash\{0\}$.

Beweis: Man betrachte die Menge $S' = \{x \mid 2 \cdot x \in S\}$. Für das Volumen von S' gilt:

$$\text{vol}(S') = 2^{-n} \text{vol}(S) > \det(L)$$

Nach dem Theorem von Blichfeldt 2.2.1 existieren zwei verschiedene Punkte $z_1, z_2 \in S'$ mit $z_1 - z_2 \in L\backslash\{0\}$. Damit sind $2z_1, 2z_2 \in S$ und die Symmetrie von S zum Ursprung impliziert $-2z_2 \in S$. Weil S konvex ist, gilt:

$$\frac{1}{2}(2z_1 + (-2z_2)) = z_1 - z_2 \in S.$$

Folglich enthält S den Gitterpunkt $v = z_1 - z_2 \neq 0$.

□

Mit Hilfe dieses Theorems kann man die Länge der kürzesten von 0 verschiedenen Gittervektoren in L bezüglich der ℓ_∞-Norm beschränken.

Satz 2.2.3 *Sei L ein beliebiges Gitter vom Rang n. Dann gilt für die Länge des kürzesten Gittervektors bezüglich der ℓ_∞-Norm:*

$$\lambda_1^{(\infty)}(L) < \det(L)^{\frac{1}{n}}$$

Beweis: Sei $S = B(0, \det(L)^{\frac{1}{n}}) \cap \text{span}(L)$ die offene Kugel mit dem Radius $\det(L)^{\frac{1}{n}}$ in $\text{span}(L)$. Die Menge S ist konvex, symmetrisch zum Ursprung und $\text{vol}(S) = (2 \det L^{\frac{1}{n}})^n = 2^n \det(L)$. Nach Minkowskis Convex body theorem 2.2.2 existiert ein von 0 verschiedener Gittervektor $v \in L\backslash\{0\}$ mit $v \in S$, das heißt $||v||_\infty < \det(L)^{\frac{1}{n}}$. Damit ist die Länge des kürzesten Gittervektors in L bezüglich der ℓ_∞-Norm nach oben beschränkt:

$$\lambda_1^{\infty}(L) < \det(L)^{\frac{1}{n}}$$

□

Als Folgerung aus diesem Satz erhält man eine obere Schranke für die Länge der kürzesten von 0 verschiedenen Gittervektoren in einem Gitter bezüglich der ℓ_2-Norm.

Korollar 2.2.4 Minkowskis 1. Theorem
Sei L ein beliebiges Gitter vom Rang n. Dann gilt für die Länge des kürzesten Gittervektors bezüglich der ℓ_2-Norm:

$$\lambda_1^{(2)}(L) < \sqrt{n}\det(L)^{\frac{1}{n}}.$$

Beweis: Die Behauptung folgt direkt aus Satz 2.2.3, da für alle $v \in L$ gilt:

$$||v||_2 \leq \sqrt{n}||v||_\infty.$$

□

2.3. Duale Gitter

Analog zum Dualraum in der Theorie der Vektorräume kann man duale Gitter betrachten. Durch die Abbildung $\text{span}(L) \to (\text{span}(L))^*$, $v \mapsto f_v$ mit $f_v(y) = \langle v, y\rangle$ kann man den Vektorraum $\text{span}(L)$ mit seinem Dualraum $(\text{span}(L))^* = \text{Hom}(\text{span}(L), \mathbb{R})$ identifizieren. Das duale Gitter L^* von L ist dann

$$L^* = \text{Hom}(L, \mathbb{Z}) = \{y \in \mathbb{R}^n | \langle v, y\rangle \in \mathbb{Z} \text{ für alle } v \in L\}.$$

Definition 2.3.1 *Für ein Gitter L ist sein duales Gitter definiert durch*

$$L^* = \{y \in \text{span}(L) | \langle v, y\rangle \in \mathbb{Z} \textit{ für alle } v \in L\}.$$

Das Duale eines Gitter L ist die Menge aller Punkte des von L aufgespannten Vektorraumes, deren Skalarprodukt mit jedem Punkt des Gitters ganzzahlig ist.

Geometrisch liegt die Menge aller Punkte, deren Skalarprodukt mit einem Gitterpunkt $v \in L$ ganzzahlig ist, in einer Menge von Hyperebenen orthogonal zu diesem Gitterpunkt. Eine Hyperebene enthält jeweils die Punkte, deren Skalarprodukt mit v den gleichen Wert hat. Sei $v \in L$ und $v_0 \in \text{span}(L)$ mit $\langle v_0, v\rangle = 1$. Dann haben die Hyperebenen, in denen das duale Gitter enthalten ist, in Bezug auf v folgende Darstellung:

$$\begin{aligned} H_0 &= \{y \in \text{span}(L) | \langle v, y\rangle = 0\} \\ H_i &= \{y \in \text{span}(L) | \langle v, y\rangle = i\} \\ &= \{i \cdot v_0 + y | y \in \text{span}(L) \text{ mit } \langle v, y\rangle = 0\} \\ &= i \cdot v_0 + H_0 \qquad \text{für } i \in \mathbb{Z}. \end{aligned}$$

Der Abstand zwischen den einzelnen Hyperebenen beträgt $\frac{1}{||v_0||_2}$. Damit erzwingt jeder Gittervektor $v \in L$, dass alle Punkte aus L^* in einer dieser Hyperebenen liegen.

Definition 2.3.2 *Für eine Gitterbasis $B = [b_1, \ldots, b_n] \in \mathbb{R}^{m\times n}$ ist die duale Basis $D = [d_1, \ldots, d_n] \in \mathbb{R}^{m\times n}$ definiert als die eindeutig bestimmte Basis mit den folgenden Eigenschaften:*

- $\text{span}(D) = \text{span}(B)$,
- $B^T D = I$, *das heißt* $\langle b_i, d_j \rangle = \delta_{ij}$.

Die Matrix D ist als Lösung eines linearen Gleichungssystems eindeutig bestimmt. Im Allgemeinen erhält man D durch $D = B(B^T B)^{-1}$. Falls $B \in \mathbb{R}^{n \times n}$, das heißt falls $\mathcal{L}(B)$ ein volles Gitter ist, so ist $D = (B^T)^{-1}$.

Das folgende Lemma zeigt, dass L^* wirklich ein Gitter im Sinne der Definition ist.

Lemma 2.3.3 *Sei D die duale Basis von B. Dann ist*

$$(\mathcal{L}(B))^* = \mathcal{L}(D).$$

Beweis: Jeder Gittervektor $x \in \mathcal{L}(B)$ hat die Darstellung $x = \sum_{i=1}^n a_i b_i$ mit $a_i \in \mathbb{Z}$. Nach Definition der dualen Basis D gilt für alle $j \in \{1, \ldots, n\}$:

$$\langle x, d_j \rangle = \sum_{i=1}^n a_i \langle b_i, d_j \rangle = a_i \in \mathbb{Z}$$

und damit $D \subseteq (\mathcal{L}(B))^*$. Unter Berücksichtigung der Abgeschlossenheit von $(\mathcal{L}(B))^*$ bezüglich der Addition ist damit auch $\mathcal{L}(D) \subseteq (\mathcal{L}(B))^*$.
Um zu zeigen, dass $\mathcal{L}(B))^*$ in $\mathcal{L}(D)$ enthalten ist, betrachtet man einen beliebigen Vektor $y \in (\mathcal{L}(B))^*$. Dann ist $y \in \text{span}(B) = \text{span}(D)$ und damit kann y als Linearkombination der dualen Basis dargestellt werden:

$$y = \sum_{i=1}^n a_i d_i \text{ mit } a_i \in \mathbb{R}.$$

Nach Voraussetzung ist $\langle y, b_j \rangle \in \mathbb{Z}$ für alle $j \in \{1, \ldots, n\}$. Wegen $\langle y, b_j \rangle = \sum_{i=1}^n a_i \langle d_i, b_j \rangle = a_j$ sind die Koeffizienten der betrachteten Linearkombination ganzzahlig, das heißt $a_j \in \mathbb{Z}$. Damit ist $y \in \mathcal{L}(D)$.

□

Lemma 2.3.4 *Für jedes Gitter L gilt:*

$$(L^*)^* = L$$

Beweis: Sei B eine Basis von L. Dann ist $B(B^T B)^{-1}$ eine Basis von L^* und

$$B(B^T B)^{-1} \left(\left(B(B^T B)^{-1} \right)^T B(B^T B)^{-1} \right)^{-1} = B.$$

Folglich ist B eine Basis von $(L^*)^*$.

□

Das folgende Lemma zeigt, dass das Volumen des Fundamentalbereiches von L^* reziprok zu dem Volumen des Fundamentalbereiches von L ist.

Lemma 2.3.5 *Für jedes Gitter L gilt:*

$$\det(L^*) = \frac{1}{\det(L)}$$

Beweis: Sei B eine Basis des Gitters L und D die duale Basis von B. Dann erhält man durch Berechnung:

$$\begin{aligned}
\det(L^*) &= \sqrt{\det(D^T D)} \\
&= \sqrt{\det((B(B^T B)^{-1})^T B(B^T B)^{-1})} \\
&= \frac{1}{\sqrt{\det(B^T B)}} \\
&= \frac{1}{\det(L)}
\end{aligned}$$

□

2.4. Transferschranken

Die Beziehungen zwischen einem Gitter L und seinem dualen Gitter L^* werden durch Transferschranken beschrieben. Die folgenden zwei Sätze beschreiben elementare Transferschranken, die direkt aus dem Theorem von Minkowski beziehungsweise aus den Eigenschaften des dualen Gitters folgen.

Satz 2.4.1 *Sei L ein Gitter vom Rang n. Dann gilt bezüglich der ℓ_2-Norm:*

$$\lambda_1(L) \cdot \lambda_1(L^*) \leq n.$$

Beweis: Aus dem Theorem von Minkowski, 2.2.4, folgt:

$$\begin{aligned}
\lambda_1(L) &\leq \sqrt{n}\sqrt[n]{\det(L)} \\
\lambda_1(L^*) &\leq \sqrt{n}\sqrt[n]{\det(L^*)} = \frac{\sqrt{n}}{\sqrt[n]{\det(L)}} \\
\Longrightarrow \lambda_1(L) \cdot \lambda_1(L^*) &\leq n
\end{aligned}$$

□

Satz 2.4.2 *Sei L ein beliebiges Gitter vom Rang n. Dann gilt bezüglich der ℓ_2-Norm:*

$$\lambda_1(L) \cdot \lambda_n(L^*) \geq 1$$

Beweis: Sei $u \in L$ mit $||u||_2 = \lambda_1(L)$. Wenn man eine beliebige Menge $x_1, \ldots, x_n$ von n linear unabhängigen Vektoren in L^* betrachtet, so sind nicht alle Vektoren orthogonal zu u. Es existiert ein $i \in \{1, \ldots, n\}$ mit $\langle x_i, u \rangle \neq 0$. Nach Definition des dualen Gitters gilt $\langle x_i, u \rangle \in \mathbb{Z}$. Der Vektor x_i liegt nicht auf der Hyperebene orthogonal zu u, die 0 enthält, da das Skalarprodukt ungleich 0 ist. Damit gilt:

$$||x_i||_2 \geq \frac{1}{||u||_2},$$

□

Es soll an dieser Stelle noch eine Transferschranke von Cai genannt werden, die im späteren Verlauf benötigt wird. Sie stellt eine Beziehung zwischen der Länge der kürzesten Basis eines Gitters L und der Länge der kürzesten Gittervektoren des dualen Gitters L^* her.

Satz 2.4.3 Transferschranke von Cai
Sei L ein Gitter der Dimension n und $c > \frac{3}{2\pi}$ konstant. Dann gilt für n genügend groß:

$$\mathrm{bl}(L)\lambda_1(L^*) \leq cn.$$

Der Beweis dieses Satzes benutzt Techniken aus der Funktionentheorie und ist im Anhang A einsehbar.

2.5. Das „Problem des kürzesten Gittervektors" und das „Problem des nächsten Gittervektors"

Das 1. Theorem von Minkowski 2.2.4 liefert eine obere Schranke für die Länge $\lambda_1(L)$ der kürzesten von 0 verschiedenen Gittervektoren in einem Gitter L. Die Länge $\lambda_1(L)$ kann beliebig klein werden. Außerdem ist der Beweis von Minkowskis 1. Theorem nicht konstruktiv. Man kann zwar zeigen, dass jedes Gitter einen Vektor kürzester Länge besitzt, aber aus dem Beweis folgt keine Methode, wie man einen solchen Vektor berechnen kann. Das Problem, in einem Gitter L einen Vektor der Länge $\lambda_1(L)$ zu finden, ist auch bekannt als das „Problem des kürzesten Gittervektors".

Definition 2.5.1 Problem des kürzesten Gittervektors (SVP)
Gegeben sei ein Gitter L. Man finde einen von 0 verschiedenen Vektor $u \in L$ mit

$$||u|| \leq ||v|| \text{ für alle } v \in L\backslash\{0\}.$$

Bis jetzt ist noch kein Algorithmus bekannt, der das Problem des kürzesten Gittervektors in polynomieller Zeit löst.

Ein mit dem Problem des kürzesten Gittervektors verwandtes Problem ist das Problem des nächsten Gittervektors:

Definition 2.5.2 Problem des nächsten Gittervektors (CVP)
Gegeben sei ein Gitter L und ein Vektor $t \in \text{span}(L)$. Gesucht ist ein Vektor $z \in L$, der zu t am nächsten liegt, das heißt es soll gelten:

$$||z - t|| \leq ||v - t|| \text{ für alle } v \in L.$$

Bei der Untersuchung der Probleme SVP und CVP kann man verschiedene Fragestellungen betrachten:

Suchproblem: Finde einen von 0 verschiedenen Gittervektor $z \in L$, so dass $||z - t||$ beziehungsweise $||z||$ minimiert wird.

Optimierungsproblem: Gesucht ist das Minimum von $||z - t||$ beziehungsweise $||z||$ über alle $z \in L$ beziehungsweise $z \in L\backslash\{0\}$.

Entscheidungsproblem: Gegeben ist eine Zahl $r \in \mathbb{Q}$. Entscheide, ob es einen von 0 verschiedenen Gittervektor $z \in L$ gibt mit $||z - t|| \leq r$ beziehungsweise $||z|| \leq r$.

Alle zur Zeit bekannten Exponentialzeitalgorithmen für SVP und CVP lösen das Suchproblem, während sich alle bisher bekannten Komplexitätsresultate auf das Optimierungsproblem oder das Entscheidungsproblem beziehen.

Für zweidimensionale Gitter kann SVP bezüglich der ℓ_2-Norm exakt gelöst werden. Der Algorithmus beruht auf einer Idee von Gauß aus dem Jahr 1801. Der schnellste zur Zeit bekannte Algorithmus zur Lösung von SVP für beliebige Gitter ist der Algorithmus von Ajtai, Kumar und Sivakumar aus dem Jahr 2001 [2]. Er löst SVP probabilistisch in der Zeit $2^{\mathcal{O}(n)}$. Auf einer Variante dieses Algorithmus basiert die in dieser Arbeit vorgestellte Samplemethode zur Lösung von SVP beziehungsweise zur Approximation von CVP. Der erste Algorithmus, der SVP in exponentieller Zeit exakt löste, war der Algorithmus von Kannan [22], der 1983 veröffentlicht wurde. Er hat eine Laufzeit von $2^{\mathcal{O}(n \log_2 n)}$. Helfrich konnte 1985 die Laufzeit im Exponenten um eine Konstante der Größenordnung $\frac{1}{2}$ verbessern [19]. Im Gegensatz zum Algorithmus von Ajtai, Kumar und Sivakumar ist dieser Algorithmus deterministisch. Ebenfalls deterministisch ist der schnellste zur Zeit bekannte Algorithmus zur Lösung von CVP. Er wurde von Blömer im Jahr 2000 entwickelt und löst das Problem des nächsten Gittervektors in $\mathcal{O}(n!)$ [7].

Van Emde Boas zeigte 1981, dass CVP für jede ℓ_p-Norm und SVP für die ℓ_∞-Norm NP-hart ist [15]. 1998 konnte Ajtai beweisen, dass SVP unter randomisierter Reduktion bezüglich der ℓ_2-Norm NP-hart ist [1]. Das Entscheidungsproblem von CVP ist NP-vollständig und damit kann es keinen deterministischen Algorithmus geben, der CVP in Polynomialzeit löst, es sei denn, es gilt P = NP [15].

Auf Grund der Schwierigkeit, das Problem des kürzesten Gittervektors und das Problem des nächsten Gittervektors exakt zu lösen, werden Approximationsvarianten dieser Probleme betrachtet.

Definition 2.5.3 Approximation des Problems des kürzesten Gittervektors mit dem Faktor c
Gegeben sei ein Gitter L. Gesucht ist ein Vektor $u \in L\backslash\{0\}$ mit

$$||u|| \leq c||v|| \text{ für alle } v \in L\backslash\{0\}.$$

Definition 2.5.4 Approximation des Problems des nächsten Gittervektors mit dem Faktor c
Gegeben sei ein Gitter L und ein Vektor $t \in \text{span}(L)$. Gesucht ist ein Vektor $z \in L$ mit

$$||z - t|| \leq c||v - t|| \text{ für alle } v \in L.$$

Der Approximationsfaktor c kann auch als Funktion in Bezug auf eine Invariante des Gitters aufgefasst werden. Üblicherweise verwendet man als Invariante den Rang n des Gitters. Die besten zur Zeit bekannten Polynomialzeitalgorithmen approximieren – teilweise probabilistisch – SVP und CVP im schlechtesten Fall mit einem Faktor $c(n)$, der einfach exponentiell in n ist. Der bekannteste Polynomialzeitalgorithmus zur Approximation von SVP ist der LLL-Basisreduktionsalgorithmus von Lenstra, Lenstra und Lovász [26] aus dem Jahr 1982. Er beruht auf dem Algorithmus von Gauß, der SVP für die Dimension 2 exakt löst und approximiert in einem Gitter der Dimension n einen kürzesten Gittervektor bezüglich der ℓ_2-Norm mit dem Faktor $2^{\frac{n-1}{2}}$. Schnorr verbesserte den Approximationsfaktor im Jahr 1987 auf $2^{\mathcal{O}(\frac{n(\log\log n)^2}{\log n})}$ [29]. Bisher ist noch nicht bekannt, ob man SVP oder CVP in polynomieller Zeit mit einem polynomiellen Faktor approximieren kann. Mit Hilfe des LLL-Algorithmus kann man auch das Problem des nächsten Gittervektors approximativ lösen. Dieser Algorithmus ist als „Nearest plane algorithm" bekannt und wurde 1998 von Babai entwickelt [5]. Durch aufeinander aufbauende Arbeiten [29], [21], [30], [2] konnten Schnorr, Kannan und Ajtai den Approximationsfaktor für CVP auf $2^{\mathcal{O}(\frac{n\ln\ln n}{\ln n})}$ reduzieren.

Auf Grundlage des Resultates von Ajtai, dass das Problem des kürzesten Gittervektors unter randomisierter Reduktion NP-hart ist, bewiesen Cai und Nerurkar 1999, dass die Approximation des Problems des kürzesten Gittervektors mit dem Faktor $(1 + \frac{1}{n^\epsilon})$ NP-hart ist [9]. Für $p > 1$ wurde von Khot unter der Annahme $NP \not\subseteq RP$ gezeigt, dass es keinen Algorithmus mit polynomieller Laufzeit geben kann, der SVP bezüglich ℓ_p-Norm mit einem konstanten Faktor approximiert [24]. Im Jahr 1997 fanden Arora, Babai, Stern und Sweedyk [4] heraus, dass das Problem, CVP mit dem Faktor $2^{\log(1-\epsilon)n}$ zu approximieren, NP-hart ist, es sei denn $NP \subseteq DTIME(2^{\text{poly}(\log n)})$. Der Faktor konnte im darauffolgendem Jahr von Dinur, Kindler und Safra [12] verbessert werden. Sie zeigten, dass das Problem, den nächsten Gittervektor mit dem Faktor $2^{\mathcal{O}(\frac{\log n}{\log\log n})}$ zu approximieren, NP-hart ist. Im Jahr 1999 bewiesen Goldreich, Micciancio, Safra und Seifert durch eine Turingreduktion von CVP auf SVP, dass jede Schwierigkeit bezüglich einer Approximation von SVP die gleiche Schwierigkeit bezüglich der Approximation von CVP impliziert [18].

3. Samplemethode zur Berechnung eines Gittervektors konstanter Größe

In diesem Kapitel soll eine Methode vorgestellt werden, wie man einen Gittervektor mit einer Länge kleiner als eine Konstante berechnen kann. Sie ist eine Verallgemeinerung der von Regev in [23] vorgeschlagenen Samplemethode, die auf einem Vorschlag von Madhu Sudan in [2] beruht. Wichtig an dieser Samplemethode ist in erster Linie nicht ihr Resultat, das heißt, dass sie einen Gittervektor aus einer Kugel mit konstantem Radius berechnet, sondern ihre Funktionsweise und die Beobachtung, dass man auf Grund der Randomisierung und mit Hilfe einer Modifikation zumindest gewisse Aussagen über die Verteilung der Ausgabevektoren machen kann. Die allgemeinen Aussagen, die in diesem Kapitel bewiesen werden, kann man in den Kapiteln 4 und 5 dazu verwenden, um zu zeigen, dass Varianten der Samplemethode zur Lösung des Problems des kürzesten Gittervektors sowie zur Approximation des nächsten Gittervektors verwendet werden können.

Im Folgenden betrachtet man volldimensionale Gitter vom Rang n.

3.1. Siebprozedur

Wesentlicher Bestandteil der im folgenden Abschnitt vorgestellten Samplemethode ist eine Siebprozedur, die in einer Menge $\{x_1, \ldots, x_N\}$ von Punkten aus einer Kugel vom Radius R eine Teilmenge J mit höchstens $(2a+1)^n$ sogenannten Repräsentanten findet, so dass der Abstand von jedem Punkt der Menge zu seinem Repräsentanten höchstens $\frac{R}{a}$ ist. Dabei ist $a \geq 2$ eine beliebige natürliche Zahl. Die Zuordnung der Punkte $x_1, \ldots, x_N$ zu ihren Repräsentanten erfolgt durch eine Abbildung

$$\eta : \{1, \ldots, N\} \longrightarrow J,$$

das heißt, es gilt:

$$||x_i - x_{\eta(i)}||_p \leq \frac{R}{a} \text{ für alle } i \in \{1, \ldots, N\}.$$

Algorithmus 3.1.1 Siebprozedur: `Eingabe:` $x_1, \ldots, x_N \in B(0, R)$

`Setze` $J = \emptyset$
`Für` $j = 1, 2, \ldots, N$

`Falls ein` $i \in J$ `existiert mit` $||x_i - x_j||_p \leq \frac{R}{a}$`, definiere` $\eta(i) = j$.
`Sonst` $J = J \cup \{i\}$ `und definiere` $\eta(i) = i$.

Satz 3.1.2 *Sei $R \in \mathbb{R}$, $R > 0$, $a \in \mathbb{N}$ mit $a \geq 2$.*
Zu einer beliebigen Punktemenge $x_1, \ldots, x_N \in B(0, R)$ berechnet die Siebprozedur eine Teilmenge $J \subseteq \{1, 2 \ldots, N\}$ mit $|J| \leq (2a+1)^n$ und eine Abbildung $\eta : \{1, 2, \ldots, N\} \to J$, so dass gilt:

$$||x_i - x_{\eta(i)}||_p \leq \frac{R}{a} \text{ für alle } i \in \{1, \ldots, N\}$$

Die Siebprozedur hat eine Laufzeit von $\mathcal{O}(N^2 \cdot \text{poly}(m))$, wenn die Punkte $x_1, \ldots, x_N$ rationale Zahlen sind und eine Darstellung der Länge höchstens $\mathcal{O}(m)$ haben.

Beweis: Nach Definition der Prozedur ist offensichtlich, dass für alle $i \in \{1, \ldots, N\}$ gilt:

$$||x_i - x_{\eta(i)}||_p \leq \frac{R}{a}.$$

Es ist also noch zu zeigen: $|J| \leq (2a+1)^n$.

Falls $i, j \in J$ existieren mit $||x_i - x_j||_p \leq \frac{R}{a}$, so gilt einerseits nach Definition $\eta(i) = i$, da $i \in J$. Andererseits existiert $j \in J$ mit $||x_i - x_j||_p \leq \frac{R}{a}$. Dies ist gleichbedeutend mit $\eta(i) = j$ und stellt somit einen Widerspruch dar. Also gilt:

$$||x_i - x_j||_p > \frac{R}{a} \text{ für alle } i, j \in J.$$

Wenn man also für jedes $i \in J$ eine offene Kugel um den Punkt x_i mit dem Radius $\frac{R}{2a}$ betrachtet, so sind diese Kugeln paarweise disjunkt:

$$B(x_i, \frac{R}{2a}) \cap B(x_j, \frac{R}{2a}) = \emptyset \text{ für alle } i, j \in J, i \neq j.$$

Da $x_i \in B(0, R)$ für alle $i \in \{1, \ldots, N\}$, liegt die Vereinigung aller dieser Kugeln in der offenen Kugel $B(0, R + \frac{1}{2a}R) = B(0, (1 + \frac{1}{2a})R)$.
Damit ist die Ordnung von J beschränkt durch die Anzahl disjunkter Kugeln $B(0, \frac{1}{2a}R)$, die maximal in der Kugel $B(0, (1 + \frac{1}{2a})R)$ enthalten sein können:

$$\frac{\text{vol}\, B\left(0, (1 + \frac{1}{2a})R\right)}{\text{vol}\, B\left(0, \frac{1}{2a}R\right)} = \frac{\left(\frac{2a+1}{2a}\right)^n}{\left(\frac{1}{2a}\right)^n} = (2a+1)^n.$$

Die Anzahl der Schleifendurchläufe der Siebprozedur und damit die Anzahl arithmetischer Operationen beträgt:

$$\sum_{i=1}^{N}(N - i) = \sum_{i=0}^{N-1} i = \mathcal{O}(N^2).$$

Ohne Einschränkung kann man davon ausgehen, dass die Eingabe $x_1, \ldots, x_N$ rationale Zahlen sind. Da $x_i \in B(0, R)$ für alle $i \in \{1, \ldots, N\}$, ist die Länge von x_i beschränkt. Die Laufzeit der Siebprozedur hängt nun davon ab, wodurch die Genauigkeit, das heißt die Größe der Nenner, beschränkt ist. Unter der Voraussetzung, dass man mit einer Genauigkeit von m Bits ($m \geq \log_2 R$) rechnet, erhält man eine Laufzeit von

$$\mathcal{O}(N^2 \cdot \text{poly}(m)).$$

□

3.2. Samplemethode

Mit Hilfe der Siebprozedur 3.1.1 kann man in einem Gitter $L = \mathcal{L}(b_1, \ldots, b_n)$ Gitterpunkte berechnen, die eine bestimmte maximale Länge haben. Der Algorithmus wählt N Punkte zufällig, unabhängig und gleichverteilt aus einer Kugel $B(0, r)$ vom Radius r aus und betrachtet für jeden dieser Punkte x_i mit $i \in \{1, \ldots, N\}$ den Punkt y_i aus dem Fundamentalbereich des Gitters, so dass $y_i - x_i$ ein Gitterpunkt ist. Für $x_i = \sum_{j=1}^{n} \alpha_j b_j$ mit $\alpha_j \in \mathbb{R}$ ist $y_j = \sum_{j=1}^{n} (\alpha_j - \lfloor \alpha_j \rfloor) b_j$.

Man wendet dann die Siebprozedur iterativ auf die Vektoren y_i an. Mit Hilfe der Abbildung $\eta : \{1, \ldots, N\} \longrightarrow J$ erhält man für jeden Vektor einen Repräsentanten $y_{\eta(i)}$, so dass der Abstand zwischen y_i und seinem Repräsentanten höchstens $\frac{R}{a}$ ist. Damit ist die Länge des Gittervektors $(y_i - x_i) - (y_{\eta(i)} - x_{\eta(i)})$ kleiner als eine Konstante und man ersetzt y_i durch $y_i - (y_{\eta(i)} - x_{\eta(i)})$. Dieses Verfahren wird solange fortgesetzt, bis der Abstand zwischen einem Vektor und dem von der Siebprozedur berechneten Repräsentanten kleiner als eine Konstante ist.

Der Algorithmus verwendet die Parameter $a \in \mathbb{N}$ mit $a \geq 2$, $r > 0$ und θ. Sie sind frei wählbar, wobei $\theta > \frac{a}{a-1} \cdot r$ gelten muss. Die Samplemethode berechnet dann eine Menge von Gittervektoren der Länge kleiner als $\theta + r$.

Algorithmus 3.2.1 Samplemethode
`Eingabe: Eine Gitterbasis` $B = \{b_1, \ldots, b_n\}$

1. $R_0 \leftarrow n \cdot \max_i ||b_i||_p$
   `Wähle` $N = 2^{c \cdot n} \log_2 R_0$ `Punkte` $x_1, \ldots, x_N$ `zufällig, unabhängig, gleichverteilt in` $B(0, r)$`, wobei` $c \in \mathbb{N}$.
   `Berechne` $y_i \equiv x_i \mod \mathcal{L}(B)$ `für` $i = 1, \ldots, N$.
   `Setze` $\mathcal{Z} = \{(x_1, y_1), \ldots, (x_N, y_N)\}$.
   $R \leftarrow R_0$
2. `Solange` $R > \theta$
   a) `Anwendung der Siebprozedur auf` $\{y_i | (x_i, y_i) \in \mathcal{Z}\}$ `mit den Parametern` a `und` R.
      `Man erhält eine Menge` J `und eine Abbildung` η.
   b) `Entferne aus der Menge` $\mathcal{Z}$ `alle Paare` (x_i, y_i) `mit` $i \in J$.
   c) `Ersetze jedes verbleibende Paar` $(x_i, y_i) \in \mathcal{Z}$ `durch` $(x_i, y_i - (y_{\eta(i)} - x_{\eta(i)}))$.
   d) $R \leftarrow \frac{R}{a} + r$
3. `Ausgabe ist die Menge` $\{y_i - x_i | (x_i, y_i) \in \mathcal{Z}\}$.

Wenn man mit einer Bitgenauigkeit von $n^7 \cdot \log_2 R_0$ rechnet, so ist diese Genauigkeit für die Anwendungen der Samplemethode zur Lösung des Problems des kürzesten Gittervektors und der Approximation des Problems des nächsten Gittervektors ausreichend. Die Gründe, warum die Bitgenauigkeit nicht beliebig gewählt werden kann, werden in Abschnitt 3.4 beschrieben.

Für ein Paar $(x_i, y_i) \in \mathcal{Z}$ mit $i \in J$, ist $\eta(i) = i$ und damit $y_i - (y_{\eta(i)} - x_{\eta(i)}) - x_i = 0$. Man erhält also als Gitterpunkt den Nullvektor. Indem man aus der Menge $\mathcal{Z}$ alle Paare (x_i, y_i) mit

$i \in J$ entfernt, erreicht man, dass in der Menge $\mathcal{Z}$ keine offensichtlich redundanten Elemente enthalten sind.

Im nächsten Satz wird gezeigt, dass die Samplemethode auf Grund der Eigenschaften der Siebprozedur Gittervektoren berechnet, die höchstens die Länge $\theta+r$ haben. Da θ und r frei wählbare Konstanten sind, kann man also mit Hilfe der Samplemethode Gittervektoren berechnen, die höchstens eine gegebene konstante Länge haben.

Satz 3.2.2 *Die Samplemethode berechnet bei Eingabe einer Gitterbasis B eine Menge von Vektoren aus $\mathcal{L}(B) \cap B(0, \theta + r)$.*

Beweis: Der Algorithmus wählt N Punkte $x_1, \ldots, x_N$ aus $B(0, r)$ und definiert für alle $i \in \{1, \ldots, N\}$ den Vektor y_i durch $y_i \equiv x_i \mod \mathcal{L}(B)$, das heißt $y_i - x_i \in \mathcal{L}(B)$. Im Verlauf der Iteration werden von y_i nur Vektoren der Form $y_j - x_j$ subtrahiert und da $\mathcal{L}(B)$ bezüglich der Addition eine abelsche Gruppe ist, gilt:

$$(y_i - (y_j - x_j)) - x_i = \underbrace{y_i - x_i}_{\in \mathcal{L}(B)} - \underbrace{(y_j - x_j)}_{\in \mathcal{L}(B)} \in \mathcal{L}(B).$$

Damit sind alle ausgegebenen Vektoren Gittervektoren.

Auf Grund der Definition des Vektors y_i durch $y_i \equiv x_i \mod \mathcal{L}(B)$ gilt vor Beginn des zweiten Schrittes $y_i \in \mathcal{P}(B) = \{\sum_{i=1}^{n} \alpha_i b_i | 0 \leq \alpha_i < 1, i = 1, \ldots, N\}$. Damit ist die Länge von y_i für alle $i \in \{1, \ldots, N\}$ beschränkt durch:

$$\begin{aligned} ||y_i||_p &= ||\sum_{i=1}^{n} \underbrace{\alpha_i}_{<1} b_i||_p \\ &\leq \sum_{i=1}^{n} ||b_i||_p \\ &\leq n \cdot \max_i ||b_i||_p \\ &= R_0 = R \end{aligned}$$

Die Abbildung η ist so definiert, dass $||y_i - y_{\eta(i)}||_p \leq \frac{R}{a}$ für alle y_i mit $(x_i, y_i) \in \mathcal{Z}$. Damit bleibt die Eigenschaft, dass die Länge des Vektors y_i durch den Parameter R beschränkt ist, auch während der Iteration erhalten:

$$\begin{aligned} ||y_i - (y_{\eta(i)} - x_{\eta(i)})||_p &\leq ||y_i - y_{\eta(i)}||_p + ||x_{\eta(i)}||_p \\ &\leq \frac{R}{a} + ||x_{\eta(i)}||_p \qquad (3.1.2) \\ &< \frac{R}{a} + r, \text{ da } x_{\eta(i)} \in B(0, r) \\ &\leq R \end{aligned}$$

Die letzte Ungleichung folgt aus der Tatsache, dass nach jeder Iteration R durch $\frac{R}{a} + r$ ersetzt wird.

Die Iteration bricht ab, falls $R \leq \theta$. Damit gilt für die in der Menge $\mathcal{Z}$ verbliebenen Paare (x_i, y_i):

$$||y_i - x_i||_p \leq ||y_i||_p + ||x_i||_p \leq \theta + r$$

und alle ausgegebenen Vektoren haben eine Länge kleiner als $\theta + r$.

□

Für die Laufzeit der Samplemethode ist die Anzahl der Iterationen in Schritt 2 von wesentlicher Bedeutung. Da die Parameter a, θ und r konstant gewählt werden, ist die Anzahl der Iterationen nach oben beschränkt.

Lemma 3.2.3 *Die Samplemethode durchläuft bei fest gewählten Parametern a, θ und r mit $\theta > \frac{a}{a-1} \cdot r$ im zweiten Schritt höchstens*

$$2 \log_2 a \cdot \log_2 R_0$$

Iterationen.

Beweis: Die Anzahl der Iterationen ist abhängig von den Parametern a, θ und r, die konstant gewählt werden. Nach i Schritten hat der Laufparameter R die Größe:

$$\frac{R_0}{a^i} + r \sum_{j=0}^{i-1} a^{-j}$$

Die Schleife im zweiten Schritt der Samplemethode bricht ab, falls der Laufparameter R einen Wert kleiner gleich der Konstanten θ hat. Verwendet man zur Abschätzung von R die geometrische Reihe

$$\frac{R_0}{a^i} + r \sum_{j=0}^{i-1} a^{-j} \leq \frac{R_0}{a^i} + r \frac{a}{a-1},$$

so bricht die Schleife spätestens ab, wenn gilt:

$$\begin{array}{rrcl} & \frac{R_0}{a^i} + r\frac{a}{a-1} & \leq & \theta \\ \iff & \frac{R_0}{a^i} & \leq & \theta - r\frac{a}{a-1} = \frac{\theta(a-1) - ra}{a-1} \\ \iff & a^i & \geq & \frac{R_0(a-1)}{\theta(a-1) - ra} \\ \iff & i & > & \log_2 a \cdot (\log_2 R_0 + \log_2(a-1) - \log_2(\theta(a-1) - ra)) \end{array}$$

Da a, θ und r konstant gewählt werden, durchläuft der Algorithmus in Schritt 2 damit höchstens

$$\begin{array}{rl} & \log_2 a \cdot (\log_2 R_0 + \log_2(a-1) - \log_2(\theta(a-1) - ra)) \\ \leq & \log_2 a \cdot (\log_2 R_0 + \log_2 a) \\ \leq & 2 \log_2 a \cdot \log_2 R_0 \end{array}$$

Iterationen.

□

Mit Hilfe dieser Abschätzung kann man nun die Laufzeit der Samplemethode berechnen.

Satz 3.2.4 *Die Samplemethode hat bei fest gewählten Parametern a, θ und r mit $\theta > \frac{a}{a-1} \cdot r$ eine Laufzeit von*

$$2^{\mathcal{O}(n)} \operatorname{poly}(\log_2 R_0).$$

Beweis: Wesentlich für die Laufzeit des Algorithmus ist die Anzahl Iterationen in Schritt 2. Bei konstanter Wahl der Parameter a, θ und r, sowie $\theta > \frac{a}{a-1} \cdot r$ durchläuft der Algorithmus nach Lemma 3.2.3 höchstens

$$2 \log_2 a \cdot \log_2 R_0 = \mathcal{O}(\log_2 R_0)$$

Iterationen. In jedem Iterationsschritt wird die Siebprozedur einmal aufgerufen, die bei Rechnung mit einer Bitgenauigkeit von $n^7 \log_2 R_0$ eine Laufzeit von

$$\mathcal{O}(|\mathcal{Z}|^2 \operatorname{poly}(n^7 \log_2 R_0)) = \mathcal{O}(N^2 \operatorname{poly}(n^7 \log_2 R_0))$$

hat. Damit hat der Algorithmus eine Laufzeit von

$$\mathcal{O}(\log_2 R_0) \cdot \mathcal{O}(N^2 \operatorname{poly}(n^7 \log_2 R_0)) = \mathcal{O}((\log_2 R_0)^k) 2^{\mathcal{O}(n)},$$

für ein $k \in \mathbb{N}$. Mit einer Eingabelänge von höchstens $\log_2 R_0$ erhält man eine Gesamtlaufzeit von

$$2^{\mathcal{O}(n)} \mathcal{O}(\log_2 R_0)^k.$$

□

In jedem Schritt werden aus der Menge $\mathcal{Z}$ alle Paare (x_i, y_i) mit $i \in J$ entfernt. Die Anzahl der zu Beginn der Samplemethode gewählten Punkte muss also so gewählt werden, dass in der Ausgabemenge noch entsprechend viele Vektoren enthalten sind. Der folgende Satz zeigt, dass nach der Schleife in der Menge $\mathcal{Z}$ noch mindestens $2^{(c-1)n}$ Paare enthalten sind, wenn zu Beginn der Samplemethode $N = 2^{cn} \log_2 R_0$ Paare gewählt wurden. Dabei ist die Konstante c abhängig von dem Parameter a.

Satz 3.2.5 *Sei $N = 2^{cn} \log_2 R_0$ mit $c \in \mathbb{N}$ genügend groß in Bezug auf die Konstante a. Dann enthält die Menge $\mathcal{Z}$ in Schritt 4 noch mindestens $2^{(c-1)n}$ Paare.*

Beweis: Die Siebprozedur wird nach Lemma 3.2.3 maximal $2 \log_2 a \log_2 R_0$-mal wiederholt. Als Ausgabe erhält man bei jedem Aufruf eine Menge J der Kardinalität höchstens $(2a+1)^n$. Damit werden pro Iteration maximal $(2a+1)^n$ Paare aus $\mathcal{Z}$ entfernt. Insgesamt werden also höchstens $2 \log_2 a \log_2 R_0 \cdot (2a+1)^n$ Paare im Schritt 2 aus $\mathcal{Z}$ entfernt und die Menge $\mathcal{Z}$ enthält nach der Iteration noch mindestens

$$\begin{aligned}
N - 2 \log_2 a \log_2 R_0 (2a+1)^n &= (2^{cn} - 2 \log_2 a (2a+1)^n) \log_2 R_0 \\
&> (2^{cn} - 2 \log_2 a (2(a+1))^n) \log_2 R_0 \\
&= \left(2^{cn} - 2^{(\log_2(a+1)+1)n+1+\log_2 \log_2 a}\right) \log_2 R_0 \\
&= 2^{(c-1)n} \left(2^n - 2^{(\log_2(a+1)+2-c)n+1+\log_2 \log_2 a}\right) \log_2 R_0 \\
&\geq 2^{(c-1)n}
\end{aligned}$$

Paare (x_i, y_i) für $c > \log_2(a+1) + 2$ genügend groß.

□

Auch wenn die Menge $\mathcal{Z}$ nach der Schleife noch $2^{\mathcal{O}(n)}$ Paare enthält, so bedeutet dies nicht, dass die Samplemethode $2^{\mathcal{O}(n)}$ verschiedene Gittervektoren ausgibt, denn ein Gittervektor kann durch zwei verschiedene Paare $(x_i, y_i), (x_j, y_j) \in \mathcal{Z}$ repräsentiert werden.

3.3. Modifikation der Samplemethode

Mit dieser allgemeinen Analyse der Samplemethode 3.2.1 kann man allerdings nichts über die Verteilung der Gittervektoren aussagen, die von der Samplemethode berechnet werden. Deswegen betrachtet man zur weiteren Analyse nicht die Samplemethode, sondern eine modifizierte Samplemethode, für die man im Einzelfall eine Aussage über die Verteilung der Ausgabevektoren machen kann. Die Samplemethode wird allerdings nur so modifiziert, dass sich die modifizierte Samplemethode und die ursprüngliche Samplemethode noch exakt gleich verhalten. Aus diesem Grund kann man dann auch eine Aussage über die Verteilung der Ausgabevektoren für die ursprüngliche Samplemethode machen und zeigen, dass bei entsprechender Betrachtung der Menge $\mathcal{Z}$ die Samplemethode dazu verwendet werden kann, sowohl das Problem des kürzesten Gittervektors zu lösen, als auch eine $c(1+\epsilon)^2$-Approximation des nächsten Gittervektors zu finden.

Für die Modifikation betrachtet man einen beliebigen, aber festen Gittervektor $u \in \mathcal{L}(B)$. Indem man diesen Vektor entsprechend wählt, kann man in den Kapiteln 4 und 5 zeigen, dass man mit Hilfe der Samplemethode das Problem des kürzesten Gittervektors lösen sowie eine Approximation des nächsten Gittervektors finden kann.

Im Folgenden sei $u \in \mathcal{L}(B)$ ein beliebiger, aber fester Gittervektor mit $||u||_p \in [r, 2r)$. Man definiert dann folgende Mengen:

$$C_1 := B(0, r) \cap B(u, r) \text{ und}$$

$$C_2 := B(0, r) \cap B(-u, r).$$

Auf Grund der Länge von u schneiden sich die Kugeln $B(u, r)$ und $B(-u, r)$ nicht. Damit schneiden sich auch die Mengen C_1 und C_2 nicht. Die Lage von C_1 und C_2 wird in Abbildung 3.1 veranschaulicht.

Mit Hilfe der Mengen C_1 und C_2 kann man eine schwache Uniformitätsbedingung für die ausgegebenen Gittervektoren zeigen. Es existiert eine bijektive Abbildung $B(0, r)$ auf sich selbst, die C_1 auf C_2 abbildet und umgekehrt. Damit existiert zu jedem Punkt aus C_1 ein Punkt aus C_2, der von der Samplemethode mit der gleichen Wahrscheinlichkeit ausgegeben wird.

Man definiere eine Abbildung $\tau_u : B(0, r) \to B(0, r)$:

$$\tau_u(x) = \begin{cases} x + u & , \ x \in C_2 \\ x - u & , \ x \in C_1 \\ x & , \ \text{sonst} \end{cases}$$

Sei $x \in C_1$. Dann ist $||x||_p < r$ und $||x - u||_p < r$. Damit gilt:

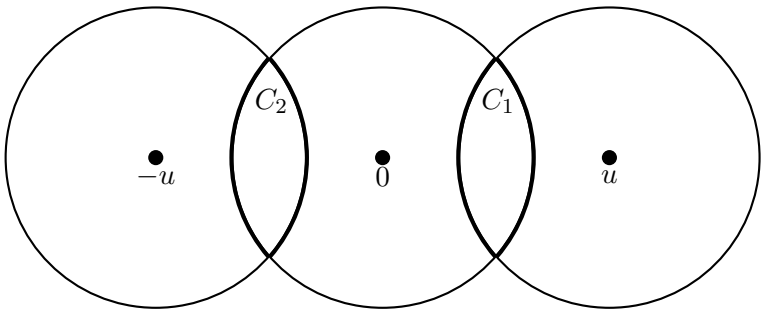

Abbildung 3.1.: Die Mengen C_1 und C_2

- $||\tau_u(x)||_p = ||x - u||_p < r$,
- $||\tau(x) - (-u)||_p = ||x - u + u||_p = ||x||_p < r$.

Also ist $\tau_u(x) \in C_2$. Analog sieht man, dass $\tau_u(x) \in C_1$, falls $x \in C_2$. Damit ist τ_u bijektiv und bildet C_1 auf C_2, C_2 auf C_1 und $B(0,r)\backslash(C_1 \cup C_2)$ auf sich selbst ab. Falls $x \in B(0,r)$ zufällig, unabhängig und gleichverteilt gewählt wird, ist deswegen auch $\tau_u(x)$ zufällig, unabhängig und gleichverteilt gewählt.

Die Abbildung τ_u ist für jeden Vektor $u \in L$ mit der Eigenschaft $r \leq ||u||_p < 2r$ bei entsprechender Definition der Mengen C_1 und C_2 wohldefiniert. Unter Verwendung dieser Abbildung τ wird folgende modifizierte Samplemethode betrachtet, die in den folgenden Kapiteln benötigt wird, um zu zeigen, dass man mit Hilfe der Samplemethode SVP lösen und CVP approximieren kann.

Algorithmus 3.3.1 Modifizierte Samplemethode
Eingabe: Eine Gitterbasis $B = \{b_1, \ldots, b_n\}$
Sei $u \in \mathcal{L}(B)$ mit $r \leq ||u||_p < 2r$.

1. $R_0 \leftarrow n \cdot \max_i ||b_i||_p$.
   Wähle $N = 2^{cn} \log_2 R_0$ Punkte $x_1, \ldots, x_N$ zufällig, unabhängig, gleichverteilt in $B(0,r)$, wobei $c \in \mathbb{N}$.
   Berechne $y_i \equiv x_i \mod \mathcal{L}(B)$ für $i = 1, \ldots, N$.
   Setze $\mathcal{Z} = \{(x_1, y_1), \ldots, (x_N, y_N)\}$.
   $R \leftarrow R_0$
2. Solange $R > \theta$
   a) Anwendung der Siebprozedur auf $\{y_i | (x_i, y_i) \in \mathcal{Z}\}$ mit den Parametern a und R.
   Man erhält eine Menge J und eine Abbildung η.
   Entferne aus der Menge $\mathcal{Z}$ alle Paare (x_i, y_i) mit $i \in J$.
   b) Entscheide für jedes Paar (x_i, y_i) mit $i \in J$ zufällig, unabhängig, gleichverteilt, ob x_i durch $\tau_u(x_i)$ ersetzt wird.
   c) Ersetze jedes verbleibende Paar $(x_i, y_i) \in \mathcal{Z}$ durch $(x_i, y_i - (y_{\eta(i)} - x_{\eta(i)}))$.

d) $R \leftarrow \frac{R}{a} + r$

3. Entscheide für alle Paare $(x_i, y_i) \in \mathcal{Z}$ zufällig, unabhängig, gleichverteilt, ob x_i durch $\tau_u(x_i)$ ersetzt wird.

4. Ausgabe ist die Menge $\{y_i - x_i | (x_i, y_i) \in \mathcal{Z}\}$.

Die modifizierte Samplemethode wird nur zur Analyse benötigt. Damit ist die Laufzeit unerheblich, ebenso wie die Tatsache, dass man zur Berechnung der Abbildung τ_u den Gittervektor u kennen muss. Diese zweite Eigenschaft ist für die Verwendung der Samplemethode zur Lösung des kürzesten Gittervektors sowie zur Approximation des nächsten Gittervektors sehr wichtig, da man hier für den Gittervektor u einen kürzesten von 0 verschiedenen Gittervektor beziehungsweise den nächsten Gittervektor verwendet.

Satz 3.3.2 *Die Samplemethode und die modifizierte Samplemethode verhalten sich exakt gleich.*

Beweis: Die Samplemethode wählt für jedes $i \in \{1, \ldots, N\}$ einen Punkt $x_i \in B(0, r)$ zufällig, unabhängig und gleichverteilt. Die Abbildung $\tau_u : B(0, r) \longrightarrow B(0, r)$ ist bijektiv. Wenn man also $x_i \in B(0, r)$ zufällig, unabhängig und gleichverteilt wählt, so ist auch $\tau_u(x_i)$ zufällig, unabhängig und gleichverteilt. Dies ist auch dann noch der Fall, wenn man zufällig, unabhängig und gleichverteilt entscheidet, ob x_i unverändert bleibt, oder ob man τ_u auf x_i anwendet.

Da $u \in \mathcal{L}(B)$, hat die Entscheidung, ob man x_i oder $\tau_u(x_i)$ verwendet, keinen Einfluß auf die Arbeitsweise des Algorithmus. Der Vektor y_i wird definiert durch

$$y_i \equiv x_i \mod \mathcal{L}(B),$$

das heißt man erhält denselben Vektor $y_i \in \mathcal{P}(B)$, egal ob x_i oder $\tau_u(x_i)$ verwendet wird. Deswegen ist es unerheblich, in welchem Schritt des Algorithmus man die zufällige Wahl trifft, ob die Samplemethode x_i oder $\tau_u(x_i)$ verwendet.

Die Entscheidung, ob man im weiteren Verlauf des Algorithmus x_i oder $\tau_u(x_i)$ verwendet, kann man also auch erst dann treffen, wenn sie wirklich Auswirkungen macht. Während der Iteration wird jedes Paar (x_i, y_i) mit $i \notin J$ durch $(x_i, y_i - (y_{\eta(i)} - x_{\eta(i)}))$ ersetzt, wobei $\eta(i) \in J$. An dieser Stelle macht es einen Unterschied, ob $x_{\eta(i)}$ oder $\tau_u(x_{\eta(i)})$ benutzt wird. Deswegen wird nach Anwendung der Siebprozedur in Schritt 2b für jedes Paar (x_i, y_i) mit $i \in J$ entschieden, ob x_i oder $\tau_u(x_i)$ verwendet wird. Alle Paare (x_i, y_i) mit $i \in J$ werden aus der Menge $\mathcal{Z}$ entfernt, so dass nach der Schleife nur noch Paare in der Menge $\mathcal{Z}$ enthalten sind, für die noch nicht entschieden wurde, ob man x_i durch $\tau_u(x_i)$ ersetzt. Für diese Paare trifft man die Entscheidung im modifizierten Algorithmus im Anschluß an die Schleife.

Damit arbeitet die modifizierte Samplemethode genauso wie die ursprüngliche Samplemethode und beide Methoden haben die gleiche Wahrscheinlichkeitsverteilung auf den Ausgabevektoren. □

Auf Grund dieses Resultates genügt es, bei Anwendung der Samplemethode zur Lösung des Problems des kürzesten Gittervektors beziehungsweise zur Approximation des nächsten Gittervektors die modifizierte Samplemethode zu analysieren. Wenn man für die modifizierte Samplemethode zeigen kann, dass mit hoher Wahrscheinlichkeit ein gewünschter Vektor ausgegeben wird, so gilt dies auch für die ursprüngliche Samplemethode.

Für die Analyse der Modifikation wird die Wahrscheinlichkeit benötigt, mit der ein Punkt x, der zufällig, unabhängig und gleichverteilt aus $B(0,r)$ gewählt wird, in der Menge $C_1 \cup C_2$ enthalten ist. Um aber eine Aussage über die Verteilung der Ausgabevektoren der modifizierten Samplemethode machen zu können, muss man die Länge des Vektors u abschätzen können:

$$||u||_p \leq l \cdot r \text{ für ein } 1 \leq l < 2$$

Dies ist eine zusätzliche Einschränkung zu der auf Seite 19 geforderten Bedingung: $r \leq ||u||_p < 2r$.

Sei $1 \leq l < 2$ mit $||u||_p \leq l \cdot r$.

Lemma 3.3.3 *Sei* $k := 2^{\lfloor \log_2 \frac{2-l}{l} \rfloor} < \frac{2-l}{l}$. *Dann gilt:*

$$\frac{\text{vol}(C_1)}{\text{vol}(B_n(0,r))} = \frac{\text{vol}(C_2)}{\text{vol}(B_n(0,r))} \geq k(2-k-l)^{n-1}2^{-n}$$

Beweis: Es ist offensichtlich, dass $\text{vol}(C_1) = \text{vol}(C_2)$.
Damit ist nur noch zu zeigen: $\frac{\text{vol}(C_1)}{\text{vol}(B(0,r))} \geq k \cdot (2-k-l)^{n-1}2^{-n}$, wobei $k = 2^{\lfloor \log_2 \frac{2-l}{l} \rfloor}$. Dazu überlegt man sich zunächst, dass C_1 einen Zylinder der Höhe $k \cdot r$ mit dem Radius $\frac{1}{2}(2-k-l)r$ um den Punkt $\frac{u}{2}$ enthält.

Da $k = 2^{\lfloor \log_2 \frac{2-l}{l} \rfloor} < \frac{2-l}{l}$ und $l \geq 1$, ist $0 < k < 1$. Daraus folgt:

$$\frac{1}{2}(1-k)||u||_p \leq \frac{1}{2}(1+k)||u||_p < \frac{1}{2}(1+\frac{2-l}{l})l \cdot r = r.$$

Damit gilt für die Punkte $\frac{u}{2} + k \cdot \frac{u}{2}$ und $\frac{u}{2} - k \cdot \frac{u}{2}$:

$$\begin{aligned} ||\frac{u}{2} + k \cdot \frac{u}{2}||_p &= \frac{1}{2}(1+k)\,||u||_p < r \\ ||\frac{u}{2} + k \cdot \frac{u}{2} - u||_p &= \frac{1}{2}\,|-1+k|\,||u||_p \leq \frac{1}{2}(1-k)||u||_p < r \end{aligned}$$

Damit gilt $\frac{u}{2} + k \cdot \frac{u}{2} \in C_1$ und es ist $\frac{u}{2} - k \cdot \frac{u}{2} \in C_1$, da

$$\begin{aligned} ||\frac{u}{2} - k \cdot \frac{u}{2}||_p &= \left(\frac{1}{2} - \frac{1}{2}k\right)||u||_p < \frac{1}{2}(1-k)||u||_p < r \\ ||\frac{u}{2} - k \cdot \frac{u}{2} - u||_p &= \left|\frac{1}{2}(-1-k)\right|||u||_p < \frac{1}{2}(1+k)||u||_p < r \end{aligned}$$

Die beiden Punkte haben von $\frac{u}{2}$ mindestens den Abstand

$$\begin{aligned} ||\frac{u}{2} + k \cdot \frac{u}{2} - \frac{u}{2}||_p &= ||k \cdot \frac{u}{2}||_p = \frac{k}{2}||u||_p \geq \frac{1}{2}k \cdot r \\ ||\frac{u}{2} - k \cdot \frac{u}{2} - \frac{u}{2}||_p &\geq \frac{1}{2}k \cdot r \end{aligned}$$

und somit ist es möglich, in C_1 einen Zylinder der Höhe $\frac{1}{2}k \cdot r + \frac{1}{2}k \cdot r = k \cdot r$ um den Punkt $\frac{u}{2}$ zu legen.

Um zu zeigen, dass dieser Zylinder den Radius $\frac{1}{2}(2-k-l)r$ haben kann, betrachtet man den Unterraum $U \subseteq \mathbb{R}^n$ orthogonal zur Achse $k \cdot u$, $k \in \mathbb{Z}$.
Sei $s \in \mathbb{R}^n$ mit $||s - \frac{u}{2}||_p \leq \frac{1}{2}k \cdot r$. Dann hat s die maximale Länge

$$||s||_p \leq ||s - \frac{u}{2}||_p + ||\frac{u}{2}||_p < \frac{1}{2}k \cdot r + \frac{1}{2}l \cdot r = \frac{1}{2}(k+l)r$$

und von u höchstens den Abstand

$$||s - u||_p \leq ||s - \frac{u}{2}||_p + ||\frac{u}{2}||_p < \frac{1}{2}(k+l)r.$$

Sei $x \in U$ mit $||x - s||_p < \frac{1}{2}(2-k-l)r$. Da nach Definition gilt $k < \frac{2-l}{l}$, ist $k + l < 2$. Es gilt:

$$||x||_p \leq ||x - s||_p + ||s||_p < \frac{1}{2}(2-k-l)r + \frac{1}{2}(k+l)r = r$$

und

$$||x - u||_p \leq ||x - s||_p + ||s - u||_p < \frac{1}{2}(2-k-l)r + \frac{1}{2}(k+l)r = r.$$

Damit ist $||x||_p < r$ und $||x - u||_p < r$, das heißt $x \in C_1$ und C_1 enthält einen Zylinder der Höhe $k \cdot r$ mit dem Radius $\frac{1}{2}(2-k-l)r$. Man erhält als Abschätzung für das Volumen von C_1:

$$\operatorname{vol} C_1 \geq \operatorname{vol}(\underbrace{B_{n-1}(0, \frac{1}{2}(2-k-l)r)}_{B_{n-1}(\frac{u}{2}, \frac{1}{2}(2-k-l)r)}) \cdot k \cdot r$$

Eine Abschätzung für das Volumen von $B_n(0,r)$ erhält man, indem man sich überlegt, dass die Kugel $B_n(0,r) = (\frac{r}{2})^n B_n(0,2)$ und $B_n(0,2)$ in einem Zylinder vom Radius 2 mit Höhe 4 enthalten ist:

$$\operatorname{vol}(B_n(0,r)) \leq (\frac{r}{2})^n 4 \cdot B_{n-1}(0,2)$$

Man erhält also insgesamt die Abschätzung:

$$\begin{aligned}
\frac{\operatorname{vol} C_1}{\operatorname{vol} B_n(0,r)} &\geq \frac{k \cdot r \operatorname{vol} B_{n-1}(0, \frac{1}{2}(2-k-l)r)}{(\frac{r}{2})^n 4 \operatorname{vol} B_{n-1}(0,2)} \\
&= \frac{k \cdot r (\frac{1}{2})^{n-1}(2-k-l)^{n-1} r^{n-1}}{(\frac{r}{2})^n \cdot 4 \cdot 2^{n-1}} \\
&= k(2-k-l)^{n-1} 2^{-(n-1)} 2^n 2^{-2} 2^{-(n-1)} \\
&= k(2-k-l)^{n-1} 2^{-n}
\end{aligned}$$

□

Wenn man davon ausgeht, dass man weiß, mit welcher Wahrscheinlichkeit ein Punkt, der zufällig, unabhängig und gleichverteilt aus $B(0,r)$ ausgewäht wird, in der Menge $C_1 \cup C_2$ enthalten ist, kann man ausrechnen, wieviele Punkte insgesamt in der Menge $C_1 \cup C_2$ erwartet werden können, wenn man N Punkte zufällig, unabhängig und gleichverteilt aus $B(0,r)$ auswählt.

Lemma 3.3.4 *Für N gewählt wie in Satz 3.2.5 werden die Punkte $x_1, \ldots, x_N$ der Ursprungsmenge zufällig, unabhängig und gleichverteilt aus $B(0,r)$ gewählt. Für $i \in \{1, \ldots, N\}$ sei die Wahrscheinlichkeit, dass $x_i \in C_1 \cup C_2$ größer als $p = 2^{-c'n}$ mit $c' \in \mathbb{N}$. Dann gibt es mit Wahrscheinlichkeit größer als $1 - \frac{4}{N \cdot p}$ mindestens $\frac{p \cdot N}{2}$ Punkte x_i in der Ursprungsmenge $\{x_1, \ldots, x_n\}$ mit $x_i \in C_1 \cup C_2$.*

Beweis: Für $i \in \{1, \ldots, N\}$ wird x_i zufällig, unabhängig und gleichverteilt aus $B(0,r)$ gewählt und mit Wahrscheinlichkeit p gilt $x_i \in C_1 \cup C_2$. Damit ist die erwartete Anzahl Punkte, die aus der Menge $C_1 \cup C_2$ gewählt werden $p \cdot N$ mit der Varianz $N \cdot p(1-p) < N \cdot p$.
Unter Verwendung der Ungleichung von Tschebyschew folgt:

$$P\left(|X - \underbrace{E(X)}_{=p \cdot N}| \geq \underbrace{\frac{p \cdot N}{2}}_{=:\epsilon}\right) \leq \frac{\mathrm{Var}(X)}{\epsilon^2} < \frac{N \cdot p}{\frac{1}{4}(N \cdot p)^2} = \frac{4}{N \cdot p}.$$

Damit ist die Wahrscheinlichkeit, dass weniger als

$$\frac{p \cdot N}{2}$$

Punkte in $C_1 \cup C_2$ enthalten sind, kleiner als

$$\frac{4}{N \cdot p},$$

also exponentiell klein für $N = 2^{cn} \log_2 R_0$ und $p = 2^{-c'n}$ mit $c' \in \mathbb{N}$.

□

Dieses Lemma hat eine große Bedeutung, weil für die Analyse der modifizierten Samplemethode nur die Gittervektoren $y - x$ interessant sind, für die $x \in C_1 \cup C_2$ gilt, denn nur für diese Vektoren ist die Abbildung τ_u nicht die Identität. Für $x \in B(0,r) \backslash (C_1 \cup C_2)$ gilt: $\tau_u(x) = x$.

3.4. Uniformes Wählen aus einem konvexen Körper

Die in Abschnitt 3.2 beschriebene Samplemethode ist ein randomisierter Algorithmus. Zu Beginn werden N Punkte zufällig, unabhängig und gleichverteilt aus der Kugel $B(0,r)$ bezüglich der ℓ_p-Norm gewählt. Bei der algorithmischen Umsetzung der Samplemethode kann man aber nicht mit beliebiger Genauigkeit arbeiten. Man muss $B(0,r)$ diskretisieren und die kontinuerliche Gleichverteilung möglichst gut approximieren.

Dazu muss man sich zum einen überlegen, wie man aus einer Diskretisierung von $B(0,r)$ einen Punkt zufällig und unabhängig auswählt, so dass die Wahrscheinlichkeit für jeden Punkt ausgewählt zu werden, ungefähr gleichverteilt ist. Zum anderen muss man sich überlegen, mit welcher Genauigkeit die Diskretisierung zu erfolgen hat, ohne dass die Analyse der Samplemethode verfälscht wird.

Diese Aspekte sind für die beschriebene Samplemethode wichtig, da für die Analyse der Samplemethode beziehungsweise der modifizierten Samplemethode nur die Punkte von Bedeutung sind, die aus $B(0,r) \cap (C_1 \cup C_2)$ gewählt werden. Die Mengen C_1 und C_2 können relativ klein

sein. Deswegen muss sichergestellt werden, dass die Auswahl von Punkten aus der Menge $B(0,r)$ so erfolgt, dass die algorithmischen Abweichungen die Funktionsweise der Samplemethode nicht beeinträchtigen. Es muss also gewährleistet werden, dass die Diskretisierung so fein ist, dass mindestens jeweils ein Punkt in den Mengen C_1 und C_2 enthalten ist. Bei Rechnung mit einer Bitgenauigkeit von $n^7 \log_2 R_0$ erhält man eine ausreichend feine Diskretisierung für die Verwendung der Samplemethode zur Lösung des Problems des kürzesten Gittervektors sowie zur Lösung des Problems des nächsten Gittervektors, da in diesem Fall die Diskretisierung feiner ist als die Größe der Mengen C_1 und C_2, die auf Seite 30 sowie auf Seite 54 berechnet wird.

Die Kugel $B(0,r)$ ist jeweils in Bezug auf die entsprechende ℓ_p-Norm definiert. Sie ist ein konvexer Körper im euklidischen Raum $\mathbb{R}^n$ bezüglich der ℓ_2-Norm. Ziel ist es also, Punkte aus einem konvexen Körper möglichst uniform zu wählen. Dyer, Frieze und Kannan haben 1991 einen randomisierten Polynomzeitalgorithmus entwickelt, der das Volumen eines konvexen Körpers approximiert und auf einer Methode basiert, wie man in einem konvexen Körper fast uniform einen Punkt auswählen kann [13]. Voraussetzung ist lediglich, dass man feststellen kann, ob ein Punkt Element des Körpers ist oder nicht. Mit Hilfe dieses Algorithmus kann man aus $B(0,r)$ mit ausreichender Genauigkeit Punkte auswählen.

4. Lösung des Problems des kürzesten Gittervektors mit Hilfe einer Samplemethode

Der in diesem Kapitel beschriebene Algorithmus zur Lösung des Problems des kürzesten Gittervektors für die ℓ_p-Norm beruht auf einer Vorlesungsmitschrift [23] von Regev an der Universität von Tel Aviv, in der eine Samplemethode zur Lösung von SVP in der ℓ_2-Norm vorgestellt wird. Sie greift eine von Sudan vorgeschlagene Siebprozedur auf, die in [2] erwähnt wird. Der Algorithmus von Regev wird hier verallgemeinert, so dass er das Problem des kürzesten Gittervektors für jede ℓ_p-Norm löst.

Die im letzten Kapitel vorgestellte Samplemethode kann dazu verwendet werden, um in einem Gitter, dessen kürzeste Gittervektoren eine Länge im Intervall $[2, 3)$ haben, einen solchen zu berechnen. Mit dem folgenden Satz 4.0.1 wird gezeigt, dass man unter dieser Voraussetzung in jedem beliebigen Gitter einen kürzesten Gittervektor finden kann.

Zur Berechnung verwendet man unter anderem den LLL-Algorithmus von Lenstra, Lenstra und Lovász [26]. Er approximiert bei gegebener Basis B einen kürzesten von 0 verschiedenen Gittervektor in $\mathcal{L}(B)$ mit dem Faktor $2^{\frac{n-1}{2}}$ und benötigt dazu höchstens $\mathcal{O}(n^4 \log_2 \max_k ||b_k||_2)$ arithmetische Operationen beziehungsweise hat eine Laufzeit von $\mathcal{O}(n^6 \log_2 \max_k ||b_k||_2)$.

Satz 4.0.1 *Gegeben sei ein Algorithmus $\mathcal{A}$, der einen kürzesten von 0 verschiedenen Gittervektor bezüglich der ℓ_p-Norm in einem Gitter mit $2 \leq \lambda_1 < 3$ mit Laufzeit T findet. Dann kann ein kürzester Gittervektor in einem beliebigen Gitter, gegeben durch eine Basis B, mit höchstens $\mathcal{O}(n) \cdot T + \mathcal{O}(n^4 \log_2 \max_k ||b_k||_2)$ arithmetischen Operationen gefunden werden.*

Beweis: Sei $\lambda_1^{(p)}$ die Länge des kürzesten Gittervektors in $\mathcal{L}(B)$ bezüglich der ℓ_p-Norm.
Es gilt folgende Abschätzung:

$$||x||_\infty \leq ||x||_p \leq \sqrt[p]{n}||x||_\infty$$

Algorithmus zur Berechnung eines kürzesten Gittervektors in $\mathcal{L}(B)$
`Gegeben: Gitterbasis` B

1. `Anwendung des LLL-Algorithmus auf` $\mathcal{L}(B)$
   `Man erhält als Ausgabe` $\tilde{\lambda}_1$.
2. `Anwendung von` $\mathcal{A}$ `auf` $B_0, B_1, \ldots, B_{2n}$, `wobei`

$$B_k := \frac{1}{\tilde{\lambda}_1}(\frac{3}{2})^k B, \text{ das heißt } b_{ik} = \frac{1}{\tilde{\lambda}_1}(\frac{3}{2})^k \cdot b_i.$$

   `Man erhält als Ausgabe Vektoren` $v_0, \ldots, v_{2n}$.
3. `Definiere` $v'_k := \tilde{\lambda}_1(\frac{2}{3})^k v_k$.

`Ausgabe: Der kürzeste Vektor bezüglich der` ℓ_p`-Norm der Vektoren` $v'_0, \ldots, v'_{2n}$`, der in` $\mathcal{L}(B)\backslash\{0\}$ `enthalten ist.`

Der Beweis, dass dieser Algorithmus wirklich einen von 0 verschiedenen Vektor des Gitters $\mathcal{L}(B)$ berechnet, erfolgt in zwei Schritten. Zunächst wird gezeigt, dass man mit Hilfe eines kürzesten von 0 verschiedenen Gittervektors in $\mathcal{L}(B_k)$ einen kürzesten von 0 verschiedenen Gittervektor in $\mathcal{L}(B)$ berechnen kann, und dass ein $k \in \mathbb{N}$ existiert, so dass die Länge $\lambda_1^{(p)}$ der kürzesten Gittervektoren in $\mathcal{L}(B_k)$ im halboffenen Intervall zwischen 2 und 3 liegt. Im zweiten Teil wird dann gezeigt, dass ein solches k höchstens die Größe $2n$ hat.

Gegeben ist eine Basis $B = \{b_1, \ldots, b_n\}$ des Gitters $\mathcal{L}(B)$. Dann ist das Gitter $\mathcal{L}(B_k)$ gegeben durch

$$B_k = \left\{ \frac{1}{\tilde{\lambda}_1}(\frac{3}{2})^k b_1, \ldots, \frac{1}{\tilde{\lambda}_1}(\frac{3}{2})^k b_n \right\}.$$

Wenn $v = \sum_{i=1}^n a_i b_i$ mit $a_i \in \mathbb{Z}$ ein kürzester Gittervektor in $\mathcal{L}(B)$ bezüglich der ℓ_p-Norm ist, so ist $v' := \sum_{i=1}^n a_i \frac{1}{\tilde{\lambda}_1}(\frac{3}{2})^k b_i \in \mathcal{L}(B_k)$ ein kürzester Gittervektor in $\mathcal{L}(B_k)$ bezüglich der ℓ_p-Norm, denn für einen beliebigen Gittervektor $w \in \mathcal{L}(B)$ gilt:

$$\begin{aligned} & ||v||_p \leq ||w||_p \\ \iff ||v'||_p = \frac{1}{\tilde{\lambda}_1}(\frac{3}{2})^k ||v||_p & \leq \frac{1}{\tilde{\lambda}_1}(\frac{3}{2})^k ||w||_p = ||w'||_p \end{aligned}$$

Damit ist v' ein kürzester Vektor in $\mathcal{L}(B_k)$. Wenn man also im Gitter $\mathcal{L}(B_k)$ einen kürzesten von 0 verschiedenen Gittervektor berechnen kann, so kann man auch im Gitter $\mathcal{L}(B)$ einen kürzesten von 0 verschiedenen Gittervektor berechnen. Für die Länge des kürzesten Gittervektors in $\mathcal{L}(B_k)$ gilt:

$$||v'||_p = \frac{1}{\tilde{\lambda}_1}(\frac{3}{2})^k ||v||_p = \frac{1}{\tilde{\lambda}_1}(\frac{3}{2})^k \lambda_1^{(p)}.$$

Die Länge liegt im Intervall $[2, 3)$, falls folgende Bedingungen erfüllt sind:

$$\begin{aligned} \left(\frac{3}{2}\right)^k \frac{\lambda_1^{(p)}}{\tilde{\lambda}_1} < 3 & \iff k < \frac{\log_2 3\tilde{\lambda}_1 - \log_2 \lambda_1^{(p)}}{\log_2 3 - 1} \\ \left(\frac{3}{2}\right)^k \frac{\lambda_1^{(p)}}{\tilde{\lambda}_1} \geq 2 & \iff k \geq \frac{1 + \log_2 \tilde{\lambda}_1 - \log_2 \lambda_1^{(p)}}{\log_2 3 - 1} \end{aligned}$$

Der kürzeste Gittervektor des Gitters $\mathcal{L}(B_k)$ ist also genau dann im Intervall $[2, 3)$ enthalten, wenn

$$\frac{1 + \log_2 \tilde{\lambda}_1 - \log_2 \lambda_1^{(p)}}{\log_2 3 - 1} \leq k < \frac{\log_2 3\tilde{\lambda}_1 - \log_2 \lambda_1^{(p)}}{\log_2 3 - 1}$$

Da die Länge dieses Intervalls größer als 1 ist, existiert ein $k \in \mathbb{N}_0$, so dass die Länge des kürzesten Vektors in $\mathcal{L}(B_k)$ im Intervall $[2, 3)$ liegt.
Bei Anwendung des LLL-Algorithmus erhält man eine Näherung $\tilde{\lambda}_1$ für die Länge des kürzesten Gittervektors bezüglich der ℓ_2-Norm mit

$$\begin{aligned} \tilde{\lambda}_1 & \leq 2^{\frac{n-1}{2}} \lambda_1^{(2)} \\ & \leq 2^{\frac{n-1}{2}} \sqrt{n} \lambda_1^{(\infty)} \\ & \leq 2^{\frac{n-1}{2}} \sqrt{n} \lambda_1^{(p)} \end{aligned}$$

Damit erhält man als maximale Größe von k:

$$\begin{aligned} k &< \frac{\log_2 3\tilde{\lambda}_1 - \log_2 \lambda_1^{(p)}}{\log_2 3 - 1} \\ &\leq \frac{\log_2 3 \cdot 2^{\frac{n-1}{2}}\sqrt{n}\lambda_1^{(p)} - \log_2 2\lambda_1^{(p)}}{\log_2 3 - 1} \\ &= \frac{\log_2 3 \cdot 2^{\frac{n-3}{2}}\sqrt{n}}{\log_2 3 - 1} \\ &= \frac{\log_2 3 + \frac{n-3}{2}\log_2 2 + \frac{1}{2}\log_2 n}{\log_2 3 - 1} \\ &= \frac{\log_2 3 - \frac{3}{2}}{\log_2 3 - 1} + \frac{1}{2(\log_2 3 - 1)}n + \frac{1}{2(\log_2 3 - 1)}\log_2 n \\ &\leq 2n \end{aligned}$$

und es existiert ein $k \in \{0, \ldots, 2n\}$, so dass die Länge des kürzesten Vektors von $\mathcal{L}(B_k)$ im Intervall $[2, 3)$ liegt.

Der LLL-Algorithmus wird einmal aufgerufen. Bei Eingabe einer Gitterbasis B benötigt der LLL-Algorithmus höchstens $\mathcal{O}(n^4 \log_2 \max_k ||b_k||_2)$ arithmetische Operationen. Der Algorithmus $\mathcal{A}$ mit Laufzeit T wird $2n$-mal aufgerufen. Damit benötigt man höchstens

$$\mathcal{O}(n) \cdot T + \mathcal{O}(n^4 \log_2 \max_k ||b_k||_2)$$

arithmetische Operationen, um in einem beliebigen Gitter einen kürzesten von 0 verschiedenen Gittervektor zu berechnen.

□

4.1. Samplemethode

Die im Folgenden vorgestellte Variante der Samplemethode aus Kapitel 3 benutzt die Siebprozedur 3.1.2 mit $a = 2$, das heißt man sucht in einer beliebigen Menge von Punkten aus einer Kugel vom Radius R eine Teilmenge mit höchstens 5^n Repräsentanten, so dass der Abstand von jedem Punkt der Menge zu seinem Repräsentanten höchstens $\frac{R}{2}$ ist. Mit Hilfe dieser Siebprozedur kann man in einem Gitter L mit $2 \leq \lambda_1(L) < 3$ einen kürzesten Vektor berechnen.

Die Samplemethode berechnet eine Menge $\mathcal{Z}$ mit Gittervektoren, die höchstens die Länge 8 haben. Wenn man die paarweisen Differenzen zwischen allen Elementen aus der Menge $\mathcal{Z}$ betrachtet, kann man mit Hilfe der Randomisierung der Methode beziehungsweise mit Hilfe der modifizierten Samplemethode argumentieren, dass sich ein kürzester von 0 verschiedener Gittervektor $u \in L$ mit hoher Wahrscheinlichkeit unter diesen Differenzen befinden muss. Falls sowohl ein Gittervektor $v \in L$ als auch $v + u \in L$ in der Menge $\mathcal{Z}$ enthalten sind, so ist der Vektor $u = v + u - v$ in der Menge der betrachteten Differenzen enthalten.

Man verwendet die Samplemethode aus Kapitel 3 mit den Parametern

- $r = 2$,

- $\theta = 6$,
- $N = 2^{9n} \log_2 R_0$,

wobei R_0 abhängig von der Eingabe ist, und modifiziert die Ausgabe im Vergleich zur Samplemethode 3.2.1 aus Kapitel 3 in der Form, dass man alle Differenzen von jeweils zwei Paaren aus $\mathcal{Z}$ betrachtet und eine Differenz mit der kürzesten Länge ausgibt.

Algorithmus 4.1.1 Samplemethode
Eingabe: Eine Gitterbasis $B = \{b_1, \ldots, b_n\}$ mit $\lambda_1(\mathcal{L}(B)) \in [2, 3)$.

1. $R_0 \leftarrow n \cdot \max_i ||b_i||_p$
   Wähle $N = 2^{9n} \log_2 R_0$ Punkte $x_1, \ldots, x_N$ zufällig, unabhängig, gleichverteilt in $B(0, 2)$.
   Berechne $y_i \equiv x_i \mod \mathcal{L}(B)$ für $i = 1, \ldots, N$.
   Setze $\mathcal{Z} = \{(x_1, y_1), \ldots, (x_N, y_N)\}$.
   $R \leftarrow R_0$
2. Solange $R > 6$
   a) Anwendung der Siebprozedur (3.1.2) auf $\{y_i | (x_i, y_i) \in \mathcal{Z}\}$ mit den Parametern $a = 2$ und R.
   Man erhält eine Menge J und eine Abbildung η.
   b) Entferne aus der Menge $\mathcal{Z}$ alle Paare (x_i, y_i) mit $i \in J$.
   c) Ersetze jedes verbleibende Paar $(x_i, y_i) \in \mathcal{Z}$ durch $(x_i, y_i - (y_{\eta(i)} - x_{\eta(i)}))$.
   d) $R \leftarrow \frac{R}{2} + 2$
3. Betrachte für alle Paare $(x_i, y_i),\ (x_j, y_j) \in \mathcal{Z}$ die Differenz $(y_i - x_i) - (y_j - x_j)$.
   Ausgabe ist ein kürzester von 0 verschiedener Vektor von diesen Differenzen.

Die Analyse des Algorithmus ist analog zur Analyse der allgemeinen Samplemethode in Kapitel 3. Die Samplemethode hat nach Satz 3.2.4 also eine Laufzeit von

$$2^{\mathcal{O}(n)} \mathcal{O}(\log_2 R_0)^k.$$

Da $N = 2^{9n} \log_2 R_0$ und $a = 2$ enthält die Ausgabemenge $\mathcal{Z}$ nach Satz 3.2.5 noch mindestens 2^{8n} Paare. Wenn der Algorithmus einen Vektor ungleich 0 ausgibt, so hat man eine Approximation mit konstantem Faktor für den kürzesten Gittervektor gefunden.

4.2. Analyse mit Berücksichtigung der Randomisierung

Im Folgenden wird die entsprechende modifizierte Samplemethode betrachtet. Für sie kann man zeigen, dass mit hoher Wahrscheinlichkeit ein von 0 verschiedener Gittervektor kürzester Länge ausgegeben wird. Da sich die modifizierte Samplemethode und die ursprüngliche Samplemethode exakt gleich verhalten, gibt damit auch die Samplemethode mit hoher Wahrscheinlichkeit einen kürzesten von 0 verschiedenen Gittervektor aus.

Sei u ein kürzester von 0 verschiedener Vektor in $\mathcal{L}(B)$, das heißt $||u||_p \in [2, 3)$. Man betrachte die in Abschnitt 3.3 definierten Mengen C_1 und C_2 mit $r = 2$ für diesen Vektor u, sowie die

entsprechende Abbildung $\tau_u : B(0,2) \to B(0,2)$. Die bijektive Abbildung τ_u ist nun genau so gewählt, dass die Differenz $\tau_u(x) - x$ für einen Punkt $x \in C_1 \cup C_2$ der Gittervektor $\pm u$ ist, das heißt, wenn die Samplemethode einen Punkt aus C_1 und den zugehörigen Punkt aus C_2 ausgibt, ist der Vektor $\pm u$ Element der betrachteten Differenzen der Ausgabemenge $\mathcal{Z}$. Der Algorithmus berechnet also in diesem Fall wirklich einen kürzesten von 0 verschiedenen Gittervektor von L.

Unter Verwendung des Gittervektors u erhält man folgende modifizierte Samplemethode, die im weiteren Verlauf analysiert werden soll. Da man die modifizierte Samplemethode lediglich zur Analyse verwendet, kann man den Vektor beziehungsweise die Abbildung τ_u im Algorithmus verwenden, obwohl dieser Vektor und entsprechend diese Abbildung nicht bekannt ist.

Algorithmus 4.2.1 Modifizierte Samplemethode
Eingabe: Eine Gitterbasis $B = \{b_1, \ldots, b_n\}$ mit $\lambda_1(\mathcal{L}(B)) \in [2,3)$.

1. $R_0 \leftarrow n \cdot \max_i ||b_i||_p$
   Wähle $N = 2^{9n} \log_2 R_0$ Punkte $x_1, \ldots, x_N$ zufällig, unabhängig, gleichverteilt in $B(0,2)$.
   Berechne $y_i \equiv x_i \mod \mathcal{L}(B)$ für $i = 1, \ldots, N$.
   Setze $\mathcal{Z} = \{(x_1, y_1), \ldots, (x_N, y_N)\}$.
   $R \leftarrow R_0$
2. Solange $R > 6$
   a) Anwendung der Siebprozedur 3.1.2 auf $\{y_i | (x_i, y_i) \in \mathcal{Z}\}$ mit den Parametern R und $a = 2$.
   Man erhält eine Menge J und eine Abbildung η.
   b) Entscheide für jedes Paar (x_i, y_i) mit $i \in J$ zufällig, unabhängig, gleichverteilt, ob x_i durch $\tau_u(x_i)$ ersetzt wird.
   Entferne aus der Menge $\mathcal{Z}$ alle Paare (x_i, y_i) mit $i \in J$.
   c) Ersetze jedes verbleibende Paar $(x_i, y_i) \in \mathcal{Z}$ durch $(x_i, y_i - (y_{\eta(i)} - x_{\eta(i)}))$.
   d) $R \leftarrow \frac{R}{2} + 2$
3. Entscheide für jedes Paar $(x_i, y_i) \in \mathcal{Z}$ zufällig, unabhängig, gleichverteilt, ob x_i durch $\tau_u(x_i)$ ersetzt wird.
4. Betrachte für alle Paare (x_i, y_i), $(x_j, y_j) \in \mathcal{Z}$ die Differenz $(y_i - x_i) - (y_j - x_j)$.
   Ausgabe ist der kürzeste Vektor ungleich 0 von diesen Differenzen.

Unter Verwendung von Lemma 3.3.3 kann man nun berechnen, mit welcher Wahrscheinlichkeit ein Punkt x, der zufällig, unabhängig und gleichverteilt aus $B(0,2)$ gewählt wird, in der Menge $C_1 \cup C_2$ enthalten ist. Das Gitter L hat die Eigenschaft $2 \leq \lambda_1(L) < 3$. Damit ist die Länge des Vektors u kleiner als $3 = \frac{3}{2} \cdot 2$. Nach Lemma 3.3.3 mit $r = 2$ und $l = \frac{3}{2}$ ist

$$\begin{aligned} k &= 2^{\lfloor \log_2 \frac{2-l}{l} \rfloor} \\ &= 2^{\lfloor \log_2 \frac{1}{3} \rfloor} \\ &= \frac{1}{4} \end{aligned}$$

und es gilt:

$$\begin{aligned}\frac{\mathrm{vol}(C_1)}{\mathrm{vol}(B(0,2))} = \frac{\mathrm{vol}(C_2)}{\mathrm{vol}(B(0,2))} &\geq k\cdot(2-k-l)^{n-1}2^{-n}\\ &= \frac{1}{4}(\frac{1}{4})^{n-1}2^{-n}\\ &= 2^{-2n}2^{-n} = 2^{-3n}.\end{aligned}$$

Damit ist für $i \in \{1,\ldots,N\}$ die Wahrscheinlichkeit p, dass ein Punkt x_i, der zufällig, unabhängig und gleichverteilt aus $B(0,2)$ gewählt wird, in der Menge $C_1 \cup C_2$ enthalten ist, größer als 2^{-3n}. Nach Lemma 3.3.4 mit $p = 2^{-3n}$ und $N = 2^{9n}\log_2 R_0$ gibt es mit Wahrscheinlichkeit exponentiell nahe an 1 mindestens

$$\frac{p\cdot N}{2} = 2^{6n-1}\log_2 R_0$$

Punkte aus $C_1 \cup C_2$ in der Menge $\{x_1,\ldots,x_n\}$ der zu Beginn des Algorithmus ausgewählten Punkte und damit in der Menge $\mathcal{Z}$. Da nach Satz 3.2.5 maximal $2\cdot 5^n \log_2 R_0$ Paare während der Schleife aus der Menge $\mathcal{Z}$ entfernt werden, befinden sich nach der Schleife noch mindestens

$$\begin{aligned}(2^{6n-1} - 2\cdot 5^n)\log_2 R_0 &> (2^{6n-1} - 2\cdot(2^3)^n)\log_2 R_0\\ &= (2^{6n-1} - 2^{3n+1})\log_2 R_0\\ &= 2^{5n}\underbrace{(2^{n-1} - \underbrace{2^{-2n+1}}_{<1})}_{>1}\log_2 R_0\\ &> 2^{5n}.\end{aligned}$$

Paare (x,y) in der Menge $\mathcal{Z}$, für die gilt $x \in C_1 \cup C_2$. Für jedes dieser Paare ist $y - x \in B(0,8)$. Damit hat man mindestens 2^{5n} Gittervektoren $w = y - x$ mit der Eigenschaft $x \in C_1 \cup C_2$ und einer Länge kleiner als 8. Diese Gittervektoren müssen nicht alle verschieden sein. Mit Hilfe des folgenden Lemmas kann man aber zeigen, dass viele Paare der Menge $\mathcal{Z}$ den gleichen Gittervektor repräsentieren müssen, da die Anzahl verschiedener Gitterpunkte in $B(0,8)$ weniger als 2^{4n} ist.

Lemma 4.2.2 *Sei L ein Gitter mit $\lambda_1(L) \geq l$ und sei $R > 0$. Dann gilt:*

$$|B(0,R)\cap L| < \left(\frac{2R+l}{l}\right)^n.$$

Beweis: Der Abstand zwischen zwei Gitterpunkten beträgt mindestens $\lambda_1(L) \geq l$, das heißt, wenn man um jeden Gitterpunkt eine offene Kugel mit dem Radius $\frac{l}{2}$ betrachtet, so sind diese Kugeln disjunkt:

$$B(v,\frac{l}{2}) \cap B(w,\frac{l}{2}) = \emptyset \text{ für alle } v,w \in B(0,R)\cap L.$$

Da nur Gittervektoren aus $B(0,R)$ betrachtet werden, liegt die Vereinigung aller Kugeln in $B(0,R+\frac{l}{2})$. Die Anzahl Elemente von $B(0,R)\cap L$ ist damit durch die Anzahl disjunkter Kugeln $B(0,\frac{l}{2})$ beschränkt, die maximal in der Kugel $B(0,R+\frac{l}{2})$ enthalten sein können.

$$|B(0,R)\cap L| \leq \frac{\mathrm{vol}(B(0,R+\frac{l}{2}))}{\mathrm{vol}(B(0,\frac{l}{2}))} = \frac{(R+\frac{l}{2})^n}{(\frac{l}{2})^n} < \left(\frac{2R+l}{l}\right)^n$$

□

Mit $\lambda_1(\mathcal{L}(B)) \geq 2$ und $R = 8$ erhält unter Verwendung von Lemma 4.2.2 man

$$|B(0,8) \cap \mathcal{L}(B)| < \left(\frac{2 \cdot 8 + 2}{2}\right)^n = 9^n < 2^{4n}.$$

Also ist die Anzahl verschiedener Gitterpunkte in $B(0,8)$ weniger als 2^{4n}, während sich in der Menge $\mathcal{Z}$ mit hoher Wahrscheinlichkeit mindestens 2^{5n} Paare befinden.

Satz 4.2.3 *Die modifzierte Samplemethode berechnet mit Wahrscheinlichkeit exponentiell nahe an 1 einen von 0 verschiedenen kürzesten Gittervektor in einem Gitter L mit $2 \leq \lambda_1(L) < 3$.*

Beweis: In der Menge $\mathcal{Z}$ befinden sich mit hoher Wahrscheinlichkeit mindestens 2^{5n} Paare (x_i, y_i) mit $x_i \in C_1 \cup C_2$ und damit 2^{5n} Gittervektoren der Form $y_i - x_i$ mit $x_i \in C_1 \cup C_2$. Jeder dieser Vektoren hat eine Länge kleiner als 8. Die Anzahl verschiedener Gitterpunkte in $B(0,8)$ ist nach Lemma 4.2.2 weniger als 2^{4n}. Damit gibt es einen Gittervektor $v \in L$ für den mindestens

$$\frac{2^{5n}}{2^{4n}} = 2^n$$

verschiedene Indizes $i \in \{1, \ldots, N\}$ mit $v = y_i - x_i$ und $x_i \in C_1 \cup C_2$ existieren.

Der Gittervektor $u \in L$ wird dann vom Algorithmus ausgegeben, wenn er als Differenz

$$u = (y_i - x_i) - (y_j - x_j)$$

von zwei Paaren (x_i, y_i), $(y_j, x_j) \in \mathcal{Z}$ dargestellt werden kann.

Im dritten Schritt der modifizierten Samplemethode wird für jedes verbleibende Paar $(x_i, y_i) \in \mathcal{Z}$ zufällig, unabhängig und gleichverteilt entschieden, ob τ_u angewendet wird, oder nicht. Falls $x_i \in C_1 \cup C_2$, so erhält man also mit $v = y_i - x_i$ mit Wahrscheinlichkeit $\frac{1}{2}$ den Gitterpunkt $v + u$ beziehungsweise $v - u$ und mit Wahrscheinlichkeit $\frac{1}{2}$ den Gitterpunkt v. Wenn die Abbildung τ_u mindestens einmal auf den Vektor v angewendet wird und v mindestens einmal nicht verändert wird, so erhält man die Differenz

$$v - (v - u) = u$$

und somit einen kürzesten von 0 verschiedenen Gittervektor.

Die Wahrscheinlichkeit, dass zwei Indizes $i, j \in \{1, \ldots, N\}$ existieren mit $(x_i, y_i), (x_j, y_j) \in \mathcal{Z}$ und $(y_i - x_i) - (y_j - x_j) = v - (v - u) = u$ ist

$$> 1 - 2 \cdot 2^{-2^n}.$$

Also findet der Algorithmus mit Wahrscheinlichkeit exponentiell nahe an 1 den Vektor u und damit einen kürzesten von 0 verschiedenen Gittervektor des Gitters L.

□

Da sich nach Satz 3.3.2 die Samplemethode und die modifizierte Samplemethode exakt gleich verhalten, gilt:

Satz 4.2.4 *Die Samplemethode berechnet mit Laufzeit* $2^{\mathcal{O}(n)} \operatorname{poly}(\log_2 R_0)$ *mit Wahrscheinlichkeit exponentiell nahe an 1 einen von 0 verschiedenen Gittervektor in einem Gitter* L *mit* $2 \leq \lambda_1(L) < 3$*, wobei* $R_0 = n \cdot \max_k ||b_k||_p$ *die Eingabegröße ist.*

Mit Hilfe des Algorithmus aus Lemma 4.0.1 kann man dann einen kürzesten Gittervektor in einem beliebigen Gitter berechnen und das Problem des kürzesten Gittervektors mit einem randomisierten Algorithmus in einfach exponentieller Zeit lösen.

Satz 4.2.5 *Man kann in einem beliebigen Gitter einen kürzesten Gittervektor ungleich 0 bezüglich der* ℓ_p*-Norm mit Laufzeit* $2^{\mathcal{O}(n)} \operatorname{poly}(\log_2 R_0)$ *berechnen, wobei* $R_0 = n \cdot \max_k ||b_k||_p$ *die Eingabegröße ist.*

Beweis: Die Berechnung eines kürzesten von 0 verschiedenen Gittervektors erfolgt mit folgendem Algorithmus.

Algorithmus zur Berechnung eines kürzesten Gittervektors in $\mathcal{L}(B)$
`Eingabe: Eine Gitterbasis` B

1. `Anwendung des LLL-Algorithmus auf` $\mathcal{L}(B)$.
   `Man erhält als Ausgabe` $\tilde{\lambda_1}$.

2. `Anwendung der Samplemethode 4.1.1 auf` $B_0, B_1, \ldots, B_{2n}$`, wobei`

$$B_k := \frac{1}{\tilde{\lambda_1}}(\frac{3}{2})^k B\text{, das heißt } b_{ik} = \frac{1}{\tilde{\lambda_1}}(\frac{3}{2})^k \cdot b_i.$$

   `Man erhält als Ergebnis Vektoren` $v_0, \ldots, v_{2n}$.

3. `Definiere` $v'_k := \tilde{\lambda}_1(\frac{2}{3})^k v_k$.

`Ausgabe: Der kürzeste von 0 verschiedene Vektor bezüglich der` ℓ_p`-Norm der Vektoren` $v'_0, \ldots, v'_{2n}$`, der in` $\mathcal{L}(B)\backslash\{0\}$ `enthalten ist.`

Die Samplemethode ist nach Satz 4.2.4 ein randomisierter Algorithmus, der einen kürzesten von 0 verschiedenen Gittervektor bezüglich der ℓ_p-Norm in einem Gitter mit $2 \leq \lambda_1 < 3$ mit Wahrscheinlichkeit exponentiell nahe an 1 findet. Damit berechnet der angegebene Algorithmus nach Lemma 4.0.1 einen kürzesten von 0 verschiedenen Gittervektor in einem beliebigen Gitter. Da die Samplemethode eine Laufzeit von

$$2^{\mathcal{O}(n)} \operatorname{poly}(\log_2 R_0)$$

und der LLL-Algorithmus die Laufzeit $\mathcal{O}(n^6 \log_2 \max_k ||b_k||_2)$ hat, hat der oben angegebene Algorithmus zur Berechnung eines kürzesten von Null verschiedenen Gittervektors die Laufzeit

$$\begin{aligned} & \mathcal{O}(n) \cdot 2^{\mathcal{O}(n)} \operatorname{poly}(\log_2 R_0) + \mathcal{O}(n^6 \log_2 \max_k ||b_k||_2) \\ = \; & 2^{\mathcal{O}(n)} \operatorname{poly}(\log_2 R_0) + \mathcal{O}(n^5 \log_2 R_0) \\ = \; & 2^{\mathcal{O}(n)} \operatorname{poly}(\log_2 R_0). \end{aligned}$$

□

5. Approximation des Problems des nächsten Gittervektors mit Hilfe einer Samplemethode

In diesem Kapitel wird eine $2^{\mathcal{O}(n)}$-Turingreduktion vom Problem des nächsten Gittervektors auf das Problem des kürzesten Gittervektors vorgestellt. Unter der Voraussetzung, dass man SVP exakt lösen kann, kann man eine $c(1+\epsilon)^2$-Approximation für CVP finden. Zur exakten Lösung von SVP ist es zum Beispiel möglich, den in Kapitel 4 vorgestellten Algorithmus zu verwenden. In diesem Fall erhält man damit einen randomisierten $2^{\mathcal{O}(n+\frac{1}{\epsilon})}$-Algorithmus, der eine $c(1+\epsilon)^2$-Approximation von CVP berechnet. Dabei ist c der Approximationsfaktor. Die Größe von c wird in Abschnitt 5.3.4 beschrieben. Die vorgestellte Reduktion basiert im Wesentlichen auf einer Turingreduktion von Ajtai, Kumar und Sivakumar [3], wobei es allerdings nicht nicht gelungen ist, die dort vorgeschlagene Samplemethode vollständig umzusetzen. Aus diesem Grund wird für die Reduktion eine von Blömer entwickelte Variante der Samplemethode aus Kapitel 3 verwendet. Sie wird in Abschnitt 5.3 beschrieben. Allerdings erreicht man mit Hilfe dieser Samplemethode nur den Approximationsfaktor $c(1+\epsilon)^2$ anstatt wie Ajtai, Kumar und Sivakumar $(1+\epsilon)$.

Gegeben ist ein Gitter L vom Rang n und ein Vektor $t \in \text{span}(L)$. Gesucht ist der zu t nächste Gittervektor $z \in L$. Mit D_t bezeichnet man den Abstand von t zum Gitter L, das heißt $D_t = ||z-t||_2$.

5.1. Voraussetzungen für die Reduktion

Bei der Reduktion kann man ohne Einschränkung von gewissen Eigenschaften des Gitters ausgehen. Diese Eigenschaften werden in diesem Abschnitt genannt und ihre Allgemeingültigkeit bewiesen.

Grundlegende Voraussetzung für die Reduktion ist, dass man das Problem des kürzesten Gittervektors exakt lösen kann. Dies wird im Folgenden vorausgesetzt. Unter dieser Voraussetzung kann man ohne Einschränkung davon ausgehen, dass die Länge der kürzesten von 0 verschiedenen Gittervektoren im betrachteten Gitter L gleich 1 ist.

Satz 5.1.1 Konstante Länge des kürzesten Gittervektors
Wenn man das Problem des nächsten Gittervektors mit dem Approximationsfaktor $\delta \geq 1$ für ein Gitter lösen kann, dessen kürzeste Gittervektoren die Länge 1 haben, dann kann man das Problem des nächsten Gittervektors mit dem Approximationsfaktor δ für ein beliebiges Gitter lösen.

Beweis: Der folgende Algorithmus löst das Problem des nächsten Gittervektors mit dem Approximationsfaktor δ.

Algorithmus zur Berechnung des nächsten Gittervektors in $\mathcal{L}(B)$
`Eingabe: Gitterbasis` B `des Gitters` L `und` $t \in \text{span}(L)$

1. `Berechne einen kürzesten von 0 verschiedenen Vektor` $u \in L$.
   `Dann ist` $\lambda_1(L) = ||u||_2$.
2. `Definiere das Gitter` $L' = \mathcal{L}(B')$ `mit`
   $$B' = \{\frac{1}{\lambda_1(L)}b_1, \ldots, \frac{1}{\lambda_1(L)}b_n\}.$$
   `Setze` $t' := \frac{1}{\lambda_1(L)} \cdot t \in \text{span}(L')$.
3. `Löse CVP für das Gitter` L' `und den Vektor` t'.
   `Man erhält einen Vektor` $z' \in L'$ `mit` $||t' - z'||_2 \leq \delta D_{t'}$.

`Ausgabe:` $z = \lambda_1(L)z' \in L$

Um zu beweisen, dass der Algorithmus eine δ-Approximation des zu t nächsten Gittervektors berechnet, muss zum einen gezeigt werden, dass das Gitter L' die Bedingung $\lambda_1(L') = 1$ erfüllt, und zum anderen, dass man mit Hilfe einer δ-Approximation des zu t' nächsten Gittervektors eine δ-Approximation des zu t nächsten Gittervektors berechnen kann.

Sei $w \in L\backslash\{0\}$ ein von 0 verschiedener Gittervektor. Dann ist $w' := \frac{1}{\lambda_1(L)}w \in L'$ und es gilt:

$$\begin{aligned} & ||w||_2 \geq \lambda_1(L) \\ \iff & ||w'||_2 = \frac{1}{\lambda_1(L)}||w||_2 \geq \frac{1}{\lambda_1(L)}\lambda_1(L) = 1. \end{aligned}$$

Damit ist $\lambda_1(L') = 1$ und man kann nach Voraussetzung einen Vektor $z' \in L'$ berechnen mit

$$||t' - z'||_2 \leq \delta D_{t'},$$

wobei $D_{t'}$ der Abstand von t' zum Gitter L' ist.
Sei $z := \lambda_1(L) \cdot z' \in L$. Dann ist

$$||t - z||_2 = ||\lambda_1(L)t' - \lambda_1(L)z'||_2 = \lambda_1(L)||t' - z'||_2 \leq \lambda_1(L)\delta D_{t'}.$$

Der Vektor z ist eine δ-Approximation des zu t nächsten Gittervektors, wenn gilt: $D_{t'} = \frac{1}{\lambda_1(L)}D_t$. Um dies zu zeigen, betrachtet man die Fälle $D_t < \lambda_1(L)D_{t'}$ und $D_t > \lambda_1(L)D_{t'}$ und führt diese jeweils zu einem Widerspruch:

1. Es sei $D_t < \lambda_1(L)D_{t'}$.
   Für $w \in L$ mit $||t - w||_2 = D_t$ ist $w' := \frac{1}{\lambda_1(L)}w \in L'$ und es gilt:
   $$||t' - w'||_2 = \frac{1}{\lambda_1(L)}||t - w|| = \frac{1}{\lambda_1(L)}D_t < D_{t'}.$$
   Dies ist ein Widerspruch zur Definition von $D_{t'} = \min\{||t' - v'||_2 | v' \in L'\}$.
2. Sei $D_t > \lambda_1(L)D_{t'}$.
   Für $w' \in L'$ mit $||t' - w'||_2 = D_{t'}$ ist $w := \lambda_1(L)w' \in L$ und man erhält wegen
   $$||t - w||_2 = \lambda_1(L)||t' - w'||_2 = \lambda_1(L)D_{t'} < D_t$$
   einen Widerspruch zur Definition von D_t.

Deswegen muss gelten: $D_t = \lambda_1(L)D_{t'}$ und damit ist

$$||t - z||_2 \leq \delta D_t.$$

Der vom Algorithmus berechnete Vektor $z \in L$ ist also eine δ-Approximation des zu t nächsten Gittervektors.

□

Im Folgenden soll gezeigt werden, dass ohne Einschränkung $D_t \leq \frac{n^4}{2\epsilon^2}$ angenommen werden kann, denn falls $D_t > \frac{n^4}{2\epsilon^2}$, so kann man CVP mit dem Approximationsfaktor $c(1+\epsilon)^2$ lösen, indem man CVP mit dem Approximationsfaktor $c(1+\hat{\epsilon})^2$ für ein $\hat{\epsilon} > 0$ in einem Gitter vom Rang $n-1$ löst.

Satz 5.1.2 Obere Schranke für den Abstand zum Gitter
Unter der Voraussetzung, dass man in einem beliebigen Gitter vom Rang $n-1$ das Problem des nächsten Gittervektors mit dem Approximationsfaktor $c(1+\hat{\epsilon})^2$ für alle $\hat{\epsilon} > 0$ und einer Konstante c lösen kann, kann man das Problem des nächsten Gittervektors mit dem Approximationsfaktor $c(1+\epsilon)^2$ für alle $\epsilon > 0$ in einem beliebigen Gitter vom Rang n mit $D_t > \frac{n^4}{2\epsilon^2}$ lösen.

Beweis: Sei $D_t > \frac{n^4}{2\epsilon^2}$.
Nach Satz 5.1.1 kann man ohne Einschränkung davon ausgehen, dass für das Gitter L gilt: $\lambda_1(L) = 1$. Durch Anwendung eines Algorithmus für das Problem des kürzesten Gittervektors findet man einen Gittervektor $u \in L$ mit $||u||_2 = 1$.

Sei $B = \{b_1, \ldots, b_n\}$ eine Basis von L, das heißt $L = \mathcal{L}(b_1, \ldots, b_n)$. Man erhält die orthogonale Projektion $\hat{L}$ von L auf u wie folgt:
Für $i \in \{1, \ldots, n\}$ setze

$$\hat{b}_i := b_i - \frac{\langle b_i, u\rangle}{\langle u, u\rangle} u.$$

Dann ist $\hat{b}_i$ die Projektion von b_i orthogonal zu u, denn es gilt:

$$\begin{aligned} \langle \hat{b}_i, u\rangle &= \langle b_i, u\rangle - \frac{\langle b_i, u\rangle}{\langle u, u\rangle}\langle u, u\rangle \\ &= \langle b_i, u\rangle - \langle b_i, u\rangle \\ &= 0. \end{aligned}$$

Die Vektoren $\hat{B} = \{\hat{b_1}, \ldots, \hat{b_n}\}$ bilden ein Erzeugendensystem des Gitters $\hat{L}$. Sei $w \in L$ beliebig mit $w = \sum_{i=1}^n w_i b_i$ und $w_i \in \mathbb{Z}$ für alle $i \in \{1, \ldots, n\}$. Dann ist

$$\hat{w} := \sum_{i=1}^n w_i \hat{b}_i \in \hat{L}$$

die Projektion von w orthogonal zu u.
Sei $\hat{t}$ die Projektion von $t = \sum_{i=1}^n \alpha_i b_i$ mit $\alpha_i \in \mathbb{R}$ für alle $i \in \{1, \ldots, n\}$ in den Unterraum $\text{span}(\hat{L})$:

$$\hat{t} := \sum_{i=1}^n \alpha_i \hat{b}_i.$$

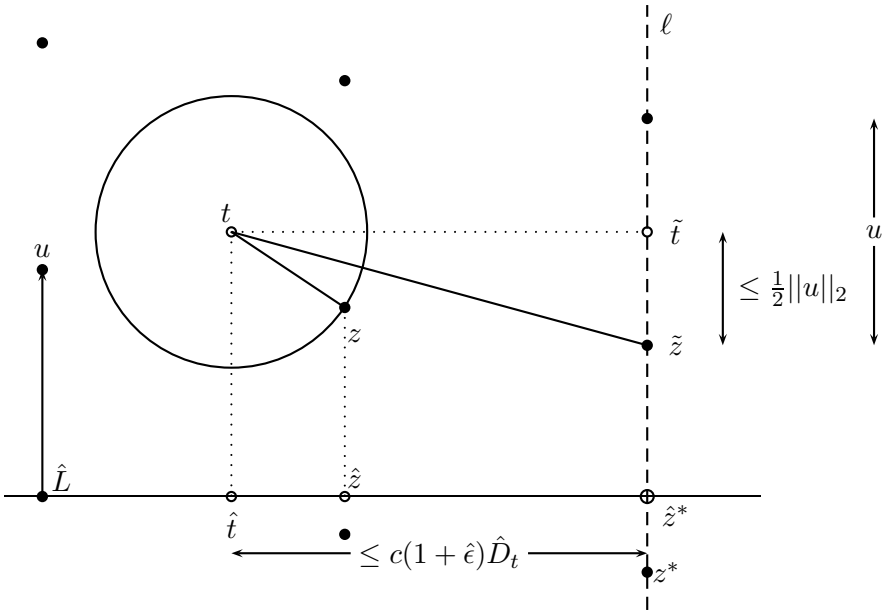

Abbildung 5.1.: Kannans Homogenisierungstechnik

Die Lage von L und $\hat{L}$ ist in Abbildung 5.1 dargestellt. Dabei werden alle Gitterpunkte des Gitters L durch ausgefüllte Punkte repräsentiert, während alle sonstigen Punkte durch nicht ausgefüllte Punkte symbolisiert werden.
Das Gitter $\hat{L}$ ist ein Gitter vom Rang $n-1$. Sei $D_{\hat{t}}$ sei der Abstand von $\hat{t}$ zum Gitter $\hat{L}$.
Setze

$$\hat{\epsilon} := \epsilon\left(1 - \frac{1}{n^4}\right).$$

Dann findet man nach Voraussetzung einen Vektor $\hat{z}^* = \sum_{i=1}^{n} \beta_i \hat{b}_i \in \hat{L}$ mit $\beta_i \in \mathbb{Z}$ für alle $i \in \{1, \ldots, n\}$, so dass gilt:

$$||\hat{z}^* - \hat{t}||_2 \leq c(1+\hat{\epsilon})^2 D_{\hat{t}}.$$

Sei $z^* := \sum_{i=1}^{n} \beta_i b_i \in L$. Es ist

$$\begin{aligned} t - \hat{t} &= \sum_{i=1}^{n} \alpha_i (b_i - \hat{b}_i) \\ &= \sum_{i=1}^{n} \alpha_i \frac{\langle b_i, u\rangle}{\langle u, u\rangle} u \\ &=: \alpha \cdot u \end{aligned}$$

mit $\alpha \in \mathbb{R}$ und

$$\begin{aligned} z^* - \hat{z}^* &= \sum_{i=1}^{n} \beta_i (b_i - \hat{b}_i) \\ &= \sum_{i=1}^{n} \beta_i \frac{\langle b_i, u \rangle}{\langle u, u \rangle} u \\ &=: \beta \cdot u \end{aligned}$$

mit $\beta \in \mathbb{R}$. Man betrachte den Vektor

$$\tilde{z} := z^* + \lfloor \alpha - \beta \rceil \cdot u \in L,$$

wobei $\lfloor \alpha - \beta \rceil$ die zu $\alpha - \beta$ nächste ganze Zahl bezeichnet. Auf diese Weise liftet man den Vektor $\hat{z}^*$ zu einem Gittervektor $\tilde{z}$ und es gilt:

$$\begin{aligned} ||t - \tilde{z}||_2^2 &\leq ||t - z^* - \lfloor \alpha - \beta \rceil \cdot u||_2^2 \\ &= ||\alpha \cdot u + \hat{t} - \beta \cdot u - \hat{z}^* - \lfloor \alpha - \beta \rceil \cdot u||_2^2 \\ &\leq ||\hat{t} - \hat{z}^*||_2^2 + \underbrace{|(\alpha - \beta) - \lfloor \alpha - \beta \rceil|^2}_{\leq (\frac{1}{2})^2} ||u||_2^2 \\ &\leq ||\hat{t} - \hat{z}^*||_2^2 + (\frac{1}{2}||u||_2)^2 \\ &\leq c^2(1+\hat{\epsilon})^4 \hat{D}_t^2 + \frac{1}{4} \\ &\leq (\frac{1}{2} + c(1+\hat{\epsilon})^2 D_t)^2 \\ &< \left(c\frac{\epsilon^2}{n^4} + c(1 + 2\hat{\epsilon} + \hat{\epsilon}^2) \right)^2 D_t^2 \qquad \left(\text{mit } \frac{1}{2} = \frac{n^4}{2\epsilon^2} \cdot \frac{\epsilon^2}{n^4} < D_t \frac{\epsilon^2}{n^4} < c D_t \frac{\epsilon^2}{n^4} \right) \\ &= c^2 \left(\frac{\epsilon^2}{n^4} + 1 + 2\epsilon - 2\frac{\epsilon}{n^4} + \epsilon^2 - 2\frac{\epsilon^2}{n^4} + \frac{\epsilon^2}{n^8} \right)^2 D_t^2 \qquad \left(\text{mit } \hat{\epsilon} = \epsilon(1 - \frac{1}{n^4}) \right) \\ &= c^2 \left((1+\epsilon)^2 - \frac{2\epsilon}{n^4} - \frac{\epsilon^2}{n^4} + \frac{\epsilon^2}{n^8} \right)^2 D_t^2 \\ &\leq c^2 (1+\epsilon)^2 D_t^2 \\ \Longrightarrow ||t - z^*||_2 &\leq c(1+\epsilon)^2 D_t \end{aligned}$$

Damit ist $z^* \in L$ eine $c(1+\epsilon)^2$-Approximation des zu t nächsten Gittervektors. Die in diesem Beweis verwendete Technik ist auch unter dem Namen „Kannans Homogenisierungstechnik" bekannt [21].

□

Falls also der Abstand von t zum Gitter L größer als $\frac{n^4}{2\epsilon^2}$ ist, findet man eine $c(1+\epsilon)^2$-Approximation des Problems des nächsten Gittervektors, indem man eine Approximation von CVP in einem Gitter vom Rang $n-1$ findet. Für $n = 2$ kann man CVP exakt lösen. Für die spätere Berechnung der Laufzeit ist es an dieser Stelle wichtig, folgendes festzustellen: Da man nicht weiß, ob $D_t \leq \frac{n^4}{2\epsilon^2}$ oder $D_t > \frac{n^4}{2\epsilon^2}$, muss man das Problem des nächsten Gittervektors für beide Fälle lösen. Die beste Approximation des zu t nächsten Gittervektors ist dann derjenige

berechnete Gittervektor, der von t den kleinsten Abstand hat. Da man für $D_t > \frac{n^4}{2\epsilon^2}$ CVP nur rekursiv lösen kann, muss man also insgesamt für jedes $i \in \mathbb{N}$ mit $2 < i \leq n$ zweimal das Problem des nächsten Gittervektors lösen, wobei man jeweils in einem Fall – $D_t > \frac{n^4}{2\epsilon^2}$ – auf eine Lösung von CVP für $i-1$ zurückgreift und diesen Vektor zu einer neuen Lösung liftet.

Im Folgenden sei also $D_t \leq \frac{n^4}{2\epsilon^2}$.

Es wird nun gezeigt, dass man im Weiteren ohne Einschränkung davon ausgehen kann, dass das Gitter L eine Basis der Länge $\text{poly}(n)D_t = \text{poly}(n, \frac{1}{\epsilon})$ hat.

Satz 5.1.3 Polynomielle Länge der Basis
Unter der Voraussetzung, dass man in einem beliebigen Gitter vom Rang $n-1$ das Problem des nächsten Gittervektors mit dem Approximationsfaktor $c(1+\epsilon)^2$ lösen kann, kann man das Problem des nächsten Gittervektors für ein Gitter L vom Rang n, das keine Basis polynomieller Länge hat, mit dem Approximationsfaktor $c(1+\epsilon)^2$ lösen.

Beweis: Sei L^* das duale Gitter von L und $u \in L^*$ ein kürzester von 0 verschiedener Gittervektor, das heißt $\lambda_1(L^*) = ||u||_2$.

Falls $\lambda_1(L^*) \geq \frac{1}{3(1+\epsilon)^2 D_t}$, so hat L eine Basis polynomieller Länge, denn nach einer Transferschranke von Cai, Satz 2.4.3, gilt: $1 \leq \lambda_1(L^*)\,\text{bl}(L) \leq n$ und damit hat L eine Basis der Länge

$$\text{bl}(L) \leq \frac{1}{\lambda_1(L^*)} n \leq 3n(1+\epsilon)^2 D_t.$$

Sei also $\lambda_1(L^*) < \frac{1}{3(1+\epsilon)^2 D_t}$, das heißt $D_t < \frac{1}{3(1+\epsilon)^2 \lambda_1(L^*)}$.
Sei H das Untergitter von L orthogonal zu u vom Rang $n-1$. Da L ein Gitter vom Rang n ist, existiert $i \in \{1, \ldots, n\}$ mit $\langle b_i, u\rangle = 0$. Ohne Einschränkung sei $\langle b_n, u\rangle = 0$.

$$\begin{aligned} H &= \{v \in L | \langle u, v\rangle = 0\} \\ &= \{v \in \mathcal{L}(b_1, \ldots, b_{n-1}) | \langle u, v\rangle = 0\} \end{aligned}$$

Zur Veranschaulichung siehe Abbildung 5.2. Sei $u_0 \in \text{span}(L^*)$ mit $\langle u_0, u\rangle = 1$. Man betrachtet die Hyperebenen

$$H_i := i \cdot u_0 + H \text{ für } i \in \mathbb{Z}.$$

Der Abstand der einzelnen Hyperebenen ist

$$\frac{1}{\lambda_1(L^*)} > 3(1+\epsilon)^2 D_t.$$

und damit ist die Hyperebene H_i, die von t den kleinsten Abstand hat, eindeutig bestimmt. Es ist $z \in H_i$, da $||t - z||_2 < \frac{3}{2}(1+\epsilon)^2 D_t$. Auf Grund der linearen Unabhängigkeit der Vektoren $\{b_1, \ldots, b_n\}$ beziehungsweise $\{b_1, \ldots, b_{n-1}, u_0\}$ gilt:

$$\hat{z} := z - i \cdot b_n \in \mathcal{L}(b_1, \ldots, b_{n-1}).$$

Sei

$$\hat{t} := t - i \cdot b_n$$

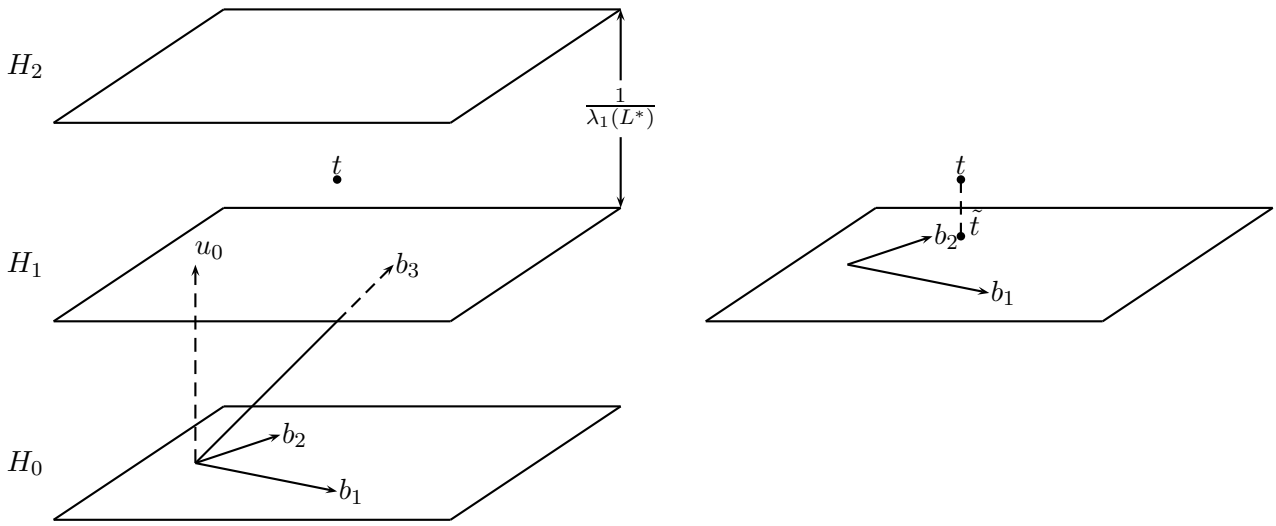

Abbildung 5.2.: Das Untergitter H und das Untergitter H_1 vom Rang $n-1$

Dann ist $\hat{z}$ der zu $\hat{t}$ nächste Gittervektor in $\mathcal{L}(b_1, \ldots, b_{n-1})$.
Das Gitter $\mathcal{L}(b_1, \ldots, b_{n-1})$ hat den Rang $n-1$. Nach Voraussetzung findet man einen Vektor $\hat{z}^* \in \mathcal{L}(b_1, \ldots, b_{n-1})$ mit

$$||\hat{t} - \hat{z}^*||_2 \leq c(1+\epsilon)^2 ||\hat{t} - \hat{z}||_2.$$

Setze $z^* := \hat{z}^* + i \cdot b_n \in \mathcal{L}(b_1, \ldots, b_n) = L$. Dann ist z^* eine $c(1+\epsilon)^2$ Approximation des zu t nächsten Gittervektors, denn

$$\begin{aligned} ||t - z^*||_2 &= ||\hat{t} + i \cdot b_n - \hat{z}^* - i \cdot b_n||_2 \\ &= ||\hat{t} - \hat{z}^*||_2 \\ &\leq c(1+\epsilon)^2 ||\hat{t} - \hat{z}||_2 \\ &= c(1+\epsilon)^2 ||t - i \cdot b_n - z + i \cdot b_n||_2 \\ &= c(1+\epsilon)^2 ||t - z||_2 \\ &= c(1+\epsilon)^2 D_t. \end{aligned}$$

Es muss allerdings nicht gelten, dass $\hat{t} \in \text{span}(b_1, \ldots, b_{n-1})$. Für $t \notin \text{span}(b_1, \ldots, b_{n-1})$ findet man eine $c(1+\epsilon)^2$-Approximation des zu $\hat{t}$ nächsten Gittervektors, indem man das Problem des nächsten Gittervektors für die orthogonale Projektion von t zu $\text{span}(b_1, \ldots, b_{n-1})$ löst. Sei

$$\tilde{t} := \hat{t} - \frac{\langle \hat{t}, u_0 \rangle}{\langle u_0, u_0 \rangle} u_0.$$

Es gilt $\tilde{t} \in \text{span}(b_1, \ldots, b_{n-1})$, da $\langle \tilde{t}, u_0 \rangle = 0$. Auf Grund der Dreiecksungleichung ist der zu $\hat{t}$ nächste Gittervektor $\hat{z}$ auch der zu $\tilde{t}$ nächste Gittervektor. Durch Lösung des Problems des nächsten Gittervektors für das Gitter $\mathcal{L}(b_1, \ldots, b_{n-1})$ und $\tilde{t}$ findet man einen Vektor $\hat{z}^* \in \mathcal{L}(b_1, \ldots, b_{n-1})$ mit

$$||\tilde{t} - \hat{z}^*||_2 < c(1+\epsilon)^2 ||\tilde{t} - \hat{z}||_2.$$

Dann gilt:

$$\begin{aligned} ||\hat{t} - \hat{z}^*||_2^2 &= ||\hat{t} - \tilde{t}||_2^2 + ||\tilde{t} - \hat{z}^*||_2^2 \\ &\leq ||\hat{t} - \tilde{t}||_2^2 + c^2(1+\epsilon)^4 ||\tilde{t} - \hat{z}||_2^2 \\ &\leq c^2(1+\epsilon)^4 (||\hat{t} - \tilde{t}||_2^2 + ||\tilde{t} - \hat{z}||_2^2) \\ &= c^2(1+\epsilon)^2 ||\hat{t} - \hat{z}||_2^2 \end{aligned}$$

und damit ist $||\hat{t} - \hat{z}^*||_2 \leq c(1+\epsilon)||\hat{t} - \hat{z}||_2$.

□

Für denn Fall, dass das Gitter L keine Basis der Länge $\text{poly}(n) D_t = \text{poly}(n, \frac{1}{\epsilon})$ hat, kann man eine $c(1+\epsilon)^2$-Approximation des zu t nächsten Gittervektors finden, indem man eine Approximation für das Problem des nächsten Gittervektors für ein Gitter vom Rang $n-1$ löst.

Um eine Approximation des zu t nächsten Gittervektors zu finden, arbeitet man nicht auf dem Gitter L, sondern verwendet ein $(n+1)$-dimensionales Gitter L', das durch

$$\{(v, 0) | v \in L\} \cup \{(t, \gamma)\}$$

erzeugt wird, wobei γ ein beliebiger Parameter ist. Da man nach Satz 5.1.3 ohne Einschränkung davon ausgehen, dass L eine Basis polynomieller Länge hat, hat auch L' eine Basis polynomieller Länge:

Satz 5.1.4 *Sei L ein beliebiges Gitter, $t \in \text{span}(L)$ und γ eine beliebige Konstante. Falls L eine Basis der Länge höchstens* $\text{poly}(n) \cdot D_t$ *hat, so hat das Gitter L', das durch $\{(v,0)|v \in L\} \cup \{(t,\gamma)\}$ erzeugt wird, eine Basis der Länge* $\max\{\text{poly}(n) \cdot D_t, 1\}$.

Beweis: Sei $B = \{b_1, \ldots, b_n\}$ eine Basis von L mit

$$||b_i||_2 \leq n^\alpha D_t \text{ für alle } i \in \{1, \ldots, n\}$$

und $\alpha \in \mathbb{N}$ konstant.
Sei $z^* \in L$ der Gittervektor, den man erhält, wenn man $t = \sum_{i=1}^{n} a_i b_i \in \text{span}(L)$ mit $a_i \in \mathbb{R}$ für alle $i \in \{1, \ldots, n\}$ in Bezug zur Basis B rundet:

$$z^* := \sum_{i=1}^{n} \lfloor a_i \rceil b_i.$$

Dann gilt für den Abstand zwischen z^* und t:

$$\begin{aligned} ||z^* - t||_2 &= ||\sum_{i=1}^{n} (\lfloor a_i \rceil - a_i) b_i||_2 \\ &\leq \sum_{i=1}^{n} ||b_i||_2 \\ &\leq \sum_{i=1}^{n} n^\alpha D_t \\ &= n^{\alpha+1} D_t \end{aligned}$$

Die Vektoren $B \cup \{(z^* - t, -\gamma)\}$ bilden ein Erzeugendensystem des Gitters L', da $(z^* - t, -\gamma) = (z^*, 0) - (t, \gamma)$ mit $z^* \in L$. Damit hat L' eine Basis der Länge $\text{poly}(n) D_t$, falls L eine Basis der Länge $\text{poly}(n) D_t$ hat und $\text{poly}(n) D_t \geq 1$.

□

Zusammenfassend lässt sich also feststellen, dass die Länge der Basis von L entweder polynomiell in n und $\frac{1}{\epsilon}$ beschränkt ist und damit dann auch die Länge der Basis von L' oder man das Problem des nächsten Gittervektors in n Rekursionsschritten lösen kann.

5.2. Reduktion

Falls D_t kleiner als $\frac{1}{2}$ ist, kann man den zu t nächsten Gittervektor dadurch bestimmen, dass man in einem konstruierten Gitter $\tilde{L}$ einen kürzesten Gittervektor bestimmt. Dies wird im folgenden Abschnitt erläutert. Für den Fall, dass D_t größer $\frac{1}{2}$ ist, benötigt man zur Bestimmung des zu t nächsten Gittervektors eine Variante der vorgestellten Samplemethode aus Kapitel 3 für das Gitter $L'(k)$. Die Vorgehensweise in diesem Fall wird in Abschnitt 5.2.2 erläutert.

5.2.1. Reduktion mit $D_t < \frac{1}{2}$

Satz 5.2.1 *Sei L ein beliebiges Gitter und $t \in Span(L)$ mit $D_t < \frac{1}{2}$. Dann kann man den zu t nächsten Gittervektor $z \in L$ berechnen, wenn man das Problem des kürzesten Gittervektors exakt lösen kann.*

Beweis: Sei $D_t < \frac{1}{2}$.
Dann kann man den zu t nächsten Gittervektor dadurch bestimmen, dass man einen kürzesten Gittervektor in dem Gitter $\tilde{L}$ bestimmt, das durch $\{(v,0)|v \in L\} \cup \{(t, \frac{1}{2})\}$ erzeugt wird, denn die kürzesten Gittervektoren in $\tilde{L}$ sind von der Form $(z,0) \pm (t, \frac{1}{2})$ mit $z \in L$ und $||z-t||_2 = D_t$.

Sei $z \in L$ mit $||z-t||_2 = D_t$. Dann haben die Gittervektoren $(z,0) \pm (t, \frac{1}{2})$ die Länge:

$$\begin{aligned} ||(z,0) \pm (t, \frac{1}{2})||_2^2 &= ||z \pm t||_2^2 + (\frac{1}{2})^2 \\ &= D_t^2 + \frac{1}{4} \\ &< \frac{1}{4} + \frac{1}{4} \\ &= \frac{1}{2} \end{aligned}$$

Kein Gittervektor $(v,0) \in \tilde{L}$ kann eine Länge kleiner als 1 haben, da $\lambda_1(L) = 1$.

Sei $(v,0) - a(t, \frac{1}{2}) \in \tilde{L}$ mit $a \in \mathbb{Z}$, $|a| \geq 2$. Dann gilt unter Berücksichtigung von $||(z,0) \pm (t, \frac{1}{2})||_2^2 < \frac{1}{2}$:

$$\begin{aligned} ||(v,0) - a(t, \frac{1}{2})||_2^2 &= ||v - at||_2^2 + a^2 \frac{1}{4} \\ &\geq a^2 \frac{1}{4} \\ &\geq 4 \frac{1}{4} \\ &> \frac{1}{2} \\ &> ||(z,0) \pm (t, \frac{1}{2})||_2^2 \end{aligned}$$

Damit sind die kürzesten Gittervektoren in $\tilde{L}$ von der Form $(z,0) \pm (t, \frac{1}{2})$. Für den Fall $D_t < \frac{1}{2}$ ist es also möglich den zu t nächsten Gittervektor $z \in L$ bestimmen, indem man einen kürzesten Gittervektor im Gitter $\tilde{L}$ bestimmt. Dies kann zum Beispiel mit der angegebenen Samplemethode aus Kapitel 4 erfolgen.

□

Die Konstante $\frac{1}{2}$ ist hier im Sinne einer einfachen Formulierung gewählt worden. Man kann als Konstante auch $(1+\epsilon)^{k_0}$ mit $k_0 \in \mathbb{Z}$ maximal mit $(1+\epsilon)^{2k_0} \left(1 + \frac{c^2}{3}(1+\epsilon)^2\right) < 1$ wählen. In diesem Fall erhält man einen zu t nächsten Gittervektor $z \in L$, indem man einen kürzesten Gittervektor in dem Gitter berechnet, das durch $\{(v,0)|v \in L\} \cup \{(t,\gamma)\}$ mit $\gamma = \frac{c}{\sqrt{3}}(1+\epsilon)^{k_0+1}$ erzeugt wird. Der Beweis dazu erfolgt analog zu dem obigen Beweis.

5.2.2. Reduktion mit $D_t \geq \frac{1}{2}$

Anders als im Fall $D_t < \frac{1}{2}$ kann man für den Fall $D_t \geq \frac{1}{2}$ das Problem des nächsten Gittervektors nicht auf eine so direkte Art und Weise lösen. Um in diesem Fall eine Approximation des zu t nächsten Gittervektors zu berechnen, benötigt man die zusätzliche Information

$$(1+\epsilon)^{k-1} \leq D_t < (1+\epsilon)^k.$$

Nur mit Hilfe dieser Information kann man eine $c(1+\epsilon)^2$-Approximation von CVP berechnen. Da man nicht weiß, für welches $k \in \mathbb{Z}$ diese Ungleichung erfüllt ist, führt man die Berechnungen für alle $k \in \mathbb{Z}$ mit $k_0 \leq k \leq k_1$ für Parameter $k_0, k_1 \in \mathbb{Z}$ durch. Für jedes k berechnet man einen Gittervektor $z_k \in L$ und gibt anschliessend denjenigen Vektor z_k aus, für den $||t - z_k||_2$ minimal wird. Wenn man k_0 und k_1 so wählt, dass

$$\frac{1}{2} = (1+\epsilon)^{k_0} \text{ und } D_t \leq (1+\epsilon)^{k_1},$$

so werden die Berechnungen – für den Fall $D_t \geq \frac{1}{2}$ – immer für das $k \in \mathbb{Z}$ durchgeführt mit $(1+\epsilon)^{k-1} \leq D_t < (1+\epsilon)^k$. Wenn man unter dieser Voraussetzung eine $c(1+\epsilon)^2$ des zu t nächsten Gittervektors berechnen kann, findet man auf diese Weise eine Approximation des zu t nächsten Gittervektors.

Es genügt, wenn man die Reduktion für $k \geq -\frac{1}{\log_2(1+\epsilon)}$ durchführt, denn es ist

$$-\frac{1}{\log_2(1+\epsilon)} = \frac{\log_2(\frac{1}{2})}{\log_2(1+\epsilon)} = \log_{1+\epsilon}\frac{1}{2}$$

und damit

$$(1+\epsilon)^{-\frac{1}{\log_2(1+\epsilon)}} = \frac{1}{2}.$$

Man setze also $k_0 := -\frac{1}{\log_2(1+\epsilon)}$. Um eine obere Schranke für D_t zu berechnen, wird verwendet, dass man nach Satz 5.1.2 ohne Einschränkung davon ausgehen kann, dass

$$\begin{aligned} D_t \leq \frac{n^4}{2\epsilon^2} &= \frac{2^{4\log_2 n}}{2 \cdot 2^{2\log_2 \epsilon}} \\ &= 2^{4\log_2 n - 2\log_2 \epsilon - 1} \\ &= 2^{4\log_2 n + 2\log_2 \frac{1}{\epsilon} - 1} \end{aligned}$$

Damit genügt es, wenn man $k_1 := 4\log_2 n + 2\log_2 \frac{1}{\epsilon} - 1$ setzt. Für die so gewählten Parameter k_0, k_1 gilt:

$$(1+\epsilon)^{k_0} \leq D_t \leq (1+\epsilon)^{k_1}$$

Im Folgenden wird nur noch beschrieben, wie man für $k \in \mathbb{Z}$ mit $k_0 \leq k \leq k_1$ und $(1+\epsilon)^{k-1} \leq D_t < (1+\epsilon)^k$ einen Gittervektor $z_k \in L$ berechnet und gezeigt, dass man in diesem Fall eine Approximation des zu t nächsten Gittervektors berechnen kann. Für alle k mit $k_0 \leq k \leq k_1$ führt man die gleichen Berechnungen durch, man kann jedoch nur im Fall $(1+\epsilon)^{k-1} \leq D_t < (1+\epsilon)^k$ zeigen, dass man eine Approximation von CVP berechnen kann.

Für jeden Wert $k \in \mathbb{Z}$ arbeitet der Algorithmus auf dem $(n+1)$-dimensionalen Gitter $L'(k)$, das durch $\{(v,0)|v \in L\} \cup \{(t,\gamma_k)\}$ erzeugt wird. Die Komponente γ_k muss dabei in der Größenordnung von D_t sein; kann also nicht konstant gewählt werden. Den Grund dafür sieht man

im Beweis von Lemma 5.2.2.
Man kann zum Beispiel

$$\gamma_k := c \cdot \frac{1}{\sqrt{3}}(1+\epsilon)^{k+1}$$

wählen. Dabei ist $c \in \mathbb{N}$ der Approximationsfaktor, mit dem der zu t nächste Gittervektor z approximiert wird.

Um einen zu t nächsten Gittervektor zu berechnen, betrachtet man zwei Teilmengen des Gitters $L'(k)$:

$$\begin{aligned} \mathcal{B} &:= \{(v,0) \in L'(k) |\ ||v||_2 < 2\gamma_k\} \\ \mathcal{G} &:= \{(v,w) \in L'(k) |\ w = \pm\gamma_k, ||(v,w)||_2 < 2\gamma_k\} \end{aligned}$$

Die Teilmengen $\mathcal{B}$ und $\mathcal{G}$ sind eine disjunkte Zerlegung der Menge $L'(k) \cap B(0, 2\gamma_k)$.

Lemma 5.2.2

$$\mathcal{G} \cup \mathcal{B} = L'(k) \cap B(0, 2\gamma_k)$$

Beweis: Es ist offensichtlich, dass $\mathcal{G} \cup \mathcal{B} \subseteq L'(k) \cap B(0, 2\gamma_k)$ gilt, da nach Definition der Mengen $\mathcal{B}$ und $\mathcal{G}$ für jeden Gittervektor $x \in \mathcal{G}$ beziehungsweise $x \in \mathcal{B}$ gilt: $||x||_2 < 2\gamma_k$.

Jeder Gittervektor $x \in L'(k) \cap B(0, 2\gamma_k)$ hat entweder die Form $(v, 0)$ mit $v \in L$ oder $(v, 0) + a(t, \gamma_k)$ mit $a \in \mathbb{Z}$ und $v \in L$.

1. Sei $x = (v, 0)$ mit $v \in L$ und $||x||_2 < 2\gamma_k$. Dann gilt für die Länge des Vektors v

   $$||v||_2 = ||x||_2 < 2\gamma_k$$

   und damit $x \in \mathcal{B} \subseteq \mathcal{G} \cup \mathcal{B}$.

2. Sei $x = (v, 0) + a(t, \gamma_k) = (v + at, a\gamma_k) \in L'$ mit $a \in \mathbb{Z}\backslash\{0\}$, $v \in L$ und $||x||_2 = ||(v + at, a\gamma_k)||_2 < 2\gamma_k$
   Für $a \neq \pm 1$, das heißt $a^2 \geq 4$, gilt

   $$||(v + at, a\gamma_k)||_2^2 = \underbrace{||v + at||_2^2}_{>0} + \underbrace{a^2\gamma_k^2}_{\geq 4\gamma_k^2}$$

   und man erhält $||x||_2 > 2\gamma_k$. Das bedeutet, dass $x = (v \pm t, \pm\gamma_k) \in L$ und damit $x \in \mathcal{G} \subseteq \mathcal{G} \cup \mathcal{B}$.

□

Dieses Lemma ist ein wesentlicher Bestandteil der Argumentation, dass man mit Hilfe einer Variante der in Kapitel 3 vorgestellten Samplemethode eine Approximation für den zu t nächsten Gittervektor finden kann. Man sieht am Beweis dieses Lemmas, dass die zweite Komponente ungefähr in der gleichen Größenordnung gewählt werden muss wie D_t. Nur so erreicht man beim obigen Beweis im zweiten Fall den erforderlichen Widerspruch.

Ziel ist es, einen Vektor aus der Menge $\mathcal{G}$ zu erhalten, denn sobald man einen solchen Vektor gefunden hat, ist man in der Lage eine $c(1+\epsilon)^2$-Approximation des zu t nächsten Gittervektors

zu berechnen. Um einen Vektor aus der Menge $\mathcal{G}$ zu ermitteln, kann man eine Variante der in Kapitel 3 vorgestellten Samplemethode verwenden, die von Blömer entwickelt wurde. Diese Variante wird im folgenden Abschnitt vorgestellt. Zunächst wird aber gezeigt, dass man mit Hilfe eines Vektors aus der Menge $\mathcal{G}$ das Problem des nächsten Gittervektors approximativ lösen kann.

Satz 5.2.3 *Sei $(v, w) \in \mathcal{G}$ und $(1+\epsilon)^{k-1} \leq D_t < (1+\epsilon)^k$.*
Dann kann man in polynomieller Zeit einen Gitterpunkt $z^* \in L$ berechnen mit

$$||z^* - t||_2 \leq c(1+\epsilon)^2 D_t$$

Beweis: Ohne Einschränkung sei $w = -\gamma_k$, sonst arbeite man mit $w = -(-\gamma_k)$.
Seien $(v, w) \in \mathcal{G}$. Dann kann (v, w) als Linearkombination der Basisvektoren von $L'(k)$ dargestellt werden:

$$(v, w) = (z^* - t, -\gamma_k) = (z^*, 0) - (t, \gamma_k) \text{ mit } z^* \in L$$

Damit ist $||(v, w)||_2^2 = ||z^* - t||_2^2 + \gamma_k^2$.
Auf Grund der Definition von $\mathcal{G}$ und unter der Voraussetzung $(1+\epsilon)^{k-1} \leq D_t$ gilt:

$$\begin{aligned}
||z^* - t||_2^2 &= ||(v, w)||_2^2 - \gamma_k^2 \\
&< (2\gamma_k)^2 - \gamma_k^2 \\
&= 3\gamma_k^2 \\
&= 3\left(\frac{c}{\sqrt{3}}(1+\epsilon)^{k+1}\right)^2 \\
&= c^2(1+\epsilon)^{2k+2} = c^2(1+\epsilon)^4(1+\epsilon)^{2(k-1)} \\
&\leq c^2(1+\epsilon)^4 D_t^2 \qquad \left(\text{mit } (1+\epsilon)^{k-1} \leq D_t\right) \\
\Longrightarrow ||z^* - t||_2 &\leq c(1+\epsilon)^2 D_t
\end{aligned}$$

Damit ist der Vektor $z^* \in L$ eine $c(1+\epsilon)^2$-Approximation des zu t nächsten Gittervektors.

□

5.3. Samplemethode zur Approximation des Problems des nächsten Gittervektors

In diesem Abschnitt wird eine von Blömer entwickelte Variante der Samplemethode aus Kapitel 3 beschrieben, mit der man einen Vektor aus der auf Seite 45 definierten Menge

$$\mathcal{G} = \{(v, w) \in L'(k) |\ w = \pm\gamma_k, ||(v, w)||_2 < 2\gamma_k\}$$

berechnen kann, wobei $\gamma_k = c \cdot \frac{1}{\sqrt{3}}(1+\epsilon)^{k+1}$. Die Argumentation, dass der Algorithmus wirklich einen Gittervektor aus der Menge $\mathcal{G}$ ausgibt, ist ähnlich wie die bei der Samplemethode zur Lösung von SVP. Man verwendet auch in diesem Fall einen modifizierten Algorithmus, indem man für jeden zufällig gewählten Punkt x der Ursprungsmenge zufällig, unabhängig und gleichverteilt

entscheidet, ob eine bijektive Abbildung τ_u auf den Punkt x angewendet wird. Die Abbildung τ_u ist definiert wie die entsprechende Abbildung auf Seite 19 in Kapitel 3, allerdings ist u in diesem Fall nicht ein kürzester Gittervektor in dem Gitter $L'(k)$, sondern man wählt

$$u := (z - t, -\gamma_k),$$

wobei $z \in L$ der zu t nächste Gittervektor ist:

$$\begin{aligned} \tau_u : B(0,r) &\longrightarrow B(0,r) \\ \tau_u(x) &= \begin{cases} x+u & , x \in C_2 \\ x-u & , x \in C_1 \\ x & , \text{ sonst} \end{cases} \end{aligned}$$

5.3.1. Problematik bei der Verwendung der Samplemethode zur Approximation des nächsten Gittervektors

Im Gegensatz zu der in Kapitel 4 vorgestellten Methode kann man nicht erreichen, dass die Samplemethode den Vektor u in einfach exponentieller Laufzeit ausgibt. Denn um dies mit einer Wahrscheinlichkeit exponentiell nahe an 1 zu erreichen, müssen sich am Ende der Samplemethode in der Menge $\mathcal{Z}$ mehr Paare befinden, als es Gittervektoren der Länge $r = 2\gamma_k$ gibt, damit man eine Kollision finden kann. Eine obere Schranke für die Anzahl Gittervektoren der Länge kleiner als $2\gamma_k$ im Gitter L erhält man durch Lemma 4.2.2 unter Berücksichtigung von $\lambda_1(L) = 1$:

$$\begin{aligned} |B(0, 2\gamma_k) \cap L| &\leq \left(\frac{2 \cdot 2\gamma_k + 1}{1}\right)^n \\ &= (4\gamma_k + 1)^n. \end{aligned}$$

Damit befinden sich im Gitter L und entsprechend auch im Gitter $L'(k)$ ungefähr $(4\gamma_k + 1)^n$ Gitterpunkte, die die Länge kleiner als $2\gamma_k$ haben. Zu Beginn der Samplemethode müssen also in Schritt 1 mindestens $N = (4\gamma_k + 1)^n$ Punkte x zufällig, unabhängig und gleichverteilt gewählt werden, um zu erreichen, dass sich in der Menge $\mathcal{Z}$ nach dem Schleifendurchlauf noch genügend Elemente befinden.

Für den Parameter k gilt nach der in Abschnitt 5.2.2 beschriebenen Reduktion: $k \leq k_1 = 4\log_2 n + 2\log_2 \frac{1}{\epsilon} - 1$ und damit

$$\begin{aligned} 4\gamma_k &= 4c\frac{1}{\sqrt{3}}(1+\epsilon)^k \\ &= \text{poly}(n, \frac{1}{\epsilon}). \end{aligned}$$

Die Laufzeit der Samplemethode ist nach dem Beweis von Satz 3.2.4 polynomiell in N und aus diesem Grund erhält man für

$$N \geq (4\gamma_k + 1)^n = \text{poly}(n, \frac{1}{\epsilon})^n$$

eine Laufzeit, die nicht mehr einfach exponentiell ist. Man kann also die Samplemethode aus Kapitel 3 nicht dazu verwenden, um den Vektor $u = (z - t, -\gamma_k)$ zu berechnen.

Der Unterschied zwischen der Situation in diesem Abschnitt und der Situation in Kapitel 4 bei Verwendung der Samplemethode zur Lösung von SVP ist, dass bei der Berechnung eines Vektors aus der Menge $\mathcal{G}$ der Radius r der Kugel, aus der der entsprechende Vektor gewählt wird, nicht konstant ist.

Allgemein kann man zeigen, dass sich schon durch eine geringe Vergößerung des Radius R einer Kugel $B(0,R)$ die Anzahl von Gitterpunkten in dieser Kugel um einen exponentiellen Faktor erhöhen kann:

Lemma 5.3.1 *Seien $a > b > 0$ konstant, $c = \log_2 \frac{4a}{b} > 0$. Sei L ein n-dimensionales Gitter und $R > 0$. Dann gilt:*

$$|L \cap B(0, aR)| \leq 2^{cn} \, |L \cap B(0, bR)|$$

Beweis: Der Beweis erfolgt mit einer ähnlichen Argumentation wie der Beweis von Lemma 4.2.2.

Die Anzahl disjunkter Kugeln $B(0, \frac{b}{4}R)$, die maximal in der Kugel $B(0, aR)$ liegen können, ist beschränkt durch:

$$\begin{aligned}
\frac{\text{vol}(B(0,aR))}{\text{vol}(B(0,\frac{b}{4}R))} &= \frac{(aR)^n}{(\frac{b}{4}R)^n} \\
&= \left(\frac{4a}{b}\right)^n \\
&= 2^{\log_2(\frac{4a}{b})^n} \\
&= 2^{n \log_2(\frac{4a}{b})} \\
&= 2^{cn}
\end{aligned}$$

Wenn man den Radius der Kugeln $B(0, \frac{b}{4}R)$ verdoppelt, das heißt Kugeln mit Radius $\frac{b}{2}R$ betrachtet, so kann man also mit Hilfe von höchstens 2^{cn} Kugeln vom Radius $\frac{b}{2}R$ eine Überdeckung der Kugel $B(0, aR)$ konstruieren. Damit ist die Anzahl der Gitterpunkte in $B(0, aR)$ höchstens 2^{cn}-mal so groß wie die Anzahl Gitterpunkte in einer beliebigen Kugel dieser Überdeckung mit Radius $\frac{b}{2}R$:

$$|L \cap B(0, aR)| \leq 2^{cn} |L \cap B(y, \frac{b}{2}R)|,$$

wobei $B(y, \frac{b}{2}R)$ eine Kugel der Überdeckung mit maximaler Anzahl Gitterpunkte ist.

Da $0 \in L$ und $0 \in B(0, aR)$, muss $B(y, \frac{b}{2}R)$ mindestens ein Element aus L enthalten, das heißt:

$$L \cap B(0, \frac{b}{2}R) \neq \emptyset.$$

Sei $z \in L$ der nächste Gittervektor von y. Dann gilt:

$$||y - z||_2 < \frac{b}{2}R,$$

denn falls $||y - z||_2 \geq \frac{bR}{2}$, so wäre $L \cap B(y, \frac{bR}{2}) = \emptyset$.

Man betrachte die Abbildung

$$\begin{aligned} \varphi : B(0, aR) &\longrightarrow B(0, aR) \\ x &\longmapsto x - z \end{aligned}$$

Es gelten die folgenden Eigenschaften:

- $\varphi\left(B(y, \frac{b}{2}R)\right) = B(y - z, \frac{b}{2}R)$, denn für $x \in B(y, \frac{b}{2}R)$ ist:

$$||\varphi(x) - (y - z)||_2 = ||x - z - y + z||_2 = ||x - y||_2 < \frac{bR}{2}.$$

- Die Abbildung

$$\varphi_{|B(y, \frac{b}{2}R)} : B(y, \frac{b}{2}R) \longrightarrow B(y - z, \frac{b}{2}R)$$

  ist injektiv. Da $z \in L$ ist, gilt damit

$$\left|L \cap B(y, \frac{b}{2}R)\right| \leq \left|L \cap B(y - z, \frac{b}{2}R)\right|.$$

- Sei $x \in B(y - z, \frac{b}{2}R)$. Da $||y - z||_2 < \frac{b}{2}R$ gilt:

$$||x||_2 \leq ||x - (y - z)||_2 + ||y - z||_2 < \frac{b}{2}R + \frac{b}{2}R = bR.$$

  Damit ist $B(y - z, \frac{b}{2}R) \subseteq B(0, bR)$ und es gilt:

$$\left|L \cap B(y - z, \frac{b}{2}R)\right| \leq |L \cap B(0, bR)|$$

Insgesamt erhält man aus diesen Eigenschaften:

$$|L \cap B(0, aR)| \leq 2^{cn}|L \cap B(y, \frac{b}{2}R)| \leq 2^{cn}|L \cap B(0, bR)|.$$

□

Für $a = \gamma_{k+1} = (1 + \epsilon) \cdot \gamma_k$, $b = \gamma_k$ und $R = 2$ ist

$$c = \log_2 \frac{4a}{b} = \log_2 4(1 + \epsilon) > 2.$$

Damit kann sich also nach Lemma 5.3.1 die Anzahl verschiedener Gitterpunkte in der Menge $B(0, 2\gamma_{k+1})$ um den Faktor 2^{2n} im Vergleich zur Anzahl verschiedener Gitterpunkte in $B(0, 2\gamma_k)$ vergrößern:

$$|L \cap B(0, 2\gamma_{k+1})| \leq 2^{2n} |L \cap B(0, 2\gamma_k)|$$

Das Lemma 5.3.1 zeigt also, dass es grundsätzlich mit Hilfe der Samplemethode nicht möglich ist, in einfach exponentieller Zeit einen festen Gitterpunkt aus einer Kugel mit Radius R zu berechnen, wenn der Radius nicht als konstant vorausgesetzt werden kann. Aus diesem Grund wird die Samplemethode lediglich dazu benutzt, um einen Vektor aus der Menge $\mathcal{G}$ zu berechnen.

5.3.2. Samplemethode zur Berechnung eines Vektors aus der Menge $\mathcal{G}$

Um einen Vektor aus der Menge $\mathcal{G}$ zu berechnen, verwendet man die Samplemethode aus Kapitel 3 mit folgenden Parameterwerten:

- $r = \rho$ und
- $\theta = 2\gamma_k - \rho$

Die Ausgabe der Samplemethode wird dahingehend verändert, dass ein beliebiger Vektor $y_i - x_i \in \mathcal{G}$ aus der Menge $\mathcal{Z}$ ausgegeben wird. Auf Grund der Randomisierung kann man ähnlich wie bei der Anwendung der Samplemethode zur Lösung des Problems des kürzesten Gittervektors argumentieren, dass der Algorithmus mit Wahrscheinlichkeit exponentiell nahe an 1 einen Gitterpunkt aus der Menge $\mathcal{G}$ berechnet.
Man kann die Parameter ρ und a frei wählen und erhält dann einen entsprechenden Approximationsfaktor c. Auf welche Weise dies erfolgen kann, wird in Abschnitt 5.3.4 beschrieben. Hier sind ρ und a so gewählt, dass der Approximationsfaktor $c = 2$ erreicht wird, das heißt man benutzt die Konstante

$$\gamma_k = \frac{2}{\sqrt{3}}(1+\epsilon)^{k+1}.$$

Unter Verwendung der Parameter

- $\rho = \frac{25}{48}\left(\frac{7}{4c}+1\right)\gamma_k = \frac{125}{128}\gamma_k$,
- $a = 2^7$.

erhält man folgenden Algorithmus:

Algorithmus 5.3.2
`Eingabe: Eine Gitterbasis` $B = \{b_1, \ldots, b_n\}$

1. $R_0 \leftarrow n \cdot \max_i ||b_i||_p$
   $N \leftarrow 2^{17n} \log_2 R_0$
2. `Wähle` N `Punkte` $x_1, \ldots, x_N$ `zufällig, gleichverteilt in` $B(0,\rho)$.
   `Berechne` $y_i \equiv x_i \mod \mathcal{L}(B)$ `für` $i = 1, \ldots, N$.
   `Setze` $\mathcal{Z} = \{(x_1, y_1), \ldots, (x_N, y_N)\}$
   $R \leftarrow R_0$
3. `Solange` $R > 2\gamma_k - \rho = \frac{131}{128}\gamma_k$
   a) `Anwendung der Siebprozedur (3.1.2) auf` $\{y_i | (x_i, y_i) \in \mathcal{Z}\}$ `mit den Parametern` $a = 2^7$ `und` R.
   `Man erhält eine Menge` J `und eine Abbildung` η.
   b) `Entferne aus der Menge` $\mathcal{Z}$ `alle Paare` (x_i, y_i) `mit` $i \in J$.
   c) `Ersetze jedes verbleibende Paar` $(x_i, y_i) \in \mathcal{Z}$ `durch` $(x_i, y_i - (y_{\eta(i)} - x_{\eta(i)}))$
   d) $R \leftarrow \frac{R}{128} + \rho$
4. `Betrachte` $(x_i, y_i) \in \mathcal{Z}$.
   `Ausgabe: Ein beliebiger Vektor` $y_i - x_i \in \mathcal{G}$

Die Analyse des Algorithmus ist analog zur Analyse der allgemeinen Samplemethode in Kapitel 3. Die Samplemethode hat also eine Laufzeit von

$$2^{\mathcal{O}(n)}\mathcal{O}(\log_2 R_0)^k.$$

Da man nach Satz 5.1.3 ohne Einschränkung davon ausgehen kann, dass die Basis polynomielle Länge in n und $\frac{1}{\epsilon}$ hat, erhält man eine Gesamtlaufzeit von

$$2^{\mathcal{O}(n)}\mathcal{O}\left(\log_2 n + \log_2 \frac{1}{\epsilon}\right)^k.$$

Mit der Wahl $N = 2^{17n}\log_2 R_0$ und $a = 2^7$ enthält die Ausgabemenge $\mathcal{Z}$ nach Satz 3.2.5 noch mindestens 2^{16n} Paare, wobei die Länge der entsprechenden Gittervektoren $y_i - x_i \in L'(k)$ beschränkt ist durch

$$||y_i - x_i||_p \leq ||y_i||_p + ||x_i||_p < 2\gamma_k - \rho + \rho = 2\gamma_k$$

Damit erhält man in der Ausgabemenge Vektoren aus $L'(k) \cap B(0, 2\gamma_k)$.

5.3.3. Analyse mit Berücksichtigung der Randomisierung

Um zu zeigen, dass sich in der Ausgabemenge mit Wahrscheinlichkeit exponentiell nahe an 1, ein Vektor aus der Menge $\mathcal{G}$ befindet, verwendet man die modifizierte Samplemethode. Sobald sich in der Ausgabemenge mindestens ein Gittervektor aus der Menge $\mathcal{G}$ befindet, wird dieser ausgegeben. Da sich die modifzierte Samplemethode und die ursprüngliche Samplemethode nach Satz 3.3.2 gleich verhalten, gibt damit auch die Samplemethode mit hoher Wahrscheinlichkeit einen Vektor aus der Menge $\mathcal{G}$ aus.

Durch geeignete Wahl des Vektors u kann man mit Hilfe der entsprechenden bijektiven Abbildung $\tau_u : C_1 \to C_2$ zeigen, dass es zu jedem Punkt $y - x \in \mathcal{B}$ mit $x \in C_1 \cup C_2$ einen Punkt aus $\mathcal{G}$ gibt, der von der Samplemethode bei zufälliger, unabhängiger und gleichverteilter Wahl der Menge $x_1, \ldots, x_N \in B(0, \rho)$ mit der gleichen Wahrscheinlichkeit ausgegeben wird und umgekehrt.

Man betrachte den Gittervektor $u = (z - t, -\gamma_k) \in L'(k)$, wobei $z \in L$ der zu t nächste Gittervektor ist, sowie die auf Seite 19 definierten Mengen C_1 und C_2 mit dem Parameter $r = \rho = \frac{125}{128}\gamma_k$. Für die Länge von u gilt folgende Abschätzung:

$$\begin{aligned}
||u||_p &= ||(z - t, -\gamma_k)||_p \\
&= ||(z - t, 0) + (0, -\gamma_k)||_p \\
&\leq ||z - t||_p + \gamma_k \\
&< (1 + \epsilon)^k + \gamma_k \\
&= \frac{1}{2}\sqrt{3}\frac{1}{1+\epsilon}\gamma_k + \gamma_k \\
&\leq \frac{1}{2} \cdot \frac{7}{4}\gamma_k + \gamma_k \\
&= \frac{15}{8}\gamma_k
\end{aligned}$$

Auf Grund der Länge von u schneiden sich die Kugeln $B(u,\rho)$ und $B(-u,\rho)$ nicht, falls ϵ genügend klein ist. Damit sind auch die Mengen C_1 und C_2 disjunkt:

$$\begin{aligned} & ||u||_2 = ||z-x||_2 + \gamma_k \geq (1+\epsilon)^{k-1} + \gamma_k \geq \rho \\ \iff & \frac{1}{2}\frac{\sqrt{3}}{(1+\epsilon)^2}\gamma_k + \gamma_k \geq \frac{125}{128}\gamma_k \\ \iff & \left(\frac{1}{2}\sqrt{3}+1\right)\frac{128}{125} \geq (1+\epsilon)^2 \\ \overset{\epsilon>0}{\iff} & \epsilon \leq \sqrt{\left(\frac{1}{2}\sqrt{3}+1\right)\frac{125}{128}} - 1 \doteq 0,40 \end{aligned}$$

Bei Verwendung der p-Norm erhält man an dieser Stelle eine (etwas) technischere Abschätzung.

Mit den so gewählten Parametern erhält man folgende modifzierte Samplemethode:

Algorithmus 5.3.3 Modifizierte Samplemethode
Eingabe: Eine Gitterbasis $B = \{b_1, \ldots, b_n\}$

1. $R_0 \leftarrow n \cdot \max_i ||b_i||_p$
   $N \leftarrow 2^{17n} \log_2 R_0$
   Wähle N Punkte $x_1, \ldots, x_N$ zufällig, gleichverteilt in $B(0,\rho)$.
   Berechne $y_i \equiv x_i \mod \mathcal{L}(B)$ für $i = 1, \ldots, N$.
   Setze $\mathcal{Z} = \{(x_1, y_1), \ldots, (x_N, y_N)\}$.
   $R \leftarrow R_0$
2. Solange $R > 2\gamma - \rho = \frac{131}{128}\gamma$
   a) Anwendung der Siebprozedur 3.1.2 auf $\{y_i | (x_i, y_i) \in \mathcal{Z}\}$ mit den Parametern R und $a = 2^7$.
   Man erhält eine Menge J und eine Abbildung η.
   b) Entscheide für jedes $(x_i, y_i) \in J$ zufällig, unabhängig, gleichverteilt, ob x_i durch $\tau_v(x_i)$ ersetzt wird.
   c) Entferne aus der Menge $\mathcal{Z}$ alle Paare (x_i, y_i) mit $i \in J$.
   d) Ersetze jedes verbleibende Paar $(x_i, y_i) \in \mathcal{Z}$ durch $(x_i, y_i - (y_{\eta(i)} - x_{\eta(i)}))$.
   e) $R \leftarrow \frac{R}{128} + \rho$
3. Entscheide für jedes verbleibende Paar $(x_i, y_i) \in \mathcal{Z}$ zufällig, unabhängig, gleichverteilt, ob x_i durch $\tau_u(x_i)$ ersetzt wird.
4. Betrachte $(x_i, y_i) \in \mathcal{Z}$.

Ausgabe: Ein beliebiger Vektor $y_i - x_i \in \mathcal{G}$

Unter Verwendung von Lemma 3.3.3 kann gezeigt werden, mit welcher Wahrscheinlichkeit ein Punkt x, der zufällig, unabhängig und gleichverteilt aus $B(0,\rho)$ gewählt wird, in der Menge

$C_1 \cup C_2$ enthalten ist. Die Länge des Vektor u ist nach der Abschätzung auf Seite 51 kleiner als $\frac{15}{8}\gamma_k$. Mit $r = \rho = \frac{125}{128}\gamma_k$ ist $||u||_p \leq \frac{48}{25}\rho$. Mit $l = \frac{48}{25}$ ist nach Lemma 3.3.3

$$\begin{aligned} k &= 2^{\lfloor \log_2 \frac{2-l}{l} \rfloor} \\ &= 2^{\lfloor \log_2 \frac{1}{24} \rfloor} \\ &= 2^{-5} \end{aligned}$$

und damit gilt:

$$\begin{aligned} \frac{\text{vol}(C_1)}{\text{vol}(B(0,\rho))} = \frac{\text{vol}(C_2)}{\text{vol}(B(0,\rho))} &\geq k(2-k-l)^{n-1}2^{-n} \\ &= 2^{-5}(\frac{39}{800})^{n-1}2^{-n} \\ &> 2^{-5}2^{-5(n-1)}2^{-n} \\ &= 2^{-6n}. \end{aligned}$$

Damit ist die Wahrscheinlichkeit p, dass für $i \in \{1, \ldots, N\}$ ein Punkt x_i, der zufällig, unabhängig und gleichverteilt aus $B(0,\rho)$ gewählt wird, in $C_1 \cup C_2$ enthalten ist, größer als 2^{-6n}. Nach Lemma 3.3.4 mit $p = 2^{-6n}$ und $N = 2^{17n} \log_2 R_0$ befinden sich damit mit Wahrscheinlichkeit exponentiell nahe an 1 mindestens

$$\frac{p \cdot N}{2} = 2^{11n-1} \log_2 R_0$$

Punkte aus $C_1 \cup C_2$ in der Menge der zu Beginn des Algorithmus ausgewählten Punkte $x_1, \ldots, x_N \in B(0,\rho)$ und damit in der Menge $\mathcal{Z}$. Da die Methode nach Lemma 3.2.3 höchstens $2 \cdot 7 \cdot \log_2 R_0$ Iterationen durchläuft, werden während der Schleife höchstens $2 \cdot 7(2^8+1)^n \log_2 R_0$ Paare aus der Menge $\mathcal{Z}$ entfernt werden. Nach der Schleife befinden sich also noch mindestens

$$\begin{aligned} & \frac{p \cdot N}{2} - 2 \cdot 7 \cdot (2^8+1)^n \log_2 R_0 \\ > \; & (2^{11n-1} - 2^4 \cdot 2^{9n}) \log_2 R_0 \\ = \; & 2^n(2^{10n-1} - 2^{8n+4}) \log_2 R_0 \\ > \; & 2^n \end{aligned}$$

Paare (x,y) in der Menge $\mathcal{Z}$, für die gilt $x \in C_1 \cup C_2$. Damit hat man mit Wahrscheinlichkeit exponentiell nahe an 1 mindestens 2^n Gittervektoren $w = y - x$ mit der Eigenschaft $x \in C_1 \cup C_2$ und für jedes dieser Paare gilt $y - x \in B(0, 2\gamma_k)$.

Satz 5.3.4 *Die modifizierte Samplemethode berechnet mit Wahrscheinlichkeit exponentiell nahe an 1 einen Vektor aus der Menge $\mathcal{G}$.*

Beweis: In der Menge $\mathcal{Z}$ befinden sich mit hoher Wahrscheinlichkeit 2^n Paare (x,y), die von der Abbildung τ_u nicht auf sich selbst abgebildet werden. Nach Lemma 5.2.2 ist $\mathcal{G} \bigcup \mathcal{B} = B(0, 2\gamma_k)$ und damit gilt für jedes Paar $(x,y) \in \mathcal{Z}$ entweder $y - x \in \mathcal{G}$ oder $y - x \in \mathcal{B}$.
Es wird zunächst gezeigt, dass die Abbildung τ_u folgende Eigenschaften hat:

$$\begin{aligned} \tau_{u|B(0,2\gamma_k)\setminus(C_1 \cup C_2)} &= \text{id}_{B(0,2\gamma_k)\setminus(C_1 \cup C_2)} \\ \tau_{u|C_1 \cup C_2}(\mathcal{B}) &= \mathcal{G} \\ \tau_{u|C_1 \cup C_2}(\mathcal{G}) &= \mathcal{B} \end{aligned}$$

Sei $v = y - x \in L$ mit $x \in C_1 \cup C_2$.

- Sei $v \in \mathcal{B}$. Dann ist $v = (w, 0)$ mit $w \in L$ und

$$\tau_u(v) = (w, 0) \pm (t, \gamma_k) \in \mathcal{G}.$$

- Sei $v \in \mathcal{G}$. Dann ist $v = (w, 0) \pm (t, \gamma_k)$ mit $w \in L$. Sei $v = (w, 0) + (t, \gamma_k)$.
  Annahme: $x \in C_2$. Daraus folgt:

$$\tau_u(v) = (w, 0) + 2(t, \gamma_k) \notin \mathcal{G} \cup \mathcal{B} = B(0, 2\gamma_k).$$

  Also muss gelten: $x \in C_1$ und damit $\tau_u(v) = (w, 0) \in \mathcal{B}$.
  Analog sieht man, dass für $v = (w, 0) - (t, \gamma_k)$ gilt: $\tau_u(v) \in \mathcal{B}$.

Damit ist in der Ausgabemenge genau dann mindestens ein Punkt aus $\mathcal{G}$ enthalten, wenn ein Paar $(x, y) \in \mathcal{Z}$ mit $x \in C_1 \cup C_2$ existiert, für das eine der beiden folgenden Eigenschaften gilt:

- $y - x \in \mathcal{B}$ und die Abbildung τ_u wird angewendet,
- $y - x \in \mathcal{G}$ und die Abbildung τ_u wird nicht angewendet.

In Schritt 3 der modifizierten Samplemethode wird für jedes Paar $(x, y) \in \mathcal{Z}$ zufällig, unabhängig und gleichverteilt entschieden, ob τ_u angewendet wird. Da sich in der Menge $\mathcal{Z}$ mit Wahrscheinlichkeit exponentiell nahe an 1 mindestens 2^n Paare (x, y) mit der Eigenschaft $x \in C_1 \cup C_2$ befinden, ist die Wahrscheinlichkeit, dass kein Gittervektor aus $\mathcal{G}$ ausgegeben wird, kleiner als

$$2^{-2^n}$$

Also ist der Algorithmus mit einer Wahrscheinlichkeit größer als

$$1 - 2^{-2^n}$$

erfolgreich und ein Vektor aus der Menge $\mathcal{G}$ wird ausgegeben.

□

Da nach Satz 3.3.2 die Samplemethode und die modifizierte Samplemethode das gleiche Ausgabeverhalten haben, gilt:

Satz 5.3.5 *Die Samplemethode berechnet mit Laufzeit* $2^{\mathcal{O}(n)} \operatorname{poly}(\log_2 R_0)$ *mit Wahrscheinlichkeit exponentiell nahe an 1 einen Vektor aus der Menge* $\mathcal{G}$*, wobei* $R_0 = n \max_k ||b_k||_p$ *die Eingabegröße ist.*

Wenn man mit einer Genauigkeit von $n^7 \log_2 R_0$ rechnet, ist die Diskretisierung der Kugel $B(0, \rho)$ ausreichend fein, so dass jeweils mindestens ein Punkt aus der Menge C_1 beziehungsweise C_2 existiert, denn

$$\begin{aligned} \frac{1}{64}\gamma_k &= \frac{1}{63}\frac{2}{\sqrt{3}}(1+\epsilon)^{k+1} \\ &> 2^{-6} \cdot 2 \cdot 2^{-1} \cdot 2^{-1} \\ &= 2^{-7} \end{aligned}$$

5.3.4. Wahl der Parameter

Die oben beschriebenen Parameter a, c und ρ sind frei wählbar. Ziel ist es, den Approximationsfaktor c möglichst klein zu wählen. Damit der Algorithmus korrekt arbeitet, müssen aber folgende Bedingungen erfüllt sein:

- Der Radius ρ der Kugel, aus der die Punkte $x_1, \ldots, x_N$ zufällig, unabhängig und gleichverteilt gewählt werden, muss so groß sein, dass sich $B(0, \rho)$ und $B(u, \rho)$ beziehungsweise $B(0, \rho)$ und $B(-u, \rho)$ schneiden.
- Da $||u||_2 \leq \left(\frac{\sqrt{3}}{c} + 1\right) \gamma_k$, muss $\rho > \frac{1}{2}\left(\frac{\sqrt{3}}{c} + 1\right) \gamma_k$ gewählt werden.
- ρ muss kleiner als $2\gamma_k$ sein, da man nur Vektoren mit einer Länge kleiner als $2\gamma_k$ sucht.

Je größer ρ gewählt wird, desto mehr Iterationen werden benötigt und dementsprechend viele Punkte müssen zu Beginn gewählt werden, da sich die Punktemenge $\mathcal{Z}$ in jedem Iterationsschritt im schlimmsten Fall um $(2a+1)^n$ Punkte verkleinert.
Damit der Algorithmus nur Gittervektoren der Länge kleiner als $2\gamma_k$ ausgibt, muss die Siebprozedur so oft angewendet werden, bis

$$\frac{R_0}{a^i} + \rho \sum_{j=0}^{i-1} a^{-j} < 2\gamma_k - \rho$$

beziehungsweise nach Abschätzung durch die geometrische Reihe

$$\underbrace{\frac{R_0}{a^i}}_{=:\delta} + \frac{a}{a-1}\rho + \rho < 2\gamma_k.$$

Mit $\delta < \frac{1}{\kappa}\gamma_k$ mit $\kappa \in \mathbb{N}$ und unter Verwendung der unteren Schranke für ρ erhält man:

$$\begin{aligned}
& \delta + \frac{a}{a-1}\rho + \rho < 2\gamma_k \\
\Longleftarrow \quad & \frac{1}{\kappa}\gamma_k + \frac{2a-1}{a-1} \cdot \frac{1}{2}\left(\frac{\sqrt{3}}{c} + 1\right)\gamma_k < 2\gamma_k \\
\Longleftrightarrow \quad & \frac{2a-1}{a-1} \cdot \frac{\sqrt{3}}{2c} < 2 - \frac{2a-1}{2(a-1)} - \frac{1}{\kappa} = \frac{4k(a-1) - \kappa(2a-1) - 2(a-1)}{2\kappa(a-1)} \\
\Longleftrightarrow \quad & c > \frac{2\kappa(a-1)}{4k(a-1) - \kappa(2a-1) - 2(a-1)} \cdot \frac{2a-1}{a-1} \cdot \frac{\sqrt{3}}{2} \\
\Longleftrightarrow \quad & c > \frac{\sqrt{3}\kappa(2a-1)}{4k(a-1) - \kappa(2a-1) - 2(a-1)}
\end{aligned}$$

Dafür muss gelten, dass

$$\begin{aligned}
& \frac{4\kappa(a-1) - \kappa(2a-1) - 2(a-1)}{2\kappa(a-1)} > 0 \\
\Longleftrightarrow \quad & 4\kappa(a-1) - \kappa(2a-1) - 2(a-1) > 0, \quad \text{da } a > 2 \\
\Longleftrightarrow \quad & \kappa(2a-3) > 2(a-1) \\
\Longleftrightarrow \quad & \kappa > \underbrace{\frac{2(a-1)}{2a-3}}_{<1}
\end{aligned}$$

Diese Bedingung ist für $\kappa \in \mathbb{N}$ immer erfüllt.
Damit kann man maximal den Approximationsfaktor

$$\begin{aligned} c &> \lim_{(\kappa,a)\to\infty} \frac{\sqrt{3}\kappa(2a-1)}{4\kappa(a-1)-\kappa(2a-1)-2(a-1)} \\ &= \lim_{(\kappa,a)\to\infty} \frac{\sqrt{3}(2-\frac{1}{a})}{4(1-\frac{1}{a})-(2-\frac{1}{a})-2(\frac{1}{\kappa}-\frac{1}{a\kappa})} \\ &= \sqrt{3} < 2 \end{aligned}$$

erreichen. Die untere Schranke kann wegen der scharfen Ungleichung nicht genau erreicht werden, für $\kappa = a \approx 2^{32}$ erreicht man aber bei Rechnung mit 10-stelliger Genauigkeit $c > \sqrt{3}$.

5.4. Algorithmus zur $2(1+\epsilon)^2$-Approximation des Problems des nächsten Gittervektors

In diesem Abschnitt sollen die bisher in diesem Kapitel entwickelten Resultate zu einem Algorithmus zur Approximation des Problems des nächsten Gittervektors zusammengefasst werden. Gegeben sei ein Algorithmus $\mathcal{A}$, der das Problem des kürzesten Gittervektors exakt löst. Der folgende Algorithmus berechnet unter Verwendung von $\mathcal{A}$ für jedes beliebige Gitter L und $t \in \text{span}(L)$ eine $2(1+\epsilon)^2$-Approximation des zu t nächsten Gittervektors. Man kann für $\mathcal{A}$ den in Kapitel 4 beschriebenen Algorithmus verwenden.

Die Korrektheit des Algorithmus ergibt sich aus den Resultaten in den bisherigen Abschnitten. In Klammern ist jeweils angegeben, auf welchem Ergebnis der jeweilige Schritt beruht. Zur Erhaltung der Übersichtlichkeit wird im Folgenden auf die exakte Darstellung verzichtet. Sie ist jeweils in den entsprechenden Abschnitten nachzulesen.

Algorithmus 5.4.1 Algorithmus zur Berechnung des nächsten Gittervektors in $\mathcal{L}(B')$
Gegeben: Gitterbasis B' des Gitters L' und $t' \in \text{span}(L')$

1. Berechne mit Hilfe von $\mathcal{A}$ einen kürzesten von 0 verschiedenen Vektor $u' \in L'$.
   Dann ist $\lambda_1(L') = ||u'||_2$.
   Definiere das Gitter $L = \mathcal{L}(B)$ mit

$$B = \{\frac{1}{\lambda_1(L')}b'_1, \ldots, \frac{1}{\lambda_1(L')}b'_n\}.$$

   Setze $t := \frac{1}{\lambda_1(L)} \cdot t \in \text{span}(L')$.

2. Löse CVP für das Gitter L und den Vektor t:

   a) (5.1.2)

   - Berechne mit dem Algorithmus $\mathcal{A}$ einen kürzesten von 0 verschiedenen Gittervektor $u \in L$.
   - Betrachte die Projektion $\hat{L}$ von L orthogonal zu u sowie die Projektion $\hat{t}$ von t in $\text{span}(L)$.
   - Löse CVP rekursiv für das Gitter $\hat{L}$ und $\hat{t}$.

- Lifte die Lösung $\hat{z}^* \in \hat{L}$ zu einer möglichen Lösung $z_1^{(n)} \in L$.

b) Falls L keine Basis der Länge $\mathrm{poly}(n, \frac{1}{\epsilon})$ hat:

- (5.1.3)
  - Berechne mit $\mathcal{A}$ einen kürzesten von 0 verschiedenen Gittervektor $u^* \in L^*$ im dualen Gitter L^*.
  - Betrachte das Untergitter H von L orthogonal zu u sowie die Hyperebene H_i von H die zu t den minimalen Abstand hat.
  - Sei t^* die Projektion von t in $\mathrm{span}(H_i)$
  - Löse CVP rekursiv für H_i und t^*.
  - Lifte die Lösung $z^* \in H_i$ zu einer möglichen Lösung $z_2^{(n)} \in L$.

sonst

- i. (5.2.1)
  - Berechne mit dem Algorithmus $\mathcal{A}$ einen kürzesten von 0 verschiedenen Gittervektor $\tilde{u} \in \tilde{L}$, wobei $\tilde{L}$ das Gitter ist, das durch $\{(v,0)|v \in L\} \cup \{(t, \frac{1}{2})\}$ erzeugt wird.
  - $\tilde{u} = (\tilde{z}, 0) \pm (t, \frac{1}{2})$ mit $\tilde{z} \in L$
    Mögliche Lösung: $z_3^{(n)} := \tilde{z}$

ii. (5.2.3)
Für $k = -\frac{1}{\log_2(1+\epsilon)}, \ldots, 4\log_2 n - 2\log_2 \epsilon - 1$
  - Setze $\mathcal{G} := \{(v,w) \in L'(k) | w = \pm\gamma_k,\ ||(v,w)||_2 < 2\gamma_k\}$.
  - Berechne mit Hilfe der Samplemethode 5.3.2 einen Vektor $(v,w) \in \mathcal{G}$.
  - $(v,w) = (\check{z}, 0) \pm (t, \gamma_k)$
    Mögliche Lösung: $z_k^{(n)} := \check{z}$

c) $z := \min\{z_1^{(n)}, z_2^{(n)}, z_3^{(n)}, z_4^{(n)}\} \cup \{z_k^{(n)} | k = -\frac{1}{\log_2(1+\epsilon)}, \ldots, 4\log_2 n - 2\log_2 \epsilon - 1\}$, soweit berechnet.

Ausgabe: $z' = \lambda_1(L')z \in L'$

Der Algorithmus verwendet zur Berechnung einer $2(1+\epsilon)^2$-Approximation in den Schritten 2a und 2b zwei einstufige lineare Rekursionen sowie zweimal den Algorithmus $\mathcal{A}$. Die Laufzeit von Schritt 2(b)i ist im Wesentlichen die Laufzeit des Algorithmus $\mathcal{A}$. Eine Darstellung durch die Basisvektoren ist in Zeit polynomiell in der Eingabegröße $\log_2 R_0$ möglich. Die Samplemethode zur Berechnung eines Gitterpunktes aus der Menge $\mathcal{G}$ in Schritt 2(b)ii hat nach Satz 5.3.5 eine Laufzeit von $2^{\mathcal{O}(n)}\,\mathrm{poly}(\log_2 R_0)$ mit $R_0 = n \cdot \max_k ||b_k||_p$.

Wenn man davon ausgeht, dass der Algorithmus $\mathcal{A}$ zur Lösung des Problems des kürzesten Gittervektors eine Laufzeit von $2^{\mathcal{O}(n)}\,\mathrm{poly}(\log_2 R_0)$ hat, so hat der Algorithmus zur Approximation des Problems des nächsten Gittervektors für ein Gitter vom Rang n die Laufzeit

$$\begin{aligned} & 2T(n-1) + 5 \cdot 2^{\mathcal{O}(n)}\,\mathrm{poly}(\log_2 R_0) \\ = \;& 4T(n-2) + 3 \cdot 5 \cdot 2^{\mathcal{O}(n)}\,\mathrm{poly}(\log_2 R_0) \\ = \;& 2^{\mathcal{O}(n)}\,\mathrm{poly}(\log_2 R_0), \end{aligned}$$

wobei $T(n-1)$ die Laufzeit des Algorithmus für ein Gitter vom Rang $n-1$ ist.

Insgesamt gilt:

Satz 5.4.2 *Unter der Verwendung eines Algorithmus $\mathcal{A}$ zur Lösung des Problems des kürzesten Gittervektors mit einer Laufzeit $2^{\mathcal{O}(n)}\,\mathrm{poly}(\log_2 R_0)$, wobei $\log_2 R_0$ die Eingabegröße ist, gilt: Gegeben sei ein Gitter L vom Rang n und ein Vektor $t \in \mathrm{span}(L)$. Dann kann man mit Wahrscheinlichkeit exponentiell nahe an 1 eine $2(1+\epsilon)^2$-Approximation des zu t nächsten Gittervektors berechnen, wobei $\epsilon > 0$. Die Laufzeit des randomisierten Algorithmus beträgt $2^{\mathcal{O}(n)}\,\mathrm{poly}(\log_2 R_0)$, wobei $R_0 = n \max_k ||b_k||_2$ mit $L = \mathcal{L}(B)$ die Eingabegröße ist.*

5.5. Vorschlag einer Samplemethode von Ajtai, Kumar, Sivakumar

Im Jahr 2001 haben Ajtai, Kumar und Sivakumar einen einfach exponentiellen Algorithmus zur Berechnung des kürzesten Gittervektors beschrieben [2]. Im Jahr 2002 schlugen sie eine $2^{\mathcal{O}(n)}$-Turingreduktion vom Problem des nächsten Gittervektors auf das Problem des kürzesten Gittervektors vor, die unter anderem eine Variante ihrer in [2] vorgeschlagenen Samplemethode benutzen sollte, siehe [3]. Bei Untersuchung dieser vorgeschlagenen Variante im Rahmen dieser Diplomarbeit ist es nicht gelungen, diese Samplemethode, die zur $(1+\epsilon)$-Approximation des nächsten Gittervektors benötigt wird, konkret zu entwickeln. Im Folgenden sollen nun zunächst die in [2] vorgeschlagene Samplemethode und anschließend die bei der Modifikation aufgetretenen Probleme beschrieben werden.

5.5.1. Samplemethode von Ajtai, Kumar, Sivakumar

Die Samplemethode von Ajtai, Kumar und Sivakumar wählt zur Berechnung des kürzesten Gittervektors $N = 2^{\mathcal{O}(n)}$ zufällige Gitterpunkte aus einem genügend großen Parallelepiped $\mathcal{P}$. Dabei ist jeder gewählte Gitterpunkt x_r mit $r \in \{1, \ldots, N\}$ von der Form

$$x_r = y_r + z_r,$$

wobei z_r ein Gitterpunkt ist, der gleichverteilt aus $\mathcal{P} \cap L$ gewählt wird, und $y_r \in \mathbb{R}^n$ ein normalverteilter sogenannter Störungsvektor mit Standardabweichung $\frac{1}{\sqrt{Kn}}$ ist.

Wesentlich für die Funktionsweise der Samplemethode zur Berechnung eines kürzesten Gittervektors ist, dass für jedes c' eine Konstante K existiert, so dass mit hoher Wahrscheinlichkeit

$$||y_r||_2 \leq c'$$

gilt [[2], Lemma 6]. Für die Samplemethode zur Lösung von SVP verwendet man $c' = 2$.
Mit Hilfe einer probabilistischen Methode [[2], Lemma 11] kann man iterativ eine Teilmenge $T \subseteq \{1, \ldots, N\}$ konstruieren, so dass für jedes $r \in T$ ein Gittervektor $b_r \in L$ existiert mit

$$||x_r - b_r||_2 \leq 6.$$

Dann hat der Vektor $w_r := z_r - b_r \in L$ höchstens die Länge

$$||w_r||_2 \leq ||z_r - b_r||_2 \leq ||x_r - b_r||_2 + ||y_r||_2 \leq 6 + 2 = 8$$

und damit hat man eine konstante Approximation eines kürzesten Gittervektors in L.

Für einen Gittervektor $v \in L$, sei p_v die Wahrscheinlichkeit über alle zufälligen Wahlen des Algorithmus, dass der Algorithmus den Gittervektor v ausgibt. Man kann zeigen, dass mit hoher Wahrscheinlichkeit mindestens ein Gittervektor $v \in L$ mit einer Wahrscheinlichkeit größer als 2^{-cn} mit $c \in \mathbb{N}$ konstant ausgegeben wird. Falls $u \in L$ ein kürzester Gittervektor ist, so kann man zeigen [[2], Lemma 13], dass die Wahrscheinlichkeit, dass der Gittervektor $v \pm u$ vom Algorithmus ausgegeben wird, 2^{-3Kn} mal der Wahrscheinlichkeit ist, dass der Gittervektor v ausgegeben wird:

$$p_{v \pm u} \geq 2^{-3Kn} p_v$$

Wenn man also die Samplemethode genügend oft – maximal $2^{\mathcal{O}(n)}$-mal – wiederholt, so berechnet die Samplemethode mit großer Wahrscheinlichkeit mindestens einmal den Vektor v und einmal den Vektor $v \pm u$. Analog zur in Kapitel 4 vorgestellten Samplemethode zur Lösung des Problems des kürzesten Gittervektors erhält man dann mit hoher Wahrscheinlichkeit einen von 0 verschiedenen kürzesten Gittervektor in L, wenn man die Menge aller möglichen Differenzen von Ausgaben der Samplemethode betrachtet.

Wichtiges Charakteristikum dieser Methode ist, dass die Konstante K so bestimmt wird, dass mit hoher Wahrscheinlichkeit die Länge des Störungsvektors y_r kleiner als eine vorgegebene Konstante c' ist. Hierbei hat die Konstante K wesentlichen Einfluß darauf, in welchem Verhältnis die Ausgabewahrscheinlichkeit von v zur Ausgabewahrscheinlichkeit von $v \pm u$ für einen Gittervektor u steht.

5.5.2. Vorgeschlagene Methode zur Approximation des Problems des nächsten Gittervektors

Die Turingreduktion vom Problem des nächsten Gittervektors auf das Problem des kürzesten Gittervektors, die Ajtai, Kumar und Sivakumar in [3] vorschlagen, entspricht im wesentlichen der in den Abschnitten 5.1 und 5.2 vorgestellten $2(1+\epsilon)^2$ Reduktion.

Ajtai, Kumar und Sivakumar setzen allerdings voraus, dass ein Algorithmus mit einfach exponentieller Laufzeit existiert, der einen Gittervektor aus $L \cap B(0, R)$ findet, wobei $R \leq 2\frac{1}{\sqrt{3}}(1+\epsilon)^{4\log_2 n + 2\frac{1}{\epsilon}} = \text{poly}(n)$. Dieser Algorithmus muss folgende Eigenschaft haben: Falls ein Vektor v mit Wahrscheinlichkeit p_v ausgewählt wird, dann ist $\max\{\frac{p_x}{p_y} | x, y \in L \cap B(0, R)\} \leq 2^{cn}$ für eine Konstante $c(\epsilon) > 0$, dass heißt für zwei beliebige Vektoren $x, y \in L \cap B(0, R)$ ist $p_y \geq 2^{-cn} p_x$.
Der in [2] vorgestellte Algorithmus berechnet Gitterpunkte aus einer Kugel mit konstantem Radius mit der Uniformitätseigenschaft, dass $\max\{\frac{p_x}{p_y} | x, y \in L \cap B(0, 8)\} \leq 2^{cn}$ für eine Konstante $c(\epsilon) > 0$. Für die Reduktion wird aber ein Algorithmus benötigt, der Gitterpunkte aus der Kugel

$B(0,R)$ mit $R = \text{poly}(n)$ berechnet. Um dies zu erreichen, wird von Ajtai, Kumar und Sivakumar vorgeschlagen, die Störungsvektoren y normalverteilt mit der Standardabweichung $\frac{R}{\sqrt{Kn}}$ zu wählen, anstatt mit der Standarabweichung $\frac{1}{\sqrt{Kn}}$ wie bei der Samplemethode zur Lösung des Problems des kürzesten Gittervektors.

Folgt man der Argumentationsstruktur von Ajtai, Kumar und Sivakumar in [2], so erhält man mit dieser Wahl der Standardabweichung folgendes Lemma:

Lemma 5.5.1 ([3], Lemma 21) *Falls $\xi_i, i = 1, \ldots, n$ unabhängig normalverteilte Zufallsvariablen sind mit Erwartungswert 0 und Varianz $\frac{R^2}{Kn}$, dann gilt für jede beliebige Konstante $C > 1$:*

$$Pr\left[\sum_{j=1}^{n} \xi_j^2 > C\right] \leq \exp\left(-n\left(\frac{K}{4R^2} - \frac{1}{2C}\right)\right).$$

Mit Hilfe dieses Lemmas kann gezeigt werden, dass die Länge des Störungsvektors kleiner als eine vorgegebene Konstante ist. Mit dem folgenden Lemma wird die Größe der Konstante K festgelegt, mit der die Samplemethode durchgeführt werden soll. Dabei ist $c_1 \in \mathbb{N}$ gegeben mit $N = 2^{c_1 n}$.

Lemma 5.5.2 ([3], Lemma 6) *Für jedes $c' > 1$ und $C' > 0$, existiert eine Konstante $K > 0$, so dass bei Ausführung der Sampleprozedur mit diesem K, mit Wahrscheinlichkeit mindestens $1 - 2^{-C'n}$ folgendes gilt:*

$$||y_i||_2 \leq c' \text{ für alle } i \in \{1, \ldots, N = 2^{c_1 n}\}.$$

Beweis: Sei $i \in \{1, \ldots, N\}$ beliebig, aber fest. Dann gilt mit Lemma 5.5.1:

$$\begin{aligned} Pr\left[||y_i||_2 > c'\right] &= Pr\left[||y_i||_2^2 > c'^2\right] \\ &< \exp\left(-n\left(\frac{K}{4R^2} - \frac{1}{2c'^2}\right)\right) \\ &< \exp\left(-n\left(C' + c_1\right)\right) \end{aligned}$$

für K genügend groß.
Damit ist die Wahrscheinlichkeit, dass ein $i \in \{1, \ldots, N\}$ mit $||y_i||_2 > c'$ existiert

$$< N \cdot 2^{-(C'+c_1)n} = 2^{c_1 n} 2^{-(C'+c_1)n} = 2^{-C'n}$$

und damit gilt mit Wahrscheinlichkeit $\geq 1 - 2^{-C'n}$ für alle $i \in \{1, \ldots, N\}$: $||y_i||_2 < c'$.

□

Das Problem in diesem Beweis ist, dass $R = \text{poly}(n)$. Damit gilt:

$$\exp\left(-n\left(\frac{K}{4R^2} - \frac{1}{2c'^2}\right)\right) \to 1 \text{ für } n \to \infty$$

falls K konstant gewählt werden sollte. In diesem Fall wäre die Wahrscheinlichkeit, dass die Länge aller Störungsvektoren kleiner als eine Konstante ist, fast 0. Um dies zu verhindern, muss also K so gewählt werden, dass $\frac{K}{4R^2} - \frac{1}{2c'^2} > C' + c_1$, das heißt es muss im Wesentlichen gelten:

$$K \geq R^2$$

Damit wäre K allerdings keine Konstante und für $R = \text{poly}(n)$ polynomiell. Dies würde auch bedeuten, dass man als Uniformitätsbedingung analog zu [2]

$$p_{v \pm u} \geq 2^{-3Kn} p_v = 2^{-\text{poly}(n)} p_v$$

erhalten würde, für einen Vektor $v \in L \cap B(0, R)$ mit $p_v \geq 2^{-cn}$. Der Vektor u muss in diesem Fall nicht der kürzeste Gittervektor sein, sondern kann ein beliebiger Gittervektor der Länge höchstens R sein. In diesem Fall kann also nur gezeigt werden, dass

$$\max\{\frac{p_x}{p_y} | x, y \in L \cap B(0, R)\} \leq 2^{\text{poly}(n)}.$$

Um dann zu garantieren, dass die Samplemethode mit hoher Wahrscheinlichkeit mindestens einmal den Vektor v und einmal den Vektor $v + u$ ausgibt, muss die Samplemethode $2^{\text{poly}(n)}$-mal wiederholt werden, was zu einer Laufzeit führt, die nicht mehr einfach exponentiell ist.

Das Problem bei der Übertragung der Samplemethode ist also prinzipiell das gleiche wie das in Abschnitt 5.3.1 beschriebene Problem bei der Übertragung der Samplemethode aus Kapitel 3: Man muss eine Kollision in einer Menge finden, in der mehr als einfach exponentiell viele Elemente enthalten sind.

6. Zusammenfassung und Ausblick

In dieser Arbeit wurde eine randomisierte Samplemethode vorgestellt, mit deren Hilfe man einen Gittervektor aus einer Kugel mit konstantem Radius berechnen kann. Wesentliche Charakteristik dieser Samplemethode ist die Möglichkeit, sie so zu modifizieren, dass das Ausgabeverhalten nicht beeinflusst wird, man aber in der Modifikation bereits die gesuchte Lösung verwenden kann. Auf diese Weise ist es möglich, für die modifizierte Samplemethode gewisse Unformitätsbedingungen im Ausgabeverhalten zu zeigen. Da die Modifikation ohne Beeinträchtigung des Ausgabeverhaltens erfolgt, gelten diese Uniformitätsbedingungen dann auch für die ursprüngliche Samplemethode.

Auf diese Weise ist es dann gelungen zu zeigen, dass man mit Hilfe der Samplemethode einen kürzesten von 0 verschiedenen Gittervektor mit Erfolgswahrscheinlichkeit exponentiell nahe an 1 berechnen kann. Die Laufzeit ist dabei einfach exponentiell in Bezug auf den Rang des Gitters mit einem Faktor polynomiell in der Eingabelänge.

Des Weiteren wurde gezeigt, dass man unter Verwendung dieser Samplemethode mit entsprechend gewählten Parametern das Problem des nächsten Gittervektors mit dem Approximationsfaktor $c(1+\epsilon)^2$ für $\epsilon > 0$ und c konstant in einfach exponentieller Laufzeit lösen kann. Für die Lösung des Problems wird ein Algorithmus benötigt, der das Problem des kürzesten Gittervektors exakt löst.

Leider mußte festgestellt werden, dass man die Samplemethode nicht so variieren kann, dass man nach obigem Prinzip das Problem des nächsten Gittervektors exakt lösen kann. Dies ist ein Problem, was im Weiteren noch untersucht werden müßte. Dieses Problem geht einher mit der Frage, wie Ajtai, Kumar und Sivakumar sich die Modifikation ihrer vorgeschlagenen Siebmethode zur $(1+\epsilon)$-Approximation vorstellen. Die Übertragung beider Samplemethoden scheitert ursächlich an dem gleichen Problem: Eine Kollision in einer Menge zu finden, in der mehr als einfach exponentiell viele Elemente enthalten sind.

Anhang A.

Beweis einer Transferschranke von Cai

In diesem Abschnitt wird die Transferschranke von Cai [8] bewiesen, die bereits in Satz 2.4.3 zitiert und in Kapitel 5 angewendet wurde. Sie stellt eine Beziehung zwischen der Länge der kürzesten Basis eines Gitters L und der Länge des kürzesten Gittervektors des dualen Gitters L^* dar. Der Beweis der Transferschranke ist nicht konstruktiv. Die wesentliche Beweisidee ist die Betrachtung der Fouriertransformation von Gauß-ähnlichen Maßen auf einem Gitter L sowie einem echten Untergitter von L. Deswegen wird zunächst eine Einführung in die Grundlagen der Fourier-Transformation gegeben. Eine vertiefende Einleitung in dieses Gebiet geben unter anderem [14] und [25].

Die in diesem Anhang verwendete Norm ist die ℓ_2-Norm. Um die Übersichtlichkeit in den Rechnungen zu erhalten, wird im Folgenden auf den Index $||.||_2$ verzichtet und stattdessen $||.||$ verwendet.

A.1. Fourier-Transformation

Dieser Abschnitt gibt eine kurze Einführung in die wesentlichen Eigenschaften der Fourier-Transformation für Funktionen und Maße, soweit sie für den Beweis der Transferschranke benötigt werden. Die Fourier-Transformation benutzt Techniken der Analysis und Funktionentheorie [16], [11], [17].

Definition A.1.1 *Mit $L^1(\mathbb{R}^n)$ bezeichnet man die Menge aller Funktionen $f : \mathbb{R}^n \to \mathbb{C}$ mit*

$$\int_{\mathbb{R}^n} |f(x)| \, \mathrm{dx} < \infty$$

Definition A.1.2 *Für $f \in L^1(\mathbb{R}^n)$ ist die Fourier-Transformation $\hat{f}$ definiert als*

$$\hat{f}(y) := \int_{\mathbb{R}^n} f(x) e^{-2\pi i \langle x,y \rangle} dx$$

Die im folgenden Beispiel eingeführte Funktion spielt im Beweis der Transferschranke von Cai eine wichtige Rolle.

Beispiel A.1.3 *Für $a > 0$ definiere*

$$\rho_a(x) := e^{-a||x||^2}$$

Für den Fall $a = \pi$ schreibt man $\rho := \rho_\pi$.
Es soll die Fourier-Transformation der Funktion

$$\rho_{a\pi}(x) = e^{-\pi a\left(x_1^2 + \ldots + x_n^2\right)} = e^{-\pi a x_1^2} \cdot \ldots \cdot e^{-\pi a x_n^2}$$

berechnet werden. Dazu setzt man $f_j(x_j) := e^{-\pi a x_j^2}$. Dann ist die Fouriertransformation von f_j gegeben durch:

$$\begin{aligned}
\hat{f}_j(y) &= \int_{-\infty}^{\infty} e^{-\pi a x_j^2} e^{-2\pi i x_j \cdot y} dx_j \\
&= \int_{-\infty}^{\infty} e^{-\pi\left(a x_j^2 + 2i x_j \cdot y\right)} dx_j \\
&= \int_{-\infty}^{\infty} e^{-\pi\left(\sqrt{a} x_j + i\frac{1}{\sqrt{a}} \cdot y\right)^2} e^{-\pi\frac{y^2}{a}} dx_j \\
&= e^{-\pi\frac{y^2}{a}} \int_{-\infty}^{\infty} e^{-\pi\left(\sqrt{a} x_j + i\frac{1}{\sqrt{a}} \cdot y\right)^2} dx_j
\end{aligned}$$

Nach dem Satz von Cauchy ist eine Variablentransformation $z := \sqrt{a} x_j + i \cdot \frac{y}{\sqrt{a}}$ möglich und man erhält:

$$\begin{aligned}
\hat{f}_j(y) &= e^{-\pi\frac{y^2}{a}} \int_{-\infty}^{\infty} e^{-\pi z^2} \frac{1}{\sqrt{a}} \,\mathrm{dz} \\
&= e^{-\pi\frac{y^2}{a}} \frac{1}{\sqrt{a}} \underbrace{\int_{-\infty}^{\infty} e^{-\pi z^2} dz}_{=1} \\
&= \frac{1}{\sqrt{a}} e^{-\pi\frac{y^2}{a}}
\end{aligned}$$

Nach dem Satz von Fubini folgt:

$$\begin{aligned}
\hat{f}(y) &= \int_{\mathbb{R}^n} e^{-a\pi||x||^2} e^{-2\pi i\langle x, y\rangle} dx \\
&= \prod_{j=1}^{n} \int_{\mathbb{R}} e^{-a\pi|x_j|^2} e^{-2\pi i x_j \cdot y_j} dx_j \\
&= \prod_{j=1}^{n} \frac{1}{\sqrt{a}} e^{-\pi\frac{y_j^2}{a}} \\
&= a^{-\frac{n}{2}} e^{-\frac{\pi}{a}||y||^2} \\
&= a^{-\frac{n}{2}} \rho_{\frac{\pi}{a}}(y) \\
\Longrightarrow \hat{\rho}_{a\pi}(y) &= a^{-\frac{n}{2}} \rho_{\frac{\pi}{a}}(y)
\end{aligned}$$

Es werden nun zwei wichtige Eigenschaften der Fourier-Transformation bewiesen, die für den Beweis von Lemma A.2.2 benötigt werden. Sie zeigen, dass unter der Fourier-Transformation Translationen zu Phasenverschiebungen werden und umgekehrt.

Lemma A.1.4 *Seien $f \in L^1(\mathbb{R}^n)$ und $x, y, z \in \mathbb{R}^n$. Dann gelten die folgenden Eigenschaften:*

1. *Für $h(x) := f(x+z)$ ist die Fourier-Transformation gegeben durch*

$$\hat{h}(y) = e^{2\pi i \langle y, z \rangle} \hat{f}(y)$$

2. *Für $h(x) := e^{2\pi i \langle x, z \rangle} f(x)$ ist die Fourier-Transformation gegeben durch*

$$\hat{h}(y) = \hat{f}(y - z)$$

Beweis: Der Beweis erfolgt durch Verwendung der Definition.

1. Sei $h(x) = f(x+z)$. Dann gilt:

$$\begin{aligned} \hat{h}(y) &= \int_{\mathbb{R}^n} f(x+z) e^{-2\pi i \langle x, y \rangle} \, \mathrm{dx} \\ &= \int_{\mathbb{R}^n} f(x) e^{2\pi i \langle x - z, y \rangle} \, \mathrm{dx} \\ &= e^{2\pi i \langle z, y \rangle} \int_{\mathbb{R}^n} f(x) e^{-2\pi i \langle x, y \rangle} \, \mathrm{dx} \\ &= e^{2\pi i \langle z, y \rangle} \hat{f}(y) \end{aligned}$$

2. Sei $h(x) = e^{2\pi i \langle x, z \rangle} f(x)$. Dann gilt:

$$\begin{aligned} \hat{h}(y) &= \int_{\mathbb{R}^n} e^{2\pi i \langle x, z \rangle} f(x) e^{-2\pi i \langle x, y \rangle} \, \mathrm{dx} \\ &= \int_{\mathbb{R}^n} f(x) e^{-2\pi i \langle x, y - z \rangle} \, \mathrm{dx} \\ &= \hat{f}(y - z) \end{aligned}$$

□

Die Fourier-Transformation kann man auch für Maße definieren. Als Grundlage wird zunächst die Definition einer messbaren Menge und eines Maßes angegeben.

Definition A.1.5 *Sei M eine beliebige, nichtleere Menge und $\mathcal{P}(M)$ die Potenzmenge von M. Eine nichtleere Menge $\mathcal{M} \subseteq \mathcal{P}(M)$ von Teilmengen von M heißt eine Algebra, wenn gilt:*

1. $E_1, \ldots, E_n \in \mathcal{M} \Longrightarrow E_1 \cup \ldots \cup E_n \in \mathcal{M}$
2. $E \in \mathcal{M} \Longrightarrow M \backslash E \in \mathcal{M}$

Falls zusätzlich gilt:

3. $E_j \in \mathcal{M}$ *für* $j \in \mathbb{N} \Longrightarrow \bigcup_{j\in\mathbb{N}} E_j \in \mathcal{M}$

heißt die Algebra $\mathcal{M}$ *eine* σ*-Algebra.*
Ein Paar $(M, \mathcal{M})$ *bestehend aus einer nichtleeren Menge* M *und einer* σ*-Algebra* $\mathcal{M} \subseteq \mathcal{P}(M)$ *heißt ein messbarer Raum. Die Elemente der* σ*-Algebra heißen messbare Mengen.*

Definition A.1.6 *Sei* $(M, \mathcal{M})$ *ein messbarer Raum. Eine Abbildung*

$$\mu : \mathcal{M} \to [0, \infty]$$

heißt ein Maß auf $(M, \mathcal{M})$*, wenn* $\mu(\emptyset) = 0$ *und für jede disjunkte abzählbare Familie* $E_1, E_2, \ldots$ *von messbaren Mengen gilt:*

$$\mu(\bigcup_{j=1}^{\infty} E_j) = \sum_{j=1}^{\infty} \mu(E_j).$$

In diesem Kapitel werden nur endliche Borel-Maße μ auf dem $\mathbb{R}^n$ betrachtet, das heißt zu jedem $x \in \mathbb{R}^n$ existiert eine offene Umgebung U von x mit $\mu(U) < \infty$. Für ein solches Maß wird die Fourier-Transformation hier definiert durch

$$\hat{\mu}(x) := \int_{\mathbb{R}^n} e^{2\pi i \langle x, y\rangle} d\mu(y)$$

A.2. Grundlagen für den Beweis der Transferschranke

Im Folgenden sei L ein n-dimensionales Gitter im $\mathbb{R}^n$ und $v \in L$ ein beliebiger Gittervektor. Für einen Vektor $u \in \mathbb{R}^n$ ist

$$L + u = \{w + u | w \in L\}.$$

Eine grundlegende Formel für die Verwendung der Fouriertransformation ist die Poisson'sche Summationsformel:

Theorem A.2.1 Poisson'sche Summationsformel
Sei $f : \mathbb{R}^n \to \mathbb{C}$ *eine Funktion mit folgenden Eigenschaften:*

1. $\int_{\mathbb{R}^n} |f(x)| \,\mathrm{dx} < \infty$
2. *Die Reihe* $\sum_{x\in L} |f(x+u)|$ *konvergiert gleichmäßig für alle* $u \in \mathbb{R}^n$*, die zu einer kompakten Teilmenge des* $\mathbb{R}^n$ *gehören.*
3. *Die Reihe* $\sum_{y\in L^*} \hat{f}(y)$ *ist absolut konvergent.*

Dann gilt:

$$\sum_{x\in L} f(x) = \frac{1}{\det L} \sum_{y\in L^*} \hat{f}(y).$$

Die erste Bedingung garantiert die Existenz der Fourier-Transformation $\hat{f}$ von f. Die zweite Bedingung bedeutet, dass die Funktion $F(u) := \sum_{x\in\mathbb{Z}^n} f(x + u)$ über $\mathbb{R}^n$ stetig ist.

Beweis: Man betrachte zunächst das Gitter $\mathbb{Z}^n$. Die Funktion

$$F(u) := \sum_{x \in \mathbb{Z}^n} f(x+u)$$

ist nach Voraussetzung stetig und periodisch in u, da $F(u+x) = F(x)$ für alle $x \in \mathbb{Z}^n$. Sie kann deswegen als Fourierreihe entwickelt werden:

$$F(u) = \sum_{y \in \mathbb{Z}^n} e^{2\pi i \langle u, y \rangle} a(y),$$

wobei $a(y) = \int_{[0,1]^n} F(t) e^{-2\pi i \langle y, t \rangle} \, \mathrm{dt}$. Durch Rechnung erhält man:

$$\begin{aligned} a(y) &= \int_{[0,1]^n} F(t) e^{-2\pi i \langle y, t \rangle} \, \mathrm{dt} \\ &= \int_{[0,1]^n} \sum_{x \in \mathbb{Z}^n} f(x+t) e^{-2\pi i \langle y, t \rangle} \, \mathrm{dt} \\ &= \sum_{x \in \mathbb{Z}^n} \int_{[0,1]^n} f(x+t) e^{-2\pi i \langle y, x+t \rangle} \, \mathrm{dt} \\ &= \sum_{x \in \mathbb{Z}^n} \int_{x+[0,1]^n} f(t') e^{-2\pi i \langle y, t' \rangle} \, \mathrm{dt}' \\ &= \hat{f}(y) \end{aligned}$$

Damit konvergiert die Fourierreihe von F nach Voraussetzung gegen eine stetige Funktion und in diesem Fall ist

$$F(0) = \sum_{x \in \mathbb{Z}^n} f(x) = \sum_{y \in \mathbb{Z}^n} \hat{f}(y).$$

Dies ist die Poisson'sche Summationsformel für das Gitter $\mathbb{Z}^n$, da $\det(\mathbb{Z}^n) = 1$ und $(\mathbb{Z}^n)^* = \mathbb{Z}^n$.

Man betrachte jetzt ein Basis B des Gitters L. Da L volldimensional ist, ist $B \in \mathrm{GL}(n, \mathbb{Z})$ und es gilt:

$$\begin{aligned} \sum_{x \in L} f(x) &= \sum_{x \in \mathbb{Z}^n} f(Bx) \\ &= \sum_{y \in \mathbb{Z}^n} f_B(y) \\ &= \sum_{y \in \mathbb{Z}^n} \hat{f}_B(y) \end{aligned}$$

mit

$$\begin{aligned} \hat{f}_B(y) &= \int_{\mathbb{R}^n} f(Bt) e^{2\pi i \langle t, y \rangle} \, \mathrm{dt} \\ &= \frac{1}{\det B} \int_{\mathbb{R}^n} f(t') e^{2\pi i \langle B^{-1} t', y \rangle} \, \mathrm{dt}' \qquad (t' = Bt) \\ &= \frac{1}{\det B} \int_{\mathbb{R}^n} f(t') e^{2\pi i \langle t', B^{-1} y \rangle} \, \mathrm{dt}' \\ &= \frac{1}{\det L} \hat{f}((B^T)^{-1} y) \end{aligned}$$

Da $(B^T)^{-1}$ eine Basis des dualen Gitters L^* ist, folgt die Behauptung:

$$\begin{aligned}\sum_{x\in L} f(x) &= \sum_{y\in\mathbb{Z}^n} \hat{f}((B^T)^{-1}y) \\ &= \frac{1}{\det L}\sum_{y\in L^*}\hat{f}(y)\end{aligned}$$

□

Das nächste Lemma ist eine Folgerung aus der Poisson'schen Summationsformel und ist ein wichtiges Hilfsmittel für die Beweise im weiteren Verlauf dieses Kapitels.

Lemma A.2.2 *Seien $a, b > 0$ mit $a \cdot b = \pi$.*
Sei ρ das Maß auf L gegeben durch

$$\rho_a(\{x\}) = e^{-a||x||^2}$$

1. *Für $u, y \in \mathbb{R}^n$ gilt:*

$$\sum_{x\in L+u} e^{2\pi i\langle x,y\rangle} e^{-a||x||^2} = b^{\frac{n}{2}}(\det L)^{-1}\sum_{z\in L^*} e^{-2\pi i\langle u,z\rangle} e^{-\pi b||y+z||^2}$$

2. *Für $y \in \mathbb{R}^n$ gilt:*

$$\hat{\rho}_a(y) = b^{\frac{n}{2}}(\det L)^{-1}\sum_{z\in L^*} e^{-\pi b||y+z||^2}$$

Beweis:

1. Sei $h(x) := e^{2\pi i\langle x+u,y\rangle} e^{-a||x+u||^2} = f(x+u)$ mit $f(x) := e^{2\pi i\langle x,y\rangle} e^{-a||x||^2}$. Auf Grund der Eigenschaften der Fourier-Transformation aus Lemma A.1.4 lässt sich die Fourier-Transformation von h wie folgt berechnen:

$$\hat{h}(z) = e^{2\pi i\langle z,u\rangle}\hat{f}(z)$$

Die Fourier-Transformation von $f(x) = e^{2\pi i\langle x,y\rangle} e^{-a||x||^2} = e^{2\pi i\langle x,y\rangle}\rho_{\pi\cdot\frac{1}{b}}(x)$ ist nach Lemma A.1.4 und nach Beispiel A.1.3:

$$\hat{f}(z) = \hat{\rho}_{\pi\frac{1}{b}}(z-y) = b^{\frac{n}{2}} e^{-\pi b||z-y||^2}$$

Damit erhält man für h folgende Fouriertransformation:

$$\hat{h}(z) = e^{2\pi i\langle z,u\rangle} b^{\frac{n}{2}} e^{-\pi b||z-y||^2}$$

Mit Hilfe der Poisson'schen Summenformel A.2.1 folgt die Behauptung:

$$\begin{aligned}\sum_{x\in L+u} e^{2\pi i\langle x,y\rangle} e^{-a||x||^2} &= \sum_{x\in L} e^{2\pi i\langle x+u,y\rangle} e^{-a||x+u||^2} \\ &= \frac{1}{\det L}\sum_{z\in L^*}\hat{h}(z) \\ &= \frac{1}{\det L}\sum_{z\in L^*} b^{\frac{n}{2}} e^{2\pi i\langle z,u\rangle} e^{-\pi b||z-y||^2} \\ &= \frac{1}{\det L} b^{\frac{n}{2}} \sum_{z\in L^*} e^{-2\pi i\langle z,u\rangle} e^{-\pi b||z+y||^2}\end{aligned}$$

2. Für $u = 0$ erhält man unter Verwendung von 1.:

$$\begin{aligned}\hat{\mu}_a(y) &= \sum_{x\in L} e^{2\pi i\langle x,y\rangle} e^{-a||x||^2} \\ &= b^{\frac{n}{2}}(\det L)^{-1}\sum_{z\in L^*} e^{-2\pi i\langle 0,z\rangle} e^{-\pi b||y+z||^2} \\ &= b^{\frac{n}{2}}(\det L)^{-1}\sum_{z\in L^*} e^{-\pi b||y+z||^2}\end{aligned}$$

□

Zur übersichtlicheren Darstellung definiert man die folgenden Funktionen:

$$\begin{aligned}\sigma_L(\{v\}) &:= \frac{e^{-\pi||v||^2}}{\sum_{x\in L} e^{-\pi||x||^2}} \\ \tau_L(u) &:= \frac{\sum_{y\in L+u} e^{-\pi||y||^2}}{\sum_{x\in L} e^{-\pi||x||^2}}\end{aligned}$$

Zur Vereinfachung der Darstellung sei

$$\rho(A) := \sum_{x\in A}\rho(x) = \sum_{x\in A} e^{-\pi||x||^2}$$

für $A \subseteq \mathbb{R}^n$. Dann ist

$$\begin{aligned}\sigma_L(\{v\}) &= \frac{\rho(\{v\})}{\rho(L)} \\ \tau_L(u) &= \frac{\rho(L+u)}{\rho(L)}\end{aligned}$$

Zwischen den Funktionen σ_L und τ_L gilt folgende Beziehung:

Korollar A.2.3 *Es gilt:*

$$\begin{aligned}\hat{\sigma}_L &= \tau_{L^*} \\ \hat{\sigma}_{L^*} &= \tau_L\end{aligned}$$

Beweis: Wegen $(L^*)^* = L$ genügt es $\hat{\sigma}_L = \tau_{L^*}$ zu zeigen.
Sei μ das Maß auf L gegeben durch

$$\mu(\{x\}) = e^{-a||x||^2}$$

Dann kann mit Hilfe von Lemma A.2.2 die Fourier-Transformation von σ_L berechnet werden:

$$\begin{aligned}
\hat{\sigma}_L(u) &= \int_{\mathbb{R}^n} e^{2\pi i\langle u,x\rangle}\sigma_L(x)\,\mathrm{dx} \\
&= \sum_{v\in L} e^{2\pi i\langle u,v\rangle}\sigma_L(\{v\}) \\
&= \sum_{v\in L} e^{2\pi i\langle u,v\rangle}\frac{e^{-\pi||v||^2}}{\sum_{x\in L} e^{-\pi||x||^2}} \\
&= \frac{\sum_{v\in L} e^{-\pi||v||^2} e^{\pi i\langle u,v\rangle}}{\sum_{x\in L} e^{-||x||^2} e^{\pi i\langle 0,x\rangle}} \\
&= \frac{\hat{\mu}(u)}{\hat{\mu}(0)} \\
&= \frac{1^{\frac{n}{2}}(\det L)^{-1}\sum_{z\in L^*} e^{-\pi 1||u+z||^2}}{1^{\frac{n}{2}}(\det L)^{-1}\sum_{z\in L^*} e^{-\pi 1||0+z||^2}} \qquad \text{(Lemma A.2.2 mit } b=1) \\
&= \frac{\sum_{z\in L^*} e^{-\pi||u+z||^2}}{\sum_{z\in L^*} e^{-\pi||z||^2}} \\
&= \frac{\sum_{z\in L^*+u} e^{-\pi||z||^2}}{\sum_{z\in L^*} e^{-\pi||z||^2}} \\
&= \tau_{L^*}(u)
\end{aligned}$$

□

Das folgende Lemma dient zur Vereinfachung der Rechnungen im Beweis von Lemma A.2.5.

Lemma A.2.4 *Sei $u \in \mathbb{R}^n$ beliebig, $a > 0$.*
Dann gilt für $k = 1, \ldots, n$:

$$\kappa := \frac{\sum_{x\in L+u} x_k^2 e^{-a||x||^2}}{\sum_{x\in L} e^{-a||x||^2}} \leq \frac{1}{a}$$

Für $u = 0$ gilt:

$$\kappa \leq \frac{1}{2a}$$

Beweis: Setze $b := \frac{\pi}{a}$.
Für den Beweis benötigt man zunächst einige Rechnungen. Mit $\frac{\partial f}{\partial y_k}$ wird im Folgenden die

partielle Ableitung von f nach der k-ten Komponente von y bezeichnet, mit $\frac{\partial^2 f}{\partial y_k^2}$ entsprechend die zweite partielle Ableitung.
Man verwendet das Maß

$$\mu(\{x\}) = e^{-a||x||^2}$$

auf $L + u$ und berechnet zunächst folgende partielle Ableitungen:

$$\begin{aligned}
\hat{\mu}(y) &= \sum_{x \in L+u} e^{-a||x||_2^2} e^{2\pi i \langle x, y \rangle} \\
\Longrightarrow \frac{\partial \hat{\mu}}{\partial y_k}(y) &= \sum_{x \in L+u} 2\pi i x_k e^{2\pi i \langle x, y \rangle} e^{-a||x||^2} \\
\Longrightarrow \frac{\partial^2 \hat{\mu}}{\partial y_k^2}(y) &= \sum_{x \in L+u} (2\pi i x_k)^2 e^{2\pi i \langle x, y \rangle} e^{-a||x||^2} \\
&= \sum_{x \in L+u} -4\pi^2 x_k^2 e^{2\pi i \langle x, y \rangle} e^{-a||x||^2}
\end{aligned}$$

Für $y = 0$ erhält man:

$$\begin{aligned}
\frac{\partial^2 \hat{\mu}}{\partial y_k^2}(0) &= -4\pi^2 \sum_{x \in L+u} x_k^2 e^{-a||x||^2} \\
\Longrightarrow \sum_{x \in L+u} x_k^2 e^{-a||x||^2} &= -(4\pi^2)^{-1} \frac{\partial \hat{\rho}_a}{\partial y_{kk}}(0) \qquad \text{(A.1)}
\end{aligned}$$

Nach Lemma A.2.2 gilt:

$$\begin{aligned}
\hat{\mu}(y) &= \sum_{x \in L+u} e^{2\pi i \langle x, y \rangle} e^{-a||x||^2} = b^{\frac{n}{2}} (\det L)^{-1} \sum_{z \in L^*} e^{-2\pi i \langle u, z \rangle} e^{-\pi b||y+z||^2} \\
\Longrightarrow \frac{\partial \hat{\mu}}{\partial y_k}(y) &= b^{\frac{n}{2}} (\det L)^{-1} \sum_{z \in L^*} e^{-2\pi i \langle u, z \rangle} \left(-2\pi b(y_k + z_k) e^{-\pi b||y+z||^2} \right) \\
\Longrightarrow \frac{\partial^2 \hat{\mu}}{\partial y_k^2}(y) &= b^{\frac{n}{2}} (\det L)^{-1} \sum_{z \in L^*} e^{-2\pi i \langle u, z \rangle} \left(-2\pi b e^{-\pi b||y+z||^2} + (-2\pi b(y_k + z_k))^2 e^{-\pi b||y+z||^2} \right) \\
&= b^{\frac{n}{2}} (\det L)^{-1} \sum_{z \in L^*} e^{-2\pi i \langle u, z \rangle} \left(-2\pi b + 4\pi^2 b^2 (y_k + z_k)^2 \right) e^{-\pi b||y+z||^2}
\end{aligned}$$

Für $y = 0$ erhält man:

$$\frac{\partial^2 \hat{\mu}}{\partial y_k^2}(0) = b^{\frac{n}{2}} (\det L)^{-1} \sum_{z \in L^*} e^{-2\pi i \langle u, z \rangle} \left(-2\pi b + 4\pi^2 b^2 z_k^2 \right) e^{-\pi b||z||^2} \qquad \text{(A.2)}$$

Wenn man das Maß

$$\nu(\{z\}) := e^{-\pi b||z||^2}$$

auf L^* betrachtet, so erhält man durch Berechnung der partiellen Ableitungen:

$$\begin{aligned}
\hat{\nu}(-u) &= \sum_{z\in L^*} e^{-2\pi i\langle u,z\rangle} e^{-\pi b||z||^2} && \text{(A.3)}\\
\Longrightarrow \frac{\partial\hat{\nu}}{\partial u_k}(-u) &= \sum_{z\in L^*} -2\pi i z_k e^{-2\pi i\langle u,z\rangle} e^{-\pi b||z||^2} \\
\Longrightarrow \frac{\partial^2\hat{\nu}}{\partial u_k^2}(-u) &= \sum_{z\in L^*} (-2\pi i z_k)^2 e^{-2\pi i\langle u,z\rangle} e^{-\pi b||z||^2} \\
&= \sum_{z\in L^*} -4\pi^2 z_k^2 e^{-2\pi i\langle u,z\rangle} e^{-\pi b||z||^2} && \text{(A.4)}\\
\Longrightarrow \sum_{z\in L^*} z_k^2 e^{-2\pi i\langle u,z\rangle} e^{-\pi b||z||^2} &= -(4\pi^2)^{-1}\frac{\partial^2\hat{\nu}}{\partial u_k^2}(-u) && \text{(A.5)}
\end{aligned}$$

Nach Lemma A.2.2 mit $u = y = 0$ gilt:

$$\begin{aligned}
\sum_{x\in L} e^{-a||x||^2} &= b^{\frac{n}{2}}(\det L)^{-1}\sum_{z\in L^*} e^{-\pi b||z||^2} \\
\Longrightarrow \hat{\nu}(0) &= \sum_{z\in L^*} e^{-\pi b||x||^2} = b^{-\frac{n}{2}}(\det L)\sum_{x\in L} e^{-a||x||^2} && \text{(A.6)}
\end{aligned}$$

Unter Verwendung dieser Resultate erhält man insgesamt:

$$\begin{aligned}
\kappa &= \frac{\sum_{x\in L+u} x_k^2 e^{-a||x||^2}}{\sum_{x\in L} e^{-a||x||^2}} \\
&\overset{(A.1)}{=} \frac{-(4\pi^2)^{-1}\frac{\partial^2\hat{\mu}}{\partial y_k^2}(0)}{\sum_{x\in L} e^{-a||x||^2}} \\
&\overset{(A.2)}{=} \frac{-(4\pi^2)^{-1} b^{\frac{n}{2}}(\det L)^{-1}\sum_{z\in L^*} e^{-2\pi i\langle u,z\rangle}\left(-2\pi b + 4\pi^2 b^2 z_k^2\right) e^{-\pi b||z||^2}}{\sum_{x\in L} e^{-a||x||^2}} \\
&= -(4\pi^2)^{-1}\frac{\sum_{z\in L^*} -2\pi b e^{-2\pi i\langle u,z\rangle} e^{-\pi b||z||^2} + \sum_{z\in L^*} 4\pi^2 b^2 z_k^2 e^{-2\pi i\langle u,z\rangle} e^{-\pi b||z||^2}}{b^{-\frac{n}{2}}(\det L)\sum_{x\in L} e^{-a||x||^2}} \\
&\overset{(A.6)}{=} (4\pi^2)^{-1}\frac{-2\pi b\sum_{z\in L^*} e^{-2\pi i\langle u,z\rangle} e^{-\pi b||z||^2} + 4\pi^2 b^2\sum_{z\in L^*} z_k^2 e^{-2\pi i\langle u,z\rangle} e^{-\pi b||z||^2}}{\hat{\nu}(0)} \\
&\overset{(A.3),(A.5)}{=} -(4\pi^2)^{-1}\frac{-2\pi b\hat{\nu}(-u) + 4\pi^2 b^2(-(4\pi^2)^{-1})\frac{\partial^2\hat{\nu}}{\partial u_k^2}(-u)}{\hat{\nu}(0)} \\
&= \frac{b}{2\pi}\frac{\hat{\nu}(-u)}{\hat{\nu}(0)} + \frac{b^2}{4\pi^2}\frac{\frac{\partial^2\hat{\nu}}{\partial u_k^2}(-u)}{\hat{\nu}(0)} && \text{(A.7)}
\end{aligned}$$

Sei $v \in \mathbb{R}^n$ beliebig. Dann gilt nach Lemma A.2.2 mit $y = 0$ und unter Verwendung von

$||x+v||^2 = ||x||^2 + 2\langle x, v\rangle + ||v||^2$:

$$\begin{aligned}
b^{\frac{n}{2}}(\det L)^{-1}\hat{\nu}(v) &= b^{\frac{n}{2}}(\det L)^{-1}\sum_{z\in L^*} e^{2\pi i\langle v,z\rangle} e^{-\pi b||z||^2} \\
&\overset{(A.2.2)}{=} \sum_{x\in L+v} e^{-a||x||^2} \\
&= \sum_{x\in L} e^{-a||x+v||^2} \\
&= \sum_{x\in L} \frac{1}{2}\left(e^{-a||x+v||^2} + e^{-a||(-x)-v||^2}\right) \\
&= \sum_{x\in L} \frac{1}{2}\left(e^{-a||x+v||^2} + e^{-a||x-v||^2}\right) \qquad \text{(Umsortierung der Reihe)} \\
&= e^{-a||v||^2}\sum_{x\in L} \frac{1}{2}\left(e^{-a||x||^2}e^{-2a\langle x,v\rangle} + e^{-a||x||^2}e^{2a\langle x,v\rangle}\right) \\
&= e^{-a||v||^2}\sum_{x\in L} e^{-a||x||^2}\underbrace{\cosh(2a\langle x,v\rangle)}_{\geq 1} \\
&\geq e^{-a||v||^2}\sum_{x\in L} e^{-a||x||^2}
\end{aligned}$$

Mit dieser Abschätzung gilt für den Vektor $v \in \mathbb{R}^n$:

$$\begin{aligned}
\frac{\hat{\nu}(v)}{\hat{\nu}(0)} &\overset{(A.6)}{=} \frac{\hat{\nu}(v)}{b^{-\frac{n}{2}}\det L\sum_{x\in L} e^{-a||x||^2}} \\
&= \frac{b^{\frac{n}{2}}(\det L)^{-1}\hat{\nu}(v)}{\sum_{x\in L} e^{-a||x||^2}} \\
&\geq \frac{e^{-a||v||^2}\sum_{x\in L} e^{-a||x||^2}}{\sum_{x\in L} e^{-a||x||^2}} \\
&= e^{-a||v||^2}
\end{aligned}$$

und damit

$$\begin{aligned}
\frac{\hat{\nu}(v)}{\hat{\nu}(0)} &\geq e^{-a||v||^2} \\
\Longrightarrow \frac{\frac{\partial\hat{\nu}(v)}{\partial v_k}}{\hat{\nu}(0)} &\geq -2av_k e^{-a||v||^2} \\
\Longrightarrow \frac{\frac{\partial^2\hat{\nu}(v)}{\partial v_k^2}}{\hat{\nu}(0)} &\geq -2ae^{-a||v||^2} + 4a^2v_k^2e^{-a||v||^2} \\
\Longrightarrow -\frac{\frac{\partial^2\hat{\nu}(0)}{\partial v_k^2}}{\hat{\nu}(0)} &\leq 2a\underbrace{e^{-a||v||^2}}_{\leq 1} - \underbrace{4a^2v_k^2e^{-a||v||^2}}_{\leq 0} \leq 2a
\end{aligned}$$

Durch Verwendung der Ergebnisse (A.3) und (A.4) erhält man

$$\begin{aligned}
\hat{\nu}(-u) &\overset{(A.3)}{=} \sum_{z\in L^*} e^{-2\pi i\langle u,z\rangle}e^{-\pi b||z||^2} \leq \hat{\nu}(0) \\
\Longrightarrow \quad \frac{\hat{\nu}(-u)}{\hat{\nu}(0)} &\leq 1
\end{aligned} \tag{A.8}$$

und

$$\frac{\partial^2\hat{\nu}}{\partial u_k^2}(-u) \overset{(A.4)}{=} \sum_{z\in L^*} -4\pi^2z_k^2e^{-2\pi i\langle u,z\rangle}e^{-\pi b||z||^2} \leq -\sum_{z\in L^*} -4\pi^2z_k^2e^{-\pi b||z||^2} = -\frac{\partial^2\hat{\nu}}{\partial u_k^2}(0) \tag{A.9}$$

Insgesamt gilt also

$$\frac{\frac{\partial^2\hat{\nu}}{\partial v_k^2}(-u)}{\hat{\nu}(0)} \overset{(A.9)}{\leq} -\frac{\frac{\partial^2\hat{\nu}(0)}{\partial v_k^2}}{\hat{\nu}(0)} \leq 2a \tag{A.10}$$

Mit $a \cdot b = \pi$ erhält man dann für κ die Abschätzung:

$$\begin{aligned}
\kappa \quad &\overset{(A.7)}{=} \quad \frac{b}{2\pi}\frac{\hat{\nu}(-u)}{\hat{\nu}(0)} + \frac{b^2}{4\pi^2}\frac{\frac{\partial^2\hat{\nu}(-u)}{\partial u_k^2}}{\hat{\nu}(0)} \\
&\overset{(A.8),(A.10)}{\leq} \quad \frac{1}{2a}\cdot 1 + \frac{b^2}{4\pi^2}\cdot 2a \\
&= \quad \frac{1}{2a} + \frac{1}{2a} \qquad \left(\text{mit } \frac{b}{\pi} = a\right) \\
&= \quad \frac{1}{a}
\end{aligned} \tag{A.11}$$

Für $u = 0$ ist $\frac{\partial^2\hat{\nu}}{\partial u_k^2}(0) < 0$ und damit erhält man aus (A.11) unter Verwendung von (A.8):

$$\kappa = \frac{b}{2\pi}\frac{\hat{\nu}(-u)}{\hat{\nu}(0)} + \frac{b^2}{4\pi^2}\frac{\frac{\partial^2\hat{\nu}(-u)}{\partial u_k^2}}{\hat{\nu}(0)} < \frac{1}{2a}$$

□

Lemma A.2.5 *Sei $a \geq 1$. Dann gilt:*

1. $\sum_{x\in L} e^{-\pi a^{-1}||x||^2} \leq a^{\frac{n}{2}} \sum_{x\in L} e^{-\pi||x||^2}$
2. $\sum_{x\in L+u} e^{-\pi a^{-1}||x||^2} \leq 2a^{\frac{n}{2}} \sum_{x\in L} e^{-\pi||x||^2}$ *für* $u \in \mathbb{R}^n$

Beweis:

1. Betrachte die Funktion $f(a) := \sum_{x\in L} e^{-\pi a^{-1}||x||^2}$ für $a \geq 1$.
   Es ist also zu zeigen: $f(a) \leq a^{\frac{n}{2}} f(1)$.
   Nach Lemma A.2.4 gilt:

$$\frac{\sum_{x\in L+u} x_k^2 e^{-\frac{\pi}{a}||x||^2}}{\sum_{x\in L} e^{-a||x||^2}} \leq \frac{\pi}{a} \tag{A.12}$$

   Für $u = 0$ ergibt sich:

$$\frac{\sum\limits_{x\in L} x_k^2 e^{-\frac{\pi}{a}||x||^2}}{\sum\limits_{x\in L} e^{-\frac{\pi}{a}||x||^2}} \leq \frac{a}{2\pi} \tag{A.13}$$

   Dann ist

$$\begin{aligned}
f'(a) &= \sum_{x\in L} \frac{\pi}{a^2}||x||^2 e^{-\pi a^{-1}||x||^2} \\
&= \frac{\pi}{a^2} \sum_{x\in L} \sum_{k=1}^{n} x_k^2 e^{-\pi a^{-1}||x||^2} \\
&= \frac{\pi}{a^2} \sum_{k=1}^{n} \sum_{x\in L} x_k^2 e^{-\pi a^{-1}||x||^2} \\
&\leq \frac{\pi}{a^2} \sum_{k=1}^{n} \frac{a}{2\pi} \sum_{x\in L} e^{-\pi a^{-1}||x||^2} \qquad \text{(nach } A.13\text{)} \\
&= \frac{n}{2a} \sum_{x\in L} e^{-\pi a^{-1}||x||^2} \\
&= \frac{n}{2a} f(a)
\end{aligned}$$

   Daraus folgt:

$$(\log_2 f(a))' = \frac{1}{f(a)\ln 2} f'(a) \leq \frac{n}{\ln 2 \cdot 2a} \leq \frac{n}{2a}$$

   und damit erhält man mit $f(1) \geq 1$ die Behauptung:

$$f(a) \leq e^{\frac{n}{2}\ln a} = a^{\frac{n}{2}} \leq a^{\frac{n}{2}} f(1)$$

2. Sei $u \in \mathbb{R}^n$ beliebig.
   Man betrachte die Funktion $g(a) := \sum_{x \in L+u} e^{-\pi a^{-1}||x||^2}$ für $a \geq 1$.
   Zu zeigen ist also $g(a) \leq 2 \cdot a^{\frac{n}{2}} g(1)$.
   Für die Ableitung von g gilt:

$$\begin{aligned}
g'(a) &= \frac{\pi}{a^2} \sum_{x \in L+u} ||x||^2 e^{-\pi a^{-1}||x||^2} \\
&= \frac{\pi}{a^2} \sum_{k=1}^{n} \sum_{x \in L+u} x_k^2 e^{-\pi a^{-1}||x||^2} \\
&\leq \frac{\pi}{a^2} \sum_{k=1}^{n} \frac{a}{\pi} \sum_{x \in L} e^{-\pi a^{-1}||x||^2} \qquad \text{(nach } A.12\text{)} \\
&= \frac{n}{a} \sum_{x \in L} e^{-\pi a^{-1}||x||^2} \\
&\overset{A.2.3}{\leq} \frac{n}{a} a^{\frac{n}{2}} \sum_{x \in L} e^{-\pi ||x||^2} \\
&= n a^{\frac{n}{2}-1} f(1)
\end{aligned}$$

   Damit kann man die Differenz $g(a) - g(1)$ wie folgt abschätzen:

$$\begin{aligned}
g(a) - g(1) &= \int_1^a g'(t)dt \\
&\leq n f(1) \int_1^a t^{\frac{n}{2}-1} dt \\
&= n f(1) \left[\frac{2}{n} t^{\frac{n}{2}} \right]_1^a \\
&= n f(1) \left(\frac{2}{n} a^{\frac{n}{2}} - \frac{2}{n} \right) \\
&= 2 f(1) \left(a^{\frac{n}{2}} - 1 \right) \qquad \text{(A.14)}
\end{aligned}$$

   Die Abbildung τ_L ist positiv definit. Damit gilt:

$$\frac{g(1)}{f(1)} = \frac{\rho(L+u)}{\rho(L)} = \tau_L(u) \leq \tau_L(0) = 1 \Longrightarrow g(1) \leq f(1)$$

   Unter Verwendung der Abschätzung (A.14) für die Differenz $g(a) - g(1)$ erhält man

$$\begin{aligned}
g(a) &\leq 2 f(1)(a^{\frac{n}{2}} - 1) + g(1) \\
&\leq 2 f(1)(a^{\frac{n}{2}} - 1) + f(1) \\
&= 2 a^{\frac{n}{2}} f(1) - f(1) \\
&< 2 a^{\frac{n}{2}} f(1)
\end{aligned}$$

und damit folgt die Behauptung:

$$\sum_{x \in L+u} e^{-\pi a^{-1}||x||^2} \leq 2a^{\frac{n}{2}} \sum_{x \in L} e^{-\pi||x||^2}$$

□

Die folgenden zwei Lemmata werden im Beweis der Transferschranke benötigt. Das erste Lemma wurde von Banaszczyk in [6] bewiesen und beschreibt das Maß auf dem Gitter L beziehungsweise auf $L+u$ im Vergleich zum Maß, wenn man von L beziehungsweise $L+u$ nur Vektoren betrachtet, die eine Länge größer als eine gegebene Konstante haben.

Lemma A.2.6 *Für alle $c \geq \frac{1}{\sqrt{2\pi}}$ gilt:*

1. $\rho\left(L \backslash B(0, c\sqrt{n})\right) < \left(c\sqrt{2\pi e}e^{-\pi c^2}\right)^n \rho(L)$
2. $\rho\left((L+u) \backslash B(0, c\sqrt{n}\right) < 2\left(c\sqrt{2\pi e}e^{-\pi c^2}\right)^n \rho(L)$ *für $u \in \mathbb{R}^n$.*

Beweis:

1. Sei $t \in (0,1)$. Dann ist

$$\begin{aligned}
\sum_{x \in L} e^{-\pi t||x||^2} &= \sum_{x \in L} e^{\pi(1-t)||x||^2} e^{-\pi||x||^2} \\
&> \sum_{x \in L, ||x||^2 \geq c^2 n} e^{\pi(1-t)||x||^2} e^{-\pi||x||^2} \\
&\geq \sum_{x \in L, ||x||^2 \geq c^2 n} e^{\pi(1-t)c^2 n} e^{-\pi||x||^2} \\
&= e^{\pi(1-t)c^2 n} \sum_{x \in L, ||x||^2 \geq c^2 n} e^{-\pi||x||^2}
\end{aligned}$$

Mit Hilfe dieser Abschätzung folgt aus dem ersten Teil von Lemma A.2.5 mit $a = \frac{1}{t} > 1$:

$$\begin{aligned}
\sum_{x \in L} e^{-\pi t||x||^2} &\leq (\frac{1}{t})^{\frac{n}{2}} \sum_{x \in L} e^{-\pi||x||^2} \\
\Longrightarrow e^{\pi(1-t)c^2 n} \sum_{x \in L, ||x||^2 \geq c^2 n} e^{-\pi||x||^2} &< t^{-\frac{n}{2}} \sum_{x \in L} e^{-\pi||x||^2} \\
\Longrightarrow \underbrace{\sum_{x \in L, ||x||^2 \geq c^2 n} e^{-\pi||x||^2}}_{= \rho(L \backslash B(0, c\sqrt{n})} &< t^{-\frac{n}{2}} e^{-\pi(1-t)c^2 n} \underbrace{\sum_{x \in L} e^{-\pi||x||^2}}_{\rho(L)}
\end{aligned}$$

Für $t = (2\pi c^2)^{-1} \in (0,1)$ erhält man dann die gewünschte Behauptung:

$$\begin{aligned}
\rho(L\backslash B(0, c\sqrt{n})) &< (2\pi c^2)^{\frac{n}{2}} e^{-\pi(1-(2\pi c^2)^{-1})c^2 n} \rho(L) \\
&= \left(\sqrt{2\pi} c e^{-\pi c^2} e^{\pi c^2 (2\pi c^2)^{-1}}\right)^n \rho(L) \\
&= \left(\sqrt{2\pi} c e^{-\pi c^2} e^{\frac{1}{2}}\right)^n \rho(L) \\
&= \left(\sqrt{2\pi e} c e^{-\pi c^2}\right)^n \rho(L)
\end{aligned}$$

2. Der Beweis der zweiten Behauptung ist analog zum Beweis der ersten Behauptung. Allerdings verwendet man hier die zweite Behauptung von Lemma A.2.5.
Sei $t \in (0,1)$, $u \in \mathbb{R}^n$. Dann ist

$$\begin{aligned}
\sum_{x \in L+u} e^{-\pi t ||x||^2} &= \sum_{x \in L+u} e^{\pi(1-t)||x||^2} e^{-\pi||x||^2} \\
&> \sum_{x \in L+u, ||x||^2 \geq c^2 n} e^{\pi(1-t)||x||^2} e^{-\pi||x||^2} \\
&\geq \sum_{x \in L+u, ||x||^2 \geq c^2 n} e^{\pi(1-t)c^2 n} e^{-\pi||x||^2} \\
&= e^{\pi(1-t)c^2 n} \sum_{x \in L+u, ||x||^2 \geq c^2 n} e^{-\pi||x||^2}
\end{aligned}$$

Aus dieser Abschätzung und der zweiten Behauptung von Lemma A.2.5 mit $a = \frac{1}{t} > 1$ folgt:

$$\begin{aligned}
\sum_{x \in L+u} e^{-\pi t||x||^2} &\leq 2t^{-\frac{n}{2}} \sum_{x \in L} e^{-\pi||x||^2} \\
\Longrightarrow e^{\pi(1-t)c^2 n} \sum_{x \in L+u, ||x||^2 \geq c^2 n} e^{-\pi||x||^2} &< 2t^{-\frac{n}{2}} \sum_{x \in L} e^{-\pi||x||^2} \\
\Longrightarrow \underbrace{\sum_{x \in L+u, ||x||^2 \geq c^2 n} e^{-\pi||x||^2}}_{= \rho((L+u)\backslash B(0, c\sqrt{n}))} &< 2t^{-\frac{n}{2}} e^{-\pi(1-t)c^2 n} \underbrace{\sum_{x \in L} e^{-\pi||x||^2}}_{\rho(L)}
\end{aligned}$$

Mit $t = (2\pi c^2)^{-1}$ ergibt sich die Behauptung:

$$\begin{aligned}
\Longrightarrow \rho((L+u)\backslash B(0, c\sqrt{n})) &< 2(2\pi c^2)^{\frac{n}{2}} e^{-\pi(1-(2\pi c^2)^{-1})c^2 n}\rho(L) \\
&= 2\left(\sqrt{2\pi}ce^{-\pi c^2}e^{\pi c^2(2\pi c^2)^{-1}}\right)^n \rho(L) \\
&= 2\left(\sqrt{2\pi}ce^{-\pi c^2}e^{\frac{1}{2}}\right)^n \rho(L) \\
&= 2\left(\sqrt{2\pi e}ce^{-\pi c^2}\right)^n \rho(L)
\end{aligned}$$

□

Das folgende Lemma zeigt, dass es bei Betrachtung eines echten Untergitter L_2 des Gitters L_1 mindestens einen Gittervektor $p \in L_2$ gibt, der vom Gitter L_1 einen konstanten Abstand hat.

Lemma A.2.7 *Sei L_1 ein echtes Untergitter von L_2. Dann existiert ein Gittervektor $p \in L_2$ mit*

$$\min_{q \in L_1} ||p - q|| \geq \frac{\lambda_1(L_1)}{3}$$

Da ein Gitter eine diskrete Teilmenge des $\mathbb{R}^n$ ist, wird dieses Minimum angenommen.

Beweis: Der Beweis erfolgt indirekt, das heißt man nimmt an, dass kein $p \in L_2$ existiert mit $\min_{q \in L_1} ||p - q|| \geq \frac{\lambda_1(L_1)}{3}$. Dann gilt für alle $p \in L_2$:

$$\min_{q \in L_1} ||p - q|| < \frac{\lambda_1(L_1)}{3}$$

Damit existiert für $p \in L_2\backslash L_1$ ein Gittervektor $q \in L_1$ mit $||p - q|| < \frac{\lambda_1(L_1)}{3}$.

Setze $u := p - q$. Dann ist $u \in L_2\backslash L_1$, da $||u|| = ||p - q|| < \frac{\lambda_1(L_1)}{3}$ und $u \neq 0$. Damit ist $u \notin L_1$.
Man betrachte die Menge $\{k \cdot u | k \in \mathbb{Z},\ k \geq 1\} \subseteq L_2$ aller ganzzahligen Vielfachen von u.
Nach Voraussetzung existiert für jedes Element $k \cdot u$ dieser Menge ein Gittervektor $q_k \in L_1$ mit

$$||q_k - k \cdot u|| < \frac{\lambda_1(L_1)}{3}$$

Man bezeichnet $k \cdot u$ als assoziiert zu dem Vektor q_k. Da $||u|| < \frac{\lambda_1(L_1)}{3}$, ist u assoziiert zu 0.

Für $k \geq \frac{\lambda_1(L_1)}{3||u||}$ gilt: $||ku|| \geq \frac{\lambda_1(L_1)}{3}$. Damit ist $k \cdot u$ nicht assoziiert zu $0 \in L_1$.
Sei k_0 das kleinste $k \in \mathbb{Z}$, so dass $k \cdot u$ assoziiert zu $z \in L_1\backslash\{0\}$. Dann gilt

- $||z - k_0 \cdot u|| < \frac{\lambda_1(L_1)}{3}$,
- $k_0 \geq 1$, da u assoziiert zu 0,
- $(k_0 - 1) \cdot u$ ist assoziiert zu 0, das heißt $||0 - (k_0 - 1) \cdot u|| < \frac{\lambda_1(L_1)}{3}$.

Also folgt:

$$\begin{aligned} ||z|| &= ||z-0|| \\ &= ||(z-k_0u)+u+((k_0-1)u-0)|| \\ &\leq ||z-k_0u||+||u||+||(k_0-1)u-0|| \\ &< 3\cdot\frac{\lambda_1(L_1)}{3} \\ &= \lambda_1(L_1) \end{aligned}$$

Dies ist ein Widerspruch zur Definition von $\lambda_1(L_1)$, da $z \in L_1$.

□

A.3. Beweis der Transferschranke

Mit Hilfe der im letzten Abschnitt bewiesenen Lemmata kann nun eine Transferschranke von Cai bewiesen werden. Sie stellt eine Relation zwischen der Länge der kürzesten Basis im Gitter L und der Länge der kürzesten Gittervektoren im dualen Gitter L^* her.

Theorem A.3.1 *Für jedes Gitter L der Dimension n und jede Konstante $c > \frac{3}{2\pi}$ gilt für n genügend groß:*

$$\mathrm{bl}(L)\lambda_1(L^*) \leq cn.$$

Beweis: Die Behauptung wird indirekt bewiesen, man nehme also an: $\mathrm{bl}(L)\lambda_1(L^*) > cn$.
Seien c_1, c_2 Konstanten mit

- $c_1 \cdot c_2 = c$
- $c_1 > \frac{1}{\sqrt{2\pi}}$
- $c_2 > \frac{3}{\sqrt{2\pi}}$.

Nach Voraussetzung gilt damit: $c_1 \cdot c_2 > \frac{3}{2\pi}$.

Durch Skalierung des Gitters L mit einem geeigneten Faktor s kann man ohne Einschränkung annehmen:

$$\mathrm{bl}(L) > c_1\sqrt{n}$$
$$\lambda_1(L^*) > c_2\sqrt{n}$$

Sei L' das durch $L \cap B(0, c_1\sqrt{n})$ erzeugte Untergitter von L. L' ist ein echtes Untergitter von L, da $\mathrm{bl}(L) > c_1\sqrt{n}$.

Für den Fall, dass $\dim L' < n$ gilt, sei P der von L' aufgespannte Vektorraum und $b_1, \ldots, b_i$ eine Basis von $L \cap P$ mit $i = \dim L' < n$. Diese Basis kann zu einer Basis $b_1, \ldots, b_i, \ldots, b_n$ für L ergänzt werden. Wenn man L' durch das Untergitter von L, das von den Vektoren $b_1, \ldots, b_i, \ldots, 2b_n$ erzeugt wird, ersetzt, so ist L' ein echtes Untergitter von L der Dimension n.

Man kann also ohne Einschränkung davon ausgehen, dass gilt:
$L' \subset L$ ist ein echtes Untergitter der Dimension n und $L \cap B(0, c_1\sqrt{n}) \subseteq L'$.
Für $u \in \mathbb{R}^n$ gilt:

$$\begin{aligned}
\hat{\sigma}_L(u) &= \frac{\sum_{v\in L} \rho(v) e^{-2\pi i \langle u,v\rangle}}{\sum_{x\in L}\rho(x)} \\
&= \frac{\sum_{v\in L} \rho(v) \cos(2\pi\langle u,v\rangle)}{\sum_{x\in L}\rho(x)} \\
&= \sum_{v\in L} \sigma_L(\{v\}) \cos(2\pi\langle u,v\rangle) \\
&= \sum_{v\in L'} \sigma_{L'}(\{v\}) \cos(2\pi\langle u,v\rangle) + \sum_{v\in L'} (\sigma_L(\{v\}) - \sigma_{L'}(\{v\})) \cos(2\pi\langle u,v\rangle) \\
&\quad + \sum_{v\in L\setminus L'} \sigma_L(v) \cos(2\pi\langle u,v\rangle) \\
&=: \hat{\sigma}_{L'}(\{u\}) + A + B
\end{aligned}$$

mit $A := \sum_{v\in L'} (\sigma_L(\{v\}) - \sigma_{L'}(\{v\})) \cos(2\pi\langle u,v\rangle)$ und $B := \sum_{v\in L\setminus L'} \sigma_L(v)\cos(2\pi\langle u,v\rangle)$. Ziel ist es nun, eine untere Schranke für diese Parameter zu finden.

Die Menge $L \cap B(0, c_1\sqrt{n})$ ist eine echte Teilmenge von L'. Deswegen kann man B unter Verwendung von Lemma A.2.6 wie folgt abschätzen:

$$\begin{aligned}
|B| &= \sum_{v\in L\setminus L'} \sigma_L(v)\cos(2\pi\langle u,v\rangle) \\
&\leq \sum_{v\in L\setminus B(0,c_1\sqrt{n})} \sigma_L(\{v\}) \underbrace{|\cos(2\pi < u,v >)|}_{\leq 1} \\
&= \sigma_L\left(L\setminus B(0,c_1\sqrt{n})\right) \\
&< \left(\underbrace{c_1\sqrt{2\pi e} e^{-\pi c_1^2}}_{=:\,\epsilon_1}\right)^n \\
\Longrightarrow B &> -\epsilon_1^n
\end{aligned}$$

Da L' ein echtes Untergitter von L ist, gilt:

$$\sigma_L(\{v\}) = \frac{e^{-\pi||v||^2}}{\sum_{x\in L} e^{-\pi||x||^2}} < \frac{e^{-\pi||v||^2}}{\sum_{x\in L'} e^{-\pi||x||^2}} = \sigma_{L'}(\{v\})$$

und man erhält folgende Abschätzung:

$$\begin{aligned}
|A| &\leq \sum_{v\in L'} |\sigma_L(\{v\} - \sigma_{L'}(\{v\})| \cdot \underbrace{|\cos(2\pi < u, v >)|}_{\leq 1} \\
&= \sum_{v\in L'} (\sigma_{L'}(\{v\}) - \sigma_L(\{v\})) \\
&= \sum_{v\in L'} e^{-\pi||v||^2} \left(\frac{1}{\sum_{x\,\in\, L'} e^{-\pi||x||^2}} - \frac{1}{\sum\limits_{x\in L} e^{-\pi||x||^2}} \right) \\
&= \sum_{v\in L'} e^{-\pi||v||^2} \frac{\sum\limits_{z\in L\setminus L'} e^{-\pi||z||^2}}{\sum\limits_{x\in L'} e^{-\pi||x||^2} \cdot \sum\limits_{y\in L} e^{-\pi||y||^2}} \\
&= \frac{\sum\limits_{z\in L\setminus L'} e^{-\pi||z||^2}}{\sum\limits_{y\in L} e^{-\pi||y||^2}} \\
&= \sum_{z\in L\setminus L'} \sigma_L(\{z\})
\end{aligned}$$

Es wurde bereits im Zusammenhang mit der Abschätzung von B gezeigt:

$$\sum_{z\in L\setminus L'} \sigma_L(\{z\}) \leq \sum_{v\in L\setminus B(0,c_1\sqrt{n})} \sigma_L(\{v\}) < \epsilon_1^n$$

Damit gilt auch:

$$|A| < \epsilon_1^n \Longrightarrow A \geq -\epsilon_1^n$$

Insgesamt erhält man also:

$$\hat{\sigma}_L(\{u\}) = \hat{\sigma}_{L'}(\{u\}) + A + B > \hat{\sigma}_{L'}(\{u\}) - 2\epsilon_1^n \tag{A.15}$$

Ziel ist es nun, $u \in \mathbb{R}^n$ so zu wählen, dass man mit Hilfe der Ungleichung (A.15) einen Widerspruch erhält. Wegen Korollar A.2.3 kann man für die Wahl des Vektors $u \in \mathbb{R}^n$ auch die Funktionen τ_{L^*} und $\tau_{L'^*}$ betrachten, denn es ist $\hat{\sigma}_L(\{u\}) = \tau_{L^*}(\{u\})$ und $\hat{\sigma}_{L'}(\{u\}) = \tau_{L'^*}(u)$.

Da L' ein volldimensionales, echtes Untergitter von L ist, ist L^* – nach Definition des dualen Gitters – L^* ein echtes Untergitter von L'^*. Dies folgt aus

$$\frac{\det L'^*}{\det L^*} = \frac{\det L}{\det L'} > 1$$

Nach Lemma A.2.7 existiert $u \in L'^*$ mit $\min_{q\in L^*} ||u - q|| \geq \frac{\lambda_1(L^*)}{3}$.

Da $u \in L'^*$ gilt: $L'^* + u = L'^*$ und es ist:

$$\begin{aligned}
\tau_{L'^*}(u) &= \frac{\sum\limits_{y \in L'^* + u} e^{-\pi ||y||^2}}{\sum\limits_{x \in L'^*} e^{-\pi ||x||^2}} \\
&= \frac{\sum\limits_{y \in L'^*} e^{-\pi ||y||^2}}{\sum\limits_{x \in L'^*} e^{-\pi ||x||^2}} \\
&= 1
\end{aligned} \tag{A.16}$$

Andererseits gilt nach Wahl von c_2:

$$\min_{q \in L^*} ||u - q|| \geq \frac{\lambda_1(L^*)}{3} > \frac{c_2}{3}\sqrt{n}$$

Damit existiert kein $x \in L^* + u$ mit $||x|| > \frac{c_2}{3}\sqrt{n}$ und es folgt nach Lemma A.2.6:

$$\begin{aligned}
\tau_{L^*}(u) &= \frac{\sum\limits_{v \in L^* + u} e^{-\pi ||v||^2}}{\sum\limits_{x \in L^*} e^{-\pi ||x||^2}} \\
&= \frac{\sum\limits_{v \in (L^* + u) \setminus B(0, \frac{c_2}{3}\sqrt{n})} e^{-\pi ||v||^2}}{\sum\limits_{x \in L^*} e^{-\pi ||x||^2}} \\
&< 2\left(\frac{c_2}{3}\sqrt{2\pi e} \cdot e^{-\pi \left(\frac{c_2}{3}\right)^2}\right)^n \\
&=: 2\epsilon_2^n
\end{aligned} \tag{A.17}$$

Nach Voraussetzung gilt $c_1 > \frac{1}{\sqrt{2\pi}}$, das heißt $\sqrt{2\pi} > c_1^{-1}$. Damit erhält man für ϵ_1 die Abschätzung:

$$\epsilon_1 = c_1\sqrt{2\pi e}e^{-\pi c_1^2} < c_1 c_1^{-1}\sqrt{e}e^{-\pi\frac{1}{2\pi}} = 1$$

Des Weiteren gilt nach Voraussetzung $\frac{c_2}{3} > \frac{1}{\sqrt{2\pi}}$, also $\sqrt{2\pi} > \frac{3}{c_2}$. Damit erhält man für ϵ_2 die Abschätzung:

$$\epsilon_2 = \frac{c_2}{3}\sqrt{2\pi e}e^{-\pi\left(\frac{c_2}{3}\right)^2} < \frac{c_2}{3} \cdot \frac{3}{c_2}\sqrt{e}e^{-\frac{1}{2}} = 1$$

Aus

- $\hat{\sigma}_L(\{u\}) > \hat{\sigma}_{L'}(\{u\}) - 2\epsilon_1^n$ (A.15),
- $\tau'_L(u) = \hat{\sigma}_{L'}(\{u\}) = 1$ (A.16) und
- $\hat{\sigma}_L(\{u\}) = \tau_{L^*}(u) < 2\epsilon_2^n$ (A.17)

folgt insgesamt:

$$\begin{aligned} & \hat{\sigma}_L(\{u\}) > \hat{\sigma}_{L'}(\{u\}) - 2\epsilon_1^n \\ \Longrightarrow \quad & 2\epsilon_2^n > 1 - 2\epsilon_1^n \\ \Longrightarrow \quad & 2\underbrace{\epsilon_2^n}_{\to 0} + 2\underbrace{\epsilon_1^n}_{\to 0} > 1 \end{aligned}$$

Dies bedeutet einen Widerspruch, da $\epsilon_2 < 1$ und $\epsilon_1 < 1$ und damit $0 > 1$.
Also gilt die Behauptung:

$$\mathrm{bl}(L)\lambda_1(L^*) \leq c \cdot n$$

□

Anhang B.

Literatur

[1] Ajtai, Miklós: The shortest vector problem in L_2 is NP-hard for randomized reductions. In: *Proceedings of the 30th ACM Symposium on Theory of Computing*, 1998, S. 10 – 19

[2] Ajtai, Miklós ; Kumar, Ravi ; Sivakumar, D.: A sieve algorithm for the shortest lattice vector problem. In: *Proceedings of the 33th ACM Symposium on Theory of Computing*, 2001, S. 601–610

[3] Ajtai, Miklós ; Kumar, Ravi ; Sivakumar, D.: Sampling short lattice vectors and the closest lattice vector problem. In: *Proceedings of the 17th IEEE Annual Conference on Computational Complexity - CCC*, 53 – 57

[4] Arora, Sanjeev ; Babai, László ; Stern, Jacques ; Sweedyk, Z.: The hardness of approximate optimia in lattices, codes, and systems of linear equations. In: *IEEE Symposium on Foundations of Computer Science*, 1993, S. 724 – 733

[5] Babai, László: On Lovász' lattice reduction and the nearest lattice point problem. In: *Combinatorica* 6 (1986), Nr. 1, S. 1 – 13

[6] Banaszczyk, Wojciech: New bounds in some transference theorems in the geometry of numbers. In: *Mathematische Annalen* 296 (1993), Nr. 4, S. 625 – 635

[7] Blömer, Johannes: Closest vectors, successive minima, and dual HKZ-bases of lattices. In: *Proceedings of the 17th ICALP, Lecture Notes in Computer Science 1853*, Springer, 248 – 259

[8] Cai, Jin-Yi: A new transference theorem and applications to Ajtai's connection factor. In: *Electronic Colloquium on Computational Complexity (ECCC)* 5 (1998), Nr. 5

[9] Cai, Jin-Yi ; Nerurkar, Ajay: An improved worst-case to average-case connection for lattice problems. In: *IEEE Symposium on Foundations of Computer Science*, 1997, S. 468 – 477

[10] Cassels, J. W. S.: *An Introduction to the Geometry of Numbers.* Springer, 1971

[11] Conway, John B.: *Functions of One Comple Variable.* Springer, 1973

[12] Dinur, Irit ; Kindler, Guy ; Safra, Shmuel: Approximating-CVP to within almost-polynomial factors is NP-hard. In: *IEEE Symposium on Foundations of Computer Science*, 1998, S. 99 – 111

[13] Dyer, Martin ; Frieze, Alan M. ; Kannan, Ravi: A random polynomial time algorithm for approximating the volume of convex bodies. In: *Journal of the ACM* 38 (1991), Nr. 1, S. 1 – 17

[14] Ebeling, Wolfgang: *Lattices and Codes - A Course Partially Based on Lectures by F. Hirzebruch*. Vieweg, 1994

[15] Emde Boas, Peter van: Another NP - complete partition problem and the complexity of computing short vectors in a lattice / Department of Mathematics, University of Amsterdam. 1981 (81 – 04). – Forschungsbericht

[16] Fischer, Wolfgang ; Lieb, Ingo: *Funktionentheorie*. Vieweg, 1994

[17] Forster, Otto: *Analysis 3 - Integralrechnung im $\mathbb{R}^n$ mit Anwendungen*. Vieweg, 1984

[18] Goldreich, Oded ; Micciancio, Daniele ; Safra, Shmuel ; Seifert, Jean-Pierre: Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. In: *Information Processing Letters* 71 (1999), Nr. 2, S. 55 – 61

[19] Helfrich, Bettina: Algorithms to construct Minkowski reduced and Hermite reduced bases. In: *Theoretical Computer Science* 41 (1985), S. 125 – 139

[20] Hilbert, David (Hrsg.): *Gesammelte Abhandlungen von Hermann Minkowski*. Chelsea Publishing Company, 1911

[21] Kannan, Ravi: Algorithmic geometry of numbers. In: *Annual Reviews in Computer Science* 2 (1987), S. 231 – 267

[22] Kannan, Ravi: Minkowski's convex body theorem and integer programming. In: *Mathematics of Operations Research* 12 (1987), Nr. 3, S. 415 – 440

[23] Khanevsky, Michael: *Lecture 8: $2^{\mathcal{O}(n)}$-time algorithm for SVP*. Version: 2004. `http://www.cs.tau.ac.il/~odedr/goto.php?name=ln_svpalg&link=teaching/lattices_fall_2004/ln/svpalg.pdf`. – Online Ressource, Abruf: 19. Februar 2006

[24] Khot, Subhash: Hardness of Approximating the Shortest Vector Problem in Lattices. In: *Journal of the ACM (JACM)* 52 (2005), Nr. 5, S. 789–808

[25] Kol, Gillat ; Regev, Oded (Hrsg.): *Lecture 9: Fourier Transform*. Version: 2004. `http://www.cs.tau.ac.il/~odedr/goto.php?name=ln_fourier&link=teaching/lattices_fall_2004/ln/FourierTransform.pdf`. – Online Ressource, Abruf: 19. Februar 2006

[26] Lenstra, A.K. ; Lenstra, H. W. ; Lovász, L.: Factoring polynomials with rational coefficients. In: *Mathematische Annalen* 261 (1982), S. 515–534

[27] Lenstra, H. W.: Integer programming with a fixed number of variables / Department of Mathematics, University of Amsterdam. 1981 (81 – 03). – Forschungsbericht

[28] Micciancio, Daniele ; Goldwasser, Shafi: *Complexity of Lattice Problems - A Cryptographic Perspective*. Kluwer Academic Publishers, 2002

[29] Schnorr, Claus-Peter: A hierarchy of polynomial time lattice basis reduction algorithms. In: *Theoretical Computer Science* 53 (1987), S. 201 – 224

[30] Schnorr, Claus-Peter: Block reduced lattice bases and successive minima. In: *Combinatorics, Probability & Computing* 3 (1994), S. 507 – 522