Komplexität von Gitterproblemen: Nicht-Approximierbarkeit und Grenzen der Nicht-Approximierbarkeit

Dissertation
zur Erlangung des Doktorgrades
der Naturwissenschaften

vorgelegt beim Fachbereich Mathematik
der Johann Wolfgang Goethe-Universität
in Frankfurt am Main

von
Jean-Pierre Seifert
aus Berlin-Wilmersdorf

Frankfurt 2000
(D F 1)

ZUSAMMENFASSUNG. Ein Gitter vom Rang n ist die Menge der ganzzahligen Linerkombinationen von n linear unabhängigen Vektoren im $\mathbb{R}^m$. Unter der Annahme $\mathsf{P} \neq \mathsf{NP}$ beweisen wir, daß kein Polynomialzeit-Algorithmus existiert, der eine kürzeste Gitterbasis bis auf einen Faktor $n^{O(1/\log\log n)}$ berechnet, wobei die Länge einer Menge von Vektoren durch die maximale Euklidische Länge der Vektoren definiert ist. Weiter zeigen wir, daß eine Verbesserung dieses Resultates bis hin zu einem Faktor $n/\sqrt{\log n}$ unter plausiblen Annahmen nicht möglich ist.

Ein simultaner Diophantischer Best Approximations Nenner für reelle Zahlen $\alpha_1, \ldots, \alpha_n$ und Hauptnennerschranke N ist eine natürliche Zahl q mit $1 \leq q \leq N$, so daß $\max_i \min_{p\in\mathbb{Z}} |q\alpha_i - p|$ minimal ist. Unter der Annahme, daß die Klasse NP keine fast-polynomiellen Algorithmen besitzt, beweisen wir, daß kein Polynomialzeit-Algorithmus existiert, der für gegebene rationale Zahlen $\alpha_1, \ldots, \alpha_n$ und eine Hauptnennerschranke N einen Nenner $\tilde{q}$ mit $1 \leq \tilde{q} \leq f(n)N$ berechnet, so daß $\tilde{q}$ bis auf einen Faktor $f(n) = n^{O(1/\log^{0.5+\varepsilon} n)}$ ein Best Approximations Nenner ist, wobei $\varepsilon > 0$ eine beliebige Konstante ist. Wir zeigen, daß eine Verbesserung dieses Resultates bis hin zu einem Faktor $n/\log n$ unter plausiblen Annahmen nicht möglich ist.

Wir untersuchen die Konsequenzen dieser Resultate zur Konstruktion von im Durchschnitt schwierigen Gitterproblemen.

vom Fachbereich Mathematik der
Johann Wolfgang Goethe-Universität als Dissertation angenommen.

Dekan: Prof. Dr. R. Bieri
Gutachter: Prof. Dr. C. P. Schnorr, Prof. Dr. J. Buchmann
Datum der Disputation: 16.2.2000

Inhaltsverzeichnis

Einleitung

Ein Gitter im $\mathbb{R}^m$ vom Rang n ist die Menge der ganzzahligen Linearkombinationen von n linear unabhängigen Vektoren im $\mathbb{R}^m$. Die Auswahl einer Basis für ein Gitter aus der unendlichen Menge seiner Gitterbasen, die aus möglichst kurzen Vektoren besteht, bezeichnet man als Gitterbasenreduktion.

Gitter bzw. ***Gitterbasenreduktionen*** werden seit über 200 Jahren auf Grund ihrer Verbindungen zur Zahlentheorie und insbesondere zur Diophantischen Approximation untersucht. Auch diese Arbeit beinhaltet einen Zusammenhang zwischen Gittern und Diophantischen Approximationen: in einem ersten Teil wird die Komplexität von Gitterproblemen untersucht und in einem zweiten Teil wird mit ähnlichen Methoden die Komplexität von Diophantischen Approximationsproblemen untersucht.

Der Zusammenhang zwischen Gittern und Diophantischen Approximationen motivierte früh eine algorithmische Betrachtung von Gittern. Bereits Gauss [**Gau**] gab 1801 einen effizienten Algorithmus zur Gitterbasenreduktion für Gitter vom Rang 2 an. Hierauf folgten die grundlegenden Arbeiten von Hermite [**Her**], Korkin und Zolotarev [**KZ1, KZ2, KZ3**] und Minkowski [**Min1**] zur Gitterbasenreduktion für Gitter beliebigen Ranges — allerdings ohne Angaben von Algorithmen zur effizienten Konstruktion entsprechender Basen. Der anfänglichen algorithmischen Betrachtung von Gittern folgte nun eine intensive Phase der theoretischen Grundlagenforschung, die 1910 von Minkowski [**Min2**] zum Gebiet der *Geometrie der Zahlen* formiert wurde.

Erst wieder im Jahre 1982 wurde durch den LLL-Algorithmus von Lenstra, Lenstra und Lovasz [**LLL**] zur effizienten Gitterbasenreduktion ein entscheidender algorithmischer Durchbruch für die Geometrie der Zahlen erzielt. Der LLL-Algorithmus lieferte u.a. effiziente Algorithmen zur ganzzahligen Linearen

Programmierung bei fester Anzahl von Variablen, Faktorisierung von Polynomen über den rationalen Zahlen, über endlichen Körpern und algebraischen Zahlkörpern, Widerlegung der Mertens Vermutung, Auflösbarbeit von Radikalausdrücken, zum Brechen des Merkle-Hellman Kryptosystems, Finden kleiner Lösungen von polynomialen Gleichungen, zur Kryptanalyse kryptographischer Probleme, und insbesondere für Diophantische Approximationsprobleme. Diese universelle Anwendbarkeit des LLL-Algorithmus in vielen Gebieten der Informatik, Mathematik und Kryptographie motivierte algorithmische Untersuchungen von Gitterproblemen, und führte zur *algorithmischen Geometrie der Zahlen* (siehe Kannan [**Kan2**] bzw. Lovasz [**Lov**]).

Die überraschende Entdeckung eines Zusammenhangs zwischen dem Worst-Case und dem Average-Case Rechenaufwand für bestimmte Gitterprobleme im Jahre 1996 durch Miklos Ajtai [**Ajt1, Ajt3**] brachte neue Bewegung in die algorithmische Geometrie der Zahlen. Die von Ajtai intendierte kryptographische Anwendung dieses bemerkenswerten Resultates zielt auf ein interessantes kryptographisches Projekt.

Die Sicherheit kryptographischer Verfahren erfordert für zufällige Instanzen des zugrundeliegenden Berechnungsproblems einen hohen Average-Case Rechenaufwand. Wünschenswert wäre daher eine explizite hohe untere Schranke für den Average-Case Rechenaufwand zum Brechen der Verfahren. Bis heute kann man jedoch keine solche untere Schranke für den Average-Case Rechenaufwand beweisen, selbst wenn man $\mathsf{P} \neq \mathsf{NP}$ annimmt. Ein Berechnungsproblem Φ heißt NP-hart, wenn mittels eines effizienten Algorithmus für Φ jedes NP-Problem effizient gelöst werden kann. Ein Beweis für die NP-Härte eines Problems Φ ist eine untere Worst-Case Komplexitätsschranke für Φ, sofern $\mathsf{P} \neq \mathsf{NP}$ gilt. NP-Hardness Beweise beinhalten jedoch keine unteren Average-Case Komplexitätsschranken wie sie etwa für die Kryptographie angemessen sind.

Miklos Ajtai [**Ajt1**] gelang nun erstmals der Nachweis einer unteren Average-Case Komplexitätsschranke unter der Voraussetzung, daß gewisse Gitterprobleme NP-hart sind. Er zeigte für eine natürliche Klasse Λ_n, $n \in \mathbb{N}$, von Gittern:

Existiert ein effizienter probabilistischer Algorithmus zur Berechnung kurzer nicht trivialer Vektoren in uniform gewählten Gittern aus Λ_n, so gibt es Konstanten c_0, c_1, c_2 und einen effizienten probabilistischen Algorithmus, der für ein beliebiges Gitter L vom Rang n folgende Probleme löst:

> Shortest Independent Vectors Problem (Sivp).
> *Finde in L n bis auf einen Faktor n^{c_0} kürzeste linear unabhängige Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$, wobei die Länge einer Menge von Vektoren durch $\max_{1 \leq i \leq n} \|\mathbf{v}_i\|$ definiert ist.*

SHORTEST BASIS PROBLEM (SBP).
Finde für das Gitter L *eine bis auf einen Faktor* n^{c_1} *kürzeste Basis* $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$, *wobei die Länge einer Basis durch* $\max_{1 \leq i \leq n} \|\mathbf{b}_i\|$ *definiert ist.*

SHORTEST VECTOR PROBLEM (SVP).
Berechne bis auf einen Faktor n^{c_2} *die Länge eines kürzesten von Null verschiedenen Vektors in* L.

Durch eine verbesserte Analyse von [**Ajt1**] zeigten Cai and Nerurkar [**CN**], daß das obige Theorem für $c_0 > 3$, $c_1 > 3.5$ und $c_2 > 4$ gilt. Die Faktoren n^{c_0}, n^{c_1} bzw. n^{c_2} sind die sog. Approximationsfaktoren des SIVP, SBP bzw. SVP in Ajtai's Theorem.

Die Frage ist nun, für welchen Faktor f_0, f_1 bzw. f_2 die Approximation des SIVP, des SBP bzw. des SVP NP-hart ist? Den Faktor f_i bezeichnet man als Nicht-Approximierbarkeitsfaktor des entsprechenden Problems, da ein effizienter Approximationsalgorithmus mit einem Faktor f_i der Annahme $\mathsf{P} \neq \mathsf{NP}$ widersprechen würde.

Erstmals zeigte Daniele Micciancо [**Mic**] 1998 für das SVP einen Nicht-Approximierbarkeitsfaktor nahe $\sqrt{2}$. Dieser Nicht-Approximierbarkeitsfaktor für das SVP ist allerdings weit von dem für Ajtai's Theorem erforderlichen Approximationsfaktor n^{c_2} mit $c_2 > 4$ entfernt. In der Tat ist es unter vernünftigen Annahmen nicht möglich mit Ajtai's Theorem NP-harte Instanzen des SVP auf Average-Case Instanzen des SVP zu reduzieren. Unter einer gittertheoretischen Annahme ist nämlich der Approximationsfaktor n^{c_2} für das SVP in Ajtai's Theorem nach unten durch n beschränkt. Und andererseits zeigen Goldreich und Goldwasser [**GG**] unter einer vernünftigen komplexitätstheoretischen Annahme, daß das SVP für einen Approximationsfaktor $\sqrt{n/\log(n)}$ nicht mehr NP-hart ist. Ein solches Resultat, das Grenzen für Nicht-Approximierbarkeitsfaktoren beweist, bezeichnet man als Grenze der Nicht-Approximierbarkeit.

Da eine Reduktion eines NP-harten Problems auf ein Average-Case Problem für das SVP unmöglich erscheint, und die Approximationsfaktoren in Ajtai's Theorem für das SIVP und das SBP kleiner sind, erscheinen diese Probleme für eine erfolgreiche Worst-Case/Average-Case Reduktion attraktiver. Das Hauptziel der vorliegenden Arbeit ist daher die Untersuchung der Komplexität des SIVP und des SBP, da diese bisher noch nicht behandelt worden ist.

Wir zeigen zunächst die NP-Hardness des SIVP und des SBP. Anschließend beweisen wir, daß selbst die Approximation bis auf einen Faktor $n^{O(1/\log\log n)}$ für das SIVP und das SBP NP-hart ist.

Auf der anderen Seite zeigen wir aber auch Grenzen für die Nicht-Approximierbarkeit des SIVP und des SBP. Wir beweisen, daß die Approximation

des SIVP bzw. des SBP bis auf einen Faktor $O(n)$ bzw. $O(n^{1.5})$ unter Karp-Reduktionen nicht NP-hart ist, es sei denn NP = co-NP. Weiter zeigen wir, daß die Approximation der Probleme SIVP und SBP bis auf einen Faktor $n/O(\sqrt{\log n})$ unter Karp-Reduktionen nicht mehr NP-hart ist, es sei denn, daß die Polynomialzeit-Hierarchie auf der zweiten Stufe kollabiert.

Die in dieser Arbeit bewiesenen Nicht-Approximierbarkeitsfaktoren für das SIVP und das SBP sind signifikant näher an den in Ajtai's Theorem erforderlichen Approximationsfaktoren als die für das SVP bekannten Nicht-Approximierbarkeitsfaktoren. Insbesondere lösen unsere Resultate ein ungelöstes Problem aus Ajtai [**Ajt3**, Seite 427]. Dennoch erreichen die bewiesenen Nicht-Approximierbarkeitsfaktoren für das SIVP und das SBP nicht die in Ajtai's Theorem erforderlichen Werte.

Andererseits zeigen die von uns bewiesenen Grenzen für die Nicht-Approximierbarkeit des SIVP und des SBP folgendes: Die in der jetzigen Form von Ajtai's Theorem geforderten Approximationsfaktoren n^{c_0} und n^{c_1} mit $c_0 > 3$ und $c_1 > 3.5$ für das SIVP und das SBP sind überhaupt nicht erreichbar! Eine erfolgreiche Reduktion eines NP-harten Worst-Case Problems auf ein Average-Case Problem hängt also entscheidend davon ab, ob der Approximationsfaktor n^{c_0} in Ajtai's Theorem für das SIVP erheblich verbessert werden kann.

Simultane Diophantische Approximation ist das Studium der Approximationseigenschaften reeller Zahlen $\alpha_1, \ldots, \alpha_n$ durch rationale Zahlen $\frac{p_1}{q}, \ldots, \frac{p_n}{q}$ mit einem gemeinsamen Hauptnenner q. Diophantische Approximationen stehen in direktem Zusammenhang mit Gittern und und deren Anwendungen in der Kryptographie. Von besonderem Interesse ist hierbei die sog.

> BEST SIMULTANEOUS DIOPHANTINE APPROXIMATION (BSDA).
> *Finde zu gegebenen reellen Zahlen $\alpha_1, \ldots, \alpha_n$ sowie einer Hauptnennerschranke N eine natürliche Zahl q mit $1 \leq q \leq N$, so daß $\max_i \min_{p_i \in \mathbb{Z}} |q\alpha_i - p_i|$ minimal ist; q wird Best Approximations Nenner genannt.*

Beispielsweise reduziert Wiener [**Wie**] das Brechen des Public-Key-Verschlüsselungsverfahrens, RSA, mit einem *kurzen* geheimen Schlüssel auf ein eindimensionales BSDA Problem.

Der Kettenbruchalgorithmus bietet für $n = 1$ ein effizientes Verfahren zur Lösung des BSDA Problems, und für festes n kann das BSDA Problem mit Hilfe des LLL-Algorithmus ebenfalls effizient gelöst werden. Für beliebiges n ist kein effizienter Algorithmus bekannt und auch nicht zu erwarten, da Lagarias [**Lag**] die NP-Hardness des BSDA Problems zeigte. Lagarias gab aber einen auf dem LLL-Algorithmus basierenden effizienten Approximationsalgorithmus an.

Dieser berechnet zu gegebenen rationalen Zahlen $\alpha_1, \ldots, \alpha_n$ und einer Hauptnennerschranke N in Polynomial-Zeit einen Nenner $\tilde{q}$ mit $1 \leq \tilde{q} \leq 2^{n/2}N$, der bis auf einen Faktor $\sqrt{5n}2^{(n-1)/2}$ ein Best Approximations Nenner ist.

Gleichzeitig stellte Lagarias bzgl. einer möglichen Verbesserung hinsichtlich polynomieller Faktoren allerdings folgende Vermutung auf: Existiert ein Polynomial-Zeit Algorithmus, der für gegebene rationale Zahlen $\alpha_1, \ldots, \alpha_n$ und eine Hauptnennerschranke N einen Nenner $\tilde{q}$ mit $1 \leq \tilde{q} \leq f(n)N$ berechnet, so daß $\tilde{q}$ bis auf einen polynomiellen Faktor $f(n)$ ein Best Approximations Nenner ist, so folgt $\mathsf{P} = \mathsf{NP}$. Die komplexitätstheoretische Untersuchung dieser Vermutung von Lagarias bzgl. der Approximierbarkeit von simultanen Diophantischen Best-Approximationen ist ein weiteres Ziel dieser Arbeit.

Unter der Annahme, daß die Klasse NP keine fast-polynomiellen Algorithmen besitzt, beweisen wir zunächst: Es existiert kein Polynomialzeit-Algorithmus, der für gegebene rationale Zahlen $\alpha_1, \ldots, \alpha_n$ und eine Hauptnennerschranke N einen Nenner $\tilde{q}$ mit $1 \leq \tilde{q} \leq f(n)N$ berechnet, so daß $\tilde{q}$ bis auf einen Faktor $f(n) = n^{O(1/\log^{0.5+\varepsilon} n)}$ ein Best Approximations Nenner ist, wobei $\varepsilon > 0$ eine beliebige Konstante ist. Dieses Resultat kommt der Vermutung von Lagarias sehr nahe und kann als deren Bestätigung betrachtet werden.

Andererseits zeigen wir aber auch Grenzen für die Nicht-Approximierbarkeit. Unter der Annahme, daß die Polynomialzeit-Hierachie nicht auf der zweiten Stufe kollabiert, beweisen wir: Für $f(n) = n/(c \log n)$ mit beliebigem $c < 1/2$ stimmt die Vermutung von Lagarias nicht! Die Approximation eines Best Approximations Nenners bis auf einen Faktor $n/O(\log n)$ ist also nicht mehr NP-hart.

Die vorliegende Dissertation stellt in vier Kapiteln eine Auswahl von drei meiner weiter unten aufgeführten wissenschaftlichen Arbeiten in einem einheitlichen Rahmen dar. Gleichzeitig gibt sie eine Einführung in die Worst-Case/Average-Case Reduktion von Ajtai und erläutert in diesem Zusammenhang die Relevanz der hier vorgestellten Ergebnisse für die aktuelle Gitterforschung.

Kapitel 1 führt Grundlagen sowie Notationen aus der Gittertheorie, der Theorie der Diophantischen Approximationen, der Komplexitätstheorie und der Interaktiven Protokolle ein. Kapitel 2 beinhaltet die komplexitätstheoretischen Untersuchungen des SIVP und des SBP aus [**BSei**] und benutzt ein Ergebnis aus [**GMSS**]. Kapitel 3 beweist zunächst die Nicht-Approximierbarkeit des BSDA aus [**RSei1**] und greift hierzu auf ein Ergebnis der Arbeit [**RSei3**] zurück. Anschließend wird in Kapitel 3 eine Grenze für die Nicht-Approximierbarkeit des BSDA bewiesen. Dieses Resultat stammt aus der Arbeit [**Sei**]. Kapitel 4 untersucht am skizzierten Beweis von Ajtai's Theorem die Konsequenzen der

Resultate aus Kapitel 2 zur Konstruktion von im Durchschnitt schwierigen Gitterproblemen.

Im Rahmen des DFG Leibniz Programms Schn 143/5-1, sowie aus Einladungen zu Forschungsaufenthalten an der Eidgenössischen Technischen Hochschule Zürich (Zürich, Schweiz), University of Queensland (Brisbaine, Australia) und am Massachusetts Institute of Technology (Boston, USA) entstanden folgende Publikationen:

- On the Complexity of Computing Short Linearly Independent Vectors and Short Bases in a Lattice, [**BSei**].
- On Routing in Circulant Graphs, [**CHM**$^+$].
- Tensor-based Trapdoors for CVP and their Applications to Public-Key Cryptography, [**FS**].
- Approximating shortest lattice vectors is not harder than approximating closest lattice vectors, [**GMSS**].
- The complexity of the extended GCD problem, [**HavS**].
- Extending Wiener's attack in the presence of many decrypting exponents, [**HowS**].
- Approximating Good Simultaneous Diophantine Approximations is almost NP-hard, [**RSei1**].
- The Complexity of Approximate Optima for Greatest Common Divisor Computations, [**RSei2**].
- On the hardness of approximating shortest integer relations among rational numbers, [**RSei3**].
- Arthur, Merlin and Dirichlet debate diophantine approximations, [**Sei**].

Die obigen Arbeiten untersuchen die Komplexität von Gitterproblemen bzw. Diophantischen Approximationsproblemen oder verwenden Gitterbasenreduktionen bzw. Diophantische Approximationen zur Lösung kryptographischer Fragestellungen.

Kapitel 1

Grundlagen

In Paragraph 1 dieses Kapitels werden grundlegende Begriffe und Sätze der Gittertheorie eingeführt, und Paragraph 2 wiederholt einige Begriffe zu Diophantischen Approximationen. Aus der Komplexitätstheorie benötigte Begriffe und Sätze, wie z.B. Gaps und Promise-Probleme, werden in Paragraph 3 vorgestellt. Schließlich wird in Paragraph 4 das Modell des interaktiven Protokolls und ein wichtiger Satz aus der Theorie der interaktiven Protokolle behandelt.

1.1. Gittertheorie

In dieser Arbeit bezeichnet $\mathbb{R}^m$ bzw. $\mathbb{Q}^m$ den m-dimensionalen Euklidischen Vektorraum über $\mathbb{R}$ bzw. $\mathbb{Q}$ mit dem Euklidischen inneren Produkt $\langle \cdot, \cdot \rangle$ und der Euklidischen Norm $\|\mathbf{v}\|^2 = \sum_{i=1}^{m} \mathrm{v}_i^2$. Für einen Vektor $\mathbf{v} \in \mathbb{R}^m$ bezeichnet $\|\mathbf{v}\|_\infty = \max_{1 \le i \le m} |\mathrm{v}_i|$ die Maximimum-Norm. Für Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{R}^m$ bezeichnen wir mit $[\mathbf{v}_1, \ldots, \mathbf{v}_n]$ die geordnete Menge dieser Vektoren und mit $\mathrm{span}(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ den von ihnen aufgespannten Untervektorraum. Mit $\dim(U)$ bezeichnen wir die Dimension und mit $U^\perp$ das orthogonale Komplement eines Untervektorraumes $U \subseteq \mathbb{R}^m$.

Definition 1.1. Ein *Gitter* ist eine diskrete additive Untergruppe L des $\mathbb{R}^m$. Der *Rang* $\mathrm{rg}(\mathsf{L})$ von L ist die Dimension des Untervektorraumes $\mathrm{span}(\mathsf{L})$.

Jedes Gitter L vom Rang n besitzt eine *Basis*, d.h. eine Menge von n linear unabhängigen Vektoren $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ mit

$$\mathsf{L} = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \mid x_i \in \mathbb{Z} \right\}.$$

Das von der Basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ *aufgespannte Gitter* wird mit $\mathsf{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ bezeichnet. Die folgende Proposition zeigt (siehe z.B. [**Cas1**]), daß die Basis eines Gitters nicht eindeutig bestimmt ist.

Proposition 1. *Sei* $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ *eines Basis eines Gitters* $\mathsf{L} \subseteq \mathbb{R}^m$. *Dann ist* $[\mathbf{b}'_1, \ldots, \mathbf{b}'_n]$ *genau dann eine Basis von* L, *wenn eine unimodulare* $n \times n$*-Matrix* T *mit* $[\mathbf{b}_1, \ldots, \mathbf{b}_n] = [\mathbf{b}'_1, \ldots, \mathbf{b}'_n] \cdot T$ *existiert.*

Die Determinante eines Gitters ist unabhängig von der Basis.

Definition 1.2. Sei $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ eine Basis eines Gitters $\mathsf{L} \subseteq \mathbb{R}^m$. Die *Gitterdeterminante* $\det(\mathsf{L})$ von L ist definiert durch $\det(\mathsf{L})^2 := \det[\langle \mathbf{b}_i, \mathbf{b}_j \rangle]_{1 \le i,j \le n}$.

Definition 1.3. Für ein Gitter L ist das zu L *duale Gitter* L^* definiert durch $\mathsf{L}^* := \{\mathbf{w} \in \mathrm{span}(\mathsf{L}) \mid \langle \mathbf{w}, \mathbf{v} \rangle \in \mathbb{Z} \text{ für alle } \mathbf{v} \in \mathsf{L}\}$.

Ist L ein Gitter mit Basis $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$, so gibt es eine eindeutig bestimmte Basis $B^* = [\mathbf{b}^*_1, \ldots, \mathbf{b}^*_n]$ von L^* mit

$$\langle \mathbf{b}_i, \mathbf{b}^*_j \rangle = \begin{cases} 1 & \text{falls } i + j = n + 1, \\ 0 & \text{sonst.} \end{cases}$$

Wir nennen die Basis B^* des Gitters L^* die *zu B duale Basis*. Zur Definition weiterer Konstanten eines Gitters, den sog. sukzessiven Minima eines Gitters, bezeichnen wir mit

$$B_r(\mathbf{p}) := \{\mathbf{v} \in \mathbb{R}^m \mid \|\mathbf{p} - \mathbf{v}\| \le r\}$$

die m-dimensionale Kugel mit Mittelpunkt $\mathbf{p}$ und Radius r, sowie mit

$$C_r(\mathbf{p}) := \{\mathbf{v} \in \mathbb{R}^m \mid \|\mathbf{p} - \mathbf{v}\|_\infty \le r\}$$

den m-dimensionalen Würfel mit Mittelpunkt $\mathbf{p}$ und Kantenlänge $2r$.

Definition 1.4. Das *i-te sukzessive Minimum* $\lambda_i(\mathsf{L})$ eines Gitters L vom Rang n ist für $i = 1, \ldots, n$ definiert durch

$$\lambda_i(\mathsf{L}) := \inf\{r \mid \mathrm{rg}(\mathsf{L} \cap B_r(\mathbf{0})) = i\},$$

und das *i-te sukzessive Minimum bzgl. der Maximum-Norm* $\lambda_{i,\|\cdot\|_\infty}(\mathsf{L})$ durch

$$\lambda_{i,\|\cdot\|_\infty}(\mathsf{L}) := \inf\{r \mid \mathrm{rg}(\mathsf{L} \cap C_r(\mathbf{0})) = i\}.$$

Offensichtlich gibt es für jedes Gitter in jeder nichtleeren Menge von Gittervektoren einen kürzesten Gittervektor. Für jedes Gitter L vom Rang n gibt es also linear unabhängige Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ mit $\|\mathbf{v}_i\| = \lambda_i(\mathsf{L})$ für $i = 1, \ldots, n$. Die Vektoren mit der Länge $\lambda_1(\mathsf{L})$ bezeichnen wir als *kürzeste Gittervektoren* (obwohl der Nullvektor trivialerweise kürzer ist).

Definition 1.5. Für $n \in \mathbb{N}$ ist die *Hermite-Konstante* γ_n definiert durch

$$\gamma_n := \sup_{\mathsf{L}, \mathrm{rg}(\mathsf{L})=n} \min_{\mathbf{v} \in \mathsf{L} \setminus \{\mathbf{0}\}} \frac{\|\mathbf{v}\|^2}{\det(\mathsf{L})^{2/n}}.$$

Die Hermite-Konstante γ_n ist nur für $n \leq 8$ explizit bekannt. Für jedes $n \in \mathbb{N}$ gibt es ein Gitter L mit $\lambda_1(\mathsf{L})^2 = \gamma_n$ und $\det(\mathsf{L}) = 1$. Für die Hermite-Konstante γ_n und die sukzessiven Minima $\lambda_i(\mathsf{L})$ eines Gitters L vom Rang n gilt (siehe z.B. [**Mar**]):

Theorem 1.6. (a) $\frac{1}{2\pi e} \leq \liminf_{n\to\infty} \frac{1}{n}\gamma_n \leq \limsup_{n\to\infty} \frac{1}{n}\gamma_n \leq \frac{1}{\pi e}$.

(b) $\gamma_n \leq \frac{2}{\pi}(\Gamma(n/2+2))^{2/n} \leq n$.

(c) **Minkowskis 1. Theorem:** $\lambda_1(\mathsf{L})^2 \leq \gamma_n \cdot \det(\mathsf{L})^{2/n}$.

(d) **Minkowskis 2. Theorem:** $\prod_{i=1}^n \lambda_i(\mathsf{L}) \leq \gamma_n^{n/2} \cdot \det(\mathsf{L})$.

Man beachte, daß nicht jedes Gitter L eine Basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ mit $\lambda_i(\mathsf{L}) = \|\mathbf{b}_i\|$ für $i = 1, \ldots, n$ besitzt.

Beispiel. Betrachte das von den Einheitsvektoren $\mathbf{e}_1, \ldots, \mathbf{e}_n \in \mathbb{R}^n$ und dem Vektor $\mathbf{v} = 1/2 \sum_{i=1}^n \mathbf{e}_i$ erzeugte Gitter L. Für $n \geq 5$ ist $\lambda_1(\mathsf{L}) = \ldots = \lambda_n(\mathsf{L}) = 1$ und die Einheitsvektoren sind (bis auf die Vorzeichen) die einzigen Gittervektoren mit Norm 1, die aber keine Basis von L sind.

Für die Länge einer Gitterbasis führen wir daher die folgende Größe ein:

Definition 1.7. Die *Basislänge* $\nu(\mathsf{L})$ eines Gitters L vom Rang n ist definiert durch

$$\nu(\mathsf{L}) := \min_{\text{Basen } [\mathbf{b}_1, \ldots, \mathbf{b}_n] \text{ von } \mathsf{L}} \max_{1 \leq i \leq n} \|\mathbf{b}_i\|.$$

Das vorhergehende Beispiel zeigt, daß es Gitter mit $\nu(\mathsf{L}) \geq \sqrt{n}/2\, \lambda_n(\mathsf{L})$ gibt und die folgende Proposition von Cai und Nerurkar [**CN**] besagt, daß dies die Extremsituation ist.

Proposition 2. *Für ein Gitter L vom Rang $n \geq 4$ und linear unabhängige Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ in L mit $\max_i \|\mathbf{v}_i\| \leq M$ kann in polynomieller Zeit eine Basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ von L mit $\|\mathbf{b}_i\| \leq \sqrt{n}/2M$ berechnet werden. Für alle $i = 1, \ldots, n$ gilt $\mathbf{v}_i = \sum_{j=1}^i \alpha_{i,j}\mathbf{b}_j$, wobei die $\alpha_{i,j} \in \mathbb{Z}$ und $\alpha_{i,i} > 0$ sind.*

Definition 1.8. Ein Gitter K heißt *Untergitter* eines Gitters L, falls $\mathsf{K} \subseteq \mathsf{L}$.

Wir nennen ein Untergitter K eines Gitters L ein *saturiertes Untergitter* von L, falls $\mathsf{K} = \mathsf{L} \cap \mathrm{span}(\mathsf{K})$.

Definition 1.9. Der *i-te sukzessive Erzeugendenradius* $g_i(\mathsf{L})$ eines Gitters L vom Rang n ist für $i = 1, \ldots, n$ definiert durch

$$g_i(\mathsf{L}) := \inf\{r \mid \mathsf{L} \cap B_r(\mathbf{0}) \text{ enthält saturiertes Untergitter } \mathsf{K} \text{ mit } \mathrm{rg}(\mathsf{K}) = i\}.$$

Trivialerweise gilt für $i = 1, \ldots, n$ $\lambda_i(\mathsf{L}) \leq g_i(\mathsf{L})$ sowie für $i = n$

$$\lambda_n(\mathsf{L}) \leq g_n(\mathsf{L}) \leq \nu(\mathsf{L}).$$

Für die sukzessiven Minima bzw. sukzessiven Erzeugendenradii gilt das folgende sog. Transfer-Theorem von Banaszcyk [**Ban**] bzw. Cai [**Cai1**].

Theorem 1.10. *Es gibt Konstanten C und C', so daß für jedes Gitter L vom Rang n für $i = 1, \ldots, n$ gilt:*

(1) $1 \leq \lambda_i(\mathsf{L}^*) \cdot \lambda_{n-i+1}(\mathsf{L}) \leq C\, n$,
(2) $1 \leq \lambda_i(\mathsf{L}^*) \cdot g_{n-i+1}(\mathsf{L}) \leq C'\, n$.

Das folgende Resultat von Conway und Thompson [**MH**, Kap. II, Theorem 9.5] zeigt, daß die obigen Transfer-Schranken bis auf die Konstanten C und C' optimal sind.

Proposition 3. *Es gibt Gitter L vom Rang n und Konstanten c und c', so daß für $i = 1, \ldots, n$ gilt:*

(1) $\lambda_i(\mathsf{L}^*) \cdot \lambda_{n-i+1}(\mathsf{L}) \geq c\, n$,
(2) $\lambda_i(\mathsf{L}^*) \cdot g_{n-i+1}(\mathsf{L}) \geq c'\, n$.

Aus dem obigen Transfer-Theorem und der Proposition 2 erhalten wir ein Transfer-Theorem für die Basislänge $\nu(\cdot)$ und das erste sukzessive Minimum $\lambda_1(\cdot)$.

Korollar 1. *Es gibt eine Konstante C'', so daß für jedes Gitter L gilt:*

$$1 \leq \lambda_1(\mathsf{L}^*) \cdot \nu(\mathsf{L}) \leq C''\, n^{1.5}.$$

Neben den homogenen Größen $\lambda_i(\cdot)$, $g_i(\cdot)$ und $\nu(\cdot)$ werden wir oft die folgende inhomogene Größe verwenden.

Definition 1.11. Für ein Gitter L im $\mathbb{R}^m$ und einen Vektor $\mathbf{x} \in \mathbb{R}^m$ bezeichnet $\mu(\mathbf{x}, \mathsf{L})$ die Euklidische *Distanz von $\mathbf{x}$ zum nächsten Gittervektor in L*.

1.1.1. HKZ-Reduktion. Ziel der Gitterbasenreduktionstheorie ist es, unter den Basen eines Gitters *reduzierte* auszuzeichnen und zu konstruieren: Die Vektoren einer reduzierten Basis sollen kurz sein und (möglichst) orthogonal aufeinander stehen. Die Definition einer reduzierten Basis ist nicht kanonisch. Die vorliegende Arbeit verwendet nur die im folgenden vorgestellte HKZ-Reduktion und die Reduktion der Größe $\nu(\cdot)$. Eine ausführliche Diskussion verschiedener Reduktionsbegriffe findet sich in der Arbeit [**Val**].

Zur Definition reduzierter Basen benötigen wir einige Bezeichnungen. Für eine Gitterbasis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ eines Gitters L bezeichnet $[\hat{\mathbf{b}}_1, \ldots, \hat{\mathbf{b}}_n]$ dessen *Gram-Schmidt-Orthogonalisierung*, die rekursiv berechnet wird:

$$\hat{\mathbf{b}}_i = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \hat{\mathbf{b}}_j \quad \text{für } 1 \leq i \leq n,$$

mit

$$\mu_{ij} = \frac{\langle \mathbf{b}_i, \hat{\mathbf{b}}_j \rangle}{\langle \hat{\mathbf{b}}_j, \hat{\mathbf{b}}_j \rangle} \quad \text{für } 1 \leq j < i \leq n.$$

Mit

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

bezeichnen wir die *orthogonale Projektion* auf $\operatorname{span}(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^{\perp}$. Es gilt für $i = 1, \ldots, n$:

$$\pi_i(\mathbf{b}_j) = \hat{\mathbf{b}}_j + \sum_{k=i}^{j-1} \mu_{jk} \hat{\mathbf{b}}_k$$

und insbesondere

$$\pi_i(\mathbf{b}_i) = \hat{\mathbf{b}}_i.$$

Desweiteren definieren wir für $i = 1, \ldots, n$ die Gitter

$$\mathsf{L}^{(n-i+1)} := \pi_i(\mathsf{L})$$

vom Rang $n - i + 1$ mit Basis $[\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_n)]$. Wir nennen eine Gitterbasis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ eines Gitters L *schwach reduziert*, falls $|\mu_{ij}| \leq 1/2$ für $1 \leq j < i \leq n$ gilt.

Definition 1.12. Eine Basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ eines Gitters L heißt reduziert im Sinne von Hermite, Korkin und Zolotarev oder kurz *HKZ-reduziert*, falls

(i) $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ schwach reduziert ist, und

(ii) $\|\hat{\mathbf{b}}_i\| \leq \lambda_1(\mathsf{L}^{(n-i+1)})$ für $i = 1, \ldots, n$ gilt.

Definition 1.13. Für eine Funktion $g : \mathbb{N} \to \mathbb{R}_+$ heißt eine Basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ eines Gitters L *g-approximativ HKZ-reduziert*, falls

(i) $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ schwach reduziert ist, und

(ii) $\|\hat{\mathbf{b}}_i\| \leq g(n)\lambda_1(\mathsf{L}^{(n-i+1)})$ für $i = 1, \ldots, n$ gilt.

Der folgende Satz (siehe z.B. [**LLS**]) zeigt, daß HKZ-reduzierte Basen stark reduzierte Basen sind.

Theorem 1.14. *Für eine g-approximative HKZ-Basis* $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ *eines Gitters* L *gilt für* $i = 1, \ldots, n$*:*

$$\|\mathbf{b}_i\| \leq g(n)\sqrt{\tfrac{i+3}{4}}\lambda_i(\mathsf{L}).$$

1.1.2. Relationen. Eine *(ganzzahlige) Relation* für einen Vektor $\mathbf{a} \in \mathbb{R}^n$ ist ein Vektor $\mathbf{x} \in \mathbb{Z}^n$ mit $\langle \mathbf{x}, \mathbf{a} \rangle = 0$; und eine *modulare (ganzzahlige) Relation* für einen Vektor $\mathbf{a} \in \mathbb{Z}^n$ und einen Modul $m \in \mathbb{N}_+$ ist ein Vektor $\mathbf{x} \in \mathbb{Z}^n$ mit $\langle \mathbf{x}, \mathbf{a} \rangle \equiv 0 \pmod{m}$. Die Menge der Relationen für einen Vektor $\mathbf{a} \in \mathbb{R}^n$ bildet ein Gitter

$$\mathsf{L}_{\mathbf{a}} := \{\mathbf{x} \in \mathbb{Z}^n \mid \langle \mathbf{a}, \mathbf{x} \rangle = 0\},$$

das sog. Relationengitter zu $\mathbf{a}$ mit $0 \leq \mathrm{rg}(\mathsf{L}_{\mathbf{a}}) \leq n-1$ und $\mathrm{rg}(\mathsf{L}_{\mathbf{a}}) = n-1$ für $\mathbf{a} \in \mathbb{Q}^n$. Die Menge der Relationen für einen Vektor $\mathbf{a} \in \mathbb{Z}^n$ und einen Modul $m \in \mathbb{N}$ bildet ebenfalls ein Gitter

$$\mathsf{L}_{\mathbf{a},m} := \{\mathbf{x} \in \mathbb{Z}^n \mid \langle \mathbf{a}, \mathbf{x} \rangle \equiv 0 \pmod{m}\},$$

das sog. modulare Relationengitter zu $\mathbf{a}$ und m mit $\mathrm{rg}(\mathsf{L}_{\mathbf{a},m}) = n$.

Eine ausführliche Behandlung von Relationen findet sich in der Arbeit [**HJLS**] von Håstad, Just, Lagarias und Schnorr. Die Bedeutung von modularen Relationen für die Gittertheorie i.A. wird in Paz und Schnorr [**PS**] und in Cai, Havas, Mans, Nerurkar, Seifert und Shparlinksi [**CHM**$^+$] behandelt.

1.2. Diophantische Approximationen

Wir führen nun die in dieser Arbeit verwendeten Begriffe und Sätze aus der Theorie der Diophantischen Approximationen ein, und verweisen für eine ausführliche Einführung auf [**Cas2**].

Für eine Zahl $\alpha \in \mathbb{R}$ bezeichnet $[\alpha]$ den *ganzzahligen Teil* von α, d.h. $[\alpha] \leq \alpha < [\alpha]+1$ und $\{\alpha\}$ den *reellwertigen Teil* von α, d.h. $\{\alpha\} = \alpha - [\alpha]$. Für einen Vektor $\boldsymbol{\alpha} \in \mathbb{R}^n$ definieren wir $\{\boldsymbol{\alpha}\} := (\{\alpha_1\}, \ldots, \{\alpha_n\})$.

Für einen Vektor $\boldsymbol{\alpha} \in \mathbb{R}^n$ und einen Nenner $q \in \mathbb{N}_+$ definieren wir die *Güte* $\|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty$ *der Diophantischen Approximation von* $\boldsymbol{\alpha}$ *durch rationale Zahlen mit Hauptnenner* q durch

$$\|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty := \max_{1 \leq i \leq n} \min_{p_i \in \mathbb{Z}} |q\alpha_i - p_i|.$$

Der folgende Satz (siehe z.B. [**Cas2**]) gibt Auskunkt darüber, wie gut ein Vektor $\boldsymbol{\alpha} \in \mathbb{R}^n$ mit vorgegebener Hauptnennerschranke approximiert werden kann.

Theorem 1.15 (Dirichlet)**.** *Für einen Vektor $\boldsymbol{\alpha} \in \mathbb{R}^n$ und eine positive ganze Zahl N existiert ein Nenner q mit $1 \leq q \leq N^n$, so daß gilt:*

$$\|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \leq \frac{1}{N}.$$

Neben der homogenen Diophantischen Approximation benötigen wir auch die inhomogene Diophantische Approximation. Für einen Vektor $\boldsymbol{\alpha} \in \mathbb{R}^n$, einen Vektor $\boldsymbol{\beta} \in \mathbb{R}^n$ und einen Nenner $q \in \mathbb{N}_+$ definieren wir die *Güte* $\|\boldsymbol{\beta} - q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty$ *der Inhomogenen Diophantischen Approximation von* $\boldsymbol{\alpha}$ *durch rationale Zahlen mit Hauptnenner* q durch

$$\|\boldsymbol{\beta} - q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty := \max_{1 \leq i \leq n} \min_{p_i \in \mathbb{Z}} |\beta_i - q\alpha_i - p_i|.$$

1.3. Komplexitätstheorie

Alphabete sind endliche Mengen von Symbolen. Das *binäre Alphabet* $\{0,1\}$ besteht aus den Symbolen 0 und 1 und wird in dieser Arbeit mit Σ bezeichnet. Ein *String* x ist eine endliche Folge der Länge $|x|$ von Elementen eines Alphabetes. Für ein Alphabet Γ bezeichnet Γ^* die Menge aller endlichen Strings über dem Alphabet Γ einschließlich des *leeren Strings* ϵ. Eine Teilmenge $L \subseteq \Gamma^*$ heißt *Sprache* über dem Alphabet Γ. Ohne Beschränkung der Allgemeinheit betrachten wir nur Sprachen über dem binären Alphabet Σ.

Definition 1.16. P ist die Klasse der Sprachen, deren charakteristische Funktion von deterministischen Turing-Maschinen in polynomieller Zeit berechenbar ist.

Definition 1.17. Eine Sprache L ist in NP, falls eine Boolesche Relation $R_L \subseteq \{0,1\}^* \times \{0,1\}^*$ und ein Polynom $p(\cdot)$ existieren, so daß R_L von einer deterministischen Turing-Maschine in polynomieller Zeit berechenbar ist und $x \in L$ gdw. ein y mit $|y| \leq p(|x|)$ und $(x,y) \in R_L$ existiert. Ein solches y heißt *Zeuge für* $x \in L$.

Definition 1.18. Die *Polynomialzeit-Hierachie* ist die Menge $\{\Sigma_i^{\mathrm{p}}, \Pi_i^{\mathrm{p}} \mid i \geq 0\}$ von Klassen Σ_i^{p}, Π_i^{p}, die wie folgt sind:

$i = 0$**:** $\Sigma_0^{\mathrm{p}} = \Pi_0^{\mathrm{p}} := \mathsf{P}$

$i \geq 1$**:** Eine Sprache L ist in Σ_i^{p}, falls eine Boolesche Relation $R_L \subseteq \{0,1\}^* \times \{0,1\}^*$ und ein Polynom $p(\cdot)$ existieren, so daß die Sprache $\{(x,y) \mid (x,y) \in R_L\}$ in Π_{i-1}^{p} enthalten ist und $x \in L$ gdw. $\exists y\,(|y| \leq p(|x|)) : (x,y) \in R_L$.

Eine Sprache L ist in Π_i^{p}, falls eine Boolesche Relation $R_L \subseteq \{0,1\}^* \times \{0,1\}^*$ und ein Polynom $p(\cdot)$ existieren, so daß die Sprache $\{(x,y) \mid (x,y) \in R_L\}$ in $\Sigma_{i-1}^{\mathrm{p}}$ enthalten ist und $x \in L$ gdw. $\forall y\,(|y| \leq p(|x|)) : (x,y) \in R_L$.

Man beachte, daß die nullte bzw. erste Stufe der Polynomialzeit-Hierachie, d.h. Σ_0^{p} und Π_0^{p} bzw. Σ_1^{p} und Π_1^{p} aus den elementaren Komplexitätsklassen P bzw. NP und $\mathsf{co\text{-}NP}$ besteht. Das folgende Theorem (see z.B. [**Pap**]) besagt, daß die Polynomialzeit-Hierachie keine unendliche Hierachie ist, falls sie nur auf einer einzigen Stufe kollabiert.

Theorem 1.19. *Existiert ein $i \geq 1$ mit $\Sigma_i^{\mathrm{p}} = \Pi_i^{\mathrm{p}}$, so gilt $\Sigma_j^{\mathrm{p}} = \Pi_j^{\mathrm{p}}$ für alle $j > i$.*

1.3.1. Reduktionen und Vollständigkeit. Es ist oftmals der Fall, daß ein Berechnungsproblem durch Benutzung eines effizienten Unterprogramms für ein zweites Berechnungsproblem effizient, d.h. in Polynomial-Zeit gelöst werden kann. Dieses generelle Prinzip der Reduktion eines Problems auf ein anderes Problem ist ein wesentliches Instrument der Komplexitätstheorie.

Definition 1.20. Eine Berechnungsproblem Φ heißt *randomisiert Cook-reduzierbar* bzw. *randomisiert Polynomial-Zeit reduzierbar* auf ein Berechnungsproblem Ψ, kurz $\Phi \leq_{\mathrm{C}}^{\mathrm{R}} \Psi$, falls es einen probabilistischen Polynomial-Zeit Algorithmus $\mathcal{A}$ gibt, der ein Unterprogramm $\mathcal{B}$ für Ψ benutzt, so daß

$$\Pr[\mathcal{A} \text{ löst } \Phi \text{ mit Unterprogramm } \mathcal{B}] \geq \frac{1}{2}$$

gilt. Ist $\mathcal{A}$ deterministisch, so heißt Φ *Cook-reduzierbar* bzw. *Polynomial-Zeit reduzierbar* auf Ψ, kurz $\Phi \leq_{\mathrm{C}} \Psi$.

Ein wichtiger und in dieser Arbeit häufig verwendeter Spezialfall der deterministischen Cook-Reduktion ist die einmalige Verwendung des Unterprogramms.

Definition 1.21. Eine Sprache L heißt *Karp-reduzierbar* bzw. *many-to-one-reduzierbar* auf eine Sprache M, kurz $L \leq_{\mathrm{K}} M$, falls es eine in polynomieller Zeit berechenbare Funktion f gibt, so daß für alle x gilt:

$$x \in L \iff f(x) \in M.$$

Definition 1.22. Eine Sprache M heißt NP-*hart*, falls für alle $L \in \mathsf{NP}$ $L \leq_{\mathrm{K}} M$ oder $L \leq_{\mathrm{C}} M$ gilt, und M heißt NP-*vollständig*, falls M NP-hart ist, und in NP enthalten ist.

Eine Funktion $f : \mathbb{N} \to \mathbb{R}$, die durch $n^{\mathrm{poly}\log n}$ beschränkt ist, bezeichnen wir als *fast-polynomiell* bzw. *quasi-polynomiell*.

Definition 1.23. QP ist die Klasse der Sprachen, deren charakteristische Funktion von deterministischen Turing-Maschinen in quasi-polynomieller Zeit berechenbar ist.

Definition 1.24. Eine Sprache M heißt *fast* NP-*hart*, falls es eine in fast-polynomieller Zeit berechenbare Funktion f gibt, so daß für alle $L \in \mathsf{NP}$ und alle x gilt:

$$x \in L \iff f(x) \in M.$$

1.3.2. Optimierung, Approximation, Gaps und Promise Probleme. Wir geben eine kurze Einführung in Optimierungsprobleme, Approximations-Algorithmen, Gaps und Promise-Probleme, um dann den Begriff der Nicht-Approximierbarkeit eines Optimierungsproblems vorstellen zu können.

1.3.2.1. *Optimierungsprobleme.* Ein *Optimierungsproblem* Φ besteht aus einer Menge $\mathcal{I}$ von Instanzen, einer Menge $\mathcal{S}$ von Lösungen, einer in Polynomial-Zeit berechenbaren Zielfunktion $m : \mathcal{I} \times \mathcal{S} \to \mathbb{R}_+$, die jeder Instanz I und jeder Lösung S den sog. *Wert* $m(I, S)$ der Lösung S zuordnet, sowie einer Angabe, ob es sich um ein Maximierungsproblem oder aber um ein Minimierungsproblem handelt. Für eine gegebene Instanz I soll eine Lösung S^* berechnet werden, so daß der Wert $m(I, S^*)$ über alle Lösungen $S \in \mathcal{S}$ maximal bzw. minimal ist. Für ein Optimierungsproblem Φ und eine Instanz I bezeichnet $\Phi(I)$ den *optimalen* Wert der Instanz I, der für ein Maximierungsproblem durch $\Phi(I) := \max_{S \in \mathcal{S}} m(I, S)$ und für ein Minimierungsproblem durch $\Phi(I) := \min_{S \in \mathcal{S}} m(I, S)$ definiert ist.

Alle in dieser Arbeit betrachteten Optimierungsprobleme sind stets Minimierungsprobleme. Die folgenden Berechnungsprobleme sind klassische Optimierungsprobleme für Gitter, und sind daher bereits intensiv untersucht worden. Ein aktueller Übersichtsartikel von Cai [**Cai3**] beschreibt die Untersuchungen dieser Probleme von 1801 an, mit Gauss [**Gau**] beginnend, bis zum heutigen Forschungsstand.

Definition 1.25. Shortest Vector Problem (Svp)
Gegeben: Ein Gitter $\mathsf{L} \subseteq \mathbb{Q}^m$.
Finde: Einen Vektor $\mathbf{v} \in \mathsf{L}$ mit

$$\|\mathbf{v}\| = \lambda_1(\mathsf{L}).$$

Definition 1.26. Closest Vector Problem (Cvp)
Gegeben: Ein Gitter $\mathsf{L} \subseteq \mathbb{Q}^m$ und ein Vektor $\mathbf{x} \in \mathbb{Q}^m$.
Finde: Einen Vektor $\mathbf{v} \in \mathsf{L}$ mit

$$\|\mathbf{v} - \mathbf{x}\| = \mu(\mathbf{x}, \mathsf{L}).$$

Definition 1.27. $\|\cdot\|_\infty$-Shortest Integer Relation (Sir$^\infty$).
Gegeben: Ein Vektor $\mathbf{a} \in \mathbb{Q}^n$.
Finde: Einen Vektor $\mathbf{v} \in \mathsf{L}_\mathbf{a}$ mit

$$\|\mathbf{v}\|_\infty = \lambda_{1,\|\cdot\|_\infty}(\mathsf{L}_\mathbf{a}).$$

Definition 1.28. MODULAR SHORTEST INTEGER RELATION (MSIR)
GEGEBEN: Ein Vektor $\mathbf{a} \in \mathbb{Q}^n$ und ein Modul $m \in \mathbb{N}$.
FINDE: Einen Vektor $\mathbf{v} \in \mathsf{L}_{\mathbf{a},m}$ mit

$$\|\mathbf{v}\| = \lambda_1(\mathsf{L}_{\mathbf{a},m}).$$

1.3.2.2. *Approximation.* Ein Approximations-Algorithmus für ein Optimierungsproblem Φ ist ein Algorithmus, der bei Eingabe I eine Lösung S berechnet, deren Wert $m(I,S)$ so nah wie möglich am Optimum $\Phi(I)$ ist. Approximations-Algorithmen werden in dieser Arbeit stets eine in der Länge der Eingabe polynomielle Laufzeitschranke haben.

Während die Komplexität eines Approximations-Algorithmus in der Länge der Eingabe gemessen wird, ist die Approximations-Qualität eine Funktion eines für das jeweilige Optimierungsproblem spezifischen Maß der Eingabegröße.

Insbesondere verwenden alle in dieser Arbeit betrachteten Optimierungsprobleme als Maß für die Approximations-Qualität stets den Rang des gegebenen Gitters oder aber die Dimension des gegebenen Vektors.

Definition 1.29. Ein Approximations-Algorithmus $\mathcal{A}$ für ein Minimierungsproblem Φ *approximiert* Φ *bis auf einen Faktor* $f(\cdot) \geq 1$, falls für alle Eingaben I die Ausgabe $\mathcal{A}(I)$ des Algorithmus $\mathcal{A}$

$$\Phi(I) \leq m(I, \mathcal{A}(I)) \leq f(|I|) \cdot \Phi(I)$$

erfüllt, wobei $|\cdot|$ ein für das Optimierungsproblem Φ spezifisches Maß für die Eingabegrösse ist.

1.3.2.3. *Gaps und Promise-Probleme.* Wir betrachten nun solche Instanzen eines Optimierungsproblems, für die wir das *Versprechen* haben, daß das Optimum der Zielfunktion entweder *sehr groß* ist, oder aber *sehr klein* ist. Hierzu definieren wir zu einem Optimierungsproblem ein entsprechendes Promise-Problem. Dieses hängt von zwei Polynomial-Zeit berechenbaren Funktionen $r(\cdot)$ und $f(\cdot)$ ab.

Definition 1.30. Sei Φ ein Minimierungsproblem und seien $r(\cdot) > 0$, $f(\cdot) \geq 1$ Polynomial-Zeit berechenbare Funktionen des Maß $|\cdot|$ für die Approximations-Qualität. Das *Promise-Problem* $\text{GAP}\Phi_f$ zu Φ ist durch

$$\begin{aligned} \text{JA} &:= \{(I, r(|I|)) \mid \Phi(I) \leq r(|I|)\}, \\ \text{NEIN} &:= \{(I, r(|I|)) \mid \Phi(I) > f(|I|) \cdot r(|I|)\} \end{aligned}$$

und

$$\text{GAP}\Phi_f := (\text{JA}, \text{NEIN})$$

definiert. Die Funktion $f(\cdot)$ wird als *gap-Funktion* oder kurz als *Gap* des Promise-Problems $\text{GAP}\Phi_f$ bezeichnet.

Man beachte, daß das Promise-Problem $\text{GAP}\Phi_1$, das mit dem Optimierungsproblem Φ assoziierbare *Entscheidungs-Problem* zu Φ darstellt.

Im folgenden geben wir die entsprechenden Promise-Probleme der Optimierungsprobleme SVP, CVP und SIR^∞ an. Man beachte, daß wir in den nachfolgenden ersten zwei Definitionen die Funktion $r(\cdot)$ als reellwertig auffassen. Um ein wohldefiniertes Berechnungsproblem zu erhalten, müßte die Funktion $r(\cdot)$ strenggenommen jedoch eine rationale Funktion sein. Dies kann aber dadurch leicht gelöst werden, daß man zur quadrierten Euklidischen Länge übergeht. Aus Gründen der Übersichtlichkeit verzichten wir jedoch in dieser Arbeit durchgängig auf diese Quadrierung.

Definition 1.31. Das Promise-Problem GAPSVP_g, wobei $g(\cdot)$ eine gap-Funktion bezeichnet, ist wie folgt definiert:

> JA-Instanzen sind Paare (L, r), wobei $\mathsf{L} \subseteq \mathbb{Q}^m$ ein Gitter vom Rang n ist, $r \in \mathbb{R}_+$ und $\lambda_1(\mathsf{L}) \leq r$,
>
> NEIN-Instanzen sind Paare (L, r), wobei $\mathsf{L} \subseteq \mathbb{Q}^m$ ein Gitter vom Rang n ist, $r \in \mathbb{R}_+$ und $\lambda_1(\mathsf{L}) > g \cdot r$.

Definition 1.32. Das Promise-Problem GAPCVP_g, wobei $g(\cdot)$ eine gap-Funktion bezeichnet, ist wie folgt definiert:

> JA-Instanzen sind Tripel $(\mathsf{L}, \mathbf{x}, r)$, wobei $\mathsf{L} \subseteq \mathbb{Q}^m$ ein Gitter vom Rang n ist, $\mathbf{x} \in \mathbb{Q}^m$, $r \in \mathbb{R}_+$ und $\mu(\mathbf{x}, \mathsf{L}) \leq r$,
>
> NEIN-Instanzen sind Tripel $(\mathsf{L}, \mathbf{x}, r)$, wobei $\mathsf{L} \subseteq \mathbb{Q}^m$ ein Gitter vom Rang n ist, $\mathbf{x} \in \mathbb{Q}^m$, $r \in \mathbb{R}_+$ und $\mu(\mathbf{x}, \mathsf{L}) > g \cdot r$.

Definition 1.33. Das Promise-Problem GAPSIR_g^∞, wobei $g(\cdot)$ eine gap-Funktion bezeichnet, ist wie folgt definiert:

> JA-Instanzen sind Tupel $(\mathbf{a}, r) \in (\mathbb{Q}^n, \mathbb{Q}_+)$ mit $\lambda_{1,\|\cdot\|_\infty}(\mathsf{L}_\mathbf{a}) \leq r$,
>
> NEIN-Instanzen sind Tupel $(\mathbf{a}, r) \in (\mathbb{Q}^n, \mathbb{Q}_+)$ mit $\lambda_{1,\|\cdot\|_\infty}(\mathsf{L}_\mathbf{a}) > g \cdot r$.

1.3.2.4. *Nicht-Approximierbarkeit durch Gaps.* Die Nicht-Approximierbarkeit eines Optimierungsproblems Φ bis auf einen Faktor f wird dadurch gezeigt, daß das entsprechende Promise-Problem $\text{GAP}\Phi_f$ als NP-hart nachgewiesen wird. Dies zeigt die folgende Proposition (siehe z.B. [**BGS**]).

Proposition 4. *Ein Optimierungsproblem Φ besitzt keinen Polynomial-Zeit Approximations-Algorithmus bis auf einen Faktor f:*

> *Unter der Annahme* $\mathsf{NP} \not\subseteq \mathsf{P}$*, falls* $\text{GAP}\Phi_f$ NP*-hart ist.*
>
> *Unter der Annahme* $\mathsf{NP} \not\subseteq \mathsf{QP}$*, falls* $\text{GAP}\Phi_f$ *fast* NP*-hart ist.*

1.4. Interaktive Protokolle

Wir stellen nun die in dieser Arbeit verwendeten Begriffe und Resultate aus der Theorie der Interaktiven Protokolle vor. Für eine grundlegende Einführung in das Gebiet der Interaktiven Protokolle müssen wir jedoch auf [**Gol**] bzw. [**Pap**] verweisen.

Der *Verifizierer* $\mathcal{V}$ und der *Beweiser* $\mathcal{P}$ eines *interaktiven Protokolls* sind Funktionen

$$\mathcal{V} : \Sigma^* \times \Sigma^* \times \Sigma^* \to \Sigma^* \cup \{acc, rej\}$$

und

$$\mathcal{P} : \Sigma^* \times \Sigma^* \to \Sigma^*,$$

über dem binären Alphabet $\Sigma = \{0, 1\}$. Wir bezeichnen mit $m_1 \# m_2 \# \cdots \# m_i$ die zwischen dem Verifizierer $\mathcal{V}$ und dem Beweiser $\mathcal{P}$ ausgetauschten Nachrichten $m_1, m_2, \ldots, m_i$. Die Ausgabe des Verifizierers ist entweder die nächste Nachricht m_{i+1} an den Beweiser oder aber *acc* bzw. *rej*, je nach Konklusion des interaktiven Protokolls. $\mathcal{V}(w, r, m_1 \# \cdots \# m_i) = m_{i+1}$ bedeutet, daß der Verifizierer $\mathcal{V}$ bei Eingabe w, *geheimen* Zufallsbits r und der bisherigen Nachrichtenfolge $m_1 \# \cdots \# m_i$ dem Beweiser m_{i+1} als nächste Nachricht schickt. Die Ausgabe des Beweisers ist die nächste Nachricht m_{i+1} an den Verifizierer. $\mathcal{P}(w, m_1 \# \cdots \# m_i) = m_{i+1}$ bedeutet, daß der Beweiser $\mathcal{P}$ bei Eingabe w und der bisherigen Nachrichtenfolge $m_1 \# \cdots \# m_i$ dem Verifizierer m_{i+1} als nächste Nachricht schickt. Wir schreiben $(\mathcal{V} \leftrightarrow \mathcal{P})(w, r) = acc$, falls es eine Folge $m_1, \ldots, m_k$ ausgetauschter Nachrichten zwischen $\mathcal{V}$ und $\mathcal{P}$ gibt und $\mathcal{V}(w, r, m_1 \# \cdots \# m_k) = acc$. Ein interaktives Protokoll mit k ausgetauschten Nachrichten bezeichnen wir als *k-Runden Protokoll*.

Wir definieren die Wahrscheinlichkeit, daß ein interaktives Protokoll mit einem Verifizierer $\mathcal{V}$ und einem Beweiser $\mathcal{P}$ eine Eingabe w akzeptiert durch

$$\Pr\left[\mathcal{V} \leftrightarrow \mathcal{P} \text{ akzeptiert } w\right] := \Pr_{r \in_u \Sigma^*}\left[(\mathcal{V} \leftrightarrow \mathcal{P})(w, r) = acc\right].$$

Definition 1.34. Ein *interaktives Beweis-System* für eine Sprache L besteht aus einer in polynomieller Zeit berechenbaren Funktion $\mathcal{V}$ und einer Funktion $\mathcal{P}$, so daß für jede Funktion $\tilde{\mathcal{P}}$ und jeden String w gilt:

$$w \in L \Longrightarrow \Pr\left[\mathcal{V} \leftrightarrow \mathcal{P} \text{ akzeptiert } w\right] = 1$$

und

$$w \notin L \Longrightarrow \Pr[\mathcal{V} \leftrightarrow \tilde{\mathcal{P}} \text{ akzeptiert } w] < \tfrac{1}{2}.$$

Für eine Funktion $r : \mathbb{N} \to \mathbb{N}$ bezeichnet $\mathsf{IP}(r(\cdot))$ die Klasse der Sprachen, die ein interaktives Beweis-System mit einem $r(n)$-Runden Protokoll haben, wobei n die Länge des gemeinsamen Eingabestrings w ist.

Später benötigen wir folgendes Theorem, das in kompakter Form Resultate von Babai [**Bab**], Boppana, Håstad und Zachos [**BHZ**], sowie Goldwasser und Sipser [**GS**] vereint.

Theorem 1.35. *Falls* $\mathsf{co\text{-}NP} \subseteq \mathsf{IP}(O(1))$*, so gilt* $\Sigma_2^{\mathrm{p}} = \Pi_2^{\mathrm{p}}$*, d.h. die Polynomialzeit-Hierachie kollabiert auf der zweiten Stufe.*

Das obige Theorem besagt zusammen mit dem Theorem 1.19, daß die Klasse $\mathsf{co\text{-}NP}$ kein interaktives Beweis-System mit nur *konstant* vielen Runden besitzt, sofern die Polynomialzeit-Hierachie eine unendliche Hierachie ist. Wir werden dieses Resultat in den nachfolgenden Kapiteln zum Beweis von Grenzen für die Nicht-Approximierbarkeit von Optimierungsproblemen verwenden.

Kapitel 2

Die Komplexität kurzer linear unabhängiger Vektoren und kurzer Basen

Paragraph 1 dieses Kapitels stellt das Shortest Independent Vectors Problem (Sivp) und das Shortest Basis Problem (Sbp) vor, sowie bekannte Resultate und Beziehungen zu anderen Gitterproblemen. In Paragraph 2 wird die NP-Vollständigkeit des Sivp und des Sbp bewiesen. Danach wird in Paragraph 3 die Nicht-Approximierbarkeit des Sivp und des Sbp bis auf einen großen Faktor gezeigt. In Paragraph 4 beweisen wir Grenzen für Nicht-Approximierbarkeitsresultate bzgl. des Sivp und des Sbp. Der Inhalt der Paragraphen 2 und 4 entspricht im wesentlichen dem der Arbeit [**BSei**].

2.1. Die Gitterprobleme Sivp und Sbp

Für die beiden folgenden Berechnungsprobleme in Gittern ist kein Polynomial-Zeit-Algorithmus bekannt und auch nicht zu erwarten:

Definition 2.1. Shortest Independent Vectors Problem (Sivp)
Gegeben: Ein Gitter $\mathsf{L} \subseteq \mathbb{Q}^m$ vom Rang n.
Finde: n linear unabhängige Vektoren $\mathbf{v}_1, \cdots, \mathbf{v}_n \in \mathsf{L}$ mit

$$\max_{1 \le i \le n} \|\mathbf{v}_i\| = \lambda_n(\mathsf{L}).$$

Definition 2.2. SHORTEST BASIS PROBLEM (SBP)
GEGEBEN: Ein Gitter $\mathsf{L} \subseteq \mathbb{Q}^m$ vom Rang n.
FINDE: Eine Basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ für L mit

$$\max_{1 \le i \le n} \|\mathbf{b}_i\| = \nu(\mathsf{L}).$$

In der Einleitung haben wir bereits gesehen, daß die obigen Probleme und insbesondere ihre Approximation eine zentrale Rolle in Ajtai's Theorem einnehmen, und bisher noch nicht untersucht worden sind. Ziel dieses Kapitels ist daher eine eingehende komplexitätstheoretische Untersuchung des SIVP und des SBP sowie deren Approximierbarkeit.

Aus Minkowskis 2. Theorem und Proposition 2 ergibt sich $\lambda_n(\mathsf{L}) \le \gamma_n^{n/2} \cdot \det(\mathsf{L})$ und $\nu(\mathsf{L}) \le \sqrt{n}/2\, \gamma_n^{n/2} \cdot \det(\mathsf{L})$ für ein ganzzahliges Gitter L vom Rang n. Algorithmen zum Lösen des SIVP und des SBP sind von Pohst [**Poh**] sowie Chirkov und Shevchenko [**CS**] vorgestellt worden; allerdings ist von keinem dieser Algorithmen eine polynomielle Laufzeit bewiesen worden. Für Gitter vom Rang 2 liefert der Gaussche Algorithmus [**Gau**] einen effizienten Algorithmus für das SIVP und das SBP. Mit Hilfe des LLL-Algorithmus ist das SIVP und das SBP für Gitter vom festen Rang ebenfalls effizient lösbar. Für Gitter vom Rang n löst der LLL-Algorithmus das SIVP und das SBP in Polynomial-Zeit bis auf einen Faktor $2^{(n-1)/2}$.

Wir betrachten nun generelle Beziehungen zwischen dem SVP, CVP, SIVP und dem SBP. Theorem 1.14 impliziert, daß die Approximation des SIVP und des SBP bis auf einen Faktor $f(n)\sqrt{n}$ in Polynomial-Zeit auf die Approximation des SVP bis auf einen Faktor $f(n)$ reduzierbar ist. Für die andere Richtung der Reduktion zeigen wir in diesem Kapitel zunächst, daß sowohl das SVP als auch das CVP in Polynomial-Zeit auf das SIVP bzw. SBP reduzierbar sind. Man beachte, daß ein ähnliches Resultat für die Beziehung zwischen dem SVP und dem CVP nicht bekannt ist. Nach Kannan [**Kan1**] ist lediglich die $\sqrt{n}$-Approximation des CVP in Polynomial-Zeit auf das SVP reduzierbar ist. Allerdings läßt sich mit Hilfe des Transfer-Theorems 1.10 zumindest die Approximation der *Länge des kürzesten Vektors* bis auf einen Faktor $f(n)n$ in Polynomial-Zeit auf die $f(n)$-Approximation des SIVP bzw. SBP reduzieren. Dies wird später in Kapitel 4 gezeigt werden.

Wir definieren nun die entsprechenden Promise-Probleme für das SIVP und das SBP, um deren NP-Vollständigkeit und insbesondere deren Nicht-Approximierbarkeit komplexitätstheoretisch untersuchen zu können.

Definition 2.3. Das Promise-Problem GAPSIVP$_g$, wobei $g(\cdot)$ eine gap-Funktion bezeichnet, ist wie folgt definiert:

> JA-Instanzen sind Paare (L, r), wobei $\mathsf{L} \subseteq \mathbb{Q}^m$ ein Gitter vom Rang n ist, $r \in \mathbb{R}_+$ und $\lambda_n(\mathsf{L}) \le r$,

NEIN-Instanzen sind Paare (L, r), wobei $\mathsf{L} \subseteq \mathbb{Q}^m$ ein Gitter vom Rang n ist, $r \in \mathbb{R}_+$ und $\lambda_n(\mathsf{L}) > g \cdot r$.

Definition 2.4. Das Promise-Problem GAPSBP_g, wobei $g(\cdot)$ eine gap-Funktion bezeichnet, ist wie folgt definiert:

JA-Instanzen sind Paare (L, r), wobei $\mathsf{L} \subseteq \mathbb{Q}^m$ ein Gitter vom Rang n ist, $r \in \mathbb{R}_+$ und $\nu(\mathsf{L}) \leq r$,

NEIN-Instanzen sind Paare (L, r), wobei $\mathsf{L} \subseteq \mathbb{Q}^m$ ein Gitter vom Rang n ist, $r \in \mathbb{R}_+$ und $\nu(\mathsf{L}) > g \cdot r$.

In Paragraph 2 zeigen wir zunächst, daß GAPSIVP_1 und GAPSBP_1 NP-vollständig sind. Danach beweisen wir in Paragraph 3, daß $\text{GAPSIVP}_{n^{O(1/\log\log n)}}$ und $\text{GAPSBP}_{n^{O(1/\log\log n)}}$ NP-hart sind. Dies zeigt, daß es keine Polynomial-Zeit Algorithmen gibt, die das SIVP bzw. das SBP bis auf einen Faktor $n^{O(1/\log\log n)}$ lösen. Andererseits zeigen wir in Paragraph 4, daß die Probleme $\text{GAPSIVP}_{O(n)}$ und $\text{GAPSBP}_{O(n^{1.5})}$ in $\mathsf{NP} \cap \mathsf{co\text{-}NP}$ enthalten sind, und überdies hinaus beweisen wir, daß $\text{GAPSIVP}_{n/O(\sqrt{\log n})}$ und $\text{GAPSBP}_{n/O(\sqrt{\log n})}$ in $\mathsf{NP} \cap \mathsf{co\text{-}IP}(3)$ enthalten sind. Insbesondere besagt das letzte Resultat, daß die Approximation des SIVP und des SBP bis auf einen Faktor $O(n/\sqrt{\log n})$ unter Karp-Reduktionen nicht NP-hart ist, es sei denn, daß die Polynomialzeit-Hierachie auf der zweiten Stufe kollabiert.

2.2. Die NP-Vollständigkeit von SIVP und SBP

Im Gegensatz zum NP-Vollständigkeitsbeweis des SVP von Ajtai [**Ajt2**] durch eine Karp-Reduktion vom CVP, die probabilistisch und äußerst kompliziert ist, ist unsere Reduktion des CVP auf das SIVP bzw. das SBP deterministisch und leicht verständlich.

Theorem 2.5. *Die Entscheidungs-Probleme* GAPSIVP_1 *und* GAPSBP_1 *sind* NP*-vollständig.*

Beweis. Sowohl GAPSIVP_1 als auch GAPSBP_1 sind in NP, da in polynomieller Zeit entscheidbar ist, ob:

(i) n gegebene Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ linear unabhängig sind.

(ii) Ein gegebener Vektor $\mathbf{v}$ ein Element eines gegebenen Gitters L ist.

(iii) n gegebene Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ eine Basis für ein gegebenes Gitters L bilden.

Um zu beweisen, daß GAPSIVP_1 NP-hart ist, reduzieren wir GAPCVP_1 auf GAPSIVP_1. Das Entscheidungs-Problem GAPCVP_1 ist nach Kannan [**Kan1**] NP-hart.

Sei nun $(\mathsf{L}, \mathbf{x}, r)$ eine gegebene Instanz von GAPCVP$_1$ und $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ eine Basis von L. Wir können o.B.d.A. annehmen, daß $\mathsf{L} \subseteq \mathbb{Z}^m$. Wir wählen zunächst eine Konstante

$$D > \max\{r, \lambda_n(\mathsf{L})\}.$$

Nach Minkowskis 2. Theorem können wir $D := \max\{r+1, \lceil n^{n/2} \det(\mathsf{L})\rceil\}$ wählen. Da $\det(\mathsf{L})$ in polynomieller Zeit berechenbar ist, kann D in polynomieller Zeit berechnet werden. Für das von den Spaltenvektoren der Matrix

$$\begin{bmatrix} \mathbf{b}_1 & \cdots & \mathbf{b}_n & \mathbf{x} \\ 0 & \cdots & 0 & D \end{bmatrix} =: \begin{bmatrix} \mathbf{d}_1 & \cdots & \mathbf{d}_n & \mathbf{d}_{n+1} \end{bmatrix}$$

aufgespannte Gitter M vom Rang $n+1$ definieren wir $(\mathsf{M}, \sqrt{r^2 + D^2})$ als Instanz von GAPSIVP$_1$.

Sei nun $(\mathsf{L}, \mathbf{x}, r)$ eine JA-Instanz von GAPCVP$_1$. Dann existiert ein Vektor $\mathbf{v} = \sum_{i=1}^n c_i \mathbf{b}_i \in \mathsf{L}$ mit $\|\mathbf{v} - \mathbf{x}\| \leq r$. Nach Wahl von D enthält das Gitter L n linear unabhängige Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ mit $\|\mathbf{v}_i\| \leq \lambda_n(\mathsf{L}) \leq D$ für alle $i = 1, \ldots, n$. Folglich sind

$$(\mathbf{v}_1, 0)^\top, \ldots, (\mathbf{v}_n, 0)^\top, (\mathbf{v} - \mathbf{x}, -D)^\top$$

$n+1$ linear unabhängige Vektoren in M, deren Länge durch $\sqrt{r^2 + D^2}$ beschränkt ist, d.h. $\lambda_{n+1}(\mathsf{M}) \leq \sqrt{r^2 + D^2}$.

Nun nehmen wir an, daß $(\mathsf{L}, \mathbf{x}, r)$ eine NEIN-Instanz von GAPCVP$_1$ ist, d.h. $\mu(\mathbf{x}, \mathsf{L}) > r$. Da M vom Rang $n+1$ ist, muß in jeder Menge von $n+1$ linear unabhängigen Vektoren $\{\mathbf{w}_1, \ldots, \mathbf{w}_{n+1}\}$ von M mindestens ein Vektor von $\mathbf{d}_{n+1}$ abhängen; o.B.d.A. sei dieser

$$\mathbf{w}_{n+1} = \sum_{i=1}^{n+1} c_i \mathbf{d}_i \quad \text{mit } c_{n+1} \neq 0.$$

Ist nun $|c_{n+1}| \geq 2$, so folgt

$$\|\mathbf{w}_{n+1}\| \geq \sqrt{4D^2} > \sqrt{r^2 + D^2}.$$

Ist $|c_{n+1}| = 1$, o.B.d.A. sei $c_{n+1} = -1$, so folgt ebenfalls

$$\|\mathbf{w}_{n+1}\| > \sqrt{r^2 + D^2},$$

da ansonsten $\|\sum_{i=1}^n c_i \mathbf{b}_i - \mathbf{x}\| \leq r$ ist, was ein Widerspruch zur Annahme $\mu(\mathbf{x}, \mathsf{L}) > r$ ist, da $(\mathsf{L}, \mathbf{x}, r)$ nach Annahme eine NEIN-Instanz von GAPCVP$_1$ ist. Folglich gilt $\lambda_{n+1}(\mathsf{M}) > \sqrt{r^2 + D^2}$.

Um zu zeigen, daß GAPSBP$_1$ NP-hart ist, benutzen wir die obige Reduktion von GAPCVP$_1$ auf GAPSIVP$_1$. Wir müssen nur die Konstante D ensprechend dem Problem GAPSBP$_1$ anpassen. Gemäß Proposition 2 aus Kapitel 1 gilt für ein beliebiges Gitter L

$$\nu(\mathsf{L}) \leq \tfrac{\sqrt{n}}{2} \lambda_n(\mathsf{L}).$$

Damit ist nach Minkowskis 2. Theorem $n^{(n+1)/2}\det(\mathsf{L})$ eine obere Schranke für $\nu(\mathsf{L})$. Daher können wir durch Wahl der Konstanten D mit

$$D := \max\{r+1, \lceil n^{(n+1)/2}\det(\mathsf{L})\rceil\}$$

die obige Reduktion auch zur Reduktion von GAPCVP_1 auf GAPSBP_1 benutzen.

Da für jedes Gitter M vom Rang $n+1$ $\lambda_{n+1}(\mathsf{M}) \leq \nu(\mathsf{M})$ gilt, wird eine NEIN-Instanz von GAPCVP_1 auf eine NEIN-Instanz von GAPSBP_1 abgebildet. Um zu sehen, daß eine JA-Instanz von GAPCVP_1 auf eine JA- Instanz von GAPSBP_1 abgebildet wird, sei $[\mathbf{v}_1, \ldots, \mathbf{v}_n]$ eine Basis von L mit $\|\mathbf{v}_i\| \leq \nu(\mathsf{L}) \leq D$. Beachte, daß $(\mathbf{x}, D)^\top$ als Linearkombination der Vektoren

$$(\mathbf{v}_1, 0)^\top, \ldots, (\mathbf{v}_n, 0)^\top, (\mathbf{v}-\mathbf{x}, -D)^\top$$

mit ganzzahligen Koeffizienten darstellbar ist. Folglich bilden die Vektoren $(\mathbf{v}_1, 0)^\top, \ldots, (\mathbf{v}_n, 0)^\top, (\mathbf{v}-\mathbf{x}, -D)^\top$ eine Basis von M mit $\nu(\mathsf{M}) \leq \sqrt{r^2+D^2}$. □

Korollar 2. *Das* SVP *und das* CVP *ist in polynomieller Zeit auf das* SIVP *bzw. das* SBP *reduzierbar.*

Beweis. Das Resultat für CVP folgt durch Benutzung der obigen Reduktion. Insbesondere benutzen wir dasselbe Gitter wie im Beweis des vorhergehenden Theorems. Wir nehmen zunächst an, daß wir nur die Distanz $\mu(\mathbf{x}, \mathsf{L})$ von $\mathbf{x} \in \mathbb{R}^m$ zum Gitter $\mathsf{L} \subseteq \mathbb{R}^m$ berechnen wollen. Wir wählen D so, daß D eine obere Schranke für $\lambda_n(\mathsf{L})$ bzw. $\nu(\mathsf{L})$ ist. Mit $\mu(\mathbf{x}, \mathsf{L}) \leq \|\mathbf{x}\|$ können wir

$$D > \max\{\lceil n^{n/2}\det(\mathsf{L})\rceil, \|\mathbf{x}\|\}$$

wählen, wenn wir CVP auf SIVP reduzieren wollen. Wollen wir CVP auf SBP reduzieren, so wählen wir

$$D > \max\{\lceil n^{(n+1)/2}\det(\mathsf{L})\rceil, \|\mathbf{x}\|\}.$$

Die Argumentation im vorhergehenden Beweis zeigt, daß $\sqrt{\mu(\mathbf{x}, \mathsf{L})^2 + D^2}$ die Länge der optimalen Lösung für das SIVP bzw. das SBP bei der obigen Wahl von D ist.

Damit erhält man den nächsten Gittervektor aus der der optimalen Lösung für das SIVP bzw. das SBP. Dies beweist das Resultat für CVP.

Das Resultat für SVP folgt aus dem vorherigen Resultat für CVP und der Polynomialzeit-Reduktion des SVP auf das CVP aus Goldreich, Micciancio, Safra and Seifert [**GMSS**]. □

Man beachte, daß die obige Konstruktion nicht dazu geeignet ist, aus einem Approximationsalgorithmus für SIVP oder SBP einen Approximationsalgorithmus für CVP zu erhalten. Da $D \geq \lceil n^{n/2}\det(\mathsf{L})\rceil$, hat D im Allgemeinen überhaupt keine Beziehung zu $\mu(\mathbf{x}, \mathsf{L})$. Aber jeder Approximationsalgorithmus für SIVP oder SBP, der auf das Gitter M der obigen Konstruktion angewandt

wird, liefert eine Abschätzung für $\mu(\mathbf{x}, \mathsf{L})$, die von D abhängt. Diese ist im Allgemeinen jedoch keine brauchbare Approximation von $\mu(\mathbf{x}, \mathsf{L})$.

2.3. Die Nicht-Approximierbarkeit von SIVP und SBP

Wie wir bereits erwähnten, ist die vorherige Reduktion nicht dazu geeignet, aus einem Approximationsalgorithmus für das SIVP oder SBP einen Approximationsalgorithmus für CVP zu erhalten. Damit kann i.A. kein Nicht-Approximierbarkeitsresultat für das SIVP oder SBP durch die obige Reduktion vom CVP erhalten werden. In der Tat basieren unsere Nicht-Approximierbarkeitsresultate für das SIVP und das SBP auf einer von der vorherigen Reduktion grundsätzlich verschiedenen Reduktion vom CVP. Insbesondere setzt diese neue Reduktion spezielle Eigenschaften der verwendeten CVP-Intanzen voraus. Alle bis heute bekannten NP-harten CVP-Instanzen (z.B. die von [**ABSS, AL, DKS**]) haben jedoch diese speziellen Eigenschaften.

Lemma 1. *Sei* $(\mathsf{L}, \mathbf{x}, r)$, $\mathrm{rg}(\mathsf{L}) = n$, *eine* GAPCVP$_g$ *Instanz mit folgenden zusätzlichen Eigenschaften:*

(1) $\mathbf{x} \notin \mathrm{span}(\mathsf{L})$.

(2) *Es gibt ein Polynom* $q(\cdot)$ *mit* $r = q(n)$.

(3) *Es gibt ein Polynom* $p(\cdot)$ *mit* $\lambda_n(\mathsf{L}) \leq p(n)$ *bzw.* $\nu(\mathsf{L}) \leq p(n)$.

(4) *Ist* $(\mathsf{L}, \mathbf{x}, r)$ *eine* NEIN*-Instanz, so gilt für alle* $\beta \in \mathbb{Z} \setminus \{0\} : \mu(\beta\mathbf{x}, \mathsf{L}) > g \cdot r$.

Dann kann in polynomialler Zeit eine GAPSIVP$_{g'}$ *bzw.* GAPSBP$_{g'}$ *Instanz* (M, s) *mit*

$$\mu(\mathbf{x}, \mathsf{L}) \leq r \Longrightarrow \lambda_{\mathrm{rg}(\mathsf{M})}(\mathsf{M}) \leq s \text{ bzw. } \nu(\mathsf{M}) \leq s$$

und

$$\mu(\mathbf{x}, \mathsf{L}) > g \cdot r \Longrightarrow \lambda_{\mathrm{rg}(\mathsf{M})}(\mathsf{M}) > g' \cdot s \text{ bzw. } \nu(\mathsf{M}) > g' \cdot s$$

konstruiert werden. Für $p(n) = n^\gamma$, $q(n) = n^\delta$ *und* $g(n) = n^\varepsilon$ *ist die neue gap-Funktion*

$$g'\left(\mathrm{rg}(\mathsf{M})\right) = \Omega\left(\mathrm{rg}(\mathsf{M})^{\frac{\varepsilon}{1+2\gamma-2\delta}}\right).$$

Beweis. Sei $(\mathsf{L}, \mathbf{x}, r)$ eine GAPCVP$_g$ Instanz mit den geforderten Eigenschaften und $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ eine Basis des Gitters $\mathsf{L} \subseteq \mathbb{Z}^m$. Wir zeigen nur den Beweis für GAPSIVP$_{g'}$ da der Beweis für GAPSBP$_{g'}$ identisch ist.

Wir wählen zunächst das kleinste $k \in \mathbb{N}$ mit

$$\sqrt{k} \cdot r \geq p(n).$$

Für das von den Spaltenvektoren der Matrix

$$\begin{array}{l} \text{1. Kopie} \\ \\ \vdots \\ \\ k\text{. Kopie} \end{array} \begin{pmatrix} B & & & & \mathbf{x} \\ & \ddots & & & \vdots \\ & & B & & \mathbf{x} \\ & & & \ddots & \vdots \\ & & & B & \mathbf{x} \end{pmatrix} =: \begin{bmatrix} \mathbf{c}_1 & \cdots & \mathbf{c}_{nk} & \mathbf{c}_{nk+1} \end{bmatrix}$$

aufgespannte Gitter M vom Rang $nk+1$ definieren wir die $\text{GAPSIVP}_{g(n)}$ Instanz $(\mathsf{M}, \sqrt{k}r)$. Wir zeigen zunächst die Korrektheit der Konstruktion bzgl. des gaps $g(\cdot)$ als Funktion des Ranges n von L und bestimmen anschließend das aus der Konstruktion resultierende neue gap $g'(\cdot)$ als Funktion des Ranges $\text{rg}(\mathsf{M})$ von M.

Zunächst sei $(\mathsf{L}, \mathbf{x}, r)$ eine JA-Instanz von GAPCVP_g, d.h. $\mu(\mathbf{x}, \mathsf{L}) \leq r$. Nach Konstruktion des Gitters M gilt $\lambda_{\text{rg}(\mathsf{M})}(\mathsf{M}) \leq \max\{\lambda_n(\mathsf{L}), \sqrt{k}\mu(\mathbf{x}, \mathsf{L})\} \leq \max\{\lambda_n(\mathsf{L}), \sqrt{k}r\}$. Nach Wahl von k und mit $\lambda_n(\mathsf{L}) \leq p(n)$ gilt damit folglich $\lambda_{\text{rg}(\mathsf{M})}(\mathsf{M}) \leq \sqrt{k}r$.

Sei nun $(\mathsf{L}, \mathbf{x}, r)$ eine NEIN-Instanz von GAPCVP_g. Für die Länge des Vektors $\mathbf{c}_{nk+1}$ gilt

$$\begin{aligned} \min_{\substack{\mathbf{v} \in \mathsf{L}(\mathbf{c}_1, \ldots, \mathbf{c}_{nk}) \\ \beta \in \mathbb{Z} \setminus \{0\}}} \|\beta \cdot \mathbf{c}_{nk+1} - \mathbf{v}\| &= \sqrt{k} \cdot \min_{\beta \in \mathbb{Z} \setminus \{0\}} \mu(\beta \mathbf{x}, \mathsf{L}) && \text{(Konstr. von } \mathsf{M}) \\ &> \sqrt{k} \cdot g(n) r && \text{(Eigenschaft 4)} \\ &\geq \sqrt{k} r && (g(n) \geq 1) \\ &\geq \lambda_n(\mathsf{L}) && (\lambda_n(\mathsf{L}) \leq p(n)) \\ &= \lambda_{nk}(\mathsf{L}(\mathbf{c}_1, \ldots, \mathbf{c}_{nk})) && \text{(Konstr. von } \mathsf{M}) \end{aligned}$$

Da $\text{rg}(\mathsf{M}) = nk+1$, enthält jede Menge von $\text{rg}(\mathsf{M})$ linear unabhängigen Vektoren mindestens einen Vektor, der von $\mathbf{c}_{nk+1}$ abhängig ist. Folglich gilt

$$\begin{aligned} \lambda_{\text{rg}(\mathsf{M})}(\mathsf{M}) &= \min_{\substack{\mathbf{v} \in \mathsf{L}(\mathbf{c}_1, \ldots, \mathbf{c}_{nk}) \\ \beta \in \mathbb{Z} \setminus \{0\}}} \|\beta \cdot \mathbf{c}_{nk+1} - \mathbf{v}\| \\ &> g(n) \cdot \sqrt{k} r. \end{aligned}$$

Als Funktion des Ranges n von L ist das gap $g(n) = n^{\varepsilon}$. Nun gilt $\text{rg}(\mathsf{M}) = nk + 1$ für das Gitter M und nach Wahl von k können wir $k = O(n^{2\gamma - 2\delta})$ annehmen. Folglich ist das gap für die Instanz $(\mathsf{M}, \sqrt{k}r)$ als Funktion des Ranges

$\mathrm{rg}(\mathsf{M})$ durch

$$\Omega\left(\mathrm{rg}(\mathsf{M})^{\frac{\varepsilon}{1+2\gamma-2\delta}}\right).$$

gegeben. □

Das folgende Lemma kann leicht aus dem Hauptresultat von Dinur, Kindler und Safra [**DKS**, Sec. 4] gefolgert werden. Ein analoges, aber etwas schwächeres Lemma mit einem entsprechend einfachen Beweis kann auch aus Arora, Babai, Stern und Sweedyk [**ABSS**] bzw. Arora und Lund [**AL**] gefolgert werden.

Lemma 2. *Das Problem* $\textsc{gapCvp}_{n^{1/(2\log\log n)}}$ *ist für Instanzen* $(\mathsf{L}, \mathbf{x}, r)$ *mit* $n = \mathrm{rg}(\mathsf{L})$ *und folgenden zusätzlichen Eigenschaften* NP*-hart:*

(1) $\mathbf{x} \notin \mathrm{span}(\mathsf{L})$.

(2) *Es gibt ein Polynom* $q(\cdot)$ *mit* $r = q(n)$.

(3) *Es gibt ein Polynom* $p(\cdot)$ *mit* $\lambda_n(\mathsf{L}) \leq p(n)$.

(4) *Ist* $(\mathsf{L}, \mathbf{x}, r)$ *eine* Nein*-Instanz, so gilt für alle* $\beta \in \mathbb{Z} \setminus \{0\} : \mu(\beta\mathbf{x}, \mathsf{L}) > g \cdot r$.

Wir können nun die Nicht-Approximierbarkeit von Sivp und Sbp zeigen.

Theorem 2.6. *Die Probleme* $\textsc{gapSivp}_{n^{O(1/\log\log n)}}$ *und* $\textsc{gapSbp}_{n^{O(1/\log\log n)}}$ *sind* NP*-hart.*

Beweis. Direkt aus Lemma 1 und Lemma 2 folgt, daß $\textsc{gapSivp}_{n^{O(1/\log\log n)}}$ und $\textsc{gapSbp}_{n^{O(1/\log\log n)}}$ NP-hart sind. □

Korollar 3. *Unter der Annahme* $\mathsf{P} \neq \mathsf{NP}$ *gibt es keinen polynomiellen Approximationsalgorithmus, der das* Sivp *oder* Sbp *bis auf einen Faktor* $n^{O(1/\log\log n)}$ *approximiert.*

2.4. Grenzen für die Nicht-Approximierbarkeit

Während wir im vorherigen Paragraphen 3 untere Schranken für die Nicht-Approximierbarkeit des Sivp und des Sbp erhalten haben, untersuchen wir nun, in wie weit diese verbessert werden können. Hierzu verallgemeinern und kombinieren wir die in einem ähnlichen Zusammenhang verwendeten Ideen und Methoden aus Cai [**Cai2**], Goldreich und Goldwasser [**GG**] mit denen aus Lagarias, Lenstra und Schnorr [**LLS**].

Unser erstes Resultat verwendet die Idee von Cai [**Cai2**], mit Hilfe von sog. Transfer-Theoremen (z.B. Theorem 1.10) Grenzen für Nicht-Approximierbarkeitsresultate zu erhalten.

Theorem 2.7. *Es gibt Konstanten* C *und* C''*, so daß die Probleme* $\textsc{gapSivp}_{Cn}$ *und* $\textsc{gapSbp}_{C''n^{1.5}}$ *in* $\mathsf{NP} \cap \mathsf{co\text{-}NP}$ *enthalten sind.*

Beweis. Per Definition sind GAPSIVP_{Cn} und $\text{GAPSBP}_{C''n^{1.5}}$ in NP enthalten. Wir zeigen jetzt, daß $\text{GAPSIVP}_{Cn} \in \text{co-NP}$ gilt.

Ist (L, r) eine JA-Instanz von GAPSIVP_{Cn}, d.h. $\lambda_n(\mathsf{L}) \leq r$, so gilt nach Transferschranke $1 \leq \lambda_1(\mathsf{L}^*) \cdot \lambda_n(\mathsf{L})$ aus Theorem 1.10, daß $\lambda_1(\mathsf{L}^*) \geq \frac{1}{r}$. Ist (L, r) eine NEIN-Instanz von GAPSIVP_{Cn}, d.h. $\lambda_n(\mathsf{L}) > Cn \cdot r$, so gilt nach Transferschranke $\lambda_1(\mathsf{L}^*) \cdot \lambda_n(\mathsf{L}) \leq Cn$ aus Theorem 1.10, daß $\lambda_1(\mathsf{L}^*) < \frac{1}{r}$. Ein nichtdeterministischer Polynomialzeit-Algorithmus der nur NEIN-Instanzen von GAPSIVP_{Cn} akzeptiert, rät einen Vektor $\mathbf{v} \in \mathsf{L}^*$ und akzeptiert gdw. $\|\mathbf{v}\| < \frac{1}{r}$.

Das Resultat für $\text{GAPSBP}_{C'n}$ folgt analog mit dem Korollar 1 zu Theorem 1.10. □

Das obige Theorem impliziert folgendes Korollar.

Korollar 4. *Es gibt Konstanten C und C'', so daß die Probleme GAPSIVP_{Cn} und $\text{GAPSBP}_{C''n^{1.5}}$ unter Karp-Reduktionen nicht NP-hart sind, es sei denn, daß die Polynomialzeit-Hierachie auf der ersten Stufe kollabiert.*

Durch Kombination der Methoden aus Goldreich und Goldwasser [**GG**] mit denen aus Lagarias, Lenstra und Schnorr [**LLS**] werden wir nun das obige Resultat für SIVP und SBP hinsichtlich der Grenzen $O(n)$ und $O(n^{1.5})$ verbessern. Hierzu verwenden wir die HKZ-Reduktion und das zugehörige Theorem 1.14. Die Idee besteht darin, für $g(n) := \sqrt{n/O(\log(n))}$ mit Hilfe des IP(2)-Protokolls für co-$\text{GAPSVP}_{g/2}$ aus Goldreich und Goldwasser [**GG**] interaktiv zu prüfen, ob eine vorgelegte Gitterbasis eine $g(n)$-approximative HKZ-Basis ist. Nach Theorem 1.14 approximiert der letzte Basisvektor einer $g(n)$-approximativen HKZ-Basis $\lambda_n(\cdot)$ und $\nu(\cdot)$ bis auf einen Faktor $n/O(\sqrt{\log n})$. Hieraus resultiert die verbesserte Grenze $n/O(\sqrt{\log n})$ für die Nicht-Approximierbarkeit des SIVP und des SBP.

Theorem 2.8. *Die Probleme $\text{GAPSIVP}_{n/O(\sqrt{\log n})}$ und $\text{GAPSBP}_{n/O(\sqrt{\log n})}$ sind in $\mathsf{NP} \cap \text{co-IP}(3)$.*

Beweis. Per Definition sind $\text{GAPSIVP}_{n/O(\sqrt{\log n})}$ und $\text{GAPSBP}_{n/O(\sqrt{\log n})}$ in NP enthalten. Wir zeigen jetzt, daß $\text{GAPSIVP}_{n/O(\sqrt{\log n})} \in \text{co-IP}(3)$ gilt.

Für eine beliebige Konstante $c > 0$ definiere die Funktion $g : \mathbb{N} \to \mathbb{R}_+$ durch $g(1) := 1$ und $g(n) := \sqrt{n/(c\log(n))}$ für $n > 1$. Wir geben ein IP(3)-Protokoll für co-$\text{GAPSIVP}_{\sqrt{n}g}$ an, das auf dem IP(2)-Protokoll für co-$\text{GAPSVP}_{g/2}$ aus Goldreich und Goldwasser [**GG**] basiert. Das Protokoll ist in Abbildung 2.1 dargestellt; es führt parallel für $i = 1, \ldots, n$ das IP(2)-Protokoll für co-$\text{GAPSVP}_{g/2}$ auf $(\mathsf{L}^{(n-i+1)}, \|\hat{\mathbf{b}}_i\|/g(n))$ aus. Für Implementierungsdetails verweisen wir auf [**GG**, Sec. 2].

Sei nun zunächst (L, r) eine NEIN-Instanz von $\text{GAPSIVP}_{\sqrt{n}g}$, d.h. $\lambda_n(\mathsf{L}) > \sqrt{n}g \cdot r$. Durch Senden einer HKZ-Basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ für L an den Verifizierer,

Abbildung 2.1. Interaktives 3-Runden Protokoll für „keine kurze Basis“.

$\mathcal{V}(\mathsf{L}, r)$		$\mathcal{P}(\mathsf{L}, r)$
		berechne HKZ-Basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ von L
	$\xleftarrow{\mathbf{b}_1, \ldots, \mathbf{b}_n}$	
verifiziere, daß $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ eine schwach reduzierte Basis für L ist		
verifiziere, daß $\max_i \lVert\mathbf{b}_i\rVert > \sqrt{n}g(n)r$		
berechne für $i = n, \ldots, 1$ die Gitter $\mathsf{L}^{(n-i+1)}$		
wähle für $i = 1, \ldots, n$ $\mathbf{x}_i \in_{\mathrm{u}} B_{R_i}(\mathbf{0}) \cap \mathsf{L}^{(n-i+1)}$ mit $R_i := 2^{n-i+1} \max_{i \le j \le n} \lVert\pi_i(\mathbf{b}_j)\rVert$		
wähle für $i = 1, \ldots, n$ $\boldsymbol{\eta}_i \in_{\mathrm{u}} B_{\lVert\hat{\mathbf{b}}_i\rVert/4}(\mathbf{0}) \cap \mathrm{span}(\mathsf{L}^{(n-i+1)})$		
	$\xrightarrow{\mathbf{x}_i + \boldsymbol{\eta}_i =: \mathbf{t}_i}$	
		setze $\mathbf{v}_i := \textsc{Cvp}(\mathbf{t}_i, \mathsf{L}^{(n-i+1)})$
	$\xleftarrow{\mathbf{v}_i}$	
akzeptiere gdw. $\mathbf{v}_i = \mathbf{x}_i$ für alle $i = 1, \ldots, n$ gilt		

kann der Beweiser sicherstellen, daß $\hat{\mathbf{b}}_i$ ein kürzester Vektor des Gitters $\mathsf{L}^{(n-i+1)}$ für $i = 1, \ldots, n$ ist. Demzufolge gilt also $\mu(\mathbf{x}_i + \boldsymbol{\eta}_i, \mathsf{L}^{(n-i+1)}) \le \lambda_1(\mathsf{L}^{(n-i+1)})/4 < \lambda_1(\mathsf{L}^{(n-i+1)})/2$ für die von $\mathcal{V}$ an $\mathcal{P}$ geschickten Vektoren $\mathbf{x}_i + \boldsymbol{\eta}_i$. Damit ist $\mathbf{x}_i$ der eindeutig bestimmte nächste Gittervektor zu $\mathbf{x}_i + \boldsymbol{\eta}_i$. Sendet der Beweiser $\mathcal{P}$ diese eindeutig bestimmten Vektoren $\mathbf{x}_1, \ldots, \mathbf{x}_n$, so akzeptiert der Verifizierer mit Wahrscheinlichkeit 1.

Sei nun (L, r) eine Ja-Instanz von $\textsc{gapSivp}_{\sqrt{n}g}$, d.h. $\lambda_n(\mathsf{L}) \le r$. Wir nehmen an, daß die vom Prover gesendeten Vektoren $\mathbf{b}_1, \ldots, \mathbf{b}_n$ eine schwach reduzierte Basis für L sind und insbesondere $\max_i \lVert\mathbf{b}_i\rVert > \sqrt{n}g(n)r$ erfüllen. Da $\lambda_n(\mathsf{L}) \le r$ und $\max_i \lVert\mathbf{b}_i\rVert > \sqrt{n}g(n)r$ gilt, kann $\lVert\mathbf{b}_i\rVert \le g(n)\sqrt{i}\lambda_i(\mathsf{L})$ nicht für alle $i = 1, \ldots, n$ erfüllt sein. Nach Theorem 1.14 ist damit $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ keine $g(n)$-approximative HKZ-Basis für L. Da die Basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ schwach reduziert

ist, muß die Bedingung (ii) einer $g(n)$-approximativen HKZ-Basis verletzt sein, d.h. es existiert ein $i_0 \in \{1, \ldots, n\}$ mit $\lambda_1(\mathsf{L}^{(n-i_0+1)}) < \|\hat{\mathbf{b}}_{i_0}\|/g(n)$. Gemäß der Analyse des $\mathsf{IP}(2)$-Protokolls für co-GAPSVP$_{g/2}$ in [**GG**, Claim 3.3] hat ein Beweiser höchstens eine Erfolgswahrscheinlichkeit von $1 - n^{-8c}$ den Test $\mathbf{v}_{i_0} = \mathbf{x}_{i_0}$ für die Instanz $(\mathsf{L}^{(n-i_0+1)}, \|\hat{\mathbf{b}}_{i_0}\|/g(n))$ zu bestehen. Folglich akzeptiert der Verifizierer $\mathcal{V}$ eine JA-Instanz (L, r) höchstens mit Wahrscheinlichkeit $1 - n^{-8c}$. Durch parallele Wiederholungen (siehe [**Gol**, Lemma C.1]) des obigen Beweis-Systems kann diese Wahrscheinlichkeit auf $< 1/2$ gedrückt werden.

Da $\lambda_n(\mathsf{L}) \leq \nu(\mathsf{L})$ gilt und da der Verifizierer $\mathcal{V}$ überprüft, daß die Vektoren $\mathbf{b}_1, \ldots, \mathbf{b}_n$, die vom Beweiser gesandt werden eine Basis für L bilden, ist das obige Protokoll auch ein $\mathsf{IP}(3)$-Protokoll für co-GAPSBP$_{\sqrt{n}g}$. □

Das obige Theorem impliziert in Kombination mit dem Theorem 1.35 folgendes Korollar.

Korollar 5. *Unter Karp-Reduktionen sind die Probleme* GAPSIVP$_{n/O(\sqrt{\log n})}$ *und* GAPSBP$_{n/O(\sqrt{\log n})}$ *nicht* NP*-hart, es sei denn, daß die Polynomialzeit-Hierachie auf der zweiten Stufe kollabiert.*

Kapitel 3

Die Komplexität Diophantischer Approximationen

Paragraph 1 dieses Kapitels gibt eine kurze Einführung in die Theorie der Simultanen Diophantischen Approximationen und insbesondere in das Best Simultaneous Diophantine Approximation (Bsda) Problem. In Paragraph 2 zeigen wir die Nicht-Approximierbarkeit des Bsda Problems bis auf einen großen von der Dimension abhängigen Faktor. Dieses Resultat bestätigt im wesentlichen eine vor 15 Jahren von Lagarias aufgestellte Vermutung, daß selbst die approximative Berechnung von Best Approximationen nicht effizient möglich ist. Andererseits beweisen wir in Paragraph 3 aber auch eine Grenze für die Nicht-Approximierbarkeit des Bsda Problems. Unsere Grenze für die Nicht-Approximierbarkeit präzisiert Lagarias' Vermutung hinsichtlich einer Verbesserung des Ergebnis für die Nicht-Approximierbarkeit. Der Inhalt der Paragraphen 2 und 3 entspricht im wesentlichen dem der Arbeiten [**RSei1, Sei**] und benutzt das Resultat der Arbeit [**RSei3**].

3.1. Simultane Diophantische Best-Approximationen

Simultane Diophantische Approximation ist das Studium der Approximationseigenschaften reeller Zahlen $\alpha_1, \ldots, \alpha_n$ durch rationale Zahlen $p_1/q, \ldots, p_n/q$ mit einem gemeinsamen Hauptnenner q. Trivialerweise gilt für die Güte der Diophantischen Approximation mit Hauptnenner q natürlich $\|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \leq$

$1/(2q)$. Allerdings gibt es Diophantische Approximation wesentlich besserer Güte, wenn man nur eine obere Schranke für den Hauptnenner vorgibt.

Das folgende klassische Theorem (siehe z.B. [**Cas2**]) garantiert, daß ein Vektor $\boldsymbol{\alpha} \in \mathbb{R}^n$ mit einer Güte ε approximiert werden kann, so daß der Hauptnenner q nicht zu groß ist.

Dirichlet's Theorem. *Für einen Vektor $\boldsymbol{\alpha} \in \mathbb{R}^n$ und ein ε, $0 < \varepsilon < 1$, existiert ein Nenner q mit $1 \leq q \leq \varepsilon^{-n}$ und*

$$\|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \leq \varepsilon.$$

Oftmals ist man allerdings daran interessiert, zu vorgegebener Hauptnennerschranke N einen Hauptnenner q, $1 \leq q \leq N$, bestmöglicher Güte zu finden. Diese Aufgabe wird durch das folgende Berechnungsproblem beschrieben.

Definition 3.1. Best Simultaneous Diophantine Approximation (Bsda)
Gegeben: Ein Vektor $\boldsymbol{\alpha} \in \mathbb{R}^n$ und eine Hauptnennerschranke N.
Finde: Einen Nenner $q \in [1 : N]$ mit

$$\|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty = \min_{1 \leq Q \leq N} \|Q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty.$$

Der Kettenbruchalgorithmus bietet für $n = 1$ ein effizientes Verfahren zur Lösung des Bsda Problems, und für festes n kann das Bsda Problem mit Hilfe des LLL-Algorithmus ebenfalls effizient gelöst werden. Für beliebiges n dagegen ist kein Polynomial-Zeit Algorithmus bekannt und auch nicht zu erwarten, da Lagarias [**Lag**] die NP-Vollständigkeit des Bsda Problems zeigte. Gleichzeitig gab Lagarias [**Lag**] aber einen auf dem LLL-Algorithmus basierenden effizienten Approximationsalgorithmus an. Dieser berechnet zu gegebenen rationalen Zahlen $\alpha_1, \ldots, \alpha_n$ und einer Hauptnennerschranke N in Polynomial-Zeit einen Nenner $\tilde{q}$ mit $1 \leq \tilde{q} \leq 2^{n/2}N$, so daß gilt:

$$\max_i \min_{p_i \in \mathbb{Z}} |\tilde{q}\alpha_i - p_i| \leq \sqrt{5n}\, 2^{(n-1)/2} \cdot \min_{1 \leq q \leq N} \max_i \min_{p_i \in \mathbb{Z}} |q\alpha_i - p_i|.$$

Gleichzeitig äußerte Lagarias bzgl. einer möglichen Verbesserung hinsichtlich polynomieller Faktoren allerdings die folgende Vermutung. Existiert ein Polynomial-Zeit Algorithmus, der für gegebene rationale Zahlen $\alpha_1, \ldots, \alpha_n$ sowie einer Hauptnennerschranke N einen Nenner $\tilde{q}$ mit $1 \leq \tilde{q} \leq f(n)N$ berechnet, so daß

$$\max_i \min_{p_i \in \mathbb{Z}} |\tilde{q}\alpha_i - p_i| \leq f(n) \cdot \min_{1 \leq q \leq N} \max_i \min_{p_i \in \mathbb{Z}} |q\alpha_i - p_i|$$

gilt, wobei f ein Polynom in n ist, so gilt $\mathsf{P} = \mathsf{NP}$. Die komplexitätstheoretische Untersuchung dieser Vermutung bzgl. der Nicht-Approximierbarkeit von Diophantischen Best-Approximationen ist der Hauptinhalt dieses Kapitels. Hierzu

definieren wir zunächst das entsprechende Promise-Probleme für das BSDA Problem.

Definition 3.2. Das Promise-Problem GAPBSDA_g, wobei $g(\cdot)$ eine gap-Funktion bezeichnet, ist wie folgt definiert:

> JA-Instanzen sind Tripel $(\boldsymbol{\alpha}, N, \varepsilon) \in (\mathbb{Q}^n, \mathbb{N}_+, \mathbb{Q}_+)$ mit
> $\min_{q\in[1:N]} \|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \leq \varepsilon$,
> NEIN-Instanzen sind Tripel $(\boldsymbol{\alpha}, N, \varepsilon) \in (\mathbb{Q}^n, \mathbb{N}_+, \mathbb{Q}_+)$ mit
> $\min_{q\in[1:gN]} \|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty > g \cdot \varepsilon$,

Wir beweisen in Paragraph 2, daß $\text{GAPBSDA}_{n^{O(1/\log^{0.5+\varepsilon} n)}}$ für jede Konstante $\varepsilon > 0$ fast NP-hart ist. Dies kommt der Vermutung von Lagarias sehr nahe und kann als deren Bestätigung betrachtet werden. Andererseits zeigen wir in Paragraph 3, daß $\text{GAPBSDA}_{n/O(\log n)}$ in $\mathsf{NP} \cap \mathsf{co\text{-}IP}(2)$ enthalten ist. Dieses Resultat besagt, daß $\text{GAPBSDA}_{n/O(\log n)}$ unter Karp-Reduktionen nicht NP-hart ist, es sei denn, daß die Polynomialzeit-Hierachie auf der zweiten Stufe kollabiert. Für einen Nicht-Approximierbarkeitsfaktor $f(n) = n/O(\log n)$ stimmt die Vermutung von Lagarias also nicht mehr.

3.2. Die Nicht-Approximierbarkeit von BSDA

Der nun folgende Beweis der unteren Schranke für die Nicht-Approximierbarkeit des BSDA Problems basiert auf der Dualität zwischen dem Berechnen von Simultanen Diophantischen Approximationen und dem Berechnen von ganzzahligen Relationen. Beispielsweise nutzen Just [**Jus**] und Rössner und Schnorr [**RSch**] diese Dualität, um aus einem effizienten Algorithmen zum Berechnen von kurzen ganzzahligen Relationen einen effizienten Algorithmen zum Berechnen von guten Simultanen Diophantischen Approximationen zu erhalten. Die Güte der von diesen Algorithmen berechneten Diophantischen Approximationen ist in dem Sinne optimal, daß die Dirichlet Schranke bis auf einen von der Dimension abhängigen Faktor erreicht wird.

Im folgenden wird dieser Zusammenhang in die andere Richtung verwendet werden. Insbesondere basiert die untere Schranke für die Nicht-Approximierbarkeit des BSDA Problems auf der Nicht-Approximierbarkeit des $\|\cdot\|_\infty$-SHORTEST INTEGER RELATION Problems, die von Rössner und Seifert [**RSei3**] bewiesen worden ist:

Lemma 3. *Für jede Konstante $\varepsilon > 0$ ist das Problem $\text{GAPSIR}^\infty_{n^{O(1/\log^{0.5+\varepsilon} n)}}$ für Instanzen $(\mathbf{a}, r)$ mit $r = 1$ fast* NP*-hart.*

Das folgende Lemma reduziert die Approximation des $\|\cdot\|_\infty$-SHORTEST INTEGER RELATION Problems auf die Approximation des BSDA Problems.

Lemma 4. *Sei* $(\mathbf{a}, r) \in (\mathbb{Z}^n, \mathbb{Z}_+)$ *eine* GAPSIR$_g^\infty$*-Instanz mit* $r = 1$*. In polynomieller Zeit kann eine* GAPBSDA$_g$*-Instanz* $(\boldsymbol{\alpha}, N, \varepsilon) \in (\mathbb{Q}^{n+1}, \mathbb{N}_+, \mathbb{Q}_+)$ *mit*

$$\lambda_{1,\|\cdot\|_\infty}(\mathsf{L}_\mathbf{a}) = 1 \Longrightarrow \min_{q \in [1:N]} \|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \leq \varepsilon$$

und

$$\lambda_{1,\|\cdot\|_\infty}(\mathsf{L}_\mathbf{a}) > g \Longrightarrow \min_{q \in [1:gN]} \|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty > g \cdot \varepsilon$$

konstruiert werden.

Beweis. Sei $(\mathbf{a}, 1) \in (\mathbb{Z}^n, \mathbb{Z}_+)$ eine GAPSIR$_g^\infty$-Instanz. Zunächst reduzieren wir das Problem ein nicht-triviales $\mathbf{x} \in \mathbb{Z}^n$ mit $\|\mathbf{x}\|_\infty \leq g(n)$ und

$$\langle \mathbf{x}, \mathbf{a} \rangle = 0 \tag{3.1}$$

zu finden auf ein modulares Relationenproblem. Hierzu definieren wir $A := g(n) \sum_{j=1}^n |a_j|$, bestimmen die kleinste Primzahl p_0 mit $p_0 \not| \prod_{j=1}^n a_j$ und definieren $R := \lfloor \log_{p_0} A \rfloor + 1$. Ist b die maximale Bitlänge der Zahlen a_j im Vektor $\mathbf{a} \in \mathbb{Z}^n$, so ist die Bitlänge von $\prod_{j=1}^n a_j$ durch nb beschränkt. Folglich hat das Produkt $\prod_{j=1}^n a_j$ höchstens nb verschiedene Primteiler, so daß p_0 in polynomieller Zeit berechenbar ist. Die Reduktion verwendet folgendes Lemma von Rössner und Seifert [**RSei1**, Lemma A].

Lemma 5. *In polynomieller Zeit ist eine Menge von Primzahlen* $\{Q_1, \ldots, Q_n\}$ *und eine Zahl* $T \in \mathbb{N}_+$ *berechenbar, so daß für* $i = 1, \ldots, n-1$ *gilt:*

(a) $Q_i < Q_{i+1}$,
(b) $\mathrm{ggT}(Q_i,\, p_0 \prod_{j=1}^n a_j) = 1$,
(c) $Q_1^T \geq 4\, g(n)\, (n+1)\, p_0^R$ *und*
(d) $g(n)^{1/T}\, Q_n < (g(n)+1)^{1/T}\, Q_1$.

Mit Hilfe des Chinesischen Restsatzes (siehe z.B. [**BSha**]) bestimmen wir nun für $j = 1, \ldots, n-1$ kleinste positive ganze Zahlen r_j mit

$$r_j \equiv 0 \quad \left(\bmod \prod_{\substack{i=1 \\ i \neq j}}^n Q_i^T\right) \tag{3.2a}$$

$$r_j \equiv a_j \pmod{p_0^R} \tag{3.2b}$$

$$r_j \not\equiv 0 \pmod{Q_j}, \tag{3.2c}$$

wobei $Q_1, \ldots, Q_n$ durch Lemma 5 gegeben sind. Man beachte, daß (3.2c) eine Konsequenz aus (3.2a) und (3.2b) ist; denn ist r_j^0 die kleinste positive ganze

Lösung für (3.2a) und (3.2b), so definieren wir

$$r_j := \begin{cases} r_j^0 & \text{falls } r_j^0 \not\equiv 0 \pmod{Q_j}, \\ r_j^0 + p_0^R \left(\prod_{\substack{i=1 \\ i \neq j}}^{n} Q_i^T \right) & \text{sonst.} \end{cases}$$

Mit $\mathrm{ggT}(p_0^R \prod_{i=1}^{n} Q_i^T / Q_j^T, Q_j) = 1$ wegen (b) von Lemma 5 gilt $r_j \not\equiv 0 \pmod{Q_j}$ für $j = 1, \ldots, n-1$, d.h. (3.2c) gilt für jede Wahl von r_j. Definieren wir nun $\mathbf{r} := (r_1, \ldots, r_n)$, so erhalten wir aus (3.2b) und $A < p_0^R$ die Identität

$$\begin{aligned} &\{\mathbf{x} \in \mathbb{Z}^n \cap C_{g(n)}(\mathbf{0}) \mid \langle \mathbf{a}, \mathbf{x} \rangle = 0\} \\ &= \{\mathbf{x} \in \mathbb{Z}^n \cap C_{g(n)}(\mathbf{0}) \mid \langle \mathbf{r}, \mathbf{x} \rangle \equiv 0 \pmod{p_0^R}\}. \end{aligned}$$

Für die Gitter $\mathsf{L}_{\mathbf{a}}$ und $\mathsf{L}_{\mathbf{r},p_0^R}$ gilt also $\mathsf{L}_{\mathbf{a}} \cap C_{g(n)}(\mathbf{0}) = \mathsf{L}_{\mathbf{r},p_0^R} \cap C_{g(n)}(\mathbf{0})$. Weiter definieren wir für einen Vektor $\mathbf{x} \in \mathbb{Z}^n$ mit $1 \leq \|\mathbf{x}\|_\infty \leq g(n)$

$$Z := \sum_{j=1}^{d} x_j r_j, \qquad H := \sum_{j=1}^{d} r_j \qquad \text{und} \qquad B := \prod_{j=1}^{d} Q_j^T.$$

Nach Definition gilt $|Z| \leq g(n)H$ und insbesondere impliziert (c) von Lemma 5

$$r_j \leq r_j^0 + p_0^R \left(\prod_{\substack{i=1 \\ i \neq j}}^{n} Q_i^T \right) \leq 2p_0^R \frac{B}{Q_j^T} \leq \frac{1}{2g(n)(n+1)} B,$$

folglich gilt

$$g(n)H < 1/2B.$$

Unmittelbar aus der obigen Konstruktion ergibt sich für das Gitter $\mathsf{L}_{\mathbf{r},p_0^R}$ die folgende Behauptung.

Behauptung 1. *Für das Gitter* $\mathsf{L}_{\mathbf{r},p_0^R}$ *gilt*

$$\begin{aligned} &\lambda_{1,\|\cdot\|_\infty}(\mathsf{L}_{\mathbf{r},p_0^R}) = 1 \\ \Longrightarrow &\exists Z \colon 1 \leq |Z| \leq H \wedge Z \equiv 0 (\mathrm{mod} p_0^R) \wedge \forall_{j=1}^{n} Z \equiv x_j r_j (\mathrm{mod} Q_j^T) \wedge \mathbf{x} \in C_1(\mathbf{0}), \\ &\lambda_{1,\|\cdot\|_\infty}(\mathsf{L}_{\mathbf{r},p_0^R}) > g \\ \Longrightarrow &\forall Z \colon 1 \leq |Z| \leq gH \wedge Z \equiv 0 (\mathrm{mod} p_0^R) \wedge \forall_{j=1}^{n} Z \equiv x_j r_j (\mathrm{mod} Q_j^T) \Rightarrow \mathbf{x} \notin C_g(\mathbf{0}). \end{aligned}$$

Die Konstruktion einer GAPBSDA-Instanz mit den erforderlichen Eigenschaften wird nun in folgender Behauptung gezeigt werden.

Behauptung 2. *Für die* GAPBSDA*-Instanz* $(\boldsymbol{\alpha}, H, \frac{1}{Q_1^T})$ *mit*

$$\alpha_0 := \tfrac{1}{p_0^R} \quad \textit{und} \quad \alpha_j := \tfrac{r_j^\star}{Q_j^T}, \quad 1 \leq j \leq n,$$

wobei $r_j^\star$, $1 \le r_j^\star < Q_j^T$, *das eindeutig bestimmte Inverse zu* $r_j \pmod{Q_j^T}$ *bezeichnet, gilt*

$$\exists Z\colon 1 \le |Z| \le H \wedge Z \equiv 0(\mathrm{mod} p_0^R) \wedge \forall_{j=1}^n Z \equiv x_j r_j (\mathrm{mod} Q_j^T) \wedge \mathbf{x} \in C_1(\mathbf{0})$$
$$\Longrightarrow \exists Z\colon 1 \le |Z| \le H \wedge \forall_{j=0}^n \min_{n\in\mathbb{Z}} |Z\alpha_j - n| \le \tfrac{1}{Q_1^T},$$
$$\forall Z\colon 1 \le |Z| \le gH \wedge Z \equiv 0(\mathrm{mod} p_0^R) \wedge \forall_{j=1}^n Z \equiv x_j r_j (\mathrm{mod} Q_j^T) \Rightarrow \mathbf{x} \notin C_g(\mathbf{0})$$
$$\Longrightarrow \forall Z\colon 1 \le |Z| \le gH \Rightarrow \forall_{j=0}^n \min_{n\in\mathbb{Z}} |Z\alpha_j - n| > \tfrac{g}{Q_1^T}$$

Beweis. Sei zunächst

$$\exists Z\colon 1 \le |Z| \le H \wedge Z \equiv 0(\mathrm{mod} p_0^R) \wedge \forall_{j=1}^n Z \equiv x_j r_j (\mathrm{mod} Q_j^T) \wedge \mathbf{x} \in C_1(\mathbf{0})$$

erfüllt. Offensichtlich existiert damit ein Z mit $1 \le |Z| \le H$ und insbesondere gilt wegen $Z \equiv 0(\mathrm{mod} p_0^R)$ dann auch

$$\min_{n\in\mathbb{Z}} \left| Z\tfrac{1}{p_0^R} - n \right| = 0.$$

Überdies hinaus gilt für den Nenner Z wegen (3.2c) and (a) von Lemma 5 für $1 \le j \le n$

$$\min_{n\in\mathbb{Z}} \left| Z\tfrac{r_j^\star}{Q_j^T} - n \right| = \min_{n\in\mathbb{Z}} \left| \tfrac{x_j r_j r_j^\star}{Q_j^T} - n \right| = \min_{n\in\mathbb{Z}} \left| \tfrac{x_j}{Q_j^T} - n \right| \le \tfrac{1}{Q_j^T} \le \tfrac{1}{Q_1^T}.$$

Zum Beweis der zweiten Implikation nehmen wir an, daß

$$\exists Z\colon 1 \le |Z| \le gH \wedge \forall_{j=0}^n \min_{n\in\mathbb{Z}} |Z\alpha_j - n| \le \tfrac{g}{Q_1^T}$$

gilt. Offensichtlich existiert damit wieder ein Z mit $1 \le |Z| \le H$ und insbesondere gilt wegen (c) von Lemma 5

$$\frac{1}{p_0^R} > \frac{g(n)}{Q_1^T},$$

was in Verbindung mit $\min_{n\in\mathbb{Z}} |Z\alpha_j - n| \le \frac{g(n)}{Q_1^T}$ insbesondere $\min_{n\in\mathbb{Z}} |Z\frac{1}{p_0^R} - n| = 0$ impliziert. Folglich gilt $Z \equiv 0(\mathrm{mod} p_0^R)$. Mit (a) und (d) von Lemma 5 gilt aber auch

$$\frac{g(n)+1}{Q_j^T} > \frac{g(n)}{Q_1^T},$$

welches durch Kombination mit $\min_{n\in\mathbb{Z}} |Z\alpha_j - n| \le \frac{g(n)}{Q_1^T}$ dann aber $\min_{n\in\mathbb{Z}} |Z\alpha_j - n| \le \frac{g(n)}{Q_j^T}$ erzwingt. Dies ist aber nur unter der Vorraussetzung möglich, daß

$$Z \equiv x_j r_j \pmod{Q_j^T} \wedge \mathbf{x} \in C_g(\mathbf{0})$$

erfüllt ist. □

Da die gesamte Konstruktion in polynomieller Zeit durchführbar ist, folgt der Beweis des Lemmas aus den beiden obigen Behauptungen. □

Wir können nun die Nicht-Approximierbarkeit von BSDA zeigen.

Theorem 3.3. *Das Problem* $\text{GAPBSDA}_{n^{O(1/\log^{0.5+\varepsilon} n)}}$ *ist für jede Konstante* $\varepsilon > 0$ *fast* NP*-hart.*

Beweis. Aus Lemma 4 und Lemma 3 folgt, daß $\text{GAPBSDA}_{n^{O(1/\log^{0.5+\varepsilon} n)}}$ für jede Konstante $\varepsilon > 0$ fast NP-hart ist. □

Korollar 6. *Unter der Annahme* $\mathsf{NP} \not\subseteq \mathsf{QP}$ *gibt es keinen polynomiellen Approximationsalgorithmus, der für gegebene* $\alpha_1, \ldots, \alpha_n$ *und Hauptnennerschranke* N *einen Nenner* $\tilde{q}$ *mit* $1 \leq \tilde{q} \leq n^{O(1/\log^{0.5+\varepsilon} n)} N$ *berechnet, wobei* $\varepsilon > 0$ *eine beliebige Konstante ist, so daß* $\tilde{q}$ *bis auf einen Faktors* $n^{O(1/\log^{0.5+\varepsilon} n)}$ *ein simultaner Diophantischer Best Approximations Nenner für* $\alpha_1, \ldots, \alpha_n$ *mit Hauptnennerschranke* N *ist.*

3.3. Grenzen für die Nicht-Approximierbarkeit

In diesem Abschnitt zeigen wir, daß das Promise-Problem $\text{GAPBSDA}_{n/O(\log n)}$ in $\mathsf{NP} \cap \mathsf{co\text{-}IP}(2)$ enthalten ist. Dies impliziert, daß $\text{GAPBSDA}_{n/O(\log n)}$ unter Karp-Reduktionen nicht NP-hart ist, falls nicht die Polynomialzeit-Hierarchie auf der zweiten Stufe kollabiert.

Theorem 3.4. *Das Problem* $\text{GAPBSDA}_{n/O(\log n)}$ *ist in* $\mathsf{NP} \cap \mathsf{co\text{-}IP}(2)$.

Beweis. Per Definition ist $\text{GAPBSDA}_{n/O(\log n)}$ in NP enthalten. Wir zeigen jetzt, daß $\text{GAPBSDA}_{n/O(\log n)} \in \mathsf{co\text{-}IP}(2)$ gilt.

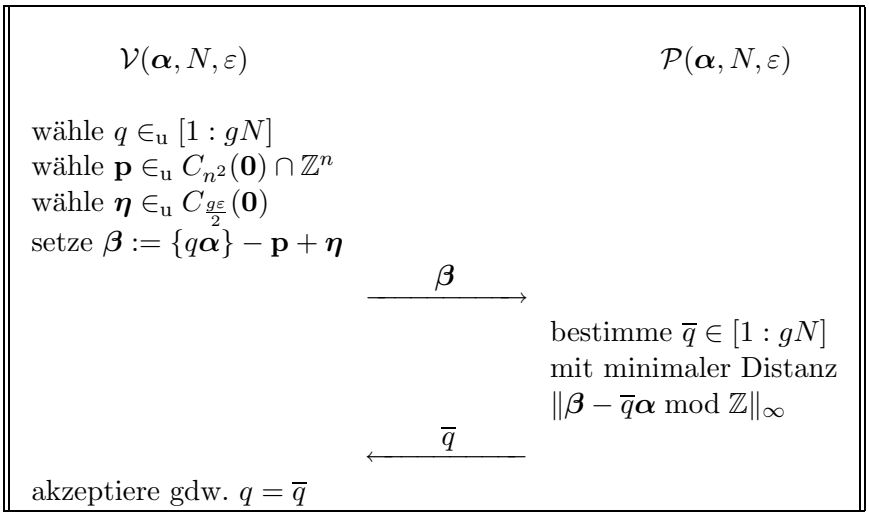
Eine $\text{GAPBSDA}_{n/O(\log n)}$-Instanz $(\boldsymbol{\alpha}, N, \varepsilon)$ erfüllt für $g(n) = n/O(\log n)$ entweder das Versprechen $\min_{q\in[1:N]} \|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \leq \varepsilon$, oder aber das Versprechen $\min_{q\in[1:gN]} \|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty > g \cdot \varepsilon$. Der Beweiser behauptet nun, daß $\min_{q\in[1:gN]} \|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty > g \cdot \varepsilon$ gilt.

Zunächst beschreiben wir die Idee des interaktiven Protokolls, das eine große Änlichkeit mit dem Beweis des klassischen Theorems von Dirichlet [**Dir**] über Diophantische Approximationen aufweist. Wir zentrieren um jeden Punkt $q\boldsymbol{\alpha} - \mathbf{p}$ mit $1 \leq q \leq gN$ und $\mathbf{p} \in \mathbb{Z}^n$ den Würfel $C_r(q\boldsymbol{\alpha} - \mathbf{p})$ mit $r = g \cdot \varepsilon/2$. Der Verifizierer wählt zunächst zufällig einen solchen Punkt $q\boldsymbol{\alpha} - \mathbf{p}$ und wählt anschließend in dem entsprechenden Würfel $C_r(q\boldsymbol{\alpha} - \mathbf{p})$ einen zufälligen Vektor $\boldsymbol{\beta}$. Nun sendet der Verifizierer den Vektor $\boldsymbol{\beta}$ an den Beweiser und akzeptiert gdw. der Beweiser den Nenner q zurückschickt. Ein ehrlicher Beweiser kann diesen Nenner q leicht finden, da q eindeutig bestimmt ist. Versucht der Beweiser dagegen zu betrügen, d.h. es gilt $\min_{q\in[1:N]} \|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \leq \varepsilon$, so existiert für jeden Nenner q mindestens ein weiterer Nenner $q' \neq q$ und ein Vektor $\mathbf{p}' \in \mathbb{Z}^n$ mit

$\|q\boldsymbol{\alpha}-\mathbf{p}-q'\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty = \|q\boldsymbol{\alpha}-\mathbf{p}-(q'\boldsymbol{\alpha}-\mathbf{p}')\|_\infty \leq \varepsilon$. In diesem Fall aber haben die Würfel $C_r(q\boldsymbol{\alpha}-\mathbf{p})$ und $C_r(q'\boldsymbol{\alpha}-\mathbf{p}')$ einen großen gemeinsamen Durchschnitt, da ihre Seitenlängen ungefähr das n-fache ihres Mittelpunktabstandes betragen. Folglich gibt es eine große Wahrscheinlichkeit dafür, daß unehrliche Beweiser das Protokoll nicht bestehen. Denn im Fall $\boldsymbol{\beta} \in C_r(q\boldsymbol{\alpha}-\mathbf{p}) \cap C_r(q'\boldsymbol{\alpha}-\mathbf{p}')$ kann der Verifizierer den Nenner q oder den Nenner q' gewählt haben — beide werden allerdings mit gleicher Wahrscheinlichkeit gezogen.

Für eine beliebige Konstante c mit $0 < c < 1/2$ definiere die Funktion $g : \mathbb{N} \to \mathbb{R}_+$ durch $g(1) := 1$ und $g(n) := n/(c\ln(n))$ für $n > 1$. Wir geben ein $\mathsf{IP}(2)$-Protokoll für co-GAPBSDA$_g$ an. Das Protokoll ist in Abbildung 3.1 dargestellt; für Implementierungsdetails verweisen wir auf [**GG**, Sec. 2].

Abbildung 3.1. Interaktives 2-Runden Protokoll für „keine gute Approximation“.



Sei nun zunächst $(\boldsymbol{\alpha}, N, \varepsilon)$ eine NEIN-Instanz von GAPBSDA$_g$:

Behauptung 3. *Gilt* $\min_{q\in[1:gN]} \|q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty > g\cdot\varepsilon$*, so existiert ein Beweiser* $\mathcal{P}$*, so daß der Verifizierer* $\mathcal{V}$ *nach Interaktion mit* $\mathcal{P}$*, mit Wahrscheinlichkeit* 1 *akzeptiert.*

Beweis. Für jede Nachricht $\boldsymbol{\beta}$ des Verifizierers $\mathcal{V}$ an den Beweiser $\mathcal{P}$ ist der Nenner $q \in [1 : gN]$ eindeutig bestimmt, d.h. es gibt nur ein q mit $\|\boldsymbol{\beta} - q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \leq \frac{g\cdot\varepsilon}{2}$. Denn gäbe es einen weiteren solchen Nenner $q' \in [1 : gN]$ mit $q \neq q'$, so wäre für $(q - q') \in [1 : gN]$ (o.B.d.A. sei $q > q'$)

$$\begin{aligned} & \|(q-q')\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \\ \leq\ & \|\boldsymbol{\beta} - q\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty + \|\boldsymbol{\beta} - q'\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \\ \leq\ & g\cdot\varepsilon \end{aligned}$$

erfüllt — ein Widerspruch. Auf Grund dieser Eindeutigkeit kann ein ehrlicher Beweiser das richtige q bestimmen und besteht folglich immer das Protokoll. □

Nun betrachten wir den Fall, daß $(\boldsymbol{\alpha}, N, \varepsilon)$ eine NEIN-Instanz von GAPBSDA$_g$ ist:

Behauptung 4. *Existiert ein $q^* \in [1\colon N]$ mit $\|q^*\boldsymbol{\alpha} \bmod \mathbb{Z}\|_\infty \leq \varepsilon$, so gilt für jeden Beweiser $\tilde{\mathcal{P}}$, daß der Verifizierer $\mathcal{V}$ nach Interaktion mit $\tilde{\mathcal{P}}$, mit Wahrscheinlichkeit höchstens $1 - O(1/n^{2c})$ akzeptiert.*

Beweis. Zunächst bemerken wir, daß $q' := q + q^*$ bei zufälliger uniformer Wahl von $q \in_{\mathrm{u}} [1 : gN]$ höchstens mit Wahrscheinlichkeit $1/g$ nicht in $[1 : gN]$ enthalten ist. Offensichtlich erfüllt q' allerdings

$$\|\{q\boldsymbol{\alpha}\} - \mathbf{p} - \{q'\boldsymbol{\alpha}\} \bmod \mathbb{Z}\|_\infty \leq \varepsilon,$$

d.h. es existiert ein $\mathbf{p}^* \in C_2(\mathbf{0}) \cap \mathbb{Z}^n$ mit

$$\|\{q\boldsymbol{\alpha}\} - \mathbf{p} - (\{q'\boldsymbol{\alpha}\} - \mathbf{p}')\|_\infty \leq \varepsilon$$

für $\mathbf{p}' := \mathbf{p} + \mathbf{p}^* \in \mathbb{Z}^n$. Man bemerke nun, daß der Punkt $\{q\boldsymbol{\alpha}\} - \mathbf{p}$ mit Wahrscheinlichkeit 1 in dem Würfel $C_{1+n^2}(\mathbf{0})$ enthalten ist, wohingegen der Punkt $\{q'\boldsymbol{\alpha}\} - \mathbf{p}'$ nur mit Wahrscheinlichkeit $\geq (1 - 4/(2n^2 + 1))^n$ in dem Würfel $C_{1+n^2}(\mathbf{0})$ enthalten ist.

Betrachten wir nun die Nachricht $\boldsymbol{\beta} = \{q\boldsymbol{\alpha}\} - \mathbf{p} + \boldsymbol{\eta}$ des Verifizierers $\mathcal{V}$ als Zufallsvariable, so definiert $\boldsymbol{\beta}' := \{q'\boldsymbol{\alpha}\} - \mathbf{p}' + \boldsymbol{\eta}$ eine neue Zufallsvariable. Bis auf die Wahrscheinlichkeiten, daß q' nicht in $[1 : gN]$ und $\{q'\boldsymbol{\alpha}\} - \mathbf{p}'$ nicht in dem Würfel $C_{1+n^2}(\mathbf{0})$ enthalten ist, sind die Zufallsvariablen $\boldsymbol{\beta}$ und $\boldsymbol{\beta}'$ identisch verteilt.

Insbesondere gilt für die Zufallsvariablen $\boldsymbol{\beta}$, $\boldsymbol{\beta}'$ und einen beliebigen Beweiser $\tilde{\mathcal{P}}$

$$\begin{aligned}
& \Pr_{\boldsymbol{\beta}}[\widetilde{P} \text{ antortet } q \text{ auf } \boldsymbol{\beta}] \\
= \;& 1/2 \left(\Pr_{\boldsymbol{\beta}}[\widetilde{P} \text{ antwortet } q \text{ auf } \boldsymbol{\beta}] - \Pr_{\boldsymbol{\beta}'}[\widetilde{P} \text{ antwortet } q \text{ auf } \boldsymbol{\beta}'] \right) + \\
& 1/2 \Pr_{\boldsymbol{\beta}}[\widetilde{P} \text{ antwortet } q \text{ auf } \boldsymbol{\beta}] + 1/2 \Pr_{\boldsymbol{\beta}'}[\widetilde{P} \text{ antwortet } q \text{ auf } \boldsymbol{\beta}'] \\
= \;& 1/2 \|\boldsymbol{\beta} - \boldsymbol{\beta}'\|_{\mathrm{SD}} + \\
& 1/2 \Pr_{\boldsymbol{\beta}}[\widetilde{P} \text{ antwortet } q \text{ auf } \boldsymbol{\beta}] + 1/2 \Pr_{\boldsymbol{\beta}'}[\widetilde{P} \text{ antwortet } q \text{ auf } \boldsymbol{\beta}'],
\end{aligned}$$

wobei $\|\boldsymbol{\beta} - \boldsymbol{\beta}'\|_{\mathrm{SD}}$ die statistische Distanz der Zufallsvariablen $\boldsymbol{\beta}$ und $\boldsymbol{\beta}'$ bezeichnet. Für zwei Zufallsvariablen X und X' über dem Wahrscheinlichkeitsraum $\mathcal{X}$ ist die *statistische Distanz* zwischen X und X' durch $\|X - X'\|_{\mathrm{SD}} :=$

$\frac{1}{2}\sum_{x\in\mathcal{X}} |\Pr_X[X = x] - \Pr_{X'}[X' = x]|$ definiert. Aus der letzten Gleichung erhalten wir

$$\begin{aligned}
\Pr_{\boldsymbol{\beta}}[\widetilde{P} \text{ antwortet } q \text{ auf } \boldsymbol{\beta}] &= \|\boldsymbol{\beta} - \boldsymbol{\beta}'\|_{\mathrm{SD}} + \Pr_{\boldsymbol{\beta}'}[\widetilde{P} \text{ antwortet } q \text{ auf } \boldsymbol{\beta}'] \\
&= \|\boldsymbol{\beta} - \boldsymbol{\beta}'\|_{\mathrm{SD}} + 1 - \Pr_{\boldsymbol{\beta}'}[\widetilde{P} \text{ antwortet } \textit{nicht } q \text{ auf } \boldsymbol{\beta}'] \\
&\leq \|\boldsymbol{\beta} - \boldsymbol{\beta}'\|_{\mathrm{SD}} + 1 - \Pr_{\boldsymbol{\beta}'}[\widetilde{P} \text{ antwortet } q' \text{ auf } \boldsymbol{\beta}'].
\end{aligned}$$

Nun sind die Ereignisse $[\widetilde{P}$ antwortet q auf $\boldsymbol{\beta}]$ und $[\widetilde{P}$ antwortet q' auf $\boldsymbol{\beta}']$ bis auf die Wahrscheinlichkeiten, daß q' nicht aus $[1 : gN]$ und $\{q'\boldsymbol{\alpha}\} - \mathbf{p}'$ nicht in dem Würfel $C_{1+n^2}(\mathbf{0})$ enthalten ist gleichwahrscheinlich. Demzufolge erhalten wir unter Benutzung der vorhergehenden Abschätzung

$$\begin{aligned}
2 \cdot \Pr_{\boldsymbol{\beta}}[\widetilde{P} \text{ antwortet } q \text{ auf } \boldsymbol{\beta}] &\leq \Pr_{\boldsymbol{\beta}}[\widetilde{P} \text{ antwortet } q \text{ auf } \boldsymbol{\beta}] + \\
&\quad \Pr_{\boldsymbol{\beta}'}[\widetilde{P} \text{ antwortet } q' \text{ auf } \boldsymbol{\beta}'] + \tfrac{1}{g} + \tfrac{2}{n} \\
&\leq \|\boldsymbol{\beta} - \boldsymbol{\beta}'\|_{\mathrm{SD}} + 1 + \tfrac{1}{g} + \tfrac{2}{n}.
\end{aligned}$$

Folglich müssen wir noch für jedes $q \in [1 : gN]$ die statistische Distanz der Zufallsvariablen $\boldsymbol{\beta}$ und $\boldsymbol{\beta}'$ nach oben beschränken.

Setzen wir $\delta := \varepsilon/(g \cdot \varepsilon/2) = 2/g$ und normalisieren wir die Seitenlängen der Würfel $C_{g\varepsilon/2}(\cdot)$, so ergibt sich die statistische Distanz der Zufallsvariablen $\boldsymbol{\beta}$ und $\boldsymbol{\beta}'$ als die statistische Distanz der Verteilungen

$$D_1 : \text{Uniforme Verteilung auf } C_1(\mathbf{0})$$

und

$$D_2 : \text{Uniforme Verteilung auf } C_1(\delta \cdot \mathbf{1}).$$

Aus der Identität

$$||D_1 - D_2||_{\mathrm{SD}} = \frac{1}{2} \cdot \frac{\mathrm{vol}(C_1(\mathbf{0})) \triangle \mathrm{vol}(C_1(\delta \cdot \mathbf{1}))}{\mathrm{vol}(C_1(\mathbf{0}))},$$

wobei $A \triangle B$ die symmetrische Differenz der Mengen A und B bezeichnet und der Abschätzung

$$\frac{\mathrm{vol}(C_1(\mathbf{0})) \triangle \mathrm{vol}(C_1(\delta \cdot \mathbf{1}))}{\mathrm{vol}(C_1(\mathbf{0}))} \leq 2 \cdot (1 - (1 - \delta)^n)$$

erhalten wir für die statistische Distanz der Verteilungen D_1 und D_2 eine obere Schranke:

$$\begin{aligned} ||D_1 - D_2||_{\mathrm{SD}} &\leq 1 - \left(1 - \frac{2}{g}\right)^n \\ &= 1 - \left(1 - \frac{2c \cdot \ln n}{n}\right)^n \\ &\leq 1 - e^{-2c\cdot\ln n}\left(1 - \frac{(2c \cdot \ln n)^2}{n}\right) \qquad \text{mit [\textbf{MR}, Prop. B.3]} \\ &\leq 1 - \frac{1}{n^{2c}}. \end{aligned}$$

Insgesamt erhalten wir damit für einen beliebigen Beweiser $\tilde{\mathcal{P}}$, daß für genügend großes n

$$\begin{aligned} \Pr_{\boldsymbol{\beta}}[\widetilde{P} \text{ antwortet } q \text{ auf } \boldsymbol{\beta}] &\leq \tfrac{1}{2}\|\boldsymbol{\beta} - \boldsymbol{\beta}'\|_{\mathrm{SD}} + \tfrac{1}{2} + \tfrac{1}{2g} + \tfrac{1}{n} \\ &= 1 - \tfrac{1}{2n^{2c}} + \tfrac{c\ln n}{2n} + \tfrac{1}{n} \\ &\leq 1 - O(1/n^{2c}) \qquad \text{mit } c < 1/2 \end{aligned}$$

gilt, womit der Beweis der Behauptung beendet ist. □

Durch parallele Wiederholungen (siehe [**Gol**, Lemma C.1]) des obigen Beweis-Systems kann die Wahrscheinlichkeit in der letzten Behauptung auf $< 1/2$ gedrückt werden. □

Das obige Theorem impliziert in Kombination mit Theorem 1.35 folgendes Korollar.

Korollar 7. *Unter Karp-Reduktionen ist das Problem* GAPBSDA$_{n/O(\log n)}$ *nicht* NP*-hart, es sei denn, daß die Polynomialzeit-Hierachie auf der zweiten Stufe kollabiert.*

Kapitel 4

Anwendungen schwieriger Gitterprobleme

In Paragraph 1 dieses Kapitels stellen wir die notwendigen Grundlagen für Ajtai's Theorem, sowie das Theorem selbst vor. Gleichzeitig zeigen wir zwei leicht zu beweisende Aussagen dieses Theorems. Den schwierigen Teil des Beweises von Ajtai's Theorem skizzieren wir im Paragraphen 2. Im Paragraph 3 untersuchen wir die Konsequenzen der Resultate aus Kapitel 2 zur Konstruktion von im Durchschnitt schwierigen Gitterproblemen am skizzierten Beweis von Ajtai's Theorem.

4.1. Ajtai's Theorem

Seien n, m und q positive ganze Zahlen und $\mathbb{Z}_q^{n\times m}$ die Menge der $n\times m$ Matrizen über $\mathbb{Z}_q$. Für jedes $M \in \mathbb{Z}_q^{n\times m}$ definiert die Menge

$$\Lambda(M) := \{\mathbf{v} \in \mathbb{Z}^m \mid M \cdot \mathbf{x} \equiv \mathbf{0} \bmod q\}$$

ein Gitter, da $\Lambda(M)$ eine diskrete additive Untergruppe des $\mathbb{Z}^m$ ist. Wir definieren nun für $n, m, q \in \mathbb{Z}_+$ die Klasse $\Lambda_{n,m,q}$ von Gittern durch

$$\Lambda_{n,m,q} := \{\Lambda(M) \mid M \in \mathbb{Z}_q^{n\times m}\}.$$

Unter der uniformen Wahl eines Gitters aus der Klasse $\Lambda_{n,m,q}$, kurz $\Lambda \in_{\mathrm{u}} \Lambda_{n,m,q}$, verstehen wir die uniforme Wahl einer Matrix $M \in \mathbb{Z}_q^{n\times m}$.

Ajtai's Theorem. *Es gibt Konstanten c_1, c_2 und c_3, so daß folgendes gilt. Gibt es einen probabilistischen Polynomial-Zeit Algorithmus $\mathcal{A}$, der in einem uniform gewählten Gitter $\Lambda \in_u \Lambda_{n,m,q}$ mit $m = \Theta(n)$ und $q = \Theta(n^3)$ einen nicht trivialen Vektor $\mathbf{x}$ der Länge höchstens n berechnet, so gibt es einen probabilistischen Polynomial-Zeit Algorithmus $\mathcal{B}$, der für ein beliebiges Gitter L vom Rang n und beliebiges $\varepsilon > 0$ mit Wahrscheinlichkeit $\geq 1/2$ folgende Probleme löst:*

(i) SIVP *bis auf Faktor $n^{c_1+\varepsilon}$:*
Finde n linear unabhängige Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathsf{L}$ mit $\max_i \|\mathbf{v}_i\| \leq n^{c_1+\varepsilon}\lambda_n(\mathsf{L})$.

(ii) SBP *bis auf Faktor $n^{c_2+\varepsilon}$:*
Finde eine Basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ von L mit $\max_i \|\mathbf{b}_i\| \leq n^{c_2+\varepsilon}\nu(\mathsf{L})$.

(iii) SVP *bis auf Faktor $n^{c_3+\varepsilon}$:*
Finde die Länge des kürzesten Vektors in L bis auf einen Faktor von $n^{c_3+\varepsilon}$, d.h. eine Abschätzung $\tilde{\lambda}_1$ mit $\tilde{\lambda}_1 \leq \lambda_1(\mathsf{L}) \leq n^{c_3+\varepsilon}\tilde{\lambda}_1$.

Man beachte, daß nach Minkwoski's 1. Theorem für jedes $c > 0$ ein $c' > 0$ existiert, so daß für jedes $\Lambda \in \Lambda_{n,c'n,n^c}$ in der Tat $\lambda_1(\Lambda) \leq n$ gilt.

Beweis. Wir zeigen zunächst, wie die Probleme (ii) und (iii) für $c_2 = c_1 + 0.5$ und $c_3 = c_1 + 1$ mit Hilfe eines n^{c_1}-Approximationsalgorithmus für das SIVP gelöst werden können. Im nächsten Paragraphen skizzieren wir für $c_1 = 3 + \varepsilon$, $\varepsilon > 0$, entsprechend der Analyse von Cai und Nerurkar [**CN**], den Beweis des schwierigeren Teils (i).

Nach Annahme berechnet der n^{c_1}-Approximationsalgorithmus für das SIVP für ein beliebiges Gitter L vom Rang n linear unabhängige Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathsf{L}$ mit $\max_i \|\mathbf{v}_i\| \leq n^{c_1}\lambda_n(\mathsf{L})$. Nach Proposition 2 können wir aus diesen n linear unabhängigen Vektoren in polynomieller Zeit eine Basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ von L mit $\max_i \|\mathbf{b}_i\| \leq n^{c_1+0.5}\lambda_n(\mathsf{L}) \leq n^{c_1+0.5}\nu(\mathsf{L})$ berechnen. Dies beweist den Teil (ii).

Wir beweisen nun den Teil (iii). Wenden wir den n^{c_1}-Approximationsalgorithmus für das SIVP auf das duale Gitter L^* eines gegebenen Gitters L vom Rang n an, so erhalten wir n linear unabhängige Vektoren $\mathbf{v}_1^*, \ldots, \mathbf{v}_n^* \in \mathsf{L}^*$ mit $\lambda_n(\mathsf{L}^*) \leq \tilde{\lambda}_n(\mathsf{L}^*) \leq n^{c_1}\lambda_n(\mathsf{L}^*)$, wobei $\tilde{\lambda}_n(\mathsf{L}^*) = \max_i \|\mathbf{v}_i^*\|$ gilt. Definieren wir jetzt $\tilde{\lambda}_1 := 1/\tilde{\lambda}_n(\mathsf{L}^*)$, so folgt mit dem Transfer-Theorem 1.10

$$\lambda_1(\mathsf{L}) \geq \frac{1}{\lambda_n(\mathsf{L}^*)} \geq \frac{1}{\tilde{\lambda}_n(\mathsf{L}^*)} = \tilde{\lambda}_1 \geq \frac{1}{n^{c_1}\lambda_n(\mathsf{L}^*)} \geq \frac{\lambda_1(\mathsf{L})}{n^{c_1+1}},$$

was den Beweis von (iii) beendet. □

4.2. Die Reduktion des Worst-Case auf den Average-Case

Wir kommen nun zum schwierigen Teil (i) des Beweises von Ajtai's Theorem. Es bezeichnet im folgenden $P(\mathbf{v}_1, \ldots, \mathbf{v}_n) := \{\sum_{i=1}^n x_i \mathbf{v}_i \mid 0 \leq x_i < 1\}$ das von den Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ aufgespannte Parallelepiped.

Beweis. Zunächst beschreiben wir die Idee des Beweises für (i). Der Kern der Reduktion ist eine iterative Prozedur auf einer Menge $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, o.B.d.A. sei $\|\mathbf{v}_1\| \leq \ldots \leq \|\mathbf{v}_n\|$, von linear unabhängige Vektoren des Gitters L, die folgendes leistet:

Solange $\|\mathbf{v}_n\| > n^{3+\varepsilon}\lambda_n(\mathsf{L})$ erfüllt ist, konstruiert die Prozedur mit großer Wahrscheinlichkeit einen Gittervektor $\mathbf{w}$, so daß $\|\mathbf{w}\| \leq \|\mathbf{v}_n\|/2$ und $\mathbf{w}$ linear unabhängig von $\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}$ ist. Man wiederholt diese Prozedur solange, bis diese keinen Erfolg mehr hat, und schließt dann, daß die so konstruierte Menge S mit großer Wahrscheinlichkeit eine Menge von linear unabhängigen Vektoren mit $\max_i \|\mathbf{v}_i\| \leq n^{3+\varepsilon}\lambda_n(\mathsf{L})$ ist.

Die Prozedur besteht aus fünf Schritten: Zunächst wird ein würfelähnliches Parallelepiped aus Gittervektoren konstruiert; dies nennen wir *Pseudo-Würfel*. Dieser Pseudo-Würfel wird in viele kleine Parallelepipede zerlegt, die wir als *Unter-Pseudo-Würfel* bezeichnen. Nun wählen wir in dem Pseudo-Würfel zufällige Gitterpunkte, und ordnen diesen ihren entsprechenden Unter-Pseudo-Würfel zu, d.h. den Unter-Pseudo-Würfel, in dem sie sich befinden. Jeder solcher Unter-Pseudo-Würfel wird durch einen Vektor im $\mathbb{Z}_q^n$ repräsentiert. Wählt man m zufällige Gitterpunkte, so erhält man ein uniform gezogenes Gitter $\Lambda \in_{\mathrm{u}} \Lambda_{n,m,q}$, und kann auf dieses Gitter den Algorithmus $\mathcal{A}$ anwenden. Der von $\mathcal{A}$ berechnete Vektor $\mathbf{x} \in \Lambda$ der Länge höchstens n liefert einen kurzen Vektor, der als Differenz zweier Vektoren aus L darstellbar ist. Damit erhält man einen kurzen Vektor $\mathbf{w} \in \mathsf{L}$, der mit grosser Wahrscheinlichkeit den längsten Vektor in der Menge S ersetzen kann.

Der oben beschriebene iterative Prozeß wird auf der Menge $S = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ der Basisvektoren des gegebenen Gitters L gestartet und liefert nach polynomiell vielen Wiederholungen eine Menge $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ von linear unabhängigen Vektoren mit $\max_i \|\mathbf{v}_i\| \leq n^{3+\varepsilon}\lambda_n(\mathsf{L})$.

Wir beschreiben nun die einzelnen Konstruktionsschritte genauer und nehmen im folgenden zur Vereinfachung stets an, daß der Modul q ungerade ist.

1. Konstruktion des Pseudo-Würfels. Bezeichnen $\mathbf{e}_i$, $i = 1, \ldots, n$, die Einheitsvektoren, so definieren die Vektoren $\mathbf{p}_i := n^{1.5} M \mathbf{e}_i$ einen Würfel mit der Seitenlänge $n^{1.5}M$.

Um nun Gittervektoren $\mathbf{v}_i$ zu erhalten, die nah zu den $\mathbf{p}_i$'s sind, verwenden wir die folgende Proposition aus Cai und Nerurkar [**CN**].

Proposition 5. *Seien $\mathbf{v}_1, \ldots, \mathbf{v}_n$ linear unabhängige Vektoren eines Gitters L vom Rang n, so daß $\max_i \|\mathbf{v}_i\| \leq M$ gilt. Dann gibt es für jeden Punkt $\mathbf{p} \in \mathbb{R}^n$ einen Vektor $\mathbf{v} \in \mathsf{L}$ und einen Vektor $\boldsymbol{\delta}$ mit $\|\boldsymbol{\delta}\| \leq \sqrt{n}/2M$, so daß $\mathbf{p} = \mathbf{v} + \boldsymbol{\delta}$ gilt. Für ganzzahlige Vektoren $\mathbf{v}_i$ können $\mathbf{v}$ und $\boldsymbol{\delta}$ in Polynomial-Zeit berechnet werden.*

Damit erhalten wir entsprechende Vektoren $\mathbf{v}_i \in \mathsf{L}$ mit $\|\mathbf{p}_i - \mathbf{v}_i\| \leq \sqrt{n}/2M$, d.h. das von den Gittervektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ aufgespannte Parallelepiped $P(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ ist noch würfelähnlich. Aus diesem Grund bezeichnen wir das Parallelepiped $P(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ auch als Pseudo-Würfel.

2. Teilung des Pseudo-Würfels in Unter-Pseudo-Würfel. Wir verwenden den vergrößerten und geshifteten Pseudo-Würfel

$$\begin{aligned} C &= P(2\mathbf{v}_1, \ldots, 2\mathbf{v}_n) - \sum_{i=1}^{n} \mathbf{v}_i \\ &= \left\{ \sum_{i=1}^{n} z_i \mathbf{v}_i \mid -1 \leq z_i < 1 \right\}. \end{aligned}$$

Diesen Pseudo-Würfel C unterteilen wir in q^n Unter-Pseudo-Würfel

$$\begin{aligned} Q &= P(\tfrac{2\mathbf{v}_1}{q}, \ldots, \tfrac{2\mathbf{v}_n}{q}) - \sum_{i=1}^{n} \tfrac{\mathbf{v}_i}{q} \\ &= \left\{ \sum_{i=1}^{n} z_i \mathbf{v}_i \mid -\tfrac{1}{q} \leq z_i < \tfrac{1}{q} \right\}, \end{aligned}$$

so daß wir den Pseudo-Würfel C mit Unter-Pseudo-Würfeln der Form

$$Q + \sum_{i=1}^{n} \tfrac{2t_i}{q} \mathbf{v}_i = \left\{ \sum_{i=1}^{n} \tfrac{\gamma_i}{q} \mathbf{v}_i \mid 2t_i - 1 \leq \gamma_i < 2t_i + 1 \right\}$$

überdecken können, wobei die t_i ganze Zahlen mit

$$-\frac{q-1}{2} \leq t_i \leq \frac{q-1}{2}$$

sind. Jedem Punkt aus $\mathsf{L} \cap C$ ordnen wir außerdem eine sog. Adresse zu. Diese gibt an, in welchem Unter-Pseudo-Würfel sich der entsprechende Punkt befindet. Der Adressraum ist $\mathbb{Z}_q^n$, und die Adresse des Unter-Pseudo-Würfels $Q + \sum_{i=1}^{n} \frac{2t_i}{q} \mathbf{v}_i$ ist

$$(2t_1 \bmod q, \ldots, 2t_n \bmod q).$$

Wir repräsentieren einen Vektor $\mathbf{w} \in \mathsf{L} \cap C$ durch das Tupel $(\boldsymbol{\sigma}, \boldsymbol{\delta})$, wobei $\boldsymbol{\sigma}$ die *Adresse* von $\mathbf{w}$ ist und $\boldsymbol{\delta} \in Q$ der sog. *Restvektor*. Man beachte, daß es für den

Vektor $\mathbf{w}$ eindeutige gerade Zahlen $c_1, \ldots, c_n$ mit $-(q-1) \leq c_i \leq (q-1)$ gibt, so daß

$$(c_1, \ldots, c_n) \equiv \boldsymbol{\sigma} \bmod q$$

und

$$\mathbf{w} = \sum_{i=1}^{n} \tfrac{c_i}{q} \mathbf{v}_i + \boldsymbol{\delta}$$

gilt.

3. Wahl zufälliger Gitterpunkte. Wir beschreiben nun, wie man zu linear unabhängigen Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ eines Gitters L uniform einen Vektor $\mathbf{w} \in \mathsf{L} \cap P(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ zieht. Für einen Punkt $\mathbf{w} \in \mathsf{L}$ mit $\mathbf{w} = \sum_{i=1}^{n} x_i \mathbf{v}_i$ und $0 \leq x_i < 1$ gilt nach Proposition 2 aus Kapitel 1,

$$\begin{aligned} \mathbf{w} &= \sum_{i=1}^{n} x_i \mathbf{v}_i \\ &= \sum_{j=1}^{n} \sum_{i=j}^{n} (x_i \alpha_{i,j}) \mathbf{b}_j. \end{aligned}$$

In dieser Form ist der Koeffizient von $\mathbf{b}_n$ des Vektors $\mathbf{w}$ die ganze Zahl $x_n \alpha_{n,n}$. Wir wählen daher ein zufälliges

$$x_n \in_{\mathrm{u}} \{\tfrac{0}{\alpha_{n,n}}, \ldots, \tfrac{\alpha_{n,n}-1}{\alpha_{n,n}}\}$$

uniform aus. Der Koeffizient von $\mathbf{b}_{n-1}$ des Vektors $\mathbf{w}$ ist somit die ganze Zahl $x_{n-1}\alpha_{n-1,n-1} + x_n \alpha_{n,n-1}$. Zur Lösung $\overline{x}_{n-1}$ der Gleichung $x\alpha_{n-1,n-1} + x_n \alpha_{n,n-1} = 0$ und der zufälligen uniformen Wahl

$$y \in_{\mathrm{u}} \{\tfrac{0}{\alpha_{n-1,n-1}}, \ldots, \tfrac{\alpha_{n-1,n-1}-1}{\alpha_{n-1,n-1}}\}.$$

definieren wir daher

$$x_{n-1} := \{\overline{x}_{n-1} + y\}.$$

Entsprechend dem obigen Verfahren werden jetzt die restlichen Werte $x_1, \ldots, x_{n-2}$ für den Vektor $\mathbf{w}$ gewählt. Cai und Nerurkar [**CN**] zeigen, daß diese Wahl des Vektors $\mathbf{w}$ eine zufällige uniforme Auswahl aus $\mathsf{L} \cap P(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ generiert.

4. Uniforme Auswahl einer Matrix aus $\mathbb{Z}_q^{n \times m}$. Um einen Gitterpunkt uniform aus $\mathsf{L} \cap C$ zu ziehen, gehen wir folgt vor. Wir ziehen zunächst mit der oben beschriebenen Methode einen Gittervektor $\mathbf{w}$ uniform aus $\mathsf{L} \cap P(2\mathbf{v}_1, \ldots, 2\mathbf{v}_n)$ und erhalten dann einen Gitterpunkt aus $\mathsf{L} \cap C$ durch $\mathbf{w} - \sum_{i=1}^{n} \mathbf{v}_i$.

Allerdings müssen wir m Gitterpunkte aus $\mathsf{L} \cap C$ derart ziehen, daß ihre m Adressvektoren aus $\mathbb{Z}_q^n$ eine fast-uniforme Verteilung auf $\mathbb{Z}_q^{n \times m}$ generieren.

Um dies zu gewährleisten verwenden wir eine Pseudorandom-Verstärkung der Uniformität.

Wie eben beschrieben, ziehen wir zunächst $k := \lceil \frac{2}{\varepsilon} \rceil$ Vektoren $\mathbf{w}^{(1)}, \ldots, \mathbf{w}^{(k)}$ mit $\mathbf{w}^{(j)} = (\boldsymbol{\sigma}^{(j)}, \boldsymbol{\delta}^{(j)})$ uniform aus $\mathsf{L} \cap C$. Mit diesen Vektoren konstruieren wir nun die Vektoren

$$\boldsymbol{\alpha} := \left(\sum_{j=1}^{k} \boldsymbol{\sigma}^{(j)} \right) \bmod q$$

und

$$\boldsymbol{\eta} := \sum_{j=1}^{k} \boldsymbol{\delta}^{(j)}.$$

Man bemerke nun, daß es einen eindeutig bestimmten Unter-Pseudo-Würfel gibt, dessen Ursprungskoordinaten modulo q komponentenweise kongruent zu $\boldsymbol{\alpha}$ sind; sei dieser Ursprung des entsprechenden Unter-Pseudo-Würfels

$$\mathbf{w_o} := \sum_{i=1}^{n} \tfrac{c_i}{q} \mathbf{v}_i$$

mit

$$(c_1, \ldots, c_n) \equiv \boldsymbol{\alpha} \bmod q.$$

Insofern konstruieren wir den gewünschten Gitterpunkt durch

$$\mathbf{w} := \mathbf{w_o} + \boldsymbol{\eta}.$$

Man beachte nun, daß der so konstruierte Punkt $\mathbf{w}$ auch tatsächlich ein Gitterpunkt ist. Denn für $(c_1^{(j)}, \ldots, c_n^{(j)}) \equiv \boldsymbol{\sigma}^{(j)} \bmod q$ erhalten wir

$$\mathbf{w}^{(j)} = \sum_{i=1}^{n} \tfrac{c_i^{(j)}}{q} \mathbf{v}_i + \boldsymbol{\delta}^{(j)},$$

und somit

$$\boldsymbol{\alpha} = \left(\sum_{j=1}^{k} \boldsymbol{\sigma}^{(j)} \right) \equiv \left(\sum_{j=1}^{k} c_1^{(j)}, \ldots, \sum_{j=1}^{k} c_n^{(j)} \right) \bmod q,$$

was wiederum $\sum_{j=1}^{k} c_1^{(j)} = c_i \bmod q$ impliziert. Da aber die Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ Gittervektoren sind, ergibt sich für einen Vektor $\mathbf{v} \in \mathsf{L}$

$$\begin{aligned}\sum_{j=1}^{k} \mathbf{w}^{(j)} &= \sum_{i=1}^{n}\sum_{j=1}^{k} c_i^{(j)} \tfrac{\mathbf{v}_i}{q} + \sum_{j=1}^{k} \boldsymbol{\delta}^{(j)} \\ &= \sum_{i=1}^{n} \tfrac{c_i}{q}\mathbf{v}_i + \mathbf{v} + \boldsymbol{\eta}.\end{aligned}$$

Andererseits sind aber die Vektoren $\mathbf{w}^{(1)}, \ldots, \mathbf{w}^{(k)}$ ebenfalls Gittervektoren, so daß $\mathbf{w} = \sum_{i=1}^{n} \frac{c_i}{q}\mathbf{v}_i + \boldsymbol{\eta}$ auch ein Gittervektor sein muß.

Wir konstruieren m solche zufälligen Gitterpunkte $\mathbf{w}_1, \ldots, \mathbf{w}_m$ mit den Adressen $\boldsymbol{\alpha}_i$ und den Restvektoren $\boldsymbol{\eta}_i$, $i = 1, \ldots, m$. Für die Verteilung D der durch diesen Zufallsprozeß konstruierten Matrizen

$$M := (\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_m)$$

zeigen Cai und Nerurkar [**CN**], daß sie $1/n$-nah zur uniformen Verteilung U auf $\mathbb{Z}_q^{n\times m}$ ist, d.h. $\|D - U\|_{\mathrm{SD}} \leq 1/n$.

5. Berechnung eines kurzen Vektors in L durch $\mathcal{A}$. Auf das im vorhergehenden Schritt fast-uniform gewählte Gitter $\Lambda(M)$ wenden wir nun den Algorithmus $\mathcal{A}$ an. Dieser berechnet mit großer Wahrscheinlichkeit einen nicht trivialen Vektor $\mathbf{x} \in \Lambda(M)$ mit $M \cdot \mathbf{x} \equiv \mathbf{0} \bmod q$ und $\|\mathbf{x}\| \leq n$. Damit können wir den kurzen Gittervektor

$$\mathbf{w} := \sum_{j=1}^{m} x_j \boldsymbol{\eta}_j$$

berechnen. Zunächst zeigen wir, daß $\mathbf{w}$ in der Tat ein Vektor aus L ist, und anschließend, daß mit großer Wahrscheinlichkeit $\|\mathbf{w}\| \leq M/2$ gilt.

Nach Definition von $\mathbf{x}$ gilt natürlich

$$\sum_{j=1}^{m} \boldsymbol{\alpha}_j x_j \equiv \mathbf{0} \bmod q$$

und somit für alle $i = 1, \ldots, n$ auch

$$\sum_{j=1}^{m} c_{ij} x_j \equiv 0 \bmod q,$$

wobei $(c_{1j}, \ldots, c_{nj}) \equiv \boldsymbol{\alpha}_j \bmod q$ die Adresse des j-ten Unter-Pseudo-Würfels bezeichnet. Folglich ergibt sich

$$\sum_{j=1}^{m} x_j \mathbf{w}_j = \sum_{i=1}^{n}\sum_{j=1}^{m} x_j \tfrac{c_{ij}}{q}\mathbf{v}_i + x_j\boldsymbol{\eta}_j,$$

daß $\mathbf{w}$ also die Differenz der beiden Vektoren $\sum_{j=1}^{m} x_j \mathbf{w}_j$ und $\sum_{i=1}^{n} \sum_{j=1}^{m} x_j \frac{c_{ij}}{q} \mathbf{v}_i$ aus L ist, und damit selber ein Vektor aus L ist.

Für die Länge des Vektors $\mathbf{w}$ zeigen Cai und Nerurkar [**CN**], daß mit großer Wahrscheinlichkeit $\|\mathbf{w}\| = O(n^{1.5}W)$ erfüllt ist, wobei $W = n^{1.5}M/q$ die Seitenlänge eines Unter-Pseudo-Würfels Q ist. Durch Benutzung von $\|\mathbf{x}\| \leq n$ schätzt man zunächst den Erwartungswert $\mathbb{E}_{\mathbf{w}_1,\ldots,\mathbf{w}_m}[\|\sum_{j=1}^{m} x_j \boldsymbol{\eta}_j\|^2]$ des Vektors $\mathbf{w}$ durch $O(n^6 M^2/q^2)$ ab. Hierzu benötigt man, daß die Zufallsvariablen $\boldsymbol{\eta}_j$ fast unabhängig und zentral-symmetrisch verteilt sind. Dies folgt aus der Tatsache, daß die Seitenlängen $W = n^{1.5}M/q$ der Unter-Pseudo-Würfel für $M > n^{3+\varepsilon}\lambda_n(\mathsf{L})$ wesentlich größer als $\lambda_n(\mathsf{L})$ sind. Mit Markov's Ungleichung ergibt sich dann, daß mit großer Wahrscheinlichkeit

$$\|\mathbf{w}\| = \left\| \sum_{j=1}^{m} x_j \boldsymbol{\eta}_j \right\| = O(n^3 M/q)$$

gilt. Wählt man nun noch $q = \Theta(n^3)$, so folgt, daß in der Tat $\|\mathbf{w}\| \leq M/2$ mit großer Wahrscheinlichkeit gilt.

Es ist jetzt nur noch zu zeigen, daß der so konstruierte Vektor $\mathbf{w} \in \mathsf{L}$ mit großer Wahrscheinlichkeit den längsten Vektor $\mathbf{v}_n$ in der Menge $S = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ mit $\|\mathbf{v}_1\| \leq \ldots \leq \|\mathbf{v}_n\|$ ersetzen kann. Wir müssen also zeigen, daß $\mathbf{w}$ linear unabhängig von den Vektoren $\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}$ ist. Dies sieht man wie folgt ein. Zunächst beobachte man, daß die Ausgabe $\mathbf{x} \in \Lambda(M)$ des Algorithmus $\mathcal{A}$ nur von den Adressen und nicht von den Restvektoren der zufällig gezogenen Gitterpunkte $\mathbf{w}_1, \ldots, \mathbf{w}_m$ abhängt. Eine zufällige Wahl der Gitterpunkte kann daher auch so erhalten werden, daß man zunächst die m Adressen der Unter-Pseudo-Würfel uniform zieht, danach den Vektor $\mathbf{x} \in \Lambda(M)$ berechnet, und erst danach die Restvektoren geeignet zieht, so daß man entsprechende Gitterpunkte $\mathbf{w}_1, \ldots, \mathbf{w}_m$ erhält. Auch wenn dieser Prozeß nicht effizient durchführbar ist, erzeugt er eine zu der im vierten Schritt erhaltenen äquivalente Verteilung; daher kann dieser Randomisierungsprozeß zur probabilistischen Analyse des Vektors $\mathbf{w}$ verwendet werden.

Wir dürfen annehmen, daß $x_1 \neq 0$ ist, fixieren die letzten $m-1$ Restvektoren $\boldsymbol{\eta}_2, \ldots, \boldsymbol{\eta}_m$ und ziehen nun einen zufälligen Restvektor $\boldsymbol{\eta}_1$ um einen zufälligen Gitterpunkt in einem Unter-Pseudo-Würfel Q zu erhalten. Damit ist die Wahrscheinlichkeit, daß der so erhaltene Gitterpunkt $\mathbf{w} = \sum_{j=1}^{m} x_j \boldsymbol{\eta}_j$ in dem von den Gittervektoren $\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}$ aufgespannten Raum liegt, identisch mit der Wahrscheinlichkeit, daß ein zufälliger Punkt aus dem Unter-Pseudo-Würfel Q in solch einem Unterraum liegt. Diese Wahrscheinlichkeit ist allerdings sehr klein, da die Seitenlänge $W = n^{1.5}M/q$ des Unter-Pseudo-Würfels Q für $M > n^{3+\varepsilon}\lambda_n(\mathsf{L})$ wesentlich größer als $\lambda_n(\mathsf{L})$ ist.

Dies beendet den Beweis des schwierigen Teil (i) von Ajtai's Theorem gemäß der verbesserten Analyse von Cai und Nerurkar [**CN**]. □

4.3. Konsequenzen der SIVP- und SBP-Resultate für Ajtai's Theorem

Wie wir bereits in der Einleitung erwähnten, zielt Ajtai's Theorem auf ein interessantes kryptographisches Projekt: eine Reduktion der Worst-Case Komplexität von Gitterproblemen auf die Average-Case Komplexität von Gitterproblemen. Eine solche Reduktion zeigt nämlich unter Worst-Case Annahmen untere Average-Case Komplexitätsschranken, wie sie etwa für die Kryptographie angemessen sind. Insbesondere zeigt Ajtai's Theorem unter der Voraussetzung, daß $\text{GAPSVP}_{n^{4+\varepsilon}}$, $\text{GAPSBP}_{n^{3.5+\varepsilon}}$ oder $\text{GAPSBP}_{n^{3+\varepsilon}}$ NP-hart ist, eine untere Komplexitätsschranke zum Berechnen kurzer Vektoren in zufälligen und uniform gewählten Gittern aus der Klasse $\Lambda_{n,m,q}$. Die Frage ist nun, ob eines dieser drei Promise-Probleme tatsächlich NP-hart ist.

Zum Zeitpunkt von Ajtai's Entdeckung im Jahre 1996 war von keinem der drei Probleme die NP-Vollständigkeit bewiesen. Nach Ajtai's Entdeckung intensivierten sich jedoch die komplexitätstheoretischen Untersuchungen des SVP. Dies lag an der Bedeutung des SVP für viele Gebiete der Informatik, Mathematik, sowie der Kryptographie und insbesondere an dessen langen Geschichte als „wichtigstes ungelöstes Problem der algorithmischen Geometrie der Zahlen" (vgl. Kannan [**Kan1**]). Ajtai [**Ajt2**] selbst zeigte schließlich 1997, daß das SVP unter randomisierten Reduktionen NP-hart ist. Auf Ajtai's Beweis aufbauend zeigte Micciancio [**Mic**] kurze Zeit später, daß GAPSVP_f für $f < \sqrt{2}$ unter randomisierten Reduktionen NP-hart ist.

Dieses Nicht-Approximierbarkeitsresultat für das SVP von Micciancio [**Mic**] ist allerdings weit von einer Reduktion eines beweisbar schwierigen Worst-Case Problems auf ein Average-Case Problem entfernt. Ajtai's Theorem erfordert nämlich für das SVP einen Nicht-Approximierbarkeitsfaktor nahe n^4.

Ungeachtet möglicher Verbesserungen von Ajtai's Theorem hinsichtlich des Approximationsfaktors $n^{3+\varepsilon}$ für das SIVP gibt es plausible Gründe die eine erfolgreiche Reduktion des Worst-Case auf den Average-Case für das SVP ausschliessen. Diese wollen wir nun erläutern.

Hierzu betrachten wir den Beweis des Teils (iii) von Ajtai's Theorem. Dieser reduziert $\text{GAPSVP}_{n^{4+\varepsilon}}$ auf das Lösen des SIVP bis auf einen Faktor von $n^{3+\varepsilon}$. Die Reduktion verwendet das sog. Transfer-Theorem von Banaszcyk [**Ban**] (vgl. Theorem 1.10 in Kapitel 1) und ist die einzige bekannte Methode $\text{GAPSVP}_{nf(n)}$ auf das Lösen des SIVP bis zu einem Faktor von $f(n)$ zu reduzieren. Mit Proposition 3 aus Kapitel 1 und der Annahme, daß die Produktbeziehung $1 \leq \lambda_1(\mathsf{L}^*) \cdot \lambda_n(\mathsf{L}) \leq O(n)$ aus dem Transfer-Theorem die einzige Beziehung

zwischen λ_1 und λ_n ist, beträgt der Verlust in dem Approximationsfaktor für das SVP in dieser Reduktion mindestens n. Insbesondere bedeutet dies, daß der Verlustfaktor n für GAPSVP in Ajtai's Theorem bestmöglich ist. Andererseits zeigen Goldreich und Goldwasser [**GG**], daß GAPSVP für $f(n) = O(\sqrt{n/\log(n)})$ nicht mehr NP-hart ist, es sei denn, daß die Polynomialzeit-Hierarchie auf der zweiten Stufe kollabiert. Für das SVP gibt es also zwischen seiner Grenze der Nicht-Approximierbarkeit und dem Approximationsfaktor n^{c_2} in Ajtai's Theorem eine unüberwindliche Lücke der Größe $\sqrt{n\log(n)}$. Damit scheint eine Reduktion von NP-harten Worst-Case Instanzen des SVP auf Average-Case Instanzen des SVP ausgeschlossen zu sein.

Betrachten wir dagegen den Beweis des Teils (i) von Ajtai's Theorem, so sehen wir, daß das Problem SIVP direkt auf zufällige Instanzen der Klasse $\Lambda_{n,m,q}$ reduziert wird. Insbesondere werden keine allgemeinen Sätze aus der Geometrie der Zahlen verwendet. Vielmehr basiert der Approximationsfaktor $n^{3+\varepsilon}$ für das SIVP lediglich auf der Konstruktion der zufälligen Gitter aus der Klasse $\Lambda_{n,m,q}$. Es ist daher zu erwarten, daß Verbesserungen von Ajtai's randomisierter Konstruktion den Approximationsfaktor für das SIVP reduzieren werden. Der kleinere Approximationsfaktor von $n^{3+\varepsilon}$ und die direkte Reduktion des SIVP auf zufällige Instanzen aus $\Lambda_{n,m,q}$ machen das SIVP daher für eine erfolgreiche Worst-Case auf Average-Case Reduktion attraktiver.

In der Tat ist der in dieser Arbeit gezeigte Nicht-Approximierbarkeitsfaktor von $n^{O(1/\log\log n)}$ für das SIVP gegenüber dem Nicht-Approximierbarkeitsfaktor von ungefähr $\sqrt{2}$ für das SVP ermutigend. Beispielsweise verwendet Ajtai in einer neuesten Arbeit [**Ajt4**] zu seiner Worst-Case/Average-Case-Reduktion das SIVP bzw. das SBP, da diese ihm (nun) für dieses Projekt geeigneter erscheinen als das SVP. Andererseits zeigt der von uns bewiesene Faktor von $n/O(\sqrt{\log n})$ für die Grenze der Nicht-Approximierbarkeit des SIVP folgendes:

> *Der in der jetzigen Form von Ajtai's Theorem erforderliche Faktor von $n^{3+\varepsilon}$ für das* SIVP *kann als Nicht-Approximierbarkeitsfaktor für das* SIVP *unter plausiblen Annahmen nicht mehr bewiesen werden.*

Eine erfolgreiche Reduktion von NP-harten SIVP Instanzen auf Average-Case Instanzen des SVP hängt also entscheidend davon ab, ob der Approximationsfaktor für das SIVP in Ajtai's Theorem erheblich verbessert werden kann.

Literaturverzeichnis

[Ajt1] M. Ajtai, Generating Hard Instances of Lattice Problems, *Proc. 28th Symposium on Theory of Computing* 1996, Seiten 99-108.

[Ajt2] M. Ajtai, The Shortest Vector Problem is NP-Hard for Randomized Reductions, *Proc. 30th Symposium on Theory of Computing* 1998, Seiten 10-19.

[Ajt3] M. Ajtai, Worst-Case Complexity, Average-Case Complexity and Lattice Problems, *Proc. International Congress of Mathematicians* 1998, Vol. III, Seiten 421-428.

[Ajt4] M. Ajtai, Generating Hard Instances of the Short Basis Problem, erscheint in *Proc. 14th Colloquium on Automata, Languages and Programming* 1999.

[ABSS] S. Arora, L. Babai, J. Stern, Z. Sweedyk, The Hardness of Approximate Optima in Lattices, Codes, and Systems of Linear Equations, *Journal of Computer and System Sciences* Vol. 54, Seiten 317-331, 1997.

[AD] M. Ajtai, C. Dwork, A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence, *Proc. 29th Symposium on Theory of Computing* 1997, Seiten 284-293.

[AL] S. Arora, C. Lund, Hardness of Approximations, in D. S. Hochbaum (ed.), *Approximation Algorithms for NP-Hard Problems*, PWS Publishing, Boston, 1997.

[Bab] L. Babai, Trading Group Theory for Randomness, *Proc. 17th Symposium on Theory of Computing* 1985, Seiten 421-430.

[Ban] W. Banaszcyk, New Bounds in Some Transference Theorems in the Geometry of Numbers, *Mathematische Annalen* Vol. 296, Seiten 625-635, 1993.

[BSha] E. Bach, J. Shallit, *Algorithmic Number Theory*, MIT Press, Cambridge, 1996.

[BGS] M. Bellare, O. Goldreich, M. Sudan, Free Bits, PCPs, and Nonapproximability — Towards tight results, *SIAM J. Computing* Vol. 27, Seiten 804-915, 1998.

[BSei] J. Blömer, J.-P. Seifert, On the Complexity of Computing Short Linearly Independent Vectors and Short Bases in a Lattice, *Proc. 31st Symposium on Theory of Computing* 1999, Seiten 711-720

[BHZ] R. Boppana, J. Håstad, S. Zachos, Does Co-NP Have Short Interactive Proofs, *Information Processing Letters* Vol. 25, Seiten 127-132, 1987.

[Cas1] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer, Berlin, 1971.

[Cas2] J. W. S. Cassels, *An Introduction to Diophantine Approximations*, Cambridge University Press, Cambridge, 1957.

[Cai1] J. Y. Cai, A New Transference Theorem and Applications to Ajtai's Connection Factor, *Electronic Colloquium on Computational Complexity*, TR98-05, 1998.

[Cai2] J. Y. Cai, A relation of primal–dual lattices and the complexity of shortest lattice vector problem, *Theoretical Computer Science* Vol. 207, Seiten 105-116, 1998.

[Cai3] J. Y. Cai, Some Recent Progress on the Complexity of Lattice Problems, *Electronic Colloquium on Computational Complexity*, TR99-06, 1999.

[CN] J. Y. Cai, A. P. Nerurkar, An Improved Worst-Case to Average-Case Reduction for Lattice Problems, *Proc. 38th Symposium on Foundations of Computer Science* 1997, Seiten 468-477.

[CHM$^+$] J. Y. Cai, G. Havas, B. Mans, A. P. Nerurkar, J.-P. Seifert, I. Shparlinksi, On Routing in Circulant Graphs, erscheint in *Proc. Fifth International Computing and Combinatorics Conference* 1999.

[CS] A. Yu. Chirkov, V. N. Shevchenko, Finding successive minima of an integral lattice and vector lattice, close to a given one, *Cybernetics* Vol. 23, Seiten 492-497, 1987.

[DKS] I. Dinur, G. Kindler, S. Safra, Approximating CVP to Within Almost-Polynomial Factors is NP-Hard, *Proc. 39th Symposium on Foundations of Computer Science* 1998, Seiten 99-109.

[Dir] G. L. Dirichlet, Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen, *Sitzungsberichte der Preussischen Akademie der Wissenschaften* 1842, Seiten 93-95.

[FS] R. Fischlin, J.-P. Seifert, Tensor-based Trapdoors for CVP and their Applications to Public-Key Cryptography, erscheint in *Proc. 7th IMA International Conference on Cryptography and Coding* 1999.

[Gau] C. F. Gauss, *Disquisitiones Arithmeticae*, Fleischer, Leipzig, 1801.

[Gol] O. Goldreich, *Modern Cryptography, Probabilistisc Proofs and Pseudorandomness*, Springer, Berlin, 1999.

[GG] O. Goldreich, S. Goldwasser, On the Limits of Non-Approximability of Lattice Problems, *Proc. 30th Symposium on Theory of Computing* 1998, Seiten 1-9.

[GGH] O. Goldreich, S. Goldwasser, and S. Halevi, Collision-Free Hashing from Lattice Problems, *Electronic Colloquium on Computational Complexity*, TR96-042, 1996.

[GMSS] O. Goldreich, D. Micciancio, S. Safra, J.-P. Seifert, Approximating shortest lattice vectors is not harder than approximating closest lattice vectors, erscheint in *Information Processing Letters* 1999.

[GS] S. Goldwasser, M. Sipser, Private coins versus public coins in interactive proof systems, in S. Micali (ed.), *Advances in Computing Research 5: Randomness and Computation*, JAI Press Inc., 1989.

[HJLS] J. Håstad, B. Just, J. C. Lagarias, C. P. Schnorr, Polynomial time algorithms for finding integer relations among real numbers, *SIAM J. Computation* Vol. 18, Seiten 859-881, 1989.

[HavS] G. Havas, J.-P. Seifert, The complexity of the extended GCD problem, erscheint in *Proc. 24th Symposium on Mathematical Foundations of Computer Science* 1999.

[Her] M. C. Hermite, Extraits de lettres de M. Ch. Hermite á M. Jacobi sur différents objets de la théorie des nombres, Deuxieme lettre du 6 août 1845, *Journal für die Reine und Angewandte Mathematik* Vol. 40, Seiten 279-290, 1850.

[HowS] N. Howgrave-Graham, J.-P. Seifert, Extending Wiener's attack in the presence of many decrypting exponents, erscheint in *Proc. International Forum on CQRE (Secure) Networking* 1999.

[Jus] B. Just, Generalizing the continued fraction algorithm to arbitrary dimensions, *SIAM J. Computation* Vol. 21, Seiten 909-926, 1992.

[Kan1] R. Kannan, Minkowski's Convex Body Theorem and Integer Programming, *Mathematics of Operations Research* Vol. 12, No. 3, Seiten 415-440, 1987.

[Kan2] R. Kannan, Algorithmic Geometry of Numbers, *Ann. Rev. Comput. Science* Vol. 2, Seiten 231-267, 1987.

[KZ1] A. Korkin, G. Zolotarev, Sur les formes quadratiques positives quaternaires, *Mathematische Annalen* Vol. 5, Seiten 581-583, 1872.

[KZ2] A. Korkin, G. Zolotarev, Sur les formes quadratiques, *Mathematische Annalen* Vol. 6, Seiten 366-389, 1873.

[KZ3] A. Korkin, G. Zolotarev, Sur les formes quadratiques positives, *Mathematische Annalen* Vol. 11, Seiten 242-292, 1877.

[Lag] J. C. Lagarias, The Computational Complexity of Simultaneous Diophantine Approximation Problems, in: *SIAM J. Computing* Vol. 14, Seiten 196-209, 1985.

[Lov] L. Lovasz, *An Algorithmic Theory of Graphs, Numbers and Convexity*, SIAM Publications, Philadelphia, 1986.

[LLL] A. K. Lenstra, H. W. Lenstra, L. Lovasz, Factoring polynomials with integer coefficients, *Mathematische Annalen* Vol. 261, Seiten 513-534, 1982.

[LLS] J. Lagarias, H. W. Lenstra, C. P. Schnorr, Korkin-Zolotarev Bases and Successive Minima of a Lattice and its Reciprocal Lattice, *Combinatorica* Vol. 10, No. 4, Seiten 333-348, 1990.

[Mar] J. Martinet, Les Réseaux Parfaits des Espaces Euclidiens, Masson, Paris, 1996.

[Mic] D. Micciancio, The Shortest Vector in a Lattice is Hard to Approximate to within Some Constant, *Proc. 39th Symposium on Foundations of Computer Science* 1998, Seiten 92-98.

[MH] J. Milnor, D. Husemoller, *Symmetric Bilinear Forms*, Springer, Berlin, 1973.

[Min1] H. Minkowski, Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen, *Journal für die Reine und Angewandte Mathematik* Vol. 107, Seiten 278-297, 1891.

[Min2] H. Minkowski, *Geometrie der Zahlen*, Teubner, Leipzig, 1910.

[MR] R. Motwani, P. Raghavan, *Randomized Algorithms*, Cambridge University Press, New York, 1995.

[Pap] C. H. Papadimitriou, *Computational Complexity*, Addison Wesley, Reading, 1994.

[PS] A. Paz, C. P. Schnorr, Approximating integer lattices by lattices with cyclic factor group, *Proc. 14th Colloquium on Automata, Languages and Programming* 1987, Seiten 386-393.

[Poh] M. Pohst, On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications, *SIGSAM Bulletin* Vol. 15, Seiten 37-44, 1981.

[RSch] C. Rössner, C. P. Schnorr, An Optimal, Stable Continued Fraction Algorithm for Arbitrary Dimension, *Proc. 5th Conference on Integer Programming and Combinatorial Optimization* 1997, Seiten ?-?.

[RSei1] C. Rössner, J.-P. Seifert, Approximating good simultaneous diophantine approximations is almost NP-hard, *Proc. 21st Symposium on Mathematical Foundations of Computer Science* 1996, Seiten 494-504.

[RSei2] C. Rössner, J.-P. Seifert, The Complexity of Approximate Optima for Greatest Common Divisor Computations, *Proc. 2nd International Algorithmic Number Theory Symposium* 1996, Seiten 307-322.

[RSei3] C. Rössner, J.-P. Seifert, On the hardness of approximating shortest integer relations among rational numbers, *Theoretical Computer Science* Vol. 209, Seiten 287-297, 1998.

[Sei] J.-P. Seifert, Arthur, Merlin and Dirichlet debate diophantine approximations, Manuscript, 1998.

[Val] B. Vallée, Un problème central en géometrie algorithmique des nombres: La réduction des réseaux. Autour de l'algorithme de Lenstra-Lenstra-Lovasz, *RAIRO Inf. Theor. Appl.* Vol. 23, Seiten 345-376, 1989.

[Wie] M. Wiener, Cryptanalysis of short RSA secret exponents, *IEEE Trans. on Inform. Theory* Vol. 36, Seiten 553-558, 1990.

Symbolverzeichnis

$\mathsf{L}(\cdot,\ldots,\cdot)$	aufgespanntes Gitter, 14
$\mathrm{span}(\cdot,\ldots,\cdot)$	aufgespannter $\mathbb{R}$-Untervektorraum, 13
$\nu(\cdot)$	Basislänge, 15
BSDA	Best Simultaneous Diophantine Approximation, 40
CVP	Closest Vector Problem, 21
$\det(\cdot)$	Determinante, 14
$\dim(\cdot)$	Dimension, 13
$\|\cdot \bmod \mathbb{Z}\|_\infty$	Diophantische Approximation, 18
$\mu(\cdot,\cdot)$	Distanz zum nächsten Gittervektor, 16
$\langle\cdot,\cdot\rangle$	Euklidisches inneres Produkt, 13
$\|\cdot\|$	Euklidische Norm, 13
$[\cdot]$	ganzzahliger Anteil, 18
$[\cdot,\ldots,\cdot]$	geordnete Menge, 13
$\mathrm{ggT}(\cdot,\cdot)$	größter gemeinsame Teiler 42
μ_{ij}	Gram-Schmidt-Koeffizient, 17
γ_n	Hermite-Konstante, 15
$\|\cdot - \cdot \bmod \mathbb{Z}\|_\infty$	Inhomogene Diophantische Approximation, 19
$\cdot \leq_{\mathrm{K}} \cdot$	Karp-Reduktion, 20
$\mathsf{\Sigma}_i^{\mathrm{P}}$	Klasse der Polynomialzeit-Hierarchie auf Stufe i, 19
$\mathsf{\Pi}_i^{\mathrm{P}}$	Klasse der Polynomialzeit-Hierarchie auf Stufe i, 19
$\mathsf{IP}(r(\cdot))$	Klasse der Sprachen mit interaktivem r-Runden Protokoll, 25
$\Lambda_{n,m,q}$	Klasse von Gittern, 51
co-NP	Komplement der Klasse NP, 20
$B_r(\cdot)$	Kugel vom Radius r, 14
$\mathsf{L}_{\cdot,\cdot}$	modulares Relationengitter, 18
$\|\cdot\|_\infty$	Maximimum-Norm, 13
$\mathbb{Z}_q^{n\times m}$	Menge der $n \times m$ Matrizen über $\mathbb{Z}_q$, 51
NP	nichtdeterministisch Polynomial-Zeit entscheidbaren Sprachen, 19
$\cdot^\perp$	orthogonales Komplement, 13
$\pi_i(\cdot)$	orthogonale Projektion, 17
$\hat{\mathbf{b}}_i$	orthogonale Projektion von $\mathbf{b}_i$, 17
$P(\cdot,\ldots,\cdot)$	Parallelepiped, 53
P	Polynomial-Zeit entscheidbaren Sprachen, 19

$\mathsf{L}^{(\cdot)}$	Projektionsgitter, 17
$\textsc{gapSvp}_g$	Promise-Problem, 23
$\textsc{gapCvp}_g$	Promise-Problem, 23
$\textsc{gapSir}_g^\infty$	Promise-Problem, 23
$\textsc{gapSivp}_g$	Promise-Problem, 28
$\textsc{gapBsda}_g$	Promise-Problem, 41
$\textsc{gapSbp}_g$	Promise-Problem, 29
QP	Quasi-Polynomial-Zeit entscheidbaren Sprachen, 20
$\mathbb{Q}^m$	rationale m-dimensionale Euklidische Vektorraum, 13
$\mathbb{R}^m$	reelle m-dimensionale Euklidische Vektorraum, 13
$\{\cdot\}$	reellwertige Anteil, 18
$\mathrm{rg}(\cdot)$	Rang, 13
$\mathsf{L}.$	Relationengitter, 18
$\|\cdot - \cdot\|_{\mathrm{SD}}$	statistische Distanz, 47
$g_i(\cdot)$	sukzessiver i-ter Erzeugendenradius, 15
$\lambda_i(\cdot)$	sukzessives i-tes Minimum, 14
$\lambda_{i,\|\cdot\|_\infty}(\cdot)$	sukzessives i-tes Minimum bzgl. $\|\cdot\|_\infty$, 14
Sbp	Shortest Basis Problem, 28
$\textsc{Sir}^\infty$	Shortest Integer Relation bzgl. $\|\cdot\|_\infty$, 21
Sivp	Shortest Independent Vectors Problem, 27
Svp	Shortest Vector Problem, 21
$C_r(\cdot)$	Würfel mit Seitenlänge $2r$, 14

Index