On the Hardness of the Shortest Vector Problem

by

Daniele Micciancio

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 1998

Author .....
Department of Electrical Engineering and Computer Science
September 11, 1998

Certified by 11/98
Shafi Goldwasser
RSA Professor of Computer Science
Thesis Supervisor

Accepted by .....
Arthur C. Smith
Chairman, Departmental Committee on Graduate Students

On the Hardness of the Shortest Vector Problem

by

Daniele Micciancio

Submitted to the Department of Electrical Engineering and Computer Science
on September 11, 1998, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Abstract

An n-dimensional lattice is the set of all integral linear combinations of n linearly independent vectors in $\mathcal{R}^m$. One of the most studied algorithmic problems on lattices is the shortest vector problem (SVP): given a lattice, find the shortest non-zero vector in it. We prove that the shortest vector problem is NP-hard (for randomized reductions) to approximate within some constant factor greater than 1 in any l_p norm ($p \geq 1$). In particular, we prove the NP-hardness of approximating SVP in the Euclidean norm l_2 within any factor less than $\sqrt{2}$. The same NP-hardness results hold for deterministic non-uniform reductions. A deterministic uniform reduction is also given under a reasonable number theoretic conjecture concerning the distribution of smooth numbers.

In proving the NP-hardness of SVP we develop a number of technical tools that might be of independent interest. In particular, a lattice packing is constructed with the property that the number of unit spheres contained in an n-dimensional ball of radius greater than $1 + \sqrt{2}$ grows exponentially in n, and a new constructive version of Sauer's lemma (a combinatorial result somehow related to the notion of VC-dimension) is presented, considerably simplifying all previously known constructions.

Thesis Supervisor: Shafi Goldwasser
Title: RSA Professor of Computer Science

Contents

Chapter 1

Introduction

An n-dimensional lattice in $\mathcal{R}^m$ is the set $\Lambda = \{\sum x_i \mathbf{b}_i : x_i \in \mathcal{Z}\}$ of all integral linear combinations of n linearly independent vectors in $\mathcal{R}^m$. There are many interesting algorithmic questions concerning lattices. One of the most studied of these problems is the shortest vector problem (SVP): given a lattice Λ, find the shortest non-zero vector in Λ. I study the computational complexity of this problem.

1.1 Motivation

Lattices, and the shortest vector problem in particular, have attracted the attention of mathematicians in the last two centuries for their connections with number theory and Diophantine approximation problems. Among others, lattices have been studied (in the language of quadratic forms) by Gauss, Dirichlet and Hermite. Proving the existence of short vectors in lattices was a central problem in *Geometry of Numbers*, a field founded by Minkowski as a bridge between the study of quadratic forms and the theory of Diophantine approximation. The connections between lattice theory and other branches of mathematics is well illustrated by the use of lattices to give elegant geometric proofs of classic results is number theory like showing every number is the sum of four squares. The relation between lattices and other important mathematical problems, such as Diophantine approximation, has also motivated the study of lattices from a more algorithmic point of view. The first algorithm to solve the shortest vector

problem (in dimension 2) dates back to Gauss [27], and efforts to algorithmically solve this problem continued till now [67, 21, 47, 22, 72, 81, 45]. At the beginning of the 80's, a major breakthrough in algorithmic geometry of numbers, the development of the LLL lattice reduction algorithm [58], had a deep impact in many areas of computer science, ranging from integer programming, to cryptography. Using the LLL reduction algorithm it was possible to solve integer programming in a fixed number of variables [59, 58, 43], factor polynomials over the rationals [58, 56, 71], finite fields [55] and algebraic number fields [57], disprove century old conjectures in mathematics [64], break the Merkle-Hellman crypto-system [74, 2, 11, 49, 50, 62], check the solvability by radicals [54], solve low density subset-sum problems [53, 24, 20], heuristically factor integers [69, 18] and solve many other Diophantine and cryptanalysis problems (e.g., [51, 19, 34, 25, 10]).

The first and preeminent reason to study the computational complexity of lattice problems is therefore the wide applicability of lattice based techniques to solve a variety of combinatorial and optimization problems. In the last few years one more reason emerged to study lattices specifically from the computational complexity point of view: the design of provably secure crypto-systems (see [4, 6, 31, 63, 32]). The security of cryptographic protocols depends on the intractability of certain computational problems. The theory of NP-completeness offers a framework to give evidence that a problem is hard. Notice however that while NP-hardness results refer to the worst case complexity of a problem, what is needed for security in cryptographic applications is a problem hard to solve on the average.

In [4] Ajtai established a connection between the worst case and average case complexity of certain lattice problems, and in [6] is presented a crypto-system with worst-case/average-case equivalence.

What Ajtai showed is that if there is a probabilistic polynomial-time algorithm to find the shortest vector in a lattice uniformly chosen in a certain class of lattices, then there is a probabilistic polynomial-time algorithm to find a "good basis" and in particular a vector of length within a fixed polynomial factor n^c from the shortest (the exponent c equals 8 in [4] and was improved to 3.5 in [14]).

The importance of studying the hardness of approximating SVP is now clear: if approximating the shortest vector in a lattice within a factor n^c were NP-hard, then we could base cryptography on the P versus NP question [30]. The results in [52] and [29] point out some difficulties in bridging the gap between the approximation factors for which we can hope to prove the NP-hardness of SVP, and those required by current lattice based crypto-systems. Still, the possibility that progress in both the study of the complexity of lattice problems and the design of lattice based crypto-systems might lead to the ultimate goal of a crypto-system based on the assumption $P \neq NP$, is an extremely attractive perspective.

1.2 Historical Background

The shortest vector problem (or the equivalent problem of minimization of quadratic forms) has a long history. An algorithm to solve the shortest vector problem in 2-dimensional lattices was already given by Gauss ([27], 1801). The general problem in arbitrary dimension was formulated by Dirichlet in 1842, and studied by Hermite ([36], 1845), and Korkine and Zolotareff ([48], 1873). The subject of Geometry of Numbers, founded by Minkowski ([61], 1910), was mainly concerned with the study of the existence of short non-zero vectors in lattices. Minkowski's "Convex Body Theorem" directly implies the existence of short vectors in any lattice. Algorithms to find short vectors in lattices were given by Rosser [67], Coveyou and MacPherson [21], Knuth [47], and Dieter [22]. Unfortunately none of these algorithms run in polynomial time, even if the dimension is fixed to 2. The development of the LLL basis reduction algorithm [58] was a major breakthrough in the field. Using this algorithm it was possible to solve (in polynomial-time) the shortest vector problem in any fixed dimension and many other algorithmic problems (see section 1.1).

Despite all these successful results, SVP resisted any attempt to devise polynomial-time algorithms for arbitrary dimension. In 1981 van Emde Boas proved that SVP is NP-hard in the l_∞ norm, giving evidence that the problem is inherently intractable, and conjectured that the same problem is NP-hard in any to other l_p norm ($p \geq 1$).

The NP-hardness of SVP in the l_p ($p < \infty$) norm (most notably the Euclidean norm l_2), was a long standing open question, finally settled in [5] where Ajtai proved that the shortest vector problem (in l_2) is NP-hard for randomized reductions. The result in [5] also shows that SVP is hard to approximate within some factor rapidly approaching 1 as the dimension of the lattice grows. However, cryptographic applications requires the hardness of approximating SVP within some large polynomial factor. The main goal of this thesis is to make a first step in this direction, proving the non-approximability of SVP within some factor bounded away from 1.

1.3 Results

I prove that the shortest vector problem is NP-hard to approximate within some constant factor greater than one. The result holds for all Euclidean norms l_p ($p \geq 1$). More precisely I prove that for any l_p norm and any constant $c < 2^{1/l}$, finding the approximate length of the shortest non-zero vector in a lattice within a factor c, is NP-hard for randomized reductions[1]. In particular the shortest vector problem in the Euclidean norm l_2 is NP-hard to approximate within any factor less than $\sqrt{2}$.

The proof, by reduction from a variant of the approximate closest vector problem (CVP), is surprisingly simple, given a technical lemma regarding the existence of certain combinatorial objects. The closest vector problem is the inhomogeneous version of the shortest vector problem: given a lattice and a target vector (usually not in the lattice), find the lattice point closest to the target vector. The reduction from CVP to SVP can be regarded as a homogenization technique: given a inhomogeneous problem transform it into an equivalent homogeneous one. The reduction actually uses very little specific to lattices and can potentially be used to prove the hardness (resp. easiness) of any other inhomogeneous (resp. homogeneous) problem for which an equivalent technical lemma holds true.

The technical lemma essentially asserts the existence of an instance of the inho-

[1]Randomness can be eliminated using either non-uniformity or a reasonable number theoretic conjecture.

mogeneous problem with some special properties. The proof of the technical lemma involves the solution of problems in two related areas of computer science.

The first is a sphere packing problem: I want to pack as many unit sphere as possible in a ball of radius slightly bigger than $1+\sqrt{2}$. Connections between lattices and sphere packing problems have long been known (see [17] for an excellent exposition of the subject) and lattices have been used to efficiently pack spheres for centuries. Here I look at sphere packing problems and lattices from a new and interesting perspective: I use sphere packings to prove that lattice problems are computationally hard. In proving an NP-hardness result for approximate SVP, I give an explicit construction to pack exponentially many unit spheres is a ball of radius roughly $1+\sqrt{2}$. The construction is based on a generalization of a lattice originally used by Schnorr [69] and Adleman [3] to establish a connection between SVP and factoring (a problem apparently unrelated to sphere packing). The connection I make between this lattice and sphere packing problems is an interesting result in its own.

The second problem I address is the proof of a combinatorial result on hyper-graphs somehow related to the concept of VC-dimension. The problem is to algorithmically find an integer linear transformation that (with very high probability) surjectively maps every sufficiently large bounded degree hyper-graph onto the set of all 0-1 sequences of some shorter length. A first solution to this problem was first given by Ajtai. I present an alternative and simpler construction achieving a similar (possibly stronger) result with a considerably simpler analysis. I believe that the simplicity of my construction and analysis improves the understanding of the above combinatorial problem, and might be useful for subsequent generalizations or new applications of it.

1.4 Outline

The rest of this thesis is organized as follows. In Chapter 2, I present some basic material about lattices and review what is known about the computational complexity of the shortest vector problem and other related computational problems on lattices.

In Chapter 3, I present the main result of this thesis: I prove that the shortest vector problem is NP-hard to approximate (for randomized reductions) within some constant factor. The proof uses a technical lemma which will be proved in Chapter 6, after I develop the necessary combinatorial tools in Chapters 4 and 5. In particular, in Chapter 4, I study the sphere packing problem and in Chapter 5 the hyper-graph construction mentioned in the previous section. Both results are instrumental to the proof of the technical lemma, but also interesting in their own and are presented in a self contained manner largely independent from the rest of this thesis to allow separate reading.

Chapter 2

Preliminaries

Let $\mathcal{R}, \mathcal{Q}$ and $\mathcal{Z}$ be the sets of the reals, rationals and integers respectively. The n-dimensional Euclidean space is denoted $\mathcal{R}^n$. Unless otherwise specified, I'll use boldface lowercase letters (e.g., $\mathbf{x}, \mathbf{y}, \mathbf{b}, \ldots$) for vectors, uppercase Roman letters (e.g., $A, B, C, \ldots$) for matrices, lowercase Greek or Roman letters (e.g. $\alpha, \beta, \ldots, a, b, \ldots$) for numbers and uppercase Greek letters (e.g., $\Lambda, \Gamma, \ldots$) for lattices. A lattice in $\mathcal{R}^m$ is the set of all integral combinations $\Lambda = \{\sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathcal{Z}\}$ of n linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ in $\mathcal{R}^m$ $(m \geq n)$. The set of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is said to form a basis of the lattice. The dimension of the lattice is the number n of basis vectors, and when $n = m$ the lattice is said full dimensional. A basis can be compactly represented by the matrix $B = [\mathbf{b}_1 | \ldots | \mathbf{b}_n] \in \mathcal{R}^{m \times n}$ having the basis vectors as columns. The lattice generated by B is denoted $\mathcal{L}(B)$. Notice that $\mathcal{L}(B) = \{B\mathbf{x} : \mathbf{x} \in \mathcal{Z}^n\}$, where $B\mathbf{x}$ is the usual matrix-vector multiplication. Observe that the unit vectors $\mathbf{e}_i = (\overbrace{0, \ldots, 0}^{i-1}, 1, \overbrace{0, \ldots, 0}^{n-i})$ are a basis of the integer lattice $\mathcal{Z}^n = \mathcal{L}(\mathbf{e}_1, \ldots, \mathbf{e}_n) = \mathcal{L}(I)$, where I is the identity matrix. When discussing computational issues related to lattices, we always assume that lattices are represented by a basis matrix B and that B has integral or rational entries.

Graphically, a lattice is the set of vertices of an n-dimensional grid. For example, the lattice generated by the basis $\mathbf{b}_1 = (1, 2), \mathbf{b}_2 = (1, -1)$ is shown in figure 2-1. A lattice may have different basis. For example the lattice shown in figure 2-1 is also

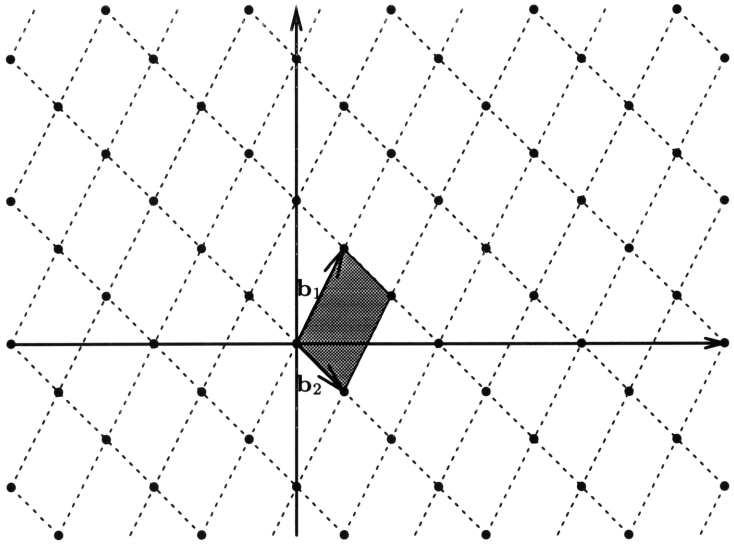

Figure 2-1: A lattice in $\mathcal{R}^2$

generated by the vectors $\mathbf{b}_1 + \mathbf{b}_2 = (2, 1)$ and $2\mathbf{b}_1 + \mathbf{b}_2 = (3, 3)$ (see figure 2-2).

Notice that any set of n linearly independent lattice vectors in a full dimensional lattice $\Lambda \subset \mathcal{R}^n$ (in particular, any basis for Λ) is a basis for $\mathcal{R}^n$ as a vector space, but it is not necessarily a lattice basis. For example, the lattice vectors $\mathbf{b}_1+\mathbf{b}_2$ and $\mathbf{b}_1-\mathbf{b}_2$, are not a basis of $\mathcal{L}(\mathbf{b}_1, \mathbf{b}_2)$ because they don't generate the whole lattice over the integers (see figure 2-3). In general, n linear independent lattice vector $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \Lambda \subset \mathcal{R}^m$ are a basis iff the fundamental parallelepiped $\{\sum_i x_i \mathbf{b}_i : 0 \leq x_i < 1\}$ they span does not contain any lattice vector other than the origin (see figures 2-1,2-2 for lattice basis and 2-3 for a non basis).

In matrix notation, two basis $B \in \mathcal{R}^{m \times n}$ and $B' \in \mathcal{R}^{m \times n'}$ generate the same lattice $\mathcal{L}(B) = \mathcal{L}(B')$ if and only if $n = n'$ and there exists a unimodular matrix $U \in \mathcal{Z}^{n \times n}$ (i.e., an integral matrix with determinant ± 1) such that $B' = BU$. Therefore the dimension of a lattice does not depend on the choice of the basis.

The determinant of a lattice, denoted $\det(\Lambda)$ is the n-dimensional volume of the fundamental parallelepiped $\{\sum_i x_i \mathbf{b}_i : 0 \leq x_i < 1\}$ spanned by the basis vectors and equals the product of the length of the vectors $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ obtained by the Gram-

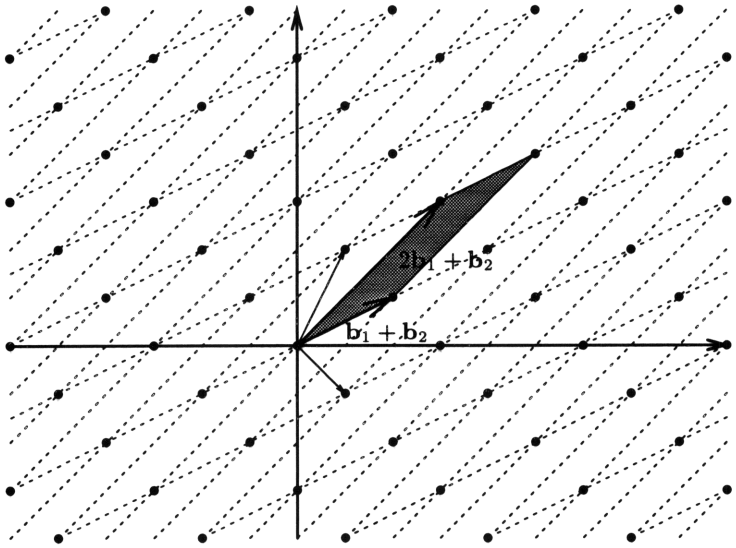

Figure 2-2: A different basis

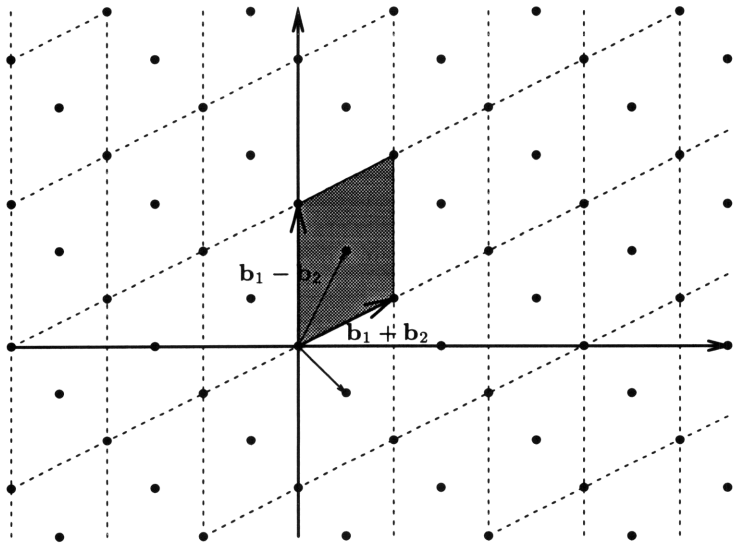

Figure 2-3: The sub-lattice generated by $\mathbf{b}_1 + \mathbf{b}_2$ and $\mathbf{b}_1 - \mathbf{b}_2$

Schmidt orthogonalization process

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j<i} \mu_{i,j} \mathbf{b}_j^*$$

$$\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle}$$

where $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{m} x_i y_i$ is the inner product in $\mathcal{R}^m$. Notice that if the $\mathbf{b}_i$ are rational vectors, then also the $\mathbf{b}_i^*$ are rationals. If lattice $\Lambda = \mathcal{L}(B)$ is full dimensional (i.e. $m = n$), than B is a non-singular square matrix and $\det(\Lambda)$ equals the absolute value of the determinant of the matrix B. In general $\det(\Lambda)$ equals the square root of the absolute value of the determinant of the Gram matrix $B^T B$, i.e., the $n \times n$ matrix whose (i, j)th entry is the inner product $\langle \mathbf{b}_i, \mathbf{b}_j \rangle$.

The determinant is also a lattice invariant (i.e., does not depend on the particular basis used to compute it) and equals the inverse of the density of lattice points in the n-dimensional vector space spanned by the basis vectors.

Lattices can also be characterized without reference to any basis. A lattice can be defined as a non-empty subset Λ of $\mathcal{R}^m$ which is closed under subtraction (if $\mathbf{x} \in \Lambda$ and $\mathbf{y} \in \Lambda$, then also $\mathbf{x} - \mathbf{y} \in \Lambda$) and discrete (there exists a positive real $\lambda > 0$ such that the distance between any two lattice vectors is at least λ). Notice that Λ always contains $\mathbf{0} = \mathbf{x} - \mathbf{x}$, and is closed under complement (if $\mathbf{x} \in \Lambda$ then $-\mathbf{x} = \mathbf{0} - \mathbf{x} \in \Lambda$), and addition (if $\mathbf{x}, \mathbf{y} \in \Lambda$ then $\mathbf{x} + \mathbf{y} \in \Lambda$). Therefore, Λ is an additive subgroup of $\mathcal{R}^m$. In fact, an alternative formulation of the definition of lattice is a discrete additive subgroup of $\mathcal{R}^m$.

Fundamental constants associated to an n-dimensional lattice Λ are its successive minima $\lambda_1, \ldots, \lambda_n$. The ith minimum $\lambda_i(\Lambda)$ is the radius of the smallest sphere centered in the origin containing i linearly independent lattice vectors. In particular, $\lambda_1(\Lambda)$ is the length of the shortest non-zero lattice vector and equals the minimum distance between lattice points:

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

The following computational problems on lattices are solvable in polynomial time:

1. *Membership:* Given a basis B and a vector $\mathbf{x}$, decide whether $\mathbf{x}$ belongs to the lattice $\mathcal{L}(B)$.

2. *Kernel:* Given an integral matrix $A \in \mathcal{Z}^{n \times m}$, find a basis of the lattice $\{\mathbf{x} \in \mathcal{Z}^m : A\mathbf{x} = \mathbf{0}\}$.

3. *Basis:* Given a set of possibly dependent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$, find a basis of the lattice they generate.

Problem 1 is clearly equivalent to deciding the feasibility of a system of linear Diophantine equations and is easily solved performing a polynomial number of arithmetic operations. The difficulty in devising a polynomial time algorithm is to prove that the size of the number involved also stays polynomially bounded. This was first accomplished in [79].

Problem 2 is the same as finding the general solution to a system of homogeneous linear Diophantine equations. Notice that this set of solutions is a lattice because is closed under subtraction and discrete. For polynomial time algorithms to solve this problem see [26, 46, 37, 38].

Problem 3 can be easily solved using techniques from any of the other problems mentioned here. For algorithms to solve these and related problems see [46, 16, 39].

2.1 Two Computational Problems on Lattices

Two problems on lattices for which no polynomial time algorithm is known are the following:

- Shortest Vector Problem (SVP): Given a lattice Λ, find the shortest non-zero vector in Λ

- Closest Vector Problem (CVP): Given a lattice Λ and a point $\mathbf{y}$, find the lattice vector closest to $\mathbf{y}$.

These problems can be defined with respect to any norm. For any $p \geq 1$, the l_p norm of a vector $\mathbf{x} \in \mathcal{R}^n$ is $\|\mathbf{x}\|_p = (\sum_{i=1}^n x_i^p)^{1/p}$. Special cases are the l_1-norm $\|\mathbf{x}\|_1 = \sum_{i=1}^n |x_i|$, the Euclidean norm $\|\mathbf{x}\|_2 = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle} = \sqrt{\sum_{i=1}^n x_i^2}$ and the max-norm $\|\mathbf{x}\|_\infty = \lim_{p \to \infty} \|\mathbf{x}\|_p = \max_{i=1}^n |x_i|$. All norms satisfy the following properties: $\|\mathbf{x}\| \geq 0$ and $\|\mathbf{x}\| = 0$ iff $\mathbf{x} = \mathbf{0}$ (definiteness), $\|\alpha \mathbf{x}\| = |\alpha| \cdot \|\mathbf{x}\|$ (homogeneity) and $\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$ (triangular inequality). From the triangular inequality it easily follows that $\|\mathbf{x} - \mathbf{y}\| \geq \|\mathbf{x}\| - \|\mathbf{y}\|$. Notice that when $p < 1$, the application $\|x\|_p$ is not a norm because it does not satisfy the triangular inequality. Of special interest is the Euclidean norm l_2, and it is assumed this is the norm being used unless otherwise specified.

The lack of polynomial time algorithms to solve the above problems has led researchers to look for approximation algorithms. An algorithm solves SVP approximately within a factor c (possibly dependent on the dimension of the lattice) if on input a lattice Λ it finds a vector $\mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}$ of length at most c times the shortest non-zero vector in Λ. Analogously, an algorithm solves CVP approximately within a factor c if on input a lattice Λ and a target vector $\mathbf{y}$ it finds a lattice vector $\mathbf{x} \in \Lambda$ such that $\|\mathbf{x} - \mathbf{y}\|$ is at most c times the distance of $\mathbf{y}$ from Λ.

A polynomial time algorithm to solve SVP in dimension 2 was already implicit in work by Gauss [27]. This algorithm is essentially a generalization to dimension 2 of the Euclidean algorithm to compute the greatest common divisor of two integers and has been extensively analyzed and improved to achieve asymptotically low bit complexity [76, 77, 72, 81, 40, 41]. Minkowski's "Convex Body Theorem" directly implies that any lattice Λ has a short non-zero vector of length at most $\sqrt{n} \det(\Lambda)^{1/n}$. However, the proof is non-constructive and does not give an effective procedure to find such short vectors. We remark that although a lattice Λ might contain vectors considerably shorter than $\sqrt{n} \det(\Lambda)^{1/n}$, it has been proved that approximating the shorter lattice vector within a polynomial (in n) factor can be reduced to finding a lattice vector of length within a polynomial factor from $\det(\Lambda)^{1/n}$. Algorithms to find the shortest vector in a lattice in arbitrary dimension were proposed by Rosser [67], Coveyou [21], Knuth [47] and Dieter [22], but none of these algorithms can be

proved to run in polynomial time, even if the dimension of the lattice is fixed to 2. With the development of the LLL basis reduction algorithm [59, 58] it was possible to approximate SVP in polynomial time within a factor $2^{n/2}$. The approximation factor was improved to $2^{\epsilon n}$ by Schnorr [68] using a modification of the LLL basis reduction algorithm. The LLL algorithm, and its variants, can also be used to find in polynomial time exact solutions to SVP for any fixed number of dimensions. The dependency of the running time on the dimension is 2^{n^2}. Better algorithms to solve SVP exactly were given by Kannan in [45] where the dependency of the running time on the dimension is $2^{n \ln n}$.

Although in practice the LLL algorithm and its variants perform much better than the theoretical worst case lower bound, to date no polynomial time algorithm is known to approximate SVP within a factor polynomial in the dimension of the lattice. Evidence of the intractability of the shortest vector problem was first given by van Emde Boas [78] who proved that SVP is NP-hard in the l_∞ norm and conjectured the NP-hardness in the Euclidean norm. Recently, Ajtai proved that SVP is NP-hard for randomized reductions, and approximating SVP within a factor $1 + 2^{-n^c}$ is also NP-hard. The non-approximability factor was improved to $1 + n^{-\epsilon}$ by Cai and Nerurkar [13], but still a factor that rapidly approaches one as the dimension of the lattice grows. The main goal of this thesis is to prove that SVP is NP-hard to approximate within a factor bounded away from one.

Verifying solutions to SVP has also been investigated. The decisional version of SVP is clearly in NP: any lattice vector is a proof that the shortest vector is at least that short. Proving that the shortest vector is long is a bit harder. Lagarias, Lenstra and Schnorr [52] proved that approximating SVP within a factor n is in coNP, that is, there exist short polynomial time verifiable proofs that the shortest vector in a lattice is at least λ_1/n (for an alternative proof see [12]). Goldreich and Goldwasser [29] proved that approximating SVP within a factor $\sqrt{n}$ is in coAM, that is, there is a constant round interactive proof system to show that the shortest vector in a lattice has length at least $\lambda_1/\sqrt{n}$. A similar result was proved by Cai in [12] for the $n^{1/4}$-unique shortest vector problem (a variant of the shortest vector problem in

which all vectors shorter than $n^{1/4}\lambda_1$ are parallel). These coNP and coAM results are usually regarded as evidence that approximating SVP within certain factors is not NP-hard. In particular [52] shows that approximating SVP within a factor n is not NP-hard unless $P = NP$, while [29] shows that approximating SVP within a factor $\sqrt{n}$ is not NP-hard[1] unless the polynomial time hierarchy collapses.

The closest vector problem had a similar history, except that polynomial time (approximation) algorithms were harder to find and stronger hardness results were more easily established. Babai [8] modified the LLL reduction algorithm to approximate in polynomial time CVP within a factor 2^n. The approximation factor was improved to $2^{\epsilon n}$ in [68, 44, 70]. Kannan [45] gave a polynomial time algorithm to solve CVP exactly in any fixed number of dimensions. The dependency of the running time on the dimension is again $2^{n \ln n}$. Finding a polynomial time algorithm to approximate CVP within a polynomial factor is a major open problem in the area.

Regarding the hardness of the closest vector problem, van Emde Boas [78] proved that CVP is NP-hard for any l_p norm ($p \geq 1$). In [7], Arora et al. used the machinery from Probabilistically Checkable Proofs to show that approximating CVP within any constant factor is NP-hard, and approximating it within $2^{\lg^{1-\epsilon} n}$ is almost NP-hard. Recently, Dinur, Kindler and Safra [23] proved that approximating CVP within that same factor is NP-hard.

The decisional version of CVP is clearly in NP: any lattice vector close to $\mathbf{y}$ gives an upper bound on the distance of $\mathbf{y}$ from the lattice. Lagarias, Lenstra and Schnorr [52] proved that approximating CVP within $n^{1.5}$ is in coNP. Hastad [33] and Banaszczyk [9] improved the approximation factor to n. Goldreich and Goldwasser [29] showed that approximating CVP within a factor $\sqrt{n}$ is in coAM. Again, these verifiability results are usually regarded as evidence that approximating CVP within certain factors is not NP-hard, unless $P = NP$ or the polynomial time hierarchy collapses.

[1] Technically, one should require NP-hardness via "smart" reductions. The reader is referred to [29] for more details.

The relation between SVP and CVP has also been considered. SVP and CVP are usually referred to as the homogeneous and inhomogeneous problem, in analogy with homogeneous and inhomogeneous Diophantine equations. Analogy with other Diophantine problems together with the faster progress in proving the hardness of CVP and the major ease in approximating SVP suggest that SVP may be easier than CVP. Although the NP-completeness of CVP implies that the decisional version of SVP can be reduced in polynomial time to CVP, there is not an obvious direct reduction between the two problems, and finding the relationship between the approximation versions of the two problems has been an open problem for a while. Notice that a SVP instance Λ is not equivalent to the CVP instance $(\Lambda, \mathbf{0})$ because the lattice vector closest to the origin is the origin itself (in CVP the solution is not required to be a non-zero vector). Recently Henk [35] gave direct proof that SVP is polynomial time Turing reducible to CVP, and similar techniques have been used by Seifert [73] to show that approximating SVP within a factor c (possibly dependent on the dimension n) is polynomial time Turing reducible to approximating CVP within the same approximation factor.

In the other direction, Kannan showed that approximating CVP within a factor $\sqrt{n}$ is polynomial-time Turing-reducible to solving SVP exactly [45], and approximating SVP within a factor $n^{3/2}f(n)^2$ is polynomial-time Turing-reducible to approximating SVP within a factor $f(n)$ for any non-decreasing function $f(n)$ [44]. More will be said about reducing CVP to SVP in the next chapter, where we prove that SVP is NP-hard to approximate by reduction from a modification of CVP. As an aside, [45] shows also that the search and decisional versions of SVP are polynomial time Turing equivalent.

2.2 Promise Problems and Hardness of Approximation

Both for CVP and SVP one can ask for different algorithmic tasks. These are (in decreasing order of difficulty):

- *(Search)* Find the (non-zero) lattice vector $\mathbf{x} \in \Lambda$ such that $\|\mathbf{x}-\mathbf{y}\|$ (resp. $\|\mathbf{x}\|$) is minimized.

- *(Optimization)* Find the minimum of $\|\mathbf{x}-\mathbf{y}\|$ (resp. $\|\mathbf{x}\|$) over $\mathbf{x} \in \Lambda$ (resp. $\mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}$).

- *(Decision)* Given a real $r > 0$, decide whether there is a (non-zero) lattice vector $\mathbf{x}$ such that $\|\mathbf{x}-\mathbf{y}\| \leq r$ (resp. $\|\mathbf{x}\| \leq r$).

We remark that to date all known (approximation) algorithms for SVP and CVP actually solve the search problem (and therefore also the associated optimization and decision problems), while all known hardness results hold for the decision problem (and therefore imply the hardness of the optimization and search problems as well). This suggests that the hardness of solving SVP and CVP is already captured by the decisional task of determining whether or not there exists a solution below some given threshold value.

The same computational tasks can be defined also for the approximation versions of SVP and CVP. We follow [29] and formalize the decisional task associated to approximate SVP and CVP in terms of the promise problems `GapSVP` and `GapCVP` to be defined.

Promise problems are a generalization of decision problems well suited to study the hardness of approximation. A promise problem is a pair $(\Pi_{\text{YES}}, \Pi_{\text{NO}})$ of disjoint languages, i.e., $\Pi_{\text{YES}}, \Pi_{\text{NO}} \subseteq \{0,1\}^*$ and $\Pi_{\text{YES}} \cap \Pi_{\text{NO}} = \emptyset$. An algorithm solves the promise problem $(\Pi_{\text{YES}}, \Pi_{\text{NO}})$ if on input an instance $I \in \Pi_{\text{YES}} \cup \Pi_{\text{NO}}$ it correctly decides whether $I \in \Pi_{\text{YES}}$ or $I \in \Pi_{\text{NO}}$. The behavior of the algorithm when $I \notin \Pi_{\text{YES}} \cup \Pi_{\text{NO}}$ (I does not satisfy the promise) is not specified.

A special case are decision problems, where $\Pi_{\text{NO}} = \{0,1\}^* \setminus \Pi_{\text{YES}}$ and the promise $I \in \Pi_{\text{YES}} \cup \Pi_{\text{NO}}$ is vacuously true. We now define the promise problem associated to the approximate SVP and CVP.

Definition 1 (Approximate SVP) *The promise problem* $\texttt{GapSVP}_g$*, where* g *(the gap function) is a function of the dimension, is defined as follows:*

- YES *instances are pairs* (B,t) *where* $B \in \mathcal{Z}^{k \times n}$ *is a lattice basis and* $t \in \mathcal{Q}$ *a threshold such that* $\|B\mathbf{z}\| \leq t$ *for some* $\mathbf{z} \in \mathcal{Z}^n \setminus \{\mathbf{0}\}$.
- NO *instances are pairs* (B,t) *where* $B \in \mathcal{Z}^{k \times n}$ *is a lattice basis and* $t \in \mathcal{Q}$ *is a threshold such that* $\|B\mathbf{z}\| > gt$ *for all* $\mathbf{z} \in \mathcal{Z}^n \setminus \{\mathbf{0}\}$.

Definition 2 (Approximate CVP) *The promise problem* $\texttt{GapCVP}_g$*, where* g *(the gap function) is a function of the dimension, is defined as follows:*

- YES *instances are triples* $(B,\mathbf{y},t)$ *where* $B \in \mathcal{Z}^{k \times n}$ *is a lattice basis,* $\mathbf{y} \in \mathcal{Z}^k$ *is a vector and* $t \in \mathcal{Q}$ *is a threshold such that* $\|B\mathbf{z} - \mathbf{y}\| \leq t$ *for some* $\mathbf{z} \in \mathcal{Z}^n$.
- NO *instances are triples* $(B,\mathbf{y},t)$ *where* $V \in \mathcal{Z}^{k \times n}$ *is a lattice,* $\mathbf{y} \in \mathcal{Z}^k$ *is a vector and* $t \in \mathcal{Q}$ *is a threshold such that* $\|B\mathbf{z} - \mathbf{y}\| > gt$ *for all* $\mathbf{z} \in \mathcal{Z}^n$.

Notice that when the approximation factor $c = 1$, the promise problems $\texttt{GapSVP}_c$ and $\texttt{GapCVP}_c$ reduce to the decision problems associated to exact SVP and CVP. Promise problems $\texttt{GapSVP}_c$ and $\texttt{GapCVP}_c$ capture the computational task of approximating SVP and CVP within a factor c in the following sense. Assume algorithm A solves approximately SVP within a factor c, i.e., on input a lattice Λ, it finds a vector $\mathbf{x} \in \Lambda$ such that $\|\mathbf{x}\| < c\lambda_1(\Lambda)$. Then A can be used to solve $\texttt{GapSVP}_c$ as follows. On input (L,t), run algorithm A on L to obtain an estimate $t' = \|\mathbf{x}\| \in [\lambda_1, c\lambda_1]$ of the shortest vector length. If $t' > ct$ then $\lambda_1 > t$ and (L,t) is a NO instance. Conversely, if $t' < ct$ then $\lambda_1 < ct$ and from the promise $(L,t) \in \Pi_{\text{YES}} \cup \Pi_{\text{NO}}$ one deduces that (L,t) is a YES instance. A similar arguments holds for the closest vector problem.

Reductions between promise problems are defined in the obvious way. A function $f\colon \{0,1\}^* \to \{0,1\}^*$ is a reduction from $(\Pi_{\text{YES}}, \Pi_{\text{NO}})$ to $(\Sigma_{\text{YES}}, \Sigma_{\text{NO}})$ if it maps YES

instances to YES instances and NO instances to NO instances, i.e., $f(\Pi_{\text{YES}}) \subseteq \Sigma_{\text{YES}}$ and $f(\Pi_{\text{NO}}) \subseteq \Sigma_{\text{NO}}$. Clearly any algorithm A to solve $(\Sigma_{\text{YES}}, \Sigma_{\text{NO}})$ can be used to solve $(\Pi_{\text{YES}}, \Pi_{\text{NO}})$ as follows: on input $I \in \Pi_{\text{YES}} \cup \Pi_{\text{NO}}$, run A on $f(I)$ and output the result. Notice that $f(I)$ always satisfy the promise $f(I) \in \Sigma_{\text{YES}} \cup \Sigma_{\text{NO}}$, and $f(I)$ is a YES instance iff I is a YES instance.

We now define one more promise problem that will be useful in the sequel. The problem is a modification of GapCVP in which YES instances are required to have a boolean solution, and in the NO instances the target vector can be multiplied by any non-zero integer.

Definition 3 (Modified CVP) *The promise problem* GapCVP'_g*, where* g *(the gap function) is a function of the dimension, is defined as follows:*

- YES *instances are triples* $(L, \mathbf{y}, t)$ *where* $L \in \mathcal{Z}^{k \times n}$ *is a lattice,* $\mathbf{y} \in \mathcal{Z}^k$ *a vector and* $t \in \mathcal{Q}$ *a threshold such that* $\|L\mathbf{z} - \mathbf{y}\| \leq t$ *for some* $\mathbf{z} \in \{0,1\}^n$.
- NO *instances are triples* $(L, \mathbf{y}, t)$ *where* $L \in \mathcal{Z}^{k \times n}$ *is a lattice,* $\mathbf{y} \in \mathcal{Z}^k$ *a vector and* $t \in \mathcal{Q}$ *a threshold such that* $\|L\mathbf{z} - w\mathbf{y}\| > gt$ *for all* $\mathbf{z} \in \mathcal{Z}^n$ *and all* $w \in \mathcal{Z} \setminus \{\mathbf{0}\}$.

In [7] it is proved that GapCVP_c and its variant GapCVP'_c are NP-hard for any constant c.

Theorem 1 *For any constant* $c \geq 1$ *there exists a polynomial time computable reduction from SAT to* GapCVP'_c.

Reductions between promise problems can be composed in the obvious way. Therefore to prove that a promise problem is NP-hard it suffices to give for some $c \geq 1$ a polynomial time computable reduction from GapCVP'_c to it.

Chapter 3

Reducing CVP to SVP

In this chapter we present the main result of this thesis: we prove that the shortest vector problem is NP-hard to approximate for randomized reduction within some constant factor. In particular we prove that for any l_p norm ($p \geq 1$), the promise problem $\texttt{GapSVP}_c$ is NP-complete (for randomized reductions) for all $c < 2^{1/p}$.

The proof is by reduction from another promise problem associated to the closest vector problem (the inhomogeneous version of the shortest vector problem). Therefore, the technique we use to reduce CVP to SVP can be considered as a "homogenization" process. This is not new in the study of the computational complexity of lattice problems (see [8, 45, 44]). However all homogenization techniques developed in the past involve some sort of recursion on the number of dimensions of the lattice and consequently introduce error factors of $n^{1/p}$ or greater. For example, [45] shows that approximating CVP within a factor $\sqrt{n}$ is polynomial-time Turing-reducible to solving SVP exactly, while [44] shows that approximating SVP within a factor $n^{3/2}f(n)^2$ is polynomial-time Turing-reducible to approximating SVP within a factor $f(n)$ for any non-decreasing function $f(n)$. Therefore, since there is some evidence that CVP is not NP-hard to approximate within factors greater than $\sqrt{n}$ [29], these reductions are unluckily to be useful in proving that SVP is NP-hard. In this chapter we introduce a novel homogenization technique that can be applied to approximation versions of CVP which are known to be NP-hard.

The idea behind our homogenization technique is the following. Assume one wants

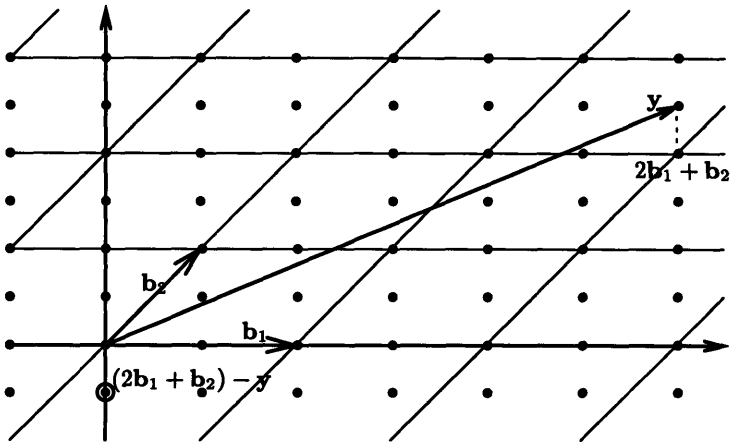

Figure 3-1: The shortest vector $2\mathbf{b}_1 + \mathbf{b}_2 - \mathbf{y}$ in the lattice generated by $\mathbf{b}_1, \mathbf{b}_2, \mathbf{y}$ correspond to the shortest vector in $\Lambda = \mathcal{L}(\mathbf{b}_1, \mathbf{b}_2)$ closest to $\mathbf{y}$.

to find the point in a lattice $\Lambda = \mathcal{L}(B)$ (approximately) closest to some vector $\mathbf{y}$. We look for the shortest vector in the lattice generated by $[B|\mathbf{y}]$, i.e., the original lattice Λ together with the target vector $\mathbf{y}$. If the shortest vector in this lattice is of the form $B\mathbf{x} - \mathbf{y}$ then $B\mathbf{x}$ is the lattice vector in Λ closest to $\mathbf{y}$ (see figure 3-1 for an illustrative example). The problem is that lattice Λ might contain vectors shorter than the distance of $\mathbf{y}$ from Λ. If this is the case, by solving the shortest vector problem in the lattice generated by $[B|\mathbf{y}]$ one simply finds the shortest vector in Λ (see figure 3-2). Another problem is that the shortest vector in $\mathcal{L}([B|\mathbf{y}])$ might correspond to a vector in Λ close to a multiple of $\mathbf{y}$ (see figure 3-3). These problems are dealt with by homogenization techniques by embedding the lattice $[B|\mathbf{y}]$ in some higher dimensional lattice, i.e., introducing some new coordinates and extending the basis vectors in B and $\mathbf{y}$ with the appropriate values in these coordinates. A similar idea is already present in [45] where the lattice $\begin{bmatrix} B & \mathbf{y} \\ \mathbf{0} & 0.51\lambda_1(B) \end{bmatrix}$ is defined (the value $\lambda_1(B)$ is computed calling an SVP oracle). Notice that the additional row forces the last basis vector to be used at most once. However, there is still the more serious problem that the last column might not be used at all, which is solved by a recursive method that introduce a $\sqrt{n}$ error factor.

We now sketch our homogenization technique. Given a lattice basis B and a target

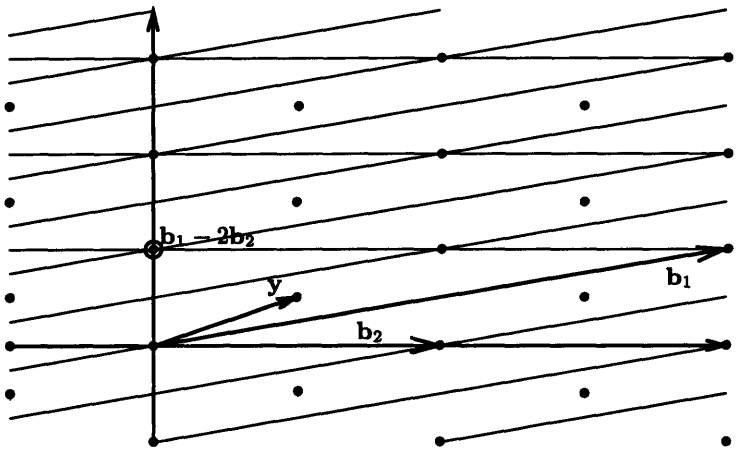

Figure 3-2: The shortest vector $\mathbf{b}_1 - 2\mathbf{b}_2$ in the lattice generated by $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{y}]$ belongs to the lattice $\Lambda = \mathcal{L}(\mathbf{b}_1, \mathbf{b}_2)$.

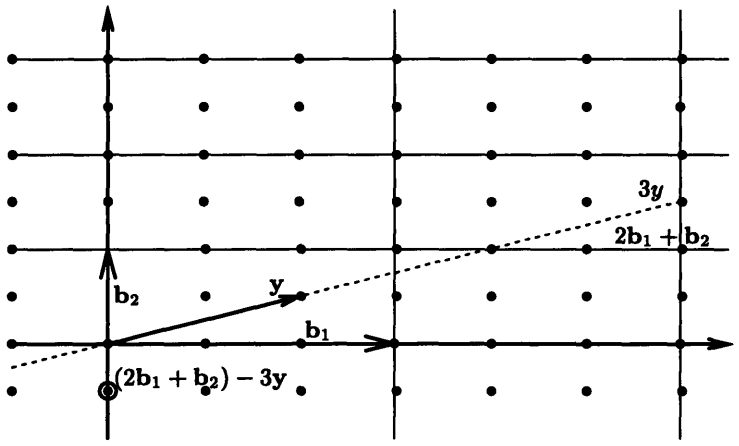

Figure 3-3: The shortest vector $2\mathbf{b}_1 + \mathbf{b}_2 - 3\mathbf{y}$ in the lattice generated by $[\mathbf{b}_1, \mathbf{b}_2, \mathbf{y}]$ correspond to the vector in $\Lambda = \mathcal{L}(\mathbf{b}_1, \mathbf{b}_2)$ closest to $3\mathbf{y}$.

vector $\mathbf{y}$, we first randomize B by multiplying it by an integer matrix C to get a set of vectors $B \cdot C$. The column of $B \cdot C$ are no longer linearly independent and have the property that lattice vectors have many possible representations as a sum of them. Then we embed the vectors in $B \cdot C$ and $\mathbf{y}$ in a higher dimensional space as follows. Let L and $\mathbf{s}$ be a lattice and a vector such that there are many lattice vectors whose distance from $\mathbf{s}$ is appreciably less than the length of the shortest vector in L. we define Γ to be the lattice generated by an appropriately scaled version of the matrix $\begin{bmatrix} B \cdot C & \mathbf{y} \\ L & \mathbf{s} \end{bmatrix}$. Any shortest vector in Γ must use the last column, because otherwise a high penalty will be incurred in the additional coordinates. Moreover, if there is a vector $B\mathbf{x}$ close to $\mathbf{y}$, a short vector in Γ can be found (with high probability) by looking for a vector $L\mathbf{z}$ close to $\mathbf{s}$ such that $C\mathbf{z} = \mathbf{x}$.

The rest of the chapter is organized as follows. In section 3.1 we formally define the property of the "homogenizing gadget" $(L, \mathbf{s}, C)$ and assert that matrices with this property can be efficiently constructed. In section 3.2 we use the homogenizing gadget to prove that SVP is NP-hard to approximate by reduction from CVP.

3.1 The Homogenizing Gadget

The core of our reduction is the following lemma regarding the existence of matrices $L, \mathbf{s}$ and C needed in our homogenization process.

Lemma 1 (Technical Lemma) *For any l_p norm ($p \geq 1$) and constant $c < 2^{1/p}$, there exists a (probabilistic) polynomial time algorithm that on input 1^k outputs a lattice $L \in Z^{m' \times m}$, a vector $\mathbf{s} \in Z^{m'}$, a matrix $C \in Z^{k \times m}$ and a rational r such that*

- *for all $\mathbf{z} \in Z^m$, $\|L\mathbf{z}\|_p > cr$.*
- *for all boolean vectors $\mathbf{x} \in \{0,1\}^k$ there exists an integer vector $\mathbf{z} \in Z^m$ such that $C\mathbf{z} = \mathbf{x}$ and $\|L\mathbf{z} - \mathbf{s}\|_p < r$.*

The lemma is illustrated in figure 3-4: it is possible to find a lattice L with minimum distance $\lambda_1 > cr$ and a sphere centered in $\mathbf{s}$ with radius r such that all

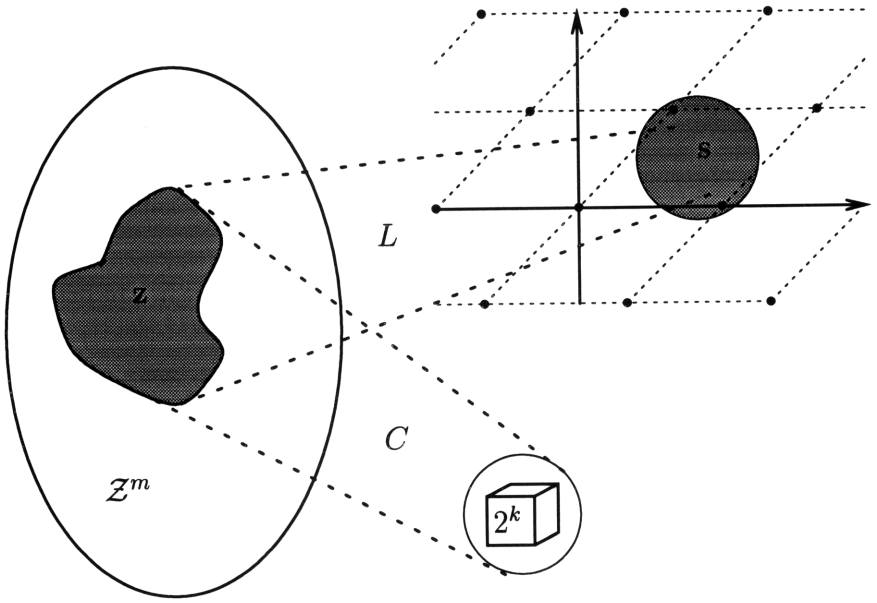

Figure 3-4: The technical lemma: lattice L has minimum distance c times the radius of sphere $\mathbf{s}$ and all boolean vectors of length k can be expressed as $C\mathbf{z}$ for some lattice vector $L\mathbf{z}$ inside the sphere.

boolean vectors of length k can be expressed as $C\mathbf{z}$ for some lattice vector $L\mathbf{z}$ in the sphere. Notice that this implies that the sphere contains at least 2^k lattice points. Proving the technical lemma will be the subject of the next chapters: in particular in Chapter 4 we build a lattice such that there exists a small sphere containing exponentially many lattice points, and in Chapter 5 we define (probabilistically) an integer linear transformation C such that all boolean vectors $\{0,1\}^k$ are in its image. The actual proof of the technical lemma is given in Chapter 6 where we combine the constructions of Chapters 4 and 5. In Chapter 4 we will also prove that for the Euclidean norm it is not possible to pack exponentially many points in a sphere at minimum distance $\sqrt{2}$ times the radius. This implies that the lemma is essentially optimal and the condition $c < \sqrt{2}$ is necessary and sufficient for $L, \mathbf{s}$ and C to exists (in the Euclidean norm). The condition $c < 2^{1/p}$ will also be the limiting factor in the proof of NP-hardness of $\texttt{GapSVP}_c$.

3.2 The Reduction

We use the homogenizing gadget defined in the previous section to prove our main theorem.

Theorem 2 *For any l_p norm ($p \geq 1$) and any $c < 2^{1/p}$, the promise problem* $\mathtt{GapSVP}_c$ *is NP-hard for randomized reductions.*

Proof: Fix an l_p norm and a constant $c < 2^{1/p}$. Let $\tilde{c}$ be a rational between c and $2^{1/p}$ and let g be an integer greater than $(c^{-p} - \tilde{c}^{-p})^{-1/p}$. We prove that $\mathtt{GapSVP}_c$ is NP-hard by reduction from the promise problem $\mathtt{GapCVP}'_g$ which is known to be NP-hard from Theorem 1. Let $(B, \mathbf{y}, d)$ be an instance of $\mathtt{GapCVP}'_g$ and let k be the dimension of lattice $\mathcal{L}(B)$. Run the (randomized) algorithm from Lemma 1 to obtain (with high probability) a lattice $L \in \mathcal{Z}^{m' \times m}$, a vector $\mathbf{s} \in \mathcal{Z}^{m'}$, a matrix $C \in \mathcal{Z}^{k \times m}$ and a rational r such that

- for all $\mathbf{z} \in \mathcal{Z}^m$, $\|L\mathbf{z}\|_p > \tilde{c}r$
- for all vectors $\mathbf{x} \in \{0,1\}^k$ there exists a $\mathbf{z} \in Z^m$ such that $C\mathbf{z} = \mathbf{x}$ and $\|L\mathbf{z} - \mathbf{s}\|_p < r$.

Define the lattice

$$V = \left[\begin{array}{c|c} \alpha B \cdot C & \alpha \mathbf{y} \\ \beta L & \beta \mathbf{s} \end{array}\right]$$

where α and β are two integer scaling factors such that $\frac{\alpha}{\beta} = \frac{\tilde{c}r}{gd}$. Let also $t = \frac{\tilde{c}r\beta}{c} = \frac{gd\alpha}{c}$. We want to prove that if $(B, \mathbf{y}, d)$ is a YES instance of $\mathtt{GapCVP}'_g$ then (V, t) is a YES instance of $\mathtt{GapSVP}'_c$, and if $(B, \mathbf{y}, d)$ is a NO instance of $\mathtt{GapCVP}'_g$ then (V, t) is a NO instance of $\mathtt{GapSVP}'_c$.

First assume that $(B, \mathbf{y}, d)$ is a YES instance, i.e. there exists a boolean vector $\mathbf{x} \in \{0,1\}^k$ such that $\|B\mathbf{x} - \mathbf{y}\| \leq d$. By construction, there exists a vector $\mathbf{z} \in Z^m$ such that $C\mathbf{z} = \mathbf{x}$ and $\|L\mathbf{z} - \mathbf{s}\| < r$. Define $\mathbf{w} = \begin{bmatrix} \mathbf{z} \\ -1 \end{bmatrix}$ and compute the norm of

the corresponding lattice vector:

$$\begin{aligned} \|V\mathbf{w}\|^p &= \alpha^p\|B\mathbf{x}-\mathbf{y}\|^p + \beta^p\|L\mathbf{z}-\mathbf{s}\|^p \\ &\leq (\alpha d)^p + (\beta r)^p \\ &= \left(\frac{ct}{g}\right)^p + \left(\frac{ct}{\tilde{c}}\right)^p \\ &\leq t^p\left(c^p(c^{-p}-\tilde{c}^{-p}) + c^p\tilde{c}^{-p}\right) \\ &= t^p. \end{aligned}$$

proving that (V,t) is a YES instance of $\mathtt{GapSVP_c}$.

Now assume $(B,\mathbf{y},d)$ is a NO instance and let $\mathbf{w} = \begin{bmatrix} \mathbf{z} \\ w \end{bmatrix}$ be a non-zero integral vector. We want to prove that $\|V\mathbf{w}\|^p \geq (ct)^p$. Notice that

$$\|V\mathbf{w}\|^p = \alpha^p\|B\mathbf{x}+w\mathbf{y}\|^p + \beta^p\|L\mathbf{z}+w\mathbf{s}\|^p.$$

We prove that either $\alpha\|N\mathbf{x}+w\mathbf{y}\| > ct$ or $\beta\|L\mathbf{z}+w\mathbf{s}\| > ct$. We distinguish the two cases:

- If $w=0$ then $\mathbf{z}\neq 0$ and by Lemma 1 one has $\beta\|L\mathbf{z}+w\mathbf{s}\| = \beta\|L\mathbf{z}\| > \beta\tilde{c}r = ct$.
- If $w\neq 0$, then by definition of $\mathtt{GapCVP'}$ one has $\alpha\|B\mathbf{x}+w\mathbf{y}\| > \alpha g d = ct$ where $\mathbf{x} = C\mathbf{z}$.

□

Notice that the randomness in the proof of Theorem 2 comes exclusively from Lemma 1. Two simple observations then follow. First of all, notice that the randomness depends only on the size of the instance of the CVP problem we are reducing from, and not from the particular instance. So, the shortest vector problem is also NP-hard to approximate via deterministic non-uniform reductions.

Corollary 1 *For any l_p norm ($p \geq 1$) and any $c < 2^{1/p}$, the promise problem $\mathtt{GapSVP_c}$ is NP-hard for deterministic non-uniform reductions.*

Moreover, if one could prove Lemma 1 via a deterministic algorithm, then the NP-hardness result for SVP would become deterministic. We don't know if there is any deterministic algorithm satisfying Lemma 1. However, the construction in the proof of Lemma 1 can be easily made deterministic using a reasonable number theoretic conjecture. The conjecture is the following:

Conjecture 1 *For any $\epsilon > 0$ there exists a $d > 0$ such that for all b large enough the interval $[b, b + b^{\epsilon}]$ contains a square-free $(\ln b)^d$-smooth number.*

The conjecture is reasonable because relatively simple number theoretic analysis shows that the average number of square-free $(\ln b)^d$-smooth numbers in $[b, b + b^{\epsilon}]$ exceeds $b^{\epsilon - \frac{1}{d}}$. Therefore, if $d = 2/\epsilon$ one expects to find $b^{\frac{\epsilon}{2}}$ square-free smooth numbers in $[b, b + b^{\epsilon}]$. If square-free smooth numbers are distributed uniformly enough then one can reasonably assume that $[b, b + b^{\epsilon}]$ contains at least one such number for all sufficiently large b. In Chapter 6 we prove the following deterministic version of Lemma 1.

Lemma 2 *If Conjecture 1 holds true, then for any l_p norm ($p \geq 1$) and any $c < 2^{1/p}$, there exists a deterministic polynomial time algorithm that on input 1^k outputs a lattice $L \in Z^{m' \times m}$, a vector $\mathbf{s} \in Z^{m'}$, a matrix $C \in Z^{k \times m}$ and a rational r such that*

- *for all $\mathbf{z} \in Z^m$, $\|L\mathbf{z}\|_p > cr$.*
- *for all boolean vectors $\mathbf{x} \in \{0,1\}^k$ there exists an integer vector $\mathbf{z} \in Z^m$ such that $C\mathbf{z} = \mathbf{x}$ and $\|L\mathbf{z} - \mathbf{s}\|_p < r$.*

From the proof of Theorem 2 and the above lemma one immediately gets the following corollary.

Corollary 2 *If Conjecture 1 holds true, then for any l_p norm ($p \geq 1$) and any $c < 2^{1/p}$, the promise problem $\mathbf{GapSVP_c}$ is NP-hard for deterministic many-one reductions.*

Chapter 4

Packing Lattice Points in a Sphere

In this chapter we study the following packing problem. How many lattice points can be packed in an n-dimensional sphere of radius ρ, while keeping the length of the shortest vector in the lattice at least λ? Clearly the answer depends on the ratio λ/ρ only. If we drop the requirement that the points must belong to a lattice, and normalize the minimum distance between points to $\lambda = 2$ we get the following sphere packing problem (see figure 4-1): how many unit balls can be packed inside an n-dimensional sphere of radius $R = 1 + \rho$? We want to determine for which values of λ/ρ we can pack exponentially (in n) many points. Notice the following (trivial) facts:

- If λ/ρ dicreases with n, say $\lambda/\rho = 2n^{-1/2}$, than one can pack exponentially many spheres. Consider for example the cubic lattice $2\mathcal{Z}^n$ with minimum distance $\lambda = 2$. The sphere centered in $\mathbf{s} = [1, \ldots, 1]$ of radius $\rho = \sqrt{n}$ contains all 2^n vertices of the hypercube $[2 \pm 2, \ldots, 2 \pm 2]$ (see figure 4-2).

- If λ/ρ is sufficiently large, than only a constant number of points can be packed, independently of the dimension. For example, if $\lambda > 2\rho$ then only one point can be packed, while if $\lambda = 2\rho$ one can pack at most 2 points.

- One can keep λ/ρ bounded and still pack arbitrarily many points in high dimension. For example, consider the *even* lattice generated by the vectors $\mathbf{e}_1 + \mathbf{e}_i$ $(i = 1, \ldots, n)$ with minimum distance $\lambda = 2$. The sphere centered in e_1 of radius

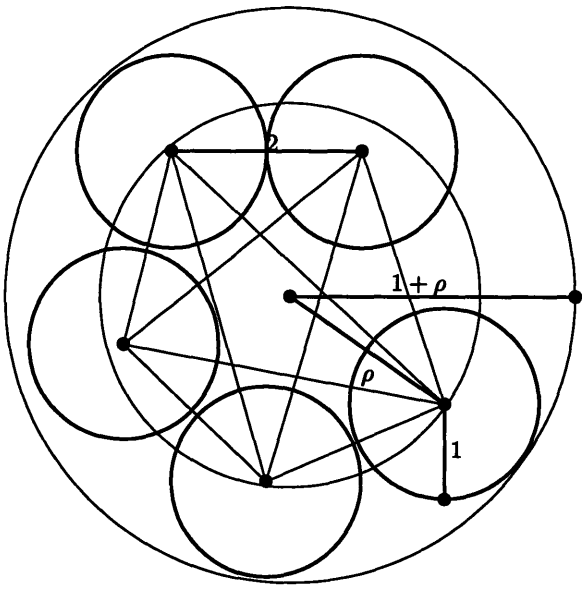

Figure 4-1: Packing spheres in a bigger sphere

$\rho = \sqrt{2}$ contains the $2n$ lattice points $\mathbf{e}_1 \pm \mathbf{e}_i$ $(i = 1, \ldots, n)$. This correspond to packing $2n$ unit spheres in a ball of radius $\sqrt{2}$ as shown in figure 4-3.

We are interested in lattices such that $\lambda/\rho \geq 1$. A few natural questions arise. Can we do any better when $\lambda/\rho = \sqrt{2}$? What happen when $\lambda/\rho > \sqrt{2}$? Can we pack exponentially many points when $\lambda/\rho \in [1, \sqrt{2})$? In the course of this chapter we will answer the previous questions and prove the following facts:

1. If $\lambda/\rho > \sqrt{2}$, then one can pack only constantly many points (independently of the dimension).

2. If $\lambda/\rho = \sqrt{2}$, then the maximum number of points is precisely $2n$.

3. For any $\rho > \sqrt{2}$, one can pack exponentially many points.

Upper bounds 1 and 2 actually hold even if we drop the requirements for the points to belong to a lattice, and were first proved in [66] for spherical codes (i.e., a sphere packing problem with the additional constraint that all points must be at the same distance from the origin).

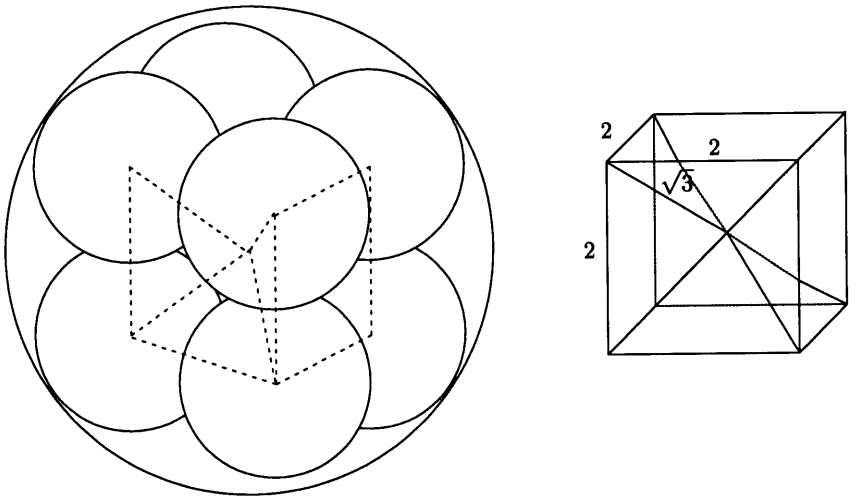

Figure 4-2: The cubic packing

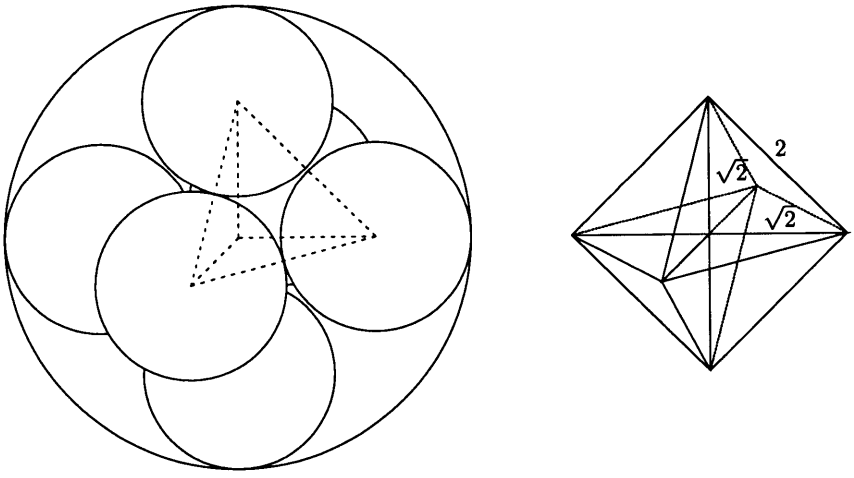

Figure 4-3: The octahedral packing

If we don't ask for the points to belong to a lattice with minimum distance λ, an exponential lower bounds for any $\lambda/\rho < \sqrt{2}$ is already implicit in Gilbert bound [28] for binary codes. Non-constructive proofs for spherical codes were given by Shannon [75] and Wyner [80]. However, the points generated by these constructions do not form a lattice. We give a proof of lower bound 3 in which the points are vertices of the fundamental parallelepiped of a lattice with minimum distance λ. The proof is constructive, meaning that a basis for the lattice and the center of the sphere can be efficiently computed.

We remark that the lower bounds in [75, 80] show that it is possible to pack $2^{\alpha n}$ points, where α is a constant that depends only on $\rho > \sqrt{2}$, while our construction succeeds in packing only $2^{n^{\alpha}}$ points. We don't know if our construction is asympthotically optimal for lattice packings.

The rest of this chapter is organized as follows. In section 4.1 we present the simple proofs of the upper bounds for the cases $\lambda/\rho \geq \sqrt{2}$. These are not immediately relevant to the construction of the homogenizing gadget of Lemma 1, but explain why $\sqrt{2}$ is a limiting factor in that lemma. In Section 4.2 we show how to pack exponentially many points when $\lambda/\rho < \sqrt{2}$. The lattice defined in Section 4.2 is a real lattice. In Section 4.3 we show that the lattice described in Section 4.2 can be efficiently approximated by a rational one. In the last section we present a few more results about our lattice packing. These results are not directly useful to the rest of this thesis, but add some insight to the construction of section 4.2.

4.1 Packing Points in Small Spheres

In this section we study the cases when $\lambda/\rho \geq \sqrt{2}$ and prove upper bounds on the number of points that can be packed in a sphere of radius ρ while keeping the minimum distance between points at least λ. Without loss of generality we assume $\lambda = 2$ and bound the maximum number of points that can be placed in a sphere of radius $\rho \leq \sqrt{2}$ while keeping the points at distance at least 2 of each other. Let's start with the simple case $\rho < \sqrt{2}$.

Proposition 1 *For any $\rho < \sqrt{2}$, the maximum number of points with minimum distance 2 that can be packed in a sphere of radius ρ is $\left\lfloor \frac{2}{2-\rho^2} \right\rfloor$.*

Proof: Let $\mathbf{x}_1, \ldots, \mathbf{x}_N$ be a set of vectors such that $\|\mathbf{x}_i\| \leq \rho < \sqrt{2}$ and $\|\mathbf{x}_i - \mathbf{x}_j\| \geq 2$ for all $i \neq j$. Notice that

$$\begin{aligned} N(N-1)4 &\leq \sum_{i=1}^{N}\sum_{j=1}^{N} \|\mathbf{x}_i - \mathbf{x}_j\|^2 \\ &= \sum_{i=1}^{N}\sum_{j=1}^{N} (\|\mathbf{x}_i\|^2 + \|\mathbf{x}_j\|^2 - 2\langle \mathbf{x}_i, \mathbf{x}_j \rangle) \\ &= 2N\sum_{i=1}^{N} \|\mathbf{x}_i\|^2 - 2\left\|\sum_{i=1}^{N} \mathbf{x}_i\right\|^2 \\ &\leq 2N^2\rho^2 \end{aligned}$$

and therefore $2(N-1) \leq N\rho^2$. Solving the linear inequality for N one gets $N \leq \frac{2}{2-\rho^2}$ and since N is an integer $N \leq \left\lfloor \frac{2}{2-\rho^2} \right\rfloor$. □

Notice that the above bound is sharp: for all $\rho < \sqrt{2}$, one can put $n = \left\lfloor \frac{2}{2-\rho^2} \right\rfloor$ unit balls on the vertices of an $(n-1)$-dimensional simplex, and inscribe the simplex inside a sphere of radius $\sqrt{2(1-\frac{1}{n+1})} \leq \rho$ (see figure 4-4). This example also shows that when $\rho = \sqrt{2}$ for every $n \geq 1$ one can pack $n+1$ spheres in the n-dimensional ball of radius $1+\rho$. In fact it is possible to do better than that. For example one can place $2n$ spheres centered in $\pm\sqrt{2}e_i$ (see figure 4-3). We now show that this packing is optimal.

Proposition 2 *The maximum number of points at distance at least 2 of each other that can be placed in a sphere of radius $\sqrt{2}$ is $2n$.*

Proof: By induction on n. If $n = 1$, the statement is true. Now assume the statement holds for some value n, and let's prove it for $n+1$. Let $\mathbf{x}_1, \ldots, \mathbf{x}_N$ vectors in $\mathcal{R}^{n+1}$ such that $\|\mathbf{x}_i\|^2 \leq 2$ and $\|\mathbf{x}_i - \mathbf{x}_j\|^2 \geq 4$. Notice that for all $i \neq j$ one has

$$\begin{aligned} \langle \mathbf{x}_i, \mathbf{x}_j \rangle &= \frac{1}{2}(\|\mathbf{x}_i\|^2 + \|\mathbf{x}_j\|^2 - \|\mathbf{x}_i - \mathbf{x}_j\|^2) \\ &\leq \frac{1}{2}(2+2-4) = 0 \end{aligned}$$

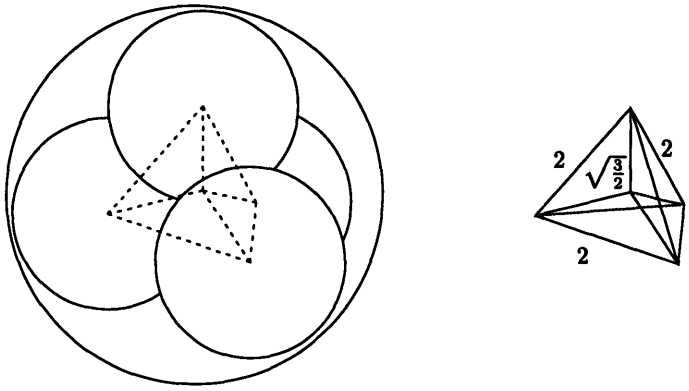

Figure 4-4: The tetrahedral packing

i.e., the angles between any pair of vectors are at least $\pi/2$. We first explain the geometric idea behind the proof. Assume without loss of generality that $\mathbf{x}_N \neq \mathbf{0}$. Think of $\mathbf{x}_N$ as the north pole. We map all point to the poles and the equator in such a way that all angles between any pair of points remain at least $\pi/2$. Then, we apply induction to the set of points on the equator.

We now give the formal proof. Define the set of vectors

$$\mathbf{x}'_i = \begin{cases} \langle \mathbf{x}_N, \mathbf{x}_N \rangle \mathbf{x}_i - \langle \mathbf{x}_i, \mathbf{x}_N \rangle \mathbf{x}_N & \text{if } \langle \mathbf{x}_N, \mathbf{x}_N \rangle \mathbf{x}_i \neq \langle \mathbf{x}_i, \mathbf{x}_N \rangle \mathbf{x}_N \\ \mathbf{x}_i & \text{otherwise} \end{cases}$$

and let $\mathbf{x}''_i = \sqrt{2}\mathbf{x}'_i / \|\mathbf{x}'_i\|$. Notice that for all i, $\|\mathbf{x}''_i\|^2 = 2$ (i.e., $\mathbf{x}''_i$ is on the surface) and either $\mathbf{x}''_i = \pm \mathbf{x}''_N$ (i.e., $\mathbf{x}''_i$ is a "pole") or $\langle \mathbf{x}''_i, \mathbf{x}''_N \rangle = 0$ (i.e., $\mathbf{x}''_i$ is on the "equator"). We now prove that $\|\mathbf{x}''_i - \mathbf{x}''_j\|^2 \geq 4$ for all $i \neq j$. If $\mathbf{x}''_i = \pm \mathbf{x}''_N$ or $\mathbf{x}''_j = \pm \mathbf{x}''_N$ it is obvious. So, assume $\mathbf{x}''_i \neq \pm \mathbf{x}''_N$ and $\mathbf{x}''_j \neq \pm \mathbf{x}''_N$. Notice that

$$\begin{aligned} \|\mathbf{x}''_i - \mathbf{x}''_j\| &= \|\mathbf{x}''_i\|^2 + \|\mathbf{x}''_j\|^2 - 2\langle \mathbf{x}''_i, \mathbf{x}''_j \rangle \\ &= 2 + 2 - 2\frac{\langle \mathbf{x}_i, \mathbf{x}_j \rangle \langle \mathbf{x}_N, \mathbf{x}_N \rangle^2 - \langle \mathbf{x}_i, \mathbf{x}_N \rangle \langle \mathbf{x}_j, \mathbf{x}_N \rangle \langle \mathbf{x}_N, \mathbf{x}_N \rangle}{\|\mathbf{x}'_i\| \cdot \|\mathbf{x}'_j\|} \\ &\geq 4 \end{aligned}$$

because $\langle \mathbf{x}_i, \mathbf{x}_j \rangle, \langle \mathbf{x}_i, \mathbf{x}_N \rangle, \langle \mathbf{x}_j, \mathbf{x}_N \rangle \leq 0$ and $\langle \mathbf{x}_N, \mathbf{x}_N \rangle > 0$. Therefore all points, except at most two of them, belong to the n-dimensional subspace orthogonal to $\mathbf{x}_N$. By

induction hypothesis there are at most $2n$ such points and $N \leq 2(n+1)$. □

4.2 The Exponential Sphere Packing

In this section we study the case $\lambda/\rho < \sqrt{2}$. For any ρ and λ satisfying $\lambda < \sqrt{2}\rho$, we prove that there exist a real lattice Λ with minimum distance λ and a sphere $B(\mathbf{s}, \rho)$ containing 2^{n^δ} lattice points (for some constant $\delta > 0$ depending on $c = \lambda/\rho$). The proof is constructive and has the additional property that the centers of the spheres are vertices of the fundamental parallelepiped of a lattice basis. The statement holds (with the appropriate changes) for any l_p norm. We first define a lattice and prove a lower bound on the length λ_1 of its shortest vector. Then we look for a sphere with radius λ_1/c containing many lattice points.

4.2.1 The lattice

We begin by defining a lattice Λ and bounding the length of its shortest vector. For notational convenience we define Λ as an m-dimensional lattice in $\mathcal{R}^{m+1}$. A full dimensional lattice with the same properties can be easily found by simple linear algebra. The definition of Λ is parametric with respect to a real $\alpha > 0$, a sequence of positive integers $\mathbf{a} = a_1, \ldots, a_m$ and an l_p norm ($p \geq 1$), and we write $\Lambda_\alpha^p[\mathbf{a}]$ when we want to make this parameters explicit. We use the logarithms of the integers a_1 to a_m as entries in the basis vectors, and define a basis vector for each a_i. The idea is to match the additive structure of the lattice with the multiplicative structure of the integers. The definition follows.

Definition 4 *For any $\alpha > 0$, integers $\mathbf{a} = a_1, \ldots, a_m$ and $p \geq 1$, let $\Lambda_\alpha^p[\mathbf{a}]$ be the m dimensional lattice in $\mathcal{R}^{m+1}$ generated by the columns of the matrix*

$$L_\alpha^p[\mathbf{a}] = \begin{bmatrix} (\ln a_1)^{1/p} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & (\ln a_m)^{1/p} \\ \alpha \ln a_1 & \cdots & \alpha \ln a_m. \end{bmatrix}$$

Variants of this lattice have appeared before in the computer science literature. This lattice (with $p = 1$) was first used by Schnorr [69] to heuristically factor integers by reduction to SVP. Adleman [3] also used the same lattice (with $p = 2$) to reduce factoring to SVP under some number theoretic assumptions. A modified version of Adleman's lattice was used by Ajtai to prove the NP-hardness of SVP [5]. As far as we know, our is the first explicit use of this lattice to build dense sphere packings.

We now bound the minimum distance between points in Λ. The bound holds for any l_p norm ($p \geq 1$). Clearly, for any lattice, one can make the minimum distance between lattice points arbitrarily large just multiplying all entries in the basis vectors by the appropriate value. The peculiarity of lattice $\Lambda_\alpha^p[\mathbf{a}]$ is that one can bound the length of the shortest vector from below by a growing function of α, a constant multiplying only the last coordinate of the basis vectors. We prove the following bound.

Lemma 3 *If $a_1, \ldots, a_m$ are relatively prime, then the shortest non-zero vector in $\Lambda_\alpha^p[\mathbf{a}]$ (in the l_p norm) has length at least $(2 \ln \alpha - 1)^{1/p}$.*

Proof: Let L be the matrix defined in Definition 4. We want to prove that for all non-zero integer vectors $\mathbf{z} \in \mathcal{Z}^m$, $\|L\mathbf{z}\|^p \geq 2 \ln \alpha - 1$. We first introduce some notation. Let $R \in \mathcal{R}^m$ be the row vector

$$R = [\ln a_1, \ln a_2, \ldots, \ln a_m]$$

and $D \in \mathcal{R}^{m \times m}$ be the diagonal matrix

$$D = \begin{bmatrix} (\ln a_1)^{1/p} & 0 & \cdots & 0 \\ 0 & (\ln a_2)^{1/p} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & (\ln a_m)^{1/p} \end{bmatrix}.$$

Fix a non-zero integer vector $\mathbf{z} \in \mathcal{Z}^m$ and define the integers

$$\begin{aligned} \hat{g} &= \prod_{i:z_i>0} a_i^{z_i} \\ \check{g} &= \prod_{i:z_i<0} a_i^{-z_i} \\ g &= \hat{g}\check{g} = \prod_{i=1}^{m} z_i^{|a_i|}. \end{aligned}$$

Notice that

$$L = \begin{bmatrix} D \\ \alpha R \end{bmatrix}.$$

and

$$\|L\mathbf{z}\|^p = \|D\mathbf{z}\|^p + \alpha^p (R\mathbf{z})^p .$$

We bound the two terms separately. The first term is at least

$$\begin{aligned} \|D\mathbf{z}\|^p &= \sum_i |z_i|^p \ln a_i \\ &\geq \sum_i |z_i| \ln a_i \\ &= \ln g \end{aligned}$$

because $p \geq 1$ and the z_i's are integers. Bounding the second term is slightly more complex:

$$\begin{aligned} |R\mathbf{z}| &= \left| \sum_i z_i \ln a_i \right| \\ &= |\ln \hat{g} - \ln \check{g}| \\ &= \ln\left(1 + \frac{|\hat{g} - \check{g}|}{\min\{\hat{g}, \check{g}\}}\right). \end{aligned}$$

Now notice that since $\mathbf{z}$ is non-zero, the integers $\hat{g}$ and $\check{g}$ are distinct and therefore $|\hat{g} - \check{g}| \geq 1$. Moreover, $\min\{\hat{g}, \check{g}\} < \sqrt{\hat{g}\check{g}} = \sqrt{g}$, and by monotonicity and concavity of function $\ln(1+x)$,

$$\ln\left(1 + \frac{|\hat{g} - \check{g}|}{\min\{\hat{g}, \check{g}\}}\right) > \ln\left(1 + \frac{1}{\sqrt{g}}\right) > \frac{\ln 2}{\sqrt{g}}.$$

Combining the two bounds one gets

$$\|L\mathbf{z}\|^p = \|D\mathbf{z}\|^p + \alpha^p (R\mathbf{z})^p \geq \ln g + \frac{(\alpha \ln 2)^p}{g^{p/2}}$$

which is a continuous function of g with derivative $g^{-(1+p/2)}(g^{p/2} - (p/2)(\alpha \ln 2)^p)$. The function is minimized when $g = (\alpha \ln 2)^2 (p/2)^{2/p}$ with minimum

$$2 \ln \alpha + 2 \ln \ln 2 + (2/p) \ln(p/2) + (2/p) > 2 \ln \alpha - 1.$$

Notice that for the special case $p = 2$, $2 \ln \ln 2 + (2/p) \ln(p/2) + (2/p) = 2 \ln \ln 2 + 1 > 0$ and the nicer bound $\|L\mathbf{z}\|^p > 2 \ln \alpha$ holds true. □

4.2.2 The sphere

In this section we look for a sphere (with radius smaller than the minimum distance in the lattice) containing many lattice points. Obviously the center of such a sphere cannot be a point in the lattice if one wants the sphere to contain more than a single lattice point. We look at spheres with center

$$\mathbf{s}_\alpha[b] = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \alpha \ln b \end{bmatrix}$$

where b is a positive integer, and show that there is a close relationship between finding lattice vectors close to $\mathbf{s}$ and approximating the integer b as a product of the a_i's.

In the next lemma we show that if b can be approximated by the product of a subset of the $a_i's$, then there are lattice points close to $\mathbf{s}$. A converse of this lemma is presented in Section 4.4.

Lemma 4 *For all reals $\alpha > 0, p \geq 1$, positive integers $\mathbf{a} = a_1, \ldots, a_m$ and boolean*

vector $\mathbf{z} \in \{0,1\}^m$, *if* $g = \prod_i a_i^{z_i} \in [b, b + b/\alpha]$ *then*

$$\|L_\alpha^p[\mathbf{a}]\mathbf{z} - \mathbf{s}_\alpha[b]\|_p \leq (\ln b + 2)^{1/p}.$$

Proof: Let D and R be defined as in the proof of Lemma 3. Notice that since $\mathbf{z}$ is a 0-1 vector,

$$\|D\mathbf{z}\|^p = R\mathbf{z} = \ln g$$

and therefore

$$\begin{aligned} \|L\mathbf{z} - \mathbf{s}\|^p &= \|D\mathbf{z}\|^p + \alpha^p |R\mathbf{z} - \ln b|^p \\ &= \ln g + \alpha^p (\ln g - \ln b)^p \\ &= \ln b + \ln \frac{g}{b} + \left(\alpha \ln \frac{g}{b}\right)^p. \end{aligned}$$

From the assumption $g \in [b, b + b/\alpha]$ and using the inequality $\ln(1+x) \leq x$ one gets

$$\ln \frac{g}{b} \leq \ln\left(1 + \frac{1}{\alpha}\right) < \frac{1}{\alpha}$$

which, substituted in the expression above gives

$$\|L\mathbf{z} - \mathbf{s}\|^p \leq \ln b + \frac{1}{\alpha} + 1 \leq \ln b + 2.$$

□

Let now ϵ be a small positive real constant and set $\alpha = b^{(1-\epsilon)}$. From Lemma 3, the minimum distance between lattice points is at least $\lambda = (2(1-\epsilon)\ln b - 1)^{1/p}$, and there are many lattice points within distance $(\ln b + 2)^{1/p} \approx \lambda 2^{-\frac{1}{p}}$ from $\mathbf{s}$, provided that the interval $[b, b + b^\epsilon]$ contains many numbers expressible as the product of a subset of the a_i's. If $a_1, \ldots, a_m$ is the set of all prime numbers less than some integer N, this is the same as saying that $[b, b + b^\epsilon]$ contains many square-free N-smooth numbers. In the next subsection we show how to find a b such that this is true.

4.2.3 Choosing the center

We defined a family (indexed by an integer b) of lattices Λ and points $\mathbf{s}$ such that there is a lattice vector within distance $\lambda_1(\Lambda)/c$ from $\mathbf{s}$ for every square-free smooth number in the interval $[b, b+b^\epsilon]$. We now show that by an accurate choice of the parameters we can always make sure that $[b, b+b^\epsilon]$ contains many square free smooth numbers. Let m and n be any two integers with $n < m$. Let $p_1, \ldots, p_m$ be the set of the first m (odd) prime numbers and let S be the set of all products of n distinct primes less than or equal to p_m. By the Prime Number Theorem, $p_m = O(m \ln m)$ and $S \subset [1, M]$ for some $M = O(m \ln m)^n$. Notice that $|S| = \binom{m}{n} > \left(\frac{m}{n}\right)^n$. Divide the positive real semi-axis into intervals of the form $[b, b+b']$ with $b' \leq b^\epsilon$. For example, for all integers i, divide $[2^i, 2^{i+1}]$ into $2^{(1-\epsilon)i}$ intervals of size $2^{\epsilon i}$. Notice that the segment $[1, M]$ is divided into

$$\begin{aligned}
\sum_{i=0}^{\lfloor \lg_2 M \rfloor} 2^{(1-\epsilon)i} &= \frac{2^{(1-\epsilon)\lceil \lg_2 M \rceil} - 1}{2^{1-\epsilon} - 1} \\
&< \frac{2M^{(1-\epsilon)} - 1}{2^{1-\epsilon} - 1} \\
&= O(M^{(1-\epsilon)})
\end{aligned}$$

intervals. Therefore, by an averaging argument, there exists an interval $[b, b+b^\epsilon]$ containing at least $\Omega\left(\frac{m^\epsilon}{n \ln^{1-\epsilon} m}\right)^n$ square-free p_m-smooth numbers. If we choose $n = m^\delta$ for some $\delta < \epsilon$, then the number of lattice points close to $\mathbf{s}$ is at least $2^n = 2^{m^\delta}$.

This proves that there always exists a b such that $[b, b+b^\epsilon]$ contains exponentially many square-free p_m-smooth numbers, but still leaves the problem of algorithmically find such a b open. If square-free smooth numbers are distributed uniformly enough, any choice of b is good. Unfortunately, we don't know enough about the distribution of smooth numbers to make such a statement about small intervals $[b, b+b^\epsilon]$ (it can be easily proved that for all b the interval $[b, 2b]$ contains square-free smooth numbers, but not much is known about interval of sub-linear size).

Therefore one needs either to conjecture that smooth numbers are distributed uniformly enough or exploit the smooth number distribution (whatever it is) to bias

the choice of the interval in favor of the intervals containing many smooth numbers. This can be easily accomplished as follows. Select a random subset (of size n) of the primes $p_1, \ldots, p_m$ and select the interval containing their product. It is a simple observation that each interval is picked up with a probability proportional to the number of square-free p_m-smooth numbers contained in it. So, for example, intervals that contains no smooth numbers are never selected. The probability of choosing an interval containing few points is bounded in the next lemma.

Lemma 5 *Let $B_1, \ldots, B_k$ be k (disjoint) intervals containing an average of A points each. If B is chosen by selecting a point at random and letting B be the interval containing that point then for any $\delta > 0$,*

$$\Pr\{\#B < \delta A\} < \delta$$

where $\#B$ denotes the number of points in interval B.

Proof: Let N be the total number of points. Observe that $A = N/k$ and $\Pr\{B_i\} = \#B_i/N$. Therefore,

$$\begin{aligned} \Pr\{\#B < \delta A\} &= \Pr\{\Pr\{B\}N < \delta A\} \\ &= \sum_{\Pr\{B_i\}N < \delta A} \Pr\{B_i\} \\ &\leq \frac{k\delta A}{N} = \delta. \end{aligned}$$

□

We can now prove our sphere packing theorem.

Theorem 3 *For any l_p norm ($p \geq 1$) and positive constants $c < 2^{1/p}$, $\epsilon < \frac{2-c^p}{2}$, there exists a probabilistic polynomial time algorithm that on input 1^n and 1^m outputs a lattice $L \in \mathcal{R}^{m' \times m}$, a vector $\mathbf{s} \in \mathcal{R}^{m'}$ and a real r such that for all m and n sufficiently large with probability exponentially close to 1*

- *the shortest vector in L has length at least cr*

- *there are at least* $\left(\frac{m^\epsilon}{n \ln m}\right)^n$ *vectors* $\mathbf{z} \in \{0,1\}^m$ *with exactly* n *ones such that* $L\mathbf{z}$ *is within distance* r *from* $\mathbf{s}$.

Proof: Let $p_1, \ldots, p_m$ be the first m (odd) primes and let S be the set of all products of n distinct primes less than or equal to p_m. Notice that $|S| = \binom{m}{n}$ and from the prime number theorem $S \subset [1, M]$ where $M = O(m \ln m)^n$. Select $d \in S$ at random and let

$$b = 2^{\lfloor \lg_2 s \rfloor} + 2^{\epsilon \lfloor \lg_2 s \rfloor} \left\lfloor \frac{d - 2^{\lfloor \lg_2 s \rfloor}}{2^{\epsilon \lfloor \lg_2 s \rfloor}} \right\rfloor.$$

This is equivalent to partitioning $[1, M]$ into $O(m \ln m)^{(1-\epsilon)n}$ intervals and select one as described in Lemma 5. It follows that

$$\begin{aligned} \Pr\left\{ |[b, b + b^\epsilon] \cap S| < \left(\frac{m^\epsilon}{n \ln m}\right)^n \right\} &< \left(\frac{m^\epsilon}{n \ln m}\right)^n \frac{O(m \ln m)^{(1-\epsilon)n}}{\binom{m}{n}} \\ &= O\left(\frac{m^\epsilon n (m \ln m)^{1-\epsilon}}{nm \ln m}\right)^n \\ &= \Omega(\ln m)^{-\epsilon n} \end{aligned}$$

Define L, $\mathbf{s}$ and r as follows:

$$\begin{aligned} L &= L^p_{b^{1-\epsilon}}[p_1, \ldots, p_m] \\ \mathbf{s} &= \mathbf{s}_{b^{1-\epsilon}}[b] \\ r &= (\ln b + 2)^{1/p}. \end{aligned}$$

From Lemma 3 the shortest vector in L has length at least $(2(1-\epsilon)\ln b - 1)^{1/p} > cr$ for all sufficiently large n (notice that $\ln b > n$). Finally, applying Lemma 4 to all $\mathbf{z}$ such that $\prod p_i^{z_i} \in [b, b^\epsilon]$ we get that with probability exponentially close to one there are at least $\left(\frac{m^\epsilon}{n \ln m}\right)^n$ vectors $\mathbf{z} \in \{0,1\}^m$ with exactly n ones such that $L\mathbf{z}$ is within distance r from $\mathbf{s}$. □

4.3 Working with Finite Precision

In the previous section we proved our packing theorem assuming a model of computation in which one can store and operate on arbitrarily real numbers using constant space and time. We now show how to achieve the same result using finite precision arithmetic. In particular we define integer lattice L and sphere $B(\mathbf{s}, r)$ satisfying the conditions in Theorem 3.

In the next two lemmas we bound the error incurred by truncating the entries in in L and $\mathbf{s}$ to some rational approximation. More precisely we multiply $L, \mathbf{s}$ and r by a relatively small value and truncate all entries to the closest integer.

Lemma 6 *For all $\delta > 0$ and all integer vectors $\mathbf{z} \in \mathcal{Z}^m$*

$$\|L'\mathbf{z}\| \geq (\delta^{-1} - 1)m\|L\mathbf{z}\|$$

where $L' = \lfloor (m/\delta)L \rceil$ is the matrix obtained multiplying $L = L^p_\alpha[\mathbf{a}]$ by m/δ and truncating each entries to the closest integer.

Proof: By triangular inequality

$$\begin{aligned} \|L'\mathbf{z}\| &= \|(m/\delta)L\mathbf{z} + (L' - (m/\delta)L)\mathbf{z}\| \\ &\geq \|(m/\delta)L\mathbf{z}\| - \|(L' - (m/\delta)L)\mathbf{z}\| \\ &= \delta^{-1}m\|L\mathbf{z}\| - \|(L' - (m/\delta)L)\mathbf{z}\|. \end{aligned}$$

It remains to prove that $\|(L' - (m/\delta)L)\mathbf{z}\| \leq m\|L\mathbf{z}\|$. Notice that all entries in $(L' - (m/\delta)L)$ are less than $1/2$ in absolute value. Therefore

$$\begin{aligned} \|(L' - (m/\delta)L)\mathbf{z}\| &\leq \frac{1}{2}\left(\|\mathbf{z}\|^p + (\sum |z_i|)^p\right)^{1/p} \\ &\leq \frac{1}{2}\left(\|\mathbf{z}\|^p + m^p\|\mathbf{z}\|^p\right)^{1/p} \\ &\leq m\|\mathbf{z}\|. \end{aligned}$$

Furthermore,

$$\begin{aligned} \|L\mathbf{z}\|^p &= \|D\mathbf{z}\|^p + \alpha^p |R\mathbf{z}|^p \\ &\geq \|D\mathbf{z}\|^p \\ &\geq \|\mathbf{z}\|^p \end{aligned}$$

because D is diagonal with all entries greater than 1. This proves that $\|(L' - (m/\delta)L)\mathbf{z}\| \leq m\|L\mathbf{z}\|$ and therefore $\|L'\mathbf{z}\| \geq (\delta^{-1} - 1)m\|L\mathbf{z}\|$. □

Lemma 7 *For all $\delta > 0$ and all integer vectors $\mathbf{z} \in \mathcal{Z}^m$*

$$\|L'\mathbf{z} - \mathbf{s}'\| \leq (\delta^{-1} + 1)m\|L\mathbf{z} - \mathbf{s}\|$$

where $L' = \lfloor (m/\delta)L \rceil$ and $\mathbf{s}' = \lfloor (m/\delta)\mathbf{s} \rceil$ are the matrices obtained multiplying $L = L_\alpha^p[\mathbf{a}]$ and $\mathbf{s} = \mathbf{s}_\alpha[b]$ by m/δ and truncating each entry to the closest integer.

Proof: By triangular inequality

$$\begin{aligned} \|L'\mathbf{z} - \mathbf{s}'\| &= \|((m/\delta)L\mathbf{z} - (m/\delta)\mathbf{s}) + (L' - (m/\delta)L)\mathbf{z} - (\mathbf{s}' - (m/\delta)\mathbf{s})\| \\ &\leq \|((m/\delta)L\mathbf{z} - (m/\delta)\mathbf{s})\| + \|(L' - (m/\delta)L)\mathbf{z} - (\mathbf{s}' - (m/\delta)\mathbf{s})\| \\ &= \delta^{-1}m\|L\mathbf{z} - (m/\delta)\mathbf{s}\| + \|(L' - (m/\delta)L)\mathbf{z} - (\mathbf{s}' - (m/\delta)\mathbf{s})\|. \end{aligned}$$

Notice that all entries in $(L' - (m/\delta)L)$ and $(\mathbf{s}' - (m/\delta)\mathbf{s})$ are less than $1/2$ in absolute value. Therefore

$$\|(L' - (m/\delta)L)\mathbf{z} - (\mathbf{s}' - (m/\delta)\mathbf{s})\|^p \leq (1/2)^p(\|\mathbf{z}\|^p + (\sum |z_i| + 1)^p) < m^p\|\mathbf{z}\|^p.$$

Furthermore,

$$\|L\mathbf{z} - \mathbf{s}\| \geq \|D\mathbf{z}\| \geq \|\mathbf{z}\|$$

because D is diagonal with all entries greater than 1. This proves that

$$\|(L' - (m/\delta)L)\mathbf{z} - (\mathbf{s}' - (m/\delta)\mathbf{s})\| \leq m\|L\mathbf{z} - \mathbf{s}\|$$

and therefore

$$\|L'\mathbf{z} - \mathbf{s}'\| \leq (\delta^{-1} + 1)\|L'\mathbf{z} - \mathbf{s}'\|.$$

□

Using Lemmas 6 and 7 in the proof of Theorem 3 one easily gets the following corollary.

Corollary 3 *For any l_p norm ($p \geq 1$) and positive constants $c < 2^{1/p}$, $\epsilon < \frac{2-c^p}{2}$, there exists a probabilistic polynomial time algorithm that on input 1^n and 1^m outputs a lattice $L \in \mathcal{Z}^{m' \times m}$, a vector $\mathbf{s} \in \mathcal{Z}^{m'}$ and an integer r such that for all m and n sufficiently large with probability exponentially close to 1*

- *the shortest vector in L has length at least cr*
- *there are at least $\left(\frac{m^\epsilon}{n \ln m}\right)$ vectors $\mathbf{z} \in \{0,1\}^m$ with exactly n ones such that $L\mathbf{z}$ is within distance r from $\mathbf{s}$.*

4.4 On the Optimality of Some Choices

In this last section we prove a few more facts about our lattice packing. These results are not directly useful to the rest of this thesis, but might be useful in subsequent developments of this work.

We first give a closed expression for the determinant of lattice $\Lambda^2_\alpha[a_1, \ldots, a_m]$. Then we prove a converse of Lemma 4 for the l_1 norm. Namely, we show that any lattice point sufficiently close to $\mathbf{s}$ corresponds to a Diophantine approximation of the integer b.

Proposition 3 *For any choice of the integers $a_1, \ldots, a_m$, the determinant of lattice $\Lambda^2_\alpha[a_1, \ldots, a_m]$ is*

$$\sqrt{(1 + \alpha^2 \sum \ln a_i) \prod_{i=1}^{m} \ln a_i}.$$

Proof: Compute the Gram matrix $B^T \cdot B$ and evaluate its determinant by induction on m. □

The determinant of a lattice equals the inverse of the density of lattice points in space. Notice that lattice $\Lambda^2_\alpha[\mathbf{a}]$ is not particularly dense. In fact, the expected number of lattice points in a random sphere of radius ρ is much less than what predicted by Theorem 3. This is not surprising, because our lattice packing has a very special geometric structure.

Finally, we present a converse of lemma 4 for the special case of $p = 1$ (similar results might hold in any l_p norm, but assuming $p = 1$ makes the calculations much simpler). A slightly weaker result was first used in [69] to heuristically reduce factoring integers to solving the closest vector problem. In Lemma 4 we showed that if b can be approximated as a product of a subset of the a_i's then there exists a lattice point close to $\mathbf{s}$. We now show that if there are lattice points close to $\mathbf{s}$ (in the l_1 norm) then b can be approximated as a product of the a_i's.

Proposition 4 *For any integer vector* $\mathbf{z}$ *such that* $\|L\mathbf{z} - \mathbf{s}\|_1 < \ln b$, $g = \prod a_i^{x_i}$ *is a Diophantine* b/α*-approximation of* b, *i.e., if* $\hat{g} = \prod_{x_i>0} a_i^{x_i}$ *and* $\check{g} = \prod_{x_i<0} a_i^{x_i}$, *then* $|\hat{g} - \check{g}b| < b/\alpha$.

Proof: Let $g, \hat{g}, \check{g}$ be defined as in the lemma. We want to find the maximum of the function $|\hat{g} - \check{g}b|$ subject to the constraint $\|L\mathbf{z} - \mathbf{s}\|_1 < \ln b$. Notice that

$$\|L\mathbf{z} - \mathbf{s}\|_1 = \ln \hat{g} + \ln \check{g} + \alpha|\ln \hat{g} - \ln \check{g}b|$$

and $|\hat{g} - \check{g}b|$ are symmetric with respect to $\hat{g}$ and $\check{g}b$, i.e., if one replaces $\hat{g}$ by $\check{g}b$ and $\check{g}$ by $\hat{g}/b$ the value of the functions is unchanged. Assume without loss of generality that $\hat{g} \geq \check{g}b$. The problem become to maximize $\hat{g} - \check{g}b$ subject to the constraint

$$(1+\alpha)\ln \hat{g} + (1-\alpha)\ln \check{g} < (1+\alpha)\ln b.$$

For every fixed value $\check{g}$, the function $\hat{g} - \check{g}b$ is maximized subject to the above constraint when $\hat{g} = b\check{g}^{\frac{\alpha-1}{\alpha+1}}$. So, let's compute the (unconstrained) maximum of the function

$$b\check{g}^{\frac{\alpha-1}{\alpha+1}} - \check{g}b$$

This is a continuous function of $\check{g}$ with derivative

$$b\left(\frac{\alpha-1}{\alpha+1}\right)\check{g}^{-\frac{2}{\alpha+1}} - b.$$

The maximum is achieved when $\check{g} = \left(\frac{\alpha-1}{\alpha+1}\right)^{(\alpha+1)/2}$ and equals

$$\left(1-\frac{2}{\alpha+1}\right)^{\frac{\alpha-1}{2}}\frac{2b}{\alpha+1} < \frac{b}{\alpha}$$

for all $\alpha \geq 3$. □

In particular, if $\alpha = b^{1-\epsilon}$ then for every lattice vector within distance $\ln b$ from $\mathbf{s}$, the integer g associated to the vector is a Diophantine b^{ϵ}-approximation of b.

Chapter 5

A Combinatorial Theorem on Low-degree Hyper-graphs

In this chapter we study the following combinatorial problem. Let $Z \subseteq \{0,1\}^m$ be a set of m-dimensional boolean vectors. We want to find an integer linear transformation $C \in \mathcal{Z}^{k \times m}$ (with k as large as possible) such that every boolean vector $\mathbf{x} \in \{0,1\}^k$ can be expressed as $C\mathbf{z}$ for some $\mathbf{z} \in Z$.

In the rest of this chapter U will be some fixed set of size m, and the boolean vectors in Z are identified with the subsets of U in the obvious way. In other words, (U, Z) is regarded as a hyper-graph with nodes U and hyper-edges Z. Notice that for any two vectors $\mathbf{x}, \mathbf{y} \in \{0,1\}^m$, the scalar product $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{m} x_i y_i$ equals the size of the intersection of the corresponding sets. We restrict our attention to matrices C with boolean entries, so that the rows of C can also be identified with subsets of U, and the above problem can be reformulated as follows. We want to find a sequence of sets $C_1, \ldots, C_k$ with the property that for every bit string $x_1 \cdots x_k$ there exists a set $A \in Z$ such that $|C_i \cap A| = x_i$ for all $i = 1, \ldots, k$.

It can be proved that if $|Z| > m^k$, there exists a solution consisting of singleton sets $C_i = \{c_i\}$. This is essentially a combinatorial result proved, independently, by Sauer (1972), Perles and Shelah, and, in a slightly weaker form, by Vapnik and Chervonenkis, which we refer to as *Sauer's Lemma.* The proof of this result is relatively simple, but not constructive: it only asserts that C exists, but it does not give any

effective (even probabilistic) way to find it.

A probabilistic variant of Sauer's combinatorial lemma was first found by Ajtai. In [5], Ajtai shows that if Z is regular (all elements of Z have exactly size n) and $|Z|$ is sufficiently big ($|Z| > n^{cn}$ for some constant c), then by choosing C at random according to a given (easily sample-able) probability distribution, then with high probability all $\mathbf{x} \in \{0,1\}^k$ belongs to $CZ = \{C\mathbf{z}: \mathbf{z} \in Z\}$, where k, m and n are polynomially related. The exact relationship among the parameters k, m, n and c can in principle be deduced from the proof in [5], but the technicality of the proof makes it hard to extract and it is currently not known.

We present an alternative construction with a much simpler analysis. We prove that if Z is n-regular, $|Z| > n!m^{\omega(\sqrt{n}k)}$, and $C \in \{0,1\}^{k\times m}$ is chosen by selecting each entry independently at random with probability $p = o(\frac{1}{nk})$, then $\{0,1\}^k \subset CZ$ with probability $1 - o(1)$. We first prove a weaker result: we show that every vector $\mathbf{x} \in \{0,1\}^k$ belongs to CZ with very high probability. The difference between the weak and strong version of the theorem is in the order of quantification. While the theorem in its strong form asserts that with high probability C is good for all target vectors $\mathbf{x}$, the weak version only says that for any fixed target vector $\mathbf{x}$, matrix C is good with high probability. The weak version of the theorem can be proved by a relatively simple argument based on Chebychev inequality. We then show that the strong version of the theorem easily follows from the weak one.

The rest of the chapter is organized as follows. In Section 5.1 Sauer's combinatorial result is presented and it is explained why it fails to be constructive. Then our probabilistic construction is presented in Section 5.2 where the weak version of our theorem is proved. The strong version of our theorem is proved in the last section using the weak theorem and the ideas from the proof of Sauer's lemma.

5.1 Sauer's Lemma

In this section we present a proof of Sauer's Lemma. This combinatorial result is usually stated in terms of the Vapnik-Chervonenkis dimension (VC-dimension) of a

range space. In order to avoid the introduction of new concepts, we reformulate Sauer's Lemma in terms of the sets $C_1, \ldots, C_k$ and Z. Sauer's result is essentially a solution to our combinatorial problem with the restriction that the C_i must be singleton sets, i.e., sets containing exactly one element.

When the rows of C are singleton sets, the linear operation associated to C is more easily described by the projection onto some set $G \subseteq U$ as follows. For any hyper-graph (U, Z) and for any subset of nodes $G \subseteq U$, define the restriction of Z to G by

$$Z|_G = \{A \cap G : A \in Z\}.$$

Notice that for every set $G \subseteq U$, the following two condition are equivalent:

- $Z|_G = 2^G$,
- $\{0,1\}^G \subseteq CZ$ where $C \in \{0,1\}^{G \times U}$ is the matrix defined by $C_{g,u} = 1$ iff $g = u$.

Lemma 8 (Sauer's Lemma) *Let U be a set of size m and Z be a collection of subsets of U. Let*

$$[m,k] = \sum_{i=0}^{k} \binom{m}{i}$$

be the number of subsets of U of size at most k. For all k, if $|Z| \geq [m,k]$ then there exists a set G of size k such that $Z|_G = 2^G$.

Proof: The proof is by induction on $m + k$. If $m = k = 0$ the assertion is trivially true. Notice that $[m,k] = [m-1,k] + [m-1,k-1]$. Assume that the lemma holds for $m-1, k$ and $m-1, k-1$, and let's prove it for m, k. Let $|U| = m$ and $|Z| \geq [m,k]$. Pick an element a from U and define $U' = U \setminus \{a\}$ and the following two collections of subsets of U':

$$Z_0 = \{A \subseteq U' : A \in Z\}$$

$$Z_1 = \{A \subseteq U' : A \cup \{a\} \in Z\}.$$

Notice that $|U'| = m - 1$ and

$$|Z_0 \cup Z_1| + |Z_0 \cap Z_1| \;=\; |Z_0| + |Z_1|$$

$$
\begin{aligned}
&= |Z| \\
&\geq [m,k] \\
&= [m-1,k]+[m-1,k-1].
\end{aligned}
$$

Therefore, either $|Z_0 \cup Z_1| \geq [m-1,k]$ or $|Z_0 \cap Z_1| \geq [m-1,k-1]$. We deal with the two cases separately:

- if $|Z_0 \cup Z_1| \geq [m-1,k]$, then by inductive hypothesis there exist a set $G \subseteq U' \subset U$ of size $|G| = k$ such that $(Z_0 \cup Z_1)|_G = 2^G$. Since $a \notin G$, $Z|_G = (Z_0 \cup Z_1)|_G = 2^G$.

- if $|Z_0 \cap Z_1| \geq [m-1,k-1]$, by inductive hypothesis, there exists a set $G' \subseteq U' \subset U$ such that $(Z_0 \cap Z_1)|_{G'} = 2^{G'}$. Let $G = G' \cup \{a\}$. We now show that $Z|_G = 2^G$. The inclusion $Z|_G \subseteq 2^G$ is obvious. So, let's prove $2^G \subseteq Z|_G$. Let $A \in 2^G$. Notice that $A \setminus \{a\}$ belongs to both $Z_0|_{G'}$ and $Z_1|_{G'}$. Therefore $A \setminus \{a\} \in Z_G$ and $A \cup \{a\} \in Z_G$. Since A equals either $A \setminus \{a\}$ or $A \cup \{a\}$, $A \in Z_G$.

□

Since $[m,k] < m^k$, one immediately gets the following corollary.

Corollary 4 *Let $Z \subset \{0,1\}^m$ be a collection of boolean vectors. If $|Z| \geq m^k$ then there exists a matrix $C \in \{0,1\}^{k \times m}$ such that $\{0,1\}^k \subset CZ$.*

Observe that the bound in Sauer's Lemma is tight: if Z is the set of all subsets of U of size k or less, $|Z| = [m,k]$ and any set G satisfying the assertion in the lemma has size at most k. The proof of the lemma suggests a possible way to find the set G: select the elements of U one at a time. For each $a \in U$, if there are a lot of subsets A such that both $A \setminus \{a\}$ and $A \cup \{a\}$ belong to Z, then include a in G, otherwise discard it, project Z onto $U \setminus \{a\}$ and go on to the next element. The problem is that the step of deciding whether a given $a \in U$ is good or bad may not be effective. Notice that a single element a might belong to all sets in Z (or none of them), and still $|Z|$ be quite large, and selecting such an element a would be disastrous. We show

in a later section that when Z is very large ($|Z| \approx 2^m$), then G can be chosen at random and a probabilistic analogue of Sauer's Lemma holds. But first one has to get rid of the bad elements. This is accomplished in the proof of the weak version of the theorem.

5.2 Weak Probabilistic Construction

We now present the weak version of our randomized construction. The idea underlying this construction is that if the sets in Z are small, then there cannot be too many elements in U that belong to many $A \in Z$. If the probability that any fixed $a \in U$ belongs to some C_i is sufficiently small, then with high probability none of these bad elements will be selected. So, we assume that the sets in Z have bounded size. In particular we assume the hyper-graph (U, Z) is regular, i.e., all hyper-edges in Z have size n for some n. This is not great loss in generality because if all hyper-edges in Z have size at most n, then Z must contain a regular hyper-graph of size at least $|Z|/n$. We now state our theorem in its weak form.

Theorem 4 *Let (U, Z) be an n-regular hyper-graph with $|U| = m$ and $|Z| > n!m^{\frac{\sqrt{nk}}{\epsilon}}$. Define matrix $C \in \{0,1\}^{k \times m}$ at random by setting each entry to 1 independently with probability $p = \frac{\epsilon}{nk}$. Then, for every $\mathbf{x} \in \{0,1\}^k$,*

$$\Pr\{\exists \mathbf{z} \in Z. C\mathbf{z} = \mathbf{x}\} > 1 - 4\epsilon.$$

The proof of the theorem will take the rest of this section. We outline it here. Consider the target vector $\mathbf{x}$ as fixed. For each hyper-edge $A \in Z$, let X_A be the event $CA = \mathbf{x}$ (or more precisely, $C\mathbf{z} = \mathbf{x}$ where $\mathbf{z} \in \{0,1\}^m$ is the vector associated to A). We want to bound the probability that X_A is false for all $A \in Z$. Since the set Z is very big, the expected number of $A \in Z$ such that X_A is true is also very high. Unfortunately, this is not sufficient to conclude that with high probability there exists an $A \in Z$ such that X_A is true, because the random variables $\{X_A\}_{A \in Z}$ might be strongly correlated. Notice that if A and B are disjoint (i.e., $A \cap B = \emptyset$), then

the corresponding events are independent. However, if $|Z|$ is big many pairs in Z will intersect because there cannot be more than m/n mutually disjoint hyper-edges. However, one can still hope that for most of the pairs $A, B \in Z$, the intersection $A \cap B$ is empty or very small. The proof of the theorem is divided in three major steps:

- We first show that the probability $\Pr\{\neg\exists A \in Z.X_A\}$ can be bounded by the expectation $E[e^{\gamma R}-1]$, where γ is a small positive real, and the random variable R is the size of the intersection of two randomly chosen elements of Z.
- Then, we show that Z "contains" a hyper-graph such that the intersection of two randomly selected hyper-edges is very small with high probability.
- Finally we prove the theorem applying the bound $E[e^{\gamma R}-1]$ to this hyper-graph contained in Z.

Each of the above steps is described in the following subsections.

5.2.1 The exponential bound

We start by computing the probability that X_A is true. In the next lemma we prove a more general statement concerning the probability that two events X_A and X_B are simultaneously satisfied and relate it to the size of the intersection $R = |A \cap B|$ of the two corresponding sets.

Lemma 9 *Let $A, B \subset U$ be two sets of size n and let $C \in \{0,1\}^{k\times m}$ be chosen at random by setting each entry to 1 independently with probability p. Then, the probability $\Pr\{X_A \wedge X_B\}$ equals*

$$\Phi(R) \;=\; (1-p)^{(2n-R)k}\left[\frac{pR}{1-p}+\left(\frac{p(n-R)}{1-p}\right)^2\right]^{|\mathbf{x}|_h}.$$

where $R = |A \cap B|$ and $|\mathbf{x}|_h$ is the Hamming weight of $\mathbf{x}$, i.e., the number of ones in vector $\mathbf{x}$.

Proof: Since the rows of matrix C are chosen independently,

$$\Pr\{X_A \wedge X_B\} = \Pi_{i=1}^{k} \Pr\{|C_i \cap A| = |C_i \cap B| = x_i\}.$$

We prove that for all $i = 1, \ldots, k$,

$$\Pr\{|C_i \cap A| = |C_i \cap B| = x_i\} = (1-p)^{(2n-R)} \left[\frac{pR}{1-p} + \left(\frac{p(n-R)}{1-p} \right)^2 \right]^{x_i}.$$

First consider the case $x_i = 0$:

$$\begin{aligned} \Pr\{|A \cap C_i| = |B \cap C_i| = 0\} &= \Pr\{(A \cup B) \cap C_i = \emptyset\} \\ &= (1-p)^{|A \cup B|} \\ &= (1-p)^{2n-R}. \end{aligned}$$

Now consider the case $x_i = 1$:

$$\begin{aligned} &\Pr\{|A \cap C_i| = |B \cap C_i| = 1\} \\ &= |A \cap B| \cdot p(1-p)^{|A \cup B|-1} + |A \setminus B| \cdot |B \setminus A| \cdot p^2 (1-p)^{|A \cup B|-2} \\ &= p^2 (1-p)^{|A \cup B|-2} \left(\frac{(1-p)R}{p} + (n-R)^2 \right) \\ &= (1-p)^{(2n-R)} \left[\frac{pR}{1-p} + \left(\frac{p(n-R)}{1-p} \right)^2 \right]. \end{aligned}$$

□

By choosing $A = B$ in the previous lemma one gets the following corollary.

Corollary 5 *Let $A \subseteq U$ be a set of size n, and $C \in \{0,1\}^{k \times m}$ be chosen at random by setting each entry to 1 independently with probability p. Then,*

$$\Pr\{X_A\} = \Phi(n) = (1-p)^{nk} \left(\frac{pn}{1-p} \right)^{|\mathbf{x}|_h}.$$

Notice that when $A \cap B = \emptyset$,

$$\Pr\{X_A, X_B\} = \Phi(0) = \Phi(n)^2 = \Pr\{X_A\} \Pr\{X_B\},$$

i.e., the events X_A and X_B are independent. We can now prove the the following proposition.

Proposition 5 *Let $C \in \{0,1\}^{k \times m}$ be chosen at random by setting each entry to 1 independently with probability p. Let Z be a collection of subsets of U containing exactly n ones each. Then, for each $\mathbf{x} \in \{0,1\}^k$ the probability that $C\mathbf{z} \neq \mathbf{x}$ for all $\mathbf{z} \in Z$ is at most $E[e^{\gamma R}] - 1$, where $\gamma = \frac{kp}{1-p} + \frac{k}{pn^2}$ and R is the size of the intersection of two randomly chosen elements of Z.*

Proof: Fix some vector $\mathbf{x} \in \{0,1\}^k$ and choose C at random as specified in the theorem. For all $A \in Z$, let I_A be the indicator random variable

$$I_A = \begin{cases} 1 & \text{if } X_A \text{ is true} \\ 0 & \text{otherwise} \end{cases}$$

Define the random variable $X = \sum_{A \in Z} I_A$. Notice that

$$E[X] = \sum_{A \in Z} \Pr\{X_A\} = |Z|\Phi(n)$$

and

$$E[X^2] = E[(\sum_{A \in Z} I_A)^2] = \sum_{A,B \in Z} \Pr\{X_A, X_B\} = |Z|^2 E_{A,B}[\Phi(|A \cap B|)]$$

where the last expectation is over the choice of $A, B \in Z$. Let $R = |A \cap B|$. X_A is false for all $A \in Z$ iff $X = 0$. Therefore,

$$\begin{aligned} \Pr\{\forall A \in Z. \neg X_A\} &= \Pr\{X = 0\} \\ &\leq \Pr\{|X - E[X]| \geq E[X]\} \end{aligned}$$

which, by Chebychev's inequality, is at most

$$\begin{aligned}\frac{\mathrm{Var}[X]}{E[X]^2} &= \frac{E[X^2]-E[X]^2}{E[X]^2} \\ &= \frac{E[\Phi(R)]}{\Phi(n)^2}-1 \\ &= \frac{E[\Phi(R)]}{\Phi(0)}-1.\end{aligned}$$

Finally, notice that

$$\begin{aligned}\frac{\Phi(R)}{\Phi(0)} &= (1-p)^{-kR}\left[\frac{(1-p)R}{pn^2}+\left(1-\frac{R}{n}\right)^2\right]^{|x|_h} \\ &< \left(1+\frac{p}{1-p}\right)^{kR}\left(\frac{R}{pn^2}+1\right)^k \\ &< e^{\frac{pkR}{1-p}}e^{\frac{kR}{pn^2}} \\ &= e^{\gamma R}\end{aligned}$$

and therefore $\Pr\{X=0\} \le E[e^{\gamma R}]-1$. □

5.2.2 Well spread hyper-graphs

In the previous section we showed that the probability that X_A is false for all $A \in Z$ can be bounded by $E[e^{\gamma R}]-1$. Obviously, the bound is interesting only when $E[e^{\gamma R}] < 2$. Notice that this can be true only if $\Pr\{R=r\} < e^{-\gamma r}$ for all but a single value of r. Therefore the probability $\Pr\{R=r\}$ must decrease exponentially fast in r. This is not necessarily true for any low degree regular hyper-graph Z. In this section we show that if Z is sufficiently large, than Z must "contain" a hyper-graph such that $\Pr\{R=r\} \le 1/r!$.

More precisely we show that Z contains a hyper-graph satisfying the following property:

Definition 5 *Let (U,Z) an n-regular hyper-graph. Z is* well spread *if for all $D \subseteq U$,*

$$|\{A \in Z : D \subseteq A\}| \le \frac{|Z|}{n(n-1)\cdots(n-|D|+1)} = \frac{(n-|D|)!}{n!}|Z|.$$

Well spread hyper-graphs have the important property that the size of the intersection of two randomly selected hyper-edges is small with very high probability, as shown in the next lemma.

Lemma 10 *Let (U, Z) an n-regular well spread hyper-graph. Choose $A, B \in Z$ independently and uniformly at random and let $R = |A \cap B|$. For all $r > 0$,*

$$\Pr\{R \geq r\} < \frac{1}{r!}.$$

Proof: We prove that for any fixed set A of size n, the probability that $|A \cap B| \geq r$ when B is chosen at random from Z is at most $\frac{1}{r!}$. If $|A \cap B| \geq r$ then B contains a subset of A of size r. Therefore, by union bound,

$$\Pr_{B \in Z}\{|A \cap B| \geq r\} \leq \sum_{C \in \binom{A}{r}} \Pr_{B \in Z}\{C \subseteq B\} = \sum_{C \in \binom{A}{r}} \frac{|\{B \in Z : C \subseteq B\}|}{|Z|}.$$

Since Z is well spread, $|\{B \in Z : C \subseteq B\}| \leq \frac{(n-r)!}{n!}|Z|$, which substituted in the previous expression, gives

$$\Pr_{B \in Z}\{|A \cap B| \geq r\} \leq \binom{n}{r}\frac{(n-r)!}{n!} = \frac{1}{r!}.$$

□

We now show how to find well spread hyper-graphs "inside" any sufficiently big regular hyper-graph. For any subset $D \subseteq U$, define the induced hyper-graph

$$Z_D = \{A \subseteq U \setminus D : A \cup D \in Z\}.$$

In other words, Z_D is the set of hyper-edges containing D, with the nodes in D removed. Hyper-graph Z is well spread if for every set D, $|Z_D| \leq \frac{(n-|D|)!}{n!}|Z|$. Notice the following basic facts:

- Z_D is d-regular with $d = n - |D|$.

- If $D = \emptyset$ then $Z_D = Z$.
- If $|D| = n$, then $Z_D = \{D\}$ if $D \in Z$ and $Z_D = \emptyset$ otherwise.
- If $|D| > n$ then $Z_D = \emptyset$.

In the following lemma we prove that for any regular hyper-graph Z, there exists a small set D such that Z_D is well spread.

Lemma 11 *Let $Z \subseteq \binom{U}{n}$ an n-regular hyper-graph. If $|Z| > n!|U|^\delta$ then there exists a set $D \subset U$ of size $|D| < n - \delta$ such that Z_D is a well spread regular hyper-graph of degree $d > \delta$.*

Proof: If Z is well spread, let $D = \emptyset$ and the statement is obviously true. Otherwise, there exists some set D such that $|Z_D| > \frac{(n-|D|)!}{n!}|Z|$. Let D be a maximal (with respect to the set inclusion ordering relation) set with this property. Notice that $Z' = Z_D$ is d-regular, with $d = n - |D|$. We prove that Z' is well spread. Let A be any subset of U. There are three cases:

- if $A \cap D \neq \emptyset$ then $|Z'_A| = 0 < \frac{1}{d!}|Z'|$,
- if $A = \emptyset$, then $|Z'_A| = |Z'| = \frac{d!}{d!}|Z'|$.
- finally assume $A \neq \emptyset$ and $A \cap D = \emptyset$. By the maximality of D one gets

$$\begin{aligned} |Z'_A| &= |Z_{A \cup D}| \\ &\leq \frac{(n - |A \cup D|)}{n!}|Z| \\ &= \frac{(d - |A|)!}{d!}\frac{(n - |D|)!}{n!}|Z| \\ &< \frac{(d - |A|)!}{d!}|Z'|. \end{aligned}$$

It remains to prove the lower bound on d. From $Z' \subseteq \binom{U}{d}$ and $|Z'| \geq \frac{d!|Z|}{n!} > \frac{|Z|}{n!}$ one gets

$$\frac{|Z|}{n!} < |Z'| \leq \binom{U}{d} < |U|^d.$$

If $|Z| > n!|U|^\delta$ then $d > \delta$ and $|D| = n - d < n - \delta$. □

Combining the two lemma above, one immediately obtains the following proposition.

Proposition 6 *Let $Z \subseteq \binom{U}{n}$ be a regular hyper-graph with $|Z| > n!|U|^{\delta}$. Then there exists a set D such that*

- *The size $|D| < n - \delta$.*
- *Z_D is d-regular of degree $d > \delta$.*
- *If A, B are chosen independently at random from Z_D,*

$$\Pr\{|A \cap B| \geq r\} \leq \frac{1}{r!}.$$

5.2.3 Proof of the theorem

We now combine the tools developed in the previous sections to prove Theorem 4. Let (U, Z) be an n-regular hyper-graph with $|U| = m$ and $|Z| \geq n!m^{\delta}$ for some $\delta > \epsilon^{-1}\sqrt{n}k$. From Proposition 6, there exists a subset $D \subset S$ of size $|D| \leq n - \delta$ such that $\Pr\{|A \cap B| \geq r\} < \frac{1}{r!}$ (probability computed over the random choice of $A, B \in Z_D$).

Choose $C \in \{0,1\}^{k \times m}$ at random by setting each entry to one independently with probability $p = \frac{\epsilon}{nk}$. Let F be the event that all entries in C that belongs to the columns corresponding to elements in D are 0. Notice that $\Pr\{\neg F\} \leq |D|kp \leq nkp = \epsilon$. Notice also that

$$\Pr\{\forall \mathbf{z} \in Z. C\mathbf{z} \neq \mathbf{x} | F\} \leq \Pr\{\forall \mathbf{z} \in Z_D. C\mathbf{z} \neq \mathbf{x}\}.$$

Let $d = n - |D| > \delta$ be the degree of Z_D. Applying Proposition 5 to d-regular hyper-graph Z_D, the last expression can be bounded by $E[e^{\gamma R}] - 1$ where

$$\begin{aligned} \gamma &= \frac{kp}{1-p} + \frac{k}{pd^2} \\ &< \frac{\epsilon}{n} + \frac{k^2 n}{\epsilon \delta^2} \end{aligned}$$

$$< \frac{\epsilon}{n} + \epsilon$$

and R is the size of the intersection of two random elements in Z_D.

To bound the expectation $E[e^{\gamma R}]$ we use the following lemma.

Lemma 12 *Let w be a positive real and R be a random variable over the naturals such that $\Pr\{R \geq r\} \leq \frac{1}{r!}$. Then $E[w^R] \leq 1 + (1 - 1/w)(e^w - 1)$.*

Proof: For any integral random variable R

$$\begin{aligned} E[w^R] &= \sum_{r \geq 0} w^r \Pr\{R = r\} \\ &= \sum_{r \geq 0} w^r \left(\Pr\{R \geq r\} - \Pr\{R \geq r+1\}\right) \\ &= 1 + (1 - 1/w) \sum_{r \geq 1} w^r \Pr\{R \geq r\}. \end{aligned}$$

Using the upper bound $\Pr\{R \geq r\} \leq \frac{1}{r!}$ and the power series expansion $e^w = \sum_{r \geq 0} \frac{w^r}{r!}$ one gets

$$\begin{aligned} \sum_{r \geq 1} w^r \Pr\{R \geq r\} &\leq \sum_{r \geq 1} \frac{w^r}{r!} \\ &= e^w - 1. \end{aligned}$$

□

Since $\Pr\{R \geq r\} \leq \frac{1}{r!}$, we can apply the lemma with $w = e^\gamma$ and obtain

$$E[e^{\gamma R}] - 1 \leq (1 - e^{-\gamma})(e^{e^\gamma} - 1).$$

Now notice that $e^{-\gamma} \geq 1 - \gamma$ for all γ, and $e^{e^\gamma} - 1 < e$ for all $\gamma < 1/4$. Therefore

$$\Pr\{\forall \mathbf{z} \in Z.C\mathbf{z} \neq \mathbf{x} | F\} < e\gamma < e(1 + 1/n)\epsilon$$

and for all sufficiently large n

$$\Pr\{\forall \mathbf{z} \in Z.C\mathbf{z} = \mathbf{x}\} \leq \Pr\{\neg F\} + \Pr\{\forall \mathbf{z} \in Z.C\mathbf{z} = \mathbf{x} | F\}$$

$$\begin{aligned} &\leq \epsilon + e\left(\frac{\epsilon}{n} + \epsilon\right) \\ &< 4\epsilon. \end{aligned}$$

5.3 Strong Probabilistic Construction

We proved that for every target vector $\mathbf{x}$, if C is chosen as described in Theorem 4, then with high probability there exists a $\mathbf{z} \in Z$ such that $C\mathbf{z} = \mathbf{x}$. It follows by an averaging argument that with high probability the size of $CZ \cap \{0,1\}^m$ (the set of all boolean vectors that can be represented as $C\mathbf{z}$ for some $\mathbf{z} \in Z$) is almost equal to the size of the whole $\{0,1\}^m$. We now prove a probabilistic analogue of Sauer's Lemma that can be applied when $|Z| \approx 2^m$.

Lemma 13 *Let Z be a subset of $\{0,1\}^m$. Let G be a random subset of $\{1,\ldots,m\}$. Then*

$$\Pr\{Z|_G = \{0,1\}^G\} = \frac{|Z|}{2^m}.$$

Proof: By induction on m. If $m = 0$, then $G = \emptyset$, and $Z|_G = Z = \{0,1\}^G$ iff $|Z| = 1 = |\{0,1\}^m|$ (observe that $\{0,1\}^G = \{0,1\}^0 = \{\varepsilon\}$). Now assume the statement holds for all $Z \subseteq \{0,1\}^m$ and let's prove it for $Z \subseteq \{0,1\}^{m+1}$. Choose G at random and let $G' = G \setminus \{m+1\}$. Notice that G' is a random subset of $\{1,\ldots,m\}$. Define the following sets:

- $Z_0 = \{\mathbf{x} : \mathbf{x}0 \in Z\}$
- $Z_1 = \{\mathbf{x} : \mathbf{x}1 \in Z\}$

Notice that $|Z| = |Z_0| + |Z_1| = |Z_0 \cup Z_1| + |Z_0 \cap Z_1|$. Moreover, $Z|_G = \{0,1\}^G$ iff

- $(m+1) \notin G$ and $(Z_0 \cup Z_1)|_{G'} = 2^{G'}$, or
- $(m+1) \in G$ and $(Z_0 \cap Z_1)|_{G'} = 2^{G'}$.

Using the inductive hypothesis

$$\begin{aligned}
\Pr\{Z|_G = \{0,1\}^G\} &= \Pr\{(m+1) \in G\} \Pr\{(Z_0 \cup Z_1)|_{G'} = 2^{G'}\} \\
&\quad + \Pr\{(m+1) \notin G\} \Pr\{(Z_0 \cap Z_1)|_{G'} = 2^{G'}\} \\
&= \frac{1}{2}\left(\frac{|Z_0 \cup Z_1|}{2^m}\right) + \frac{1}{2}\left(\frac{|Z_0 \cap Z_1|}{2^m}\right) \\
&= \frac{|Z_0 \cup Z_1| + |Z_0 \cap Z_1|}{2^{m+1}} \\
&= \frac{|Z|}{2^{m+1}}.
\end{aligned}$$

□

The strong version of the theorem easily follows from Lemma 13 and Theorem 4.

Theorem 5 *Let (U, Z) be an n-regular hyper-graph with $|U| = m$ and $|Z| > n!m^{\frac{4\sqrt{n}k}{\epsilon}}$. Define matrix $C \in \{0,1\}^{k \times m}$ at random by setting each entry to 1 independently with probability $p = \frac{4\epsilon}{nk}$. Then,*

$$\Pr\{\forall \mathbf{x} \in \{0,1\}^k . \exists \mathbf{z} \in Z . C\mathbf{z} = \mathbf{x}\} > 1 - 5\epsilon.$$

Proof: Define a matrix $C' \in \{0,1\}^{4k \times m}$ at random by setting each entry to 1 independently with probability $p = \frac{4\epsilon}{nk}$, and choose a random subset $G \subseteq 1, \ldots, 4k$ of its rows. Notice that $E[\#G] = 2k$ and $\mathrm{Var}[\#G] = k$ and therefore by Chebychev's inequality

$$\begin{aligned}
\Pr\{\#G < k\} &< \Pr\{|\#G - E[\#G]| < k\} \\
&< \frac{\mathrm{Var}[\#G]}{k^2} \\
&= \frac{1}{k} < \epsilon
\end{aligned}$$

for all sufficiently large k. Therefore, one can assume that $C'|_G$ has at least k rows and contains C as a sub-matrix. We now prove that with probability at least $1 - 4\epsilon$, one has $\{0,1\}^G \subseteq C'Z|_G$. From Theorem 4, for every $\mathbf{x} \in \{0,1\}^k$, $\Pr\{\mathbf{x} \in C'Z\} > 1 - 4\epsilon$.

Using Lemma 13 and the independence of G and C', one gets

$$\begin{aligned}
\Pr\{\{0,1\}^G \subseteq C'Z|_G\} &= E_{C'}[\Pr_G\{\{0,1\}^G \subseteq C'Z|_G\}] \\
&= E_{C'}\left[\frac{|C'Z \cap \{0,1\}^{4k}|}{2^m}\right] \\
&= E_{C'}\left[\frac{1}{2^{4k}}\sum_{\mathbf{x}} I_{\{\mathbf{x}\in C'Z\}}\right] \\
&= \frac{1}{2^{4k}}\sum_{\mathbf{x}\in\{0,1\}^{4k}} E_{C'}[I_{\{\mathbf{x}\in C'Z\}}] \\
&\geq \min_{\mathbf{x}\in\{0,1\}^{4k}} \Pr_{C'}\{\mathbf{x} \in C'Z\} \\
&\geq 1 - 4\epsilon.
\end{aligned}$$

□

Chapter 6

Technical Lemma: The Proof

In this chapter we prove Lemma 1 and its deterministic variant Lemma 2 using the tools developed in the previous chapters. The proof of the probabilistic lemma follows almost immediately from the theorems we proved in Chapters 4 and 5 and is presented first. The proof of the deterministic lemma only uses Lemmas 3, 4 and their approximate versions Lemmas 6, 7 from Chapter 4, but requires slightly more work and is presented next.

6.1 Probabilistic Version

Fix a norm $\|\cdot\|_p$ and a constant $c < 2^{1/p}$ and let 1^k the input to the algorithm. We want to compute a lattice $L \in Z^{m' \times m}$, a vector $\mathbf{s} \in Z^{m'}$, a matrix $C \in Z^{k \times m}$ and an integer r such that

1. for all $\mathbf{z} \in Z^m$, $\|L\mathbf{z}\|_p > cr$.
2. for all boolean vectors $\mathbf{x} \in \{0,1\}^k$ there exists an integer vector $\mathbf{z} \in Z^m$ such that $C\mathbf{z} = \mathbf{x}$ and $\|L\mathbf{z} - \mathbf{s}\|_p < r$.

Let δ a small positive real. We show how to find $L, \mathbf{s}, C$ and r such that the above conditions are satisfied with probability at least $1 - 6\delta$. Let $m = k^{4/\epsilon+1}$ and $n = \sqrt{\frac{m^\epsilon}{e \ln m}}$. Define $L \in \mathcal{Z}^{m' \times m}$, $\mathbf{s} \in \mathcal{Z}^{m'}$ and r as described in Corollary 3 and let Z be the set of all vectors $\mathbf{z} \in \{0,1\}^m$ containing exactly n ones such that $\|L\mathbf{z} - \mathbf{s}\| < r$.

The shortest vector in $\mathcal{L}(L)$ has length at least cr proving property 1. Moreover, with probability arbitrarily close to 1, the size of Z is at least

$$\begin{aligned} |Z| &> \left(\frac{m^{\epsilon}}{n \ln m}\right)^{n} \\ &= n^{n} e^{n} \\ &> n! m^{\left(\frac{4\sqrt{n}k}{\delta}\right)\left(\frac{\delta\sqrt{n}}{4k \ln m}\right)}. \end{aligned}$$

Let $U = \{1, \ldots, m\}$. Notice that

$$\begin{aligned} \frac{\delta\sqrt{n}}{4k \ln m} &= \frac{\delta m^{\epsilon/4}}{4e^{1/4} k \ln^{5/4} m} \\ &= \frac{\delta k^{\epsilon/4}}{4e^{1/4}((4/\epsilon + 1) \ln k)^{5/4}} \\ &> 1 \end{aligned}$$

for all sufficiently large k. Therefore, (U, Z) is an regular hyper-graph with $|Z| > n!|U|^{\frac{4\sqrt{n}k}{\delta}}$. By Theorem 5, $\{0,1\}^k \subseteq CZ$ with probability at least $1 - 5\delta$, proving property 2.

6.2 Deterministic Version

In this section we prove the deterministic version of the technical lemma under Conjecture 1. We remark that although the conjecture is a plausible one, proving it is probably beyond the the possibilities of current mathematical knowledge.

Let c be any real constant less than $2^{1/l}$ and fix two constants $\epsilon < \frac{2-c^l}{2}$ and $\delta < \frac{(2(1-\epsilon))^{1/l} - c}{4}$. From Conjecture 1, there exists an integer d such that for all q large enough there is a $(\log^d q)$-smooth square-free integer in the interval $[q, q + q^{\epsilon/2}]$.

On input 1^k we want to find (in deterministic polynomial time) a lattice $L \in Z^{m' \times m}$, a vector $\mathbf{s} \in Z^{m'}$, a matrix $C \in Z^{k \times m}$ and an integer r such that

- for all $\mathbf{z} \in Z^m$, $\|L\mathbf{z}\|_p > cr$.
- for all boolean vectors $\mathbf{x} \in \{0,1\}^k$ there exists an integer vector $\mathbf{z} \in Z^m$ such

that $C\mathbf{z} = \mathbf{x}$ and $\|L\mathbf{z} - \mathbf{s}\|_p < r$.

Let $b = 2^{\frac{2k^2}{\epsilon}}$, $\alpha = b^{1-\epsilon}$, $m = k + \log^d b$, $p_1, \ldots p_k$ distinct prime numbers of size k and $p_{k+1}, \ldots, p_m$ the first $m-k$ prime numbers. Define $L \in Z^{(m+1)\times m}$, $\mathbf{s} \in Z^{m+1}$ and $C \in \{0,1\}^{k\times m}$ as follows:

$$L = \begin{bmatrix} \lfloor \frac{m(\ln p_1)^{1/l}}{\delta} \rceil & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lfloor \frac{m(\ln p_m)^{1/l}}{\delta} \rceil \\ \lfloor \frac{m\alpha \ln p_1}{\delta} \rceil & \cdots & \lfloor \frac{m\alpha \ln p_m}{\delta} \rceil. \end{bmatrix} \qquad \mathbf{s} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \lfloor \frac{m\alpha \ln b}{\delta} \rceil \end{bmatrix}$$

$$C = [I|0] = \begin{bmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & & \vdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{bmatrix}$$

and let

$$r = \left\lceil (\delta^{-1} + 1)m \left(\ln b + 2\right)^{1/l} \right\rceil.$$

From Lemma 3 and Lemma 6, the shortest non-zero vector in $\mathcal{L}(L)$ has length at least

$$(\delta^{-1} - 1)m \left(2(1-\epsilon)\ln b - 1\right)^{1/l} > cr$$

for all sufficiently large k. We now show that for all $\mathbf{x} \in \{0,1\}^k$ there exists a $\mathbf{z} \in Z^m$ such that $C\mathbf{z} = \mathbf{x}$ and $\|L\mathbf{z} - \mathbf{s}\| < r$. Fix some $\mathbf{x} \in \{0,1\}^k$ and let $g_x = \Pi_{i=1}^k p_i^{x_i}$. Define $q = b/g_x$. Notice that $g_x < 2^{k^2} = b^{\epsilon/2}$ and therefore $q > b^{1-\epsilon/2} > b^{1/2} > 2^k$. From Conjecture 1, for all sufficiently large k the interval $[q, q + q^{\epsilon/2}]$ contains a square-free p_m-smooth integer, i.e., there exists a vector $\mathbf{y} \in \{0,1\}^{m-k}$ such that $g_y = \Pi_{i=1}^{m-k} p_{k+i}^{y_i} = q + \delta$ for some $\delta < q^{\epsilon/2} < b^{\epsilon/2}$. Define the vector $\mathbf{z} = \begin{bmatrix} \mathbf{x} \\ \mathbf{y} \end{bmatrix}$. Let $g = \Pi p_i^{z_i} = g_x g_y$. Notice that

$$g - b = g_x g_y - g_x q$$

$$
\begin{aligned}
&= g_x\left((q+\delta)-q\right) \\
&= g_x\delta \\
&< b^{\epsilon/2}b^{\epsilon/2} = b^{\epsilon}
\end{aligned}
$$

Therefore from Lemma 4 and Lemma 7

$$\|L\mathbf{z}-\mathbf{s}\| < \frac{1+\epsilon}{\epsilon} m\left(\ln b+2\right)^{1/l} < r$$

Chapter 7

Discussion and Open Problems

We proved that the shortest vector problem in any l_p norm is NP-hard to approximate within some constant factor. In particular approximating the shortest vector in l_2 within any factor less than $\sqrt{2}$ is NP-hard. The result holds for both randomized and non-uniform deterministic reductions. We also proved that under a reasonable number theoretic conjecture concerning the distribution of smooth numbers, the shortest vector problem is NP-hard for (deterministic) many-one reductions.

The proof is by reduction from a variant of the approximate closest vector problem (the inhomogeneous version of SVP), and can be regarded as a general method to transform a inhomogeneous problem into an equivalent homogeneous one. The main technical contribution of this thesis is the construction of a gadget used in this homogenization process, that essentially correspond to an instance of CVP satisfying some special properties. Our gadget construction implies the existence of a lattice Λ and a vector $\mathbf{s}$ such that there are (exponentially) many vectors in Λ whose distance from $\mathbf{s}$ is less than the length from the shortest vector in Λ by some constant factor c. Using the homogenizing gadget, we proved that SVP is NP-hard to approximate within this same factor c. We gave an efficient probabilistic construction to build a lattice Λ and a vector $\mathbf{s}$ for any $c < \sqrt{2}$ (in the l_2 norm). We also proved that factors greater than or equal to $\sqrt{2}$ are not achievable. Therefore $\sqrt{2}$ is a natural limit of our proof technique to show that SVP is hard to approximate. Proving the NP-hardness of approximating SVP within any constant factor is left as an open problem.

Open Problem 1 *Is the shortest vector problem NP-hard to approximate within any constant factor?*

Our reduction from CVP to SVP transform instances of CVP in a certain dimension n into instances of SVP in a polynomially related dimension $m = n^c$, where the degree of the polynomial satisfies $c \geq 4$. Therefore, in order to assert that an instance of SVP is hard to solve in practice, m must be rather large. Finding more efficient reduction where $m = O(n)$ is an open problem.

Open Problem 2 *Is there a reduction from CVP to SVP that maps instances of CVP in dimension n to instances of SVP in dimension $O(n)$?*

The homogenizing gadget was constructed using two other results that might be of independent interest. The first is a solution to a sphere packing problem: find a lattice packing of unit spheres such that some bigger n-dimensional ball of radius $r > 1+\sqrt{2}$ contains 2^{n^c} spheres (for some constant $c < 1$ depending only on r). If the lattice requirement is dropped, than it is know that 2^{cn} spheres can be packed. An interesting open problem is if our construction is asymptotically optimal for lattice packings, and if not, find better efficiently computable lattice packings.

Open Problem 3 *For which values of λ and ρ there exists an n-dimensional lattice Λ with minimum distance λ and a sphere $B(\mathbf{s}, \rho)$ containing $2^{\Omega(n)}$ lattice points?*

The second problem we addressed in order to construct the homogenizing gadget is a combinatorial result on hyper-graphs related to the notion of VC-dimension. We gave a new proof of a result originally due to Ajtai, that considerably simplifies the original proof and allows an explicit estimate of the parameters (in Ajtai's result, the parameters are only known to be polynomially related). The value of the parameters in our theorem might already represent an improvement on Ajtai's. We leave it as an open problem if these parameters can be further improved, and if the theorem can be generalized in some interesting way.

Open Problem 4 *Can the parameters in Theorem 5 be improved?*

A last open problem is proving (or disproving) an analogous of our technical lemma for other optimization problems, e.g., the closest codeword problem.

Open Problem 5 *For some $c > 1$, is there a polynomial time algorithm that on input 1^k computes a boolean matrix $L \in \{0,1\}^{m' \times m}$, boolean vector $\mathbf{s} \in \{0,1\}^{m'}$, integer r and boolean matrix $C \in \{0,1\}^{k \times m}$ such that*

- *For all $\mathbf{z} \in \{0,1\}^m$, $\|L\mathbf{z}\|_1 \geq cr$ ($L\mathbf{z}$ computed modulo 2).*
- *For any $\mathbf{x} \in \{0,1\}^k$ there exists a $\mathbf{z} \in \{0,1\}^m$ such that $C\mathbf{z} = \mathbf{x}$ and $\|L\mathbf{z} \oplus \mathbf{s}\|_1 < r$ ($C\mathbf{z}$ and $L\mathbf{z}$ computed modulo 2).*

If such a lemma could be proved, than our same reduction could be used to prove the NP-hardness of the lightest codeword problem, a important open problem in algorithmic coding theory.

Bibliography

[1] *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, Dallas, Texas, 23–26 May 1998.

[2] L. M. Adleman. On breaking the iterated Merkle-Hellman public-key cryptosystem. In Chaum et al. [15], pages 303–308.

[3] L. M. Adleman. Factoring and lattice reduction. Manuscript, 1995.

[4] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 99–108, Philadelphia, Pennsylvania, 22–24 May 1996.

[5] M. Ajtai. The shortest vector problem in L_2 is NP-hard for randomized reductions (extended abstract). In ACM [1], pages 10–19.

[6] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pages 284–293, El Paso, Texas, 4–6 May 1997.

[7] S. Arora, L. Babai, J. Stern, and Z. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. *J. Comput. Syst. Sci.*, 54(2):317–331, Apr. 1997.

[8] L. Babai. On Lovasz' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6, 1986.

[9] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. In *Mathematiche Annalen*, volume 296, pages 625–635. 1993.

[10] M. Bellare, S. Goldwasser, and D. Micciancio. "Pseudo-random" generators within cryptographic applications:the DSS case. In Kaliski Jr. [42], pages 277–291.

[11] E. F. Brickell, J. A. Davis, and G. J. Simmons. A preliminary report on the cryptanalysis of Merkle-Hellman knapsack cryptosystems. In Chaum et al. [15], pages 289–301.

[12] J.-Y. Cai. A relation of primal-dual lattices and the complexity of the shortest lattice vector problem. *Theoretical Computer Science*, 1998. To appear.

[13] J.-Y. Cai and A. P. Nerurkar. Approximating the svp to within a factor $(1 + 1/dim^{-\epsilon})$ is NP-hard under randomized reductions. Manuscript, 1997.

[14] J.-Y. Cai and A. P. Nerurkar. An improved worst-case to average-case connection for lattice problems (extended abstract). In *38th Annual Symposium on Foundations of Computer Science*, pages 468–477, Miami Beach, Florida, 20–22 Oct. 1997. IEEE.

[15] D. Chaum, R. L. Rivest, and A. T. Sherman, editors. *Advances in Cryptology: Proceedings of Crypto 82.* Plenum Press, New York and London, 1983, 23–25 Aug. 1982.

[16] T. J. Chou and G. E. Collins. Algorithms for the solution of systems of linear Diophantine equations. *SIAM J. Comput.*, 11(4):687–708, Nov. 1982.

[17] J. H. Conway and N. J. Sloane. *Sphere Packings, Lattices and Groups.* Springer Verlag, 3rd edition, 1998.

[18] D. Coppersmith. Finding a small root of a bivariate integer equation; factoring with high bits known. In Maurer [60], pages 178–189.

[19] D. Coppersmith. Finding a small root of a univariate modular equation. In Maurer [60], pages 155–165.

[20] M. J. Coster, A. Joux, B. A. LaMacchia, A. M. Odlyzko, C.-P. Schnorr, and J. Stern. Improved low-density subset sum algorithms. *Computational Complexity*, 2(2):111–128, 1992.

[21] R. R. Coveyou and R. D. Macpherson. Fourier analysis of uniform random number generators. *J. ACM*, 14(1):100–119, Jan. 1967.

[22] U. Dieter. How to calculate shortest vectors in a lattice. *Mathematics of Computation*, 29(131):827–833, July 1975.

[23] I. Dinur, G. Kindler, and S. Safra. Approximating cvp to within almost-polynomial factors is NP-hard. In *39th Annual Symposium on Foundations of Computer Science*, Palo Alto, California, 7–10 Nov. 1998. IEEE.

[24] A. M. Frieze. On the Lagarias-Odlyzko algorithm for the subset sum problem. *SIAM J. Comput.*, 15(2):536–539, May 1986.

[25] A. M. Frieze, J. Hastad, R. Kannan, J. C. Lagarias, and A. Shamir. Reconstructing truncated integer variables satisfying linear congruences. *SIAM J. Comput.*, 17(2):262–280, Apr. 1988.

[26] M. A. Frumkin. Polynominal time algorithms in the theory of linear diophantine equations. In M. Karpiński, editor, *Proceedings of the 1977 International Conference on Fundamentals of Computation Theory*, volume 56 of *LNCS*, pages 386–392, Poznań-Kórnik, Poland, Sept. 1977. Springer.

[27] C. F. Gauss. Disquisitiones arithmeticae, (leipzig 1801), art. 171. Yale University Press, 1966. English translation by A.A. Clarke.

[28] E. N. Gilbert. A comparison of signaling alphabets. *AT&T Technical Journal*, 31:504–522, 1952.

[29] O. Goldreich and S. Goldwasser. On the limits of non-approximability of lattice problems. In ACM [1], pages 1–9.

[30] O. Goldreich and S. Goldwasser. On the possibility of basing cryptography on the assumption that $P \neq NP$. Theory of Cryptography Library, 1998.

[31] O. Goldreich, S. Goldwasser, and S. Halevi. Eliminating decryption errors in the Ajtai-Dwork cryptosystem. In Kaliski Jr. [42], pages 105–111.

[32] O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. In Kaliski Jr. [42], pages 112–131.

[33] J. Hastad. Dual vectors and lower bounds for the nearest lattice point problem. *Combinatorica*, 8:75–81, 1988.

[34] J. Hastad. Solving simultaneous modular equations of low degree. *SIAM J. Comput.*, 17(2):336–341, Apr. 1988.

[35] M. Henk. Note on shortest and nearest lattice vectors. *Inf. Process. Lett.*, 61(4):183–188, 28 Feb. 1997.

[36] C. Hermite. Extraits de lettres de m. ch. hermite à m. jacoby sur différents objects de la théorie des nombres, deuxième lettre du 6 août 1845. J. Reine Angew. Math., 1850.

[37] G. Huet. An algorithm to generate the basis of solutions to homogeneous linear diophantine equations. *Inf. Process. Lett.*, 7(3):144–147, Apr. 1978.

[38] C. S. Iliopoulos. Worst-case complexity bounds on algorithms for computing the canonical structure of infinite Abelian groups and solving systems of linear Diophantine equations. *SIAM J. Comput.*, 18(4):670–678, Aug. 1989.

[39] C. S. Iliopoulos. Worst-case complexity bounds on algorithms for computing the canonical structure of finite Abelian groups and the Hermite and Smith normal forms of an integer matrix. *SIAM J. Comput.*, 18(4):658–669, Aug. 1989.

[40] M. Kaib. The Gauss lattice basis reduction algorithm succeeds with any norm. In *Proceedings of the FCT'91*, volume 529 of *Lecture Notes in Computer Science*, pages 275–286. Springer Verlag, 1991.

[41] M. Kaib and C. P. Schnorr. The generalized Gauss reduction algorithm. *Journal of Algorithms*, 21(3):565–578, Nov. 1996.

[42] B. S. Kaliski Jr., editor. *Advances in Cryptology—CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*. Springer-Verlag, 17–21 Aug. 1997.

[43] R. Kannan. Improved algorithms for integer programming and related lattice problems. In *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*, pages 193–206, Boston, Massachusetts, 25–27 Apr. 1983.

[44] R. Kannan. Algorithmic geometry of numbers. *Annual Reviews in Computer Science*, 2:231–267, 1987.

[45] R. Kannan. Minkowski's convex body theorem and integer programming. *Mathematics of operation research*, 12(3):415–440, Aug. 1987.

[46] R. Kannan and A. Bachem. Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. *SIAM J. Comput.*, 8(4):499–507, Nov. 1979.

[47] D. E. Knuth. *The Art of computer programming, Vol. 2 : Seminumerical Algorithms*. Series in Computer Science and Information Processing. Addison-Wesley, Reading, 1969.

[48] A. Korkine and G. Zolotareff. Sur les formes quadratiques. *Math. Annalen*, 6:366–389, 1873.

[49] J. C. Lagarias. Knapsack public key cryptosystems and Diophantine approximation. In D. Chaum, editor, *Advances in Cryptology: Proceedings of Crypto 83*, pages 3–23. Plenum Press, New York and London, 1984, 22–24 Aug. 1983.

[50] J. C. Lagarias. Performance analysis of Shamir's attack on the basic Merkle-Hellman knapsack cryptosystem. In Paredaens [65], pages 312–323.

[51] J. C. Lagarias. The computational complexity of simultaneous Diophantine approximation problems. *SIAM J. Comput.*, 14(1):196–209, Feb. 1985.

[52] J. C. Lagarias, H. W. Lenstra, Jr., and C. P. Schnorr. Korkine-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatorica*, 10:333–348, 1990.

[53] J. C. Lagarias and A. M. Odlyzko. Solving low-density subset sum problems. *J. ACM*, 32(1):229–246, Jan. 1985.

[54] S. Landau and G. L. Miller. Solvability by radicals is in polynomial time. *J. Comput. Syst. Sci.*, 30(2):179–208, Apr. 1985.

[55] A. K. Lenstra. Factoring multivariate integral polynomials. *Theoretical Computer Science*, 34(1–2):207–213, Nov. 1984.

[56] A. K. Lenstra. Factoring multivariate polynomials over finite fields. *J. Comput. Syst. Sci.*, 30(2):235–248, Apr. 1985.

[57] A. K. Lenstra. Factoring multivariate polynomials over algebraic number fields. *SIAM J. Comput.*, 16(3):591–598, June 1987.

[58] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Ann.*, 261:513–534, 1982.

[59] H. W. Lenstra. Integer programming with a fixed number of variables. Technical Report 81-03, University of Amsterdam, Amsterdam, 1981.

[60] U. Maurer, editor. *Advances in Cryptology—EUROCRYPT 96*, volume 1070 of *Lecture Notes in Computer Science*. Springer-Verlag, 12–16 May 1996.

[61] H. Minkowski. Geometrie der zahlen. Leizpig, Tuebner, 1910.

[62] P. Nguyen and J. Stern. Merkle-Hellman revisited: A cryptanalysis of the Qu-Vanstone cryptosystem based on group factorizations. In Kaliski Jr. [42], pages 198–212.

[63] P. Nguyen and J. Stern. A converse to the Ajtai-Dwork security proof and its cryptographic implications. In *Electronic Colloquium on Computational Complexity, technical reports*. 1998.

[64] A. M. Odlyzko and H. te Riele. Disproof of the mertens conjecture. *J. reine angew*, 357:138–160, 1985.

[65] J. Paredaens, editor. *Automata, Languages and Programming, 11th Colloquium*, volume 172 of *Lecture Notes in Computer Science*, Antwerp, Belgium, 16–20 July 1984. Springer-Verlag.

[66] R. A. Rankin. The closest packing of spherical caps in n dimensions. In *Proc. Glasgow Math. Assoc.*, volume 2, pages 139–144. 1955.

[67] B. Rosser. A generalization of the euclidean algorithm to several dimensions. *Duke journal of mathematics*, pages 59–95, 1942.

[68] C. P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53(2–3):201–224, 1987.

[69] C. P. Schnorr. Factoring integers and computing discrete logarithms via Diophantine approximation. In D. W. Davies, editor, *Advances in Cryptology—EUROCRYPT 91*, volume 547 of *Lecture Notes in Computer Science*, pages 281–293. Springer-Verlag, 8–11 Apr. 1991.

[70] C. P. Schnorr. Block reduced lattice bases and successive minima. *Combinatorics, Probability and Computing*, 3:507–522, 1994.

[71] A. Schönhage. Factorization of univariate integer polynomials by Diophantine approximation and an improved basis reduction algorithm. In Paredaens [65], pages 436–447.

[72] A. Schönhage. Fast reduction and composition of binary quadratic forms. In S. Watt, editor, *Proceedings of ISSAC'91*, pages 128–133. ACM, 1991.

[73] J.-P. Seifert. Computing short lattice vectors via close lattice vectors. Manuscript, 1998.

[74] A. Shamir. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. In *23rd Annual Symposium on Foundations of Computer Science*, pages 145–152, Chicago, Illinois, 3–5 Nov. 1982. IEEE.

[75] C. E. Shannon. Probability of error for optimal codes in a Gaussian channel. *AT&T Technical Journal*, 38:611–656, 1959.

[76] B. Vallée. Gauss' algorithm revisited. *Journal of Algorithms*, 12(4):556–572, Dec. 1991.

[77] B. Vallée and P. Flajolet. The lattice reduction algorithm of Gauss: An average case analysis. In *31st Annual Symposium on Foundations of Computer Science*, volume II, pages 830–839, St. Louis, Missouri, 22–24 Oct. 1990. IEEE.

[78] P. van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical Report 81-04, Mathematische Instituut, Universiry of Amsterdam, 1981.

[79] J. von zur Gathen and M. Sieveking. Weitere zum erfüllungsproblem polynomial äquivalente kombinatorische aufgahen. In E. Specker and V. Strassen, editors, *Komplexität von Entscheidungsproblemen: ein Seminar*, volume 43 of *LNCS*, pages 49–71. Springer, 1976.

[80] A. D. Wyner. Capabilities of bounded discrepancy decoding. *AT&T Technical Journal*, 44:1061–1122, 1965.

[81] C. K. Yap. Fast unimodular reduction: Planar integer lattices. In *33rd Annual Symposium on Foundations of Computer Science*, pages 437–446, Pittsburgh, Pennsylvania, 24–27 Oct. 1992. IEEE.