Lecture Notes:

Lattices and Their Application to Cryptography

Stanford University, Spring Quarter, 1998

$\boxed{\boxed{\alpha\text{-Version}}}$

Cynthia Dwork
IBM Almaden Research Center

June 13, 1998

These notes are for the course *Lattices and Their Application to Cryptography*, taught at Stanford during the Spring Quarter, 1998. The material on rounding numbers is taken mostly from Lovász' monograph *An Algorithmic Theory of Numbers, Graphs and Convexity* [Lovász86].

The material on lattice theory follows the notes from Claus Schnorr's Lectures "Gittertheorie und algorithmische Geometrie, Reduktion von Gitterbasen un Polynomidealen", delivered at Johann Wolfgang Goethe University, Frankfurt/Main during the Summer semester of 1994 and the Winter semester of 1994/95, compiled by Roger Fischlin, who has graciously shared with me his LaTeX files. In particular, the Preliminaries and Chapters 2–6 are translations of these notes (with some modifications).

`dwork@almaden.ibm.com`

Cynthia Dwork

Contents

Preface

A lattice is a regular arrangement of points in space. In particular, for linearly independent $b_1, b_2, \ldots, b_n \in \mathbb{R}^n$, the lattice $L = L(b_1, b_2, \ldots, b_n)$ is the set of all integer linear combinations $a_1 b_1 + \cdots + a_n b_n$, $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, of the elments $b_1, b_2, \ldots, b_n$. The vectors $b_1, b_2, \ldots, b_n$ form a *basis* of the lattice. As we will see, there are many different bases for any given lattice. The length of a basis is the length of the longest basis vector.

Prior to 1996, lattices, and in particular, the lattice basis reduction algorithm of Lenstra, Lenstra, and Lovász, were used in cryptography principally to prove cryptographic *in*security [Adel83, Copper, CFJP, H, LaOd85, Shamir82]. We will cover several of these "negative" results; in particular,

1. breaking of knapsack-based cryptosystems

2. breaking the linear congruential pseudo-random generator

3. breaking the supposed semantic security of padded RSA.

Cryptographic constructions necessarily require random choices: if, for example, the choice of a key were deterministic, then the key could not be secret. Thus, the security of the construction relies on the intractability of a *random* instance of the problem on which the construction is based. For example, in the case of the RSA public key cryptosystem, the public key contains a modulus $N = pq$, where p and q are large primes. If an adversary can factor N then the system is insecure. When a user picks a random N, it is not enough that *some* two-prime moduli are hard to factor: the user wants that a *random* instance should be hard to factor. No such result is known; in particular, the relative difficulty of the hardest insances of factoring and random instances of factoring is not known. Indeed, even if factoring were $\mathcal{NP}$-hard (it probably is not), and even if $\mathcal{P}$ were known to be different from $\mathcal{NP}$, this would say nothing about the hardness of random instances of factoring.

It has therefore been a longstanding goal in cryptography to find a "hard" problem for which one can establish an explicit connection between the hardness of random instances and the hardness of the hardest, or worst-case, instances. Such a connection is the contribution of the celebrated paper of Ajtai, "Generating Hard Instances of Lattice Problems" [Ajtai96] (1996). Specifically, the paper presents a random problem involving a certain class of random lattices, whose solution would imply the solution of three famous worst-case problems:

1. Find the length of a shortest nonzero vector in an n-dimensional lattice approximately, up to a polynomial factor.

2. Find the shortest nonzero vector in an n-dimensional lattice L where the shortest vector v is unique in the sense than any other vector whose length is at most $n^c \|v\|$ is parallel to v, where c is a sufficiently large absolute constant.

3. Find a basis $b_1, \ldots, b_n$ in the n-dimensional lattice L whose length, defined as $\max_{i=1}^{n} \|b_i\|$, is the smallest possible up to a polynomial factor.

Motivated by Ajtai's 1996 paper, people began to explore the possibility basing the construction of cryptographic primitives on the assumed hardness of solving the above-mentioned lattice problems. This effort has been fruitful. We cover at least the following "positive" applications of lattices to cryptography:

1. Ajtai's proof shows that that certain cryptographic hash functions enjoy worst-case/average-case equivalence.

2. There exists a public key cryptosystem with worst-case/average-case equivalence.

3. The construction of the cryptosystem yields a natural pseudo-random generator with worst-case/average-case equivalence.

Rough Outline of the Course

We will begin with some classical motivation from the geometry of numbers, based on the material in Chapter 1 of Lovasz' monograph *An Algorithmic Theory of Numbers, Graphs and Convexity* [Lovász86].

We then discuss the fundamentals of lattice theory, and the LLL lattice basis reduction algorithm, following the Roger Fischlin's compilation of the notes from Claus Schnorr's Lectures "Gittertheorie und algorithmische Geometrie, Reduktion von Gitterbasen und Polynomidealen", delivered at Johann Wolfgang Goethe University, Frankfurt/Main during the Summer semester of 1994 and the Winter semester of 1994/95. In particular, I have translated from these notes the following material.

1. Introduction to Lattice Theory: terminology, basic properties of a lattice, length reduction, weight reduction;

2. Successive Minima and Two Theorems of Minkowski

3. Gauss' Basis Reduction Procedure (for 2-dimensional lattices)

4. LLL Lattice Basis Reduction

As mentioned earlier, the LLL lattice basis reduction algorithm is at the heart of several attacks on proposed cryptographic primitives. Following our study of lattice theory, we will cover some of these attacks.

The last part of the course will discuss the positive applications of lattices to cryptography, with the last day reserved for one or two outstanding newer results related to the material of the course.

Preliminaries

Notation

We let $M_{m,n}(S)$ denote the set of all $m \times n$ matrices with entries from the set S. For example, $M_{m,n}(\mathbb{Z})$ is the set of all integer $m \times n$ matrices. We may also use the alternate notation $S^{m \times n}$.

For matrix B we let B^{T} denote the transpose of B. Unless otherwise indicated, elements of $\mathbb{Z}^n$, $\mathbb{R}^n$, *etc.*, denote column vectors.

For real numbers r we let $\lceil r \rfloor := \lceil r - \frac{1}{2} \rceil$ denote the integer closest to r. We write $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$ for the set of positive real numbers.

Scalar Product

A scalar product $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ is a mapping with following properties: For all $u, v, w \in \mathbb{R}^n$ and $\lambda \in \mathbb{R}$:

- $\langle \cdot, \cdot \rangle$ is bilinear:

$$\begin{aligned} \langle u + w, v \rangle &= \langle u, v \rangle + \langle w, v \rangle \\ \langle \lambda u, v \rangle &= \lambda \langle u, v \rangle \\ \langle u, v + w \rangle &= \langle u, v \rangle + \langle u, w \rangle \\ \langle u, \lambda v \rangle &= \lambda \langle u, v \rangle \end{aligned}$$

- $\langle \cdot, \cdot \rangle$ is symmetric:

$$\langle u, v \rangle = \langle v, u \rangle$$

- $\langle \cdot, \cdot \rangle$ is positive definite:

$$\langle u, u \rangle > 0 \qquad \text{for } u \neq 0$$

For $u = 0$ it follows from the linearity in each component that $\langle u, u \rangle = 0$. The ***standard scalar product*** is defined as:

$$\left\langle (u_1, u_2, \dots, u_n)^\mathsf{T}, (v_1, v_2, \dots, v_n)^\mathsf{T} \right\rangle := \sum_{i=1}^{n} u_i v_i$$

Most applications use on the standard scalar product. Every scalar product $\langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ can be written as:

$$\langle u, v \rangle := u^\mathsf{T} S v$$

for some a positive definite matrix $S \in M_{n,n}(\mathbb{R})$. (An $n \times n$ matrix S is positive definite if and only if S is symmetric and $x^\mathsf{T} S x > 0$ for all $x \in \mathbb{R}^n \setminus \{0\}$.) In the case of the standard scalar product the matrix S is the identity matrix.

Norms

A mapping $||\cdot|| : \mathbb{R}^n \to \mathbb{R}$ is called a *norm*, if for all $u, v \in \mathbb{R}^n$ and $\lambda \in \mathbb{R}$:

$$\begin{aligned} ||\lambda v|| &= |\lambda| \cdot ||v|| && \text{(positive homogeneous)} \\ ||u + v|| &\le ||u|| + ||v|| && \text{(triangle inequality)} \\ ||u|| &> 0 \qquad \text{for } u \neq 0 && \text{(positive definiteness)} \end{aligned}$$

The real number $||u||$ is called the *norm* (or *length*) of the vector $u = (u_1, u_2, \dots, u_n)$. For every scalar product we obtain a corresponding Euclidean norm as follows:

$$||u|| := \sqrt{\langle u, u \rangle}$$

The ℓ_1 *norm* is:

$$\left\| (u_1, u_2, \dots, u_n)^\mathsf{T} \right\|_1 := \sum_{i=1}^{n} |u_i|$$

The ℓ_2 *norm* is obtained from the standard scalar product:

$$\left\| (u_1, u_2, \dots, u_n)^\mathsf{T} \right\|_2 := \sqrt{\langle u, u \rangle} = \left(\sum_{i=1}^{n} u_i^2 \right)^{\frac{1}{2}}$$

In general, the ℓ_p *Norm* is:

$$\left\| (u_1, u_2, \dots, u_n)^\mathsf{T} \right\|_p := \left(\sum_{i=1}^{n} |u_i|^p \right)^{\frac{1}{p}}$$

The *sup norm*, *maximum norm* or ℓ_∞ *norm* is:

$$\left\| (u_1, u_2, \dots, u_n)^\mathsf{T} \right\|_\infty := \max_{i=1,2,\dots,n} |u_i|$$

Inequalities

For the sup-, ℓ_1- and ℓ_2-norm, of a vector $u \in \mathbb{R}^n$ we have:

$$\begin{aligned} ||u||_2 &\leq ||u||_1 \leq \sqrt{n} \cdot ||u||_2 \\ ||u||_\infty &\leq ||u||_2 \leq \sqrt{n} \cdot ||u||_\infty \\ ||u||_\infty &\leq ||u||_1 \leq n \cdot ||u||_\infty \end{aligned}$$

Every scalar product and corresponding norm $||u|| := \sqrt{\langle u, u \rangle}$ satisfy the *Cauchy-Schwarz Inequality* (for $u, v \in \mathbb{R}^n$):

$$|\langle u, v \rangle| \leq ||u|| \cdot ||v||$$

Equality holds only when the two vectors are linearly independent.

Let $b_1, b_2, \dots, b_n \in \mathbb{R}^n$ be the column vectors (or row vectors) of the matrix $B \in M_{n,n}(\mathbb{R})$. *Hadamard's Inequality* says:

$$|\det B| \leq \prod_{i=1}^{n} ||b_i||_2$$

Equality holds when the vectors $b_1, b_2, \dots, b_n$ are orthogonal.

Chapter 1

On Rounding Numbers

The material here follows Sections 1.0 and 1.1 of [Lovász86] and Chapter 5 of [GLLS88]. We discuss two natural hardware-independent models of numbers and a set of problems involving the rounding, or approximation, of rationals.

1.1 Lengths of Rationals

We define the binary encoding length of finite objects as follows:

- $\ell(0) := 1$
- $\ell(n) := 1 + \lceil \log_2(|n| + 1) \rceil$ for $n \in \mathbb{Z}$
- $\ell\left(\frac{p}{q}\right) := \ell(p) + \ell(q)$ where $p, q \in \mathbb{Z}$, $q \neq 0$, and $\gcd(p, q) = 1$
- $\ell(A) = \sum_{i,j} \ell(a_{ij})$ for $A = [a_{ij}] \in M_{m,n}(\mathbb{Q})$

Lemma 1.1.1

1. For every rational number r, $1 + |r| \leq 2^{\ell(r)-1}$

2. For every vector $x \in \mathbb{Q}^n$, $1 + ||x|| \leq 1 + ||x||_1 \leq 2^{\ell(x)-n}$

3. For every matrix $D \in \mathbb{Q}^{n \times n}$, $|\det D| \leq 2^{\ell(D)-n^2} - 1$

Proof. 1. follows directly from the definition. To prove 2., let $x = (x_1, x_2, \dots, x_n)^\mathsf{T}$. Since for all $u \in \mathbb{R}^n$ we have $||u||_2 \leq ||u||_1$, in particular $||x||_2 \leq ||x||_1$. Then from 1. we have:

$$1 + ||x||_1 = 1 + \sum_{i=1}^{n} |x_i| \leq \prod_{i=1}^{n} (1 + |x_i|) \leq \prod_{i=1}^{n} 2^{\ell(x_i)-1} = 2^{\ell(x)-n}.$$

Let $d_1, d_2, \dots, d_n$ be the rows of D. By Hadamard's Inequality and 2. we have:

$$1 + |\det D| \leq 1 + \prod_{i=1}^{n} \|d_i\|_2 \leq \prod_{i=1}^{n} (1 + \|d_i\|_2) \leq \prod_{i=1}^{n} 2^{\ell(d_i)-n} = 2^{\ell(D)-n^2}$$

■

In contrast to the binary encoding, we could use the *arithmetic* encoding, in which each integer contributes one to the length of the input. The binary encoding allows the inputs to "appear" longer than they do in the arithmetic encoding, making algorithms appear to run faster (as a function of the input length). For example, the Euclidean algorithm for computing the greatest common divisor of two integers runs in time polynomial in the binary encoding length, but not in the arithmetic encoding length (that is, it does not run in time polynomial in 2). Conversely, in the arithmetic encoding the lengths of the arguments do not grow during execution of the algorithm. For example, n repeated squarings of an n bit number only requires n arithmetic operations but the length of the argument grows exponentially. An algorithm is ***strongly polynomial*** if it takes polynomial time in the arithmetic sense while the length of the binary encoding remains polynomial. Every strongly polynomial algorithm is polynomial.

1.2 Diophantine Approximation and Related Problems

In computations involving real numbers we replace the numbers by rational approximations. For example, if we fix an integer q then the best choice of p such that $\frac{p}{q}$ approximates α is $p = \lfloor \alpha q \rfloor$ or $p = \lceil \alpha q \rceil$. The resulting error is bounded by

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{2q}$$

Suppose we allow the denominator q to vary, subject to the constraint $q \leq Q$. We have:

Proposition 1.2.1 (Dirichelet)
For all $\alpha \in \mathbb{R}$ and integer $Q \geq 1$, there exist $p, q \in \mathbb{Z}$, $0 < q \leq Q$, such that

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{Qq}$$

The fraction $\frac{p}{q}$ whose existence is guaranteed by the theorem, can be found by the *continued fraction expansion* of α, which can be computed in polynomial time. We first give a pigeon hole proof.

Proof. Consider the circle with circumference 1. Starting from a point a_0 on the circle, move clockwise distances $\alpha, 2\alpha, \dots, Q\alpha$ on the circle to get additional points $a_1, a_2, \dots, a_Q$. (Note that we may "wrap" several times around the circle during this process.) Since we have $Q+1$ points, two of these, say, a_i and a_j, where $i < j$, have distance $d \leq \frac{1}{Q+1}$, as measured on the circle. So

$p = j\alpha - i\alpha \pm d$ is an integer. Then for $q = j - i$ we have $|q\alpha - p| = d \leq \frac{1}{Q+1} < \frac{1}{Q}$ and $q \leq Q$. ■

An expression of the form

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{\ddots + \cfrac{1}{x_{k-1} + \cfrac{1}{x_k}}}}$$

where $x_0, \dots, x_k \in \mathbb{Z}$ are all positive except, possibly, x_0, is a *finite continued fraction*, and may be denoted $\langle x_0, \dots, x_k \rangle$.

We may write:

$$\alpha = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \dots}}$$

where $x_0 = \lfloor \alpha \rfloor$ and $x_1, x_2, \dots$ are positive integers dfined by the recurrence:

$$\begin{aligned} \alpha_0 &= \alpha \\ x_0 &= \lfloor \alpha \rfloor \\ \alpha_{k+1} &= \frac{1}{\alpha_k - x_k} \\ x_{k+1} &= \lfloor \alpha_{k+1} \rfloor \end{aligned}$$

(The α_i's are reals, the x_i's are integers.) The sequence stops if and when $x_i = \alpha_i$; the expansion is infinite when α is irrational.

To see that the x_i, $i > 0$, are positive:

$$\begin{aligned} x_i &= \lfloor \alpha_i \rfloor \leq \alpha_i < x_i + 1 \\ \Rightarrow 0 &\leq \alpha_i - x_i < 1 \\ \Rightarrow 1 &< \frac{1}{\alpha_i - x_i} = \alpha_{i+1} \\ \Rightarrow 1 &\leq \lfloor \alpha_{i+1} \rfloor = x_{i=1} \end{aligned}$$

By induction on i, $\alpha = \langle x_0, x_1, x_2, \dots, x_{i-1}, \alpha_i \rangle$, so if the procedure terminates after i steps (that is, if $\alpha_i = x_i$), then $\alpha = \langle x_0, x_1, x_2, \dots, x_i, \rangle$.

Conversely, suppose $\alpha = \frac{p}{q}$, where $(p, q) = 1$. Then $\alpha_1, \alpha_2, \dots$ are all rationals. For $i = 0, 1, \dots,$ let p_i, q_i be defined by $\alpha_i = \frac{p_i}{q_i}$. Assume inductively that $(p_i, q_i) = 1$ (by assumption this is true for $i = 0$). For $i > 0$ we have already seen that $x_i = \lfloor \alpha_i \rfloor \neq 0$. If $x_0 = 0$ then $\alpha_1 = 1/(\alpha_0 - x_0) = 1/\alpha_0$, and we have $\lfloor \alpha_1 \rfloor \neq 0$. If $\lfloor \alpha_i \rfloor \neq 0$, then

$$x_i = \left\lfloor \frac{p_i}{q_i} \right\rfloor = \left\lfloor \frac{kq_i + r_i}{q_i} \right\rfloor$$

where $k > 0$ is an integer and $(r_i, q_i) = 1$. Then by definition

$$\alpha_{i+1} = \frac{1}{\alpha_i - x_i} = \frac{q_i}{r_i} = \frac{p_{i+1}}{q_{i+1}}$$

Thus, $p_i + q_i > p_{i+1} + q_{i+1} > 0$, so eventually the procedure terminates.

To see how quickly it terminates, define two auxiliary sequences, g_k and h_k, as follows.

- $g_{-2} = 0$, $g_{-1} = 1$, $h_{-2} = 1$, $h_{-1} = 0$
- $g_i = x_i g_{i-1} + g_{i-2}$, for $i = 0, 1, \ldots$
- $h_i = x_i h_{i-1} + h_{i-2}$, for $i = 0, 1, \ldots$

Note that $1 = h_0 \leq h_1 < h_2 < \ldots$ and $h_k \geq F_k$, the kth Fibonacci number.

The *kth convergent* is defined to be the rational number

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{\ddots + \cfrac{1}{x_{k-1} + \cfrac{1}{x_k}}}}$$

Lemma 1.2.2

1. The kth convergent is $\frac{g_k}{h_k}$.

2. $g_{k+1}h_k - g_k h_{k+1} = (-1)^k$

The proof is by induction on k. Note that the second assertion implies that g_k and h_k are relatively prime.

$\frac{g_k}{h_k}$ converges to α as $k \to \infty$. Moreover,

$$\left|\alpha - \frac{g_k}{h_k}\right| \leq \frac{1}{h_k h_{k+1}}$$

where since $h_k \geq F_k$ the convergence to α goes exponentially fast. If we let $k = \max\{h_k \mid h_k \leq Q\}$ then $h_{k+1} > Q$ and so

$$\left|\alpha - \frac{g_k}{h_k}\right| < \frac{1}{Qh_k}$$

which satisfies the promise of Dirichelet's theorem.

Let $\frac{g_k}{h_k}$ be the last convergent of α with $h_k \leq Q$. Let j be the maximum $j \geq 0$ such that $h_{k+1} + jh_k \leq Q$. It is not hard to show (see [Khin35], [Lovász86]) that the solution to the following Best Approximation Problem is either $\frac{g_k}{h_k}$ or $\frac{g_{k-1}+jg_k}{h_{k-1}+jh_k}$.

Definition 1.2.3 (Best Approximation Problem)

- *Given:* $\alpha \in \mathbb{Q}$ *and integer* $Q > 0$
- *Find: rational* p/q *such that* $0 < q \leq Q$ *and* $\left|\alpha - \frac{p}{q}\right|$ *is as small as possible.*

The problem is sometimes given in an equivalent but "reverse" form:

Definition 1.2.4 (Reverse Form of Best Approximation)

- *Given:* $\alpha, \varepsilon \in \mathbb{Q}$, $\varepsilon > 0$
- *Find integers* p, q *such that* $q > 0$, $\left|\alpha - \frac{p}{q}\right| < \varepsilon$, *and* q *is as small as possible.*

To prove equivalence, we will prove that both forms are equivalent to the following General Form:

Definition 1.2.5 (General Form of Best Approximation Problem)

- *Given:* $\alpha, \varepsilon \in \mathbb{Q}$, $\varepsilon > 0$, $Q \in \mathbb{Z}, Q > 0$
- *Decide if there exist* $p, q \in \mathbb{Z}$ *such that* $0 < q \leq Q$ *and* $\left|\alpha - \frac{p}{q}\right| < \varepsilon$, *and find* p *and* q *if they exist.*

Given an instance of the General Form we can take the solution p, q to the corresponding Best Approximation Problem (original version), and simply check if $\left|\alpha - \frac{p}{q}\right| < \varepsilon$. Thus, an algorithm for the Best Approximation Problem yields an algorithm for the General Form. Conversely, given an algorithm for the General Form of the Best Approximation problem we can solve the original form by binary search on the interval $(0, 1)$ to find the minimum ε for which there exists a solution, and so we can find the best approximation to α with denominator at most Q.

Similarly, given an instance of the General Form we can take the solution p, q to the corresponding Reverse Form and check whether $q < Q$. Conversely, given an algorithm for the General Form of the Best Approximation problem we can solve the reverse form as follows. Given an instance α, ϵ of the Reverse Form, we find by repeated doubling the least Q that is a power of 2, such that the instance α, ϵ, Q of the General Form has a solution. Then $Q = 2^i$ for some integer i. Assuming $i \neq 0$, perform binary search on the interval $(2^{i-1}, 2^i]$ to find the least Q (and hence, q) for which the General Form has a solution.

Now suppose we wish to round several numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$ in such a way that "simple relations" among numbers are not lost. Suppose, for example that $Q = 100$ and $\alpha_1 = 0.1422$, $\alpha_2 = 0.2213$, and $\alpha_3 = 0.6365$. To approximate the α_i individually with denominators at most Q we get:

- $\alpha_1 \approx \frac{1}{7} = 0.1428\ldots$
- $\alpha_2 \approx \frac{2}{9} = 0.2222\ldots$

- $\alpha_3 \approx \frac{7}{11} = 0.6363\ldots$

While $\alpha_1+\alpha_2+\alpha_3 = 1$, this is not true of the sum of the respective approximations. The trick will be to find a rounding procedure resulting in approximations $\frac{p_1}{q}, \frac{p_2}{q}, \ldots, \frac{p_n}{q}$ with a single common denominator, q.

Definition 1.2.6 (Simultaneous Diophantine Approximation Problem)

- *Given* $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Q}$, $\varepsilon > 0 \in \mathbb{Q}$, *and* $Q \in \mathbb{Z}$, $Q > 0$, *find integers* $p_1, p_2, \ldots, p_n$ *and* q *such that* $0 < q \leq Q$ *and*

$$\left|\alpha_i - \frac{p_i}{q}\right| \leq \frac{\varepsilon}{q} \qquad i = 1, 2, \ldots, n$$

Dirichelet's theorem, extended to the general case, asserts that there is a solution to the Simultaneous Diophantine Approximation problem if $Q \geq \varepsilon^{-n}$, but no efficient algorithm is known for the problem. Eventually we will view this as a problem involving lattices; we will see that the Lenstra, Lenstra, and L. Lovász' (LLL) lattice basis reduction algorithm provides an efficient solution whenever $Q \geq 2^{n^2}\varepsilon^{-n}$.

Definition 1.2.7 (Small Integer Combination Problem)

- *Given:* $\alpha_0, \alpha_1, \ldots, \alpha_n, \varepsilon \in \mathbb{Q}$ *and integer* $Q > 0$, *find integers* $q_0, q_1, q_2, \ldots, q_n$, *not all* 0, *such that*

$$\left|\sum_{i=0}^{n} q_i \alpha_i\right| \leq \varepsilon$$

and $q_i \leq Q$, $i = 1, \ldots, n$.

Note that there is no upper bound on q_0. An analogue of Dirichelet's theorem asserts the existence of a solution provided $Q \geq \varepsilon^{-1/n}$. The LLL algorithm solves the problem efficiently provided $Q \geq 2^n\varepsilon^{-1/n}$.

Finally, we mention the problem of *inhomogeneous diophantine approximation.*

Definition 1.2.8 (Inhomogeneous Diophantine Approximation)

- *Given:* $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_n$, $\varepsilon, Q > 0$
- *Find integers* $p_1, p_2, \ldots, p_n, q$ *such that*

$$|\alpha_i - p_i - \beta_i| \leq \varepsilon$$

and $0 < q \leq Q$.

The inhomogeneous problem may not have a solution. For example, if α_1 is an integer multiple of $\frac{1}{2}$, and $\beta_1 = \frac{1}{3}$, then $q\alpha_1$ and p_1 are both multiples of $\frac{1}{2}$, and therefore so is their difference.

Thus

$$|(q\alpha_1 - p_1) - \beta_1| \geq \frac{1}{6}$$

for any choice of p_1 and q.

Kronenecker gave a general condition for the solvability of this problem (see [Cassels71]):

Proposition 1.2.9
For any $2n$ real numbers $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_n$, either

1. *For each $\varepsilon > 0$ there exist integers $p_1, p_2, \ldots, p_n, q$ such that $q > 0$ and*

$$|q\alpha_i - p_i - \beta_i| \leq \varepsilon.$$

2. *There exist integers $u_1, u_2, \ldots, u_n$ such that $\sum_{i=1} nu_i\alpha_i$ is an integer while $\sum_{i=1} nu_i\beta_i$ is not.*

We will return to this problem, and in particular the special case in which the α_i and β_i are rationals, after we see the LLL lattice basis reduction algorithm.

Chapter 2

Complexity, $\mathcal{NP}$-Completeness

We review the basic concepts of complexity theory relating to lattice theory, especially $\mathcal{NP}$-completeness.

2.1 $\mathcal{NP}$-Completeness

Recall that we have defined the length of the binary encoding length of finite objects as follows:

- $\ell(0) := 1$
- $\ell(n) := 1 + \lceil \log_2(|n| + 1) \rceil$ for $n \in \mathbb{Z}$
- $\ell\left(\frac{p}{q}\right) := \ell(p) + \ell(q)$ where $p, q \in \mathbb{Z}$, $q \neq 0$, and $\gcd(p, q) = 1$
- $\ell(A) = \sum_{i,j} \ell(a_{ij})$ for $A = [a_{ij}] \in M_{m,n}(\mathbb{Q})$

We define the running time of an algorithm as a function of the lengths of the inputs. We are interested in polynomial time:

Definition 2.1.1 (Polynomial Time)
An algorithm runs in polynomial time if the number of steps (Turing machine or number of bit operations) is polynomially bounded in the length of the inputs:

$$\textit{Number of Steps(Inputs)} = \operatorname{poly}(\ell(\textit{Inputs}))$$

In theoretical computer science polynomial time algorithms are sometimes referred to as *efficient.*

Definition 2.1.2 (Characteristic Function)
For a set $A \subseteq \{0,1\}^*$ the characteristic function $\chi_A : \{0,1\}^* \to \{0,1\}$ is defined as: $\chi_A(a) = 1$ if and only if $a \in A$.

Using characteristic functions, we define the class of polynomial time lanuages:

Definition 2.1.3 (Class $\mathcal{P}$ of Polynomial Time Languages)
The class $\mathcal{P}$ of polynomial time languages is the set of languages $A \subseteq \{0,1\}^*$ for which the characteristic function χ_A is polynomial time computable.

The class $\mathcal{NP}$ contains the languages for which, for each word in the language there is a short, efficiently verifiable proof of membership in the language.

Definition 2.1.4 (Class $\mathcal{NP}$)
The class $\mathcal{NP}$ of nondeterministic polynomial time languages $A \subseteq \{0,1\}^*$ is defined as:

$$A \in \mathcal{NP} \iff \begin{array}{l} \exists B \in \{0,1\}^* \times \{0,1\}^*, B \in \mathcal{P} : \\ A = \{x \in \{0,1\}^* \mid \exists y \in \{0,1\}^{\text{poly}(\ell(x))} \textit{ with } (x,y) \in B\} \end{array}$$

Let $(x,y) \in B$. Then y is called a witness for $x \in A$.

Cook's thesis is that $\mathcal{P} \neq \mathcal{NP}$, that is, there exists a language in $\mathcal{NP}$ that is not recognizable in deterministic polynomial time.

Definition 2.1.5 (Karp Reduction)
Let $A, B \subseteq \{0,1\}^*$:

$$A \leq_{pol} B \iff \begin{array}{l} \exists \textit{ polynomial time transformation } h \textit{ with:} \\ \forall x \in \{0,1\}^* : x \in A \Leftrightarrow h(x) \in B \end{array}$$

If $A \leq_{\text{pol}} B$ and $B \leq_{\text{pol}} C$ then $A \leq_{\text{pol}} C$. $A \leq_{\text{pol}} B$ then it is possible in polynomial time to decide if $x \in A$ with a single query to an oracle for B.

A more general type of polynomial time reduction (a *Cook* reduction), allows multiple calls to the oracle for B, provided that the total computation time, including the setting up of the calls to the oracle (each oracle call itself has unit cost) and any subsequent analysis, is polynomially bounded.

We will also be interested in *randomized* reductions, in which there is a probabilistic polynomial time machine M that, using an oracle for B, can decide membership in A.

Definition 2.1.6 ($\mathcal{NP}$-Complete)
$A \subseteq \{0,1\}^*$ is said to be $\mathcal{NP}$-complete, if:

1. $A \in \mathcal{NP}$
2. $\forall B \in \mathcal{NP} : B \leq_{pol} A$

If there is a polynomial time algorithm for any $\mathcal{NP}$-complete problem, then $\mathcal{P} = \mathcal{NP}$. This would contradict Cook's Thesis. Hence, the $\mathcal{NP}$-complete problems are the hardest problems in $\mathcal{NP}$.

2.2 Hard Algorithmic Lattice Problems

In this section we mention problems related to lattice theory that are either $\mathcal{NP}$-complete or for which no efficient algorithm is known. One such problem is integer linear programming (Integer Programming):

Definition 2.2.1 (Integer Linear Programming)
The problem of integer, linear programming is:

- *Given:* $m, n \in \mathbb{N}$, $A \in M_{m,n}(\mathbb{Z})$ *and* $b \in \mathbb{Z}^m$
- *Find* $x \in \mathbb{Z}^n$ *with* $Ax \leq b$ *or show that no such vector exists.*

Integer linerar programming is "hard". We show in Proposition 2.2.5 that the corresponding decision problem is $\mathcal{NP}$-complete:

Definition 2.2.2 (Decision Problem for Integer Linear Programming)
The decision problem for integer linear programming is:

- *Given:* $m, n \in \mathbb{N}$, $A \in M_{m,n}(\mathbb{Z})$ *and* $b \in \mathbb{Z}^m$
- *Decide if there exists* $x \in \mathbb{Z}^n$ *with* $Ax \leq b$.

If $\mathcal{P} \neq \mathcal{NP}$, then no polynomial time algorithm solves this problem. In contrast, there is a polynomial time algorithm for the analogous problem of rational linear programming:

Definition 2.2.3 (Rational Linear Programming)
The problem of rational linear programming is:

- *Given:* $m, n \in \mathbb{N}$, $A \in M_{m,n}(\mathbb{Z})$ *and* $b \in \mathbb{Q}^m$
- *Find* $x \in \mathbb{Q}^n$ *with* $Ax \leq b$ *or show that no such vector exists.*

The first polynomial time algorithm for rational linear programming is the ellipsoid method of L.G. Khachiyan [Khach79, Khach80]. This method is, however, impractical. A provably polynomial time algorithm that also appears to be practical was developed by M. Karmarkar [Karma84], whose starting point was the classical interior point method. Another polynomial time algorithm is due to Y. Ye [Ye91]. A simple, practical procedure is the simplex algorithm [Dantzig63, Schrijver86] of G.B. Dantzig, which has exponential running time in the worst case. The following problem can be solved in polynomial time:

Proposition 2.2.4 (Sieveking 1976)
Given $m, n \in \mathbb{N}$, $A \in M_{m,n}(\mathbb{Z})$ *and* $b \in \mathbb{Z}^m$, *in polynomial time one can:*

a) Solve $Ax = b$, $x \in \mathbb{Z}^n$ or show that no solution exists.

b) Find a $\mathbb{Z}$-Basis $b_1, b_2, \ldots, b_k$ for $\{x \in \mathbb{Z}^n \mid Ax = 0\}$, the $\mathbb{Z}$-kernel. A $\mathbb{Z}$-Basis is a set of linearly independent vectors $b_1, b_2, \ldots, b_k$, where:

$$\{x \in \mathbb{Z}^n \mid Ax = 0\} = \left\{ \sum_{i=1}^{k} t_i b_i \;\middle|\; t_1, t_2, \ldots, t_k \in \mathbb{Z} \right\}$$

Proof. Modification of Gaussian elimination (M. Sieveking in [SpStr76]). Alternate proof in [KaBa79]. ■

Proposition 2.2.5
The following languages are $\mathcal{NP}$-complete:

1. *Integer-Programming:*

$$\mathrm{IP} := \left\{ (m, n, A, b) \;\middle|\; \begin{array}{l} A \in M_{m,n}(\mathbb{Z}), b \in \mathbb{Z}^m, \\ \exists x \in \mathbb{Z}^n : Ax \le b \end{array} \right\}$$

2. *Knapsack or Subset Sum:*

$$\mathrm{SubsetSum} := \left\{ (n, a_1, a_2, \ldots, a_n, b) \in \mathbb{N}^{n+2} \;\middle|\; \exists x \in \{0,1\}^n : \sum_{i=1}^{n} a_i x_i = b \right\}$$

3. *$\{0,1\}$-Integer-Programming:*

$$\{0,1\}\text{-IP} := \left\{ (m, n, A, b) \;\middle|\; \begin{array}{l} A \in M_{n,m}(\mathbb{Z}), b \in \mathbb{Z}^m, \\ \exists x \in \{0,1\}^n : Ax \le b \end{array} \right\}$$

4. *Weak Dependence:*

$$\left\{ (n, a_1, a_2, \ldots, a_n) \in \mathbb{N}^{n+1} \;\middle|\; \exists\, (x_1, x_2, \ldots, x_n) \in \{0, \pm 1\}^n \setminus \{0^n\} : \sum_{i=1}^{n} a_i x_i = 0 \right\}$$

Proof. For 1,2,3 see [GaJo79, SpStr76], for 4 see [EmBoas81]. In Proposition 2.2.6 we prove that integer programming has a polynomial length witness and hence IP $\in \mathcal{NP}$. ■

Proposition 2.2.6 (von zur Gathen, Sieveking 1978)
IP $\in \mathcal{NP}$.

Proof. The witness for $(m, n, A, b) \in$ IP will be a suitable $x \in \mathbb{Z}^n$ with $Ax \le b$. Obviously, if such an x exists, then $(m, n, A, b) \in$ IP. We need only show that the witness has polynomial length. Let $A =: (a_{ij})$ and $b =: (b_1, b_2, \ldots, b_m)^{\mathsf{T}}$. Set $M := \max_{i,j} \{|a_{ij}|, |b_i|\}$. Von zur Gathen and Sieveking [GaSi78] prove:

$$(\exists x \in \mathbb{Z}^n : Ax \le b) \quad \Longleftrightarrow \quad \left(\exists x \in \mathbb{Z}^n : Ax \le b,\ \|x\|_\infty \le (n+1) n^{\frac{n}{2}} M^n\right)$$

The upper bound on $||x||_\infty$ implies that the length of the witness x is polynomially bounded in the length of A und b. Since $\ell(m, n, A, b) \geq nm + \log_2 M$ we have:

$$\ell(x) = \mathcal{O}\left(n^2(\log n + \log M\right) = \mathcal{O}\left(\ell(m, n, A, b)^3\right)$$

■

We make the following definitions, which will be needed in the next Chapter.

Definition 2.2.7 (Lattice, Basis, Dimension, Rank)
Let $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$ be linearly independent vectors. We call the additive subgroup

$$L(b_1, b_2, \ldots, b_n) := \sum_{i=1}^{n} b_i\mathbb{Z} = \left\{ \sum_{i=1}^{n} t_i b_i \;\middle|\; t_1, t_2, \ldots, t_m \in \mathbb{Z} \right\}$$

of $\mathbb{R}^m$ a lattice with basis $b_1, b_2, \ldots, b_n$. When the sequence of the basis vectors is fixed, speak of an ordered basis. The rank or the dimension of the lattice is $\text{rank}(L) := n$.

We consider an example:

Example 2.2.8 (Lattice)
$\mathbb{Z}^m$ is a lattice of rank m, the standard unit vectors $e_1, \ldots, e_m$ form a basis. Given the matrix $A \in M_{m,n}(\mathbb{Z})$ the set $\{x \in \mathbb{Z}^n \mid Ax = 0\}$ is a lattice of rank $n - \text{rank}(A)$; by Proposition 2.2.4 we can construct a basis in polynomial time. ◇

Through lattice reduction we search for a shortest, non-trivial, lattice vector. In the case of the sup norm this cannot be done efficiently under the assumption that $\mathcal{P} \neq \mathcal{NP}$:

Corollary 2.2.9
The problem of finding the shortest lattice vector with respect to the $||\cdot||_\infty$ norm:

$$L_\infty\text{-SVP} := \left\{ (m, n, b_1, b_2, \ldots, b_n) \;\middle|\; \begin{array}{l} m, n \in \mathbb{N}, b_1, b_2, \ldots, b_n \in \mathbb{Z}^m, \\ \exists x \in L(b_1, b_2, \ldots, b_n) : \; ||x||_\infty = 1 \end{array} \right\}$$

is $\mathcal{NP}$-complete.

Proof. The problem of finding the $||\cdot||_\infty$-shortest lattice vector is in $\mathcal{NP}$: The witness of membership is a vector $x \in L(b_1, b_2, \ldots, b_n) \setminus \{0\}$ with $||x||_\infty = 1$. The $\mathcal{NP}$-complete problem "weak dependence" from Proposition 2.2.5 can be reduced in polynomial time to the $||\cdot||_\infty$-shortest lattice vector. ■

The problem of the shortest lattice vector in the ℓ_2 norm is, given a lattice basis $b_1, b_2, \ldots, b_n$ and k, decide whether there is a lattice vector $z \in L(b_1, b_2, \ldots, b_n)$ with $z \neq 0$ and $||z||_2 \leq \sqrt{k}$.

Definition 2.2.10 (Shortest Vector Problem SVP)
The language of the shortest lattice vectors in the ℓ_2-norm is:

$$L_2\text{-SVP} := \left\{ (k,m,n,b_1,b_2,\dots,b_n) \;\middle|\; \begin{array}{l} k,m,n, \in \mathbb{N}, b_1,b_2,\dots,b_n \in \mathbb{Z}^m, \\ \exists x \in L(b_1,b_2,\dots,b_n) \setminus \{0\} : \ \|x\|_2^2 \le k \end{array} \right\}$$

The status of this problem is open. Efforts to show that L_2-SVP is $\mathcal{NP}$-hard, in contrast to the sup-norm-SVP (see Corollary 2.2.9) have failed (see [Kannan87]). However, Ajtai [Ajtai98] has shown that this problem is $\mathcal{NP}$-hard with respect to *randomized* reductions.

The problem of the shortest lattice vector is the homogeneous special case of the problem of the closest lattice vector, which, however, is known to be $\mathcal{NP}$-complete for *any* norm:

Proposition 2.2.11 (Closest Vector Problem CVP)
The problem of the ℓ_2-closest lattice vector

$$L_2\text{-CVP} := \left\{ (k,m,n,b_1,b_2,\dots,b_n,z) \;\middle|\; \begin{array}{l} k,m,n, \in \mathbb{N}, b_1,b_2,\dots,b_n,z \in \mathbb{Z}^m, \\ \exists x \in L(b_1,b_2,\dots,b_n) : \ \|z-x\|^2 \le k \end{array} \right\}$$

is $\mathcal{NP}$-complete.

Proof. See [Kannan87, Theorem6.2]. ■

Later we will see an approximate solution due to Babai, based on the LLL algorithm, yielding a vector in the lattice that is nearest within a factor of c^n, for a fixed constant c.

Summarizing: given a lattice basis $b_1,b_2,\dots,b_n \in \mathbb{Z}^m$, the following tasks are thought to be hard algorithmic lattice problems:

- Find a short non-trivial lattice vector.
- Find a basis comprised of short lattice vectors.
- Find for a given $z \in \operatorname{span}(b_1,b_2,\dots,b_n)$ the closest lattice vector.

In contrast, given a system of generators $b_1,b_2,\dots,b_n \in \mathbb{Z}^m$ for a lattice L, $n \ge \operatorname{rank}(L)$, it is possible to construct a basis for L in polynomial time.

Chapter 3

Introduction to Lattice Theory

We define the Hermite normal form of a matrix and show that the Hermite normal form of an integer matrix is unique. We characterize lattices as discrete, addititve, subgroups of $\mathbb{R}^m$. We discuss the set of all bases of a lattice, primitive systems of lattice vectors, the lattice determinant, and the Gram-Schmidt orthogonalization of a lattice. We define length reduction and weight reduction of a lattice basis, and show that every lattice has a length reduced and a weight reduced bases.

3.1 Terminology

Let $\langle \cdot, \cdot \rangle : \mathbb{R}^m \times \mathbb{R}^m \to \mathbb{R}$ be an arbitrary scalar product on the vector space $\mathbb{R}^m$. Then $\|x\| = \sqrt{\langle x, x \rangle}$ is called the length of the vector x. For linearly independent vectors $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$ we let

$$L(b_1, b_2, \ldots, b_n) := \sum_{i=1}^{n} b_i \mathbb{Z}$$

denote the lattice with basis $b_1, b_2, \ldots, b_n$. For arbitrary vectors $b_1, b_2, \ldots, b_n$ let

$$\operatorname{span}(b_1, b_2, \ldots, b_n) := \sum_{i=1}^{n} b_i \mathbb{R}$$

be the space spanned by $b_1, b_2, \ldots, b_n$ and let

$$\operatorname{span}(b_1, b_2, \ldots, b_n)^{\perp} := \{ y \in \mathbb{R}^m \mid \langle y, b_i \rangle = 0 \text{ for } i = 1, 2, \ldots, n \}$$

denote the orthogonal complement of this space in $\mathbb{R}^m$.

An integer matrix with determinant ± 1 is said to be *unimodular*. The set of all unimodular matrices is denoted $\mathrm{GL}_n(\mathbb{Z})$:

Definition 3.1.1 ($\mathbf{GL}_n(\mathbb{Z})$)
$\mathrm{GL}_n(\mathbb{Z})$ is the group of integer $n \times n$ matrices with determinant ± 1:

$$\mathrm{GL}_n(\mathbb{Z}) := \{A \in M_{n,n}(\mathbb{Z}) \mid \det A = \pm 1\}$$

We argue that $\mathrm{GL}_n(\mathbb{Z})$ is a group. The identity matrix is unimodular and from that fact that if $S, T \in \mathrm{GL}_n(\mathbb{Z})$ then $\det(ST) = \det S \cdot \det T$, we see that the product ST is a unimodular matrix. Let $T \in \mathrm{GL}_n(\mathbb{Z})$. From

$$\det\left(T^{-1}\right) = \frac{1}{\det T}$$

we have that $\det\left(T^{-1}\right) = \pm 1$, and by Cramer's rule the (i, j) entry in the matrix T^{-1} is:

$$\frac{(-1)^{i+j} \cdot \det T_{ij}}{\det T} = \pm \det T_{ij},$$

where T_{ij} denotes T with the ith row and j-th column deleted. Since T_{ij} is an integer matrix, it follows that $\det T_{ij} \in \mathbb{Z}$. Thus, for $T \in \mathrm{GL}_n(\mathbb{Z})$ we have $T^{-1} \in \mathrm{GL}_n(\mathbb{Z})$.

The following *elementary column operations* can be performed on a matrix by right-multiplication with an appropriately chosen unimodular matrix:

- Exchange two columns
- Mulitiplication of a column by -1
- Addition of an integer multiple of one column to another

It can be shown that every unimodular matrix is the product of these three matrix types. So multiplication by a unimodular matrix corresponds to carrying out a set of elementary column operations.

3.2 Fundamentals and Properties

In this section we define the fundamentals of lattice theory and show some elmentary properties.

3.2.1 Discrete, Additive Subgroups of $\mathbb{R}^m$ and Lattices

Definition 3.2.1 (Discrete Set)
A set $S \subseteq \mathbb{R}^m$ is called discrete, when S has no limit point in $\mathbb{R}^m$.

We have:

Lemma 3.2.2
Let $G \subseteq \mathbb{R}^m$ be an additive group. Then the following statements are equivalent:

a) G *is discrete.*

b) 0 *is is not a limit point of* G*.*

c) $\{x \in G \,:\, \|x\| < r\}$ *is finite for all* $r > 0$*.*

d) $\inf\{\|x - y\| \,:\, x \neq y, x, y \in G\} > 0$*; that is, there is a positive, real,* δ *such that* $\forall x, y \in G$, $\|x - y\| \geq \delta$*.*

Proposition 3.2.3
$L \subseteq \mathbb{R}^m$ *is a lattice if and only if* L *is a discrete, additive, subgroup of* $\mathbb{R}^m$*.*

Proof. We show both directions:

"$\Rightarrow$" We must show that every lattice $L := L(b_1, b_2, \dots, b_n) \subseteq \mathbb{R}^m$, where $b_1, b_2, \dots, b_n$ are linearly independent, is discrete. Let $\varphi : \mathbb{R}^n \to \text{span}(L)$ the linear mapping

$$\varphi(t_1, t_2, \dots, t_n) = \sum_{i=1}^{n} t_i b_i$$

φ is an isomorphism with $\varphi(\mathbb{Z}^n) = L$. Thus, intuitively, φ and φ^{-1} preserve local structure. Since $\mathbb{Z}^n$ is discrete and φ^{-1} is continuous on $\text{span}(L)$, it follows that L is discrete.

"$\Leftarrow$" Let $L \subseteq \mathbb{R}^m$ be a discrete, additive, subgroup. Let n be the maximum number of linearly independent vectors in L. Then $n \leq m$. By induction on n we will show that L is a lattice of rank n. Note that this implies that the rank of a lattice L is the maximal number of linearly independent vectors in L.

- $n = 1$

  Let $b \in L$ be a shortest vector with $b \neq 0$ (such a vector exists, since 0 is not a limit point of L). Then it is not hard to verify that $L(b) = L$.

- $n > 1$

  Choose $b_1 \in L \setminus \{0\}$ with $\frac{1}{k} \cdot b_1 \notin L$ for all $k \geq 2$. Then

  $$L(b_1) = L \cap \text{span}(b_1) \tag{3.1}$$

  The orthogonal projection $\pi : \mathbb{R}^m \to \text{span}(b_1)^{\perp}$ is defined by:

  $$\pi(b) = b - \frac{\langle b_1, b \rangle}{\langle b_1, b_1 \rangle} \cdot b_1$$

  The inductive step follows from the following assertions:

  1. $\pi(L)$ is discrete and is a lattice of rank $n - 1$.
  2. For every basis $\pi(b_2), \pi(b_3), \dots, \pi(b_n)$ for $\pi(L)$ with $b_2, b_3, \dots, b_n \in L$ we have:

  $$L = L(b_1, b_2, \dots, b_n)$$

The first assertion says that there exists a basis for $\pi(L)$ of $n-1$ linearly independent vectors. These vectors are necessarily the images of vectors in L, say, $b_2, \dots, b_n$. So let $\pi(b_2), \dots, \pi(b_n)$ be a basis for $\pi(L)$. The second assertion says that for every such basis for $\pi(L)$, if we add b_1 to the set of pre-images, then $L = L(b_1, b_2, \dots, b_n)$ and so by definition is a lattice. Proof of the two assertions:

1. We show that 0 is not a limit point of $\pi(L)$. For the sake of contradiction, assume that 0 is a limit point of $\pi(L)$. Let $\left(y^{(i)}\right)_{i \in \mathbb{N}}$ be a sequence in L, so that the vectors $\pi\left(y^{(i)}\right)$ are pairwise distinct and $\lim\limits_{i \to \infty} \pi\left(y^{(i)}\right) = 0$. For these vectors

$$\pi\left(y^{(i)}\right) = y^{(i)} - \frac{\langle y^{(i)}, b_1 \rangle}{\langle b_1, b_1 \rangle} \cdot b_1$$

we compute $\overline{y}^{(i)}$ defined by:

$$\overline{y}^{(i)} := y^{(i)} - \underbrace{\left\lceil \frac{\langle y^{(i)}, b_1 \rangle}{\langle b_1, b_1 \rangle} \right\rfloor}_{\text{integer}} b_1$$

Then $\overline{y}^{(i)} \in L$ $\pi\left(\overline{y}^{(i)}\right) = \pi\left(y^{(i)}\right)$, and:

$$\left\| \overline{y}^{(i)} - \pi\left(y^{(i)}\right) \right\| \leq \tfrac{1}{2} \|b_1\|$$

Since $\lim\limits_{i \to \infty} \left\| \pi\left(\overline{y}^{(i)}\right) \right\| = 0$, there are infinitely many vectors $\overline{y}^{(i)} \in L$ with:

$$\left\| \overline{y}^{(i)} \right\| \leq \|b_1\|$$

This contradicts the fact that L is discrete, and hence the assumption that $\pi\left(y^{(i)}\right)$ are pairwise distinct and $\pi\left(\overline{y}^{(i)}\right) = \pi\left(y^{(i)}\right)$. Thus 0 is not a limit point of $\pi(L)$, and by Lemma 3.2.2 $\pi(L)$ is discrete. The maximum number of linearly independent vectors in $\pi(L)$ is $n-1$. By the inductive hypothesis $\pi(L)$ is a lattice of rank $n-1$.

2. Let $\pi(b_2), \pi(b_3), \dots, \pi(b_n)$ be a basis for $\pi(L)$ with $b_2, b_3, \dots, b_n \in L$. We will show that $L \subseteq L(b_1, b_2, \dots, b_n)$. Let $b \in L$. From

$$\pi(b) \in \pi(L) = L\left(\pi(b_2), \pi(b_3), \dots, \pi(b_n)\right)$$

there is a $\overline{b} \in L(b_2, b_3, \dots, b_n)$ with $\pi(b) = \pi\left(\overline{b}\right)$. We have $b - \overline{b} \in \operatorname{span}(b_1)$. By the choice of b_1 and from

$$b - \overline{b} \in \left(L \cap \operatorname{span}(b_1)\right) \overset{(3.1)}{=} L(b_1)$$

it follows that $b - \overline{b} \in L(b_1)$. Thus, $b \in L(b_1, b_2, \dots, b_n)$.

■

The above proof also shows that the rank of a lattice is the maximum number of linearly independent lattice vectors. It follows from the next Proposition that every lattice has many different bases. Let $[b_1, b_2, \dots, b_n]$ be the matrix with column vectors $b_1, b_2, \dots, b_n$. Recall that $\mathrm{GL}_n(\mathbb{Z})$ is the group of integer $n \times n$ matrices with determinant ± 1.

Proposition 3.2.4
The vectors $\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n \in \mathbb{R}^m$ form a basis of the lattice $L(b_1, b_2, \dots, b_n)$ if and only if there exists a matrix $T \in \mathrm{GL}_n(\mathbb{Z})$ such that:

$$\left[\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n\right] = [b_1, b_2, \dots, b_n] \cdot T$$

Proof. We prove both directions:

"$\Rightarrow$" Since $\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n \in L(b_1, b_2, \dots, b_n)$ there is a $T \in M_{n,n}(\mathbb{Z})$ with:

$$\left[\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n\right] = [b_1, b_2, \dots, b_n] \cdot T$$

Since $\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n$ are linearly independent, we have $\det T \neq 0$. It follows that

$$\left[\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n\right] \cdot T^{-1} = [b_1, b_2, \dots, b_n]$$

Since $b_i \in L\left(\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n\right)$ for $i = 1, 2, \dots, n$, T^{-1} has integer entries. Since $\det T \cdot \det T^{-1} = 1$ and $\det T$, $\det T^{-1}$ are both integer, it follows that $|\det T| = 1$.

"$\Leftarrow$" Let us suppose for some $T \in \mathrm{GL}_n(\mathbb{Z})$ that

$$\left[\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n\right] = [b_1, b_2, \dots, b_n] \cdot T$$

It follows that $\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n \in L(b_1, b_2, \dots, b_n)$. Similarly, it follows from

$$\left[\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n\right] \cdot T^{-1} = [b_1, b_2, \dots, b_n],$$

that $b_1, b_2, \dots, b_n \in L\left(\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n\right)$. Thus,

$$L\left(\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n\right) = L(b_1, b_2, \dots, b_n)$$

■

Since elementary column operations can be achieved by right multiplication of the basis matrix by a unimodular matrix, this says that if we modify basis $B = [b_1, b_2, \dots, b_n]$ by

1. reordering the columns
2. multiplying any number of columns by -1
3. adding integer multiples of some columns to other columns

then the resulting matrix is a basis matrix for the same lattices.

3.2.2 Definition of Hermite Normal Form

We introduce the Hermite Normal Form of a matrix and prove its uniqueness. In Chapter ?? on Page ?? we will show an algorithm for obtainng the Hermite Normal Form of an arbitrary matrix.

Definition 3.2.5 (Hermite Normal Form)
A matrix $[a_{ij}] \in M_{m,n}(\mathbb{R})$ with $m \leq n$ is in Hermite Normal Form (HNF) when:

a) $a_{ij} = 0$ for $j > i$, i.e., A is lower triangular.

b) $a_{ii} > 0$ for $i = 1, 2, \ldots, m$.

c) $0 \leq a_{ij} < a_{ii}$ for $j < i$.

It is arbitrary to require that the Hermite Normal Form will be lower triangular rather than upper triangular (see Corollary 3.2.8). Alternatives for Point c) appear in the literature. In [DKT87] the authors require

$$a_{ij} \leq 0 \text{ and } |a_{ij}| < a_{ii} \quad \text{for } j < i$$

In [PaSchn87] the authors require that the elements to the left of the diagonal should be relatively small:

$$|a_{ij}| < \tfrac{1}{2}\,|a_{ii}| \quad \text{for } j < i$$

We can obtain the different variants of Point c) of Hermite Normal Form by addition of integer multiples of one column to another column. Thus, for our purposes the different Hermite Normal Forms are equivalent, since by Proposition 3.2.4 they yield the same lattice.

The following Proposition was first proved by C. Hermite [Hermite1850] for square matrices:

Proposition 3.2.6 (Hermite 1850)
For every matrix $A \in M_{m,n}(\mathbb{Q})$ with $\operatorname{rank}(A) = m \leq n$, there is a matrix $T \in \mathrm{GL}_n(\mathbb{Z})$, so that AT is in Hermite Normal Form. The Hermite Normal Form AT is unique.

Proof. Let a be the least common multiple of the denominators of the entries of matrix A. Then $aA \in M_{m,n}(\mathbb{Z})$ and $\frac{1}{a}(aA)T$ is its Hermite Normal Form. We can therefore restrict our attention to the case that $A \in M_{m,n}(\mathbb{Z})$.

A polynomial algorithm for computing the Hermite Normal Form appears in [BaKa84]. (see Algorithm ??, ?? ?? of these notes). It remains to show uniqueness. Suppose for the sake of contradiction that there exist two normal forms, $B, C \in M_{m,n}(\mathbb{Z})$ for A.

$$B = \begin{bmatrix} b_{11} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ b_{21} & b_{22} & \ddots & 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & 0 & 0 & \cdots & 0 \\ b_{m1} & b_{m2} & \cdots & b_{mm} & 0 & \cdots & 0 \end{bmatrix} \qquad C = \begin{bmatrix} c_{11} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ c_{21} & c_{22} & \ddots & 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & 0 & 0 & \cdots & 0 \\ c_{m1} & c_{m2} & \cdots & c_{mm} & 0 & \cdots & 0 \end{bmatrix}$$

Let $B_1, B_2, \ldots, B_n$ and $C_1, C_2, \ldots, C_n$ be the column vectors for B and C, respectively. Since both Hermite Normal Forms for A can be obtained from each other by multiplication with unimodular matrices, we have by Proposition 3.2.4 that $L(B) = L(C)$. In particular, $B_m \in L(C)$ and $C_m \in L(B)$. Since the diagonal elements are all non-zero, B_m must be an integer multiple of C_m and conversely, so $c_{mm} = b_{mm}$.

Let j be the maximal index with $B_j \neq C_j$. Since $c_{mm} = b_{mm}$, we have $j + 1 \leq m$. Since $L(B) = L(C)$ there exist integer coefficients $t_j, t_{j+1}, \ldots, t_m \in \mathbb{Z}$, so that for every i with $j \leq i \leq m$ we have (note: $c_{ik} = 0$ for $k > i$):

$$b_{ij} = \sum_{k=j}^{i} t_k c_{ik} \tag{3.2}$$

As in the case of the mth column vectors, we obtain $b_{jj} = c_{jj}$, so $t_j = 1$. For $i = j + 1$ we have

$$b_{j+1,j} = t_j \cdot c_{j+1,j} + t_{j+1} \cdot c_{j+1,j+1} = c_{j+1,j} + t_{j+1} \cdot c_{j+1,j+1} \tag{3.3}$$

and we obtain

$$c_{j+1,j+1} \mid t_{j+1} \cdot c_{j+1,j+1} = (b_{j+1,j} - c_{j+1,j}) \tag{3.4}$$

Since B is in Hermite Normal Form, we have by the choice of j the maximum index with $B_j \neq C_j$:

$$0 \leq b_{j+1,j} < b_{j+1,j+1} = c_{j+1,j+1}$$

Since C is also in Hermite Normal Form, we have $0 \leq c_{j+1,j} < c_{j+1,j+1}$, and we obtain:

$$|b_{j+1,j} - c_{j+1,j}| < c_{j+1,j+1}$$

¿From (3.4) it follows that $b_{j+1,j} = c_{j+1,j}$ and from (3.3) we have $t_{j+1} = 0$. One shows inductively that likewise

$$t_{j+2} = t_{j+3} = \cdots = t_m = 0$$

and thus obtain by (3.2) the contradiction $B_j = 0$. ■

We will compute the Hermite Normal Form for a special case:

Example 3.2.7 (Hermite Normal Form)
We consider the case that the matrix A has one row

$$A = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \end{bmatrix}$$

and the minimum entry is non-zero. Note that the operations of the Euclidean Algorithm on the values $a_1, a_2, \ldots, a_n$ can be expressed by right-multiplication with unimodular matrices. This yields $g := \gcd(a_1, a_2, \ldots, a_n)$ in the leftmost position, the remaining values being 0. We obtain the Hermite Normal Form of A

$$\mathrm{HNF}(A) = \begin{bmatrix} g & 0 & \cdots & 0 \end{bmatrix}$$

Note that the column vectors of A and HNF(A) yield the same lattice, namely

$$\sum_{i=1}^{n} \mathbb{Z} a_i = \mathbb{Z} \cdot \gcd(a_1, a_2, \dots, a_n)$$

In Proposition 3.2.4 we will see that this is not a coincidence. The Euclidean Algorithm is the basis for the procedure in Chapter ?? to obtain the Hermite Normal Form of an arbitrary matrix $A \in M_{m,n}(\mathbb{Z})$.

Up to this point, we have been careful to stipulate that the basis vectors $b_1, b_2, \dots, b_n \in \mathbb{R}^m$ for $L = L(b_1, b_2, \dots, b_n)$ are linearly independent. Clearly, when $m < n$ the "basis" vectors cannot all be linearly independent. When this occurs, the vectors impose a gcd-like structure; the we have $\sum_{i=1}^{n} b_i\mathbb{Z} = \sum_{i=1}^{m} c_i\mathbb{Z}$, where $c_1, c_2, \dots, c_m$ are the first m columns of the HNF form of $[b_1, b_2, \dots, b_n]$. ◇

We have formulated Proposition 3.2.6 only for rational and in particular for integer matrices. For real matrices the proposition does not generally hold. For example, for

$$A := \begin{bmatrix} 1 & \sqrt{2} \\ 3 & 4 \end{bmatrix} \in M_{2,2}(\mathbb{R})$$

there is no matrix $T \in \mathrm{GL}_2(\mathbb{Z})$, so that AT is in Hermite Normal Form (proof by contradiction).

Corollary 3.2.8
For every matrix $A \in M_{m,n}(\mathbb{Q})$ with $\operatorname{rank}(A) = m \leq n$ there is a matrix $T \in \mathrm{GL}_n(\mathbb{Z})$, so that AT is upper triangular.

Proof. We define matrix $U := [u_{ij}] \in \mathrm{GL}_n(\mathbb{Z})$ by $u_{ij} := \delta_{i,n+1-j}$. U is obtained from the identity matrix by reversing the order of the column vectors. It is obvious that $U = U^{-1}$. Multiplication of a matrix by U

- on the left reverses the order of the row vectors and
- on the right reverses the order of the column vectors.

We obtain for UAU by Proposition 3.2.6 the Hermite Normal Form $(UAU) \cdot S$ with $S \in \mathrm{GL}_n(\mathbb{Z})$. $(UAU) \cdot S$ is lower triangular. We define the matrix $T := USU \in \mathrm{GL}_n(\mathbb{Z})$. By reversing the order of the row and column vectors we obtain the of the matrix $(UAU) \cdot S$, we obtain the upper triangular matrix:

$$U \cdot (UAUS) \cdot U = AUSU = AT$$

■

3.2.3 Determinant and Basic Block

We define the determinant of a lattice:

Definition 3.2.9 (Determinant)
The determinant $\det L$ *of lattice* $L = (b_1, b_2, \ldots, b_n) \subseteq \mathbb{R}^m$ *is defined by:*

$$\det L = \left(\det\left[\langle b_i, b_j\rangle\right]_{1\leq i,j\leq n}\right)^{\frac{1}{2}}$$

For the scalar product $\langle u, v\rangle = u^{\mathsf{T}}Sv$ we have: $\det L = \det(B^{\mathsf{T}} \cdot S \cdot B)^{\frac{1}{2}}$, where $B := [b_1, b_2, \ldots, b_n]$.

Proposition 3.2.10
The determinant of a lattice is independent of the choice of basis $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$.

Proof. Let $B, \overline{B}$ be basis matrices of the lattice and let $T \in \mathrm{GL}_n(\mathbb{Z})$ satisfy $\overline{B} = B \cdot T$ (the proof holds in general for $T \in \mathrm{GL}_n(\mathbb{R})$). Let $S \in M_{m,m}(\mathbb{R})$ be the symmetric matrix with $\langle u, v\rangle = u^{\mathsf{T}}Sv$. ¿From $\det T = 1$ we have:

$$\begin{aligned}\det L &= \left(\det\left[\langle b_i, b_j\rangle\right]_{1\leq i,j\leq n}\right)^{\frac{1}{2}}\\ &= \det\left(B^{\mathsf{T}} \cdot S \cdot B\right)^{\frac{1}{2}}\\ &= \det\left(T^{\mathsf{T}} \cdot B^{\mathsf{T}} \cdot S \cdot B \cdot T\right)^{\frac{1}{2}}\\ &= \det\left((BT)^{\mathsf{T}} \cdot S \cdot (BT)\right)^{\frac{1}{2}}\end{aligned}$$

Since $\overline{B} = B \cdot T$ it follows that:

$$\begin{aligned}\det L &= \det\left(\overline{B}^{\mathsf{T}} \cdot S \cdot \overline{B}\right)^{\frac{1}{2}}\\ &= \left(\det\left[\langle \bar{b}_i, \bar{b}_j\rangle\right]_{1\leq i,j\leq n}\right)^{\frac{1}{2}}\\ &= \det \overline{L}\end{aligned}$$

■

The parallelepiped determined by the basis vectors of the lattice is the basic block of the lattice with respect to the given basis. Figure 3.2.1 shows the basic block of the lattice determined by a, b in $\mathbb{R}^2$.

Definition 3.2.11 (Basic Block)
Let $b_1, b_2, \ldots, b_n$ *be a basis of the lattice* L*. The parallelepiped*

$$\left\{\sum_{i=1}^{n} t_i b_i \;\middle|\; 0 \leq t_1, t_2, \ldots, t_n < 1\right\}$$

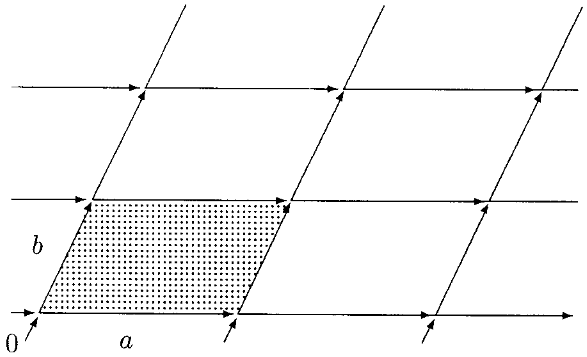

Figure 3.2.1: Basic Block of the Lattice $L(a, b)$

is the basic block with respect to basis $b_1, b_2, \dots, b_n$. We are mostly interested in the case that the dimension of the lattice $L \subseteq \mathbb{R}^m$ is equal to m.

Definition 3.2.12 (Full Dimensional Lattice)
A lattice $L \subseteq \mathbb{R}^m$ is full dimensional when $\operatorname{rank}(L) = m$.

The following lemma relates the standard scalar product to the determinant of a lattice:

Lemma 3.2.13
For every lattice $L = L(b_1, b_2, \dots, b_n) \subseteq \mathbb{R}^m$ and the standard scalar product we have (note: volume implicitly relies on the scalar product):

$$\det L = \operatorname{vol}_n \left(\left\{ \sum_{i=1}^{n} t_i b_i \;\middle|\; 0 \leq t_1, t_2, \dots, t_n < 1 \right\} \right)$$

In words: The n-dimensional volume of the basic block equals the lattice determinant. For a full dimensional lattice the lattice determinant is equal to the determinant of the basis matrix.

Proof. We first consider full dimensional lattices. In this case, for basis matrix $B := [b_1, b_2, \dots, b_n]$, we have:

$$\det L = |\det B| = \left(\det B^{\mathsf{T}} B\right)^{\frac{1}{2}} = \left(\det \left[\langle b_i, b_j \rangle\right]_{1 \leq i,j \leq n}\right)^{\frac{1}{2}}$$

In the general case, where $\operatorname{rank}(L) = n \leq m$, we will later show that there is an isometric mapping $T : \operatorname{span}(L) \to \mathbb{R}^m$, such that for all $u, v \in \operatorname{span}(L)$, $\langle u, v \rangle = \langle T(u), T(v) \rangle$. We apply the lemma to the full dimensional lattice $T(L)$ and use the fact that T preserves the volume and scalar product:

$$\det L = \det T(L) = \left(\det\left[\langle T(b_i), T(b_j)\rangle\right]_{1\leq i,j\leq n}\right)^{\frac{1}{2}} = \left(\det\left[\langle b_i, b_j\rangle\right]_{1\leq i,j\leq n}\right)^{\frac{1}{2}}$$

■

As in the proof of Lemma 3.2.13 we can always restrict our attention to the case of full dimensional lattices when considering geometric invariants. This is because the invariants remain unchanged by isometric mappings. Examples of geometric invariants are volumes, determinants, scalar products, and vector lengths. The principle that full dimensional lattices suffice for geometric considerations depends on the fact that for every lattice L of rank n there is an isometric mapping from $\text{span}(L)$ to $\mathbb{R}^n$. This isometric mapping does not in general maintain the integrality of vectors. Combinatoric and algorithmic investigation should thus not be restricted to the case of full dimensional lattices.

3.2.4 Sub-Lattices

We define a sub-lattice as a subset of lattice points that form a lattice of the same rank:

Definition 3.2.14 (Sub-Lattice)
Let L_1, L_2 be lattices of the same rank with $L_1 \subseteq L_2$. Then we say that L_1 is a sub-lattice of L_2.

Example 3.2.15 (Sub-Lattice)
We consider a sub-lattice of the lattice $\mathbb{Z}^n$ (which has basis matrix the 2×2 identity matrix I_2). Let

$$A := \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

$L(A) \subseteq \mathbb{Z}^2$ is a sub-lattice of $\mathbb{Z}^2$ with $\text{rank}(L(A)) = 2$ (see Figure 3.2.2). There is a matrix $T \in M_{2,2}(\mathbb{Z})$ with $A = I_2 \cdot T$:

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \underbrace{\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}}_{=:T}$$

We will see in Proposition 3.2.16 that such a T always exists, and moreover (Lemma 3.2.18), that $\det L_1 = \det L_2 \cdot |\det T|$.

Proposition 3.2.16
Let L_1 be a sub-lattice of $L_2 \subseteq \mathbb{R}^m$.

a) For every basis $a_1, a_2, \ldots, a_n$ of L_1 there exists a basis $b_1, b_2, \ldots, b_n$ for L_2 with

$$[a_1, a_2, \ldots, a_n] = [b_1, b_2, \ldots, b_n] \cdot T \tag{3.5}$$

for an upper triangular matrix $T \in M_{n,n}(\mathbb{Z})$.

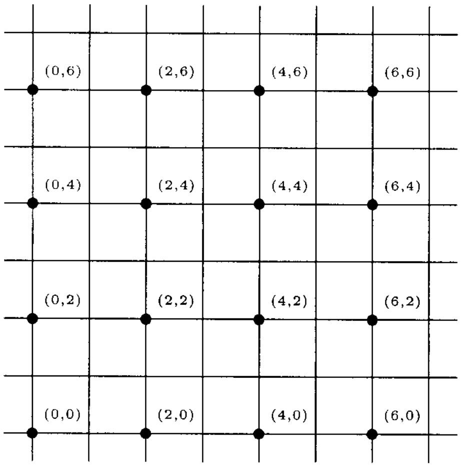

Figure 3.2.2: Sub-Lattice $L(A)$ of $\mathbb{Z}^2$

b) *Conversely, for every basis* $b_1, b_2, \dots, b_n$ *for* L_2 *there is a basis* $a_1, a_2, \dots, a_n$ *for* L_1 *with property* (3.5).

Remark 3.2.17
¿From Property (3.5) *with upper triangular matrix* T, *we have that:*

$$\operatorname{span}(a_1, a_2, \dots, a_i) = \operatorname{span}(b_1, b_2, \dots, b_i) \qquad \textit{for } i = 1, 2, \dots, n$$

Proof (of Proposition 3.2.16). We show both statements:

a) Let $\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n$ be an arbitrary basis for L_2. Then since $L_1 \subseteq L_2$ each element of L_1 can be expressed as an integer linear combination of the basis elements of L_2. Thus, there exists a matrix $S \in M_{n,n}(\mathbb{Z})$ with $\det S \neq 0$ and:

$$[a_1, a_2, \dots, a_n] = \left[\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n\right] \cdot S \tag{3.6}$$

The HNF-Proposition 3.2.6 ensures that for S^T there exists a $U \in \mathrm{GL}_n(\mathbb{Z})$, such that $S^\mathsf{T} U^\mathsf{T} = (US)^\mathsf{T}$ is lower triangular. Define $T := US$ (an upper triangular matrix) and basis matrix for L_2:

$$[b_1, b_2, \dots, b_n] := \left[\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n\right] \cdot U^{-1}$$

By (3.6) we obtain:

$$[a_1, a_2, \dots, a_n] = \left[\bar{b}_1, \bar{b}_2, \dots, \bar{b}_n\right] \cdot S = [b_1, b_2, \dots, b_n] \cdot U \cdot S$$

b) Let $\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_n$ be an arbitrary basis for L_1. There is a matrix $S \in M_{n,n}(\mathbb{Z})$ with $\det S \neq 0$ and:

$$[\,\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_n] = [b_1, b_2, \ldots, b_n] \cdot S$$

By Corollary 3.2.8 there is a $U \in \mathrm{GL}_n(\mathbb{Z})$ such that SU is upper triangular. The statement follows for the basis

$$[a_1, a_2, \ldots, a_n] := [\,\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_n] \cdot U$$

and $T := SU$.

■

Contintuing our previous example, the factor group $\mathbb{Z}^2/L(A)$ consists of the four equivalence classes

$$\begin{bmatrix}0\\0\end{bmatrix} + L(A), \quad \begin{bmatrix}1\\0\end{bmatrix} + L(A), \quad \begin{bmatrix}0\\1\end{bmatrix} + L(A), \quad \begin{bmatrix}1\\1\end{bmatrix} + L(A)$$

Thus $\left[\mathbb{Z}^2 : L(A)\right] = 4$. In Lemma 3.2.18 we show that in general the index (*i.e.*, the number of distinct cosets) is equal to $|\det T|$. We represent the equivalence classes through their respective representatives, which lie in the basic block. ◇

Lemma 3.2.18
Let $L_2 = L(b_1, b_2, \ldots, b_n)$ be a lattice and $L_1 = L(a_1, a_2, \ldots, a_n)$ a sub-lattice of L_2. Let $T \in M_{n,n}(\mathbb{Z})$ with $A = B \cdot T$ for $A := [a_1, a_2, \ldots, a_n]$ and $B := [b_1, b_2, \ldots, b_n]$. Then:

$$\det L_1 = \det L_2 \cdot |\det T|$$

Proof. Let $S \in M_{m,m}(\mathbb{R})$ be the symmetric matrix with $\langle u, v\rangle = u^{\mathsf{T}} S v$. Then:

$$\begin{aligned}
\det L_1 &= \det\left(A^{\mathsf{T}} \cdot S \cdot A\right)^{\frac{1}{2}} \\
&= \det\left((BT)^{\mathsf{T}} \cdot S \cdot (BT)\right)^{\frac{1}{2}} \\
&= \det\left(T^{\mathsf{T}} B^{\mathsf{T}} \cdot S \cdot BT\right)^{\frac{1}{2}} \\
&= \det\left(T^{\mathsf{T}} T\right)^{\frac{1}{2}} \cdot \left(\det B^{\mathsf{T}} \cdot S \cdot B\right)^{\frac{1}{2}} \\
&= |\det T| \cdot \left(\det B^{\mathsf{T}} \cdot S \cdot B\right)^{\frac{1}{2}} \\
&= |\det T| \cdot \det L_2
\end{aligned}$$

■

Definition 3.2.19 (Index of a Sub-Lattice)
The integer $|\det T| = \frac{\det L_1}{\det L_2}$ from Lemma 3.2.18 is called the index of the sublattice L_1 in L_2.

The index is independent of the choice of lattice basis. In particular, L_1 is a subgroup of the additive group L_2 of index $|\det T|$.

Let $L_1 = L(a_1, a_2, \dots, a_n)$ be a sub-lattice of $L_2 = L(b_1, b_2, \dots, b_n)$, so that bases $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$ satisfy equation (3.5) with $T = [t_{ij}]$. Then L_2/L_1 is a finite group, the index $[L_2 : L_1]$ of L_1 in L_2 satisfies:

$$[L_2 : L_1] = \frac{\det L_1}{\det L_2} = \det T = \prod_{i=1}^{n} |t_{ii}| \tag{3.7}$$

In particular, $L_1 = L_2$ if and only if $|\det T| = 1$. This relation can be used to prove that $a_1, a_2, \dots, a_n$ form a basis for L_2. Let L_1 be the lattice defined by $a_1, a_2, \dots, a_n$. Then we know $\frac{\det L_1}{\det L_2}$ and a basis $b_1, b_2, \dots, b_n$ for L_2. Further, the system of vectors $a_1, a_2, \dots, a_n$ satisfies Property (3.5). Thus:

$$L_2 = L(a_1, a_2, \dots, a_n) \iff \prod_{i=1}^{n} |t_{ii}| = \frac{\det L_1}{\det L_2} = 1$$

It follows from (3.7) that:

Corollary 3.2.20
Let $a = (a_1, a_2, \dots, a_n)^{\mathsf{T}} \in \mathbb{Z}^n \setminus \{0\}$ and $b \in \mathbb{N}$. If $L_{a,b}$ is the integer lattice

$$L_{a,b} = \{x \in \mathbb{Z}^n \mid \langle x, a \rangle \equiv 0 \pmod b\}$$

(where $\langle \cdot, \cdot \rangle$ is the standard scalar product), then

$$\det L_{a,b} = \frac{b}{\gcd(a_1, a_2, \dots, a_n, b)}$$

Proof. We first show that $L_{a,b}$ is a sub-lattice of $\mathbb{Z}^n$, that is, the lattice $L_{a,b} \subseteq \mathbb{Z}^n$ has full rank. Let $v_n = (1, \dots, 1)^{\mathsf{T}} \in \mathbb{Z}^n$. Choose $n-1$ integer vectors $v_1, v_2, \dots, v_{n-1}$, so that $bv_1, bv_2, \dots, bv_n \in \mathbb{Z}^n$ are linearly independent (for example, the first $n-1$ identity vectors). Since

$$\langle bv_i, a \rangle \equiv b \cdot \langle v_i, a \rangle \equiv 0 \pmod b \qquad \text{for } i = 1, 2, \dots, n$$

it follows that $bv_1, bv_2, \dots, bv_n \in \mathbb{Z}^n$ are in the lattice $L_{a,b}$ and form a basis. Thus $L_{a,b}$ is a sub-lattice of $\mathbb{Z}^n$. ¿From $\det \mathbb{Z}^n = 1$ it follows from (3.7) that:

$$\det L_{a,b} = [\mathbb{Z}^n : L_{a,b}] \tag{3.8}$$

The factor group $\mathbb{Z}^n / L_{a,b}$ has at most b residue classes, namely $R_0, R_1, \dots, R_{b-1}$ with:

$$R_i := \{x \in \mathbb{Z}^n \mid \langle x, a \rangle \equiv i \pmod b\}$$

We show that the factor group has exactly these b residue classes. We first consider the case

$$\gcd(a_1, a_2, \dots, a_n, b) = 1 \tag{3.9}$$

Then there exist integer coefficients $t_1, t_2, \ldots, t_{n+1} \in \mathbb{Z}$ with:

$$\sum_{j=1}^{n} t_j \cdot a_j + t_{n+1} \cdot b = 1$$

For the vector $t := (t_1, t_2, \ldots, t_n) \in \mathbb{Z}^n$ we have:

$$\langle t, a \rangle \equiv 1 - t_{n+1} \cdot b \equiv 1 \pmod{b}$$

For the vectors $c_i := i \cdot t \in \mathbb{Z}^n$ with $i = 0, 1, \ldots, b-1$ we obtain:

$$\langle c_i, a \rangle \equiv i \cdot \langle t, a \rangle \equiv i \pmod{b}$$

The residue classes $R_0, R_1, \ldots, R_{b-1}$ are thus non-empty. From (3.9) we obtain by (3.8):

$$\det L_{a,b} = [\mathbb{Z}^n : L_{a,b}] = \frac{b}{1} = \frac{b}{\gcd(a_1, a_2, \ldots, a_n, b)}$$

We also consider the case

$$d := \gcd(a_1, a_2, \ldots, a_n, b) > 1$$

Then for all $x \in \mathbb{Z}^n$ we have

$$\begin{aligned} \langle x, a \rangle \equiv 0 \pmod{b} &\iff b \mid \langle x, a \rangle \\ &\iff \tfrac{b}{d} \mid \langle x, \tfrac{a}{d} \rangle \\ &\iff \langle x, \tfrac{a}{d} \rangle \equiv 0 \pmod{\tfrac{b}{d}}, \end{aligned}$$

so $L_{a,b} = L_{\frac{a}{d},\frac{b}{d}}$. Since $\gcd\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}, \frac{b}{d}\right) = 1$ we obtain:

$$\det L_{a,b} = \det L_{\frac{a}{d},\frac{b}{d}} = \frac{b}{d} = \frac{b}{\gcd(a_1, a_2, \ldots, a_n, b)}$$

■

3.2.5 Primitive System

In Proposition 3.2.22 we characterize systems of lattice vectors, which can be completed to obtain a basis for the lattice. These criteria are useful for the construction of special lattice bases.

Definition 3.2.21 (Primitive System)
Let $L \subseteq \mathbb{R}^n$ be a lattice. The vectors $b_1, b_2, \ldots, b_k \in L$ form a primitive system for L if

1. *$b_1, b_2, \ldots, b_k$ are linearly independent.*
2. *$\operatorname{span}(b_1, b_2, \ldots, b_k) \cap L = L(b_1, b_2, \ldots, b_k)$*

Since the inclusion $\mathrm{span}(b_1, b_2, \ldots, b_k) \cap L \subseteq L(b_1, b_2, \ldots, b_k)$ for arbitrary lattice vectors $b_1, b_2, \ldots, b_k$, what is significant is that $\mathrm{span}(b_1, b_2, \ldots, b_k) \cap L \supseteq L(b_1, b_2, \ldots, b_k)$. A single vector $b \in L$ forms a primitive system when $\frac{1}{k}b \notin L$ for all $k \in \mathbb{Z}$ with $|k| \geq 2$, so the greatest common divisor of the vector entries is 1.

Proposition 3.2.22
Let $L \subseteq \mathbb{R}^n$ be a lattice with $\mathrm{rank}(L) = n$ and $b_1, b_2, \ldots, b_k \in L$. The vectors $b_1, b_2, \ldots, b_k$ form a primitive system for L if and only if they can be completed for form a basis for L.

Proof. We show both directions:

"⇒" Let $b_1, b_2, \ldots, b_k, b_{k+1}, \ldots, b_n$ be a basis of the lattice L. The vectors $b_1, b_2, \ldots, b_k$ are linearly independent. Each vector $b \in L$ can be uniquely described as $b = \sum_{i=1}^{n} t_i b_i$ with $t_1, t_2, \ldots, t_n \in \mathbb{Z}$. We have,

$$b \in \mathrm{span}(b_1, b_2, \ldots, b_k) \quad \Longleftrightarrow \quad t_{k+1} = t_{k+2} = \cdots = t_n = 0$$

So $\mathrm{span}(b_1, b_2, \ldots, b_k) \cap L \subseteq L(b_1, b_2, \ldots, b_k)$.

"⇐" Let $b_1, b_2, \ldots, b_k$ be a primitive system and let π be the orthogonal projection $\pi : \mathrm{span}(L) \to \mathrm{span}(b_1, b_2, \ldots, b_k)^{\perp}$. By the proof of Proposition 3.2.3, $\pi(L)$ is a lattice of dimension $n - k$. The lattice $\pi(L)$ has basis $\pi(b_{k+1}), \pi(b_{k+2}), \ldots, \pi(b_n)$ with $b_{k+1}, b_{k+2}, \ldots, b_n \in L$.

We show that $L = L(b_1, b_2, \ldots, b_n)$. Let $b \in L$. From

$$\pi(b) \in L\big(\pi(b_{k+1}), \pi(b_{k+2}), \ldots, \pi(b_n)\big)$$

there is a $\bar{b} \in L(b_{k+1}, b_{k+2}, \ldots, b_n)$ with $\pi(\,\bar{b}\,) = \pi(b)$. Let

$$\pi(b) = \sum_{i=k+1}^{n} t_i \pi(b_i) \qquad \text{und} \qquad \bar{b} = \sum_{i=k+1}^{n} t_i b_i$$

Then $b - \bar{b} \in \mathrm{span}(b_1, b_2, \ldots, b_k)$. Since $b_1, b_2, \ldots, b_k$ form by assumption a primitive system, we have $b - \bar{b} \in L(b_1, b_2, \ldots, b_k)$. Thus $b \in L(b_1, b_2, \ldots, b_n)$.

■

The following notion, of a Minkowski-reduced basis, is not algorithmically motivated and is mentioned here only for completeness (for a procedure to obtaine a Minkowski-reduced basis see B. Helfrichs Arbeit [Helfrich85]):

Definition 3.2.23 (Minkowski-Reduced)
Let $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$ be an ordered basis for attice L; that is, the order of the vectors is fixed. The ordered basis is said to be Minkowski-reduced if for $i = 1, 2, \ldots, n$:

$$\|b_i\| = \min\left\{ \|b\| \;\middle|\; \begin{array}{l} b \in L \text{ and } (b_1, b_2, \ldots, b_{i-1}, b) \\ \text{is a primitive system for } L \end{array} \right\}$$

Definition 3.2.24 (Isometric Lattices)
Two lattices $L \subseteq \mathbb{R}^m$ and $\overline{L} \subseteq \mathbb{R}^m$ are isometric, when there is an isometric mapping $T : \mathbb{R}^m \to \mathbb{R}^n$ with $T(L) = \overline{L}$.

Let L and $\overline{L}$ be isometric lattices and let T be an isometric mapping with $T(L) = \overline{L}$ so that $b_1, b_2, \ldots, b_n$ is a basis for L. Then for the basis $\overline{b}_i := T(b_i)$, $i = 1, 2, \ldots, n$:

$$\langle b_i, b_j \rangle = \left\langle \overline{b}_i, \overline{b}_j \right\rangle \qquad \text{for } 1 \leq i, j \leq n$$

We say that two such bases are *isometric*. For the scalar product $\langle u, v \rangle = u^\mathsf{T} S v$ we have: The isometry class of a lattice basis $B = [b_1, b_2, \ldots, b_n]$ is characterized by the matrix $B^\mathsf{T} \cdot S \cdot B$. In particular, two lattices are isometric if and only if they have isometric bases. For example, in the case of the standard scalar product:

$$B := \begin{bmatrix} \sqrt{2} & 1/\sqrt{2} \\ 0 & \sqrt{3/2} \end{bmatrix} \qquad \overline{B} := \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad B^\mathsf{T} \cdot B = \overline{B}^\mathsf{T} \cdot \overline{B} = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

3.2.6 Orthogonal Systems

The goal of lattice basis reduction is, given an arbitrary lattice basis, obtain a basis of shortest possible vectors; that is, vectors as close as possible to mutually orthogonal.

Definition 3.2.25 (Orthogonal System, Orthogonal Projection π_i)
Let $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$ be an ordered lattice basis where $L = L(b_1, b_2, \ldots, b_n)$ is of rank n. Define

$$\pi_i : \mathbb{R}^m \to \operatorname{span}(b_1, b_2, \ldots, b_{i-1})^\perp$$

to be the orthogonal projection, that is, for all $b \in \mathbb{R}^m$:

$$\begin{aligned} \pi_i(b) &\in \operatorname{span}(b_1, b_2, \ldots, b_{i-1})^\perp \\ b - \pi_i(b) &\in \operatorname{span}(b_1, b_2, \ldots, b_{i-1}) \end{aligned}$$

We write $\widehat{b}_i := \pi_i(b_i)$.

We can obtain $\widehat{b}_1, \widehat{b}_2, \ldots, \widehat{b}_n$ by the Gram-Schmidt procedure:

(3.10) $$\widehat{b}_1 := b_1$$

(3.11) $$\widehat{b}_i := \pi_i(b_i) = b_i - \sum_{j=1}^{i-1} \mu_{i,j} \widehat{b}_j \qquad \text{for } i = 2, 3, \ldots, n$$

where the *Gram-Schmidt coefficients* $\mu_{i,j}$ are defined by:

$$\mu_{i,j} := \frac{\left\langle b_i, \widehat{b}_j \right\rangle}{\left\langle \widehat{b}_j, \widehat{b}_j \right\rangle} = \frac{\left\langle b_i, \widehat{b}_j \right\rangle}{||\widehat{b}_j||^2}$$

In particular, $\mu_{i,i} = 1$ and for $j > i$, $\mu_{i,j} = 0$. By definition (3.10) and (3.11) we can express the vector b_i in terms of the orthogonal system:

$$b_i = \widehat{b}_i + \sum_{j=1}^{i-1} \mu_{i,j} \widehat{b}_j \tag{3.12}$$

Then $\sum_{j=1}^{k} \mu_{i,j} \widehat{b}_j$ is the projection of b_i onto $\operatorname{span}(b_1, b_2, \ldots, b_k)$ and $\sum_{j=k+1}^{i} \mu_{i,j} \widehat{b}_j$ the projection of b_i onto $\operatorname{span}(b_1, b_2, \ldots, b_k)^{\perp}$. Moreover, for $i = 1, 2, \ldots, n$ we have

$$\operatorname{span}(b_1, b_2, \ldots, b_i) = \operatorname{span}\left(\widehat{b}_1, \widehat{b}_2, \ldots, \widehat{b}_i\right)$$

The description (3.12) of the basis vectors $b_1, b_2, \ldots, b_n$ can be expressed in matrix form:

$$[b_1, b_2, \ldots, b_n] = \left[\widehat{b}_1, \widehat{b}_2, \ldots, \widehat{b}_n\right] \cdot [\mu_{i,j}]^{\mathsf{T}}_{1 \le i,j \le n}$$

Note that if $m = n$ then $\widehat{B}$ is square with non-zero determinant and we have

$$\det B = \det \widehat{B} \cdot \det [\mu_{i,j}]^{\mathsf{T}}_{1 \le i,j \le n} = \det \widehat{B} = \prod_{i=1}^{n} ||\widehat{b}_i||$$

because $\det [\mu_{i,j}]^{\mathsf{T}}_{1 \le i,j \le n} = 1$ (upper triangular with 1's on the diagonal). The last equality holds because the columns of $\widehat{B}$ are mutually orthogonal. If $m > n$, then consider the mapping $T : \operatorname{span}(L) \to \mathbb{R}^n$ with

$$T(b_i) = \left[\mu_{i,1} ||\widehat{b}_1||, \quad \mu_{i,2} ||\widehat{b}_2||, \quad \ldots \quad , \mu_{i,n} ||\widehat{b}_n||\,\right]^{\mathsf{T}}$$

T is easily shown to be is isometric, so the matrix

$$[T(b_1), T(b_2), \ldots, T(b_n)] = \begin{bmatrix} ||\widehat{b}_1|| & 0 & \cdots & 0 \\ 0 & ||\widehat{b}_2|| & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & ||\widehat{b}_n|| \end{bmatrix} \cdot \begin{bmatrix} 1 & \mu_{2,1} & \mu_{3,1} & \cdots & \mu_{n,1} \\ 0 & 1 & \mu_{3,2} & & \mu_{n,2} \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \mu_{n,n-1} \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}$$

is a basis for a lattice in $\mathbb{R}^n$ that is isometric to $L(b_1, b_2, \ldots, b_n)$. We can now proceed as in the case $m = n$: Since $\det[\mu_{i,j}]^{\mathsf{T}}_{1 \le i,j \le n} = 1$, we have from the proof of Proposition 3.2.10:

$$\det L(b_1, b_2, \ldots, b_n) = \prod_{i=1}^{n} ||\widehat{b}_i|| \tag{3.13}$$

Proposition 3.2.26
Let $L = L(b_1, b_2, \dots, b_n)$ and let $\widehat{b}_1, \widehat{b}_2, \dots, \widehat{b}_n$ denote the Gram-Schmidt orthogonalization of $b_1, b_2, \dots, b_n$. Let $\Lambda(L)$ denote the length, using the ℓ_2 norm, of the shortest non-zero lattice vector in L. Then $\Lambda(L) \geq \min_i \left\|\widehat{b}_i\right\|_2$.

Proof. In the proof, we let $||\cdot||$ denote the ℓ_2 norm. Let $a \in L$ be a minimum length lattice vector in L. Since $a \in L$ we can write $a = \sum_{i=1}^n \lambda_i b_i$, where $\lambda_i \in \mathbb{Z}$ for $i = 1, 2, \dots, n$. Expressing each b_i in terms of the Gram-Schmidt orthogonalization we get:

$$a = \sum_{i=1}^{n} \lambda_i \sum_{j=1}^{i} \mu_{ij} \widehat{b}_j$$

Let k be the last index for which $\lambda_k \neq 0$, so $\lambda_j = 0$ for all $j > k$. Let us define λ_j^* for $1 \leq j \leq n$ by

$$\lambda_j^* = \sum_{i=j}^{n} \lambda_i \mu_{ij}$$

(Note that by choice of k, $\lambda_k^* = \lambda_k$.) Then $a = \sum_{j=1}^n \lambda_j^* \widehat{b}_j$. Since the $\widehat{b}_j$ are mutually orthogonal, we have

$$||a||^2 = \sum_{j=1}^{n} (\lambda_j^*)^2 \left\|\widehat{b}_j\right\|^2 \geq (\lambda_k)^2 \left\|\widehat{b}_k\right\|^2$$

Thus, $||a|| \geq |\lambda_k^*| \left\|\widehat{b}_k\right\| = |\lambda_k| \left\|\widehat{b}_k\right\|$. Since $\lambda_k \in \mathbb{Z} \setminus \{0\}$ we have $|\lambda_k| \geq 1$, and the proof is complete. ■

We define the orthogonality defect, a measure of how far the basis vectors are from being mutually orthogonal:

Definition 3.2.27 (Orthogonality Defect)
The orthogonality defect of a basis $b_1, b_2, \dots, b_n$ of the lattice L is:

$$\text{OrthDefect}(L) := \frac{\prod_{i=1}^n ||b_i||}{\det L},$$

Since $||b_i|| \geq ||\widehat{b}_i||$, the orthogonality defect is greater than or equal to 1. It is 1 precisely when the basis vectors are mutually orthogonal, and thus $b_i = \widehat{b}_i$ for $i = 1, 2, \dots, n$ (see (3.13)).

3.2.7 Quadratic Forms

In this section the scalar product always denotes the standard scalar product. A basis matrix $B = [b_1, b_2, \dots, b_n]$ yields the following *quadratic form* QF_B in the real variables $x_1, x_2, \dots, x_n$:

$$\text{QF}_B(x_1, x_2, \dots, x_n) := \sum_{1 \leq i,j \leq n} \langle b_i, b_j \rangle \, x_i x_j$$

This quadratic form QF_B is positive definite, that is, $\mathrm{QF}_B(x_1, x_2, \ldots, x_n) \geq 0$ and $\mathrm{QF}_B(x_1, x_2, \ldots, x_n) = 0$ if and only if $x_1 = x_2 = \ldots x_n = 0$. QF_B is positive definit implies:

$$\mathrm{QF}_B(x_1, x_2, \ldots, x_n) = \left\| \sum_{i=1}^{n} x_i b_i \right\|^2$$

and $\sum_{i=1}^{n} x_i b_i$ is the null vector exactly when $x_1 = x_2 = \ldots x_n = 0$. For integer $x_1, x_2, \ldots, x_n \mathrm{QF}_B$ takes the value of the square of the length of the corresponding lattice vector in $L(b_1, b_2, \ldots, b_n)$.

Conversely, for every positive definite, symmetrische, quadratic form

$$\mathrm{QF} = \sum_{1 \leq i,j \leq n} q_{ij} x_i x_j$$

there is a lattice basis $b_1, b_2, \ldots, b_n$, so that $\langle b_i, b_j \rangle = q_{ij}$ for $1 \leq i, j \leq n$. Then every positive definit, symmetric matrix $(q_{ij}) \in M_{n,n}(\mathbb{R})$ can be written as $(q_{ij}) = B^{\mathsf{T}} B$ with $B \in M_{n,n}(\mathbb{R})$.

Two lattice bases $B, \overline{B}$ yield the same quadratic form $\mathrm{QF}_B = \mathrm{QF}_{\overline{B}}$, precisely when there is an isometric mapping that transforms B into $\overline{B}$. The quadratic, positive definite forms express uniquely the isometry classes of the lattice basis. The theory of lattice bases and positive definite forms is in this sense equivalent. The older contributions, of J.L. Lagrange, C.F. Gauß, C. Hermite, A. Korkine, G. Zolotareff und H. Minkowski, were expressed in terms of quadratic forms. Two quadratic forms

$$\mathrm{QF}_Q = \sum_{1 \leq i,j \leq n} q_{ij} x_i x_j \qquad \text{and} \qquad \mathrm{QF}_{\overline{Q}} = \sum_{1 \leq i,j \leq n} \overline{q}_{ij} x_i x_j$$

are *congruent*, when they can be transformed into one another through unimodular transformations, that is, there exists a matrix $U \in \mathrm{GL}_n(\mathbb{Z})$ with:

$$[q_{ij}]_{1 \leq i,j \leq n} = U^{\mathsf{T}} \left[\overline{q}_{ij}\right]_{1 \leq i,j \leq n} U$$

For example, for two bases B and $\overline{B}$ of the same lattice, the corresponding quadratic forms QF_B and $\mathrm{QF}_{\overline{B}}$ are congruent.

3.2.8 Dual and Whole Lattice

In this section the scalar product is the standard scalar product. We define the dual lattice:

Definition 3.2.28 (Dual (polar, reciprocal) Lattice)
Let L be a lattice. The dual (polar, reciprocal) lattice id defined as:

$$L^* := \{x \in \operatorname{span}(L) \mid \forall b \in L : \langle x, b \rangle \in \mathbb{Z}\}$$

Proposition 3.2.29
Let $L \subseteq \mathbb{R}^n$ be a lattice of full rank with basis matrix $B := [b_1, b_2, \ldots, b_n]$. Then $\left(B^{-1}\right)^T$ is a basis matrix of the dual lattice L^*. In particular, $(L^*)^* = L$.

Proof. Let

$$B^* := [b_1^*, b_2^*, \dots, b_n^*] := \left(B^{-1}\right)^{\mathsf{T}}$$

We must show that $L^* = L(B^*)$. We show both inclusions:

- $L(B^*) \subseteq L^*$: For the identity matrix I

$$I = B^{-1} \cdot B = \left(\left(B^{-1}\right)^{\mathsf{T}}\right)^{\mathsf{T}} \cdot B = (B^*)^{\mathsf{T}} \cdot B = \begin{bmatrix} \langle b_1^*, b_1\rangle & \langle b_1^*, b_2\rangle & \cdots & \langle b_1^*, b_n\rangle \\ \langle b_2^*, b_1\rangle & \langle b_2^*, b_2\rangle & \cdots & \langle b_2^*, b_n\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle b_n^*, b_1\rangle & \langle b_n^*, b_2\rangle & \cdots & \langle b_n^*, b_n\rangle \end{bmatrix}$$

  Thus $\langle b_i^*, b_j\rangle \in \{0,1\}$ for $i,j = 1,2,\dots,n$. For $x = \sum_{i=1}^n t_i b_i^* \in L(B^*)$ with $t_1, t_2, \dots, t_n \in \mathbb{Z}$ we have:

$$\langle x, b_j\rangle = \sum_{i=1}^n t_i \cdot \langle b_i^*, b_j\rangle \in \mathbb{Z} \qquad \text{for } j = 1,2,\dots,n$$

  Since $b_i^* \in \mathbb{R}^n = \operatorname{span}(L)$ for $i = 1,2,\dots,n$, it follows for all $x \in L(B^*)$, that $x \in L^*$.

- $L(B^*) \supseteq L^*$: For every $a \in L^*$ we must show that $a \in L(B^*)$. Since $b_1, b_2, \dots, b_n \in L$, we obtain from the definition of the dual lattice:

$$B^{\mathsf{T}} \cdot a = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} \cdot a = \begin{bmatrix} \langle b_1, a\rangle \\ \langle b_2, a\rangle \\ \vdots \\ \langle b_n, a\rangle \end{bmatrix} \in \mathbb{Z}^n$$

  Further,

$$a = E \cdot a = \left(B \cdot B^{-1}\right)^{\mathsf{T}} \cdot a = \left(B^{-1}\right)^{\mathsf{T}} \cdot B^{\mathsf{T}} \cdot a = B^* \cdot \underbrace{\left(B^{\mathsf{T}} \cdot a\right)}_{\in \mathbb{Z}^n}$$

  Let $t_i := \langle b_i, a\rangle \in \mathbb{Z}$ for $i = 1,2,\dots,n$. Then a can be expressed as

$$a = \sum_{i=1}^n t_i b_i^*$$

  and $a \in L(B^*)$.

Moreover, $(L^*)^* = L$, since the operations of inverting and transposition commute. ■

Definition 3.2.30 (Self-Dual Lattice)
A lattice L is called self-dual when $L = L^*$.

For example, $\mathbb{Z}^n$ is a self-dual lattice. To conlcude this section, we define a whole lattice:

Definition 3.2.31 (Whole Lattice)
A lattice L is called whole when $\langle a, b\rangle \in \mathbb{Z}$ for all $a, b \in L$.

Proposition 3.2.32
For every whole lattice L, $L \subseteq L^* \subseteq \frac{1}{\det L^2} L$.

Proof. The proof is left to the reader. ■

3.3 Length- and Weight- Reduced Lattice Bases

In this section we define two algorithmically motivated types of reducedness: length reduced and weight reduced lattice bases.

Definition 3.3.1 (Length Reduced Basis)
The ordered basis $b_1, b_2, \ldots, b_n$ is length reduced when $|\mu_{i,j}| \leq \frac{1}{2}$ for $1 \leq j < i \leq n$.

Proposition 3.3.2
For every ordered, length reduced basis $b_1, b_2, \ldots, b_n$:

$$||b_i||^2 \leq ||\widehat{b}_i||^2 + \frac{1}{4}\sum_{j=1}^{i-1} ||\widehat{b}_j||^2 \qquad \textit{for } i = 1, 2, \ldots, n$$

Proof. ¿From Equation (3.12) on Page 44 we have for $i = 1, 2, \ldots, n$:

$$b_i = \widehat{b}_i + \sum_{j=1}^{i-1} \mu_{i,j}\widehat{b}_j$$

The vectors $\widehat{b}_1, \widehat{b}_2, \ldots, \widehat{b}_n$ of the orthogonal system are mutually orthogonal, so it follows that:

$$||b_i||^2 = \left\|\widehat{b}_i\right\|^2 + \sum_{j=1}^{i-1} \mu_{i,j}^2 ||\widehat{b}_j||^2$$

Since the basis is by assumption length reduced, we have $|\mu_{i,j}| \leq \frac{1}{2}$, whence the Proposition follows. ■

Algorithm 3.3.1 transforms a given lattice basis into a length reduced basis for the same lattice. To prove correctness of the length reduction algorithm we consider the basis vectors expressed in

Algorithm 3.3.1 Length Reduction

```
INPUT:   Ordered Lattice Basis $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$

  1. FOR $i = 2, 3, \ldots, n$ DO
             FOR $j = i-1, i-2, \ldots, 1$ DO
                   $b_i := b_i - \lceil \mu_{i,j} \rfloor \cdot b_j$
             END for j
     END for i

OUTPUT:   Length Reduced Basis $b_1, b_2, \ldots, b_n$
```

terms of their coordinates in the orthogonal system:

$$\begin{array}{cccccccccc}
 & & & \widehat{b}_1 & \widehat{b}_2 & \widehat{b}_3 & & \widehat{b}_{n-1} & \widehat{b}_n & \\
b_1 & = & (& 1 & 0 & 0 & \cdots & 0 & 0 &) \\
b_2 & = & (& \mu_{2,1} & 1 & 0 & & 0 & 0 &) \\
b_3 & = & (& \mu_{3,1} & \mu_{3,2} & 1 & & 0 & 0 &) \\
\vdots & = & (& \vdots & & & \ddots & 0 & \vdots &) \\
b_{n-1} & = & (& \mu_{n-1,1} & \mu_{n-1,2} & \mu_{n-1,3} & & 1 & 0 &) \\
b_n & = & (& \mu_{n,1} & \mu_{n,2} & \mu_{n,3} & & \mu_{n,n-1} & 1 &)
\end{array}$$

We observe that:

- The step $b_i := b_i - \lceil \mu_{i,j} \rfloor b_j$ causes $\mu_{i,j}^{\text{new}} := \mu_{i,j}^{\text{old}} - 1 \cdot \lceil \mu_{i,j}^{\text{old}} \rfloor$.
- In particular, $\left|\mu_{i,j}^{\text{new}}\right| \leq \frac{1}{2}$, and the $\mu_{i,\nu}$ remain unchanged for $\nu > j$.

This is a weak form of reduction.

Definition 3.3.3 (Weight Reduced Basis)
The ordered basis $b_1, b_2, \ldots, b_n$ is weight reduced when:

a) $\dfrac{|\langle b_i, b_j \rangle|}{\|b_j\|^2} \leq \dfrac{1}{2}$ *for* $1 \leq j < i \leq n$

b) $\|b_i\| \leq \|b_{i+1}\|$ *for* $i = 1, 2, \ldots, n-1$

Note that the first requirement does *not* refer to the Gram-Schmidt coefficients

$$\mu_{i,j} = \frac{\left\langle b_i, \widehat{b}_j \right\rangle}{\|\widehat{b}_j\|^2}$$

Property b) of weight reducedness says that the basis vectors are in ascending order of length:

$$||b_1|| \leq ||b_2|| \leq ||b_3|| \leq \cdots \leq ||b_{n-1}|| \leq ||b_n||$$

Property a) is equivalent to

$$||b_i|| \leq ||b_i \pm b_j|| \qquad \text{for } 1 \leq j < i \leq n$$

From

$$||b_i \pm b_j||^2 = \langle b_i \pm b_j, b_i \pm b_j \rangle = ||b_i||^2 \pm 2 \cdot \langle b_i, b_j \rangle + ||b_j||^2$$

it follows that

$$||b_i||^2 \leq ||b_i \pm b_j||^2 \quad \Longleftrightarrow \quad \pm \langle b_i, b_j \rangle \leq \tfrac{1}{2} \cdot ||b_j||^2 \quad \Longleftrightarrow \quad |\langle b_i, b_j \rangle| \leq \tfrac{1}{2} \cdot ||b_j||^2$$

In Chapter 5 we will consider the special case $n = 2$, in which the basis consists of two lattice vectors.

Algorithm 3.3.2 Weight Reduction

```
INPUT:   Lattice Basis $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$

  1. $F$ :=true
  2. WHILE ($F$) DO
       2.1. Order $b_1, b_2, \ldots, b_n$ so that $||b_1|| \leq ||b_2|| \leq \cdots \leq ||b_n||$
       2.2. $F$ :=false
       2.3. FOR $i = 1, 2, \ldots, n$ DO
                 FOR $j = 1, 2, \ldots, i-1$ DO      /* reduction step */
                      $r := \langle b_i, b_j \rangle \cdot ||b_j||^{-2}$
                      IF $|r| > \frac{1}{2}$ THEN $b_i := b_i - \lceil r \rfloor b_j$ and $F$ :=true
                 END for j
            END for i
     END while

OUTPUT:   Weight Reduced Basis $b_1, b_2, \ldots, b_n$
```

Proposition 3.3.4
Every lattice has a weight reduced basis.

The proof of the Proposition is immediate from the correctness of Algorithm 3.3.2, which transforms an arbitrary lattice basis into a weight reduced basis for the same lattice. The correctness of the algorithm follows from the two observations:

- It is clear by inspection that the ouptut is a weight reduced basis.
- The algorithm terminates, since every reduction step reduces the length of one basis vector while leaving the remaining basis vectors unchanged, and every lattice is discrete.

In contrast with Algorithm 3.3.1 for length reduction, the weight reduction procedure exchanges the sequence of the vectors, and in particular the shortest basis vector is the first one. However, the algorithm is not efficient. In the following chapters we will study stronger notions of reduction: LLL reduction in chapter 6 and HKZ- and β-reduction in Chapter ??.

3.4 Examples

In this section we describe some lattices and their respective bases. The scalar product is the standard one. The first successive minimum λ_1 is the length of the shortest non-zero lattice vector (a formal definition follows later).

For the lattice

$$A_n := \left\{ (x_0, x_1, \dots, x_n) \in \mathbb{Z}^{n+1} \;\middle|\; \sum_{i=0}^{n} x_i = 0 \right\}$$

the following row vectors form a basis:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n-1} \\ b_n \end{bmatrix} := \begin{bmatrix} -1 & +1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & +1 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & \cdots & 0 & -1 & +1 & 0 \\ 0 & \cdots & 0 & 0 & -1 & +1 \end{bmatrix}$$

Clearly, $L(b_1, b_2, \dots, b_n)$ is a sub-lattice of A_n, since $b_1, b_2, \dots, b_n \in A_n$ and they are linearly independent. Conversely, let $x = (x_0, x_1, \dots, x_n) \in A_n$ be an arbitrary element of A_n. For $i = n, n-1, \dots, 2$, subtract the vector b_i from x, until the $(i+1)$th component is zero. Only the first two entries of the vector x' are non-zero, and it is in A_n. Moreover, $x'_0 = -x'_1$, and the vector is an integer multiple of b_1.

The lattice

$$D_n := \left\{ (x_1, x_2, \dots, x_n) \in \mathbb{Z}^n \;\middle|\; \sum_{i=0}^{n} x_i \equiv 0 \pmod 2 \right\}$$

has a basis comprised of the following row vectors:

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_{n-1} \\ b_n \end{bmatrix} := \begin{bmatrix} +2 & 0 & 0 & 0 & \cdots & 0 \\ +1 & -1 & 0 & 0 & \cdots & 0 \\ 0 & +1 & -1 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & \cdots & 0 & +1 & -1 & 0 \\ 0 & \cdots & 0 & 0 & +1 & -1 \end{bmatrix}$$

Alternatively, $b_1' = (-1, -1, 0, \dots, 0)$. Since $b_1 = -b_1' + b_2$ one obtains the same lattice. Clearly $L(b_1, b_2, \dots, b_n)$ is a sublattice of D_n, since $b_1, b_2, \dots, b_n \in D_n$ and they are linearly independent. Conversely, let $x = (x_1, x_2, \dots, x_n) \in D_n$ be an arbitrary vector in D_n. For $i = n, n-1, \dots, 2$, remove from x the vector b_i until the ith component is 0. The only non-zero entry in the vector is the first one, and the vector lies in D_n. Thus $x_1 \equiv 0 \pmod 2$, and the vector is an integer multiple of b_1. Note that $\det D_n = 2$. Clearly there is no lattice vector shorter than the basis vectors, so $\lambda_1(D_n) = \sqrt{2}$.

Let $n \equiv 0 \bmod 4$. The lattice

$$E_n := \left\{ (x_1, x_2, \dots, x_n) \in \mathbb{Z}^n \;\middle|\; \begin{array}{ll} \sum_{i=0}^{n} x_i \equiv 0 & \pmod 4 \text{ and} \\ x_j \equiv x_{j+1} & \pmod 2 \text{ for } 1 \le j < n \end{array} \right\}$$

has a basis comprised of the following row vectors:

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_{n-1} \\ b_n \end{bmatrix} := \begin{bmatrix} +4 & 0 & 0 & 0 & \cdots & 0 \\ +2 & -2 & 0 & 0 & \cdots & 0 \\ 0 & +2 & -2 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & \cdots & 0 & +2 & -2 & 0 \\ +1 & \cdots & +1 & +1 & +1 & +1 \end{bmatrix}$$

Clearly $L(b_1, b_2, \dots, b_n)$ is a sub-lattice of E_n, since $b_1, b_2, \dots, b_n \in E_n$ and they are linearly independent. Conversely, let $x = (x_1, x_2, \dots, x_n) \in E_n$ be an arbitrary vector in E_n. Consider $x' := x - x_n b_n \in E_n$, whose last component is 0. Since $x' \in E_n$ and the last component is 0, all its entries are even. For $i = n-1, n-2, \dots, 2$, remove from x' the vector b_i until the ith component is 0. The only non-zero entry of the resulting vector is the first one, and the vector is in E_n. Thus $x_1 \equiv 0 \pmod 4$, and the vector is an integer multiple of b_1. Since $\det E_n = 2^n$ we have:

$$\lambda_1(E_n)^2 = \begin{cases} 4 & \text{if } n = 4 \\ 8 & \text{else} \end{cases}$$

For $n = 4$, $u := (1, 1, 1, 1)$ is a vector in E_4 with $\|u\|^2 = 4$; for $n > 4$, $v := (2, -2, 0, \dots, 0)$ is a vector in E_n with $\|v\|^2 = 8$. Are there shorter lattice vectors? (Note that for all lattice vectors $x \in E_n$, $x_{n-1} \equiv x_n \pmod 2$).

Let $a = (a_1, a_2, \dots, a_n) \in \mathbb{Z}^n \setminus \{0\}$. Consider the lattice of integer vectors orthognal to a:

$$L_a := \operatorname{span}(a)^\perp \cap \mathbb{Z}^n = \{ t \in \mathbb{Z}^n \mid \langle a, t \rangle = 0 \}$$

We show:

$$\det L_a = \frac{\|a\|}{\gcd(a_1, a_2, \dots, a_n)}$$

The lattice L_a clearly has dimension $n - 1$. Let $c_2, c_3, \dots, c_n$ be a basis for L_a. Since

$$\operatorname{span}(L_a) \cap \mathbb{Z}^n = L_a$$

the vectors of the basis form a primitive system for the lattice $\mathbb{Z}^n$ and by Proposition 3.2.22 there exists a vector $c_1 \in \mathbb{Z}$ with:

$$L(c_1, c_2, \ldots, c_n) = \mathbb{Z}^n$$

The entries of the vector c_1 are relatively prime, since c_1 is a primitive vector with respect to $\mathbb{Z}^n$. The part of c_1 orthogonal to L_a is

$$\frac{\langle c_1, a \rangle}{\|a\|^2} \cdot a$$

and has length

$$\left\langle \frac{\langle c_1, a \rangle}{\|a\|^2} \cdot a, \frac{\langle c_1, a \rangle}{\|a\|^2} \cdot a \right\rangle^{\frac{1}{2}} = \frac{\langle c_1, a \rangle}{\|a\|^2} \cdot \langle a, a \rangle^{\frac{1}{2}} = \frac{\langle c_1, a \rangle}{\|a\|}$$

We obtain from the geometric interpretation of the lattice determinant as the volume of the basic block ("surface area $\det L_a$ times height $\frac{|\langle c_1, a \rangle|}{\|a\|}$"):

$$\det \mathbb{Z}^n = 1 = \det L_a \cdot \frac{|\langle c_1, a \rangle|}{\|a\|}$$

that $|\langle c_1, a \rangle|$ is the least positive whole number in the principal ideal $\sum_{i=1}^{n} \mathbb{Z} a_i = \mathbb{Z} \cdot \gcd(a_1, a_2, \ldots, a_n)$, for which there exists a $\bar{c}_1 \in \mathbb{Z}^n$ with

$$\langle \bar{c}_1, a \rangle = \gcd(a_1, a_2, \ldots, a_n)$$

and $c_1 = k \cdot \bar{c}_1$ for some $k \in \mathbb{Z}$. Since the entries of the vector c_1 are relatively prime, it follows that $|k| = 1$. We thus obtain

$$\langle c_1, a \rangle = \gcd(a_1, a_2, \ldots, a_n),$$

and the claim follows.

Chapter 4

Sucessive Minima, Minkowski's Theorems, and the Hermite Constant

In this chapter we define the successive minima of a lattice. We present two well known theorems of Minkowski. We define the Hermite constant γ_n and present lower and upper bounds for this value. Unless otherwise state, the scalar product is the standard one: $\langle \cdot, \cdot \rangle$ and $||x|| = \sqrt{\langle x, x \rangle}$ denotes the Euclidean norm.

4.1 Successive Minima and the First Minkowski Theorem

In chapter 3.4 we informally introduced the first successive minimum. In general, the successive minima are defined by:

Definition 4.1.1 (Successive Minima $\lambda_1, \lambda_2, \ldots, \lambda_n$)
Let $||\cdot||$ be an arbitrary norm. For every lattice $L \subseteq \mathbb{R}^m$ of rank n the successive minima $\lambda_1, \lambda_2, \ldots, \lambda_n$ with respect to the norm $||\cdot||$ are defined as:

$$\lambda_i = \lambda_i(L) := \inf \left\{ r > 0 \;\middle|\; \begin{array}{l} \textit{There are } i \textit{ linearly independent} \\ \textit{vectors } c_1, c_2, \ldots, c_i \in L \\ \textit{with } ||c_j|| \leq r \textit{ for } j = 1, 2, \ldots, i \end{array} \right\} \qquad \textit{for } i = 1, 2, \ldots, n$$

The definition of successive minima is due to H. Minkowski. Figure 4.1.1 illustrates the concept for a lattice $L(a.b)$: The first successive minimum with respect to the Euclidean norm is the vector x.

$\underline{\lambda_1} \leq \lambda_2 \leq \cdots \leq \lambda_n$. The successive minima with respect to a Euclidean norm $||u|| := \sqrt{\langle u, u \rangle}$ are geometric lattice invariants; that is, these values remain unchanged under isometric

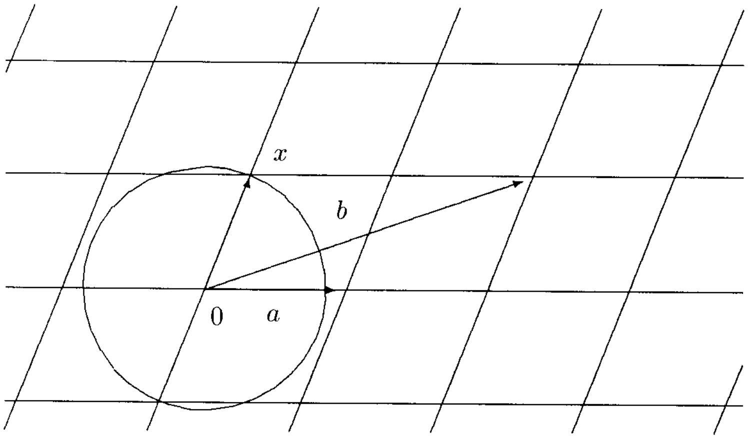

Figure 4.1.1: Example of the first successive minimum $\lambda_1(L(a,b))$

transformations of the lattice. For every lattice basis $b_1, b_2, \ldots, b_n$, for $i = 1, 2, \ldots, n$:

$$\max_{j=1,2,\ldots,i} \|b_j\| \geq \lambda_i$$

The successive minima yield a measure of the reducedness of a lattice basis. A basis is "reduced", when the values $\frac{\|b_i\|}{\lambda_i}$ for $i = 1, 2, \ldots, n$ are "small" ("close" to 1). The vectors of a reduced basis are nearly orthogonal. In general there is no basis $b_1, b_2, \ldots, b_n$ with $\|b_i\| = \lambda_i$ for $i = 1, 2, \ldots, n$. Consider for example the lattice

$$L := \mathbb{Z}^n + \mathbb{Z}\underbrace{\left(\tfrac{1}{2}, \ldots, \tfrac{1}{2}\right)}_{n}^{\mathsf{T}}$$

and the Euclidean norm. For $n \geq 5$, $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 1$ and the canonical unit vectors (the only vectors with length 1) do not form a basis.

The successive minima depend on the underlying norm. In particular, consider the first successive minimum in the Euclidean norm

$$\|L\| := \lambda_1(L) = \min\{\|b\| \ : \ b \in L \setminus \{0\}\}$$

and in the sup-norm:

$$\|L\|_\infty := \lambda_{1,\infty}(L) = \min\{\|b\|_\infty \ : \ b \in L \setminus \{0\}\}$$

For lattice $L \subseteq \mathbb{R}^m$ it follows from $\|x\|_\infty \leq \|x\| \leq \sqrt{n} \cdot \|x\|_\infty$ for all $x \in \mathbb{R}^m$, that:

$$\lambda_{1,\infty}(L) \leq \lambda_1(L) \leq \sqrt{n} \cdot \lambda_{1,\infty}(L)$$

The quantity $\|L\|_\infty$ is not a geometric invariant. However, we have the following tight bound:

Proposition 4.1.2 (Minkowski 1896)
Let $L \subseteq \mathbb{R}^m$ be a lattice of rank n. Then $\|L\|_\infty \leq (\det L)^{\frac{1}{n}}$.

This bound is tight since $||\mathbb{Z}^n||_\infty = 1 = (\det \mathbb{Z}^n)^{\frac{1}{n}}$.

We first give the proof sketch appearing in [Lovász86] for the case $n = m$. Let Q denote the cube

$$Q := \left\{ x \in \mathbb{R}^n \ : \ ||x||_\infty \leq \tfrac{1}{2}(\det L)^{1/n} \right\}$$

Then Q has n-dimensional volume $\det L$. Consider the cubes $Q + b$, where $b \in L$. If all these cubes were pairwise disjoint, then the density of their union would be less than 1; however, a simple counting argument shows that it is exactly one. Thus, there exist $b_1, b_2 \in L$ such that $(Q + b_1) \cap (Q + b_2) \neq \emptyset$. Let $y \in Q + b_1 \cap Q + b_2$. Then $||y - b_1||_\infty, ||b_2 - y||_\infty \leq \frac{1}{2}(\det L)^{1/n}$. It follows from the triangle inequality that

$$||b_2 - b_1||_\infty \leq ||y - b_1||_\infty + ||b_2 - y||_\infty \leq (\det L)^{1/n}$$

Since $b_2 - b_1 \in L$ we are done. As a simple corollary, since $||b||_2 \leq \sqrt{n}\, ||b||_\infty$, we have that for every full dimensional lattice L, there exists $b \in L$ with $||b||_2 \leq \sqrt{n}(\det L)^{1/n}$. (The same follows from Proposition 4.1.2 for the general case $n \leq m$.)

Following the proof sketch, we can find $b \in L$ with $||b||_\infty \leq (\det L)^{1/n}$ by searching for $b' \in L$ such that $Q + b'$ intersects Q. For simplicity, let us assume $\det A = 1$. If $L = L(a_1, a_2, \ldots, a_n)$, then we "only" need to consider vectors $b = \lambda_1 a_1 + \cdots + \lambda_n a_n$ where

$$|\lambda_i| = |\det [a_1, a_2, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n]| \leq 2^{\ell(A)}.$$

(The equality comes from Cramer's rule. The inequality requires proof. The key points are that, assuming $||b||_\infty < ||a_i||_\infty$ (since otherwise there is no need to search), $||b||_1 < n\, ||a_i||_1$; and

$$|\det [a_1, a_2, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n]| \leq ||b||_2 \prod_{j \neq i} ||a_j||_2 \leq ||b||_1 \prod_{j \neq i} ||a_j||_1 \leq n \prod_{j=1}^{n} ||a_j||_1$$

The rest of the proof follows from arguments similar to those in the proof of Lemma 1.1.1.) This is exponential even if the entries of A are restricted to $\{0, \pm 1\}$. If the dimension n is fixed then a shortest vector can be found in polynomial time ([Lenstra83]). Later, we will see that we can find an exponential approximation to the shortest vector using the LLL algorithm when n is not fixed. In contrast, recall that finding the shortest vector with respect to the ∞-norm is $\mathcal{NP}$-hard; and that finding the shortest vector with respect to the ℓ_2-norm is $\mathcal{NP}$-hard with respect to randomized reductions [Ajtai98].

Before proving Proposition 4.1.2, we present a result of H.F. Blichfeldt [Blich14]:

Lemma 4.1.3 (Blichfeldt 1914)
Let $L \subseteq \mathbb{R}^m$ be a lattice of full rank and let $Q \subseteq \mathbb{R}^m$ be compact with $\mathrm{vol}(Q) \geq \det L$. Then there exists $b \in L \setminus \{0\}$ with $Q \cap (Q + b) \neq \emptyset$, that is, there exists $x, y \in Q$ with $x - y \in L \setminus \{0\}$.

Proof. For $i \in \mathbb{N}$ the sets $\left(1 + \frac{1}{i}\right) Q$ and $\left(1 + \frac{1}{i}\right) Q + b_i$ with $b_i \in L \setminus \{0\}$ are not pairwise disjoint, since the volume of $\left(1 + \frac{1}{i}\right) Q$ exceeds that of the basic block. For every i there is a $b_i \in L \setminus \{0\}$, so that the following intersection is non-empty and we can therfore choose from the intersection y_i:

$$y_i \in \left(1+\tfrac{1}{i}\right) Q \cap \left[\left(1+\tfrac{1}{i}\right) Q + b_i\right] \qquad\qquad i = 1, 2, \dots$$

Since Q is compact, the sequence $(y_i)_{i \in \mathbb{N}}$ has a limit point $y \in Q$. Let $y \in Q$ be a boundary point of a subsequence $\left(y_{\alpha(i)}\right)_{i \in \mathbb{N}}$. The sequence $\left(b_{\alpha(i)}\right)_{i \in \mathbb{N}} \subseteq L$ converges to y. The sequence $\left(b_{\alpha(i)}\right)_{i \in \mathbb{N}} \subseteq L$ is bounded and runs through only finitely many lattice points. At least one lattice point $b \in L \setminus \{0\}$ appears infinitely often. It follows that $y \in Q \cap (Q + b)$. ■

Proof (of Proposition 4.1.2). We first consider the case in which L is full dimensional, that is, $n = m$. We apply Lemma 4.1.3 to the set

$$Q := \left\{ x \in \mathbb{R}^m \ : \ \|x\|_\infty \leq \tfrac{1}{2} (\det L)^{\frac{1}{m}} \right\}$$

Q is an m-dimensional cube with side length $(\det L)^{\frac{1}{m}}$. Then $\operatorname{vol}(Q) = \det L$. By Lemma 4.1.3 there exists a $b \in L \setminus \{0\}$ and $y \in Q \cap (Q + b)$. Since $y, y - b \in Q$ we have:

$$\|y\|_\infty \leq \tfrac{1}{2} (\det L)^{\frac{1}{m}}$$
$$\|y - b\|_\infty \leq \tfrac{1}{2} (\det L)^{\frac{1}{m}}$$

It follows from the triangle inequality that:

$$\|b\|_\infty \leq \|y\|_\infty + \|y - b\|_\infty \leq (\det L)^{\frac{1}{m}}$$

The case $n < m$ reduces to the case $n = m$. For $I = (i_1, i_2, \dots, i_n)$ with $1 \leq i_1 < i_2 < \cdots < i_n \leq m$ let:

$$\varphi_I(x_1, x_2, \dots, x_m) := (x_{i_1}, x_{i_2}, \dots, x_{i_n})$$

For some choice of I $\operatorname{span}(\varphi_I(\operatorname{span}(L)) = \mathbb{R}^n$.

Claim 4.1.4
$\det \varphi_I(L) \leq \det L$.

Proof. Let B be the $m \times n$ matrix with columns $b_1, b_2, \dots, b_n$, and let $\widehat{B}$ be the $m \times n$ matrix with columns $\widehat{b}_1, \widehat{b}_2, \dots, \widehat{b}_n$. Then there exists an $n \times n$ matrix T with determinant ± 1 such that $\widehat{B} = BT$. Then

$$\begin{aligned} \det B^{\mathsf{T}} B &= \det \widehat{B}^{\mathsf{T}} \widehat{B} \\ &= \prod_{i=1}^{n} \|\widehat{b}_i\|^2 \\ &\geq \prod_{i=1}^{n} \left\|\varphi_I(\widehat{b}_i)\right\|^2 \\ &\geq \det\left(\varphi_I(\widehat{B})^{\mathsf{T}} \varphi_I(\widehat{B})\right) \end{aligned}$$

We conclude the proof of the claim by showing that $\det \varphi_I(\widehat{B})^{\mathsf{T}} \varphi_I(\widehat{B}) = \det \varphi_I(B)^{\mathsf{T}} \varphi_I(B)$. Let $f : \mathbb{R}^m \to \mathbb{R}^m$ be defined as follows. For $b \in \mathbb{R}^m$ the value of $f(b)$ is the vector in $\mathbb{R}^m$ that agrees with b on all the coordinates in the index set I (so $\varphi_I(f(b)) = \varphi_I(b)$) and is zero on all the coordinates not in I. Then $\|f(b)\| = \|\varphi_I(b)\|$ for all $b \in \mathbb{R}^m$, and in general, for all $x, y \in \mathbb{R}^m$, $\langle f(x), f(y)\rangle = \langle \varphi_I(x), \varphi_I(y)\rangle$. Thus,

$$\det \varphi_I(\widehat{B})^{\mathsf{T}} \varphi_I(\widehat{B}) = \det f(\widehat{B})^{\mathsf{T}} f(\widehat{B})$$
$$\det \varphi_I(B)^{\mathsf{T}} \varphi_I(B) = \det f(B)^{\mathsf{T}} f(B)$$

and it remains to prove that

$$\det f(\widehat{B})^{\mathsf{T}} f(\widehat{B}) = \det f(B)^{\mathsf{T}} f(B)$$

Now, since $\widehat{B} = BT$, we have $f(\widehat{B}) = f(BT) = f(B)T$ (we can zero out a given row before or after right-multiplication by T and obtain the same result). Thus,

$$\begin{aligned} \det f(\widehat{B})^{\mathsf{T}} f(\widehat{B}) &= \det((f(B)T)^{\mathsf{T}} f(B)T) \\ &= \det(T^{\mathsf{T}} f(B)^{\mathsf{T}} f(B)T) \\ &= \det f(B)^{\mathsf{T}} f(B) \end{aligned}$$

and the proof of the claim is complete. ■

Let $x \in L$ have sup-norm $\lambda_{1,\infty}(L)$. Write $x = (x_1, x_2, \dots, x_n)^{\mathsf{T}}$, and let j be such that $|x_j| = \|x\|_\infty$. Then there exists a choice for I such that $j \in I$ and $\varphi_I(L)$ is of full rank. For this choice of I:

$$\|L\|_\infty = \|x\|_\infty = \|\varphi_I(b)\|_\infty \le \left(\det \varphi_I(L)\right)^{\frac{1}{n}} \le (\det L)^{\frac{1}{n}}$$

■

We define:

Definition 4.1.5 (Convex, Null-Symmetric Set)
$S \subseteq \mathbb{R}^m$ is convex, if when $x, y \in S$ and $\xi \in [0,1]$ it is also the case that $\xi x + (1-\xi)y \in S$. S is called null-symmetric, or simply, symmetric, if $-x$ is in S whenever x is in S.

Proposition 4.1.2 with $n = m$ is a special case of the following theorem, commonly known as "Minkowski's Theorem for Convex Bodies."

Proposition 4.1.6 (Minkowski's First Theorem 1893)
Let $L \subseteq \mathbb{R}^m$ be a full dimensional lattice and $S \subseteq \mathbb{R}^m$ a convex, symmetric, compact set with $\mathrm{vol}(S) \ge 2^m \cdot \det L$. Then $|S \cap L| \ge 3$, that is, S contains at least two non-zero vectors $\pm y \in L$.

Proof. We take:

$$Q := \tfrac{1}{2}S = \left\{ \tfrac{1}{2} \cdot x \;\middle|\; x \in S \right\} \subseteq \mathbb{R}^m$$

Then $\mathrm{vol}(Q) = 2^{-m}\,\mathrm{vol}(S) \geq \det L$. By Blichfeldt's Lemma 4.1.3, there exists $b \in L \setminus \{0\}$ with:

$$\left(\tfrac{1}{2}S\right) \cap \left(\tfrac{1}{2}S + b\right) \neq \emptyset$$

Let y be in this intersection. Then $y \in \frac{1}{2}S$ and $y = x + b$ with $x \in \frac{1}{2}S$. Let $w = 2x$ and $z = -2y$. Then $w, z \in S$. Moreover, since S is convex, $\frac{1}{2}w + (1 - \frac{1}{2})z \in S$. Thus, $b = x - y \in S$. In particular, $\{0, \pm b\} \subseteq S \cap L$. ■

Proposition 4.1.6 applied to $S = \left\{x \in \mathbb{R}^m \ : \ \|x\|_\infty \leq (\det L)^{1/m}\right\}$ yields Proposition 4.1.2 for $n = m$, since $\mathrm{vol}(S) = 2^m \cdot \det L$. A further consequence of Proposition 4.1.6 is a proof G.L. Dirichlet's [Di1842] theorem regarding simultaneous approximation of real numbers by rationals discussed in Chapter 1:

Proposition 4.1.7 (Dirichlet 1842)
Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be real numbers and $\epsilon \in (0, \frac{1}{2})$. Then there exist integers $p_1, p_2, \ldots, p_n$ and q with $0 < q \leq \epsilon^{-n}$, so that:

$$\left|\alpha_i - \frac{p_i}{q}\right| \leq \frac{\epsilon}{q} \qquad \textit{for } i = 1, 2, \ldots, n$$

Proof. By Proposition 4.1.6 with $L = \mathbb{Z}^{n+1}$ and

$$S := \left\{(p_1, p_2, \ldots, p_n, q) \in \mathbb{R}^{n+1} \ : \ |q| \leq \epsilon^{-n}, \quad |p_i - q\alpha_i| \leq \epsilon \text{ for } i = 1, 2, \ldots, n\right\}$$

S is a rectangle with side length 2ϵ in the first n dimensions and $2\epsilon^{-n}$ in the last, so

$$\mathrm{vol}(S) = (2\epsilon)^n 2\epsilon^{-n} = 2^{n+1} \cdot \det \mathbb{Z}^{n+1}$$

S is convex, symmetric, and compact. By Proposition 4.1.6 there exists non-null $(p_1, p_2, \ldots, p_n, q) \in S \cap \mathbb{Z}^{n+1}$. Moreover, $q \neq 0$ since if $|p_i| \leq \epsilon < \frac{1}{2}$ and $p_i \in \mathbb{Z}$ we would have $(p_1, p_2, \ldots, p_n, q) = 0$. ■

Following [Lovász86], we may cast the problem of finding a good simultaneous diophantine approximation as an instance of the problem of finding a short vector in a lattice. Suppose we are given $\alpha_1, \alpha_2, \ldots, \alpha_n, \varepsilon \in \mathbb{Q}$ and $Q \in \mathbb{Z}$, $Q > 0$. Consider the matrix

$$A := \begin{bmatrix} 1 & 0 & 0 & \cdots & \alpha_1 \\ 0 & 1 & 0 & \cdots & \alpha_2 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & \alpha_n \\ 0 & \cdots & 0 & 0 & \varepsilon/Q \end{bmatrix}$$

and the lattice $L(A)$ generated by the columns of A. Every vector $b \in L(A)$ can be written as $b = Ap$, where $p = p_1, p_2, \dots, p_{n+1}^{\mathsf{T}} \in \mathbb{Z}^{n+1}$. Let $b \in L(A)$ be non-zero with $||b||_2 \leq \varepsilon$. Then $p_{n+1} \neq 0$. Assume without loss of generality that $p_{n+1} < 0$ and let $q = -p_{n+1}$. Then

$$|b_i| = |p_i - \alpha_i q| \leq \varepsilon \qquad \text{for } i = 1, 2, \dots, n$$

and

$$|b_{n+1}| = \frac{\varepsilon}{Q} q \leq \varepsilon$$
$$\Rightarrow q \leq Q$$

So if $b = Ap \in L(A)$ is non-zero with $||b|| \leq \varepsilon$, then the coordinates of p provide a solution to the given simultaneous diophantine approximation problem: $||b||_\infty \leq ||b||_2 \leq \varepsilon$. Recall that by Dirichelet's Theorem there exists a solution if $Q \geq \varepsilon^{-n}$. The LLL algorithm will permit us to find a solution in polynomial time provided $Q \geq 2^{n(n+1)/4}\varepsilon^{-n}$.

4.2 Hermite Constant and Critical Lattice

In this section we define the Hermite constant γ_n, for which we obtain upper and lower bounds. We study critical lattices. The Hermite constant γ_n is defined for the Euclidean norm:

Definition 4.2.1 (Hermite Constant γ_n)
For $n \in \mathbb{N}$, the Hermite constant γ_n is defined as:

$$\gamma_n := \sup \left\{ \frac{\lambda_1(L)^2}{(\det L)^{\frac{2}{n}}} \;\middle|\; L \subseteq \mathbb{R}^n \textit{ full dimensional lattice} \right\}$$

The first successive minimum in the definition is with respect to the Euclidean norm.

(For historical reasons the definition of γ_n is given inters of the sqare.) It suffices to consider the supremum, over all full dimensional lattices $L \subseteq \mathbb{R}^m$, where $\lambda_1(L)$ and $\det L$ are geometric invariants. Since

$$\frac{\lambda_1(L)^2}{(\det L)^{\frac{2}{n}}} = \frac{\lambda_1(\alpha L)^2}{(\det \alpha L)^{\frac{2}{n}}} \qquad \text{for } \alpha \in \mathbb{R} \setminus \{0\}$$

it suffices to consider the supremum over all full dimensional lattices $L \subseteq \mathbb{R}^m$ for which $\det L = 1$. Since the reduced bases of this lattice vary over a compact space of $\mathbb{R}^{n^2}$ variables, the suprememum is achieved, that is, we can define the Hermite constant as the maximum of the set. Thus $\gamma_1 = 1$.

Remark 4.2.2
Since $\lambda_1(L) \leq \sqrt{n} \cdot (\det L)^{\frac{1}{n}}$ it follows from Proposition 4.1.2 that $\gamma_n \leq n$.

In the following we improve this upper bound. We denote by

$$S_n(r) := \{x \in \mathbb{R}^n \ : \ \|x\| \leq r\}$$

the n dimensional ball with rRadius r centered at the origin. The volume of the n dimensional ball with radius 1 is

$$\text{vol}(S_n(1)) = \frac{\pi^{\frac{n}{2}}}{\Gamma\left(1+\frac{n}{2}\right)} = \frac{2 \cdot \pi^{\frac{n}{2}}}{n \cdot \Gamma\left(\frac{1}{2}n\right)} \tag{4.1}$$

The Gamma function is defined by $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$, $\Gamma(n+1) = n!$ for $n \in \mathbb{N}$ and in general for $x \in \mathbb{R}^+$:

$$\Gamma(x+1) = x \cdot \Gamma(x)$$

We obtain from this an upper bound for the Hermit constant γ_n:

Proposition 4.2.3

$$\gamma_n \leq \frac{4}{\text{vol}(S_n(1))^{\frac{2}{n}}} = \frac{4}{\pi} \cdot \Gamma\left(1+\frac{n}{2}\right)^{\frac{2}{n}} \leq \frac{2n}{e\pi} + \mathcal{O}(1) \approx 0,2342n + \mathcal{O}(1)$$

Proof. Let $L \subseteq \mathbb{R}^m$ be a full dimensional lattice with $\gamma_n = \frac{\lambda_1(L)^2}{(\det L)^{\frac{2}{n}}}$ and $\det L = 1$. We apply Proposition 4.1.6 to the ball $S_n(r)$. We choose radius:

$$r := \frac{2}{\text{vol}(S_n(1))^{\frac{1}{n}}}$$

Then $\text{vol}(S_n(r)) = 2^n$. By Proposition 4.1.6 there exists $b \in S_n(r) \cap L$ with $b \neq 0$. We obtain with (4.1):

$$\lambda_1(L) \leq \|b\| \leq r = \frac{2}{\text{vol}(S_n(1))^{\frac{1}{n}}} = \frac{2}{\sqrt{\pi}} \cdot \Gamma\left(1+\frac{n}{2}\right)^{\frac{1}{n}}$$

By Stirling's approximation [Knuth71, 1.2.11.2,Aufgabe 5]:

$$\Gamma(x+1) = \sqrt{2\pi x} \cdot \left(\frac{x}{e}\right)^x \left(1 + \mathcal{O}\left(\frac{1}{x}\right)\right) \qquad \text{for } x \in \mathbb{R}^+, \tag{4.2}$$

and $x = \frac{n}{2}$ follows from the fact that $\det L = 1$:

$$\begin{aligned}
\gamma_n &= \frac{\lambda_1(L)^2}{(\det L)^{\frac{2}{n}}} \\
&\leq \frac{4}{\pi} \cdot \left[\sqrt{\pi n}\left(\frac{n}{2e}\right)^{\frac{n}{2}} \left(1 + \mathcal{O}\left(\frac{1}{n}\right)\right)\right]^{\frac{2}{n}} \\
&= \frac{4n}{2e\pi} \cdot (n\pi)^{\frac{1}{n}} \cdot \left(1 + \mathcal{O}\left(\frac{1}{n}\right)\right)^{\frac{2}{n}}
\end{aligned}$$

Since $\lim_{n\to\infty} n^{\frac{1}{n}} = 1$, that is, $n^{\frac{1}{n}} = 1 + \mathcal{O}(1)$, we obtain:

$$\gamma_n \leq \frac{2n}{e\pi} + \mathcal{O}(1)$$

■

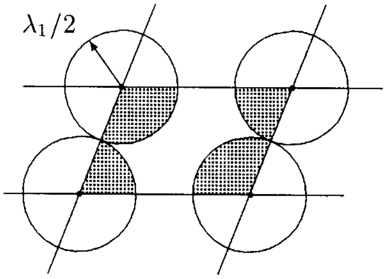

Figure 4.2.1: Illustration for the Proof of Proposition 4.2.3

The proof of Proposition 4.2.3 can be illustrated as follows (see Figure 4.2.1): Place a ball of radius $r := \frac{1}{2}\lambda_1$ on every point of the full dimenional lattice $L \subseteq \mathbb{R}^n$ This yields the gittertige??? sphere packing of L, defined as follows.

Definition 4.2.4 (Gitterartige Sphere Packing)
Let $M \subseteq \mathbb{R}^n$ be a non-empty discrete set and $r > 0$. The sphere packing for M and r is:

$$\{m + S_n(r) \mid m \in M\}$$

The sphere packing is called gitterartig, when for every pair of neighboring points $m_1, m_2 \in M$ the balls $m_1 + S_n(r)$ and $m_2 + S_n(r)$ share no interior point.

Let us consider the gitterartige sphere packing for L and $\frac{1}{2}\lambda_1$. The 2^n partial balls in a basic block of the lattice yield together one ball of radius $\frac{1}{2}\lambda_1$. It follows that:

$$\det L \geq \operatorname{vol}\left(S_n\left(\tfrac{1}{2}\lambda_1\right)\right) = \frac{\lambda_1^n \cdot \operatorname{vol}(S_n(1))}{2^n} \tag{4.3}$$

Definition 4.2.5 (Width of a Lattice)
The width of a full dimensional lattice $L \subseteq \mathbb{R}^n$ is the width of the gitterartige sphere packing for L, that is, the volume—volumenanteil??? of the ball of the gitterartige sphere packing in $\mathbb{R}^n$.

The width of the sphere packing of lattice L is:

$$\frac{\operatorname{vol}\left(S_n\left(\frac{1}{2}\lambda_1\right)\right)}{\det L} = \frac{\lambda_1^n}{\det L} \cdot \frac{\operatorname{vol}(S_n(1))}{2^n}$$

For fixed n, the width is maximal when the factor $\frac{\lambda_1^n}{\det L}$ is as large as possible. By the definition of the Hermite constant

$$\gamma_n = \max\left\{ \frac{\lambda_1(L')^2}{(\det L')^{\frac{2}{n}}} \;\middle|\; L' \subseteq \mathbb{R}^n \text{ full dimensional lattice} \right\}$$

we obtain that the width of the lattice $L \subseteq \mathbb{R}^n$ is maximal exactly when

$$\frac{\lambda_1^n}{\det L} \overset{!}{=} (\gamma_n)^{\frac{n}{2}} = \max\left\{ \frac{\lambda_1(L')^n}{\det L'} \;\middle|\; L' \subseteq \mathbb{R}^n \text{ full dimensional lattice} \right\}$$

We define the globally extreme, or critical lattice:

Definition 4.2.6 (Globally Extreme (or Critical) Lattice)
A full dimensional lattice $L \subseteq \mathbb{R}^n$ is called globally extreme, or critical, when

$$\frac{\lambda_1(L)^2}{(\det L)^{\frac{2}{n}}} = \gamma_n,$$

that is, $\frac{\lambda_1(L)^2}{(\det L)^{\frac{2}{n}}}$ is the absolute maximum for lattices of rank n.

A lattice is critical exactly when the ball of radius $\frac{1}{2}\lambda_1$ around the lattice points forms the widest gitterartige sphere packing of $\mathbb{R}^n$.

Definition 4.2.7 (Locally Extreme Lattice)
A full dimensional lattice $L = L(b_1, b_2, \ldots, b_n) \subseteq \mathbb{R}^n$ is said to be locally extreme when

$$\frac{\lambda_1(L)^2}{(\det L)^{\frac{2}{n}}}$$

does not increase with infinitesimally small changes to the basis vectors.

This property does not depend on the choice of basis for L. Every critical lattice is locally extreme, but the converse is not true. Die der Basis $b_1, b_2, \ldots, b_n$ zugeordnete Form $F(x_1, x_2, \ldots, x_n) := \sum_{i=1}^{n} \langle b_i, b_j \rangle\, x_i x_j$ nennt man dann *Extremform*???.

The upper bound $\gamma_n \leq \frac{2n}{e\pi} + \mathcal{O}(1)$ for the Hermite constant from Proposition 4.2.3 on page 62 was improved by H.F. Blichfeldt [Blich14]:

$$\gamma_n \leq \frac{2}{\pi} \cdot \Gamma\left(1 + \frac{n}{2}\right)^{\frac{2}{n}} \leq \frac{n}{e\pi} + o(n)\,. \tag{4.4}$$

This bound takes into consideration that in the proof of Proposition 4.2.3 only a very small portion of the space of the ball with radius $\frac{1}{2}\lambda_1$ overlaps and estimates this portion by $\left(\sqrt{2} + o(1)\right)^{-n}$ form above. For example, $\gamma_{10} \leq \frac{2}{\pi}(6!)^{0,2} \approx 2,373$. G.A. Kabatiansky und V.I. Levenshtein [KaLe78] showed in 1978, that:

$$\gamma_n \leq \frac{1,744}{2e\pi} n + \mathrm{o}(n) \approx 0,1021n + \mathrm{o}(n)$$

These improvements show that the first Minkowski Theorem for convex bodies (Proposition 4.1.6, page 59) is not optimal for balls. For a lower bound for the Hermit constant γ_n we have:

$$\gamma_n \geq \frac{1}{\pi}\left(1 + \frac{n}{2}\right) = \frac{n}{2e\pi} + \mathrm{o}(n)$$

This lower bound is obtained by application of the following theorem of H. Minkowski und E. Hlawka [Hlawka44] for balls $S := S_n(r)$. The proof is, however, not constructive, it shows only the existence of certain lattices; explicit constructions are not known.

Proposition 4.2.8 (Minkowski, Hlawka)
Let $S \subseteq \mathbb{R}^n$ have Jordan volume less than 1. Then there is a full dimensional lattice $L \subseteq \mathbb{R}^n$ with $\det L = 1$ *and* $(L \cap S) \setminus \{0\} \neq \emptyset$.

Proof. See [GrLek87, Theorem 1,Paragraph 19, Chapter 3]. ■

Taken together, we have for the Hermite constant the following estimates:

$$\frac{n}{2e\pi} + \mathrm{o}(n) \leq \gamma_n \leq \frac{n}{e\pi} + \mathrm{o}(n)$$

It is conjectured that γ_n grows monotonically as a function of n. In [GrLek87] (Paragraph 38, Chapter 6) the following estimates appear:

$$\frac{1}{2e\pi} \leq \liminf_{n\to\infty} \frac{\gamma_n}{n} \leq \limsup_{n\to\infty} \frac{\gamma_n}{n} \leq \frac{1}{e\pi}$$

It is not known if $\lim_{n\to\infty} \frac{\gamma_n}{n}$ exists.

The Hermite constants $\gamma_2, \gamma_3, \gamma_4, \gamma_5$ were obtained in the second half of the 1900's by A. Korkine und G. Zolotareff [KoZo1872, KoZo1873, KoZo1877]. In 1935, H.F. Blichfeldt [Blich35] obtained $\gamma_6, \gamma_7, \gamma_8$:

n	2	3	4	5	6	7	8
$(\gamma_n)^n$	$\frac{3}{4}$	2	4	8	$\frac{2^6}{3}$	$\frac{2^7}{2}$	2^8
$\gamma_n \Big/ \frac{2}{\pi} \cdot \Gamma\left(1 + \frac{n}{2}\right)^{\frac{2}{n}}$	0,907	0,887	0,907	0,892	0,907	0,918	0,949

The last row shows the relation γ_n divided by Blichfeldt's estimate (4.4). Blichfeldt's proof is complicated and was improved by G.L. Watson [Watson66] and N.M. Vetchinkin [Vetchin82]. For $n = 9, 10$ only the upper bounds $(\gamma_9)^9 \leq 2^9$ and $(\gamma_{10})^{10} \leq \frac{1}{3} \cdot 2^{10}$ are known.

For $n = 2, 3, \ldots, 8$ the critical lattice of rank n with $\lambda_1 = 1$ is uniquely determined up to isometry (without the requirement $\lambda_1 = 1$ they are uniquely determined up to isometry and scaling, hence similarity). This was shown by E.S. Barnes [Barnes59] and N.M. Vetchinkin [Vetchin82]. We show that these lattices have a basis $b_1, b_2, \ldots, b_n$ wih the property that:

$$\langle b_i, b_j \rangle = \begin{cases} 1 & \text{for } i = j \\ \frac{1}{2} & \text{for } |i-j| \leq 2 \text{ und } i \neq j \\ 0 & \text{for } |i-j| > 2 \end{cases} \tag{4.5}$$

The scalar products $\langle b_i, b_j \rangle$ determine the corresponding lattice basis $b_1, b_2, \ldots, b_n$ up to isometry. In the isometry class of lattice bases with the scalar products $\langle b_i, b_j \rangle$ described above, there is exactly one upper triangular matrix $[b_1, b_2, \ldots, b_n]$ with positive diagonal elements. The corresdponding lower triangular matrix $[b_1, b_2, \ldots, b_n]^\mathsf{T}$ has the following row vectors:

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \end{bmatrix} := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & \sqrt{\frac{3}{4}} & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & \frac{1}{\sqrt{12}} & \sqrt{\frac{2}{3}} & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{6}} & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{\frac{3}{8}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{2}} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{8}} & \sqrt{\frac{3}{8}} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} & \frac{3}{\sqrt{3}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \sqrt{\frac{2}{3}} & \frac{1}{\sqrt{12}} & \frac{3}{2} \end{bmatrix}$$

Let $L^{(n)} := (b_1, b_2, \ldots, b_n)$ for $n \leq 8$. Since $\|b_1\| = 1$ we have $\lambda_1 \leq 1$. Let $b := \sum_{i=1}^n t_i b_i$ with $t_1, \ldots, t_n \in \mathbb{Z}$ be an arbitrary non-zero lattice vector in $L^{(n)}$. We wish to show that $\|b\| \geq 1$. From

$$\|b\|^2 = \left\langle \sum\nolimits_{i=1}^n t_i b_i, \sum\nolimits_{j=1}^n t_j b_j \right\rangle = \sum_{i=1}^n t_i \left\langle b_i, \sum\nolimits_{j=1}^n t_j b_j \right\rangle = \sum_{i=1}^n t_i \cdot \sum_{j=1}^n \langle b_i, b_j \rangle \cdot t_j$$

it follws from (4.5) that $\langle b_i, b_j \rangle \in \left\{0, \frac{1}{2}, 1\right\}$ and $\|b_i\|^2 = 1$, so that we obtain

$$\|b\|^2 = \sum_{i=1}^n \left(t_i \langle b_i, b_i \rangle + \sum_{\substack{j=1 \\ j \neq i}}^n t_j \langle b_i, b_j \rangle \right) = \underbrace{\sum_{i=1}^n \left(t_i \langle b_i, b_i \rangle + 2 \sum_{j<i} t_j \langle b_i, b_j \rangle \right)}_{\in \mathbb{Z} \setminus \{0\}} \geq 1$$

Since for every vector $b \in L \setminus \{0\}$ we have $\|b\| \geq 1$, the vektor b_1 with $\|b_1\| = 1$ is one of the shortest, non-trivial lattice vectors. It follows that $\lambda_1 = 1$.

In particular, one sees from the construction of the vectors $b_1, b_2, \ldots,$ that the widest sphere packing in $\mathbb{R}^n$, $n \leq 8$, extends the widest sphere packing in $\mathbb{R}^{n-1}$. The above scheme cannot be extended to $n \geq 9$, since $[b_1, b_2, \ldots, b_9]$ is singular. The lattice $\sqrt{2} L^{(8)}$ is *self-dual*, that is,

$$\sqrt{2} L^{(8)} = \left(\sqrt{2} L^{(8)} \right)^*$$

We describe the construction of the above-mentioned critical lattice. First two definitions:

Definition 4.2.9 (Deep Hole)
Let L be a lattice. The point $x \in \operatorname{span}(L)$ is called a deep hole of the lattice L, when

$$\min\{\|x-y\| \,:\, y \in L\} = \max_{p \in \operatorname{span}(L)} (\min\{\|p-y\| \,:\, y \in L\})$$

Definition 4.2.10 (Laminated Lattice)
The lattice $L(b_1, b_2, \ldots, b_{n+1})$ is laminated with respect to $L(b_1, b_2, \ldots, b_n)$, when

$$b_{n+1} - \pi_{n+1}(b_{n+1}) \in \operatorname{span}(b_1, b_2, \ldots, b_n)$$

is a deep hole of the lattice $L(b_1, b_2, \ldots, b_n)$.

To construct the lattice $L^{(n)}$, we choose $(1, 0, \ldots, 0) \in \mathbb{R}^n$ and $b_2, b_3, \ldots, b_n$ so that, respectively $L(b_1, b_2, \ldots, b_i)$ is laminated with respect to $L(b_1, b_2, \ldots, b_{i-1})$ and $\|b_i\| = 1$ for $i = 2, 3, \ldots, n$. Figure 4.2.2 shows this construction for the two lattices $L^{(2)}$ and $L^{(3)}$.

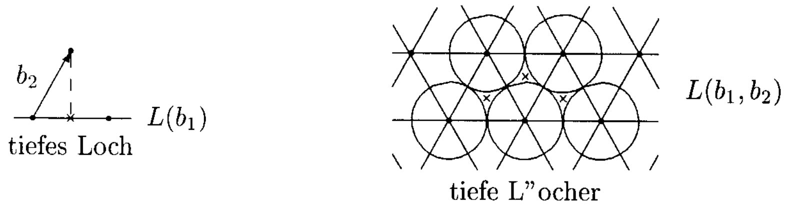

Figure 4.2.2: Construction of $L^{(2)}$ and $L^{(3)}$

The following inequality of H. Minkowski sharpens the inequaltiy $\lambda_1^2 \le \gamma_n (\det L)^{\frac{2}{n}}$, and holds for all lattices L of rank n.

Proposition 4.2.11 (Minkowski's Inequality)
For every lattice L of rank n,

$$\prod_{i=1}^{n} \lambda_i(L) \le (\gamma_n)^{\frac{n}{2}} \cdot \det L$$

Remark 4.2.12
Since for a critical lattice $(\gamma_n)^{\frac{n}{2}} \det L = \lambda_1^n$ and in general $\prod_{i=1}^n \lambda_i \ge \lambda_1^n$, for a critical lattice $\lambda_1 = \lambda_2 = \cdots = \lambda_n$.

Proof (of Proposition 4.2.11). Let $a_1, a_2, \ldots, a_n \in L$ be linearly independent vectors such that:

$$\|a_i\| = \lambda_i \qquad \text{for } i = 1, 2, \ldots, n$$

$L_1 = L(a_1, a_2, \ldots, a_n)$ is a sub-lattice of L. Choose basis $b_1, b_2, \ldots, b_n$ for L, so that for $L_2 := L$ Proposition 3.2.16 (page 37) yields: there exists an upper triangular matrix $T \in M_{n,n}(\mathbb{Z})$ with:

$$[b_1, b_2, \ldots, b_n] \cdot T = [a_1, a_2, \ldots, a_m]$$

For all $b \in L(b_1, b_2, \ldots, b_n)$ and $s = 1, 2, \ldots, n$:

$$b \notin L(b_1, b_2, \ldots, b_{s-1}) \quad \Longrightarrow \quad \|b\| \geq \lambda_s \tag{4.6}$$

Thus, from $b \notin L(b_1, b_2, \ldots, b_{s-1})$ and $b \in L$ it follows that $b \notin \operatorname{span}(b_1, b_2, \ldots, b_{s-1})$, and since T is upper triangular we have from Remark 3.2.17 on page 38:

$$\operatorname{span}(b_1, b_2, \ldots, b_{s-1}) = \operatorname{span}(a_1, a_2, \ldots, a_{s-1}),$$

so that $a_1, a_2, \ldots, a_{s-1}, b$ are linearly independent. For $i = 1, 2, \ldots, n$ we let

$$\bar{b}_i := \sum_{j=1}^{i} \frac{\mu_{i,j} \widehat{b}_j}{\lambda_j}$$

and consider the lattice $\bar{L} := L\left(\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_n\right)$. Claim:

$$\lambda_1\left(\bar{L}\right) \geq 1 \tag{4.7}$$

Let $b := \sum_{i=1}^{n} t_i \bar{b}_i$ be an arbitrary vector in $\bar{L} \setminus \{0\}$ and $s := \max_i \{i \mid t_i \neq 0\}$. Then,

$$\left\| \sum_{i=1}^{n} t_i \bar{b}_i \right\|^2 = \sum_{j=1}^{s} \left(\sum_{i=j}^{s} t_i \mu_{i,j} \right)^2 \frac{\|\widehat{b}_j\|^2}{\lambda_j^2} \geq \sum_{j=1}^{s} \left(\sum_{i=j}^{s} t_i \mu_{i,j} \right)^2 \frac{\|\widehat{b}_j\|^2}{\lambda_s^2},$$

so that from (4.6) and $t_s \neq 0$ it follows that:

$$\left\| \sum_{i=1}^{n} t_i \bar{b}_i \right\|^2 \geq \frac{1}{\lambda_s^2} \sum_{j=1}^{s} \left(\sum_{i=j}^{s} t_i \mu_{i,j} \cdot \|\widehat{b}_j\| \right)^2 = \frac{1}{\lambda_s^2} \left\| \sum_{i=1}^{s} t_i b_i \right\|^2 \geq 1$$

From $\det \bar{L} = \frac{\det L}{\prod_{i=1}^{n} \lambda_i}$, inequality (4.7) and the definition of the Hermite constant $\frac{\lambda_1^2}{(\det L)^{\frac{2}{n}}} \leq \gamma_n$ we get:

$$1 \leq \lambda_1\left(\bar{L}\right)^2 \leq \gamma_n \cdot \left(\det \bar{L}\right)^{\frac{2}{n}} = \gamma_n \cdot (\det L)^{\frac{2}{n}} \left(\prod_{i=1}^{n} \lambda_i \right)^{-\frac{2}{n}}$$

By raising to the power $\frac{n}{2}$ and multiplying by $\prod_{i=1}^{n} \lambda_i$ we get the assertion:

$$\prod_{i=1}^{n} \lambda_i(L) \leq (\gamma_n)^{\frac{n}{2}} \det L$$

■

The lattice determinant yields a lower bound on the product of the successive minima:

Proposition 4.2.13 (Minkowski's Second Theorem)
For every lattice L of rank n:

$$\prod_{i=1}^{n} \lambda_i \geq \det L$$

Proof. Let $a_1, a_2, \ldots, a_n$ be linearly independent lattice vectors with $||a_i|| = \lambda_i$ for $i = 1, 2, \ldots, n$. Since $L(a_1, a_2, \ldots, a_n)$ is a sub-lattice of L:

$$\det L(a_1, a_2, \ldots, a_n) \geq \det L \tag{4.8}$$

Moreover, by Hadamard's inequality:

$$\prod_{i=1}^{n} ||a_i|| \geq \det L(a_1, a_2, \ldots, a_n) \tag{4.9}$$

¿From the estimates (4.8) and (4.9) we get the claimed bound $\prod_{i=1}^{n} \lambda_i \geq \det L$. ■

4.3 Gauge Functions and Minkowski's Theorems

We introduce the guage function (see for example [GrLek87, Siegel89]) and formulate both of Minkowski's theorems for the lattice $\mathbb{Z}^n$ and generalize them. We first define the notion of a convex body.

Definition 4.3.1 (Convex Body)
A convex body $B \subseteq \mathbb{R}^n$ is a bounded, convex, open set.

The set ∂B for a convex body is the set of all points $p \in \mathbb{R}^m \setminus B$, so that every neighborhood of p contains a point outside of B.

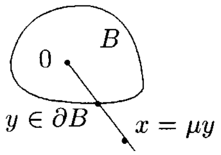

Figure 4.3.1: Illustration of the Gauge Function

Definition 4.3.2 (Gauge Function)
Let $B \subseteq \mathbb{R}^m$ be a convex body with $0 \in B$. The guage function $f : \mathbb{R}^n \to [0, \infty)$ is defined as follows:

$$f(x) := \begin{cases} 0 & \textit{if } x = 0 \\ 1 & \textit{if } x \in \partial B \\ \mu & \textit{if } x \neq 0,\ x \notin \partial B,\ x = \mu y \textit{ with } y \in \partial B \textit{ and } \mu > 0 \end{cases}$$

A guage function f is symmetric if for all $x \in \mathbb{R}^n$ $f(-x) = f(x)$.

We obtain the ℓ_2-norm with

$$B := \left\{(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n \ :\ x_1^2 + x_2^2 + \ldots x_n^2 < 1\right\}$$

and the sup-Norm with

$$B := \{(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n \ :\ |x_i| < 1 \text{ for } i = 1, 2, \ldots, n\}$$

Proposition 4.3.3
Let f be the guage function of a convex body $B \subseteq \mathbb{R}^n$ where $0 \in B$. Then for $x, y \in \mathbb{R}^n$:

a) $f(\mu \cdot x) = \mu \cdot f(x)$ *for* $\mu > 0$

b) $f(x) > 0$ *for* $x \neq 0$ *and* $f(0) = 0$

c) $f(x + y) \leq f(x) + f(y)$.

Proof. See [Siegel89, Theorems 4, 5 and 6]. ■

Proposition 4.3.4
Let $f : \mathbb{R}^n \to \mathbb{R}$ be a function with:

a) $f(\mu \cdot x) = \mu \cdot f(x)$ *for* $\mu > 0$ *and* $x \in \mathbb{R}^n$

b) $f(x) > 0$ *for* $x \neq 0$

c) $f(x + y) \leq f(x) + f(y)$.

Then there exists a convex body $B \subseteq \mathbb{R}^n$ with guage function f.

Proof. See [Siegel89, Theorem 7] mit $B := \{x \in \mathbb{R}^m \mid f(x) < 1\}$. ■

Let $B \subset \mathbb{R}^n$ be a convex body. The point 0 is the *center* of B if:

$$x \in \partial B \quad \Longleftrightarrow \quad -x \in \partial B$$

Proposition 4.3.5
Let f be a guage function of a convex body B. Then 0 is the center of B, if and only if f symmetric.

Proof. See [Siegel89, Theorems 8 and 9]. ■

Symmetric guage functions correspond to norms. The first Minkowski theorem can be expressed in terms of guage function as follows (see Proposition 4.1.6 on page 59):

Proposition 4.3.6 (First Minkowski Theorem)
Let $f : \mathbb{R}^n \to [0, \infty)$ be a symmetric guage function for the convex body $B \subseteq \mathbb{R}^n$. If $\operatorname{vol}(B) \geq 2^n$, then there exists $g \in \mathbb{Z}^n \setminus \{0\}$ with $f(g) \leq 1$.

Proof. See [Siegel89, Theorems 10 and 11]. ■

Corollary 4.3.7
Let $f : \mathbb{R}^n \to [0, \infty)$ be a symmetric guage function for the convex body $B \subseteq \mathbb{R}^n$, $\mu := \min_{x \in \mathbb{Z}^n \setminus \{0\}} f(x)$ and $V := \operatorname{vol}(B)$. Then $\mu^n V \leq 2^n$.

Proof. For $\nu > 0$ let $B_\nu := \{x \in \mathbb{R}^n \mid f(x) \leq \nu\}$. Then $\operatorname{vol}(B_\nu) = \nu^n V$ and for $0 < \nu_1 < \nu_2$ we have $B_{\nu_1} \subset B_{\nu_2}$. Let

$$\nu_0 := \sup \{\nu > 0 \mid B_\nu \cap \mathbb{Z}^n = \{0\}\}$$

B_{ν_0} is open and contains no integer point other than 0. By the first Minkowski Theorem 4.3.6:

$$(\nu_0)^n V \leq 2^n$$

We show that $\mu \leq \nu_0$: Suppose for the sake of contradiction that $\mu > \nu_0$, that is, there is an $\epsilon > 0$ with $\nu_0 + \epsilon = \mu$. By the definition of ν_0 it follows that there exists a point $g \in \mathbb{Z}^n \setminus \{0\}$ with $g \in B_{\nu_0+\epsilon}$ exists. This yields a contradiction:

$$f(g) < \nu_0 + \epsilon = \mu = \min_{x \in \mathbb{Z}^n \setminus \{0\}} f(x) \leq f(g)$$

Remark: It follows from the definition of ν_0 that since $\mu < \nu_0$ it is not possible that $\nu_0 = \mu$. ■

One can sharpen the bound of Proposition 4.3.7 and obtain the Second Minkowski theorem:

Proposition 4.3.8 (Second Minkowski Theorem 1907)
Let $\lambda_1, \lambda_2, \ldots, \lambda_n$ be the successive minima of the lattice $\mathbb{Z}^n$ according to the symmetric guage function $f : \mathbb{R}^n \to [0, \infty)$. Let V be the volume of the convex body $B := \{x \in \mathbb{R}^n \mid f(x) < 1\}$. Then:

$$\frac{2^n}{n!} \leq V \cdot \lambda_1 \cdot \lambda_2 \ldots \lambda_n \leq 2^n$$

Proof. See Paragraph 9.1 in Chapter 2 of [GrLek87]. For the upper bound see also Theorem 16 of [Siegel89] with proof, in Lecture IV. ■

Proposition 4.3.9 (Second Minkowski Theorem for General Lattice)
Let $\lambda_1, \lambda_2, \dots, \lambda_n$ be the successive minima of the full dimensional lattice $L \subseteq \mathbb{R}^n$ according to the symmetric guage function $f : \mathbb{R}^n \to [0, \infty)$. Let V be the volume of the convex body $B := \{x \in \mathbb{R}^n \mid f(x) < 1\}$. Then

$$\frac{\det L}{n!} \leq \frac{V}{2^n} \cdot \prod_{i=1}^{n} \lambda_i \leq \det L$$

For the case that f is the sup-norm, we have

$$B := \{(x_1, x_2, \dots, x_n) \in \mathbb{R}^n \ : \ |x_i| < 1 \text{ for } i = 1, 2, \dots, n\},$$

and $V = 2^n$. For every full dimensional lattice $L \subseteq \mathbb{R}^n$ we obtain from the second Minkowski theorem:

$$\prod_{i=1}^{n} \lambda_{i,\infty} \leq \det L$$

Chapter 5

Gauss' Basis Reduction Procedure

In this chapter we present Gauss' basis reduction procedure for two dimensional lattices. The procedure is a generalization of the Euclidean Algorithm. We will study the reduction procedure for the special case of the Euclidean norm and then consider the general case of an arbitrary norm.

While in Chapter 4.1 we saw by an example that in the general case there is no basis whose vectors have the lengths, respectively, of the successive mimima; however, in the two dimensional case such a basis always exists.

5.1 Reduced Basis

We introduce a notion of reducedness for two-vector bases:

Definition 5.1.1 (Gauß Reduced Basis)
An ordered lattice basis $a, b \in \mathbb{R}^n$ is (Gauß) reduced with respect to norm $||\cdot||$, when:

$$||a|| \leq ||b|| \leq ||a-b|| \leq ||a+b||$$

We consider the case that the norm is given by the scalar product $||x|| = \sqrt{\langle x, x\rangle}$. For the Gram-Schmidt coefficients $\mu_{2,1} = \frac{\langle a,b\rangle}{||a||^2}$ we have:

$$\begin{array}{rclcrl} \mu_{2,1} & \leq & \frac{1}{2} & \Longleftrightarrow & ||b|| & \leq ||a-b|| \\ \mu_{2,1} & \geq & 0 & \Longleftrightarrow & ||a-b|| & \leq ||a+b|| \end{array}$$

Thus the basis a, b is reduced if and only if:

a) $||a|| \leq ||b||$

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

In contrast with a weight reduced basis, we require that not only does the absolute value of $\mu_{2,1}$ lie between 0 and $\frac{1}{2}$, but $\mu_{2,1}$ itself does. This can be ensured by replacing b with $-b$. Figure 5.1.1 shows the Gauss reducedness condition in the case of the standard scalar product. The angle ϕ between the two lattice vectors of the reduced basis is between 60° and 90°:

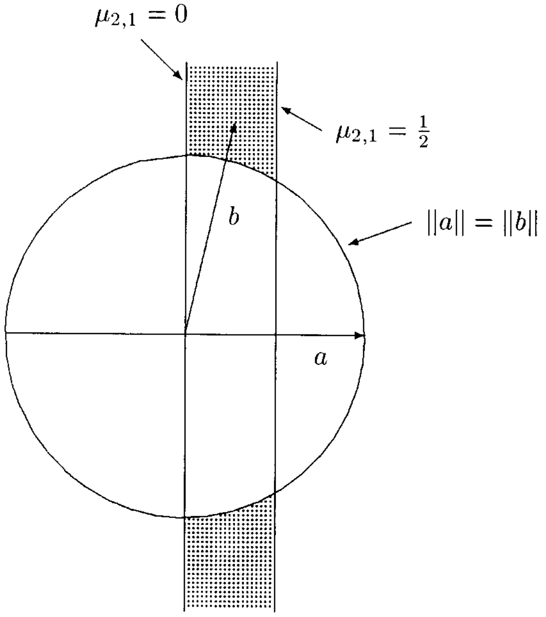

Figure 5.1.1: Reduced Basis for Standard Scalar Product

$$\cos\phi = \frac{\langle a, b\rangle}{||a|| \cdot ||b||} = \mu_{2,1} \cdot \frac{||a||}{||b||}$$

Since $0 \le \mu_{2,1} \le \frac{1}{2}$ and $||a|| \le ||b||$:

$$0 \le \cos\phi \le \tfrac{1}{2}$$

If a, b is reduced with $\mu_{2,1} = 0$, then $-a, b$ is also a reduced basis. Similarly, if a, b is reduced with $\mu_{2,1} = \frac{1}{2}$, then $a, a - b$ is also reduced. If a, b is reduced with $||a|| = ||b||$, then b, a is also reduced. In the remaining cases we have only the reduced basis $\pm a, \pm b$.

Proposition 5.1.2
For a reduced basis $a, b \in \mathbb{R}^n$, $||a||$ and $||b||$ are the two successive minima of the lattice $L = \mathbb{Z}a + \mathbb{Z}b$.

Proof. Without loss of generality, assume $||a|| \le ||b||$. The claim says:

$$\begin{aligned} ||a|| &\le ||ra + sb|| && \forall (r,s) \in \mathbb{Z}^2 \setminus \{(0,0)\} \\ ||b|| &\le ||ra + sb|| && \forall r \in \mathbb{Z} \text{ and } s \in \mathbb{Z} \setminus \{0\} \end{aligned}$$

These inequalities follow together from the following properties, which we prove below.

$$
\begin{array}{lll}
 & \|a\| \le \|b\| & \\
(5.1) & \|a\| \le \|ra\| & \forall r \in \mathbb{Z} \setminus \{0\} \\
 & \|b\| \le \|\xi a + \eta b\| & \forall \xi, \eta \in \mathbb{R} \text{ with } |\xi|, |\eta| \ge 1
\end{array}
$$

We now prove inequalities (5.1). Consider Figure 5.1.2: In the union of the four "quadrants" indicated by small dots, the norm takes its minimum on some subset of the four points $\pm a \pm b$. Of the lattice points lying on the thicker lines, the norm is minimized in the middle points. That is, from the Gauss reducedness conditions it is easy (but tedious) to verify that

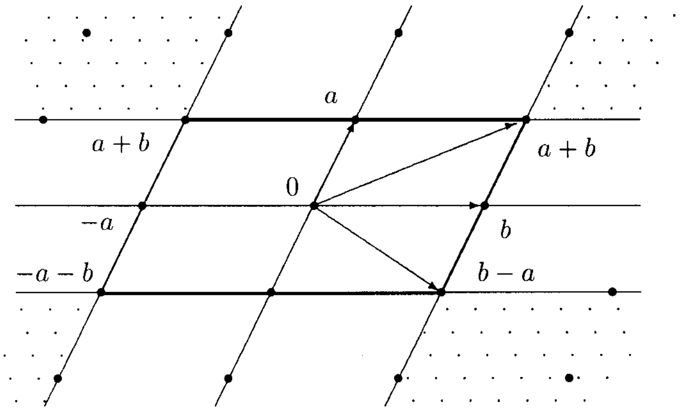

Figure 5.1.2: Reduced Basis a, b

$$
\begin{array}{ccccc}
\|\pm a - b\| & \ge & \|\pm a\| & \le & \|\pm a + b\| \\
\|-a \pm b\| & \ge & \|\pm b\| & \le & \|a \pm b\|
\end{array}
$$

By the convexity of the norm, for $|\xi| \ge 1$:

$$
\begin{array}{ccccc}
\|\pm a \pm \xi b\| & \ge & \|\pm a \pm b\| & \ge & \|\pm a\| \\
\|\pm \xi a \pm b\| & \ge & \|\pm a \pm b\| & \ge & \|\pm b\|
\end{array}
$$

Thus the points $\pm a \pm b$ have the minimal norm on the thick lines. By convexity, the norm is minimized on the boundary, hence on the thick lines. ■

Definition 5.1.3 (Well Ordered, Reduced Basis)
An ordered lattice basis $a, b \in \mathbb{R}^n$ is well ordered reduced according to norm $\|\cdot\|$ when:

$$\|a\| \le \|a - b\| \le \|b\|$$

5.2 Algorithms

We present two algorithms for obtaining a reduced basis for a two dimensional lattice: one for general norms and one for the special case of the Euclidean norm.

5.2.1 Reduction Algorithm for the Euclidean Norm

Algorithm 5.2.1 Gauß' Reduction Procedure for the Euclidean Norm

```
INPUT :   Lattice Basis $a, b \in \mathbb{R}^n$ with $||a|| \leq ||b||$

  1. WHILE $|\mu_{2,1}| > \frac{1}{2}$ DO
       1.1. $[a, b] := [a, b] \cdot \begin{bmatrix} -\lceil \mu_{2,1} \rfloor & 1 \\ 1 & 0 \end{bmatrix}$
       1.2. IF $||a|| > ||b||$ THEN exchange $a$ and $b$
     END while
  2. $b := b \cdot \mathrm{sign}(\mu_{2,1})$      /* $\mu_{2,1} \geq 0$ */

OUTPUT :   Reduced Basis $a, b$
```

Algorithm 5.2.1 produces a reduced basis according to the Euclidean norm. An iteration of Algorithm 5.2.1 reduces b by $b := b - \lceil \mu_{2,1} \rfloor a$ and then exchanges a und b. The output is clearly correct.

Proposition 5.2.1
On input a, b with $||a|| \leq ||b||$, Algorithm 5.2.1 terminates in at most

$$\left\lceil \log_{1+\sqrt{2}} \left(\frac{||a||}{\lambda_2} \right) \right\rceil + 3$$

iterations.

Proof. See Proposition 4.4 of [Schnorr94b]. ■

5.2.2 Reduction Algorithm for Arbitrary Norm

Gauß' Reduction Procedure for the Euclidean Norm can be generalized (Algorithm 5.2.2). A detailed analysis appears in [KaSchn96] by M. Kaib und C.P. Schnorr in M. Kaib's Dissertation [Kaib94], which describes efficient implementations of Step 1.1 in the l_1- and sup- norms.

Algorithm 5.2.2 Gauß' Reduction Procedure for Arbitrary Norm

```
INPUT :   Lattice Basis $a, b \in \mathbb{R}^n$ with $||a|| \leq ||b||$

  1. WHILE $||b|| > ||a - b||$ DO
        1.1. $b := b - \mu a$, $\mu \in \mathbb{Z}$ chosen so that $||b - \mu a||$ is minimal
        1.2. IF $||a + b|| < ||a - b||$ THEN $b := -b$
        1.3. exchange $a$ und $b$
     END while

OUTPUT :   Reduced Basis $a, b$
```

Chapter 6

LLL Reduced Lattice Basis

The following notion of reducedness for ordered lattice basis $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$ of arbitrary rank n was proposed in 1982 by A.K. Lenstra, H.W. Lenstra und L. Lovász [LLL82]. It uses the Euclidean norm.

6.1 Definition and Properties

We introduce the notion of LLL reduced basis and show properties of an LLL reduced basis; in particular we consider how well the length of the first reduced basis vector approximates the first successive minimum of the lattice. Let $\widehat{b}_1, \widehat{b}_2, \ldots, \widehat{b}_n$ be the Gram-Schmidt orthogonalization of the basis $b_1, b_2, \ldots, b_n$, and let $\mu_{i,j}$ $(1 \leq i, j \leq n)$ be the corresponding Gram-Schmidt coefficients.

Definition 6.1.1 (LLL Reduced Basis)
An ordered lattice basis $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$ is called LLL reduced (L^3-reduced) with parameter δ, $\frac{1}{4} < \delta \leq 1$, when:

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

b) $\delta \cdot \|\widehat{b}_{k-1}\|^2 \leq \|\widehat{b}_k\|^2 + \mu_{k,k-1}^2 \cdot \|\widehat{b}_{k-1}\|^2$ *for* $k = 2, 3, \ldots, n$

The first property is the criterion for length reducedness (see Definition 3.3.1 on page 48). The parameter δ describes how well reduced the basis is: a larger value for δ implies a more strongly reduced basis. A.K. Lenstra, H.W. Lenstra und L. Lovász [LLL82] originally defined LLL reducedness for the value $\delta = \frac{3}{4}$. With the orthogonal projection

$$\pi_k : \mathbb{R}^m \to \operatorname{span}(b_1, b_2, \ldots, b_{k-1})^\perp$$

the second condition can be written as:

$$\delta \cdot \|\pi_{k-1}(b_{k-1})\|^2 \leq \|\pi_{k-1}(b_k)\|^2 \quad \text{for } k = 2, 3, \ldots, n$$

If the basis consists of two vectors, then when $\delta = 1$ we obtain a Gauß reduced basis. Let $T : \operatorname{span}(b_1, b_2, \ldots, b_n) \to \mathbb{R}^n$ be the isometric mapping with

$$T(\widehat{b}_i) = ||\widehat{b}_i|| \cdot e_i \quad \text{for } i = 1, 2, \ldots, n,$$

where e_i is the ith unit vector in $\mathbb{R}^m$. The basis matrix $[T(b_1), T(b_2), \ldots, T(b_n)]$ for the lattice $T(L)$, isometric to L, is an upper triangular matrix:

$$[T(b_1), \ldots, T(b_n)] = \begin{bmatrix} ||\widehat{b}_1|| & 0 & \cdots & 0 \\ 0 & ||\widehat{b}_2|| & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & ||\widehat{b}_n|| \end{bmatrix} \begin{bmatrix} 1 & \mu_{2,1} & \mu_{3,1} & \cdots & \mu_{n,1} \\ 0 & 1 & \mu_{3,2} & & \mu_{n,2} \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \mu_{n,n-1} \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} ||\widehat{b}_1|| & * & * & * & * \\ & \ddots & * & * & * \\ & & \begin{bmatrix} ||\widehat{b}_{k-1}|| & \mu_{k,k-1}||\widehat{b}_{k-1}|| \\ 0 & ||\widehat{b}_k|| \end{bmatrix} & * & * \\ & & & \ddots & * \\ & & & & ||\widehat{b}_n|| \end{bmatrix}$$

The basis $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$ is LLL reduced with δ if and only if:

a) the basis $b_1, b_2, \ldots, b_n$ is length reduced;

b) the 2×2 matrices on the diagonal

$$\begin{bmatrix} ||\widehat{b}_{k-1}|| & \mu_{k,k-1}||\widehat{b}_{k-1}|| \\ 0 & ||\widehat{b}_k|| \end{bmatrix}$$

for $k = 2, 3, \ldots, n$, are LLL reduced with parameter δ.

Let $b_1, b_2, \ldots, b_n$ be LLL reduced with δ. Then $\pi_k(b_k), \pi_k(b_{k+1}), \ldots, \pi_k(b_j)$ is LLL reduced with δ for $1 \leq k < j \leq n$. We now examine other properties of LLL reduced lattice bases.

Lemma 6.1.2
Let $b_1, b_2, \ldots, b_n$ be LLL reduced with parameter δ. Then for $\alpha = \frac{1}{\delta - \frac{1}{4}}$:

$$||\widehat{b}_i||^2 \leq \alpha^{j-i} \cdot ||\widehat{b}_j||^2 \quad \textit{for } 1 \leq i \leq j \leq n$$

In particular, if $\delta = \frac{3}{4}$, then $\alpha = 2$ and $||b_1||^2 \leq 2^{j-1} \cdot ||\widehat{b}_j||^2$, and in general the length of $\widehat{b}_j$ for large j can't be arbitrarily small with respect to the lengths of $\widehat{b}_i$ for smaller i.

Proof. ¿From Properties a) und b) of LLL reducedness it follows that:

$$\delta \cdot ||\widehat{b}_i||^2 \overset{b)}{\leq} ||\widehat{b}_{i+1}||^2 + \mu_{i+1,i}^2 ||\widehat{b}_i||^2 \overset{a)}{\leq} ||\widehat{b}_{i+1}||^2 + \tfrac{1}{4}||\widehat{b}_i||^2$$

and thus:

$$\underbrace{\left(\delta - \tfrac{1}{4}\right)}_{=1/\alpha} \cdot ||\widehat{b}_i||^2 \leq ||\widehat{b}_{i+1}||^2$$

The claim follows by induction over $j - i$. ■

Corollary 6.1.3
Let $b_1, b_2, \ldots, b_n$ be LLL reduced with parameter δ. Then for $\alpha = \frac{1}{\delta - \frac{1}{4}}$, $||b_1||_2 \leq \alpha^{(n-1)/2}\lambda_1(L)$.

Proof. By Proposition 3.2.26, we have $\lambda_1(L) \geq \min\{||\widehat{b}_1||, \ldots, ||\widehat{b}_n||\}$. Let the minimum length basis vector be b_k. Then

$$\begin{aligned} ||\widehat{b}_1||^2 &\leq \alpha^{k-1}||\widehat{b}_k||^2 \quad \text{by Lemma 6.1.2} \\ &\leq \alpha^{n-1}||\widehat{b}_k||^2 \quad \text{because } \alpha \geq 1 \text{ and } k \leq n \\ &\leq \alpha^{n-1}(\lambda_1(L))^2 \end{aligned}$$

By taking square roots we obtain the statement of the Corollary. ■

The next lemma is a generalization of Proposition 3.2.26.

Lemma 6.1.4
Let $b_1, b_2, \ldots, b_n$ be a basis of the lattice L. Then for $i = 1, 2, \ldots, n$:

$$\lambda_j \geq \min_{i=j,j+1,\ldots,n} ||\widehat{b}_i||$$

Proof. There are linearly independent vectors $a_1, a_2, \ldots, a_n \in L$, so that $||a_j|| = \lambda_j(L)$ for $j = 1, 2, \ldots, n$. Let

$$a_k = \sum_{i=1}^{n} t_{ik} b_i = \sum_{i=1}^{n} \bar{t}_{ik} \widehat{b}_i \quad \text{for } k = 1, 2, \ldots, n$$

Hence the coefficients t_{ik} are integers and the $\bar{t}_{ik}$ are reals. Let

$$\mu(k) := \max\{i \;:\; t_{ik} \neq 0\}$$

Since the vectors $b_1, b_2, \ldots, b_{\mu(k)}$ are linearly independent, $\bar{t}_{\mu(k),k} = t_{\mu(k),k} \in \mathbb{Z}$. ¿From the linear independence of the vectors $a_1, a_2, \ldots, a_j$, for each j there is a $k \leq j$ with $\mu(k) \geq j$. Assume the contrary. Then by the assumption that $\mu(k) < j$ for $k = 1, 2, \ldots, j$ it follows that

$$a_1, a_2, \ldots, a_j \in \operatorname{span}(b_1, b_2, \ldots, b_{j-1}),$$

so that $a_1, a_2, \ldots, a_j$ are linearly dependent, which yields a contradiction. We therefore obtain

$$\lambda_j^2 \geq \lambda_k^2 = \|a_k\|^2 \geq \bar{t}^2_{\mu(k),k} \|\widehat{b}_{\mu(k)}\|^2 \geq \|\widehat{b}_{\mu(k)}\|^2 \geq \min_{i=j,j+1,\ldots,n} \|\widehat{b}_i\|^2$$

■

While the lower bound on λ_j in Lemma 6.1.4 applies to arbitrary bases, the following theorem shows that the lengths $\|b_j\|$ in an LLL reduced basis are "rough" approximations to the successive minima λ_j.

Proposition 6.1.5 (Lenstra, Lenstra, Lovász 1982)
Let $b_1, b_2, \ldots, b_n$ be an LLL reduced lattice basis with parameter δ. Then for $\alpha = \frac{1}{\delta - \frac{1}{4}}$:

a) $\alpha^{1-j} \leq \dfrac{\|\widehat{b}_j\|^2}{\lambda_j^2}$ *for* $j = 1, 2, \ldots, n$

b) $\dfrac{\|b_j\|^2}{\lambda_j^2} \leq \alpha^{n-1}$ *for* $j = 1, 2, \ldots, n$

c) $\|b_k\|^2 \leq \alpha^{j-1} \cdot \|\widehat{b}_j\|^2$ *for* $k \leq j$

Proof. $\exists k$, $1 \leq k \leq j$, such that $\lambda_j \leq \|b_k\|$. It follows that:

$$\begin{aligned}
\lambda_j^2 &\leq \|b_k\|^2 \\
&\leq \|\widehat{b}_k\|^2 + \tfrac{1}{4}\sum_{i=1}^{k-1} \|\widehat{b}_i\|^2 && \text{(by the LLL reducedness properties)} \\
&\leq \|\widehat{b}_j\|^2 \left(\alpha^{j-k} + \tfrac{1}{4}\sum_{i=1}^{k-1} \alpha^{j-i}\right) && \text{(by Lemma 6.1.2)} \\
&\leq \|\widehat{b}_j\|^2 \alpha^{j-1} \left(\alpha^{1-k} + \tfrac{1}{4}\sum_{i=1}^{k-1} \alpha^{1-i}\right)
\end{aligned}$$

We show:

$$\alpha^{1-k} + \tfrac{1}{4}\sum_{i=1}^{k-1} \alpha^{1-i} \leq 1$$

For $k = 1$ the inequality is obvious. For $k \geq 2$, since $\alpha^{-1} = \delta - \frac{1}{4} \leq \frac{3}{4}$:

$$\alpha^{1-k} + \frac{1}{4} \underbrace{\sum_{i=1}^{k-1} \alpha^{1-i}}_{\text{geo m. series}} \leq \left(\frac{3}{4}\right)^{k-1} + \frac{1}{4} \cdot \frac{1 - (\frac{3}{4})^{k-1}}{1 - \frac{3}{4}} = \frac{1}{4} \cdot \frac{1}{1 - \frac{3}{4}} = 1$$

Thus,

$$\lambda_j^2 \leq \|b_k\|^2 \leq \|\widehat{b}_j\|^2 \alpha^{j-1}$$

and so we have proved the first and third assertions. By Lemma 6.1.4 there is a $k \geq j$, so that $\lambda_j \geq \|\widehat{b}_k\|$. It follows from Lemma 6.1.2 that:

$$\begin{aligned}
\lambda_j^2 &\geq \|\widehat{b}_k\|^2 && \text{(from Lemma 6.1.4)}\\
&\geq \alpha^{-k+j} \cdot \|\widehat{b}_j\|^2 && \text{(from Lemma 6.1.2)}\\
&\geq \alpha^{-k+1} \cdot \|b_j\|^2 && \text{(from Assertion (c) with } k = j\text{)}\\
&\geq \alpha^{-n+1} \cdot \|b_j\|^2 && \text{(since } k \leq n \text{ and } \alpha \geq 1\text{)}
\end{aligned}$$

■

Corollary 6.1.6
Let $b_1, b_2, \ldots, b_n$ be an LLL reduced basis of the lattice L. Then for $\alpha = \frac{1}{\delta - \frac{1}{4}}$:

a) $\|b_1\|^2 \leq \alpha^{\frac{n-1}{2}} (\det L)^{\frac{2}{n}}$

b) $\displaystyle\prod_{i=1}^{n} \|b_i\|^2 \leq \alpha^{\binom{n}{2}} (\det L)^2$

Proof. We have $\prod_{i=1}^{n} \|\widehat{b}_i\|^2 = (\det L)^2$. By the third Assertion of Theorem 6.1.5:

$$\|b_1\|^2 \leq \|\widehat{b}_i\|^2 \cdot \alpha^{i-1}$$

It follows that:

$$\|b_1\|^{2n} \leq \alpha^1 \alpha^2 \cdots \alpha^{n-1} \prod_{i=1}^{n} \|\widehat{b}_i\|^2 = \alpha^{\binom{n}{2}} \cdot (\det L)^2$$

Thus we obtain part (a): $\|b_1\|^2 \leq \alpha^{\frac{n-1}{2}} (\det L)^{\frac{2}{n}}$.

Part (b) follows from $\prod_{i=1}^{n} \|\widehat{b}_i\|^2 = (\det L)^2$ and $\|b_i\|^2 \leq \|\widehat{b}_i\|^2 \alpha^{i-1}$, the third Assertion of Theorem 6.1.5. ■

Remark 6.1.7
The proof of Corollary 6.1.3 uses only the fact that the $|\mu_{i+1,i}| \leq \frac{1}{2}$, and not the full power of weak-reducedness. Moreover, since the proof of Corollary 6.1.3(a) only uses case $k = 1$ of Proposition 6.1.5, the same is true there. However, the proof of Corollary 6.1.3(b) uses the full strength of weak reducedness. Lovász remarks that to guarantee that the numbers occurring in the procedure do not grow too big the full power of weak reducedness seems to be necessary [Lovász86].

6.1.1 Two Applications of LLL Reducedness

We return briefly to the Simultaneous Diophantine Approximation and Small Integer Combination Problems described in Chapter 1. Let us assume the existence of an algorithm that efficiently obtains an LLL reduced basis with $\delta = \frac{3}{4}$ (the "'LLL algorithm," described in Section 6.2, has this property). At the end of Section 4.1 we cast the SDA in terms of finding a short vector in the lattice defined by the columns of the matrix A:

$$A = \begin{bmatrix} 1 & 0 & \dots & 0 & \alpha_1 \\ 0 & 1 & \dots & 0 & \alpha_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & 1 & \alpha_n \\ 0 & 0 & \dots & 0 & \varepsilon/Q \end{bmatrix}$$

$\det L(A) = \varepsilon/Q$. Let $Q = 2^{n(n+1)/4}\varepsilon^{-n}$. Using the LLL algorithm, we can obtain a vector $b \in L(A)$ such that

$$||b||_2 \leq 2^{n/4}(\det L(A))^{\frac{1}{n+1}} = 2^{n/4}\left(\frac{\varepsilon}{Q}\right)^{\frac{1}{n+1}} = \varepsilon$$

Since $b \in L(A)$ there exist integers $p_1, p_2, \dots, p_n, q$ such that

$$b = \begin{bmatrix} p_1 - q\alpha_1 \\ p_2 - q\alpha_n \\ \vdots \\ p_n - q\alpha_n \\ q\frac{\varepsilon}{Q} \end{bmatrix}$$

Since $||b||_\infty \leq ||b||_2$ it follows that

$$|p_i - q\alpha_i| \leq \varepsilon$$

and moreover $\left|q\frac{\varepsilon}{Q}\right| \leq \varepsilon$, or in other words, $|q| \leq Q$. Thus we obtain an approximate solution to the simultaneous diophantine approximation problem, in which the denominator q is at most a factor of $2^{n(n+1)/4}$ greater than optimal.

We may cast the Small Integer Combination problem in terms of a lattice problem as follows. Recall that the problem is, given rationals $\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_n$, and rationals $\varepsilon, Q > 0$, to find $q_0, q_1, q_2, \dots, q_n \in \mathbb{Z}$, not all 0, such that

$$\left|\sum_{i=0}^{n} q_i\alpha_i\right| \leq \varepsilon$$

and $q_i \leq Q$ for $1 \leq i \leq n$. Traditionally, $\alpha_0 = 1$, so we will make that assumption here. We define

$$B = \begin{bmatrix} \alpha_0 & \alpha_1 & \dots & \alpha_n \\ 0 & \varepsilon/Q & \dots & 0 \\ \vdots & \ddots & & \vdots \\ 0 & 0 & \dots & \varepsilon/Q \end{bmatrix}$$

Then $\det B = \alpha_0(\varepsilon/Q)^n$, or, since we are assuming $\alpha_0 = 1$, we have simply $\det B = (\varepsilon/Q)^n$. Let $b = Bq$, $q \in \mathbb{Z}^{n+1}$, satisfy $\|b\|_2 \leq \varepsilon$, $b \neq 0$. Then $\|b\|_\infty \leq \varepsilon$ and so

$$|q_0\alpha_0 + \cdots + q_n\alpha_n| \leq \varepsilon$$

and $\left|q_i \frac{\varepsilon}{Q}\right| \leq \varepsilon$, or in other words $|q_i| \leq Q$.

Choosing $\varepsilon = 2^{n/4}(\det B)^{\frac{1}{n+1}}$, i.e., $Q = 2^{(n+1)/4}\varepsilon^{-1/n}$, we have by Corollary 6.1.6(b) that the LLL algorithm will find such a vector $b \in L(B)$ in polynomial time.

6.2 The LLL Reduction Algorithm

Given an arbitrary lattice basis, we present a procedure to obtain an LLL reduced basis for the same lattice. We analyze the running time and size of the coefficients in the calculations. We generalize the procedure to systems Erzeugendensysteme??? – systems of generators, in which the vectors need not be linearly independent.

6.2.1 Algorithm

Algorithm 6.2.1, transforms, for a given δ, $\frac{1}{4} < \delta < 1$, an integer lattice basis into a basis for the same lattice that is LLL reduced with parameter δ. For each exchange $b_{k-1} \leftrightarrow b_k$, the values of $\|\widehat{b}_k\|^2$, $\|\widehat{b}_{k-1}\|^2$ and $\mu_{i,\nu}$, $\mu_{\nu,i}$, for $\nu = k-1, k$ and $i = 1, 2, \ldots, n$, must be recalculated (see the proof of Lemma 6.2.3). Correctness follows from the invariant: Upon entry to stage k, the basis $b_1, b_2, \ldots, b_{k-1}$ is LLL reduced with δ. At the end of the algorithm, $k = n+1$, so the whole basis $b_1, b_2, \ldots, b_n$ is reduced.

We analyze the running time of Algorithm 6.2.1. Consider the determinants:

$$D_i := \det L(b_1, b_2, \ldots, b_i)^2 = \det\left[\langle b_s, b_t\rangle\right]_{1 \leq s,t \leq i} = \prod_{j=1}^{i} \|\widehat{b}_j\|^2 \tag{6.1}$$

Note that we are working with the squares of the lattice determinants. We set

$$D := \prod_{j=1}^{n-1} D_j \tag{6.2}$$

Lemma 6.2.1
For integer inputs $b_1, b_2, \ldots, b_n \in \mathbb{Z}^m$ the algorithm stops after at most

$$\left\lfloor \log_{1/\delta}\left(D^{Start}\right)\right\rfloor$$

exchanges $b_{k-1} \leftrightarrow b_k$. For $M := \max_i \left\|b_i^{Start}\right\|^2$:

$$\#\textit{Exchanges} \leq \binom{n}{2} \log_{1/\delta} M$$

Algorithm 6.2.1 LLL Reduction Algorithm

```
INPUT : ▷ Lattice Basis $b_1, b_2, \dots, b_n \in \mathbb{Z}^m$
        ▷ Parameter $\delta$ with $\frac{1}{4} < \delta < 1$

  1. $k := 2$     /* $k$ is the stage */
  2. Calculate $\mu_{i,j}$ for $1 \leq j < i \leq n$ and $\|\widehat{b}_i\|^2$ for $i = 1, 2, \dots, n$
  3. WHILE $k \leq n$ DO
          /* Invariant: $b_1, b_2, \dots, b_{k-1}$ is LLL reduced */
          3.1. Length reduce $b_k$ and correct $\mu_{k,j}$ for $j = 1, 2, \dots, k-1$
          3.2. IF $\delta \cdot \|\widehat{b}_{k-1}\|^2 > \|\widehat{b}_k\|^2 + \mu_{k,k-1}^2 \|\widehat{b}_{k-1}\|^2$ THEN
                 3.2.1. $b_{k-1} \leftrightarrow b_k$, i.e. exchange $b_{k-1}$ and $b_k$
                 3.2.2. $k := \max(k-1, 2)$
               ELSE $k := k + 1$
     END while

OUTPUT :  LLL Reduced Basis With $\delta$ $b_1, b_2, \dots, b_n$
```

Proof. For $j = 1, 2, \dots, n$, D_j is always a positive integer. We show that every exchange results in $D^{\text{new}} \leq \delta \cdot D^{\text{old}}$. Since $D^{\text{End}} \in \mathbb{N}$ this implies:

$$D^{\text{Start}} \geq D^{\text{End}} \cdot \left(\frac{1}{\delta}\right)^{\#\text{Exchanges}} \geq \left(\frac{1}{\delta}\right)^{\#\text{Exchanges}} \tag{6.3}$$

Thus we obtain the first part of the Lemma. The lattice $L(b_1, b_2, \dots, b_j)$ with $j \neq k-1$ remains unchanged by the exchange $b_{k-1} \leftrightarrow b_k$. Thus the determinants D_j with $j \neq k-1$, remain unchanged. By the pre-condition for the exchange:

$$\delta \cdot \|\widehat{b}_{k-1}^{\text{old}}\|^2 \;>\; \|\widehat{b}_k^{\text{old}}\|^2 + \underbrace{\left(\mu_{k,k-1}^{\text{old}}\right)^2 \cdot \|\widehat{b}_{k-1}^{\text{old}}\|^2}_{=\|\widehat{b}_{k-1}^{\text{new}}\|^2} \;\geq\; \|\widehat{b}_{k-1}^{\text{new}}\|^2$$

Since $D_{k-1} = \prod_{i=1}^{k-1} \|\widehat{b}_i\|^2$ the exchange $b_{k-1} \leftrightarrow b_k$ ensures that

$$D_{k-1}^{\text{new}} \leq \delta \cdot D_{k-1}^{\text{old}}$$

It follows from (6.2), that $D^{\text{new}} \leq \delta \cdot D^{\text{old}}$. We obtain the first claim from (6.3). The second claim follows from $D_i^{\text{Start}} \leq M^i$ for $i = 1, 2, \dots, n-1$ and $D^{\text{Start}} \leq M^{\binom{n}{2}}$. ■

What is the running time of the algorithm for real (rather than integer) lattice bases? For $\delta \leq 1$ the algorithm terminates; moreover it is known to stop in polynomial time if $\delta < 1$. The proof of the following lemma is similar to that of Lemma 6.2.1, but we use Minkowski's inequality to bound d^{End} from below, together with the simple bound $\gamma_j \leq j$.

Lemma 6.2.2
Let $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$ be a real input basis and $M := \max_i \|\widehat{b}_i\|^2$. Then for $\delta < 1$ the algorithm terminates after at most

$$\log_{1/\delta}\left[\prod_{j=1}^{n-1}\left(\frac{\|\widehat{b}_j\|}{\lambda_j}\right)^{2(n-j)} \cdot (\gamma_j)^j\right] \leq \binom{n}{2}\log_{1/\delta}\left(\frac{M}{\lambda_1^2}\right) + \binom{n}{2}\log_{1/\delta} n$$

exchanges $b_{k-1} \leftrightarrow b_k$ (γ_j is the Hermite constant for dimension j)

Proof.

$$D^{\text{Start}} = \prod_{j=1}^{n-1} \|\widehat{b}_j\|^{2(n-j)} \leq M^{\binom{n}{2}}$$

and $D^{\text{End}} = \prod_{j=1}^{n-1} D_j$, where we bound D_j from below using Minkowski's inquality:

$$D_j = \prod_{i=1}^{j} \|\widehat{b}_i\|^2 \geq (\gamma_j)^{-j} \prod_{i=1}^{j} \lambda_i^2$$

With $M = \max_i \|\widehat{b}_i\|^2$ and the simple bound $\gamma_j \leq j$ from Remark 4.2.2 on Page 61 it follows that:

$$\begin{aligned}
\#\ \text{Exchanges} &\leq \log_{1/\delta}\left(\frac{D^{\text{Start}}}{D^{\text{End}}}\right) \\
&\leq \log_{1/\delta}\left(\prod_{j=1}^{n-1}\left(\frac{\|\widehat{b}_j\|}{\lambda_j}\right)^{2(n-j)} \cdot (\gamma_j)^j\right) \\
&\leq \log_{1/\delta}\left(\prod_{j=1}^{n-1}\left(\frac{M}{\lambda_1^2}\right)^{n-j}\right) + \log_{1/\delta}\left(\prod_{j=1}^{n-1} n^j\right)
\end{aligned}$$

We obtain:

$$\begin{aligned}
\#\ \text{Exchanges} &\leq \binom{n}{2}\log_{1/\delta}\left(\frac{M}{\lambda_1^2}\right) + \sum_{j=1}^{n-1}\log_{1/\delta} n^j \\
&\leq \binom{n}{2}\log_{1/\delta}\left(\frac{M}{\lambda_1^2}\right) + \binom{n}{2}\log_{1/\delta} n
\end{aligned}$$

■

Having analyzed the number of exchanges $b_{k-1} \leftrightarrow b_k$ in the LLL algorithm, we will next analyze the number of arithmetic steps in a single exchange, to obtain a bound on the complexity of the algorithm.

Lemma 6.2.3
The exchange $b_{k-1} \leftrightarrow b_k$ results in $\mu := \mu_{k,k-1}$ and $\mu^{\text{new}} := \mu^{\text{new}}_{k,k-1}$, such that:

a) $$||\widehat{b}^{\text{new}}_{k-1}||^2 \;=\; ||\widehat{b}_k||^2 + \mu^2||\widehat{b}_{k-1}||^2$$

b) $$||\widehat{b}^{\text{new}}_{k}||^2 \;=\; \frac{||\widehat{b}_k||^2 \cdot ||\widehat{b}_{k-1}||^2}{||\widehat{b}^{\text{new}}_{k-1}||^2}$$

c) $$\mu_{\text{new}} \;=\; \mu \cdot \frac{||\widehat{b}^{\text{new}}_{k}||^2}{||\widehat{b}^{\text{new}}_{k-1}||^2}$$

d) $$\left[\mu^{\text{new}}_{ij}\right]^T_{k-1\le i,j\le k} \;=\; \begin{bmatrix}\mu_{\text{new}} & 1-\mu\mu_{\text{new}} \\ 1 & -\mu\end{bmatrix} \cdot [\mu_{i,j}]^T_{k-1\le i,j\le k} \cdot \begin{bmatrix}0 & 1 \\ 1 & 0\end{bmatrix}$$

Proof. We show the four claims together (note that $\widehat{b}_k$ und $\widehat{b}_{k-1}$ are mutually orthogonal).

a) This follows from $\widehat{b}^{\text{new}}_{k-1} = \widehat{b}_k + \mu_{k,k-1}\widehat{b}_{k-1}$.

b) This follows because the product $||\widehat{b}_k||\cdot||\widehat{b}_{k-1}||$ remains unchanged by the exchange $b_{k-1} \leftrightarrow b_k$.

c) Since

$$\mu_{\text{new}} = \frac{\left\langle b^{\text{new}}_k, \widehat{b}^{\text{new}}_{k-1}\right\rangle}{||\widehat{b}^{\text{new}}_{k-1}||^2} = \frac{\left\langle b_{k-1}, \widehat{b}_k + \mu\widehat{b}_{k-1}\right\rangle}{||\widehat{b}^{\text{new}}_{k-1}||^2}$$

we obtain:

$$\mu_{\text{new}} = \frac{\left\langle b_{k-1}, \widehat{b}_k\right\rangle + \left\langle b_{k-1}, \mu\widehat{b}_{k-1}\right\rangle}{||\widehat{b}^{\text{new}}_{k-1}||^2} = \frac{\mu||\widehat{b}_{k-1}||^2}{||\widehat{b}^{\text{new}}_{k-1}||^2}$$

d) $\widehat{b}^{\text{new}}_{k-1} = \widehat{b}_k + \mu\widehat{b}_{k-1}$ and according to the backwards exchange $\widehat{b}_{k-1} = \widehat{b}^{\text{new}}_k + \mu_{\text{new}}\widehat{b}^{\text{new}}_{k-1}$. From these two equalities it follows that:

$$\left[\widehat{b}_{k-1}, \widehat{b}_k\right] \;=\; \left[\widehat{b}^{\text{new}}_{k-1}, \widehat{b}^{\text{new}}_k\right] \cdot \begin{bmatrix}\mu_{\text{new}} & 1-\mu\mu_{\text{new}} \\ 1 & -\mu\end{bmatrix}$$

One thus obtains (on the diagonal dots are 1's; the other entries are all 0):

$$
\begin{aligned}
&\left[b_1, b_2, \dots, b_{k-2}, b^{\text{new}}_{k-1}, b^{\text{new}}_{k}, b_{k+2}, \dots, b_m\right] \\
&= \left[\widehat{b}_1, \dots, \widehat{b}_m\right] [\mu_{i,j}]^{\mathrm{T}}_{1 \le i,j \le n} \begin{bmatrix} \ddots & & \\ & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & \\ & & \ddots \end{bmatrix} \\
&= \left[\widehat{b}^{\text{new}}_1, \dots, \widehat{b}^{\text{new}}_m\right] \begin{bmatrix} \ddots & & \\ & \begin{bmatrix} \mu_{\text{new}} & 1 - \mu\mu_{\text{new}} \\ 1 & -\mu \end{bmatrix} & \\ & & \ddots \end{bmatrix} [\mu_{i,j}]^{\mathrm{T}}_{1 \le i,j \le n} \begin{bmatrix} \ddots & & \\ & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & \\ & & \ddots \end{bmatrix} \\
&= \left[\widehat{b}^{\text{new}}_1, \dots, \widehat{b}^{\text{new}}_m\right] [\mu^{\text{new}}_{ij}]^{\mathrm{T}}_{1 \le i,j \le n}
\end{aligned}
$$

The claim follows.

■

We bound from above the number of arithmetic operations for an exchange by:

Proposition 6.2.4
An exchange $b_{k-1} \leftrightarrow b_k$ requires at most $\mathcal{O}(k)$ arithmetic operations. The length reduction of b_k requires at most $\mathcal{O}(nk)$ arithmetic operations.

Proof. The first claim follows from Lemma 6.2.3. The second claim is follows from the fact that the operation $b_k = b_k - \mu b_j$ alters the Gram-Schmidt coefficients by:

$$\mu_{k,i} := \mu_{k,i} - \mu \cdot \mu_{j,i} \qquad \text{for } i = 1, 2, \dots, j$$

■

We have analyzed the number of arithmetic steps in the LLL Algorithm. How large can the numbers grow? We study this question and obtain an upper bound on how large the coefficients can grow during the calculation.

Lemma 6.2.5
For an integer input basis $b_1, b_2, \dots, b_n \in \mathbb{Z}^m$:

a) $D_{i-1} \cdot \widehat{b}_i \in \mathbb{Z}^m$

b) $D_j \cdot \mu_{i,j} \in \mathbb{Z}$

Moreover, $D_j = \det L(b_1, b_2, \dots, b_j)^2 = \prod_{i=1}^{j} \|\widehat{b}_i\|^2$ is an integer.

Proof. The second claim will follow from the first.

a) From $[b_1, b_2, \dots, b_n] = \left[\widehat{b}_1, \widehat{b}_2, \dots, \widehat{b}_n\right] \cdot [\mu_{i,j}]^{\mathsf{T}}$ it follows for $[\nu_{ij}] := [\mu_{i,j}]^{-1}$:

$$\left[\widehat{b}_1, \widehat{b}_2, \dots, \widehat{b}_n\right] = [b_1, b_2, \dots, b_n] \cdot [\nu_{ij}]^{\mathsf{T}}$$

Moreover, $[\nu_{ij}]^{\mathsf{T}}$ like $[\mu_{i,j}]$ is an upper triangular matrix with 1's on the diagonal. Since $\left\langle \widehat{b}_i, b_j \right\rangle = 0$ for $j = 1, 2, \dots, i-1$ it follows from $\widehat{b}_i = b_i + \sum_{t=1}^{i-1} \nu_{it} b_t$ and $\nu_{ii} = 1$ that:

$$-\langle b_i, b_j \rangle = \sum_{t=1}^{i-1} \nu_{it} \langle b_t, b_j \rangle \qquad \text{for } j = 1, 2, \dots, i-1$$

These $i-1$ inequalities define $\nu_{i1}, \nu_{i2}, \dots, \nu_{i,i-1}$. The determinant of the system of equations is:

$$D_{i-1} = \det\left[\langle b_j, b_k \rangle\right]_{1 \le j,k \le i-1}$$

Since $D_{i-1} \neq 0$, it follows from Cramer's rule that:

$$D_{i-1}\nu_{ij} \in \mathbb{Z} \qquad \text{for } j = 1, 2, \dots, i-1$$

Since $\widehat{b}_i = b_i + \sum_{j=1}^{i-1} \nu_{ij} b_j$ and $b_1, b_2, \dots, b_n \in \mathbb{Z}^m$, the claim $D_{i-1} \cdot \widehat{b}_i \in \mathbb{Z}^m$ follows.

b) By definition (6.1) of the determinants $D_j = \prod_{s=1}^{j} \|\widehat{b}_s\|^2$ we have:

$$D_j \cdot \mu_{i,j} = D_j \cdot \frac{\left\langle b_i, \widehat{b}_j \right\rangle}{\|\widehat{b}_j\|^2} = D_{j-1} \cdot \left\langle b_i, \widehat{b}_j \right\rangle = \left\langle b_i, D_{j-1} \cdot \widehat{b}_j \right\rangle$$

From the first claim, $\widehat{b}_j \cdot D_{j-1} \in \mathbb{Z}^m$, it follows that $\left\langle b_i, D_{j-1} \cdot \widehat{b}_j \right\rangle \in \mathbb{Z}$. We thus obtain the claim $D_j \cdot \mu_{i,j} \in \mathbb{Z}$.

■

The value $\max_i \|\widehat{b}_i\|^2$ does not grow, and the value $\min_i \|\widehat{b}_i\|^2$ does not shrink during the execution of the LLL Algorithm. The first claim holds, since for each exchange $b_{k-1} \leftrightarrow b_k$:

a) $\|\widehat{b}_{k-1}^{\text{new}}\|^2 \le \delta \cdot \|\widehat{b}_{k-1}^{\text{old}}\|^2$

b) $\|\widehat{b}_{k}^{\text{new}}\|^2 \le \|\widehat{b}_{k-1}^{\text{old}}\|^2$

The second claim follows from:

a) $\|\widehat{b}_{k-1}^{\text{new}}\|^2 \ge \|\widehat{b}_{k}^{\text{old}}\|^2$

b) $\|\widehat{b}_{k}^{\text{new}}\|^2 \ge \delta^{-1} \cdot \|\widehat{b}_{k}^{\text{old}}\|^2$

We give bounds for the coefficients $\mu_{i,j}$ that occur in the LLL Algorithm. For an integer input basis $b_1, b_2, \ldots, b_n \in \mathbb{Z}^m$ let

$$M := \max_{i=1,2,\ldots,n} \|b_i\|^2$$

in the following.

Lemma 6.2.6
In the LLL Algorithm, at the beginning of Stage k with $\alpha := \frac{1}{1-\delta}$ for $i = 1, 2, \ldots, n$:

a) $\|b_i\|^2 \leq \frac{i+3}{4} \cdot M$

b) $|\mu_{i,j}|^2 \leq \frac{i+3}{4} \cdot M \cdot \alpha^{j-1}$ *for $j < k$*

Proof. We show both claims:

1. Since b_i is length reduced, for $i < k$:

$$\|b_i\|^2 = \sum_{j=1}^{i} \mu_{i,j}^2 \|\widehat{b}_j\|^2 \leq \|b_i\|^2 + \frac{i-1}{4} \max_{j=1,2,\ldots,i-1} \|\widehat{b}_j\|^2$$

   With $M = \max_{i=1,2,\ldots,n} \|b_i\|^2$ it follows that:

$$\|b_i\|^2 \leq M + \frac{i-1}{4} \cdot M = \frac{i+3}{4} \cdot M$$

   For $i \geq k$ one can show by induction on the number of iterations that the inequality $\|b_i\|^2 \leq \frac{i+3}{4} M$ remains unchanged:

   - For $k = i$, the inequality holds, since b_{k-1}, b_k by the exchange $b_{k-1} \leftrightarrow b_k$ are length reduced.
   - For $i > k$ the inequality holds by the inductive claim, since the vector b_i does not change.

2. In general, it follows from the definition of the Gram-Schmidt coefficients and the Cauchy-Schwarz Inequality that:

$$|\mu_{i,j}|^2 = \frac{\left|\left\langle b_i, \widehat{b}_j \right\rangle\right|^2}{\|\widehat{b}_j\|^4} \leq \frac{\|b_i\|^2 \cdot \|\widehat{b}_j\|^2}{\|\widehat{b}_j\|^4} \leq \frac{\|b_i\|^2}{\|\widehat{b}_j\|^2}$$

   From the first claim, Lemma 6.1.2 ($b_1, b_2, \ldots, b_{k-1}$ is LLL reduced), and $b_1 \in \mathbb{Z}^m$, we obtain:

$$\begin{aligned} |\mu_{i,j}|^2 &\leq \frac{i+3}{4} \cdot M \cdot \|\widehat{b}_j\|^{-2} && \text{(from Claim 1: } \|b_i\|^2 \leq \tfrac{n+3}{4} M\text{)} \\ &\leq \frac{i+3}{4} \cdot M \cdot \alpha^{j-1} \cdot \|\widehat{b}_1\|^{-2} && \text{(from Lemma 6.1.2)} \\ &\leq \frac{i+3}{4} \cdot M \cdot \alpha^{j-1} && \text{(since } \|b_1\| = \|\widehat{b}_1\| \in \mathbb{Z}\text{)} \end{aligned}$$

■

Lemma 6.2.7
During execution of Stage k, for $j = 1, 2, \dots, k-1$, it is always the case that:

$$|\mu_{k,j}|^2 \le \frac{k+3}{4} \cdot M \cdot \left(\frac{9\alpha}{4}\right)^{k-1}$$

Proof. In stage k the length reduction step

$$b_k := b_k - \lceil \mu_{k,i} \rfloor \cdot b_i$$

yields, for $j = 1, 2, \dots, k-1$:

$$\mu_{k,j} := \mu_{k,j} - \lceil \mu_{k,i} \rfloor \underbrace{\mu_{i,j}}_{|\mu_{i,j}| \le 1/2} \tag{6.4}$$

Each of the $k-1$ operations (6.4) changes $M_k := \max_{j=1,2,\dots,k-1} |\mu_{k,j}|$ so that from $\lceil \mu_{k,i} \rfloor \le M_k + \frac{1}{2}$ we can bound the new M_k from above by:

$$M_k^{\text{new}} \le M_k^{\text{old}} + \tfrac{1}{2}\left(M_k^{\text{old}} + \tfrac{1}{2}\right) \le \tfrac{3}{2} \cdot M_k^{\text{old}} + \tfrac{1}{4} \tag{6.5}$$

By Lemma 6.2.6 at the beginning of Stage k

$$M_k \le \sqrt{\frac{k+3}{4} \cdot M \cdot \alpha^{k-1}}$$

¿From the bound (6.5) the value M_k grows by at most the factor $\left(\frac{3}{2}\right)^{k-1}$ (the summand $\frac{1}{4}$ becomes negligible). Thus:

$$|\mu_{k,j}|^2 \le \left(\frac{3}{2}\right)^{2(k-1)} \cdot \left(\frac{k+3}{4} \cdot M \cdot \alpha^{k-1}\right) = \frac{k+3}{4} \cdot M \cdot \left(\frac{9\alpha}{4}\right)^{k-1}$$

during Stage k. The claim follows. ■

At the start of Stage k the values $\mu_{i,j}$ with $j > k$ can be very large, in which case the procedure is no longer stable. For $j > k$, from the two claims of Lemma 6.2.6 we can only get the bound

$$|\mu_{i,j}|^2 \le \frac{n+3}{4} \cdot M^j.$$

¿From the inequality

$$|\mu_{i,j}|^2 \le \frac{||b_i||^2}{||\widehat{b}_j||^2},$$

from $D_j = \prod_{i=1}^{j} ||\widehat{b}_i||^2$, and from Lemma 6.2.6 on Page 91 we have:

$$|\mu_{i,j}|^2 \le ||b_i||^2 \frac{D_{j-1}}{D_j} \le \frac{n+3}{4} \cdot M \cdot D_{j-1} \le \frac{n+3}{4} \cdot M^j$$

The LLL Algorithm with iterative orthogonalization (Algorithm 6.2.2) avoids the values $\mu_{i,j}$ with $j > k$, and calculates in Stage k only with the values $\mu_{i,j}$ where $1 \leq j < i \leq k$. The formulas for Step 2 of Algorithm 6.2.2 are relevant when $\mu_{i,j}$ and $||\widehat{b}_i||^2$ are floating point numbers. Since the basis $b_1, b_2, \ldots, b_{k-1}$ is already LLL-reduced, it follows from Lemma 6.1.2, page 80, and $\widehat{b_1} = b_1$:

$$||\widehat{b}_j||^2 \geq ||b_1||^2 \, \alpha^{1-j} \qquad \text{for } j = 1, 2, \ldots, k$$

The divisors $c_j = ||\widehat{b}_j||^2$ in the calculation of $\mu_{k,j}$ in Step 2 are thus not arbitrarily small. This is important for limiting errors in floating point computations.

Algorithm 6.2.2 LLL Algorithm with Iterative Orthogonalization

```
INPUT: ▷ Lattice Basis $b_1, b_2, \ldots, b_n \in \mathbb{Z}^m$
       ▷ $\delta$ mit $\frac{1}{4} < \delta < 1$

  1. $c_1 := ||b_1||^2$, $k := 2$     /* $k$ is the stage */
  /* On entry to stage $k$ we have obtained:
       • $\mu_{i,j}$ for $1 \leq j < i < k$
       • $c_i = ||\widehat{b}_i||^2$ for $1 \leq i < k$
  */
  2. WHILE $k \leq n$ DO
       2.1. IF $k = 2$ THEN $c_1 := ||b_1||^2$
       2.2. FOR $j = 1, 2, \ldots, k-1$ DO
                $\mu_{k,j} := \frac{\langle b_k, b_j \rangle - \sum_{i=1}^{j-1} \mu_{j,i}\mu_{k,i}c_i}{c_j}$
            END for
       2.3. $c_k := \langle b_k, b_k \rangle - \sum_{j=1}^{k-1} \mu_{k,j}^2 c_j$
       2.4. Length reduce $b_k$ und correct $\mu_{k,1}, \mu_{k,2}, \ldots, \mu_{k,k-1}$
       2.5. IF $\delta c_{k-1} \geq c_k + \mu_{k,k-1}^2 c_{k-1}$ THEN
                2.5.1. $b_{k-1} \leftrightarrow b_k$, i.e. exchange $b_{k-1}$ und $b_k$
                2.5.2. $k := \max(k-1, 2)$
            ELSE $k := k + 1$
     END while

OUTPUT: $\delta$ LLL-reduced Basis $b_1, b_2, \ldots, b_n$
```

Proposition 6.2.8
On input an integer lattice basis $b_1, b_2, \ldots, b_n \in \mathbb{Z}^m$ with $M := \max_{i=1,2,\ldots,n} \|b_i\|^2$, Algorithm 6.2.2 performs

$$\mathcal{O}\left(n^2 m \left(1 + n \log_{1/\delta} M\right)\right)$$

arithmetic steps on rationals $|\mu_{i,j}| \leq \sqrt{\frac{n+3}{4} \cdot M^j}$ and $|\mu_{k,j}| \leq \sqrt{\frac{n+3}{4} \cdot M \left(\frac{9\alpha}{4}\right)^{k-1}}$, $\|\widehat{b}_j\|^2 \leq M$, and vectors b_i with $\|b_i\|^2 \leq \frac{n+3}{4} \cdot M$. The absolute values of these numerators and denominators of these rationals are bounded by

$$M^{n-\frac{1}{2}} \sqrt{\frac{n+3}{4} \cdot \left(\frac{9\alpha}{4}\right)^n}$$

Proof. By Lemma 6.2.1:

$$\#\text{Exchanges} \leq \binom{n}{2} \cdot \log_{1/\delta} M = \mathcal{O}\left(n^2 \log_2 M\right)$$

Since the stage k is 2 at the beginning of the algorithm and $n+1$ at the end, it is clear that

$$\#\text{Iterations} \leq n - 1 + 2 \cdot \#\text{Exchanges}$$

Every iteration with an exchange and stage reduction yields at most one iteration without an exchange. Every iteration requies at most $\mathcal{O}(nm)$ arithmetic steps. The upper bound on the number of steps follows.

By Lemma 6.2.5 the denominators of the numbers μ_{ij} for $j < n$ are bounded by $D_j \leq M^{n-1}$. By the second claim of Lemma 6.2.6 and by Lemma 6.2.7 we have:

$$|\mu_{i,j}|^2 \leq \frac{n+3}{4} \cdot M \cdot \left(\frac{9\alpha}{4}\right)^{n-1}$$

Thus the numerators of the $\mu_{i,j}$ are bounded in absolute value by

$$\sqrt{\frac{n+3}{4}} \cdot M^{n-\frac{1}{2}} \cdot \left(\frac{9\alpha}{4}\right)^{\frac{n-1}{2}}$$

The numerators and denominators of $\|\widehat{b}_j\|^2 = \frac{D_j}{D_{j-1}}$ are bounded by M^j. The coefficients of the vectors b_i are bounded by $\|b_i\|$ and so by Lemma 6.2.6 on Page 91 they are bounded by $\sqrt{nM}$. Thus the algorithm need only manipulate integers bounded in absolute value by

$$\sqrt{\frac{n+3}{4}} M^{n-\frac{1}{2}} \left(\frac{9\alpha}{4}\right)^{\frac{n-1}{2}}$$

$\blacksquare$

Chapter 7

Babai's Approximation to CVP

In this chapter we present Babai's application of the LLL algorithm to the problem of approximating the closest lattice vector to a given point in $\mathbb{R}^n$. We show an application to the inhomogeneous Diophantine approximation problem. All the material in this chapter appears in [Babai86].

7.1 Approximate CVP

Consider the following "inhomogeneous" version of the shortest vector problem:

Definition 7.1.1
Closest Vector Problem (CVP)

- *Given:* $L \subset \mathbb{R}^n$ *of full rank and* $x \in \mathbb{R}^n$
- *Find:* $x \in \mathbb{R}^n$ *such that* $||x - b||$ *is minimized.*

CVP can be solved in $O(n^{cn})$ arithmetic operations; moreover, given an oracle for the shortest vector problem, CVP can be approximated to within a factor of n in polynomial time [Kannan83]. CVP is $\mathcal{NP}$-hard for any norm; indeed, approximating CVP within a factor of $2^{\lg^{1-\epsilon} n}$ is $\mathcal{NP}$-hard [DKS98]. In this chapter we consider only the 2-norm.

Definition 7.1.2
Approximate CVP

- *Given: basis* $(b_1, b_2, \ldots, b_n)$ *for lattice* L *of full rank and* $x \in \mathbb{R}^n$
- *Find:* $w \in L$ *such that* $||x - w|| \leq c_n ||x - u||$, *where* u *is a nearest neighbor of* x *in* L *and* c_n *depends only on* n.

Let $\delta = \frac{3}{4}$. An LLL-reduced basis with $\delta = \frac{3}{4}$ satisfies

- $|\mu_{ij}| \leq \frac{1}{2}$
- $\frac{1}{\sqrt{2}}\|\widehat{b}_{k-1}\| \leq \|\widehat{b}_k\|$, $k = 2, \dots, n$

Babai [Babai86] presents two simple procedures for solving the approximate CVP yielding, respectively, $c_n = 2^{n/2}$ and $c_n = 1 + 2n(9/2)^{n/2}$.

Procedure 1: Rounding Off
Solve the equation $x = \sum_{i=1}^{n} \beta_i b_i$, for reals $\beta_1, \beta_2, \dots, \beta_n$. For $i = 1, \dots, n$, set $\alpha_i = \lceil \beta_i \rfloor$. Output $w = \sum_{i=1}^{n} \alpha_i b_i$.

Procedure 2: Nearest Plane

1. Let $U = \sum_{i=1}^{n-1} \mathbb{R} b_i$ denote the linear subspace of $\mathbb{R}^n$ equal to $\operatorname{span}(b_1, b_2, \dots, b_{n-1})$. Let $L' = L \cap \operatorname{span}(b_1, b_2, \dots, b_{n-1})$ be the $(n-1)$-dimensional sublattice of L contained in U: $L' = L \cap U$.
2. Find (details explained below) $v \in L$ such that the distance from x to $U + v$ is minimal. Let x' be the orthogonal projection of x onto $U + v$.
3. Recursively find $y \in L'$ near $x' - v$.
4. Output $w = y + v$.

For Step 2, write x as a real linear combination of the orthogonalized vectors $x = \sum_{i=1}^{n} \gamma_i \widehat{b}_i$, where $\gamma_1, \gamma_2, \dots, \gamma_n \in \mathbb{R}^n$. Let $\delta = \lceil \gamma_n \rfloor$. Let $x' = \sum_{i=1}^{n-1} \gamma_i \widehat{b}_i + \delta \widehat{b}_n$. Note that although $U + v$ is the coset of U intersecting L nearest to x, it is not necessarily the case that the nearest neighbor of x in L is in $U + v$. In this way the algorithm "makes a mistake" and so we only get an approximate solution.

Proposition 7.1.3
If B is LLL-reduced with $\delta = \frac{3}{4}$, then Procedure Rounding Off finds a lattice point w nearest to x within a factor of $1 + 2n(9/2)^{/2}$.

Proof. The proof of the Proposition uses the following result regarding the shape of LLL-reduced lattice parallelepipeds, which is of independent interest.

Proposition 7.1.4
Let $b_1, b_2, \dots, b_n$ be LLL-reduced. For $k = 1, \dots, n$, let $U_k = \sum_{j \neq k} \mathbb{R} b_j$, and let Θ_k be the angle between b_k and U_k. Then $\sin \Theta_k \geq (\sqrt{2}/3)^n$.

Proof. See [Babai86]. ■

Since

$$\sin \Theta_k = \min_{m \in U_k} \frac{||m - b_k||}{||b_k||}$$

an equivalent statement of Proposition 7.1.4 is that, for all $m \in U_k$,

$$||b_k|| \leq (9/2)^{n/2} \, ||m - b_k|| \tag{7.1}$$

Let $d_n = (9/2)^{n/2}$. Let w be the output of Procedure Rounding Off. Let us write

$$w - x = \sum_{i=1}^{n} \delta_i b_i \tag{7.2}$$

where for $i = 1, \ldots, n$, $|\delta_i| \leq \frac{1}{2}$ because we rounded the real coefficients in $x = \sum \alpha_i b_i$ to get w.

Let u be a nearest lattice point to x. Write $u - w = \sum_{i=1}^{n} \varphi_i b_i$. Since u and w are both lattice points, $\varphi_1, \varphi_2, \ldots, \varphi_n \in \mathbb{Z}$.

Lemma 7.1.5
$||u - w|| \leq 2nd_n \, ||u - x||$.

Proof. Assume $u \neq w$. Let k satisfy

$$||\varphi_k b_k|| = \max_{1 \leq j \leq n} \{||\varphi_j b_j||\}.$$

Then

$$||u - w|| \leq \sum_{j=1}^{n} ||\varphi_j b_j|| \leq n \, ||\varphi_k b_k|| \tag{7.3}$$

But

$$u - x = (u - w) + (w - x) = \sum_{i=1}^{n} (\varphi_i + \delta_i) b_i$$

Letting

$$m = -\frac{1}{\varphi_k + \delta_k} \sum_{j \neq k} (\varphi_j + \delta_j) b_j$$

we have $m \in U_k$, and we can write

$$u - x = \sum_{i=1}^{n} (\varphi_i + \delta_i) b_i = (\varphi_k + \delta_k)(b_k - m)$$

Thus, by Inequality 7.1, and the fact that the δ_i's are all bounded in absolute value by $\frac{1}{2}$, and $\varphi_k \in \mathbb{Z} \setminus \{0\}$ we have:

$$||u - x|| = |\varphi_k + \delta_k| \, ||b_k - m|| \geq |\varphi_k + \delta_k| \frac{||b_k||}{d_n} \geq \frac{|\varphi_k|}{2d_n} ||b_k||$$

Thus,

$$||u - x|| \, 2d_n \geq |\varphi_k| \, ||b_k|| \tag{7.4}$$

From inequalities 7.3 and 7.4 we have

$$||u - w|| \leq n \, |\varphi| \, ||b_k|| \leq n2d_n \, ||u - x|| \tag{7.5}$$

This completes the proof of the Lemma. ■

By the triangle inequality and Lemma 7.1.5 we have:

$$||x - w|| \leq ||x - u|| + ||u - w|| \leq ||x - u|| \, (1 + 2nd_n).$$

This completes the proof of Proposition 7.1.3. ■

7.2 Inhomogeneous Diophantine Approximation

Recall the definition of the inhomogeneous Diophantine approximation problem from Chapter 1:
Inhomogeneous Diophantine Approximation

- Given: $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_n$, $\varepsilon, Q > 0$
- Find integers $p_1, p_2, \ldots, p_n, q$ such that

$$|\alpha_i - p_i - \beta_i| \leq \varepsilon$$

and $0 < q \leq Q$, or show no such solution exists.

Recall also that Kronecker gave a general condition for the solvability of this problem (see [Cassels71]):

For any $2n$ real numbers $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_n$, either

1. For each $\varepsilon > 0$ there exist integers $p_1, p_2, \ldots, p_n, q$ such that $q > 0$ and

$$|q\alpha_i - p_i - \beta_i| \leq \varepsilon.$$

2. There exist integers $u_1, u_2, \ldots, u_n$ such that $\sum_{i=1}^{n} u_i\alpha_i$ is an integer while $\sum_{i=1}^{n} u_i\beta_i$ is not.

Suppose $\alpha_1, \alpha_2, \dots, \alpha_n$ and $\beta_1, \beta_2, \dots, \beta_n$ are all rationals. Then the first choice in Kronecker's theorem says that there exist $p_1, p_2, \dots, p_n, q$ such that $q\alpha_i - p_i = \beta_i$ for $i = 1, \dots, i$. This is a special kind of linear diophantine equation which, without a bound on q, can be solved in polynomial time (see, *e.g.*, [Frumkin76]). To find a least common denominator $q = q(\varepsilon)$ is $\mathcal{NP}$-hard [EmBoas81]. We next describe a poylnomial time algorithm due to Babai for obtaining a denominator q at most 3^n times larger than optimal, yielding an error of at most $3^n\varepsilon$ [Babai86].

Proposition 7.2.1
Given $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n$, and $\varepsilon > 0$, all in $\mathbb{Q}$, in time polynomial in the lengths of the inputs one can find either

1. *integers $p_1, p_2, \dots, p_n, q$ s.t.*

$$|q\alpha_i - p_i - \beta_i| \le c_n\varepsilon$$
$$|q| \le c_n q(\varepsilon)$$

where $c_n = 4\sqrt{n}2^{n/2}$, or:

2. *a proof that $q = q(\varepsilon)$ is infinite (no solution exists).*

Proof. Replace ε by δ such that $\varepsilon \in (\delta/2, \delta]$ and $\delta = 2^i$ for $i \in \mathbb{Z}$, so that $\ell(\delta) < |\log_2 \varepsilon| + 2$. Define Q to be the product of the denominators of the α_i, $i = 1, 2, \dots, n$ (without loss of generality we can assume these are all positive).

Note that if $q(\varepsilon)$ is finite, then $q(\varepsilon) < Q$. To see this, suppose we have a solution to $|q\alpha_i - p_i - \beta_i| \le \varepsilon$. Let us write $q = kQ + q'$, where $k \in \mathbb{Z}$ and $0 \le q' < Q$. Then we can replace q with q' and replace each p_i with $p_i - kQ\alpha_i$ ($kQ\alpha_i \in \mathbb{Z}$ because the denominator of α_i divides Q). In Procedure Approximate, described below, we will use a guessed value s for the unknown $q(\delta)$. Ultimately, we will find a value for s within $\sqrt{2}$ of $q(\delta)$ by starting with $s = 1$ and repeatedly doubling s, ending with $s = 2^{\lceil \log Q \rceil}$.

Procedure Approximate$(s, \alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n)$

1. Choose a lattice: For $i = 1, 2, \dots, n$, let $e_i \in \mathbb{R}^{n+1}$ denote the ith standard basis vector and let $b_i = -e_i$. Let $b_{n+1} = \sum_{i=1}^n \alpha_i e_i + \frac{\delta}{s} e_{n+1}$.
2. Let $x = \sum_{i=1}^n \beta_i e_i$.
3. Apply the LLL algorithm to $L = L(b_1, b_2, \dots, b_{n+1})$ to obtain a reduced basis $c_1, c_2, \dots, c_{n+1}$ for L.
4. Apply the Nearest Plane procedure within inputs $c_1, c_2, \dots, c_{n+1}, x$ to obtain $w = \sum_{i=1}^n p_i b_i + q b_{n+1} \in L$ near to x.
5. Output $p_1, p_2, \dots, p_n, q$.

Clearly, the $\log Q$ executions of Procedure Approximate require together at most time polynomial in the lengths of the inputs. Let s_0 be the least choice for s for which the output of Procedure

Approximate satisfies Inequality 7.6, if any. If no such s exists then $q(\delta)$ is infinite. Moreover, since if there is a solution with error at most ε then there is a solution with error at most $\delta > \varepsilon$, if no such s exists then $q(\varepsilon)$ is infinite.

Assume now that $q(\varepsilon)$ is finite. Then we have just argued that so is $q(\delta)$. Let $s = 2^i \in (\frac{q(\delta)}{\sqrt{2}}, \sqrt{2}q(\delta)]$. Let $u = \sum_{i=1}^{n} \bar{p}_i b_i + \bar{q}_i b_{i+1}$, where $\bar{p}_1, \bar{p}_2, \ldots, \bar{p}_n, \bar{q}$ satisfy the constraints in Inequalities 7.6 with ε replaced by δ. Then

$$\begin{aligned} \|u - x\|_\infty &= \max_i \{ |\bar{q}\alpha_i - \bar{p}_i - \beta_i| , \frac{|\bar{q}| \, \delta}{s} \} \\ &\leq \delta \cdot \max\{1, \frac{|\bar{q}|}{s}\} \end{aligned}$$

Now, $s \geq \frac{q(\delta)}{\sqrt{2}}$ and $|\bar{q}| \leq q(\delta)$, so

$$\frac{|\bar{q}|}{s} \leq \frac{q(\delta)}{q(\delta)/\sqrt{2}} = \sqrt{2}$$

Thus $\|u - x\|_\infty \leq \delta\sqrt{2}$, whence

$$\|u - x\|_2 \leq \sqrt{2n}\delta$$

The Nearest Plane procedure is shown in [Babai86] to obtain an approximation to within $2^{d/2}$ of the closest vector in lattices of dimension d. Thus,

$$\|w - x\|_2 \leq 2^{\frac{n+1}{2}} \|u - x\|_2 \tag{7.6}$$

$$\leq 2^{\frac{n+1}{2}} \sqrt{n} 2^{\frac{1}{2}} \delta \tag{7.7}$$

$$= 2\sqrt{n} 2^{n/2} \delta \tag{7.8}$$

Moreover,

$$\|w - x\|_2 \geq \|w - x\|_\infty = \max_i \{ |q\alpha_i - p_i - \beta_i| , \frac{|q| \, \delta}{s} \} \tag{7.9}$$

so

$$\begin{aligned} |q\alpha_i - p_i - \beta_i| &\leq 2\sqrt{n}2^{n/2}\delta < 4\sqrt{n}2^{n/2}\varepsilon \\ |q| &\leq 2\sqrt{n}2^{n/2}s < \sqrt{n}2^{(n+3)/2}q(\delta) < \sqrt{n}2^{(n+3)/2}q(\varepsilon) \end{aligned}$$

Finally, since s_0 is "at least as good" as s, the proof is complete. ■

Chapter 8

Breaking the Linear Congruential Generator

We present a general technique of Frieze, Hastad, Kannan, Lagarias, and Shamir for reconstructing truncated integer variables satisfying given linear congruences, and the application of this technique to breaking pseudo-random generators based on linear congruential sequences. The material for this chapter appears in [FHKLS88].

8.1 Linear Congruential Sequences

Knuth [Knuth80] attributes the idea of using a linear congruential sequence as a pseudo-random sequence generator to D.H. Lehmer in 1948. The generator has four parameters:

1. the seed $x_0 \geq 0$;
2. the multiplier $a \geq 0$;
3. the increment $c \geq 0$;
4. the modulus $M > x_0, a, c$.

The corresponding linear congruential sequence is:

$$x_{n+1} = (ax_n + c) \bmod M$$

The sequence always cycles (we want cycles to be long). If $c = 0$ then the period is generally shorter, but the computational cost is lower. Other restrictions on the choice of parameters are studied extensively in [Knuth80], where there is also a long and interesting discussion of the "right" definition of a pseudorandom sequence. This discussion motivated Yao's modern definition of pseudo-random sequences in terms of polynomial time statistical tests [Yao82]. An alternative definition, involving unpredictability, had previously been proposed by Blum and Micali [BluMi]. For completeness, these two definitions, proved equivalent by Yao [Yao82], are stated in Section 8.4.

As usual, we assume that the *method* for generating the sequence is known; the values of (some of) the parameters are secret.

If a, c, and M are unknown, but all of the bits of x_i, $1 \leq i \leq k$ are known, then Boyar showed predictability of the sequence with high accuracy even for relatively small values of k [Boyar82]. In particular, she finds $\widehat{a}, \widehat{c}$, and $\widehat{M}$, consistent with the available data, and extrapolates. If the extrapolated sequence differs from the actual sequence, then the guessed values are corrected accordingly. Boyar shows that at most $O(\log M)$ disagreements can ever occur.

If a and c are unknown, $M = 2^n$ is known, and the $n - \ell$ high order bits y_i of each x_i are known, $1 \leq i \leq k$, then Knuth gives an attack which usually reconstructs a, c, and the seed in $O(n^2 2^{2\ell}/k^2)$ steps [Knuth80].

If c is unknown, M and a are known, and the high order bits y_i of each x_i, $1 \leq i \leq k$, are given as data, then an attack due to Frieze, Hastad, Kannan, Lagarias, and Shamir [FHKLS88] yields:

- a polynomial time reconstruction or prediction procedure (see below), proved to be successful on nearly all problems in which sufficiently many bits of data are known to permit unique reconstruction information-theoretically, provided M is square-free;

- a nearly always polynomial time reconstruction procedure for all M provided $\frac{\ell(y_i)}{\ell(x_i)} \geq \frac{1}{3}$, given only three samples (i.e., $k = 3$).

While unique reconstruction of x_0 may be possible if $c = 0$, the case $c \neq 0$ is different. If we set $x'_i = x_{i+1} - x_i$ and $y'_i = y_{i+1} - y_i$, then x'_i satisfies the recurrence

$$x'_{i+1} \equiv a x'_i (\bmod M)$$

and y'_i is essentially a truncated version of x'_i. This is because x_i and $x_i + d$ yield the same sequence x'_i for any d yet both are linear congruential sequences; indeed, for small d the sequences $\{x_i\}$ and $\{x_i + d\}$ will usually have the same high order bits. In this case future values of the generator may be predicted with great accuracy, even if exact reconstruction is not possible.

Joux and Stern [JoSt94] extend the results of [FHKLS88] to the case in which a and M are unknown, in that in polynomial time they obtain a value $\widehat{M}$ and a heuristic argument that $\widehat{M}$ decreases quickly to M, together with a technique that, given M, finds a.

8.2 A General Reconstruction Result

Frieze *et al.* give a general result, of which the reconstruction of the congruential generator is a simple special case. The general problem is:

Definition 8.2.1 (Reconstruction Problem)

- *Given:* a_{ij} *for* $1 \leq i \leq \ell$ *and* $1 \leq j \leq k$, c_i *for* $1 \leq i \leq \ell$, M, *and* ℓ *modular equations*

$$\sum_{j=1}^{k} a_{ij} x_j \equiv c_i \bmod M \qquad 1 \leq i \leq \ell \tag{8.1}$$

where $0 \leq x_j < M$ *are unknown, and given also some "side information" about some of the bits of the* x_j, *specifically, blocks of consecutive binary digits:*

$$y_j = \left[\frac{x_j}{2^{\ell_2}}\right] \bmod 2^{\ell_1} \qquad 1 \leq j \leq k \tag{8.2}$$

- *Find: the sequence of integer variables* $x_1, x_2, \ldots, x_k$

The interesting case is when ℓ, the number of equations, is strictly less than k, the number of unknowns.

We first consider the question of how much side information is needed to make unique reconstruction possible. Suppose $2^{n-1} \leq M < 2^n$, so that $\ell(x_j) = n$. Each y_j reveals a δ-fraction of the bits of x_j, where $\delta = \ell_1 / \log_2 M$, whenever $\ell_1 + \ell_2 \leq [\log_2 M]$. Suppose we know a block of δn successive bits of each x_j. Usually, ℓ modular equations with side conditions $1 \leq x_i < M$ can be used to eliminate ℓ of the variables. This leaves $k - \ell$ remaining variables, which together contain $(k - \ell)n$ unknown bits. Thus, the $k\delta n$ bits of information given by $y_1, y_2, \ldots, y_k$ must contain enough information to determine $(k - \ell)n$ unknown bits. Hence, we obtain the information-theoretic lower bound: $k\delta n \geq (k - \ell)n$, or in other words, $\delta \geq 1 - \frac{\ell}{k}$.

[FHKLS88] shows that for $\delta = 1 - \frac{\ell}{k} + \varepsilon$, where $\varepsilon = O(k/\log M)$, given δn of the highest order bits of each x_j it is possible to efficiently reconstruct $x_1, x_2, \ldots, x_k$ in "most" instances (see Remark 8.2.3 below). A similar result holds for the case in which we are given the δn lowest order bits of each x_j. For arbitrarily placed windows of consecutive bits, the authors require twice as many bits.

Assume we are given the matrix $A = [a_{ij}] \in \mathbb{Z}^{\ell \times k}$ and the vector $C \in \mathbb{Z}^{\ell}$ satisfying $Ax \equiv C(\bmod M)$. We define the matrix $B \in \mathbb{Z}^{(\ell+k) \times k}$ to be

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1k} \\ a_{21} & a_{22} & \ldots & a_{2k} \\ & & \vdots & \\ a_{\ell 1} & a_{\ell 2} & \ldots & a_{\ell k} \\ M & 0 & \ldots & 0 \\ 0 & M & \ldots & 0 \\ 0 & \ldots & & M \end{bmatrix}$$

Let the lattice $L(A, M)$ be the set of all integer linear combinations of the rows of B. (Recall that we can find a basis for $L(A, M)$ by putting B into Hermite Normal Form.) Let $\widehat{C} \in \mathbb{Z}^{\ell \times k}$ be the vector that agrees with C in positions 1 through ℓ and is 0 in the last k positions. Let $x = (x_1, x_2, \ldots, x_k)^{\mathrm{T}}$. Since $x_i \in \mathbb{Z}$, we have $x_i M \equiv 0(\bmod M)$, and so

$$Bx \equiv \widehat{C} \bmod M$$

Proposition 8.2.2 (Frieze, Hastad, Kannan, Lagarias, and Shamir)
The system

$$\sum_{j=1}^{k} a_{ij}x_j \equiv c_i \bmod M \qquad 1 \leq i \leq \ell$$

has at most one solution $x \in \mathbb{Z}^k$ satisfying $\|x\|_2 \leq M\lambda_k(L(A,M))^{-1}2^{-(k/2)-1}$ (i.e., at most one "small solution). If the a_{ij}, c_i, and M are known, then there exists a polynomial time algorithm that either finds x or proves that no such x exists.

Remark 8.2.3
Let us give some intuition for the application of Proposition 8.2.2. If the x_i are large but we know the most significant bits, then we can rewrite the modular relations in such a way that the new unknowns are "small." Assume this has already been done. If $L(A,M)$ has very small kth successive minimum λ_k, then the claimed polynomial time algorithm can find relatively larger unknowns ($\frac{M}{\lambda_k}$ is larger when λ_k is smaller). If, however, $\lambda_k(L(A,M))$ is large, then the x_i must be smaller in order for the algorithm to be sure to find them. Intuitively, this means that we need more bits of the original x_i's, so that when we rewrite the equations the unknowns are smaller. The bulk of the proof of applicability of the theorem is in analyzing the expected value of $\lambda_k(L(A,M))$ when A is chosen at random (as in most cryptographic applications). Much depends on the structure of M. See [FHKLS88] for details.

Proof. (Sketch) The upper bound λ_k is found via the following result of Lenstra, Lenstra, and Schnorr [LLS90]:

$$\lambda_1^*\lambda_k \leq k^2$$

That is, for full dimensional lattices in $\mathbb{R}^k$, the product of the first successive minimum of the dual and the kth successive minimum of the primal is bounded above by k^2.

The structure of the proof of Proposition 8.2.2 is as follows:

1. Reduce the basis for $L = L(A,M)$ using the LLL algorithm to get modular relations wth small coefficients.

2. Use the (assumed) size constraints on the x_j's to transform these modular equations to equations over the integers.

3. Solve these equations over the integers to recover the exact values of $x_1, x_2, \ldots, x_k$.

We now explain these steps in more detail.

For the first step, starting with the matrix B defined above, in polynomial time find $V \in GL_{k+\ell}(\mathbb{Z})$ such that VB is in Hermite Normal Form with non-zero rows $z_1, z_2, \ldots, z_k$. Thus, $z_1, z_2, \ldots, z_k$ is a basis for the lattice $L(A,M)$. Let Z be the $k \times k$ matrix with rows $z_1, z_2, \ldots, z_k$. Next, define $X \in \mathbb{Z}^{k\times(k+\ell)}$ such that $X(VB) = Z$.

Apply the LLL algorithm with $\delta = \frac{3}{4}$ to the k-dimensional lattice with basis $z_1, z_2, \dots, z_k$ to obtain a unimodular matrix $U \in GL_k(\mathbb{Z})$ and the reduced basis $w_1, w_2, \dots, w_k$ such that, if W is the $k \times k$ matrix with rows $w_1, w_2, \dots, w_k$ we have $UZ = W$ and, by the reducedness of W,

$$||w_i||_2 \leq 2^{k/2}\lambda_k \qquad 1 \leq i \leq k$$

Let $Y = UXV$. Then $W = YB$.

What has happened to our initial set of equations? We had:

$$Bx \equiv \widehat{C} \bmod M$$

and so

$$Y(Bx) \equiv Y\widehat{C} \bmod M$$

and hence

$$(YB)x \equiv Y\widehat{C} \bmod M$$

Let $C' = Y\widehat{C} \bmod M$ (since Y and $\widehat{C}$ are known we can easily find C'). Then since $W = YB$ we have the modular equalities

$$Wx \equiv C' \bmod M \tag{8.3}$$

Let us write $x = (x_1, x_2, \dots, x_k)^{\mathsf{T}}$. For the second step of the algorithm (transformation to a system of equations over $\mathbb{Z}$) observe that, for $1 \leq i \leq \ell$,

$$\begin{aligned} |c'_i| &= \left|\sum_{j=1}^{k} w_{ij}x_j\right| \\ &= |\langle w_i, x\rangle| \\ &\leq ||w_i||\,||x|| \\ &< 2^{k/2}\lambda_k M \lambda_k^{-1} 2^{-(k/2)-1} \\ &= \frac{M}{2} \end{aligned}$$

where the upper bound on the absolute value of the scalar product $\langle w_i, x\rangle$ is real (rather than modular), and the second inequality follows by the reducedness of W and the assumed upper bound on $||x||_2$. Thus, by choosing each c'_i to satisfy $|c'_i| < \frac{M}{2}$ we have that $Wx = C'$ holds over the integers.

Finally, $Wx = C'$ gives us k equations in k unknowns over the integers. We can solve this exactly using Gaussian elimination.

We have used an assumed upper bound on $||x||_2$ to conclude that $|c'_i| < \frac{M}{2}$ "without modding out." ■

Corollary 8.2.4
Let $s_0 = \log \lambda_k + \frac{k}{2} + \frac{1}{2}\log k + 1$. The system

$$\sum_{j=1}^{k} a_{ij}x_j \equiv c_i \bmod M \qquad 1 \le i \le \ell$$

has at most one solution x in which the s_0 most significant bits of each x_j are specified.

Proof. Write $x_i = x_i^{(1)} + x_i^{(2)}$ where $x_i^{(1)}$ are the known s_0 most significant bits of x_i and

$$\left|x_i^{(2)}\right| \le \frac{M}{2^{s_0}} = M\lambda_k^{-1}2^{-(k/2)-1}k^{-1/2}$$

Since this is implies the bound on $||x||$ assumed in Proposition 8.2.2 we can substitute in the known $x_i^{(1)}$ and then apply the Proposition. ■

Remark 8.2.5
We can actually apply the algorithm of Proposition 8.2.2 (and the Corollary) without *knowing λ_k. We follow the steps of the algorithm until we obtain the reduced basis $w_1, w_2, \ldots, w_k$. We then check if the number of bits known in each x_j is at least*

$$\max_i\{\log_2 ||w_i||\} + \frac{1}{2}\log k + 1$$

This provides a sufficient condition for the algorithm to work, because $\max_i \log_2 ||w_i|| \ge \log_2 \lambda_k$ *since, by definition of the kth successive minimum, for any basis $b_1, b_2, \ldots, b_k$ for $L(A, M)$,* $\max_i ||b_i||_2 \ge \lambda_k$.

8.3 Application to the Linear Congruential Generator

For reasons discussed above, we may restrict discussion to the case in which $c = 0$. Thus there are unknowns $x_1, x_2, \ldots, x_k$ that satisfy the congruences $x_{i+1} \equiv ax_i \bmod M$, and we are given the high order bits of the x_i's.

It is easy to see by induction that $a^{i-1}x_1 - x_i \equiv 0 \bmod M$, for $2 \le i \le k$. We define the lattice $L = L(A, M)$ to be the set of all integer linear combinations of the rows of the following matrix:

$$\begin{bmatrix} M & 0 & & \ldots & 0 \\ a & -1 & & \ldots & 0 \\ a^2 & 0 & -1 & \ldots & 0 \\ & & \vdots & & \\ a^{k-1} & 0 & & \ldots & -1 \end{bmatrix}$$

Note that $\det L = M$.

Proposition 8.3.1 (Frieze, Hastad, Kannan, Lagarias, and Shamir)
For square-free $M > c(\varepsilon, k)$ there is an exceptional set $E(M, \varepsilon, k)$ of multipliers of cardinality $|E(M, \varepsilon, k)| \leq M^{1-\varepsilon}$ such that for any multiplier not in $E(M, \varepsilon, k)$ the following is true. The x_i are uniquely determined by knowledge of the $(1/k + \varepsilon) \log M + c(k)$ leading bits of all $\{x_i : 1 \leq i \leq k\}$, where

$$c(k) = \frac{k}{2} + (k-1)\log 3 + \frac{7}{2}\log k + 2.$$

Furthermore, there is an algorithm which runs in time polynomial in $\log M + k$ which finds the x_i.

Remark 8.3.2

1. *The number of bits needed for reconstruction is almost optimal on information-theoretic grounds.*

2. *$a = 1$ is clearly exceptional (although extrapolation is easy in this case!).*

3. *The proof actually shows that ε approaches $\frac{c}{\log \log M}$ as M approaches infinity.*

4. *The x_j are treated as independent unknowns.*

5. *For the special case $k = 3$ [FHKLS88] are able to show that, for any $\varepsilon > 0$, for all M, knowledge of $(\frac{1}{3} + \varepsilon) \log M + c(k)$ leading bits of x_1, x_2, and x_3, allows recovery in polynomial time for all multipliers a except a set of cardinality $c(\varepsilon) M^{1-\varepsilon/2}$.*

8.4 Modern Definitions of Pseudo-Randomness

We present two equivalent definitions of pseudor-random sequences, due, respectively, to Blum and Micali [BluMi] and to Yao [Yao82].

Definition 8.4.1 (ensemble)
Let Σ^k denote the set of all binary strings of length k. An ensemble S is a sequence $\{S_k\}$ such that each S_k is a probability distribution on Σ^k. The random ensemble $R = \{R_k\}$ is the sequence of uniform distributions i.e., $R_k(x) = 2^{-k}$ for all $x \in \Sigma^k$.

Definition 8.4.2 (polynomial-size family of circuits)
A polynomial-size family of circuits is a sequence of circuits $C = \{C_k\}$ such that for some positive integer d, C_k has at most k inputs and at most k^d gates.

Definition 8.4.3 (predicting collection)
A predicting collection is a polynomial-size family of circuits C such that each C_k has $i < k$ inputs and one output bit.

Definition 8.4.4 (unpredictable by C)
For $i < k$, let π_k be the probability that on input the first i bits of $s \in_R S_k$, the circuit C_k outputs the $(i+1)$st bit of s. The ensemble S is unpredictable by C if $\exists d_k \forall k \geq k_d$

$$\pi_k < \frac{1}{2} + \frac{1}{k^d}$$

Definition 8.4.5 (next bit test)
The ensemble S passes the next bit test if it is unpredictable by all predicting collections.

Definition 8.4.6 ($C_k(S)$)
Let C_k be a circuit with k inputs and one output, and let S be any ensemble. Then $C_k(S)$ is the probability that C_k outputs 1 on input $s \in_R S_k$.

Generally speaking, a statistical test is an algorithm than on any input produces a single Boolean output.

Definition 8.4.7 (polynomial-size statistical test; pass a test)
A polynomial-size statistical test is a polynomial-size family of circuits. An ensemble S passes test $T = \{T_k\}$ if $\forall d \exists k_d \forall k \geq k_d$

$$|T_k(S) - T_k(R)| < \frac{1}{k^d}$$

Proposition 8.4.8 (Yao)
Ensemble S passes the next-bit test if and only if it passes all polynomial-size statistical tests.

Proof. See [BoHi89]. ■

Bibliography

[Adel83] L. Adleman, On Breaking Generalized Knapsack Public Key Cryptosystems, Proceedings 15th Annual ACM Symposium on Theory of Computing, 1983, pp. 402–412

[Ajtai96] M. Ajtai, Generating Hard Instances of Lattice Problems, Proceedings 28th Annual ACM Symposium on Theory of Computing, 1996, pp. 99–108 *Electronic Colloquium on Computational Complexity TR96-007*, http://www.eccc.uni-trier.de/eccc-local/Lists/TR-1996.html

[Ajtai98] M. Ajtai, The Shortest Vector Problem in L_2 is NP-Hard for Randomized Reductions, *to appear, Proceedings 30th Annual ACM Symposium on Theory of Computing, 1998*

[AjtDw97] M. Ajtai, C. Dwork, A Public-Key Cryptosystem with Average-Case/Worst-Case Equivalence, Proceedings 29th Annual ACM Symposium on Theory of Computing, 1997; see also *Electronic Colloquium on Computational Complexity TR96-065*, http://www.eccc.uni-trier.de/eccc-local/Lists/TR-1996.html

[Babai86] L. Babai (1986): **On Lovász' Lattice Reduction and the nearest Lattice Point Problem**, Combinatorica, Band 6, Seiten 1–13.

[Barnes59] E.S. Barnes (1959): **The Contruction of perfect and extreme Forms II**, Acta Arithmetica, Band 5, Seiten 205-222.

[BaKa84] A. Bachem und R. Kannan (1984): **Lattices and the Basis Reduction Algorithm**, Technischer Report, Carnegie-Mellon-Universit"at (USA).

[BeWe93] Th. Becker und V. Weispfennig (1993): **Gr"obner Bases — a computational Approach to commutative Algebra**, Graduate Texts in Mathematics, Band 141, Springer-Verlag, Berlin/Heidelberg.

[Blich14] H.F. Blichfeldt (1914): **A new Principle in the Geometry of Numbers with some Applications**, Transaction of the American Mathematical Society, Band 15, Seiten 227–235.

[Blich29] H.F. Blichfeldt (1929): **The Minimum Value of quadratic Forms and the closet Packing of Sphere**, Mathematische Annalen, Band 101, Seiten 366-389.

[Blich35] H.F. Blichfeldt (1935): **The minimum Value of positive Quadratic Forms in six, seven and eight Variables**, Mathematische Zeitschrift, Band 39, Seiten 1–15.

[BluMi] M. Blum and S. Micali (1984): **How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits**, SIAM J. Computing, Vol. 13, No. 4, pp.850–864

[BoHi89] R.B. Boppana and R. Hirschfeld (1989), **Pseudorandom Generators and Complexity Classes**, in Randomness and Computation, Vol. 5, S. Micali Editor, Advances in Computing Research, JAI Press, Greenwich, pp. 1–26.

[Boyar82] J. Boyar (1982): **Inferring Sequences Produced by Pseudo-Random Number Generators**, Proc. 23rd IEEE Conference on Foundations of Computer Science, pp. 153–159.

[Bb65] B. Buchenberger (1965): **Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal**, Dissertation, Fachbereich Mathematik, Universit"at Insbruck ("Osterreich).

[Cassels71] J.W.S. Cassels (1971): **An Introduction to the Geometry of Numbers**, Springer-Verlag, Berlin/Heidelberg.

[Cohen93] H. Cohen (1993): **A Course in Computational Algebraic Number Theory**, Graduate Texts in Mathematics, Band 138, Springer-Verlag, Berlin/Heidelberg.

[CoSl88] J.H. Conway und N.J. Sloane (1988): **Sphere Packings, Lattices and Groups**, Springer-Verlag, New York.

[Copper] D. Coppersmith, Finding a Small Root of a Univariate Modular Equation, *Proc. EUROCRYPT'96*

[CFJP] D. Coppersmith, M. Franklin, J. Patarin, and M. Reiter, Low Exponent RSA with Related Messages, *Proc. EUROCRYPT'96*

[CJLOSS92] M.J. Coster, A. Joux, B.A. LaMacchina, A.M. Odlyzko, C.P. Schnorr und J. Stern (1992): **An improved low-density Subset Sum Algorithm**, Computational Complexity, Band 2, Seiten 111–128.

[CR88] B. Chor und R.L. Rivest (1988): **A Knapsack type Public Key Cryptosystem based on Arithmetic in finite Fields**, IEEE Transaction Information Theory, Band IT-34, Seiten 901–909.

[Di1842] G.L. Dirichlet (1842): **Verallgemeinerung eines Satzes aus der Lehrere von Kettenbr"uchen nebst einigen Anwendungen auf die Theorie der Zahlen**, Bericht "uber die zur Bekanntmachung geeigneter Verhandlungen der K"oniglich Preussischen Akademie der Wissenschaften zu Berlin, Seiten 93–95.

[Dåmgard89] I.B. Dåmgard (1989): **A Design Principle for Hash Functions**, Advances in Cryptology — Proceedings EuroCrypt '89, Lecture Notes in Computer Science, Band 435 (1990), Springer-Verlag, Berlin/Heidelberg, Seiten 416–427.

[Dantzig63] G.B. Dantzig (1963): **Linear Programming and Extensions**, Princeton University Press, Princeton, New Jersey (dt. "Ubersetzung "'Lineare Programmierung und Erweiterungen"' 1966 im Springer-Verlag, Berlin/Heidelberg, erschienen).

[DKS98] I. Dinur, G. Kindler, S. Safra, **Approximating CVP to Within Almost-Polynomial Factors is $\mathcal{NP}$-Hard**, manuscript 1998.

[DKT87] P.D. Domich, R. Kannan und L.E. Trotter (1987): **Hermite normal Form Computation using modulo Determinant Arithmetic**, Mathematics of Operation Research, Band 12, Nr. 1 (Februar), Seiten 50–59.

[EmBoas81] P. van Emde Boas (1981): **Another $\mathcal{NP}$-complete Partition Problem and the Complexity of Computing short Vectors in a Lattice**, Technischer Report 81-04, Fachbereich Mathematik der Universit"at Amsterdam.

[Euchner91] M. Euchner (1991): **Praktische Algorithmen zur Gitterreduktion und Faktorisierung**, Diplomarbeit, Fachbereich Informatik der Johann-Wolfgang-Goethe-Universit"at, Frankfurt/Main.

[Feller68] W. Feller (1968): **An Introduction to Probability Theory and its Application**, Band I, 3. Auflage, John Wiley & Sons, New York.

[Frieze86] A.M. Frieze (1986): **On the Lagarias-Odlyzko Algorithm for the Subset Sum Problem**, SIAM Journal on Computing, Band 15, Nr. 2, Seiten 536–539.

[FHKLS88] A. Frieze, J. Hastad, R. Kannan, J. Lagarias, and A. Shamir (1988): **Reconstructing Truncated Integer Variables Satisfying Linear Congruences**, SIAM Journal on Computing, Volume 17, No. 2, pp 262–280.

[Frumkin76] M. A. Frumkin (1976): **Polynomial Time Algorithms in the Theory of Linear Diophantine Equations**, Fundamentals of Computation Theory, M. Karpinski, ed., Lecture Notes in Computer Science 56, Springer, Berlin, pp. 386–392.

[GaSi78] J. von zur Gathen und M. Sieveking (1978): **A Bound on Solution of linear Integer Equations and Inequations**, Proceedings of the American Mathematical Society, Band 72, Seiten 155–158.

[GaJo79] M.R. Garey und D.S. Johnson (1979): **Computer and Intractability: A Guide to the Theory of $\mathcal{NP}$-Completness**, W.H. Freeman and Company, San Francisco.

[Gauß1801] C.F. Gauß (1801): **Disquisitiones Arithmeticae**, Gerhard Fleischer, Leipzig. Deutsche "Ubersetzung (1889): "'Untersuchung "uber h"ohere Arithmetik"', Springer-Verlag, Berlin/Heidelberg.

[GrLek87] M. Gruber und C.G. Lekkerkerker (1987): **Geometry of Numbers**, 2. Auflage, North-Holland, Amsterdam.

[GLLS88] M. Grötschel, L. Lovász und A. Schrijver (1988): **Geometric Algorithms and combinatorial Optimization**, Algorithms and Combinatorics, Band 2, Springer-Verlag, Berlin/Heidelberg.

[HaMcC91] J. Hafner und K. McCurley (1991): **Asymptotic Fast Triangulation of Matrices over Ring**, SIAM Journal on Computing, Band 20, Nr. 6, Seiten 1068–1083.

[H] J. Hastad, Solving Simultaneous Modular Equations of Low Degree, *SIAM J. Computing 17*(2), pp.336–341, 1988

[HJLS89] J. Håstad, B. Just, J.C. Lagarias und C.P. Schnorr (1989): **Polynomial Time Algorithms for Finding Integer Relations among real Numbers**, SIAM Journal on Computing, Band 18, Nr. 5, Seiten 859–881.

[Helfrich85] B. Helfrich (1985): **Algorithms to construct Minkowski reduced and Hermite reduced Lattice Bases**, Theoretical Computer Science, Band 41, Seiten 125–139.

[Hermite1850] C. Hermite (1850): **Extraits de lettres de M. Ch. Hermite à M. Jacobi sur differents objets de la théorie des nombres, Deuxième lettre**, Reine Angewandte Mathematik, Band 40, Seiten 279–290.

[Hlawka44] E. Hlawka (1944): **Zur Geometrie der Zahlen**, Mathematische Zeitschrift, Band 49, Seiten 285–312.

[Hörner94] H.H. H"orner (1994): **Verbesserte Gitterbasenreduktion; getestet am Chor-Rivest-Kryptosystem und an allgemeinen Rucksackproblemen**, Diplomarbeit, Fachbereich Mathematik der Johann-Wolfgang-Goethe-Universit"at, Frankfurt/Main.

[ImpNa96] R. Impagliazzo and M. Naor, Efficient Cryptographic Schemes Provably as Secure as Subset Sum, *J. Cryptology 9*, pp. 199–216, 1996

[John48] F. John (1948): **Extremum Problems with Inequalities as subsidiary Conditions**, in K.O. Friedrichs, O.E. Neugebauer und J.J. Stoker (Ed.): "'Studies and Essays presented to R. Courant on his 60th Birthday Januar 8, 1948"', Interscience Publisher, New York, Seiten 187–204.

[JoSt94] A. Joux und J. Stern (1994): **Lattice Reduction: A Toolbox for the Cryptanalyst**, Technischer Report, DGA/CELAR, Bruz (Frankreich). To appear, Journal of Cryptology.

[KaLe78] G.A. Kabatiansky und V.I. Levenshtein (1978): **Bounds for Packings on a Sphere and in Space**, Problems of Information Transmission, Band 14, Seiten 1–17.

[Kaib91] M. Kaib (1991): **The Gauß Lattice Basis Reduction succeeds with any Norm**, Proceedings of Fundamentals of Computation Theory (FCT '91), Springer Lecture Notes in Computer Science, Band 591, Seiten 275–286.

[Kaib94] M. Kaib (1994): **Gitterbasenreduktion f"ur beliebige Normen**, Dissertation, Fachbereich Mathematik der Johann-Wolfgang-Goethe-Universit"at, Frankfurt/Main.

[KaSchn96] M. Kaib und C.P. Schnorr (1996): **The Generalized Gauss Reduction Algorithm**, Journal of Algorithms, Band 21, Nr. 3 (November), Seiten 565–578.

[KaBa79] R. Kannan und A. Bachem (1979): **Polynomial Algorithm for Computing the Smith and the Hermite Normal Form of an Integer Matrix**, SIAM Journal on Computing, Band 8, Seiten 499–507.

[Kannan83] R. Kannan (1983): **Improved Algorithms for Integer Programming and Related Lattice Problems**, Proceedings of the 15th ACM Symposium on Theory of Computing, pp.193–206

[Kannan87] R. Kannan (1987): **Minkowski's Convex Body Theorem and Integer Programming**, Mathematics of Operation Research, Band 12, Nr. 3 (August), Seiten 415–440.

[Karma84] M. Karmarkar (1984): **A new Polynomial-Time Algorithm for Linear Programming**, Combinatorica, Band 4, Seiten 373–395.

[Khach79] L.G. Khachiyan (1979): **A Polynomial Algorithm in Linear Programming**, Soviet Mathmatics Doklady, Band 20, Seiten 191–194.

[Khach80] L.G. Khachiyan (1980): **Polynomial Algorithms in Linear Programming**, U.S.S.R. Computational Mathematics and Mathematical Physics, Band 20, Seiten 53–72.

[Khin35] A. Khintchine (1935): **Continued Fractions**, Moscow-Leningrad

[KoZo1872] A. Korkine und G. Zolotareff (1872): **Sur les formes quadratique positive quaternaires**, Mathematische Annalen, Band 5, Seiten 366-389.

[KoZo1873] A. Korkine und G. Zolotareff (1873): **Sur les formes quadratique**, Mathematische Annalen, Band 6, Seiten 366–389.

[KoZo1877] A. Korkine und G. Zolotareff (1877): **Sur les formes quadratique positive**, Mathematische Annalen, Band 11, Seiten 242–292.

[Knuth71] D.E. Knuth (1971): **The Art of Computer Programming**, Fundamental Algorithms, Band I, Addison-Wesley, Reading.

[Knuth80] D.E. Knuth (1980): **The Art of Computer Programming**, Fundamental Algorithms, Volume II, Addison-Wesley, Reading, MA.

[LARIFARI] M. Kaib, R. Mirwald, C. R"ossner, H.H. H"orner, H. Ritter (1994): **Programmieranleitung f"ur LARIFARI — Version 13.07.1994**, Fachbereiche Mathematik und Informatik der Johann-Wolfgang-Goethe-Universit"at, Frankfurt/Main.

[La1773] J.L. Lagrange (1773): **Recherches d'arithmétique**, Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres, Berlin, Seiten 265–312.

[Lang93] S. Lang (1993): **Algebra**, 3. Auflage, Addison-Wesley, Reading.

[LLS90] J.C. Lagarias, H.W. Lenstra und C.P. Schnorr (1990): **Korkin-Zolotarev Bases and successive Minima of a Lattice and its reciprocal lattice**, Combinatorica, Band 10, Seiten 333–348.

[LaOd85] J.C. Lagarias und A.M. Odlyzko (1985): **Solving low-density Subset Sum Problems**, Journal of ACM, Band 32, Nr. 1, Seiten 229–246.

[LLL82] A.K. Lenstra, H.W. Lenstra und L. Lovász (1982): **Factoring Polynomials with Rational Coefficients**, Springer Mathematische Annalen, Band 261, Seiten 515–534.

[Lenstra83] H.W. Lenstra (1983): **Integer Programming in a fixed Number of Variables**, Mathematics of Operation Research, Band 8, Nr. 4 (November), Seiten 538–548

[Lovász86] L. Lovász (1986): **An algorithmic Theory of Numbers, Graphs and Convexity**, CBMS-NSF Regional Conference Series in Applied Mathematics, Band 50, SIAM Publications, Philadelphia.

[LoSc92] L. Lovász und H. Scarf (1992): **The Generalized Basis Reduction Algorithm**, Mathematics of Operation Research, Band 17, Nr. 3 (August), Seiten 751–764.

[MaOd90] J.E. Mazo und A.M. Odlyzko (1990): **Lattice Points in high-dimensional Sphere**, Monatsheft Mathematik, Band 110, Seiten 47–61.

[Mink1896] H. Minkowski (1896): **Geometrie der Zahlen**, erste Auflage, Teubner-Verlag, Leipzig.

[Mink1911] H. Minkowski (1911): **Gesammelte Abhandlungen**, Band I und II, Teubner-Verlag, Leipzig.

[Mishra93] B. Mishra (1993): **Algorithmic Algebra**, Texts and Monographs in Computer Science, Springer-Verlag, New-York.

[Orton1994] G. Orton (1994): **A multiple-iterated Trapdoor for dense compact Knapsacks**, Advances in Cryptology — Proceedings EuroCrypt '94, Lecture Notes in Computer Science, Band 950 (1995), Springer-Verlag, Berlin/Heidelberg, Seiten 112–130.

[PaSchn87] A. Paz und C.P. Schnorr (1987): **Approximating Integer Lattices by Lattices with cyclic Factor Group**, 14.th International Colloquium on Automata, Languages and Programming (ICALP), Lecture Notes in Computer Science, Band 267, Springer-Verlag, Berlin/Heidelberg, Seiten 386–393.

[Rieger78] G.J. Rieger (1978): **"uber die mittlere Schrittzahl bei Divisionsalgorithmen**, Mathematische Nachrichten, Band 82, Seiten 157–180.

[Ritter96] H. Ritter (1996): **Breaking Knapsack Cryptosystems by ℓ_∞-norm Enumeration**, Proceedings of the 1.st International Conference on the Theory and Applications of Cryptography — PragoCrypt '96, CTU Publishing House, Prag, Seiten 480–492.

[Ritter97] H. Ritter (1997): **Aufz"ahlung kurzer Gittervektoren in allgemeiner Norm**, Dissertation, Fachbereich Mathematik der Johann-Wolfgang-Goethe-Universit"at, Frankfurt/Main.

[Rogers64] C.A. Rogers (1964): **Packing and Covering**, Cambridge University Press, Cambridge.

[Schnorr87] C.P. Schnorr (1987): **A Hierarchy of polynomial time Lattice Basis Reduction Algorithms**, Theoretical Computer Science, Band 53, Seiten 201–224.

[Schnorr88] C.P. Schnorr (1988): **A more efficient Algorithm for Lattice Basis Reduction**, Journal of Algorithms, Band 9, Seiten 47–62.

[Schnorr91a] C.P. Schnorr (1991): **Gittertheorie und ganzzahlige Optimierung**, Skript zur Vorlesung, Johann-Wolfgang-Goethe-Universit"at, Frankfurt/Main.

[Schnorr91b] C.P. Schnorr (1991): **Factoring Integers and Computing Discrete Logarithms via Diophantine Approximation**, Advances in Cryptology – Proceedings EuroCrypt '91, Lecture Notes in Computer Science, Band 547, Springer-Verlag, Berlin/Heidelberg, Seiten 171–181.

[SchnEu91] C.P. Schnorr und M. Euchner (1991): **Lattice Basis Reduction: improved Algorithms and solving Subset Sum Problems**, Proceedings of Fundamentals of Computation Theory (FCT '91), Lecture Notes in Computer Science, Band 591, Springer-Verlag, Berlin/Heidelberg, Seiten 68–85.

[Schnorr93] C.P. Schnorr (1993): **Factoring Integers and Computing Discrete Logarithms via Diophantine Approximation**, Advances in Computational Complexity, Ed. Jim-Yi Cai, AMS DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Band 13, Seiten 171–182.

[Schnorr94a] C.P. Schnorr (1994): **Block Reduced Lattice Bases and Successive Minima**, Combinatorics, Probability and Computing, Band 3, Seiten 507–522.

[Schnorr94b] C.P. Schnorr (1994): **Gittertheorie und Kryptographie**, Ausarbeitung, Johann-Wolfgang-Goethe-Universit"at, Frankfurt/Main.

[SchnHö95] C.P. Schnorr und H.H. H"orner (1995): **Attacking the Chor-Rivest Cryptosystem by improved Lattice Reduction**, Advances in Cryptology — Proceedings EuroCrypt '95, Lecture Notes in Computer Science, Band 921, Springer-Verlag, Berlin/Heidelberg, Seiten 1–12.

[Schrijver86] A. Schrijver (1986): **Theory of Linear and Integer Programming**, Wiley-Interscience Series in discrete Mathematics and Optimization, John Wiley & Son Ltd.

[Seysen93] M. Seysen (1993): **Simultaneous Reduction of a Lattice and its reciprocal Basis**, Combinatorica, Band 13, Seiten 363–376.

[Shamir82] A. Shamir, A Polynomial-Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem, *Proc. 23rd Annual Symposium on Foundations of Computer Science*, 1982, pp. 145–152

[Siegel89] C.L. Siegel (1989): **Lectures on the Geometry of Numbers**, Springer-Verlag, Berlin/Heidelberg.

[Smith1861] H.J.S. Smith (1861): **On Systems of linear indeterminate Equations and Congruences**, Philosophical Transaction of the Royal Society of London, Band 151, Seiten 293–326.

[SpStr76] E. Specker und V. Strassen (1976): **Komplexit"at von Entscheidungsproblemem**, Lecture Notes in Computer Science, Band 43, Springer-Verlag, Berlin/Heidelberg.

[Vetchin82] N.M. Vetchinkin (1982): **Uniqueness of Classes of positive quadratic Forms on which Values of the Hermite Constants are attained for $6 \leq n \leq 8$**, Proceedings of the Steklov Institute of Mathematics, Nr. 3, Seiten 37–95.

[Watson66] G.L. Watson (1966): **On the Minimum of a positiv Quadratic Form in n ($n \leq 8$) Variables (Verification of Blichfeldt's Calculations)**, Proceeedings of the Cambrigde Philosophical Society (Mathematical and Physical Science), Band 62, Seite 719.

[Ye91] Y. Ye (1991): **Potential Reduction Algorithm for Linear Programming,** Mathematical Programming, Band 51, Seiten 239–258.

[Yao82] A. Yao (1982): **Theory and Applications of Trapdoor Functions**, Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science

Positive Applications of Lattices to Cryptography[*]

Cynthia Dwork

IBM Almaden Research Center.

Abstract. We describe constructions of several cryptographic primitives, including hash functions, public key cryptosystems, pseudo-random bit generators, and digital signatures, whose security depends on the assumed worst-case or average-case hardness of problems involving lattices.

1 Introduction

Initiated by Ajtai's paper "Generating Hard Instances of Lattice Problems," a burgeoning effort to build cryptographic primitives based on the assumed hardness of worst-case or random instances of problems involving lattices has proved extremely fruitful. Prior to Ajtai's work, lattices, and in particular, the lattice basis reduction algorithm of Lenstra, Lenstra, and Lovász, were used in cryptography principally to prove cryptographic *in*security [1, 9, 10, 20, 22, 25]. We describe more positive applications of lattices: constructions for public key cryptosystems, cryptographically strong hash functions, and pseudo-random bit generators whose security depends only on the worst-case hardness of the underlying lattice problem; a digital signature scheme whose security depends on the average hardness of the underlying problem.

2 Definitions

Many of the definitions included here are *extremely* informal. References for precise definitions are included in every case.

2.1 Cryptography

A *one-way* function is easy to compute and hard to invert. A *trapdoor* function is a one-way function for which there exists some special "trapdoor" information, so that given the trapdoor information the function is easy to invert, but without the trapdoor information the function is hard to invert (see [12]).
A *public key cryptosystem* is a method of encrypting messages using publicly known information called the *public key*, in such a way that only the party knowing the corresponding *private key* can decrypt the ciphertext. Thus, encryption has a trapdoor nature: without the trapdoor information (the private key) decryption is hard, but decryption is easy given the private key (see [16] and [11]).
A *digital signature scheme* is a method of generating a (public key, private key) pair, together with a pair of procedures SIGN, and VERIFY. SIGN requires as input the message to be signed and the private key of the signer, while VERIFY, requires as input the message, its purported signature, and the public key of the claimed signer. Let (K, s) be a (public key, private key) pair. Let (m, α) be a claimed (message, signature) pair. Given (m, α, K) the VERIFY procedure, without knowing the secret s, verifies that $\alpha = \text{SIGN}(m, s)$ (see [17]).
A *one-way hash function* is a one-way function h mapping long strings to short strings, say, $h : \{0,1\}^n \rightarrow \{0,1\}^\ell$ for $n > \ell$. *One-way* hash functions have many uses in cryptography. In particular they are used to "shrink" long messages before signing (see [24]). Thus, what is actually signed is $h(m)$ rather than m ($h(m)$ is sometimes called a *message digest*). In this case the VERIFY procedure checks that $\alpha = \text{SIGN}(h(m), s)$. For this application it is essential that, given $h(m)$, it is hard to find a different message $m' \neq m$, for which $h(m') = h(m)$. A little more formally, a family of *universal one-way hash functions* is a collection $\mathcal{F}$ of functions $f : \{0,1\}^m \rightarrow \{0,1\}^{l(m)}$ with the property that for any element $x \in \{0,1\}^m$,

[*] This paper appeared in the proceedings of the 22nd International Symposium on Mathematical Foundations of Computer Science, *LNCS 1295*, Springer, 1997.

if f is chosen at random from the collection $\mathcal{F}$, then it is hard to find an element $y \neq x$ such that $f(y) = f(x)$. Each choice of $l(m)$ yields a class of hash functions. A slightly stronger notion is *collision-intractability*: for a randomly selected function $f \in \mathcal{F}$, it is hard to find x, y such that $x \neq y$ and $f(x) = f(y)$.

A *pseudorandom bit generator* is a (deterministic) function that takes as input a string $s \in \{0,1\}^n$ and produces as output a string $p \in \{0,1\}^m$ where $m > n$. Moreover, the strings produced in this way when the inputs s are random should be polynomial-time indistinguishable from truly random strings of length m. Thus these functions appear to manufacture some additional bits of randomness (see [6, 26]; extensive treatment appears in [23]).

The *subset sum problem* of dimensions m and l is: given m numbers $\mathbf{a} = (a_1, \ldots, a_m)$, each of length l, and a number T, find a subset $S \subset \{1, \ldots, m\}$ such that $\sum_{i \in S} a_i = T \bmod 2^l$. The subset sum problem can be viewed as that of inverting the function $f(\mathbf{a}, S) = \mathbf{a}, \sum_{i \in S} a_i \bmod 2^{l(n)}$.

2.2 Lattices

The fundamental concepts concerning lattices can be found in [8, 18, 19].

If $a_1, ..., a_n$ are linearly independent vectors in $\mathbb{R}^n$, then we say that the set $\{\sum_{i=1}^n k_i a_i | k_1, ..., k_n \in \mathbb{Z}\}$ is a lattice in $\mathbb{R}^n$. We will denote this lattice by $L(a_1, ..., a_n)$. The set $a_1, ..., a_n$ is called a basis of the lattice; its length is $\max_{1 \leq i \leq n} \|a_i\|$. The determinant of a lattice L will be the absolute value of the determinant of the matrix whose columns are the vectors $a_1, ..., a_n$. We let $\mathrm{bl}(L)$ denote the length of the shortest basis for L.

The *dual* lattice of L, denoted L^*, is defined as

$$L^* = \{x \in \mathbb{R}^n \mid x^T y \in \mathbb{Z} \text{ for all } y \in L\}.$$

If $(b_1, \ldots, b_n)$ is a basis of L then $(c_1, \ldots, c_n)$ is a basis for L^*, where

$$c_i^T b_j = \begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j \end{cases}$$

Thus, if we represent the lattice $L = L(b_1, \ldots, b_n)$ by a matrix B with columns $b_1, \ldots, b_n$, then the dual of L is the lattice spanned by the rows of B^{-1}. Each basis vector b_i in $L = L(b_1, \ldots, b_n)$ induces a collection of mutually parallel $(n-1)$-dimensional hyperplanes, where, for $k \in \mathbb{Z}$, the kth hyperplane in the collection is the set of all points whose inner product with b_i is equal to k. The distance between adjacent hyperplanes in the collection is $\|b_i\|^{-1}$. Thus, if $\|b_i\| < \|b_j\|$, then adjacent hyperplanes in the ith collection are farther apart than adjacent hyperplanes in the jth collection. As the formula for computing the basis for the dual makes clear, the dual lattice is the set of points that are intersections of n hyperplanes, one from each of the n collections.

Assume n is a positive integer, $M > 0$, $d > 0$ are real numbers, and $L \subseteq \mathbb{Z}^n$ is a lattice which has an $n-1$ dimensional sublattice L' with the following properties:

1. L' has a basis of length at most M;
2. if H is the $n-1$ dimensional subspace of $\mathbb{R}^n$ containing L' and $H' \neq H$ is a coset of H intersecting L, then the distance of H and H' is at least d.

We say that L is a (d, M)-lattice. If $d > M$, then L' is unique. In this case L' will be denoted by $L^{(d,M)}$.

If $a_1, \ldots, a_n \in \mathbb{R}^n$ are linearly independent vectors, then $\mathcal{P}^-(a, \ldots, a_n)$ denotes the half-closed parallelepiped $\{\sum_{i=1}^n \gamma_i a_i | 0 \leq \gamma_i < 1, i = 1, \ldots, n\}$. By "$x \bmod \mathcal{P}$" we mean the unique vector $x' \in \mathcal{P}^-(a_1, \ldots, a_n)$ so that $x - x'$ is an integer linear combination of the vectors $a_1, \ldots, a_n$.

The *orthogonality defect* of an $n \times n$ matrix B is the quantity $\frac{1}{det(B)} \prod_{i=1}^n \|b_i\|$. The *dual orthogonality defect* of B is the quantity $\frac{1}{det(B^{-1})} \prod_{i=1}^n \|\hat{b_i}\|$, where for $1 \leq i \leq n$, $\hat{b_i}$ is the ith row of B^{-1}.

3 Generating Hard Instances of Lattice Problems

Cryptographic constructions necessarily require random choices: if, for example, the choice of a key were deterministic, then the key could not be secret. Thus, the security of the construction relies on the intractability of a *random* instance of the problem on which the construction is based. It has therefore been a longstanding goal in cryptography to find a "hard" problem for which one can establish an explicit connection between the hardness of random instances and the hardness of the hardest, or worst-case, instances.

Such a connection is the contribution of the celebrated paper of Ajtai, "Generating Hard Instances of Lattice Problems" [2]. Specifically, the paper presents a random problem whose solution would imply the solution of three famous worst-case problems:

1. Find the length of a shortest nonzero vector in an n-dimensional lattice approximately, up to a polynomial factor.
2. Find the shortest nonzero vector in an n-dimensional lattice L where the shortest vector v is unique in the sense than any other vector whose length is at most $n^c\|v\|$ is parallel to v, where c is a sufficiently large absolute constant.
3. Find a basis $b_1, \ldots, b_n$ in the n-dimensional lattice L whose length, defined as $\max_{i=1}^n \|b_i\|$, is the smallest possible up to a polynomial factor.

Ajtai's Random Lattice Problem. For $n, m, q \in \mathcal{N}$ such that $n \log q < m \leq \frac{q}{2n^4}$ and $q = O(n^c)$ for a fixed $c > 0$, given a matrix $M \in \mathbb{Z}_q^{n \times m}$ (that is, an $n \times m$ matrix of integers in [0,q-1] of a certain form described below), find a vector $x \neq 0 \in \mathbb{Z}_q^m$ so that $Mx \equiv 0 \bmod q$ and $\|x\| < n$. The lattices are defined modulo q, in the sense that if two vectors are congruent modulo q then either both are in the lattice or neither is in the lattice. Thus the matrix M and the integer q define the lattice: $x \in \Lambda(M, q)$ iff $Mx \equiv 0(\text{mod} q)$.

The matrix M is obtained as follows. Randomize vectors $v_1, \ldots, v_{m-1}$ independently and with uniform distribution on the set of all vectors $\langle x_1, \ldots, x_n \rangle \in \mathbb{Z}_q^n$. Independently randomize a $0, 1$ sequence $\delta_1, \ldots, \delta_{m-1}$, where the numbers δ_i are chosen independently and uniformly. Then define $v_m = -\sum_{i=1}^{m-1} \delta_i v_i \bmod q$ with the additional constraint that each component of v_m is an integer in $[0, q-1]$. The matrix M has columns $v_1, \ldots, v_m$. The class of lattices $\Lambda(M, q)$ defined by matrices of this type will be called λ. The random problem is to find a vector in $\Lambda(M, q)$ of length less than n. Note that $(\delta_1, \ldots, \delta_{m-1}, 1) \in \Lambda(M, q)$ and its length is $O(\sqrt{m})$, so this vector is a solution when $m < n^2$.

Let L be an n-dimensional lattice, let $a_1, \ldots, a_n$ be a set of linearly independent vectors in L and let $M = \max_{i=1}^n \|a_i\|$. The heart of Ajtai's work is a procedure which, if $M > n^c \text{bl}(L)$ for a fixed consant c, uses an oracle for the random lattice problem just defined to obtain another set of linearly independent elements in L whose maximum length is at most $\frac{1}{2} \max_{1 \leq i \leq n} \|a_i\|$.

In rough outline the procedure works as follows. Starting from $a_1, \ldots, a_n$, construct a set of linearly independent lattice vectors $f_1, \ldots, f_n$ such that $\max_{i=1}^n \|f_i\| \leq n^3 M$ and $W = \mathcal{P}(f_1, \ldots, f_n)$ is close to a cube, in the sense that each vertex of W will be at most distance nM from a fixed cube. If the space is covered with the cells of a lattice determined by a short basis, then most of the cells intersecting W lie completely in the interior of W. This implies that every parallelepiped of the form $u + W$, $u \in \mathbb{R}^n$, has roughly the same number of lattice points. Moreover, this also holds for parallelepipeds of the form $u + \frac{1}{q}W$ for $q = [n^{c_2}]$, where c_2 is sufficiently small with respect to c. Thus, if we pick a lattice point v at random from a set D of parallelepipeds of the form $u + \frac{1}{q}W$ with non-overlapping interiors, then the distribution induced on D – that is, the choice of which element in D contains v – is very close to the uniform distribution.

The set D of parallelepipeds $u + \frac{1}{q}W$ that is of interest to us is that obtained by cutting W into q^n small parallelepipeds by dividing each of the vectors f_i into q pieces of equal length. Thus each of the small parallelepipeds is of the form $(\sum_{i=1}^n t_i \frac{f_i}{q}) + \frac{1}{q}W$, where $0 \leq t_i < q$, $i = 1, \ldots, n$ is a sequence of integers; that is, $\langle t_1, \ldots t_n \rangle \in \mathbb{Z}_q^n$. Let us call the vector $o = \sum_{i=1}^n t_i \frac{f_i}{q}$ the *origin* of the parallelepiped. We will name an element of D by the vector $t(o) = \langle t_1, \ldots, t_n \rangle$ of coefficients of the $\frac{f_i}{q}$ defining its origin. If we choose a random set of lattice points $\xi_1 \ldots, \xi_m$ in W and look at, for each ξ_j, the name $t(o_j)$ of the parallelepiped containing ξ_j, then we get a sequence $t(o_1), \ldots, t(o_m)$ of elements chosen almost uniformly from D. Express each ξ_j as the sum of the origin o_j and an offset $\delta_j \in \frac{1}{q}W$. Note that the offset is relatively short: since δ_j is contained in $\frac{1}{q}W$, $\|\delta_j\|$ is bounded by n times the length of the longest side of W. That is, $\max_{1 \leq j \leq m} \|\delta_j\| \leq n(\frac{1}{q}n^3 M)$.

By definition of D and the fact that the distribution induced on D by the choice of ξ is almost uniform, each $t(o_j)$ is distributed almost uniformly in $\mathbb{Z}_q^n$. Let $m = [c_1 n \log n]$. Consider the sequence $t(o_1), \ldots, t(o_m)$ as a value of the random variable λ (it is shown in [2] that the distribution of

$t(o_1), \ldots, t(o_m)$ is extremely close to that of λ). If there exists an algorithm $\mathcal{A}$ that can solve Ajtai's random lattice problem, then using $\mathcal{A}$ we can find a short (length at most n) vector $h = \langle h_1, \ldots, h_m \rangle \in \mathbb{Z}^m$ satisfying $\sum_{j=1}^{m} h_j t(o_j) \equiv 0 \bmod q$.
Writing the lattice vector $\sum_{j=1}^{m} h_j \xi_j$ as the weighted sum of origins and offsets, we get

$$w = \sum_{j=1}^{m} h_j \xi_j = \sum_{j=1}^{m} h_j o_j + \sum_{j=1}^{m} h_j \delta_j \ .$$

Critically, since $\sum_j h_j t(o_j) \equiv 0 \bmod q$, we have that $\sum_j h_j o_j$ is an integer linear combination of the vectors $(f_1, \ldots, f_n)$. Since the f_i are lattice vectors, so is $\sum_j h_j o_j$. Since w is also in L the difference $w - \sum_j h_j o_j = \sum_j h_j \delta_j \in L$. Finally, since $| \sum_{j=1}^{m} h_j^2 | \leq n^2$ and, as noted above, each of the offsets is also relatively short, the lattice vector $\sum_{1 \leq j \leq n} h_j \delta_j$ is relatively short: $\| \sum_{1 \leq j \leq n} h_j \delta_j \| \leq n^2 (n^4 M \frac{1}{q})$, which is less than $\frac{M}{2}$ if q is sufficiently large (say, $q \geq n^7$).
Recently, Ajtai's results have been tightened by Cai and Nerurkar [7]. Through a number of technical steps, Cai and Nerurkar are able to shrink the constant c in Ajtai's reduction, slightly better than halving it.
Based solely on the results in [2], it is possible to design a number of *interactive* cryptographic procedures, including schemes for identification, bit commitment, and coin flipping [3].

4 Hashing

The reduction described in the previous section has implications for the security of the following family of hash functions, studied by Impagliazzo and Naor [21]:
Let $l(m) = (1 - c)m$ for $c > 0$. For $a_1, \ldots, a_m \in \{0,1\}^{l(m)}$ the function $f_{\mathbf{a}} = f_{a_1, \ldots, a_m} : \{0,1\}^m \rightarrow \{0,1\}^{l(m)}$ is defined as follows. Let the m-bit number x be written $x = x_1 x_2 \ldots x_m$ where each $x_i \in \{0,1\}$. Then $f_{\mathbf{a}}(x) = \sum_{i=1}^{m} x_i a_i \bmod 2^{l(m)}$.
The bits of x act as selectors to determine which of the a_i are summed. We can represent the function as a $1 \times m$ matrix M with columns $a_1, \ldots, a_m$. Given $x \in \{0,1\}^m$, the value of the function is $Mx \bmod 2^{l(m)}$.
As we next explain, Ajtai's proof shows that the ability to solve a random instance of the subset sum problem implies the ability to solve the worst-case lattice problems listed in Section 3 (additional details appear in [2]). So if we assume that these worst-case problems are hard for dimension n, then these randomized subset sum problems will be hard as well. To illustrate this connection, let $q = [n^{c_2}]$ and $m = [c_1 n \log n]$ as in the discussion of Ajtai's reduction in Section 3. Let $N = q_1 q_2 \ldots q_n$ where each q_i is a distinct prime in $[q, 2q]$. Let $a_1, \ldots, a_m, b$ be random integers modulo N. Consider the subset sum problem of finding $x \in \{0,1\}^m$ such that $\sum_{i=1}^{m} x_i a_i \equiv b \bmod N$.

Remarks.
(1) The numbers a_i are of length $l(m) \approx n \log q = (1 - c)m$ for some $c > 0$ if $c_1 > c_2$. So subset sum problems of this type are essentially those in the Impagliazzo-Naor family of hash functions.
(2) If $x \in \{0,1\}^m$ then $\|x\| \leq \sqrt{m} < n$.

We may express each a_i as a vector of remainders modulo the primes $q_1, \ldots, q_n$: $a'_i = (a^i_1, \ldots, a^i_n)$, where $a^i_j \in \mathbb{Z}_{q_j}$, for $1 \leq i \leq m$ and $1 \leq j \leq n$. Note that if a_i is chosen uniformly from $\mathbb{Z}_N$ then a'_i is implicitly chosen uniformly from $\mathbb{Z}_{q_1} \times \ldots \times \mathbb{Z}_{q_n}$. Similarly, let b' be the Chinese remainder decomposition of b. Let M be the $n \times m$ matrix with columns $a'_1, \ldots, a'_n$. If we can find $x \in \{0,1\}^m$ satisfying $\sum_{i=1}^{m} x_i a_i \equiv b \bmod N$, then $Mx \equiv b'$ (where the jth component of the product is reduced modulo q_j, $1 \leq j \leq n$).
The hardness of this problem follows from Ajtai's proof. The key modification is as follows. Recall that $W = \mathcal{P}(f_1, \ldots, f_n)$. Rather than cutting each vector f_i, $1 \leq i \leq n$, into q equal pieces (for a fixed q), instead for each $1 \leq i \leq n$, cut f_i into q_i pieces. Thus, instead of having q^n little parallelepipeds we will have $N = q_1 \ldots q_n$ of them. Any solution x plays the role of the solution $h = \langle h_1, \ldots, h_m \rangle$ in the original proof. See [2] for more details and extensions of these results.
Impagliazzo and Naor proved that if the subset sum function for length $(1 - c)m$, $c > 0$, is one-way in the sense that no polynomial time algorithm can invert the function on a random input, then it is also

a family of universal one-way hash functions [21]. Since this class of subset sum problem is hard on average (assuming the worst-case lattice problems are difficult for dimension n), the Impagliazzo and Naor construction yields a family of universal one-way hash functions.

In a related note, Goldreich, Goldwasser, and Halevi [13] observed that these hash functions are actually *collision-intractable*. Specifically, they show that if M is a random matrix in $Z_q^{n\times m}$, then finding collisions of the function $h(x) = Mx \bmod q$ is hard provided a slight modification of Ajtai's random lattice problem is hard. The modification is to only require that the vector x have coefficients in $\{-1, 0, 1\}$ (rather than to require $x \in \mathbb{Z}_q^m$ and $||x|| < n$), and the proof of collision-intractability relies on the fact that Ajtai's results hold even if the random lattice problem is relaxed so that $||x||$ is bounded by a polynomial in n. (The more relaxed version incurs a cost in the quality of the approximation obtained in Ajtai's reduction.) Collision-intractability follows from the fact that if it were easy to find $x, y \in \{0, 1\}^m$ such that $Mx \equiv My \bmod q$ then $M(x - y) \equiv 0 \bmod q$. Since $x - y \in \{-1, 0, 1\}^m$, finding such a pair x, y is difficult.

5 Public Key Cryptography

Ajtai and Dwork constructed a public key cryptosystem generator with the property that if a random instance of the cryptosystem can be broken, that is, if for a random instance the probability that an encryption of a zero can be distinguished from an encryption of a one (without the private key) in polynomial time is at least $\frac{1}{2} + n^{-c_1}$ for some absoloute constant $c_1 > 0$, then the worst-case unique shortest vector problem has a probabilistic polynomial time solution. Intuitively, this worst-case/average-case equivalence means that there are essentially no "bad" instances of the cryptosystem.

In this discussion we will work with real numbers, ignoring issues of finite precision. The private key is a vector $u \in \mathbb{R}^n$ chosen uniformly at random from the n-dimensional unit ball. u induces a collection of $(n - 1)$-dimensional hyperplanes, where for $i \in \mathbb{Z}$ the ith hyperplane is the set of vectors v whose inner product satisfy $u \cdot v = i$. Very roughly speaking, the public key is a method of generating a point guaranteed to be near one of the hyperplanes in the collection. The public key is chosen so as not to reveal the collection of hyperplanes – indeed, Ajtai and Dwork prove that any ability, given only the public key, to discover the collection implies the ability to solve the worst-case unique shortest vector problem. Encryption is bit-by-bit: zero is encrypted by using the public key to find a random vector $v \in \mathbb{R}^n$ near one of the hyperplanes – the ciphertext is v; one is encrypted by choosing a random vector u uniformly from $\mathbb{R}^n$ – the ciphertext is simply u. Decryption of a ciphertext x is simple using the private key u: if $u \cdot x$ is close to an integer then x is by definition near one of the hidden hyperplanes, and so x is interpreted as zero; otherwise x is interpreted as one.

If a lattice Λ has an n^c-unique shortest vector v, then $L = \Lambda^*$ is a $(||v||^{-1}, n^{-c'}||v||^{-1})$ lattice, where c' is roughly $c - 2$ (a proof appears in [2]). Moverover, v is orthogonal to the $(n - 1)$-dimensional space containing $L' = L^{(||v||^{-1}, n^{-c'}||v||^{-1})}$, and if H is the $(n - 1)$-dimensional subspace of $\mathbb{R}^n$ containing L', then the hyperplanes induced by v are the cosets of H intersecting L (recall the discussion of the dual in Section 2).

Define pert(R) to be a random variable that, roughly speaking, is normally distributed about the origin in a ball of radius R. Let $\mathcal{K}$ be a very large cube, and let $R = n^c$. It is first shown that if the n^{c_1}-unique shortest vector problem is hard, for c_1 sufficiently larger than c, then the distribution obtained by choosing a random lattice point in $\mathcal{K}$ and perturbing it by adding a value of pert(R) (for sufficiently large R) is polynomially indistinguishable from the distribution obtained by choosing a vector uniformly at random from $\mathcal{K}$.

To see this, suppose we are given a *random* lattice Λ with an n^{c_1}-unique shortest vector v, and let $L = \Lambda^*$. Let $d = ||v||^{-1}$ and $M = n^{-c_1'}||v||^{-1}$, where c_1' is roughly $c_1 - 2$. Then L is a (d, M) lattice. Let $L' = L^{(d,M)}$ have basis $b_1, \ldots, b_{n-1}$. Let $H = H_0$ be the $(n-1)$-dimensional hyperplane containing L'. If R is sufficiently large with respect to $b_1, \ldots, b_{n-1}$, then the random variable obtained by sampling pert(R), projecting the result onto the $(n - 1)$-dimensional hyperplane containing L', and taking the projection modulo $\mathcal{P}^-(b_1, \ldots, b_{n-1})$ is extremely close to the value obtained by choosing a point uniformly in $\mathcal{P}^-(b_1, \ldots, b_{n-1})$.

Intuitively, this means that any algorithm distinguishing between "lattice point + pert(R)" and the uniform distribution is really distinguishing between points close to the cosets of H intersecting L and random points. ¿From this it is possible (with some effort – see [4]) to find H. Finally, given H we can recover v, the unique shortest vector in $\Lambda = L^*$ as follows. As noted above, v is perpendicular to H. By definition $\|v\| = d^{-1}$; given a basis for L (computable from the given basis for Λ), we can sample points from L and compute for each its distance from H. By taking the gcd of many random such distances we can find d.

The next step is to dispense with the lattice L. Let u be chosen uniformly at random from the n-dimensional unit ball and let $\mathcal{H}_u$ be the collection of hyperplanes induced by u. The distribution obtained by choosing a random point in $\mathcal{H}_u \cap \mathcal{K}$ and then sufficiently perturbing the chosen point, is indistinguishable from the uniform distribution in $\mathcal{K}$ – otherwise there would be a way of distinguishing points close to the hyperplanes from random points. The scheme is therefore as follows.

Private Key: vector u chosen at random from the n-dimensional unit ball

Public Key: $v_1, \ldots, v_m$: a collection of perturbations of points chosen uniformly from $\mathcal{H}_u \cap \mathcal{K}$, and a parallelepiped $\mathcal{P}$

Encryption: To encrypt zero, choose $\delta_1, \ldots, \delta_m$, each $\delta_i \in_R \{0, 1\}$. The ciphertext is $\sum_{i=1}^{m} \delta_i \bmod \mathcal{P}$. To encrypt one, choose a random point in $\mathcal{P}^-$.

Decryption: given ciphertext x, compute $x \cdot u$. If the result is sufficiently close (as a function of R) to an integer, then decrypt x as zero; else decrypt x as one.

There is some chance of a decryption error. This can be avoided by including in the public key a point B obtained by averaging two encryptions of zero lying on hyperplanes of different parity. (A related solution appears in [15].) The procedure for encrypting one becomes: follow the procedure for encrypting zero but add B before modding out by $\mathcal{P}$.

Very roughly, worst-case/average-case equivalence is shown as follows. Suppose we have an algorithm $\mathcal{A}$ that can break random instances of the cryptosystem with non-negligible probability over the choice of u. Given any instance L of the unique shortest vector problem, we convert it to an instance of the cryptosystem by choosing a number of random linear transformations $U = \theta\nu$ where $\theta \in \mathbb{R}$ and ν is an orthogonal linear transformation. Intuitively, ν rotates the lattice L leaving the lengths of the basis vectors unchanged, while θ scales the rotated basis. If v is the unique shortest vector and we choose enough transformations, then for one of them $\|Uv\| < 1$ and $\mathcal{A}$ can crack the instance of the cryptosystem defined by u. Note that v is the n^c-unique shortest vector of L if and only if Uv is the n^c-unique shortest vector of UL. It follows that J, the dual lattice of UL, is a $(1, n^{-c'})$ lattice, where $c' \sim c - 2$. Moreover, the distribution obtained by perturbing points of J is exponentially close to the distribution obtained by perturbing points in the hyperplanes induced by Uv. But Uv describes (the private key of) a *random* instance of the Ajtai-Dwork cryptosystem: it is random because U is random. Moreover, the ability to distinguish zeros – points close to the hyperplanes induced by Uv – from ones – random points– would imply the ability to distinguish perturbations of lattice points in J from random points. As argued above, this ability would yield Uv, the unique shortest vector in J^*, and hence, by the invertibility of U, v.

6 Pseudorandom Bit Generators

The Ajtai-Dwork construction suggests a pseudorandom bit generator with a very natural geometrical interpretation. Note that, given the secret information u, it requires fewer bits to describe a point that is close to one of the hyperplanes induced by u than to describe a point chosen at random from $\mathbb{R}^n$. To see this, consider a basis $b_1, \ldots, b_n$ for $\mathbb{R}^n$ in which the first $n-1$ vectors lie in H_0, the $(n-1)$-dimensional space orthogonal to u, and b_n is parallel to u. Using this basis it is easy to see that to describe a random point requires more bits than to describe a point close to one of the hyperplanes because, intuitively, there are more choices for the random point (the distance of a random point to the nearest hyperplane can be any value in $[0, \|u\|/2]$, while the distance of a point close to the hyperplane is in $[0, n^{-c}]$ for a fixed constant $c > 0$).

7 Digital Signatures

Goldreich, Goldwasser, and Halevi have suggested a digital signature scheme based on a trapdoor function related to the problem of finding the lattice vector closest to a given vector v [14]. Their approach, which also yields a public-key cryptosystem, depends on the hardness of random instances of the underlying problem (rather than worst-case instances). Naor and Yung have shown how to obtain a digital signature scheme from any one-way function [24]. Other than schemes obtained by applying this general construction to the one-way functions of [2, 4], we know of no proposed digital signature scheme with worst-case/average-case equivalence.

The trapdoor function proposed by Goldreich, Goldwasser, and Halevi relies on the difficulty, given a basis B for a lattice L, of finding a basis for L with small dual orthogonality defect. Call such a basis *reduced.*

The trapdoor information is a reduced basis R for an n-dimensional lattice (defined implicitly by R). Given R, it is possible to generate a second basis B for $L = L(R)$ so that B has high dual orthogonality defect. The trapdoor function is specified by B and a real parameter $\sigma \in \mathbb{R}$. Given vectors $v, e \in \mathbb{R}^n$, the function $f_{(B,\sigma)}(v, e) = Bv + e$. Note that the value σ does not appear in the definition of the function. Rather, σ governs the selection of e: each entry in e is chosen at random according to a distribution with zero mean and variance σ^2. For example, each entry in e can be chosen uniformly from $\{\sigma, -\sigma\}$.

Assume e is chosen as described and each component of v is chosen uniformly from, say, $\{-n^2, -n^2 + 1, \ldots, n^2 - 1, n^2\}$. Let $c = f_{(B,\sigma)}(v, e) = Bv + e$. If σ is chosen carefully, the function can be inverted using R by applying Babai's rounding technique [5]: represent c as a linear combination of the columns of R and then round the coefficients in the linear combination to the nearest integers to obtain a lattice point (integer linear combination of the columns of R). Once v is recovered we find $e = c - Bv$.

In the Goldreich, Goldwasser, and Halevi digital signature scheme, the private key is a reduced basis R and the public key is a non-reduced basis B. To sign a message m encoded as a vector $v \in \mathbb{R}^n$, the signer computes, using the reduced basis, a lattice vector w close to v. The public verification key is a threshold τ and the non-reduced basis B; the signature is verified by checking that $\|v - w\| \leq \tau$. As the authors point out, if $u, u' \in \mathbb{R}^n$ are sufficiently close, then a signature on u is likely also to be a signature on u'; it is therefore important to use a "good hash function" to hash a message before interpreting it as a vector in $\mathbb{R}^n$ [14].

References

1. L. Adleman, On Breaking Generalized Knapsack Public Key Cryptosystems, Proceedings 15th Annual ACM Symposium on Theory of Computing, 1983, pp. 402–412
2. M. Ajtai, Generating Hard Instances of Lattice Problems, Proceedings 28th Annual ACM Symposium on Theory of Computing, 1996, pp. 99–108 *Electronic Colloquium on Computational Complexity TR96-007*, http://www.eccc.uni-trier.de/eccc-local/Lists/TR-1996.html
3. M. Ajtai, *discussion with the author*, 1996
4. M. Ajtai, C. Dwork, A Public-Key Cryptosystem with Average-Case/Worst-Case Equivalence, Proceedings 29th Annual ACM Symposium on Theory of Computing, 1997; see also *Electronic Colloquium on Computational Complexity TR96-065*, http://www.eccc.uni-trier.de/eccc-local/Lists/TR-1996.html
5. L. Babai, On Lovász' Lattice Reduction and the Nearest Lattice Point Problem, *Combinatorica 6*(1), 1986, pp. 1–13
6. M. Blum and S. Micali, How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits, *SIAM J. Computing 13*, 1984, pp. 850–864
7. J.-Y. Cai and A. P. Nerurkar, An Improved Worst-Case to Average-Case Connection for Lattice Problems, *private communication*, 1997
8. J.W.S. Cassels, *An Introduction to the Geometry of Numbers*, Springer, 1959
9. D. Coppersmith, Finding a Small Root of a Univariate Modular Equation, *Proc. EUROCRYPT'96*
10. D. Coppersmith, M. Franklin, J. Patarin, and M. Reiter, Low Exponent RSA with Related Messages, *Proc. EUROCRYPT'96*

11. D. Dolev, C. Dwork, and M. Naor, Non-Malleable Cryptography, Proceedings 23th Annual ACM Symposium on Theory of Computing, 1991, pp. 542–550
12. O. Goldreich, *Foundations of Cryptography (Fragments of a Book)*, http://www.wisdom.weizmann.ac.il/people/homepages/oded/frag.html
13. O. Goldreich, S. Goldwasser, and S. Halevi, Collision-Free Hashing from Lattice Problems, *Electronic Colloquium on Computational Complexity TR96-042*, http://www.eccc.uni-trier.de/eccc-local/Lists/TR-1996.html
14. O. Goldreich, S. Goldwasser, and S. Halevi, Public-Key Cryptosystems from Lattice Reduction Problems, *Electronic Colloquium on Computational Complexity TR96-056*, http://www.eccc.uni-trier.de/eccc-local/Lists/TR-1996.html
15. O. Goldreich, S. Goldwasser, and S. Halevi, Eliminating the Decryption Error in the Ajtai-Dwork Cryptosystem, *to appear, Proc. CRYPTO'97*
16. S. Goldwasser and S. Micali, Probabilistic Encryption, *J. Comput. System Sci. 28*, 1984, pp. 270–299
17. S. Goldwasser, S. Micali, and R. Rivest, A "Paradoxical" Solution to the Signature Problem, *SIAM J. Computing 17*, 1988, pp. 281–308
18. M. Grötschel, Lovász, A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, Springer, Algorithms and Combinatorics 2, 1988
19. P.M. Gruber, C.G. Lekkerkerker, *Geometry of Numbers*, North-Holland, 1987
20. J. Hastad, Solving Simultaneous Modular Equations of Low Degree, *SIAM J. Computing 17*(2), pp.336–341, 1988
21. R. Impagliazzo and M. Naor, Efficient Cryptographic Schemes Provably as Secure as Subset Sum, *J. Cryptology 9*, pp. 199–216, 1996
22. J.C. Lagarias, A.M. Odlyzko, Solving low-density subset sum problems, *Journal of the Association for Computing Machinery 32* pp. 229-246, 1985. An earlier version appeared in *Proc. 24th Annual Symposium on Foundations of Computer Science*, 1983
23. M. Luby, **Pseudo-randomness and applications**, Princeton University Press, 1996.
24. M. Naor and M. Yung, Universal One-Way Hash Functions and Their Cryptographic Applications, Proceedings 21th Annual ACM Symposium on Theory of Computing, 1989, pp. 33–43
25. A. Shamir, A Polynomial-Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem, *Proc. 23rd Annual Symposium on Foundations of Computer Science*, 1982, pp. 145–152
26. A. C. Yao, Theory and Applications of Trapdoor Functions, *Proc. 23rd Annual Symposium on Foundations of Computer Science*, 1982, pp. 80–91

This article was processed using the LaTeX macro package with LLNCS style