Chapter 16

Lattices

The word "lattice" has two different meanings in mathematics. One meaning is related to the theory of partial orderings on sets (for example, the lattice of subsets of a set). The other meaning, which is the one relevant to us, is discrete subgroups of $\mathbb{R}^n$.

There are several reasons for presenting lattices in this book. First, there are hard computational problems on lattices that have been used as a building block for public key cryptosystems (e.g., the Goldreich-Goldwasser-Halevi (GGH) cryptosystem, the NTRU cryptosystem, the Ajtai-Dwork cryptosystem, and the LWE cryptosystem); however, we do not present these applications in this book. Second, lattices are used as a fundamental tool for cryptanalysis of public key cryptosystems (e.g., lattice attacks on knapsack cryptosystems, Coppersmith's method for finding small solutions to polynomial equations, attacks on signatures, and attacks on variants of RSA). Third, there are applications of lattices to efficient implementation of discrete logarithm systems (such as the GLV method; see Section 11.3.3). Finally, lattices are used as a theoretical tool for security analysis of cryptosystems, for example the bit security of Diffie-Hellman key exchange using the hidden number problem (see Section 21.7) and the security proofs for RSA-OAEP.

Some good references for lattices, applications of lattices and/or lattice reduction algorithms are: Cassels [122], Siegel [563], Cohen [136], von zur Gathen and Gerhard [238], Grötschel, Lovász and Schrijver [269], Nguyen and Stern [462, 463], Micciancio and Goldwasser [422], Hoffstein, Pipher and Silverman [289], Lenstra's chapter in [113], Micciancio and Regev's chapter in [50] and the proceedings of the conference LLL+25.

Notation used in this part

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$	Integers, rational, real numbers
$\underline{b}, \underline{v}, \underline{w}$	Row vectors (usually in $\mathbb{R}^m$)
$\underline{0}$	Zero vector in $\mathbb{R}^m$
$\underline{e}_i$	i-th unit vector in $\mathbb{R}^m$
I_n	$n \times n$ identity matrix
$\langle \underline{x}, \underline{x} \rangle$	Inner product
$\\|\underline{x}\\|$	Euclidean length (ℓ_2 norm)
$\\| \cdot \\|_a$	ℓ_a-norm for $a \in \mathbb{N}$
$\mathrm{span}\{\underline{v}_1, \dots, \underline{v}_n\}$	Span of a set of vectors over $\mathbb{R}$
$\mathrm{rank}(A)$	Rank of a matrix A
$\lfloor x \rceil$	Closest integer to x, $\lfloor 1/2 \rceil = 1$
B	Basis matrix for a lattice
L	Lattice
$\underline{b}_i^*$	Gram-Schmidt vector arising from ordered basis $\{\underline{b}_1, \dots, \underline{b}_n\}$
$\mu_{i,j}$	Gram-Schmidt coefficient $\langle \underline{b}_i, \underline{b}_j^* \rangle / \langle \underline{b}_j^*, \underline{b}_j^* \rangle$
B_i	$\\|\underline{b}_i^*\\|^2$
λ_i	Successive minima of a lattice
$\det(L)$	Determinant of a lattice
γ_n	Hermite's constant
X	Bound on the size of the entries in the basis matrix L
$B_{(i)}$	$i \times m$ matrix formed by the first i rows of B
d_i	Determinant of matrix of $\langle \underline{b}_j, \underline{b}_k \rangle$ for $1 \leq j, k \leq i$
D	Product of d_i
$\mathcal{P}_{1/2}(B)$	Fundamental domain (parallelepiped) for lattice basis B
$F(x)$, $F(x,y)$	Polynomial with “small” root
$G(x), G(x,y)$	Polynomial with “small” root in common with $F(x)$ (resp., $F(x,y)$)
X, Y	Bounds on size of root in Coppersmith's method
b_F	Coefficient vector of polynomial F
$R(F,G), R_x(F(x), G(x))$	Resultant of polynomials
W	Bound in Coppersmith's method
P, R	Constants in noisy Chinese remaindering
$\mathrm{amp}(x)$	The amplitude $\gcd(P, x - R)$ in noisy Chinese remaindering
B, B'	Basis matrices for GGH encryption
I_n	$n \times n$ identity matrix
U	Invertible matrix disguising the private key in GGH
$\underline{m}$	Message in McEliece or GGH
$\underline{e}$	Error vector in McEliece or GGH
$\underline{c}$	Ciphertext in McEliece or GGH
σ	Entry in error vector in GGH
M	Size of coefficients in message in GGH
$\underline{s}$	GGH signature
$a_1, \dots, a_n$	Subset sum weights
$b_1, \dots, b_n$	Superincreasing sequence
$s = \sum_{i=1}^{n} x_i a_i$	The sum in a subset sum instance, with $x_i \in \{0, 1\}$
d	Density of a subset sum instance
π	Permutation of $\{1, \dots, n\}$ used in the Merkle-Hellman cryptosystem
$\underline{\sigma}$	Vector in Nguyen attack
M	Modulus in Merkle-Hellman knapsack
W	Multiplier in Merkle-Hellman knapsack
U	$W^{-1} \pmod{M}$ in Merkle-Hellman
t	Number of iterations in iterated Merkle-Hellman knapsack

16.1 Basic Notions on Lattices

A lattice is a subset of the vector space $\mathbb{R}^m$. We write all vectors as **rows**; be warned that many books and papers write lattice vectors as columns. We denote by $\|\underline{v}\|$ the Euclidean norm of a vector $\underline{v} \in \mathbb{R}^m$; though some statements also hold for other norms.

Definition 16.1.1. Let $\{\underline{b}_1, \dots, \underline{b}_n\}$ be a linearly independent set of (row) vectors in $\mathbb{R}^m$ $(m \geq n)$. The **lattice** generated by $\{\underline{b}_1, \dots, \underline{b}_n\}$ is the set

$$L = \left\{ \sum_{i=1}^{n} l_i \underline{b}_i \ : \ l_i \in \mathbb{Z} \right\}$$

of **integer** linear combinations of the $\underline{b}_i$. The vectors $\underline{b}_1, \dots, \underline{b}_n$ are called a **lattice basis**. The **lattice rank** is n and the **lattice dimension** is m. If $n = m$ then L is said to be a **full rank lattice**.

Let $L \subset \mathbb{R}^m$ be a lattice. A **sublattice** is a subset $L' \subset L$ that is a lattice.

A **basis matrix** B of a lattice L is an $n \times m$ matrix formed by taking the rows to be basis vectors $\underline{b}_i$. Thus $B_{i,j}$ is the j-th entry of the row $\underline{b}_i$ and

$$L = \{\underline{x}B : \underline{x} \in \mathbb{Z}^n\}.$$

By assumption the rows of a basis matrix are always linearly independent.

Example 16.1.2. The lattice in $\mathbb{R}^2$ generated by $\{(1,0),(0,1)\}$ is $L = \mathbb{Z}^2$. The corresponding basis matrix is $B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Any 2×2 integer matrix B of determinant ± 1 is also a basis matrix for L.

We will mainly assume that the basis vectors $\underline{b}_i$ for a lattice have integer entries. In cryptographic applications this is usually the case. We interchangeably use the words **points** and **vectors** for elements of lattices. The vectors in a lattice form an Abelian group under addition. When $n \geq 2$ there are infinitely many choices for the basis of a lattice.

An alternative approach to lattices is to define $L = \mathbb{Z}^n$ and to have a general length function $q(\underline{v})$. One finds this approach in books on quadratic forms or optimisation problems, e.g., Cassels [121] and Schrijver [531]. In particular, Section 6.2 of [531] presents the LLL algorithm in the context of reducing the lattice $L = \mathbb{Z}^n$ with respect to a length function corresponding to a positive-definite rational matrix.

We now give an equivalent definition of lattice, which is suitable for some applications. A subset $L \subseteq \mathbb{R}^m$ is called **discrete** if, for any real number $r > 0$, the set $\{\underline{v} \in L : \|\underline{v}\| \leq r\}$ is finite. It is clear that a lattice is a subgroup of $\mathbb{R}^m$ that is discrete. The following result shows the converse.

Lemma 16.1.3. *Every discrete subgroup of* $\mathbb{R}^m$ *is a lattice.*

Proof: (Sketch) Let $\{\underline{v}_1, \dots, \underline{v}_n\}$ be a linearly independent subset of L of maximal size. The result is proved by induction. The case $n = 1$ is easy (since L is discrete there is an element of minimal non-zero length). When $n > 1$ consider $V = \operatorname{span}\{\underline{v}_1, \dots, \underline{v}_{n-1}\}$ and set $L' = L \cap V$. By induction, L' is a lattice and so has a basis $\underline{b}_1, \dots, \underline{b}_{n-1}$. The set $L \cap \{\sum_{i=1}^{n-1} x_i \underline{b}_i + x_n \underline{v}_n : 0 \leq x_i < 1 \text{ for } 1 \leq i \leq n-1 \text{ and } 0 < x_n \leq 1\}$ is finite and so has an element with smallest x_n, call it $\underline{b}_n$. It can be shown that $\{\underline{b}_1, \dots, \underline{b}_n\}$ is a basis for L. For full details see Theorem 6.1 of [586]. □

Exercise 16.1.4. Given an $m \times n$ integer matrix A show that $\ker(A) = \{\underline{x} \in \mathbb{Z}^m : \underline{x}A = \underline{0}\}$ is a lattice. Show that the rank of the lattice is $m - \operatorname{rank}(A)$. Given an $m \times n$ integer matrix A and an integer M show that $\{\underline{x} \in \mathbb{Z}^m : \underline{x}A \equiv \underline{0} \pmod{M}\}$ is a lattice of rank m.

In the case $m > n$ it is sometimes convenient to project the lattice L into $\mathbb{R}^n$ using the following construction. The motivation is that a linear map that preserves lengths preserves volumes. Note that if the initial basis for L consists of vectors in $\mathbb{Z}^n$ then the resulting basis does not necessarily have this property.

Lemma 16.1.5. *Let B be an $n \times m$ basis matrix for a lattice L where $m > n$. Then there is a linear map $P : \mathbb{R}^m \to \mathbb{R}^n$ such that $P(L)$ is a rank n lattice and $\|P(\underline{v})\| = \|\underline{v}\|$ for all $\underline{v} \in L$. Furthermore, $\langle \underline{b}_i, \underline{b}_j \rangle = \langle P(\underline{b}_i), P(\underline{b}_j) \rangle$ for all $1 \le i < j \le n$.*

If the linear map is represented by an $m \times n$ matrix P so that $P(\underline{v}) = \underline{v}P$ then a basis matrix for the image of L under the projection P is the $n \times n$ matrix BP, which is invertible.

Proof: Given the $n \times m$ basis matrix B with rows $\underline{b}_i$, define $V = \operatorname{span}\{\underline{b}_1, \dots, \underline{b}_n\} \subset \mathbb{R}^m$, which has dimension n by assumption. Choose (perhaps by running the Gram-Schmidt algorithm) a basis $\underline{v}_1, \dots, \underline{v}_n$ for V that is orthonormal with respect to the inner product in $\mathbb{R}^m$. Define the linear map $P : V \to \mathbb{R}^n$ by $P(\underline{v}_i) = \underline{e}_i$ and $P(V^\perp) = \{0\}$. For $\underline{v} = \sum_{i=1}^n x_i \underline{v}_i \in V$ we have $\|\underline{v}\| = \sqrt{\langle \underline{v}, \underline{v} \rangle} = \sqrt{\sum_{i=1}^n x_i^2} = \|\underline{v}P\|$. Since the vectors $\underline{b}_i$ form a basis for V, the vectors $P(\underline{b}_i) = \underline{b}_i P$ are linearly independent. Hence, BP is an invertible matrix and $P(L)$ is a lattice of rank n. □

We can now prove the following fundamental result.

Lemma 16.1.6. *Two $n \times m$ matrices B and B' generate the same lattice L if and only if B and B' are related by a* ***unimodular matrix****, i.e., $B' = UB$ where U is an $n \times n$ matrix with integer entries and determinant ± 1.*

Proof: ($\Rightarrow$) Every row of B' is an integer linear combination

$$\underline{b}'_i = \sum_{j=1}^n u_{i,j} \underline{b}_j$$

of the rows in B. This can be represented as $B' = UB$ for an $n \times n$ integer matrix U.

Similarly, $B = U'B' = U'UB$. Now applying the projection P of Lemma 16.1.5 we have $BP = U'UBP$ and, since BP is invertible, $U'U = I_n$ (the identity matrix). Since U and U' have integer entries it follows that $\det(U), \det(U') \in \mathbb{Z}$. From $\det(U)\det(U') = \det(I_n) = 1$ it follows that $\det(U) = \pm 1$.

($\Leftarrow$) Since U is a permutation of $\mathbb{Z}^n$ we have $\{\underline{x}B' : \underline{x} \in \mathbb{Z}^n\} = \{\underline{x}B : \underline{x} \in \mathbb{Z}^n\}$. □

The Hermite normal form is defined in Section A.11. The following result is a direct consequence of Lemma 16.1.6 and the remarks in Section A.11.

Lemma 16.1.7. *If B is the basis matrix of a lattice L then the Hermite normal form of B is also a basis matrix for L.*

The **determinant** of a lattice L is the volume of the fundamental parallelepiped of any basis B for L. When the lattice has full rank then using Definition A.10.7 and Lemma A.10.8 we have $\det(L) = |\det(B)|$. For the case $n < m$ our definition uses Lemma 16.1.5.

Definition 16.1.8. Let the notation be as above. The **determinant** (or **volume**) of a lattice L with basis matrix B is $|\det(BP)|$, where P is a matrix representing the projection of Lemma 16.1.5.

Lemma 16.1.9. *The determinant of a lattice is independent of the choice of basis matrix B and the choice of projection P.*

Proof: Let P and P' be two projection matrices corresponding to orthogonal bases $\{\underline{v}_1, \dots, \underline{v}_n\}$ and $\{\underline{v}'_1, \dots, \underline{v}'_n\}$ for $V = \operatorname{span}\{\underline{b}_1, \dots, \underline{b}_n\}$. Then, by Lemma A.10.3, $P' = PW$ for some orthogonal matrix W (hence $\det(W) = \pm 1$). It follows that $|\det(BP)|$ does not depend on the choice of P.

Let B and B' be two basis matrices for a lattice L. Then $B' = UB$ where U is an $n \times n$ matrix such that $\det(U) = \pm 1$. Then $\det(L) = |\det(BP)| = |\det(UBP)| = |\det(B'P)|$. □

We have seen that there are many different choices of basis for a given lattice L. A fundamental problem is to compute a "nice" lattice basis for L; specifically one where the vectors are relatively short and close to orthogonal. The following exercise shows that these properties are intertwined.

Exercise 16.1.10. Let L be a rank 2 lattice in $\mathbb{R}^2$ and let $\{\underline{b}_1, \underline{b}_2\}$ be a basis for L.

1. Show that
$$\det(L) = \|\underline{b}_1\| \|\underline{b}_2\| |\sin(\theta)| \tag{16.1}$$
where θ is the angle between $\underline{b}_1$ and $\underline{b}_2$.

2. Hence deduce that the product $\|\underline{b}_1\|\|\underline{b}_2\|$ is minimised over all choices $\{\underline{b}_1, \underline{b}_2\}$ of basis for L when the angle θ is closest to $\pm\pi/2$.

Definition 16.1.11. Let L be a lattice in $\mathbb{R}^m$ of rank n with basis matrix B. The **Gram matrix** of B is BB^T. This is an $n \times n$ matrix whose (i, j)th entry is $\langle \underline{b}_i, \underline{b}_j \rangle$.

Lemma 16.1.12. *Let L be a lattice in $\mathbb{R}^m$ of rank n with basis matrix B. Then $\det(L) = \sqrt{\det(BB^T)}$.*

Proof: Consider first the case where $m = n$. Then $\det(L)^2 = \det(B)\det(B^T) = \det(BB^T) = \det((\langle \underline{b}_i, \underline{b}_j \rangle)_{i,j})$. Hence, when $m > n$ and $B' = BP$, $\det(L) = |\det(B')| = \sqrt{\det(B'(B')^T)}$. Now, the (i, j)th entry of $B'(B')^T = (BP)(BP)^T$ is $\langle \underline{b}_i P, \underline{b}_j P \rangle$, which is equal to the (i, j)th entry of BB^T by Lemma 16.1.5. The result follows. □

Note that an integer lattice of non-full rank may not have integer determinant.

Exercise 16.1.13. Find an example of a lattice of rank 1 in $\mathbb{Z}^2$ whose determinant is not an integer.

Lemma 16.1.14. *Let $\underline{b}_1, \dots, \underline{b}_n$ be an ordered basis for a lattice L in $\mathbb{R}^m$ and let $\underline{b}^*_1, \dots, \underline{b}^*_n$ be the Gram-Schmidt orthogonalisation. Then $\det(L) = \prod_{i=1}^n \|\underline{b}^*_i\|$.*

Proof: The case $m = n$ is already proved in Lemma A.10.8. For the general case let $\underline{v}_i = \underline{b}^*_i / \|\underline{b}^*_i\|$ be the orthonormal basis required for the construction of the projection P. Then $P(\underline{b}^*_i) = \|\underline{b}^*_i\| \underline{e}_i$. Write B and B^* for the $n \times m$ matrices formed by the rows $\underline{b}_i$ and $\underline{b}^*_i$ respectively. It follows that B^*P is an $n \times n$ diagonal matrix with diagonal entries $\|\underline{b}^*_i\|$. Finally, by the Gram-Schmidt construction, $B^* = UB$ for some $n \times n$ matrix U such that $\det(U) = 1$. Combining these facts gives[1]

$$\det(L) = |\det(BP)| = |\det(UBP)| = |\det(B^*P)| = \prod_{i=1}^{n} \|\underline{b}^*_i\|.$$

□

[1] The formula $BP = U^{-1}(B^*P)$ is the QR decomposition of BP.

Exercise 16.1.15. Let $\{\underline{b}_1, \dots, \underline{b}_n\}$ be an ordered lattice basis in $\mathbb{R}^m$ and let $\{\underline{b}_1^*, \dots, \underline{b}_n^*\}$ be the Gram-Schmidt orthogonalisation. Show that $\|\underline{b}_i\| \geq \|\underline{b}_i^*\|$ and hence $\det(L) \leq \prod_{i=1}^n \|\underline{b}_i\|$.

Definition 16.1.16. Let $\{\underline{b}_1, \dots, \underline{b}_n\}$ be a basis for a lattice L in $\mathbb{R}^m$. The **orthogonality defect** of the basis is

$$\left(\prod_{i=1}^n \|\underline{b}_i\| \right) / \det(L).$$

Exercise 16.1.17. Show that the orthogonality defect of $\{\underline{b}_1, \dots, \underline{b}_n\}$ is 1 if and only if the basis is orthogonal.

Definition 16.1.18. Let $L \subset \mathbb{R}^m$ be a lattice of rank n. The **successive minima** of L are $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ such that, for $1 \leq i \leq n$, λ_i is minimal such that there exist i linearly independent vectors $\underline{v}_1, \dots, \underline{v}_i \in L$ with $\|\underline{v}_j\| \leq \lambda_i$ for $1 \leq j \leq i$.

It follows that $0 < \lambda_1 \leq \lambda_2 \cdots \leq \lambda_n$. In general there is not a basis consisting of vectors whose lengths are equal to the successive minima, as the following example shows.

Example 16.1.19. Let $L \subset \mathbb{Z}^n$ be the set

$$L = \{(x_1, \dots, x_n) : x_1 \equiv x_2 \equiv \cdots \equiv x_n \pmod{2}\}.$$

It is easy to check that this is a lattice. The vectors $2\underline{e}_i \in L$ for $1 \leq i \leq n$ are linearly independent and have length 2. Every other vector $\underline{x} \in L$ with even entries has length ≥ 2. Every vector $\underline{x} \in L$ with odd entries has all $x_i \neq 0$ and so $\|\underline{x}\| \geq \sqrt{n}$.

If $n = 2$ the successive minima are $\lambda_1 = \lambda_2 = \sqrt{2}$ and if $n = 3$ the successive minima are $\lambda_1 = \lambda_2 = \lambda_3 = \sqrt{3}$. When $n \geq 4$ then $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 2$. For $n \leq 4$ one can construct a basis for the lattice with vectors of lengths equal to the successive minima. When $n > 4$ there is no basis for L consisting of vectors of length 2, since a basis must contain at least one vector having odd entries.

Exercise 16.1.20. For $n = 2, 3, 4$ in Example 16.1.19 write down a basis for the lattice consisting of vectors of lengths equal to the successive minima.

Exercise 16.1.21. For $n > 4$ in Example 16.1.19 show there is a basis for the lattice such that $\|\underline{b}_i\| = \lambda_i$ for $1 \leq i < n$ and $\|\underline{b}_n\| = \sqrt{n}$.

Definition 16.1.22. Let $L \subseteq \mathbb{R}^m$ be a lattice and write $V \subseteq \mathbb{R}^m$ for the $\mathbb{R}$-vector space spanned by the vectors in L. The **dual lattice** of L is $L^* = \{\underline{y} \in V : \langle \underline{x}, \underline{y} \rangle \in \mathbb{Z} \text{ for all } \underline{x} \in L\}$.

Exercise 16.1.23. Show that the dual lattice is a lattice. Let B be a basis matrix of a full rank lattice L. Show that $(B^T)^{-1}$ is a basis matrix for the dual lattice. Hence, show that the determinant of the dual lattice is $\det(L)^{-1}$.

16.2 The Hermite and Minkowski Bounds

We state the following results without rigorously defining the term “volume” and without giving proofs (see Section 1.3 of Micciancio and Goldwasser [422], Chapter 1 of Siegel [563], Chapter 6 of Hoffstein, Pipher and Silverman [289] or Chapter 12 of Cassels [121] for details).

Theorem 16.2.1. *(Blichfeldt) Let L be a lattice in $\mathbb{R}^m$ with basis $\{\underline{b}_1, \ldots, \underline{b}_n\}$ and S any measurable set such that $S \subset \operatorname{span}\{\underline{b}_i : 1 \le i \le n\}$. If the volume of S exceeds $\det(L)$ then there exist two distinct points $\underline{v}_1, \underline{v}_2 \in S$ such that $(\underline{v}_1 - \underline{v}_2) \in L$.*

Proof: See Theorem 1.3 of [422] or Section III.2.1 of [121]. □

Theorem 16.2.2. *(Minkowski convex body theorem) Let L be a lattice in $\mathbb{R}^m$ with basis $\{\underline{b}_1, \ldots, \underline{b}_n\}$ and let S be any convex set such that $S \subset \operatorname{span}\{\underline{b}_i : 1 \le i \le n\}$, $\underline{0} \in S$ and if $\underline{v} \in S$ then $-\underline{v} \in S$. If the volume of S is $> 2^n \det(L)$ then there exists a non-zero lattice point $\underline{v} \in S \cap L$.*

Proof: See Section III.2.2 of Cassels [121], Theorem 6.28 of Hoffstein, Pipher and Silverman [289], Theorem 1.4 of Micciancio and Goldwasser [422], or Theorem 6.1 of Stewart and Tall [586]. □

The convex body theorem is used to prove Theorem 16.2.3. The intuition behind this result is that if the shortest non-zero vector in a lattice is large then the volume of the lattice cannot be small.

Theorem 16.2.3. *Let $n \in \mathbb{N}$. There is a constant $0 < \gamma_n \le n$ such that, for any lattice L of rank n in $\mathbb{R}^n$ having first minimum λ_1 (for the Euclidean norm),*

$$\lambda_1^2 < \gamma_n \det(L)^{2/n}.$$

Proof: See Theorem 1.5 of [422], Theorem 6.25 of [289], or Theorem 12.2.1 of [121]. □

Exercise 16.2.4. Show that the convex body theorem is tight. In other words find a lattice L in $\mathbb{R}^n$ for some n and a symmetric convex subset $S \subseteq \mathbb{R}^n$ such that the volume of S is $2^n \det(L)$ and yet $S \cap L = \{0\}$.

Exercise 16.2.5. Show that, with respect to the ℓ_∞ norm, $\lambda_1 \le \det(L)^{1/n}$. Show that, with respect to the ℓ_1 norm, $\lambda_1 \le (n! \det(L))^{1/n} \approx n \det(L)^{1/n}/e$.

Exercise 16.2.6.★ Let $a, b \in \mathbb{N}$. Show that there is a solution $r, s, t \in \mathbb{Z}$ to $r = as + bt$ such that $s^2 + r^2 \le \sqrt{2}b$.

Definition 16.2.7. Let $n \in \mathbb{N}$. The smallest real number γ_n such that

$$\lambda_1^2 \le \gamma_n \det(L)^{2/n}$$

for all lattices L of rank n is called the **Hermite constant**.

Exercise 16.2.8. This exercise is to show that $\gamma_2 = 2/\sqrt{3}$.

1. Let $\{\underline{b}_1, \underline{b}_2\}$ be a Lagrange-Gauss reduced basis (see Definition 17.1.1 of the next Section) for a dimension 2 lattice in $\mathbb{R}^2$. Define the quadratic form $N(x, y) = \|x\underline{b}_1 + y\underline{b}_2\|^2$. Show that, without loss of generality, $N(x, y) = ax^2 + 2bxy + cy^2$ with $a, b, c \ge 0$ and $a \le c$.

2. Using $N(1, -1) \ge N(0, 1)$ (which follows from the property of being Lagrange-Gauss reduced), show that $2b \le a$. Hence show that $3ac \le 4(ac - b^2)$

3. Show that $\det(L)^2 = |b^2 - ac|$. Hence deduce that Hermite's constant satisfies $\gamma_2 \le 2/\sqrt{3}$.

4. Show that the lattice $L \subset \mathbb{R}^2$ with basis $\{(1,0),(-1/2,\sqrt{3}/2)\}$ satisfies $\lambda_1^2 = (2/\sqrt{3})\det(L)$.

   (Optional) Show that L is equal to the ring of algebraic integers of $\mathbb{Q}(\sqrt{-3})$. Show that centering balls of radius $1/2$ at each point of L gives the most dense lattice packing of balls in $\mathbb{R}^2$.

Section 6.5.2 of Nguyen [456] lists the first 8 values of γ_n, gives the bound $\frac{n}{2\pi e} + o(1) \le \gamma_n \le \frac{n}{\pi e}(1 + o(1))$ and gives further references.

Theorem 16.2.9. *(Minkowski) Let L be a lattice of rank n in $\mathbb{R}^n$ with successive minima $\lambda_1, \dots, \lambda_n$ for the Euclidean norm. Then*

$$\left(\prod_{i=1}^{n} \lambda_i \right)^{1/n} < \sqrt{n} \det(L)^{1/n}.$$

Proof: See Theorem 12.2.2 of [121]. (The term $\sqrt{n}$ can be replaced by $\sqrt{\gamma_n}$.) □

The **Gaussian heuristic** states that the shortest non-zero vector in a "random" lattice L of dimension n in $\mathbb{R}^n$ is expected to have length approximately

$$\sqrt{\frac{n}{2\pi e}} \det(L)^{1/n}.$$

We refer to Section 6.5.3 of [456] and Section 6.5.3 of [289] for discussion and references.

16.3 Computational Problems in Lattices

There are several natural computational problems relating to lattices. We start by listing some problems that can be efficiently solved using linear algebra (in particular, the Hermite normal form).

1. **lattice membership**: Given an $n \times m$ basis matrix B for a lattice $L \subseteq \mathbb{Z}^m$ and a vector $\underline{v} \in \mathbb{Z}^m$ determine whether $\underline{v} \in L$.

2. **lattice basis**: Given a set of vectors $\underline{b}_1, \dots, \underline{b}_n$ in $\mathbb{Z}^m$ (possibly linearly dependent) find a basis for the lattice generated by them.

3. **kernel lattice**: Given an $m \times n$ integer matrix A compute a basis for the lattice $\ker(A) = \{\underline{x} \in \mathbb{Z}^m : \underline{x}A = \underline{0}\}$.

4. **kernel lattice modulo** M: Given an $m \times n$ integer matrix A and an integer M compute a basis for the lattice $\{\underline{x} \in \mathbb{Z}^m : \underline{x}A \equiv \underline{0} \pmod{M}\}$.

Exercise 16.3.1.★ Describe explicit algorithms for the above problems and determine their complexity.

Now we list some computational problems that seem to be hard in general.

Definition 16.3.2. Let L be a lattice in $\mathbb{Z}^m$.

1. The **shortest vector problem (SVP)** is the computational problem: given a basis matrix B for L, compute a non-zero vector $\underline{v} \in L$ such that $\|\underline{v}\|$ is minimal (i.e., $\|\underline{v}\| = \lambda_1$).

2. The **closest vector problem (CVP)** is the computational problem: given a basis matrix B for L and a vector $\underline{w} \in \mathbb{Q}^m$ (one can work with high-precision approximations in $\mathbb{R}^m$, but this is essentially still working in $\mathbb{Q}^m$), compute $v \in L$ such that $\|\underline{w} - \underline{v}\|$ is minimal.
3. The **decision closest vector problem (DCVP)** is: given a basis matrix B for a lattice L, a vector $\underline{w} \in \mathbb{Q}^m$ and a real number $r > 0$, decide whether or not there is a vector $\underline{v} \in L$ such that $\|\underline{w} - \underline{v}\| \le r$.
4. The **decision shortest vector problem** is: given a basis matrix B for a lattice L and a real number $r > 0$ to decide whether or not there is a non-zero $\underline{v} \in L$ such that $\|\underline{v}\| \le r$.
5. Fix $\gamma > 1$. The **approximate SVP problem** is: given a basis matrix B for L, compute a non-zero vector $\underline{v} \in L$ such that $\|\underline{v}\| \le \gamma\lambda_1$.
6. Fix $\gamma > 1$. The **approximate CVP problem** is: given a basis matrix B for L and a vector $\underline{w} \in \mathbb{Q}^m$, compute $\underline{v} \in L$ such that $\|\underline{w} - \underline{v}\| \le \gamma\|\underline{w} - \underline{x}B\|$ for all $\underline{x} \in \mathbb{Z}^n$.
7. Fix $0 < \alpha < 1/\sqrt{2}$. The **bounded distance decoding problem (BDD)** is: given a basis matrix B for a lattice L and a vector $\underline{w} \in \mathbb{Q}^m$ such that there is a lattice point $\underline{v} \in L$ with $\|\underline{w} - \underline{v}\| \le \alpha\lambda_1(L)$, to compute $\underline{v}$. In other words, this is a CVP instance that is especially close to a lattice point.

In general, these computational problems are known to be hard[2] when the rank is sufficiently large. It is known that CVP is NP-hard (this is shown by relating CVP with subset-sum; for details see Chapter 3 of [422]). Also, SVP is NP-hard under randomised reductions and non-uniform reductions (see Chapter 4 of [422] for explanation of these terms and proofs). Nguyen [456] gives a summary of the complexity results and current best running times of algorithms for these problems.

On the other hand, if a lattice is sufficiently nice then these problems may be easy.

Example 16.3.3. Let $L \subset \mathbb{R}^2$ be the lattice with basis matrix

$$B = \begin{pmatrix} 1001 & 0 \\ 0 & 2008 \end{pmatrix}.$$

Then every lattice vector is of the form $(1001a, 2008b)$ where $a, b \in \mathbb{Z}$. Hence the shortest non-zero vectors are clearly $(1001, 0)$ and $(-1001, 0)$. Similarly, the closest vector to $\underline{w} = (5432, 6000)$ is clearly $(5005, 6024)$.

Why is this example so easy? The reason is that the basis vectors are orthogonal. Even in large dimensions, the SVP and CVP problems are easy if one has an orthogonal basis for a lattice. When given a basis that is not orthogonal it is less obvious whether there exists a non-trivial linear combination of the basis vectors that gives a vector strictly shorter than the shortest basis vector. A basis for a lattice that is "as close to orthogonal as it can be" is therefore convenient for solving some computational problems.

[2] We do not give details of complexity theory in this book; in particular we do not define the term "NP-hard".