Chapter 2
Lattices and Applications

A lattice in $\mathbb{R}^n$ is a set of points (vectors) composed by all integer linear combinations of independent vectors.

Definition 2.1 Let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m$ be linearly independent vectors in $\mathbb{R}^n$. A *lattice* Λ with basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m\}$ is defined as

$$\Lambda = \{u_1\mathbf{b}_1 + \cdots + u_m\mathbf{b}_m : u_1, \ldots, u_m \in \mathbb{Z}\}. \tag{2.1}$$

The integer m is called the *rank* of Λ. If $m = n$, we say that Λ is *full rank*.
We may also consider the set $\{(0, \ldots, 0)\} \subset \mathbb{R}^n$ as a (degenerate) lattice of rank 0.

Definition 2.2 A *generator matrix* B for a lattice Λ is a matrix whose columns[1] are a basis for it, i.e.,

$$B = \begin{bmatrix} \mathbf{b}_1 & \mathbf{b}_2 & \ldots & \mathbf{b}_m \end{bmatrix}.$$

A vector $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$ is in Λ if and only if it can be written as

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \mathbf{b}_1 & \mathbf{b}_2 & \ldots & \mathbf{b}_m \end{bmatrix} \begin{bmatrix} u_1 \\ \vdots \\ u_m \end{bmatrix}, u_1, \ldots u_m \in \mathbb{Z}. \tag{2.2}$$

In other words, $\Lambda = \{B\mathbf{u} : \mathbf{u} \in \mathbb{Z}^m\}$, where $\mathbb{Z}^m$ denotes the set of m-uples of integers. Note that in the above definition, B is a matrix of rank m and it is not unique, since a lattice, for $m \geq 2$, has infinitely many bases (as it will be seen next).

[1] Some authors use the row convention of considering basis vectors as rows of a generator matrix; we follow here the column convention.

S.I.R. Costa et al., *Lattices Applied to Coding for Reliable and Secure Communications*, SpringerBriefs in Mathematics,
https://doi.org/10.1007/978-3-319-67882-5_2

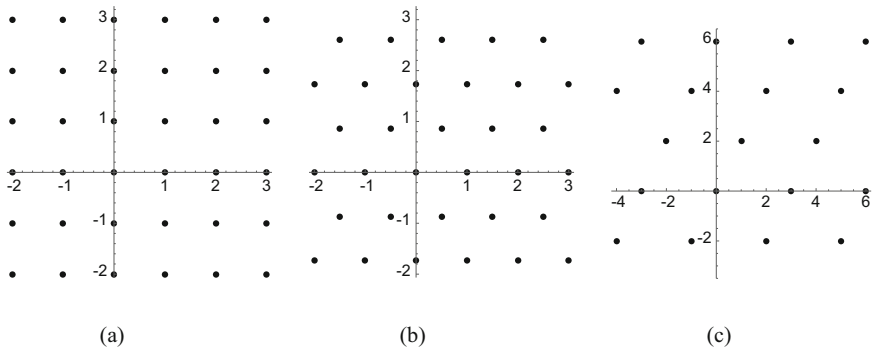


Fig. 2.1 Three lattices in $\mathbb{R}^2$. (**a**) The square lattice $\mathbb{Z}^2$. (**b**) The hexagonal lattice. (**c**) A lattice Λ with basis $\{(3,0),(1,2)\}$

Example 2.1 We start with three examples of rank 2 lattices in $\mathbb{R}^2$. In Fig. 2.1a the *square lattice* $\mathbb{Z}^2$ is displayed. A natural basis for it is $\{(1,0),(0,1)\}$. In Fig. 2.1b the so-called *hexagonal lattice* is displayed. One of its bases is $\left\{(1,0),(1/2,\sqrt{3}/2)\right\}$. A third lattice Λ is depicted in Fig. 2.1c, which has a natural basis given by $\{(3,0),(1,2)\}$.

Example 2.2 The *cubic lattice* $\mathbb{Z}^n \subset \mathbb{R}^n$ (also called the integer lattice) is the set of all n-uples of integers. A basis for $\mathbb{Z}^n$ is the canonical basis of $\mathbb{R}^n$, $\{\mathbf{e}_1,\ldots,\mathbf{e}_n\}$, where $\mathbf{e}_1 = (1,0,\ldots,0), \mathbf{e}_2 = (0,1,0\ldots,0),\ldots,\mathbf{e}_n = (0,0,\ldots,0,1)$. The first lattice $\mathbb{Z}^2$ of Example 2.1 is the particular case when $n = 2$.

Example 2.3 Consider the set A_2 of all vectors in $(x_1,x_2,x_3) \in \mathbb{Z}^3$ such that $x_1+x_2+x_3 = 0$. This set is parameterized by letting two coordinates be free and forcing the third one to be the negative sum of the two free coordinates (if we let say x_1, x_3 free, then $x_2 = -x_1-x_3$), showing that we can describe A_2 by integer linear combinations of two independent vectors. This is a rank 2 lattice in $\mathbb{R}^3$, since a generator matrix for it is

$$B = \begin{bmatrix} 1 & 0 \\ -1 & 1 \\ 0 & -1 \end{bmatrix}.$$

It turns out that the hexagonal lattices in Example 2.1 and A_2 are equivalent lattices, something that will be proven after Definition 2.11 (see Example 2.9). In a similar way, we can define the rank n lattice A_n in $\mathbb{R}^{n+1}$:

$$A_n = \left\{(x_1,x_2,\ldots,x_{n+1}) \in \mathbb{Z}^{n+1} : x_1 + x_2 + \cdots + x_{n+1} = 0\right\}. \tag{2.3}$$

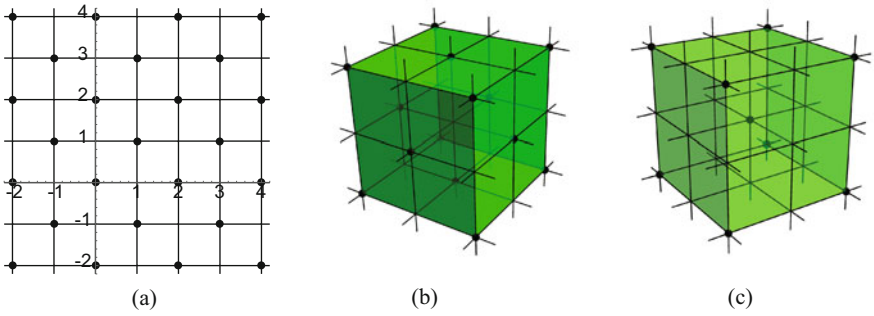


Fig. 2.2 The lattices D_2, D_3= FCC and BCC. (**a**) The D_2 lattice in $\mathbb{R}^2$. (**b**) The D_3 or FCC lattice (face-centered cubic lattice). (**c**) The BCC (body-centered cubic) lattice

Example 2.4 The full rank lattice $D_n \subset \mathbb{R}^n$, also called the checkerboard lattice, is defined as

$$D_n = \{(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n : x_1 + x_2 + \cdots + x_n \text{ is even}\}. \tag{2.4}$$

The lattices D_2 and D_3, shown in Fig. 2.2a, b, have bases $\{(1,1),(-1,1)\}$ and $\{(2,0,0),(1,1,0),(1,0,1)\}$, respectively (see Exercise 2.1). The lattice D_3 is also known as the face-centered cubic lattice, FCC, since it can be spanned from the vertices and the face centers of a cube with sides of length 2 (Fig. 2.2b). Another lattice in $\mathbb{R}^3$ "constructed" from cubes is the body-centered cubic (BCC) lattice. For example, $\{(2,0,0),(0,2,0),(1,1,1)\}$ is a basis for the BCC lattice (Fig. 2.2c).

There is an alternative definition of lattice in terms of groups. We consider the natural group structure of $\mathbb{R}^n$ with respect to vector addition. Notice that any lattice $\Lambda \subset \mathbb{R}^n$ is a set of vectors satisfying

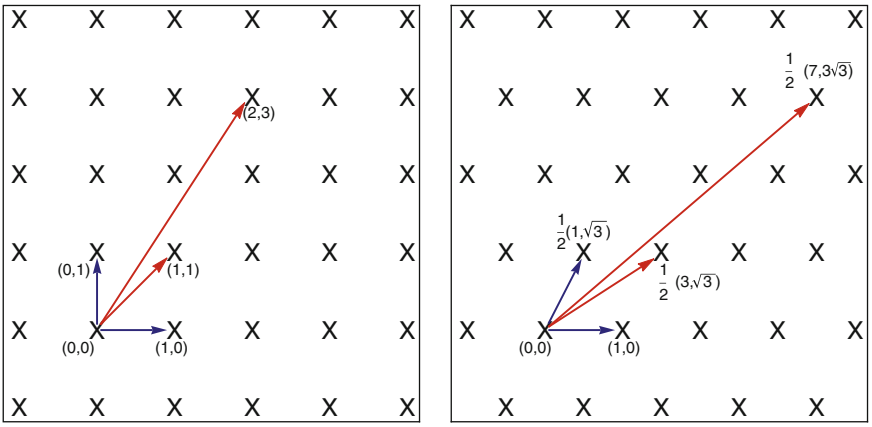
- closure: if $\mathbf{x}, \mathbf{y} \in \Lambda$, then $\mathbf{x} + \mathbf{y} \in \Lambda$,
- for every vector $\mathbf{x} \in \Lambda$, $-\mathbf{x} \in \Lambda$.

These two facts show that a lattice Λ is an *additive subgroup* of $\mathbb{R}^n$. Moreover, a lattice is also a *discrete subset* of $\mathbb{R}^n$. This means that there exists a radius r such that the balls in $\mathbb{R}^n$ centered at lattice points are disjoint. In fact, these two properties provide an equivalent definition of a lattice:

Theorem 2.1 ([20, p. 78]) *A subset of $\mathbb{R}^n$ is a lattice if and only if it is a discrete additive subgroup.*

Through the last proposition, we can see that a set composed by linear integer combinations of dependent vectors is not always a lattice. For instance, for $n = 1$, let A be the set of linear integer combinations of $v_1 = 1$ and $v_2 = \sqrt{2}$. This set is not a lattice, since it is not discrete.

As mentioned earlier, a lattice Λ has (infinitely) many bases for $m \geq 2$. Figure 2.3 illustrates different bases for the integer and for the hexagonal lattices in $\mathbb{R}^2$. The characterization of when distinct bases generate the same lattice is done next by



(a) (b)

Fig. 2.3 Examples of distinct bases for the same lattice. (**a**) $\mathbb{Z}^2$ lattice. (**b**) Hexagonal lattice

means of a special type of matrices, called unimodular. An $m \times m$ matrix U is said to be *unimodular* if it has integer entries and its determinant is 1 or -1. This is equivalent to saying that the integer matrix U has an inverse with integer entries, as stated in Exercise 2.2.

Theorem 2.2 *Two matrices B and $\overline{B}$ generate the same lattice if and only if there exists a unimodular matrix U such that $\overline{B} = BU$.*

Proof Let $\beta_1 = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ and $\beta_2 = \left\{\overline{\mathbf{b}}_1, \ldots, \overline{\mathbf{b}}_m\right\}$ be bases for Λ and $\overline{\Lambda}$, with associated generator matrices B and $\overline{B}$, respectively. Notice that $\overline{\Lambda} \subseteq \Lambda$ if and only if we can write all vectors of β_1 as integer linear combinations of β_2, i.e.,

$$\overline{\mathbf{b}}_j = \sum_{i=1}^{m} \mathbf{b}_i \alpha_{ij}, \text{ for } j = 1, \ldots m, \text{ and } \alpha_{ij} \in \mathbb{Z}.$$

In other words, $\overline{B} = BU$, where $U = (\alpha_{ij})$ is an integer matrix. Analogously, $\Lambda \subseteq \overline{\Lambda}$ if and only if $B = \overline{B}V$, for some integer matrix V. Combining both equations yields

$$\overline{B} = \overline{B}VU \Rightarrow \overline{B}(\mathbf{I} - VU) = \mathbf{0}$$

since every column of $\mathbf{I} - VU$ defines a linear equation in $\overline{\mathbf{b}}_1, \ldots, \overline{\mathbf{b}}_m$, and recalling that $\overline{\mathbf{b}}_1, \ldots, \overline{\mathbf{b}}_m$ are linearly independent, the corresponding coefficients must be all 0. Thus

$$VU = \mathbf{I} \Rightarrow \det(V)\det(U) = 1$$

which, together with the fact that U, V are matrices with integer coefficients, implies that $\det(U) = \det(V) = \pm 1$; therefore U is unimodular.

Conversely, if $\overline{B} = BU$, with U unimodular, then $\overline{\Lambda} \subseteq \Lambda$ and $B = \overline{B}U^{-1}$ where U^{-1} has integer entries, which implies that $\Lambda \subseteq \overline{\Lambda}$, concluding the proof.

Example 2.5 In Fig. 2.3 distinct bases for two lattices in the plane are illustrated. The generator matrices associated with the two different bases of the lattice $\mathbb{Z}^2$ exhibited in Fig. 2.3a are

$$B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } \overline{B} = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}.$$

For the lattice of Fig. 2.3b, we have

$$B = \begin{bmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{bmatrix} \text{ and } \overline{B} = \begin{bmatrix} 3/2 & 7/2 \\ \sqrt{3}/2 & 3\sqrt{3}/2 \end{bmatrix} = \begin{bmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}.$$

In both cases, the unimodular matrix that takes a basis into the other is given by

$$U = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}.$$

Note that the above theorem provides a way to check if two full rank square matrices A and B generate the same lattice: this will happen if and only if $B^{-1}A$ is a unimodular matrix (see Exercise 2.3).

Definition 2.3 Given a generator matrix B for a lattice Λ, we define its associated *Gram matrix* by $G = B^T B$.

Each element G_{ij} is the inner product between the basis vectors $\mathbf{b}_i$ and $\mathbf{b}_j$, $G_{ij} = \langle \mathbf{b}_i, \mathbf{b}_j \rangle$. It follows from Theorem 2.2 that, for $m \geq 2$, a lattice has infinitely many Gram matrices; in fact, any $G' = U^T G U$, where U is unimodular, is also a Gram matrix for Λ. However the determinant of a Gram matrix is the same for all bases of Λ, since $|\det U| = 1$. We can then define the *determinant of* Λ as the determinant of any of its Gram matrices. Since this is always a positive number, we can define:

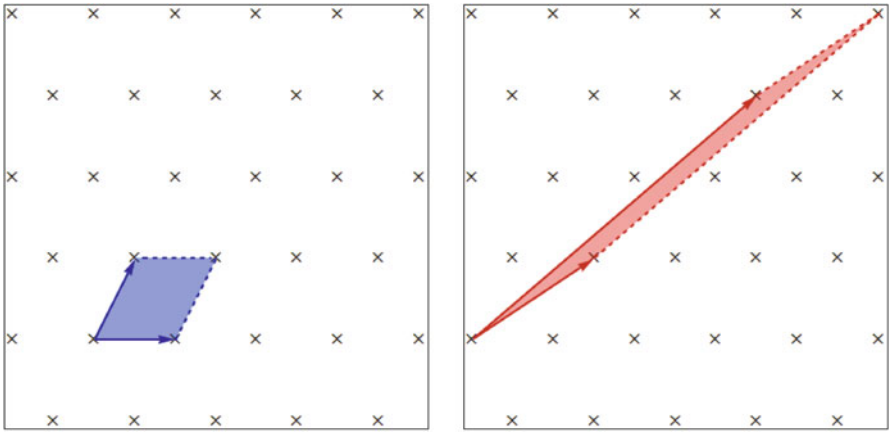
Definition 2.4 The *volume* of a lattice Λ, denoted by $V(\Lambda)$, is the (positive) square root of the determinant of a Gram matrix for Λ.

To give a geometric interpretation to the quantity $V(\Lambda)$, we define the *fundamental parallelotope* $\mathscr{P}(B)$ as

$$\mathscr{P}(B) = \{\alpha_1 \mathbf{b}_1 + \cdots + \alpha_m \mathbf{b}_m, 0 \leq \alpha_i < 1, i = 1, \ldots m\}. \tag{2.5}$$

$\mathscr{P}(B)$ is contained in the m-dimensional subspace of $\mathbb{R}^n$ generated by the set of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_m$. The Euclidean *volume* of $\mathscr{P}(B)$ is

$$V(\Lambda) = \sqrt{\det B^T B} = |\det B|. \tag{2.6}$$



(a) (b)

Fig. 2.4 Distinct fundamental parallelotopes for the hexagonal lattice. (**a**) Parallelotope associated with the basis $\left\{(1,0),(1/2,\sqrt{3}/2)\right\}$. (**b**) Parallelotope associated with the basis $\left\{(3/2,\sqrt{3}/2),(7/2,3\sqrt{3}/2)\right\}$

Example 2.6 Continuing Example 2.5, the two distinct bases for the hexagonal lattice (Fig. 2.3b) produce different fundamental parallelotopes, illustrated in Fig. 2.4. The area of both parallelotopes is equal to $\sqrt{3}/2$, the volume of the hexagonal lattice.

Given a full rank lattice Λ, it is possible to check that the disjoint union of translates of $\mathscr{P}(B)$ by vectors of Λ is equal to the whole space $\mathbb{R}^n$. In other words, the fundamental parallelotope $\mathscr{P}(B)$ *tiles* $\mathbb{R}^n$ through translations by points of Λ, that is:

(i)

$$\text{If } \mathbf{x},\mathbf{y}\in\Lambda, \mathbf{x}\neq\mathbf{y}, \textit{then } (\mathbf{x}+\mathscr{P}(B))\bigcap(\mathbf{y}+\mathscr{P}(B))=\varnothing \text{ and}$$

(ii)

$$\bigcup_{\mathbf{x}\in\Lambda}(\mathbf{x}+\mathscr{P}(B))=\mathbb{R}^n. \tag{2.7}$$

From now on in this and in the next chapters, in order to simplify the statements, we *assume all lattices to be full rank*, unless stated otherwise.

Besides the fundamental parallelotope, other regions $A\subset\mathbb{R}^n$ may as well tile $\mathbb{R}^n$ through translations by elements of Λ. In fact, item (i) of the tiling condition above can be "relaxed" to (i') requiring that for $\mathbf{x},\mathbf{y}\in\Lambda$, $(\mathbf{x}+A)$ and $(\mathbf{y}+A)$ intersect at most on their boundaries. Any region $A\subset\mathbb{R}^n$ satisfying conditions

(i') and (ii) is called a *fundamental region* for Λ. Any fundamental region for Λ has volume $V(\Lambda)$ (see, e.g., [86, p.28, Thm. 1.6]). Another important fundamental region is the *Voronoi region*. Let $\|.\|$ denote the standard Euclidean norm of a vector $\mathbf{x} \in \mathbb{R}^n$,

$$\|\mathbf{x}\| = \sqrt{x_1^2 + x_2^2 + \ldots + x_n^2}.$$

Definition 2.5 The *Voronoi region*, also called Dirichlet region, $\mathcal{V}_\Lambda(\mathbf{x})$ at a point $\mathbf{x} \in \Lambda$ is the set of all points in $\mathbb{R}^n$ which are at least as close to $\mathbf{x}$ than to any other lattice point, i.e.:

$$\mathcal{V}_\Lambda(\mathbf{x}) = \{\mathbf{y} \in \mathbb{R}^n : \|\mathbf{x} - \mathbf{y}\| \leq \|\mathbf{z} - \mathbf{y}\|, \text{for all } \mathbf{z} \in \Lambda\}. \tag{2.8}$$

The Voronoi region at the origin,

$$\mathcal{V}_\Lambda(\mathbf{0}) = \mathcal{V}(\Lambda), \tag{2.9}$$

is called the Voronoi region of the lattice, and we have that $\mathcal{V}_\Lambda(\mathbf{x}) = \mathcal{V}(\Lambda) + \mathbf{x}$. It should be remarked that although the fundamental parallelotope depends on the choice of basis, the Voronoi region of a lattice is unique and intrinsic to the standard metric structure of $\mathbb{R}^n$. If a point is in the boundary of a Voronoi region, it is equidistant from at least two lattice points. Figures 2.5, 2.6, and 2.7 illustrate the tilings of three lattices by different fundamental regions including their Voronoi regions on part (b) (see also Exercise 2.4). The Voronoi regions of the lattices $\mathbb{Z}^3$ and FCC are a cube with sides of length one and a rhombic dodecahedron centered at the origin, respectively. The Voronoi region of a lattice is a convex set of $\mathbb{R}^n$ enclosed by hyperplanes which are equidistant from the origin and a relevant lattice point. It is usually very hard to determine, particularly in high dimensions. For special classes of lattices such as the so-called root lattices (which include A_n and D_n; see (2.4)), they have been determined [25, 26]. Algorithms for numerically determining the Voronoi region have been developed in several references. Those results are important in applications of lattices to communications such as the ones regarding quantizers and channel coding (see this chapter, Sect. 2.5.1, Chap. 6, and also [26, Chaps. 2 and 3].

2.1 Sphere Packing and Covering

One of the main subjects of research on lattices is their association with the hard problem of finding dense packings in the Euclidean space, which has many applications.

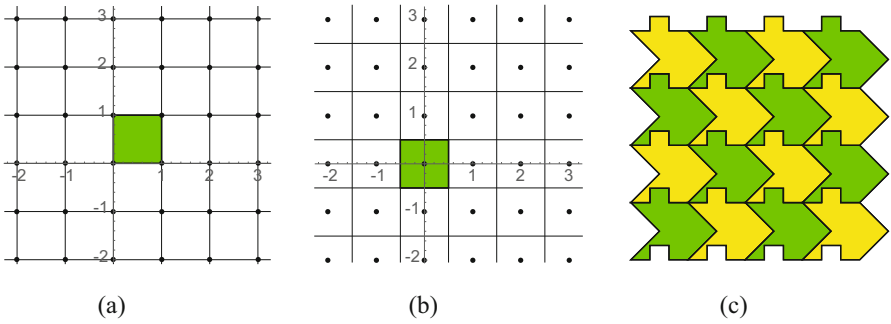


Fig. 2.5 Different fundamental regions and tilings of the plane by $\mathbb{Z}^2$. (**a**) The fundamental parallelotope of the lattice $\mathbb{Z}^2$ with basis $\{(1,0),(0,1)\}$ and associated plane tiling. (**b**) The Voronoi region of the lattice $\mathbb{Z}^2$ and its associated plane tiling. (**c**) A tiling of the plane though translations of another fundamental region of $\mathbb{Z}^2$

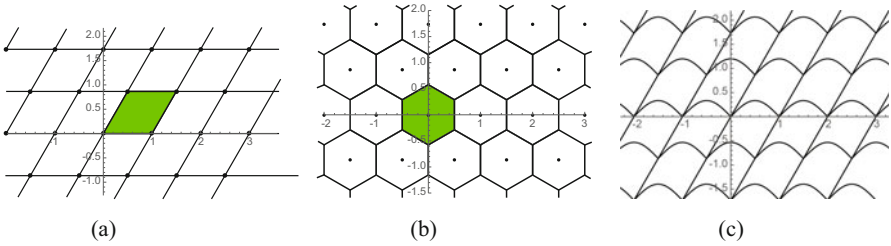


Fig. 2.6 Different fundamental regions and tilings of the plane by the hexagonal lattice A_2. (**a**) The fundamental parallelotope the hexagonal lattice for basis $\left\{(1,0),(1/2,\sqrt{3}/2)\right\}$ and associated plane tiling. (**b**) The Voronoi region of the hexagonal lattice and its associated plane tiling. (**c**) A tiling of the plane though translations of another fundamental region of the hexagonal lattice

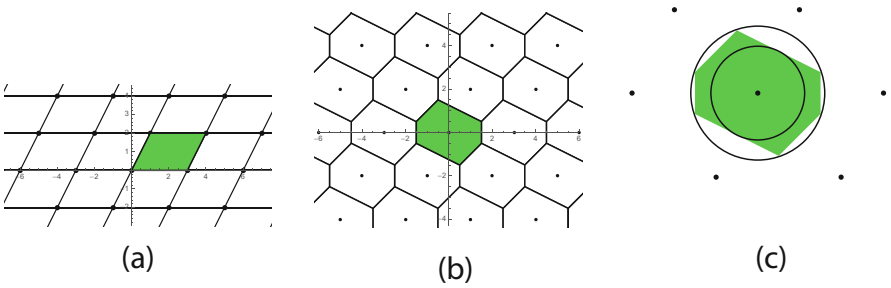


Fig. 2.7 The lattice Λ with basis $\{(3,0),(1,2)\}$: fundamental parallelotope, Voronoi region, and packing and covering balls. (**a**) The fundamental parallelotope of the lattice Λ with basis $\{(3,0),(1,2)\}$ and associated plane tiling. (**b**) The Voronoi region of the lattice Λ and its associated plane tiling. (**c**) The Voronoi region and the packing and the covering circles of Λ

The *minimum norm* (or minimum distance) of a lattice corresponds to the minimum among all norms of non-zero vectors in Λ, i.e.,[2]:

$$\lambda = \min_{\mathbf{0} \neq \mathbf{x} \in \Lambda} \|\mathbf{x}\| . \tag{2.10}$$

From the fact that a lattice is a discrete additive subgroup of $\mathbb{R}^n$ (Theorem 2.1), it can be shown that any lattice has a non-vanishing vector of minimum norm $\lambda > 0$.

Let $\mathscr{B}^n(r)$ denote a Euclidean ball of radius r around the origin, i.e.:

$$\mathscr{B}^n(r) = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leq r\} . \tag{2.11}$$

It is easy to see that $r = \lambda/2$ is the largest value for which the translates of the balls $\mathscr{B}^n(\rho)$ centered at $\mathbf{x} \in \Lambda$ have disjoint interiors. We call

$$\rho = \lambda/2 \tag{2.12}$$

the *packing radius* of Λ. Notice also that the ball $\mathscr{B}^n(\rho)$ is inside and touches the boundaries of the Voronoi region of Λ. We define a *lattice packing* as the union of translates of the ball $\mathscr{B}^n(\rho)$ by points of Λ.

The ratio vol $\mathscr{B}^n(\rho)/V(\Lambda)$ describes how much of the Voronoi region is occupied by $\mathscr{B}^n(\rho)$. Due to the lattice homogeneity, the percentage of the space $\mathbb{R}^n$ covered by translates of $\mathscr{B}^n(\rho)$ by lattice points is given by the same ratio.

Definition 2.6 The *packing density* of Λ is defined as

$$\Delta(\Lambda) = \frac{\text{vol } \mathscr{B}^n(\rho)}{V(\Lambda)}. \tag{2.13}$$

Example 2.7 In Fig. 2.8 we illustrate the lattices of Example 2.1, their packing balls and respective packing densities. The square and the hexagonal lattices both have packing radius equal to $1/2$ and packing densities $\Delta = 0.785$ and $\Delta = 0.906$, respectively. The lattice with basis $\{(3,0), (1,2)\}$ has packing radius equal to $\sqrt{5}/2$ and packing density $\Delta = 0.654$.

Notice that vol $\mathscr{B}^n(\rho) = \rho^n$vol $\mathscr{B}^n(1)$. The volume of the Euclidean ball $\mathscr{B}^n(1)$, of radius 1, is known [26]:

$$\text{vol } \mathscr{B}^n(1) = \begin{cases} \frac{\pi^{n/2}}{(n/2)!} & \text{if } n \text{ is even, and} \\ \frac{2^n \pi^{(n-1)/2}((n-1)/2)!}{n!} & \text{if } n \text{ is even} \end{cases} \tag{2.14}$$

When $n = 2, 3$ we recover the area of the unit circle (π) and the volume of the unit sphere ($4\pi/3$), respectively.

[2] In several textbooks and papers, the minimum norm is defined as the square of this number.

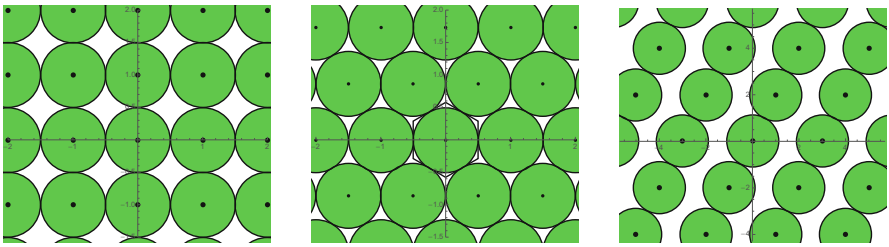


Fig. 2.8 Lattice packings. (**a**) The square lattice: ρ=1/2 and $\Delta(\mathbb{Z}^2) = 0.7854$. (**b**) The hexagonal lattice: ρ=1/2 and $\Delta(A_2) = 0.9069$. (**c**) The lattice Λ with basis $\{(3,0),(1,2)\}$: $\rho = \sqrt{5}/2$ and $\Delta(\Lambda) = 0.6545$

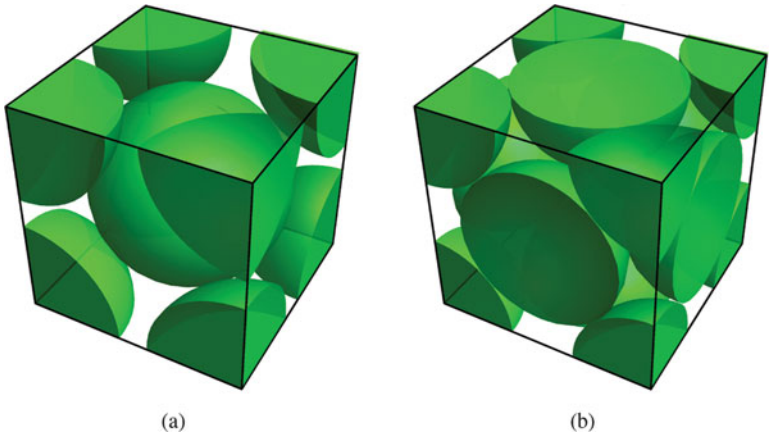


Fig. 2.9 The packing density of the BCC and the FCC lattices. (**a**) A view of the BCC packing density ($\rho = \sqrt{3}/2$, $\Delta = 0.6802$). (**b**) A view of the FCC packing density ($\rho = \sqrt{2}/2$, $\Delta = 0.7405$)

The packing densities of $\mathbb{Z}^3$ and of the lattices FCC and BCC are $\pi/6 = 0.5236$, $\pi/18 = 0.7405$, and $\pi\sqrt{3}/8 = 0.6802$, respectively (see Figs. 2.9 and 2.10).

Definition 2.7 The *center density* of a lattice is defined as $\delta(\Lambda) = \Delta(\Lambda)/\text{vol}\,\mathscr{B}^n(1) = \rho^n/V(\Lambda)$.
The center density provides a way of comparing lattices in the same dimension that avoids the complicated formula (2.14).

Attached to a sphere packing is the concept of kissing number.

Definition 2.8 The *kissing number* of a lattice is the number of packing balls that touch a fixed one, which corresponds to the number of lattice points having the minimum non-vanishing norm.
For our three lattices in Figs. 2.5, 2.6, and 2.7, this number is 4, 6, and 2, respectively.

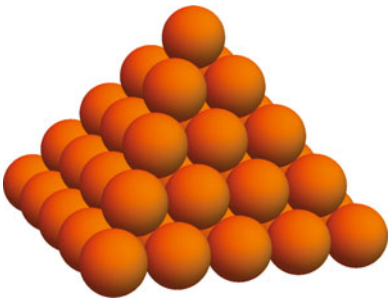


Fig. 2.10 The FCC lattice (the best packing in $\mathbb{R}^3$) represented as the centers of an orange pile

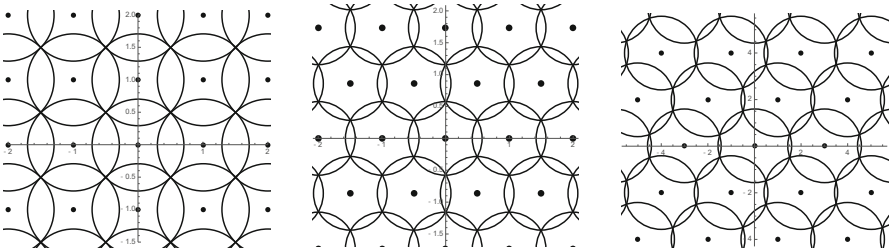


Fig. 2.11 Covering densities of three different lattices. (**a**) The square lattice: covering radius $\nu = \sqrt{2}/2$ and covering density $\theta(\mathbb{Z}^2) = 1.5708$. (**b**) The hexagonal lattice: covering radius $\mu = \sqrt{3}/3$, covering density $\Theta(A_2) = 1.2092$. (**c**) The lattice with basis $\{(3,0),(1,2)\}$: covering radius $\mu = \sqrt{10}/2$, covering density $\Theta(\Lambda) = 1.3088$

A "dual" concept to sphere packing is the one of *sphere covering* which also has several applications. In the covering problem, we ask for the thinnest possible arrangement of spheres that cover all points of $\mathbb{R}^n$. More formally:

Definition 2.9 The *covering radius* of a lattice is defined as the minimum μ such that the translates of the balls $\mathscr{B}^n(\mu)$ by points of Λ *cover* $\mathbb{R}^n$, i.e.:

$$\bigcup_{\mathbf{x}\in\Lambda} (\mathscr{B}^n(\mu) + \mathbf{x}) = \mathbb{R}^n.$$

If we consider the vertices of the Voronoi region of Λ (called holes), the covering radius is the biggest distance from one of the holes to the origin. (A hole which attains this distance is called a deep hole.) The n-dimensional covering ball $\mathscr{B}^n(\mu)$ circumscribes the Voronoi region of a lattice, whereas the packing ball is inscribed in it (see Figs. 2.11, 2.7 c).

Definition 2.10 The *covering density* is then defined as

$$\theta(\Lambda) = \frac{\text{vol}\,\mathscr{B}^n(\mu)}{V(\Lambda)}. \tag{2.15}$$

For $n \geq 2$, the covering density is always greater than 1, while the packing density is always smaller than 1. Figure 2.11 illustrates the covering density of our three different lattices in $\mathbb{R}^2$.

2.1.1 Equivalent Lattices

All lattice parameters discussed in this section remain unchanged under some transformations. For example, if we scale all lattice vectors by the same constant c, the lattice volume will be scaled by c^n and the (packing and covering) radii by c. Therefore, the packing and covering densities (as well as the kissing number) do not change. The same happens if we rotate all lattice points. Therefore, it makes sense to treat these lattices as equivalent. Equivalent lattices are obtained by rotating, reflecting, or scaling the original one. A formal definition is stated next. We recall that an $n \times n$ matrix Q is *orthogonal* if $Q^T Q = QQ^T = \mathbf{I}_n$, where $\mathbf{I}_n$ is the $n \times n$ identity matrix. Orthogonal matrices are associated with linear maps which preserve angles and lengths, defining rotations or reflections in $\mathbb{R}^n$.

Definition 2.11 Two lattices Λ_1 and Λ_2 contained in $\mathbb{R}^n$ are *equivalent* if there exist an orthogonal matrix Q, a real number c, and generator matrices B_1 and B_2 for Λ_1 and Λ_2, respectively, such that $B_1 = cQB_2$. In particular, Λ_1 and Λ_2 are called *congruent* if $|c| = 1$.
We write $\Lambda_1 \sim \Lambda_2$ for two equivalent lattices.

Remark 2.1 If we consider the Gram matrices G_1 and G_2 associated with the specific generator matrices B_1 and B_2 in the last definition, we have $G_1 = c^2 G_2$. Furthermore, it can be shown that two lattices which have Gram matrices related to specific bases satisfying $G_1 = c^2 G_2$ must be congruent, and therefore this can be taken as an alternative definition of equivalent lattices. Then congruent lattices must have identical Gram matrices related to some specific generator matrices.

Remark 2.2 Given Λ_1 and Λ_2 with arbitrary generator matrices B_1 and B_2, $\Lambda_1 \sim \Lambda_2$ if and only if there are matrices Q orthogonal and U unimodular such that $B_1 = cQB_2U$. Accordingly, two arbitrary Gram matrices G_1 and G_2 for equivalent lattices must satisfy $G_1 = c^2 U^t G_2 U$, with U unimodular.

Example 2.8 The lattice generated by

$$\begin{bmatrix} 1 & \frac{1}{2}\left(\sqrt{3}+1\right) \\ -1 & \frac{1}{2}\left(\sqrt{3}-1\right) \end{bmatrix}$$

is equivalent to the hexagonal lattice, since

$$\begin{bmatrix} 1 & \frac{1}{2}\left(\sqrt{3}+1\right) \\ -1 & \frac{1}{2}\left(\sqrt{3}-1\right) \end{bmatrix} = \sqrt{2}\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \cdot \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}.$$

It is a clockwise rotation of 45° and an expansion of factor $\sqrt{2}$ of the hexagonal lattice.

Remark 2.3 The definition above can be extended to compare lattices which are originally contained in different dimensions by identifying a lattice in $\mathbb{R}^n$ with its natural inclusion in $\mathbb{R}^t$, $t > n$, which adds $(t - n)$ zeros in the coordinates of its vectors.

Example 2.9 View the hexagonal lattice of Example 2.1 as included in $\mathbb{R}^3$, generated by $\left\{(1,0,0),(1/2,\sqrt{3}/2,0)\right\}$. We can show that it is equivalent to the lattice A_2 given in Example 2.3. In fact, for the generator matrix B_1 associated with this basis and another generator matrix B_2 for the lattice A_2 associated with the basis $\{(1,-1,0),(0,-1,1)\}$, we can see that the Gram matrices of the two lattices related to these bases are multiples: $B_2^T B_2 = 2B_1^T B_1$, which implies their equivalence (Remark 2.1). We can also write explicitly the equivalence of these lattices as described in Remark 2.2 by starting from the generator matrix for A_2 as given in Example 2.3: $\begin{bmatrix} 1 & 0 \\ -1 & 1 \\ 0 & -1 \end{bmatrix} = \sqrt{2}Q \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \\ 0 & 0 \end{bmatrix} U$, where Q is the 3×3 orthogonal matrix having for its columns the vectors $(1/\sqrt{2}, -1/\sqrt{2}, 0)$, $(-1/\sqrt{6}, -1/\sqrt{6}, 2/\sqrt{6})$, and $(1/\sqrt{3}, 1/\sqrt{3}, 1/\sqrt{3})$, while U is the 2×2 unimodular matrix having for its columns the vectors $(1,0)$ and $(0,-1)$. You may use similar arguments in Exercise 2.7 to check another example of equivalent lattices.

2.2 Sublattices

Given lattices Λ' and Λ such that $\Lambda' \subseteq \Lambda$, Λ' is said to be a *sublattice* of Λ. A subset of a lattice is a sublattice if and only if it is an additive subgroup (i.e., for any $\mathbf{x}$ and $\mathbf{y}$ in Λ', $\mathbf{x} + \mathbf{y}$ and $-\mathbf{y}$ also are in Λ').

Let $\Lambda \subset \mathbb{R}^n$ be a full rank lattice with generator matrix B, and let M be an $n \times n$ integer matrix. If $\det(M) \neq 0$, then BM is a generator matrix of a full rank sublattice Λ' of Λ. Reciprocally any generator matrix A of a full rank sublattice Λ' of Λ can be written as BM for some integer matrix M: Λ and Λ' are said to form a *nested lattice pair*, where Λ is the fine lattice and Λ' is the coarse lattice.

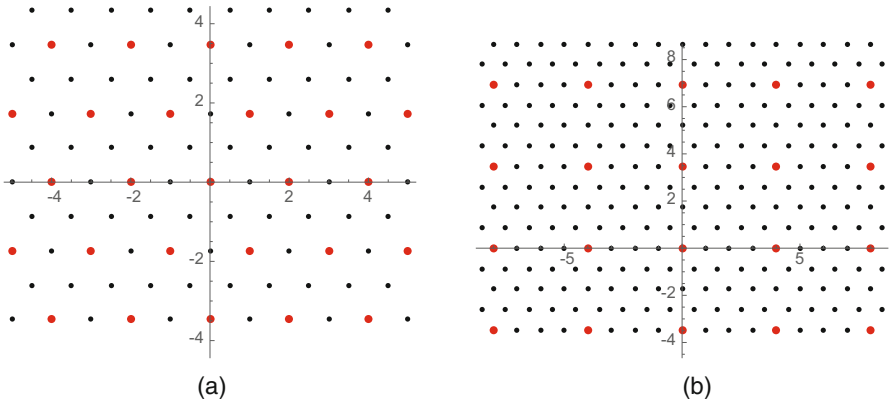


Fig. 2.12 Sublattices of the hexagonal lattice. (**a**) The hexagonal lattice and its sublattice Λ_1 with generator matrix BM_1. (**b**) The hexagonal lattice and its sublattice Λ_2 with generator matrix BM_2

Example 2.10 For the hexagonal lattice Λ with generator matrix

$$B = \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix},$$

we may consider

$$M_1 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \text{ and } M_2 = \begin{bmatrix} 4 & -2 \\ 0 & 4 \end{bmatrix}$$

and the sublattices Λ_1 and Λ_2 generated by BM_1 and BM_2 (coarse lattice) illustrated in Fig. 2.12.

Example 2.11 The lattices D_n described in Sect. 2.4 are sublattices of the integer lattice $\mathbb{Z}^n$.

Nested lattices have been used in several applications. In this book, they appear in the construction of wiretap codes in Chap. 3, spherical codes in Chap. 5, and index codes in Chap. 6.

Since a sublattice $\Lambda' \subseteq \Lambda$ is a subgroup, Λ can be partitioned into a set of cosets of Λ' which form a finite quotient group $\frac{\Lambda}{\Lambda'}$ (or Λ/Λ'). Each of these cosets can be identified using a coset leader (or coset representative) in the fundamental parallelotope of the lattice Λ. Each leader also can be chosen in the Voronoi region of Λ, as it will be seen in Chap. 6. Let B be a generator matrix for Λ and $B' = BM$ be one for Λ'. The number of elements of $\frac{\Lambda}{\Lambda'}$ is given by:

$$\left|\frac{\Lambda}{\Lambda'}\right| = \frac{V(\Lambda')}{V(\Lambda)} = |\det(M)|.$$

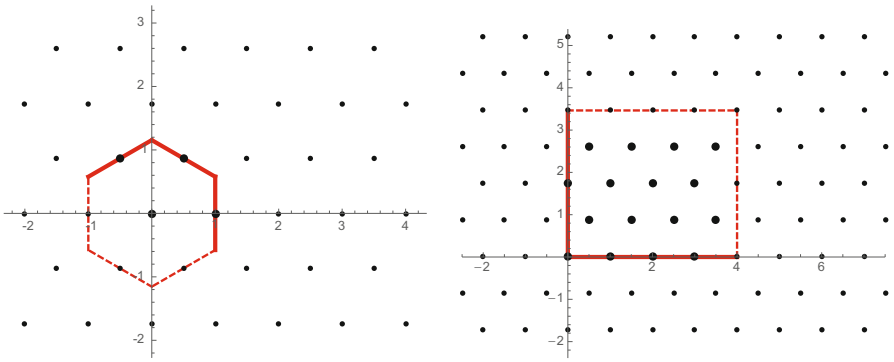


Fig. 2.13 Quotients of the hexagonal lattices. (**a**) The quotient $\frac{\Lambda}{\Lambda_1}$ represented by coset leaders inside the Voronoi set of Λ_1. (**b**) The quotient $\frac{\Lambda}{\Lambda_2}$ represented by coset leaders inside a fundamental polytope of Λ_2

In Example 2.10 above, we have $\left|\frac{\Lambda}{\Lambda'}\right| = 4$ and $\left|\frac{\Lambda}{\Lambda'}\right| = 16$ (see Fig. 2.13).

Any integer squared n-dimensional matrix M can be decomposed into the so-called *Smith normal form*: $M = UDW$ where U and W are unimodular matrices and $D = \{d_{i,j}\}$ is a diagonal matrix where $d_{j,j} \in \mathbb{N}$, $d_{i,i}|d_{i+1,i+1}$ [21, Sect. 2.4].

The Smith normal form can be used to extract special bases of a pair of nested full rank lattices.

Theorem 2.3 *Given a nested pair of full rank lattices $\Lambda' \subseteq \Lambda$, there exist special bases $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ of Λ' and $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ of Λ such that $\mathbf{w_i} = k_i\mathbf{v_i}$, for $i = 1, \ldots, n$, $k_i \in \mathbb{N}$.*

Proof Let B be a generator matrix of Λ and BM be a generator matrix of Λ'. Consider the Smith decomposition, $M = UDW$ where W, U are unimodular lattices. According to Theorem 2.2, $BMW^{-1} = (BU)D$ is also a generator matrix of Λ', and BU is a generator matrix of Λ, since U and W^{-1} are unimodular matrices. If we take $\{\mathbf{w}_1, \ldots, \mathbf{w}_n\}$ and $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ as the columns of the matrices BMW^{-1} and BU, respectively, we get $\mathbf{w}_i = d_{i,i}\mathbf{v}_i$. Take $k_i = d_{i,i}$.

Example 2.12 In the nested lattice pair $\Lambda_2 \subseteq \Lambda$ of Example 2.10, we have the following Smith decomposition for M:

$$M = UDW = \begin{bmatrix} -1 & -1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 8 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ -1 & 0 \end{bmatrix}.$$

After calculating $A = BMW^{-1} = (BU)D$ and BU, we get the basis $\{\mathbf{v}_1, \mathbf{v}_2\}$ of the hexagonal lattice, $\mathbf{v}_1 = (0, \sqrt{3})$, $\mathbf{v}_2 = (-\frac{1}{2}, \frac{\sqrt{3}}{2})$ and the basis $\{\mathbf{w}_1, \mathbf{w}_2\}$, $\mathbf{w}_1 = 2\mathbf{v}_1$, $\mathbf{w}_2 = 8\mathbf{v}_1$ for the lattice Λ_2.

For a nested pair $\Lambda' \subseteq \Lambda$ with generator matrices B and BM, the diagonal matrix of the Smith normal form of M also classifies the abelian quotient group $\frac{\Lambda}{\Lambda'}$, and this will be used in Chap. 5 to describe spherical codes.

2.3 The Dual of a Lattice

The dual of a lattice plays an important role in understanding its structure.

Definition 2.12 The *dual* lattice of a lattice Λ is by definition

$$\Lambda^* = \{\mathbf{y} \in \mathbb{R}^n \mid \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \text{ for all } \mathbf{x} \in \Lambda\}. \tag{2.16}$$

Dual lattices are sometimes called *polar* or *reciprocal* and arise in areas as distinct as crystallography, cryptography, and harmonic analysis. To understand geometrically the notion of dual, let us start with a full rank lattice $\Lambda \subset \mathbb{R}^2$ generated by the vectors $(b_{11}, b_{21}), (b_{12}, b_{22})$. From the definition, the scalar product between any vector of the dual and the original lattice must be an integer. In fact, it is enough to ensure this for the basis vectors, since lattice points are obtained by integral linear combinations. Given $i \in \mathbb{Z}$, the set of vectors

$$H_1^{(i)} = \left\{(x_1, x_2) \in \mathbb{R}^2 \mid \langle (x_1, x_2), (b_{11}, b_{21}) \rangle = x_1 b_{11} + x_2 b_{21} = i\right\}.$$

is a straight line in $\mathbb{R}^2$. By changing $i \in \mathbb{Z}$, we obtain a set of parallel straight lines. Now imposing the same condition for the second basis vector, we have the set of parallel straight lines

$$H_2^{(j)} = \left\{(x_1, x_2) \in \mathbb{R}^2 \mid \langle (x_1, x_2), (b_{12}, b_{22}) \rangle = x_1 b_{12} + x_2 b_{22} = j\right\},$$

$j \in \mathbb{Z}$. Each straight line $H_1^{(i)}$ intersects $H_2^{(j)}$ in precisely one point. The union of all these points is Λ^* (see Fig. 2.14). The same interpretation holds in $\mathbb{R}^n$. For each basis vector $\mathbf{b}_k$, we have a set of parallel hyperplanes $H_k^{(j)}$, $j \in \mathbb{Z}$. The distance between each pair of consecutive hyperplanes H_k^j and H_k^{j+1} is $1/\|\mathbf{b}_k\|$. Indeed, if $\mathbf{x}$ belongs to H_k^j, then $\mathbf{x} + \mathbf{b}_k/\|\mathbf{b}_k\|^2$ belongs to H_k^{j+1}. The distance between these points is precisely the distance between the hyperplanes, namely, $1/\|\mathbf{b}_k\|$.

Example 2.13 The lattice $\mathbb{Z}^n$ is equal to its dual.

Example 2.14 Consider the hexagonal lattice, generated by $(1, 0), (1/2, \sqrt{3}/2)$. A point in its dual has to satisfy

$$\langle (x_1, x_2), (1, 0) \rangle = x_1 = l_1 \in \mathbb{Z} \text{ and}$$

$$\left\langle (x_1, x_2), \left(\tfrac{1}{2}, \tfrac{\sqrt{3}}{2}\right) \right\rangle = \frac{x_1}{2} + \frac{\sqrt{3}x_2}{2} = l_2 \in \mathbb{Z}.$$

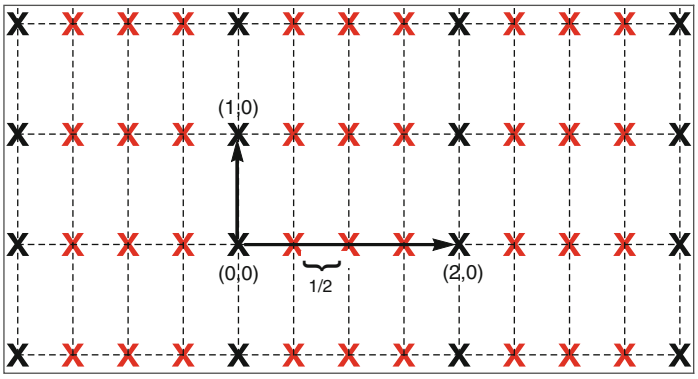


Fig. 2.14 A lattice with basis $\{\mathbf{b}_1, \mathbf{b}_2\} = \{(2,0),(0,1)\}$ and its dual, which has basis $\{\mathbf{b}_1^*, \mathbf{b}_2^*\} = \{(1/2,0),(0,1)\}$

Solving the equations for (x_1, x_2), we conclude that a point in the dual has the form $(x_1, x_2) = (l_1, (2l_2 - l_1)/\sqrt{3})$, $l_1, l_2 \in \mathbb{Z}$. In other words, the dual is a two-dimensional lattice generated by the vectors $(1, -1/\sqrt{3}), (0, 2/\sqrt{3})$. Notice that this lattice is equivalent to the hexagonal itself. See Exercise 2.10.

In general, calculating the dual lattice from the definition, as in Example 2.14, may not be worthwhile. In what follows, we summarize relations to get the parameters of Λ^* in a simple way (see [26, p.11] for (1)–(3) and Exercise 2.6 for (4)).

1 If B is a generator matrix for Λ, then $(B^T)^{-1}$ is a generator matrix for Λ^*.
2 In the same way, if G is a Gram matrix for Λ, G^{-1} is a Gram matrix for Λ^*.
3 $V(\Lambda^*) = V(\Lambda)^{-1}$.
4 If $\Lambda_1 \sim \Lambda_2$, then $\Lambda_1^* \sim \Lambda_2^*$.

Definition 2.13 We say that Λ is *integral* if it has a Gram matrix with integer entries. Note that this condition is equivalent to saying that the inner product between any two lattice vectors is an integer or that $\Lambda \subseteq \Lambda^*$.
In fact, for integer lattices we have $\Lambda \subseteq \Lambda^* \subseteq (\frac{1}{V(\Lambda)^2})\Lambda$.

Definition 2.14 If $\Lambda = \Lambda^*$, we say that Λ is *unimodular*, and this means that any of its Gram matrices is unimodular.

2.4 Important Lattices and Their Duals

Important lattices are lattices which have exceptional structures and typically are often encountered in the literature. This subsection provides a summarized description with parameters of well-known lattices, some of which will appear

Table 2.1 Relevant parameters for a lattice Λ in $\mathbb{R}^n$ with generator matrix B

Notation	Name	Reference
$\mathscr{P}(B)$	Fundamental parallelotope	(2.5)
$V(\Lambda) = \sqrt{\det(BB^T)}$	Volume	(2.6)
$\mathscr{V}(\Lambda)$	Voronoi region	(2.9)
$\mathscr{B}^n(1)$	Ball of radius 1 around the origin	(2.11)
$\lambda = \min_{\mathbf{x}\in\Lambda,\mathbf{x}\neq\mathbf{0}} \|\|\mathbf{x}\|\|$	Minimum norm (distance)	(2.10)
$\rho = \lambda/2$	Packing radius	(2.12)
$\Delta(\Lambda)$	Packing density	(2.13)
$\delta(\Lambda) = \rho^n/V(\Lambda)$	Center density	Def. 2.7
μ	Covering radius	Def. 2.9
$\theta(\Lambda)$	Covering density	(2.15)

in Table 2.4, which contains "record" lattices. Many more details regarding these lattices as well as other special types of lattices are found in [26, Chap. 4]. We recall the lattice parameters and related concepts that we have introduced so far in Table 2.1.

The Cubic Lattice $\mathbb{Z}^n$

This lattice is unimodular, $(\mathbb{Z}^n)^* = \mathbb{Z}^n$ It has minimum distance $\min_{\mathbf{x}\in\mathbb{Z}^n,\mathbf{x}\neq\mathbf{0}} ||\mathbf{x}|| = 1$, packing radius $\rho = 1/2$, covering radius $\sqrt{n}/2$ (a typical deep hole is $(1/2,\ldots,1/2)$) and kissing number $2n$. Its Voronoi region is a cube, its packing density is $\frac{\text{vol } \mathscr{B}^n(1)}{2^n}$, and its covering density $n^{\frac{n}{2}} \frac{\text{vol } \mathscr{B}^n(1)}{2^n}$.

The Lattice D_n

The checkerboard lattice D_n is defined in Example 2.4 as the full rank sublattice of $\mathbb{Z}^n$ where the sum of coordinates is even. As such, it has for basis $\{\mathbf{v}_1,\ldots,\mathbf{v}_n\}$ with $\mathbf{v}_1 = (-1,-1,0,\ldots,0)$, $\mathbf{v}_2 = (1,-1,0,\ldots,0)$, $\mathbf{v}_3 = (0,1,-1,0,\ldots,0)$, and $\ldots,\mathbf{v}_n = (0,0,\ldots,0,1,-1)$. Its minimum distance is $\sqrt{2}$, its volume is $V(D_n) = 2$ $(\det(D_n) = 4)$, its center density is $\delta(D_n) = 2^{-\frac{n}{2}-2}$, its kissing number is $2n(n-1)$, its covering radius is $\mu = 1$, for $n = 3$, and $\mu = \sqrt{\frac{n}{4}}$, for $n \geq 4$. As it can be seen in Table 2.4, D_n has the greatest lattice packing density in $\mathbb{R}^n$ for $n = 3$ (FCC), 4 and 5. The dual D_n^* has minimum distance $\frac{\sqrt{3}}{2}$, for $n = 3$, and 1, for $n \geq 4$.

The Lattice A_n

This lattice, defined in Example 2.3, is a rank-n sublattice of $\mathbb{Z}^{n+1}$ lying in the hyperplane H where the sum of the coordinates is zero $(A_n \subset D_{n+1} \subset \mathbb{Z}^{n+1})$. It has for basis $\{\mathbf{v}_1,\ldots,\mathbf{v}_n\}$ given by $\mathbf{v}_1 = (-1,1,0,\ldots,0)$, $\mathbf{v}_2 = (0,-1,1,0,\ldots,0)$, $\mathbf{v}_3 = (0,0,-1,1,0,\ldots,0),\ldots,\mathbf{v}_n = (0,0,\ldots,0,-1,1)$. If we consider the $(n+1)\times n$ generator matrix B whose columns are these basis vectors, we can see that its volume is $V(A_n) = (\det(B^TB))^{\frac{1}{2}} = n+1$. It has minimum distance $\sqrt{2}$ (minimum distance vectors are in fact given by permuting all the components of $\mathbf{v}_1$), center packing density $\delta = 2^{\frac{-n}{2}}(n+1)^{\frac{-1}{2}}$, kissing number $n(n+1)$, and covering radius $\mu = \frac{\sqrt{2}}{2}(\frac{2a(n+1-a)}{n+1})^{\frac{1}{2}}$, where $a = [(n+1)/2]$ is the integer part of $(n+1)/2$.

As mentioned in Example 2.9, A_2 is equivalent to the hexagonal lattice. Also A_3 is equivalent the lattice D_3 or the FCC lattice (see Exercise 2.7). Both A_2 and A_3 are the densest lattices in their dimensions. The dual lattice A_n^*, considered in the hyperplane H, has a very special Voronoi region given by the permutohedra with vertices being all the permutations of $\frac{1}{(n+1)}(-n, -n+2, -n+4, \ldots, n-2, n)$. As seen in Table 2.4, the lattices A_n^* have the smallest covering density known in several dimensions including dimensions $n = 3$ ($A_n^* = D_n^*$ =BCC), $n = 4, 5$, and $9 \leq n \leq 23$. For $n = 6,7$, and 8, the covering densities of A_n^* are 2.551, 3.060, and 3.666, respectively, and these densities were known to be the smallest in their dimensions until the results of [90] displayed in Table 2.4.

The Lattices E_6, E_7, and E_8

Also called the Gosset lattice after T. Gosset who was one of the first to study its geometry, the lattice E_8 is defined as

$$E_8 = \left\{ \mathbf{x} = (x_1, \ldots, x_8) \in \mathbb{Z}^8 : \mathbf{x} \in D_8 \text{ or } \mathbf{x} + \left(\frac{1}{2}, \ldots, \frac{1}{2}\right) \in D_8 \right\}. \tag{2.17}$$

A generator matrix for E_8 is given by

$$\begin{bmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{bmatrix}.$$

The lattice E_8 has minimum distance $\sqrt{2}$ and packing center density $\frac{1}{16}$ and is, up to congruence, the unique lattice in $\mathbb{R}^8$ with these minimum distance and density. It is a unimodular lattice, $E_8^* = E_8$. It is also known to be the unique (up to congruence) unimodular lattice in dimension 8 with even squared minimum distance. (In fact, up to dimension 8, the unique unimodular lattices, up to congruence, are $\mathbb{Z}^n$ and E_8 [26, Chap. 4].) The lattice E_8 has the greatest packing density in dimension 8 not only among lattices but for any *packing* [26, 98]. It has also the smallest known covering density in this dimension. Its name derives from its association with the E_8 root system (see [26, Chap. 4]).

The lattices E_7 and E_6 are lattices of ranks 7 and 6 naturally defined in $\mathbb{R}^8$ as

$$E_7 = \{\mathbf{x} = (x_1, \ldots, x_8) \in E_8 : x_1 = x_2\}, \tag{2.18}$$

$$E_6 = \{\mathbf{x} = (x_1, \ldots, x_8) \in E_8 : x_1 = x_2 = x_3\}. \tag{2.19}$$

Table 2.2 A generator matrix for the Barnes-Wall lattice

$$\left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}
4&2&2&2&2&2&2&2&2&2&2&1&0&0&0&1\\
0&2&0&0&0&0&0&0&0&0&0&1&1&0&0&1\\
0&0&2&0&0&0&0&0&0&0&0&1&1&1&0&1\\
0&0&0&2&0&0&0&0&0&0&0&1&1&1&1&1\\
0&0&0&0&2&0&0&0&0&0&0&0&1&1&1&1\\
0&0&0&0&0&2&0&0&0&0&0&1&0&1&1&1\\
0&0&0&0&0&0&2&0&0&0&0&0&1&0&1&1\\
0&0&0&0&0&0&0&2&0&0&0&1&0&1&0&1\\
0&0&0&0&0&0&0&0&2&0&0&1&1&0&1&1\\
0&0&0&0&0&0&0&0&0&2&0&0&1&1&0&1\\
0&0&0&0&0&0&0&0&0&0&2&0&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{bmatrix}$$

They can be considered as lattices in $\mathbb{R}^7$ and $\mathbb{R}^8$ and they are known to have the best lattice packing density in their dimensions.

The Barnes-Wall Lattice Λ_{16}

The so-called Barnes-Wall lattices BW_n defined in dimensions $n = 2^k$, k an integer greater than two, were introduced in [8] and have been constructed since then through several different methods, e.g., via the so-called Construction B from Reed-Muller codes [26]. They have some special properties (see [77]). $\Lambda_{16} = BW_{16}$ has the best known packing density in dimension 16. One of its generator matrices is given in Table 2.2.

The Leech Lattice Λ_{24}

The Leech lattice Λ_{24}, introduced by J. Leech in 1964, is a very special full rank lattice in $\mathbb{R}^{24}$. It is unimodular, $\Lambda_{24} = \Lambda_{24}^*$, has the greatest packing density in dimension 24, even considering non-lattice packings, and has the smallest known covering density in this dimension. Its kissing number is 196,560. There are many different constructions for this lattice (see [26, Chap. 24]). A generator matrix of the scaled version of the Leech lattice, $2\sqrt{2}\Lambda_{24}$, is given in Table 2.3.

2.4.1 Table of Record Lattices

In Table 2.4 below, the best known lattices (records) are found with respect to packing density, kissing number, and covering density, but also quantization (or more precisely, the normalized second moment (2.25)), to be approached in Sect. 2.5.1 [26, 90].

The marked boxes (†) display the lattices which were proved to be the best regarding the respective parameter among all the lattices in that dimension. The

Table 2.3 A generator for the Leech lattice Λ_{24} scaled by $2\sqrt{2}$

$$\begin{bmatrix}
8&4&4&4&4&4&4&2&4&4&4&2&4&2&2&2&4&2&2&2&0&0&0&-3\\
0&4&0&0&0&0&0&2&0&0&0&2&0&2&0&0&0&0&0&2&2&0&0&1\\
0&0&4&0&0&0&0&2&0&0&0&2&0&0&2&0&0&2&0&0&2&0&0&1\\
0&0&0&4&0&0&0&2&0&0&0&2&0&0&0&2&0&0&2&0&2&0&0&1\\
0&0&0&0&4&0&0&2&0&0&0&0&0&2&2&2&0&2&2&2&2&0&0&1\\
0&0&0&0&0&4&0&2&0&0&0&0&0&2&0&0&0&0&2&0&0&0&0&1\\
0&0&0&0&0&0&4&2&0&0&0&0&0&0&2&0&0&0&0&2&0&0&0&1\\
0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&2&0&2&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&4&0&0&2&0&2&2&2&0&2&2&2&2&2&2&1\\
0&0&0&0&0&0&0&0&0&4&0&2&0&2&0&0&0&2&0&0&0&2&0&1\\
0&0&0&0&0&0&0&0&0&0&4&2&0&0&2&0&0&0&2&0&0&0&2&1\\
0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&2&0&0&0&2&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&4&2&2&2&0&0&0&0&2&2&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&2&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&2&2&2&2&2&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&2&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&2&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{bmatrix}$$

lattices A_2, $A_3 \sim D_3 \sim FCC$, E_8, and Λ_{24} were proved to have the best packing density in their dimensions among all packings (not only lattice packings).

It was long believed that A_6^* was the best 6-dimensional covering. Recently, Schurmann and Vallentin [90] have found over 40 lattices with smaller covering density than A_6^* along with the record covering in dimensions 7, 8. We denote the best known lattice coverings presented in [90] in dimensions $n = 6, 7, 8$ by Q_n^1.

Asymptotically, a theorem by Minkowski and Hlawka (cf [20]) guarantees that there exist packings with density lower bounded by $\Delta \geq \zeta(n)/2^{n-1}$, where $\zeta(n) = 1 + 1/2^n + 1/3^n + \ldots$ is the *Riemman zeta function*. Improving this lower bound is still an active subject of research.

Remark 2.4 The classical notations for the lattices A_n, D_n, and E_n used here come from the fact that those lattices are associated with root systems in the context of the theory of Lie algebras which are known by the same symbols [1, 14]. These lattices are then called *root lattices*. The symbol Λ_n is used for a *laminated lattice* [26, Chap. 6] in dimension n. This concept was introduced in [24] to describe a lattice in dimension n constructed from layers of a suitable lattice in dimension $n-1$ in order to get the best possible density, starting from the one-dimensional lattice of

Table 2.4 Best known (record) lattices with respect to packing density, kissing number, covering density, and quantization

Dim	Packing density	Kissing number	Covering density	Quantization
1	$\mathbb{Z}$ $1^{(\dagger)}$	$\mathbb{Z}$ $2^{(\dagger)}$	$\mathbb{Z}$ $1^{(\dagger)}$	$\mathbb{Z}$ $0.0833^{(\dagger)}$
2	A_2 $0.9069^{(\dagger)}$	A_2 $6^{(\dagger)}$	A_2 $1.2092^{(\dagger)}$	A_2 $0.0802^{(\dagger)}$
3	$A_3 \sim D_3$ $0.7450^{(\dagger)}$	A_3 $12^{(\dagger)}$	$A_3^* \sim D_3^*$ $1.4635^{(\dagger)}$	$A_3^* \sim D_3^*$ 0.0785
4	D_4 $0.6169^{(\dagger)}$	D_4 $24^{(\dagger)}$	A_4^* $1.7655^{(\dagger)}$	D_4 0.0766
5	D_5 $0.4653^{(\dagger)}$	D_5 $40^{(\dagger)}$	A_5^* $2.1243^{(\dagger)}$	D_5^* 0.0756
6	E_6 $0.3730^{(\dagger)}$	E_6 $72^{(\dagger)}$	Q_6^1 2.4648*	E_6^* 0.0742
7	E_7 $0.2953^{(\dagger)}$	E_7 $126^{(\dagger)}$	Q_7^1 2.9000	E_7^* 0.0731
8	E_8 $0.2537^{(\dagger)}$	E_8 $240^{(\dagger)}$	Q_8^1 3.2013	E_8 0.0717
16	Λ_{16} 0.0147	Λ_{16} 4320	A_{16}^* 15.3109	Λ_{16} 0.0683
24	Λ_{24} $0.0019^{(\dagger)}$	Λ_{24} $196560^{(\dagger)}$	Λ_{24} $7.9035^{(\dagger)}$	Λ_{24} 0.0657

even integer points and keeping the same minimum norm. We have that $\Lambda_1 \sim \mathbb{Z}$, $\Lambda_2 \sim A_2$, $\Lambda_k \sim D_k$ for $3 \leq k \leq 5$ and $\Lambda_k \sim E_k$ for $6 \leq k \leq 8$. We also have that the Barnes-Wall lattice and the Leech lattice are the unique laminated lattices in dimensions 16 and 24, respectively [26, Chap. 6].

2.5 Applications

2.5.1 Coding

Consider the transmission of a vector $\mathbf{x}$ belonging to a discrete set of points $S \subset \mathbb{R}^n$ over an additive white Gaussian noise (AWGN) channel, meaning that the received signal $\mathbf{y}$ is of the form

$$\mathbf{y} = \mathbf{x} + \mathbf{n} \tag{2.20}$$

where $\mathbf{n}$ is a random vector whose components are independent Gaussian random variables with mean 0 and variance σ^2. The *Gaussian channel coding* problem

consists of figuring out (decoding) $\mathbf{x}$ from $\mathbf{y}$ despite the presence of the noise $\mathbf{n}$. Now if the transmitter had an infinite power at its disposal, given σ^2, it would be easy enough to solve this coding problem: just take the set S, and scale all its vectors enough so that they are well apart, meaning that the distance between any two vectors in S is much larger than $2\sigma^2$. Then choose for the decoded point the lattice point $\mathbf{x}$ which is closest to the received point $\mathbf{y}$. However we do want the transmitter not to waste too much power in transmitting $\mathbf{x}$, which is modeled by a power constraint that all the points of S lie within a sphere of radius $\sqrt{nP}$ around the origin (P thus defines a power constraint). Suppose now that S is a subset carved from a lattice Λ. The receiver will make a correct decision to choose the closest lattice point $\mathbf{x}$ from $\mathbf{y}$ as the decoded point exactly if the noise vector $\mathbf{n}$ falls in the Voronoi region $\mathcal{V}_\Lambda(\mathbf{x})$ of $\mathbf{x}$ (see Fig. 2.15), an event of probability

$$\frac{1}{(\sigma\sqrt{2\pi})^n}\int_{\mathcal{V}(\Lambda)} e^{-||\mathbf{x}||^2/2\sigma^2}\mathrm{d}\mathbf{x}.$$

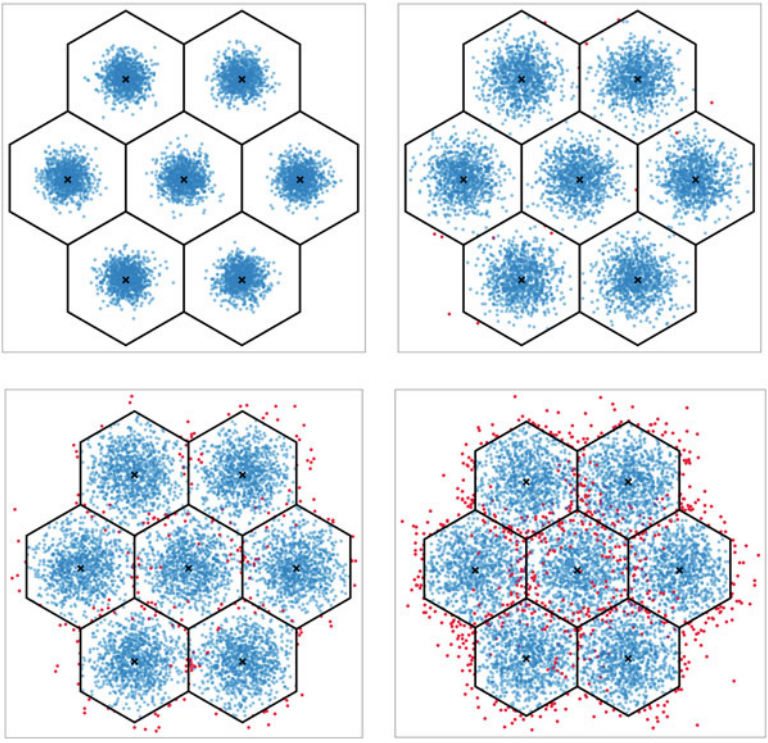


Fig. 2.15 Gaussian noise acting on a hexagonal lattice for $\sigma \in \{0.1, 0.15, 0.2, 0.25\}$. The blue (red) points correspond to received signals lying inside (outside) the Voronoi cell of the sent point

Thus if all points $\mathbf{x}$ are equally likely to be sent, the *error probability* P_e for S of decoding a lattice point $\hat{\mathbf{x}} \neq \mathbf{x}$ when $\mathbf{x}$ is sent is 1 minus the above probability. We thus want to find, given σ, the n-dimensional lattice of volume normalized to 1 for which the error probability P_e is minimized. Unfortunately, the above expression is hard to compute in a closed-form expression. It is thus usual to bound it using the so-called *union bound*.

For the sake of reasoning, suppose that the lattice Λ contains the vector $(1, 0, 0 \ldots, 0)$ and we want to decide whether $\mathbf{n}$ is closer to $(1, 0, \ldots, 0)$ than to the origin; this is equivalent to checking whether the first component of $\mathbf{n}$ is greater than $1/2$, an event that has probability

$$\frac{1}{\sigma\sqrt{2\pi}} \int_{1/2}^{\infty} e^{-x^2/2\sigma^2} \mathrm{d}x \leq \frac{1}{2} e^{-1/8\sigma^2}.$$

This reasoning generalizes to any lattice/lattice point. The probability that $\mathbf{n}$ is closer to some lattice point of norm m is bounded by (see Exercise 2.9) $(1/2)e^{-m^2/8\sigma^2}$. Therefore, the probability of an error event is given by

$$P(\mathbf{n} \text{ is closer to some } \mathbf{x} \in \Lambda \text{ than the origin}) \leq \frac{1}{2} \sum_{\mathbf{x} \in \Lambda \setminus \{0\}} e^{-\|\mathbf{x}\|^2/8\sigma^2}. \tag{2.21}$$

The dominant terms in the sum in the right-hand side of (2.21) are the ones corresponding to vectors with small norms. Therefore, dropping all terms except the ones of minimum norm, the upper bound can be approximated by

$$\frac{\kappa e^{-\rho^2/2}}{2}, \tag{2.22}$$

where we recall that ρ is the *packing radius* and κ denotes the *kissing number* of Λ. This expression is minimized if ρ is maximized (a "secondary" objective is that κ is minimized). Intuitively, we expect the number of points in S to be close to the ratio between the volume of a sphere of radius $\sqrt{nP}$ and the volume of Λ, i.e., $\mathrm{vol}\, \mathscr{B}^n(1)(nP)^n / V(\Lambda)$. Recalling the formula for the density and the approximation $|S| \approx \mathrm{vol}\, \mathscr{B}^n(\sqrt{n}P)/V(\Lambda)$, we can write expression (2.22) for the probability of error as

$$\frac{\kappa e^{-\Delta^{2/n}|S|^{-2/n}}}{2} \tag{2.23}$$

where Δ is the packing density. Therefore, for a fixed number of points, the objective of *minimizing the probability of error (or maximizing the probability of correct decision) can be achieved by maximizing the packing density of the underlying lattice*.

2.5.2 Quantization

Another important application where lattices play an important role is *quantization*. Suppose we want to represent the set of real numbers $\mathbb{R}$ by using finite precision arithmetics and a regular spaced grid. We can assume, up to scaling, that our approximation is going to be performed using the set of integers $\mathbb{Z}$. For each point $y \in \mathbb{R}$, the closest integer is denoted by $Q_{\mathbb{Z}}(y) = [y]$, and the squared error obtained in this approximation is $(Q_{\mathbb{Z}}(y) - y)^2$. Notice that for any point $y \in [-1/2, 1/2)$ (or $(-1/2, 1/2]$, depending on the rounding rule), $Q_{\mathbb{Z}}(y) = 0$ and the quantization error is y^2. Since the integers are regularly spaced, we define the *average* squared quantization error in the process by picking a point $y \in (-1/2, 1/2]$ uniformly at random and taking the average

$$\int_{-1/2}^{1/2} y^2 \mathrm{d}x = \frac{1}{12}.$$

This process can be extended by using extra dimensions to reduce the quantization error. Given a point $\mathbf{x} \in \mathbb{R}^n$ and a lattice $\Lambda \subset \mathbb{R}^n$, we define $Q_\Lambda(\mathbf{x})$ as the closest lattice point[3] to $\mathbf{y}$. Equivalently $Q_\Lambda(\mathbf{y}) = \mathbf{x}$ if and only if $\mathbf{y} \in \mathcal{V}_\Lambda(\mathbf{x})$.

Observe that $\mathbf{y} - Q_\Lambda(\mathbf{y})$ is closer to the origin than any non-zero lattice point, therefore $\mathbf{y} - Q_\Lambda(\mathbf{y}) \in \mathcal{V}_\Lambda(\mathbf{0})$ for any $\mathbf{y} \in \mathbb{R}^n$. Hence, subtracting the closest lattice point from $\mathbf{y}$ wraps the real vector $\mathbf{y}$ into the Voronoi region $\mathcal{V}_\Lambda(\mathbf{0})$ at the origin. This operation, called the *modulo-Λ* function, is denoted as

$$\mathbf{y} \bmod \Lambda = \mathbf{y} - Q_\Lambda(\mathbf{y}).$$

The modulo-Λ operation satisfies the property

$$(\mathbf{y}_1 + \mathbf{y}_2) \bmod \Lambda = (\mathbf{y}_1 \bmod \Lambda + \mathbf{y}_2) \bmod \Lambda \text{ for any } \mathbf{y}_1, \mathbf{y}_2 \in \mathbb{R}^n.$$

The modulo-Λ operation will be discussed more carefully and applied in Chap. 6. Analogous to the one-dimensional case, we define, for a point $\mathbf{x}$ drawn uniformly at random in the Voronoi cell of Λ, the average quantization error

$$E(\Lambda) = \frac{1}{V(\Lambda)} \int_{\mathcal{V}(\Lambda)} \|\mathbf{x}\|^2 \, \mathrm{d}\mathbf{x}, \tag{2.24}$$

[3] Strictly speaking, there might be more than one closest vector to $\mathbf{y}$, which might cause ambiguities. In order for $Q_\Lambda(\mathbf{y})$ to be well defined, one has to break the ties, i.e., to decide which "faces" of the Voronoi cell to use. In order to simplify notation, we will avoid such a technicality and consider that ties are broken according to some well-defined systematic rule. Considering this rule we will also, by abuse of notation, sometimes say "the" closest lattice point to $\mathbf{y}$. Notice that the faces of the Voronoi cell (i.e., the ambiguous points) have measure zero in $\mathbb{R}^n$.

where we use the subscript E_Λ to indicate that the expectation is with respect to a point uniformly distributed over the Voronoi region of Λ. Equation (2.24) gives the average mean squared quantization error, but is not the best choice to compare different lattices, since it does depend on the volume of Λ. For instance, for any scaling factor $\alpha\Lambda$, the quantization error is

$$E(\alpha\Lambda) = \alpha^2 E(\Lambda).$$

To allow a fair comparison between lattices with distinct volumes, we define the normalized second moment per dimension as

$$G(\Lambda) = \frac{1}{nV(\Lambda)^{2/n+1}} \int_{\mathcal{V}(\Lambda)} \|\mathbf{x}\|^2 \, \mathrm{d}\mathbf{x}. \tag{2.25}$$

This quantity is independent of the volume and of the dimension (Exercise 2.13) but is fairly hard to calculate in general, as it involves an integration over the Voronoi cell of a lattice. Equation (2.25) was used to calculate the last column of Table 2.1.

Best Quantizers How small can the normalized second moment be? For a given volume $V(\Lambda) = V$, the integral in Eq. (2.25) is lower bounded by the integral over an n-dimensional ball of volume V. This gives the bound $G(\Lambda) > 1/(2\pi e) \sim 0.059$ (e.g., [23]). The best lattices in terms of quantization are therefore, roughly speaking, the ones whose Voronoi cell resembles a ball.

Comparing with Table 2.1, it can be seen that, as the dimension increases, the best normalized second moment decreases. In fact, the ratio between the second moment of the one-dimensional lattice $\mathbb{Z}$ and the best possible quantizer is only[4] 1.42 and can be approached in very high dimensions. This ratio may be interpreted as the gain of using a good high-dimensional lattice over the simple quantizer that only rounds the coordinate of a vector in each dimension. Explicit constructions of lattices exhibiting the full gain are very challenging and not yet known.

2.5.3 Computational Problems and Cryptography

The parameters introduced so far, such as the minimum norm, the packing radius, or the center density, have a clean mathematical formulation, and lattices with record parameters according to them have been listed in Table 2.4 for dimensions up to 8, 16, and 24. Computing these parameters in higher dimensions becomes a computational problem. How easy is it algorithmically to compute, say the density of a given lattice? The answer is that it is usually hard. The main difficulty lies in the fact that calculating the density depends on knowing the packing radius (or

[4] Or approximately 1.53, in decibels. This number is sometimes referred to as the ultimate *shaping gain* of a lattice.

equivalently, the minimum norm (2.10)) of a lattice which, in turn, depends on the description of the given lattice Λ.

For a concrete example, let us consider the hexagonal lattice (Example 2.1). Consider the basis

$$B = \begin{bmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{bmatrix}.$$

Each vector in the lattice has the form $B\mathbf{u}$, $\mathbf{u} \in \mathbb{Z}^2$, and has norm $u_1^2 + u_1u_2 + u_2^2$. Since u_1, u_2 are integers, it follows that the minimum norm is 1, attained, for instance, by choosing $u_1 = 1, u_2 = 0$. However, if we are given instead the generator matrix

$$\overline{B} = \begin{bmatrix} 2401 & 96\sqrt{32} \\ 57649/2 & 2305\sqrt{3}/2 \end{bmatrix},$$

it is far from easy to compute that the minimum non-zero squared norm for $5792449u_1^2 + 139079089u_2u_1 + 834836569u_2^2$ is 1, attained by $u_1 = 2305$ and $u_2 = -192$. In fact, if we knew the unimodular transformation that takes B into $\overline{B}$, we could easily recover the minimum from the first basis. This tells us that, in some sense, it is easy to "hide" the minimum norm of a vector by transforming a "good" basis into a "bad one." This high-level idea is the starting point for the constructions of cryptographic primitives based on lattices (the case of public-key cryptography will be explained in more details below). The following problem is known as SVP (**S**hortest **V**ector **P**roblem):

Problem 2.1 (SVP) Given a matrix B, find the minimum norm of the lattice Λ generated by B.
A related problem is the following, known as CVP (**C**losest **V**ector **P**roblem).

Problem 2.2 (CVP) Given a generator matrix B for a lattice $\Lambda \subset \mathbb{R}^n$ and a vector $\mathbf{y} \in \mathbb{R}^n$, find the closest lattice point to $\mathbf{y}$.

This problem is relevant to coding theory, as it can be regarded as a "decoding problem," where $\mathbf{y}$ is a received signal for a message $\mathbf{x} \in \Lambda$ transmitted over a Gaussian channel, as in the previous section. CVP also depends critically on the given basis B. Suppose we start with the lattice $\mathbb{Z}^2$ and the matrix B associated with the canonical basis. Given a point $\mathbf{y} = (y_1, y_2)$, the closest point $\mathbf{x} = B\mathbf{u}$ to $\mathbf{y}$ is the one that minimizes

$$\|\mathbf{y} - \mathbf{x}\| = (y_1 - u_1)^2 + (y_2 - u_2)^2,$$

obtained by rounding the coordinates of $\mathbf{y}_1$, i.e., $u_1 = [y_1]$ and $u_2 = [y_2]$. One can think of a generalization of this algorithm for any generator matrix $\overline{B}$ as follows. First solve the system of equations $\mathbf{y} = \overline{B}\mathbf{u}$, and then round the solution, outputting the point $\mathbf{x} = \overline{B}[\mathbf{u}]$ (this is sometimes known as the Babai point, after the Hungarian mathematician Laszlo Babai). Unfortunately, even for the lattice $\mathbb{Z}^2$, depending on

the basis, this procedure may fall short of any reasonable estimate, as discussed in Exercise 2.12. In general finding the closest vector point to a given lattice basis is, in computational complexity language, an NP-hard problem [72]. This problem is closely related to the quantization problem in Sect. 2.5.1. In fact, in both cases we want to find the closest vector to a given lattice point. However the main difference lies in the fact that, from a complexity perspective, algorithms that solve CVP for *any* generator matrix (or for a large enough class) are sought, whereas from a coding theory perspective, we want to *design* a lattice with an easy CVP solver.

The two problems CVP and SVP, and their many variants, have been employed for cryptographic purposes since 1996 [3]. We provide next a general idea of how *public-key cryptography* can be performed using lattices. Suppose a user (usually called Alice in the cryptography literature) has access to a "good" generator matrix B for a high-dimensional lattice $\Lambda \subset \mathbb{R}^n$. From B, Alice generates a "bad" basis H and makes H publicly available while keeping B secret. Now anyone (say, Bob) with access to H can send an encrypted message $\mathbf{u} \in \mathbb{Z}^n$ as follows. Bob generates a noise vector $\mathbf{n}$ and sends the vector $\mathbf{y} = H\mathbf{u} + \mathbf{n}$ to Alice. Noticing that $\mathbf{x} = B\mathbf{u}$ is a lattice point, if $\mathbf{n}$ is "small" enough, Alice can recover $\mathbf{x}$ by finding the closest lattice point to $\mathbf{y}$. Roughly speaking, a "good" basis is one such that the (very efficient) rounding procedure explained in the previous paragraph will work, whereas for "bad" basis it is hard to guess the correct vector $\mathbf{x}$ (for instance, the rounding procedure will output a vector far from $\mathbf{x}$, as in Exercise 2.12). Therefore, an intruder that intercepts $\mathbf{y}$ and has access to H is not expected to efficiently guess the sent message $\mathbf{x}$.

Of course the above high-level description depends critically on how to choose the noise vector, the "good" and the "bad" basis or, in other words, the private-key B and the public-key H. For further information on this and on other applications of lattices to cryptography, the reader is referred to [73]. We close this section with a word on two relevant notions: special bases and bounds on the shortest vector.

Special Bases The rounding procedure described in this section is not sufficient to solve the closest vector problem and, depending on the chosen basis, may produce very crude estimates. To overcome this problem, we might want to preprocess the basis given to us before trying to find the closest lattice point $\mathbf{x}$ to a given point $\mathbf{y} \in \mathbb{R}^n$. For example, the best possible basis for the integer lattice $\mathbb{Z}^n$ in terms of complexity of finding the closest vector is the canonical basis. However not all lattices possess such a neat basis. Intuitively, a good basis for a lattice Λ is as close as possible from being "orthogonal," with small norm vectors. This notion has been quantified and formalized in several different ways. We present below the notion of Minkowski-reduced basis, arguably the most intuitive way of defining a "good" basis.

We say that a set of vectors $\{\mathbf{b}_1, \ldots, \mathbf{b}_i\} \subset \Lambda$ is *primitive* if it can be extended to a basis of Λ, i.e., if there exist $\{\mathbf{b}_{i+1}, \ldots, \mathbf{b}_n\}$ such that $\{\mathbf{b}_1, \ldots, \mathbf{b}_i, \mathbf{b}_{i+1}, \ldots, \mathbf{b}_n\}$ is a basis for Λ.

Definition 2.15 (Minkowski-Reduced Basis) A basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ for a lattice Λ is said to be *Minkowski-reduced if*:

(i) $\mathbf{b}_1$ *is a shortest vector in* Λ *and*

(ii) for any $i = 1, \ldots, n-1$, $\mathbf{b}_{i+1}$ *is a shortest vector in* Λ *such that* $\{\mathbf{b}_1, \ldots, \mathbf{b}_i, \mathbf{b}_{i+1}\}$ *is primitive.*

Given a basis $\alpha = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$, the above conditions (i) and (ii) will imply inequalities to be satisfied by its associated Gram matrix $G = \{b_{ij}\} = \langle \mathbf{b}_i, \mathbf{b}_j \rangle$ for this basis to be Minkowski-reduced. Some of these inequalities are [26, Chap. 15, 10.1]:

(A) $0 < b_{11} \leq b_{22} \leq \ldots \leq b_{nn}$
If $\mathbf{v} = \mathbf{b}_t - \sum_{s \in S} \epsilon_s \mathbf{b}_s$ (for some set S of subscripts $s < t$ and $\epsilon_s = \pm 1$), the inequality $\|\mathbf{b}_t\| \leq \|\mathbf{v}\|$ becomes

(B) $$2 \left| \sum_{s \in S} \epsilon_s b_{st} - \sum_{r,s \in S} \epsilon_r \epsilon_s b_{rs} \right| \leq \sum_{s \in S} b_{ss}.$$

For the cases $S = \{i\}$, $S = \{i, j\}$, and $S = \{i, j, k\}$, the above condition B can be written as:

(B1) $2 \left| b_{ij} \right| \leq b_{ii}$, $(i < j)$;
(B2) $2 \left| b_{ij} \pm b_{ik} \pm b_{jk} \right| \leq b_{ii} + b_{jj}$, $(i < j < k)$; and
(B3) $2 \left| \epsilon_1 b_{ir} + \epsilon_2 b_{jr} + \epsilon_3 b_{kr} - \epsilon_1 \epsilon_2 b_{ij} - \epsilon_1 \epsilon_3 b_{ik} - \epsilon_2 \epsilon_3 b_{jk} \right| \leq b_{ii} + b_{jj} + b_{kk}$, $(i < j < k < r)$

For $n = 2$, $n = 3$, and $n = 4$, the simultaneous conditions A and B1; A, B1, and B2; and A, B1, B2, and B3, respectively, are also sufficient to assure that the basis is Minkowski-reduced [26]. These characterizations can be used in Exercises 2.3 and 2.8. Note that condition B is related to the "more orthogonal" characteristic required for such bases. As it can be shown in Exercise 2.3, $\{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$ is a basis for the FCC lattice composed by vectors of minimum norm, but it is not Minkowski-reduced since condition B2 is not verified.

Any lattice has a Minkowski-reduced basis, but unfortunately, for high dimensions, there is no simple characterization, and producing such a basis is computationally hard. It entails, for instance, calculating the shortest vector and, therefore, should be at least as hard as solving SVP [2]. One widely used relaxation in the literature is the definition of LLL-reduced basis [73], which provides relatively small vectors and can be computed with fast algorithms. For a thorough formal complexity discussion on reduced bases and other computational aspects, the reader is referred to [73].

Minkowski Theorem If we were to search the shortest lattice vector to solve Problem 2.1 by looking at all points inside a ball, how large should the radius of this ball be? The following fundamental bound due to Minkowski gives a first approach to this question.

Theorem 2.4 *The minimum norm* λ *of a full rank lattice* $\Lambda \subset \mathbb{R}^n$ *satisfies*

$$\lambda \leq \sqrt{n} V(\Lambda)^{1/n}. \tag{2.26}$$

Before proving the theorem, we perform a quick sanity check. If Λ is scaled by $\alpha > 0$, then its minimum norm is also scaled by $\alpha > 0$, while its volume is scaled by α^n. The term $V(\alpha\Lambda)^{1/n} = \alpha V(\Lambda)^{1/n}$ then guarantees that the bound scales appropriately.

Proof From the expression for the density of Λ (2.13), we have

$$\Delta(\Lambda) = \frac{\text{vol}\,\mathscr{B}^n(\rho)}{V(\Lambda)} = \left(\frac{\lambda}{2}\right)^n \frac{\text{vol}\,\mathscr{B}^n(1)}{V(\Lambda)} \leq 1 \Rightarrow$$

$$\lambda \leq 2V(\Lambda)^{1/n}/\text{vol}\,\mathscr{B}^n(1)^{1/n}.$$

To finish the proof, we have to bound the volume of a unit ball. Notice that a maximal inscribed cube in the ball $\mathscr{B}^n(1)$ has diagonal length 2 and side length $2/\sqrt{n}$ (Exercise 2.11). In particular, we have the inclusion $[-1/\sqrt{n}, 1/\sqrt{n}]^n \subset \mathscr{B}^n(1)$, which implies the inequality

$$\text{vol}\,\mathscr{B}^n(1) \geq (2/\sqrt{n})^n.$$

□

A slightly tighter upper bound can be obtained by noticing that

$$(\text{vol}\,\mathscr{B}^n(1))^{1/n} \sim \sqrt{\frac{2\pi e}{n}} \tag{2.27}$$

in high dimensions (this follows from (2.14) and from Stirling's approximation for the factorial, e.g., [26]). The upper bound (2.26) can be far from tight, even for the simplest example $\Lambda = \mathbb{Z}^n$. However, the Minkowski-Hlawka *lower* bound briefly mentioned in Sect. 2.4.1, combined with (2.27), implies that there exist lattices with minimum norm at least $\sim V(\Lambda)^{1/n}\sqrt{n/2\pi e}$.

Remark 2.5 The ratio $\lambda^2/V(\Lambda)^{2/n}$ is called the Hermite parameter of Λ (and is of course, closely related to the packing density). The previous discussions show that the Hermite parameter of the densest n-dimensional lattice should grow linearly with n.

For the closest vector Problem 2.2, bounds of the same nature as that of Theorem 2.26 for the SVP are far more complicated. From the definition of the covering radius μ, the distance from any point to a closest lattice point should not exceed μ. However, there is no simple way of bounding μ. A very useful (nontrivial) bound is $\mu\lambda^* \leq n/2$; here λ^* is the minimum norm of Λ^*. A proof for this result is out of the scope of the book and can be found in [6].

Exercises

Exercise 2.1 Verify that the sets $\{(1,1),(-1,1)\}$ and $\{\{(2,0,0),(1,1,0),(1,0,1)\}$ in Example 2.4 are bases for D_2 and D_3, according to the definition of D_n.

Exercise 2.2 Show that an $m \times m$ matrix is unimodular (has integer entries and determinant 1 or -1) if and only if it has integer entries and is invertible and its inverse matrix has also integer entries. (Hint: Recall determinant properties and the expression for the inverse of a matrix in terms of its cofactors.)

Exercise 2.3 Show as a direct consequence of Theorem 1.2 that two full rank square matrices A and B generate the same lattice if and only if $B^{-1}A$ is a unimodular matrix and use this result to check if the sets $\alpha = \{(-1,-1,0),(1,-1,0),(0,1,-1)\}$ and $\beta = \{(1,1,0),(1,0,1),(0,1,1)\}$ are bases for the FCC lattice and if the set $\gamma = \{(1,-1,1),(1,1,-1),(1,1,1)\}$ is a basis for the BCC lattice (see Example 2.4). Show also (checking the conditions A, B1, and B2 just after Definition 2.15) that α and γ are Minkowski-reduced bases for these lattices but β is not.

Exercise 2.4

(a) Determine the Voronoi regions of the lattices in Examples 2.1, 2.2, and 2.5, and check with Fig. 2.5.
(b) Design the Voronoi region of the BCC and FCC lattices (Examples 2.3 and 2.4).

Exercise 2.5 Consider a full rank lattice Λ. Prove that a fundamental parallelotope $\mathscr{P}(B)$ of Λ tiles $\mathbb{R}^n$ by verifying (i) and (ii) (Eq. (2.7)).

Exercise 2.6 Prove that if $\Lambda_1 \sim \Lambda_2$, then $\Lambda_1^* \sim \Lambda_2^*$.

Exercise 2.7 Show that the lattice A_3 introduced in Example 2.3 is equivalent to the lattice D_3 from Example 2.4 (which is also the lattice *FCC*). You may use the technique of Example 2.9.

Exercise 2.8 This exercise explores several lattice concepts in dimension 2. Consider the lattice Λ in $\mathbb{R}^2$ generated by $\{(1,11),(2,18)\}$.

(a) Look for a "good" basis and find the minimum distance of the lattice. Is your basis a Minkowski-reduced one?
(b) Describe a fundamental parallelotope of your choice, the Voronoi region and another fundamental region.
(c) Find the packing and the covering radii, the kissing number, and the packing and covering densities of Λ.
(d) Find a rectangular sublattice Λ' of Λ and the coset classes of $\frac{\Lambda}{\Lambda'}$.
(e) Determine the dual lattice, Λ^*, and its relevant parameters.
(f) Illustrate the relation $\Lambda \subseteq \Lambda^* \subseteq (\frac{1}{V(\Lambda)^2})\Lambda$ (since Λ is an integer lattice). What lattice do you think is "better," in some sense, Λ or Λ'?

Exercise 2.9 Prove that the probability that $\mathbf{n}$ is closer to a point of norm m than to the origin is upper bounded by $(1/2)e^{-m^2/8\sigma^2}$.
(*Hint:* First show that the inner product $\langle \mathbf{n}, \mathbf{x} \rangle$ has normal distribution with variance $\|\mathbf{x}\|^2 \sigma^2$.)

Exercise 2.10 Show that the dual of the hexagonal lattice is equivalent to itself. Identify the associated rotation and scaling factor.

Exercise 2.11 A rectangle $\mathscr{R} \subset \mathbb{R}^n$ is a set of the form

$$\mathscr{R} = \{\mathbf{x} \in \mathbb{R}^n : x_i \in [a_i, b_i], i = 1, \ldots, n\} = [a_1, b_1] \times \ldots \times [a_n, b_n],$$

for integers $a_i < b_i$. The volume of a rectangle is $(b_1 - a_1) \times (b_2 - a_2) \times (b_n - a_n)$. Show that the rectangle with the smallest volume contained in $\mathscr{B}^n(1)$ is a *cube* with $a_i = -1/\sqrt{n}$ and $b_i = 1/\sqrt{n}$ (or any of its rotations).

Exercise 2.12 Let B be the matrix

$$\begin{bmatrix} 4390 & 133 \\ 439033 & 13301 \end{bmatrix}$$

and $\mathbf{y} = (1.3, -1.9)$.

(a) Using the matrix B and the rounding procedure described in Sect. 2.5.1, find an estimate for the closest point to the lattice generated by Λ.
(b) Check that the lattice generated by B is equal to $\mathbb{Z}^2$. Compare the solution to a) with the actual closest lattice point.

Exercise 2.13 The *cartesian product* between two full rank lattices $\Lambda_1 \subset \mathbb{R}^{n_1}$ and $\Lambda_2 \subset \mathbb{R}^{n_2}$ is defined as

$$\Lambda_1 \times \Lambda_2 = \{(x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}) \in \mathbb{R}^n : (x_1, \ldots, x_{n_1}) \in \Lambda_1 \text{ and } (y_1, \ldots, y_{n_2}) \in \Lambda_2\},$$

where $n = n_1 + n_2$. For instance, $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$. Show that, for any lattice $\Lambda \subset \mathbb{R}^n$:

a) The normalized second moment (2.25) of $\Lambda \times \Lambda$ equals $\mathscr{G}(\Lambda)$
b) For any lattice Λ, $\mathscr{G}(\alpha\Lambda) = \mathscr{G}(\Lambda)$.

Exercise 2.14 (*) Calculate $\mathscr{G}(A_2)$.
(*Hint:* Use the Voronoi cell computation of Exercise 2.4.)