Chapter 3
Lattices from Codes

3.1 Construction A

A natural way of constructing lattices is from error-correcting codes, using the so-called Construction A. It associates a lattice in $\mathbb{R}^n$ to a linear code in $\mathbb{Z}_q^n$ (the set $\mathbb{Z}_q$ of integers modulo q will be introduced next). Such lattices are also called q-ary lattices (or modulo-q lattices) and have several applications in information theory and cryptography. Lattice-based cryptographic schemes are usually built on q-ary lattices and are linked to the computational difficulty of the shortest and closest vector problems (SVP and CVP, defined respectively in Problems 2.1 and 2.2) in this class [73]. Regarding applications to information theory, Construction A is employed, for instance, in the development of good (capacity-achieving) codes for the Gaussian channel, for some channels with side information [111], as well as for wiretap coding.

The theory of error-correcting codes has been extensively developed (see, e.g., comprehensive books such as [53] and [66]). We will focus here on q-ary codes, that is, codes which have $\mathbb{Z}_q$ as their "alphabet," and provide a self-contained elementary introduction.

For $q \geq 2$ a positive integer, consider the set $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$ of integers modulo q, where $a \pmod q$ means for a given $a \in \mathbb{Z}$, the set of integers $a + bq$, $b \in \mathbb{Z}$, and by convention a is typically chosen to be between 0 and $q-1$. In this set, addition and multiplication modulo q are well defined. For example, in $\mathbb{Z}_5$, $3+4 = 2, 2\cdot 3 = 1$, and $-3 = 2$. There is a significant structural difference between $\mathbb{Z}_q$, where q is a composite number, and $\mathbb{Z}_p$, where p is a prime number. When q is a composite number, say $q = m_1 m_2$, $m_1, m_2 \neq 0$, then $\mathbb{Z}_q$ contains non-zero elements which are not invertible with respect to multiplication. For instance, m_1, m_2 are such elements. Indeed, if m_1 were invertible, then there would exist an element $a \in \mathbb{Z}_q$ such that $m_1 a = 1$, but then $m_2 m_1 a = m_2 = qa = 0$, a contradiction.When p

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_3

is a prime, such a behavior cannot happen and $\mathbb{Z}_p$ has a field structure, which $\mathbb{Z}_q$, $q = m_2 m_1$ does not have, and for this reason, we will use also the notation $\mathbb{F}_p$ to denote $\mathbb{Z}_p$ and emphasize this difference.

In the Cartesian product $\mathbb{Z}_q^n$, we consider the component-wise sum and multiplication modulo q. If $q = p$ is prime $\mathbb{Z}_p^n = \mathbb{F}_p^n$ is a vector space over the field $\mathbb{Z}_p = \mathbb{F}_p$, which does not hold if q is composite number. A linear code C in $\mathbb{Z}_q^n$ is by definition a subset which is an additive subgroup of $\mathbb{Z}_q^n$. Vectors in C are called codewords. Note that $\mathbf{0} \in C$, since it is the identity element of the group, that $\mathbf{a}, \mathbf{b} \in C$ implies $\mathbf{a} + \mathbf{b} \in C$ (this is the closure property for a group) and that $c\mathbf{a} \in C$ for $\mathbf{a} \in C$ and c any element of $\mathbb{Z}_q$: this is also a consequence of the closure property: $\underbrace{\mathbf{a} + \mathbf{a} + \ldots + \mathbf{a}}_{c \text{ times}} = c\mathbf{a} \in C$. As an example, $C = \{a(1,2), a \in \mathbb{Z}_5\} = \{(0,0), (1,2), (2,4), (3,1), (4,3)\}$ is a linear code in $\mathbb{Z}_5^2$. If $q = p$ is prime, a linear code is a subspace of dimension k of the vector space $\mathbb{Z}_p^n = \mathbb{F}_p^n$ (called an (n, k) code). In this last example, the code C is the subspace of $\mathbb{Z}_5^2$ of dimension 1 generated by the vector $(1, 2)$, and we use the notation $C = \langle (1,2) \rangle$.

Next we establish a connection between linear codes in $\mathbb{Z}_q^n$ and lattices. Let

$$\rho : \mathbb{Z} \to \mathbb{Z}_q = \{0, 1, \ldots, q-1\},\ x \mapsto x \ (\mathrm{mod} q),$$

be the map of reduction modulo q. Given $a \pmod q$, its pre-image $\rho^{-1}(a)$ is the set of integers that are mapped to a by ρ (see Fig. 3.1a), that is $\rho^{-1}(a) = \{a + bq,\ b \in \mathbb{Z}\}$.

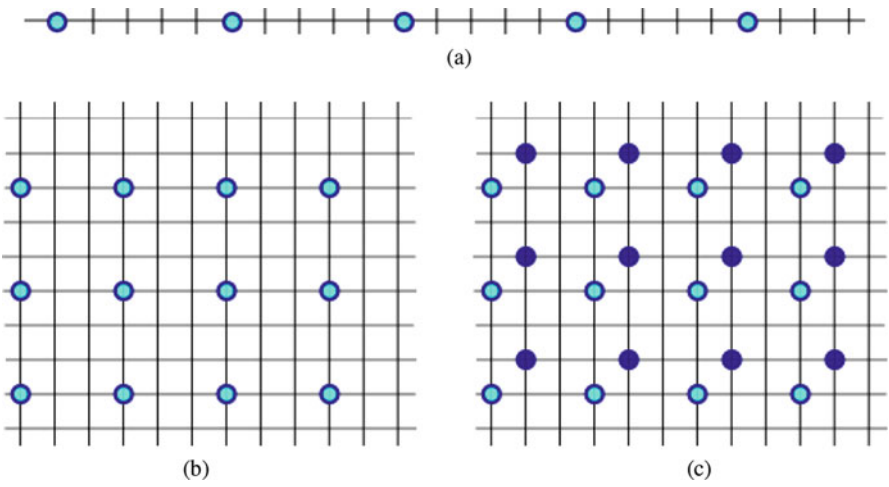

Fig. 3.1 Preimages $\rho^{-1}(S)$ for different sets S. (**a**) The pre-image $\rho^{-1}(a) \subset \mathbb{Z}$ of $a \pmod 5$. (**b**) The pre-image $\rho^{-1}((a_1, a_2)) \subset \mathbb{Z}^2$ of $(a_1 \pmod 3, a_2 \pmod 3)$. (**c**) The pre-image $\rho^{-1}(S) \subset \mathbb{Z}^2$ of $S = \{(a_1 \pmod 3, a_2 \pmod 3), (a_1 + 1 \pmod 3, a_2 + 1 \pmod 3)\}$

Now consider the Cartesian product of integers modulo q, namely, $\mathbb{Z}_q \times \mathbb{Z}_q$. An element in this set is a *two*-dimensional vector (a_1, a_2) of integers modulo q. Let

$$\rho : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_q \times \mathbb{Z}_q,\ (x_1, x_2) \mapsto (x_1 \ (\mathrm{mod} q), x_2 \ (\mathrm{mod} q)),$$

be the map of reduction modulo m component-wise. The pre-image $\rho^{-1}((a_1, a_2))$ is now the set of 2-dimensional vectors with integer entries that is mapped to a_1, a_2 by ρ (see Fig. 3.1b).

One could alternatively consider a set $S \subset \mathbb{Z}_q \times \mathbb{Z}_q$ and $\rho^{-1}(S)$, which is again the set of 2-dimensional vectors which are mapped to elements in S by ρ (see Fig. 3.1c for an example). Geometrically this inverse image spreads the set S from the inside of the $[0, q) \times [0, q)$ box into the plane.

The map ρ can be defined component-wise over an arbitrary number n of copies of $\mathbb{Z}_q$:

$$\rho : \mathbb{Z}^n \to \mathbb{Z}_q^n,\ \mathbf{x} \mapsto \rho(\mathbf{x})$$

by taking the reduction modulo q component-wise, over the n components of $\mathbf{x}$. Now one may take any arbitrary subset S of $\mathbb{Z}_q^n$ and compute $\rho^{-1}(S)$, but it is more interesting to start with S a subset that has a structure and to understand how this structure is carried over to $\rho^{-1}(S)$. We are next interested in $\rho^{-1}(S)$ where $S \subset \mathbb{Z}_q^n$ is a linear code.

We start with a result which relies on the additive group structure of $C \subset \mathbb{Z}_q^n$ and thus holds for any q.

Proposition 3.1 *Given a subset $S \subset \mathbb{Z}_q^n$, then $\rho^{-1}(S)$ is a lattice in $\mathbb{R}^n$ if and only if S is a linear code in $\mathbb{Z}_q^n$.*

Proof Suppose $S \subset \mathbb{Z}_q^n$ is a linear code. We need to check that $\rho^{-1}(C)$ is a discrete additive subgroup of $\mathbb{R}^n$ (Theorem 2.1). Since $\rho^{-1}(C) \subset \mathbb{Z}^n$, it is a discrete subset of $\mathbb{R}^n$. We next show that it is an additive subgroup.

Take $\mathbf{x}, \mathbf{y}$ two arbitrary vectors in $\rho^{-1}(C)$. To ensure closure under addition, their sum must belong to $\rho^{-1}(C)$. But $\mathbf{x} + \mathbf{y} \in \rho^{-1}(C)$ is equivalent to say that $\rho(\mathbf{x} + \mathbf{y})$ is a codeword in C. Now (in what follows q could be either prime or composite)

$$\begin{aligned}\rho(\mathbf{x} + \mathbf{y}) &= (x_1 + y_1 \ (\mathrm{mod}\ q), \ldots, x_n + y_n \ (\mathrm{mod}\ q)) \\ &= (x_1 \ (\mathrm{mod}\ q), \ldots, x_n \ (\mathrm{mod}\ q)) + (y_1 \ (\mathrm{mod}\ q), \ldots, y_n \ (\mathrm{mod}\ q)) \\ &= \rho(\mathbf{x}) + \rho(\mathbf{y}).\end{aligned}$$

Since $\mathbf{x}$ and $\mathbf{y}$ were chosen in $\rho^{-1}(C)$, this means that $\rho(\mathbf{x})$ and $\rho(\mathbf{y})$ are codewords, and since a code C is closed under addition, $\rho(\mathbf{x}) + \rho(\mathbf{y}) \in C$, thus $\rho(\mathbf{x} + \mathbf{y}) \in C$ as needed.

Since $\mathbf{0} \in C \in \mathbb{Z}_q^n$, $\mathbf{0} \in \rho^{-1}(C) \in \mathbb{Z}^n$.

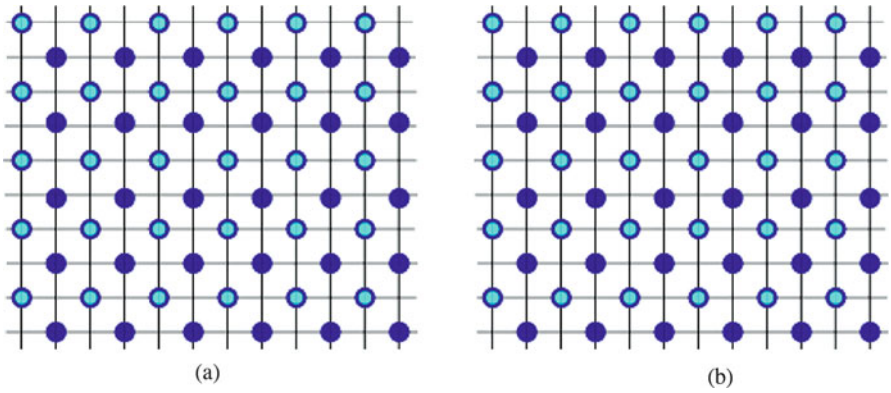

Fig. 3.2 Preimages $\rho^{-1}(S)$ for different sets S. (**a**) The pre-image $\rho^{-1}(S) \subset \mathbb{Z}^2$ of $S = \{(a_1 \pmod 3), a_2 \pmod 3), (a_1 + 1 \pmod 3), a_2 + 1 \pmod 3))\}$. (**b**) The pre-image $\rho^{-1}(C) \subset \mathbb{Z}^2$ of the linear binary code $C = \{(0,0),(1,1)\}$

We are left to check that $-\mathbf{x} \in \rho^{-1}(C)$ whenever $\mathbf{x} \in \rho^{-1}(C)$ or equivalently $\rho(-\mathbf{x}) \in C$ whenever $\rho(\mathbf{x}) \in C$. But

$$\rho(-\mathbf{x}) = (-x_1 \pmod q, \ldots, -x_n \pmod q) = -\rho(\mathbf{x}),$$

and it belongs to C since $c\mathbf{a} \in C$ for any scalar c (here $c = -1 \pmod q$).

The converse is left as an exercise (see Exercise 3.1), namely, to show that for $S \subset \mathbb{Z}_q^n$, if $\rho^{-1}(S)$ is a lattice in $\mathbb{R}^n$, then S is a linear code.

This proposition is illustrated in Fig. 3.2b. Take $C = \{(0,0),(1,1)\}$ over $\mathbb{F}_2 = \mathbb{Z}_2$. It is a linear code, because $(0,0) + (0,0)$, $(0,0) + (1,1)$, and $(1,1) + (1,1)$ all belong to C, using vector addition modulo 2. Also $(0,0) \in C$ and since the only two scalars are $0, 1$, $c(0,0)$ and $c(1,1)$ are both in C, for $c \in \{0,1\}$. As a linear code, it has dimension 1 and basis given by $(1,1)$. We can appreciate the nice lattice structure of $\rho^{-1}(C)$ in the illustration. On the other hand, take $S = \{(0,0),(1,1)\}$ but this time modulo 3. Then $(1,1) + (1,1)$ does not belong to S, so S is not a linear code, and $\rho^{-1}(S)$ is not a lattice either, as is clear from Fig. 3.2a.

Definition 3.1 Let C be a linear code in $\mathbb{Z}_q^n$, the integers modulo a positive integer $q \geq 2$, where q is either prime or composite. Let $\rho : \mathbb{Z}^n \to \mathbb{Z}_q^n$ be the component-wise reduction modulo q. Then the lattice $\Lambda_C = \rho^{-1}(C)$ is said to have been obtained via *Construction A*.

The lattice Λ_C is also known as a q-ary lattice or modulo q lattice. Note that, since $0 \in C$, $q\mathbf{e}_i \in \Lambda_C$, for all canonical vectors $\mathbf{e}_i$, hence we have that $q\mathbb{Z}^n$ is a sublattice of Λ_C and the lattice inclusions $q\mathbb{Z}^n \subset \Lambda_C \subset \mathbb{Z}_q^n$. On the other hand, any lattice Λ in $\mathbb{R}^n$ satisfying $q\mathbb{Z}^n \subset \Lambda \subset \mathbb{Z}_q^n$ is obtained from the code $C = \rho(\Lambda)$ via Construction A, and so this is an equivalent definition of q-ary lattice as it is used in lattice-based cryptography [73]. Other straightforward properties of Construction A lattices are described next:

Proposition 3.2

a) If Λ_C is the q-ary lattice associated to the code $C \subseteq \mathbb{Z}_q^n$, then: $\left|\frac{\Lambda_C}{q\mathbb{Z}^n}\right| = \frac{q^n}{V(\Lambda_C)} = |C|$, *where $|C|$ is the number of codewords of C.*

b) Any full rank integer lattice $\Lambda \subseteq \mathbb{Z}^n$ is q-ary for $q = V(\Lambda)$.

Proof The first property is direct, due to the isomorphism between $\Lambda_C/q\mathbb{Z}^n$ and C. The second one comes from the fact that since $\Lambda \subset \mathbb{Z}^n$, it follows that its volume $V(\Lambda) \in \mathbb{Z}$. Taking a generator matrix B for Λ and $q = V(\Lambda) = |det(B)|$, the linear system $B\mathbf{x} = q\mathbf{z}$ has an integer solution for any $\mathbf{z} \in \mathbb{Z}^n$, and therefore $q\mathbb{Z}^n \subset \Lambda$ (Λ is a q-ary lattice).

If q is prime, a code C is a subspace of dimension $k \leq n$ of $\mathbb{Z}_q^n = \mathbb{F}_q^n$ and hence has q^k codewords. From the last proposition, we have that $V(\Lambda_C) = q^{n-k}$.

A generator matrix (Definition 2.2) is a convenient explicit way to describe a lattice, especially for computations and applications. A generator matrix of the lattice $\rho^{-1}(C)$ can be obtained from that of C. Let us thus see how to obtain such a generator matrix, for both $\mathbb{F}_p$ and $\mathbb{Z}_q$.

If p is prime, the linear (n, k) code C over $\mathbb{Z}_p = \mathbb{F}_p$ is a subspace and has a basis, formed by k vectors. These k vectors can be stacked in a matrix, either as row or column vectors, depending on the convention, to form a generator matrix. Using the column convention adopted here, we get an $n \times k$ matrix M with elements in $\mathbb{Z}_p$ such that any codeword of C can be written as $M\mathbf{y}$, where $\mathbf{y}$ is a column vector of $\mathbb{Z}_p^k$. Note also that in this case, up to coordinate permutation, any code has a generator matrix in the reduced systematic form,

$$\begin{bmatrix} \mathbf{I}_k \\ A \end{bmatrix}$$

where $\mathbf{I}_k$ is the k-dimensional identity matrix, and A is an $(n-k) \times n$ matrix.

For C a linear code in $\mathbb{Z}_q^n$, where q is a composite number, we also have a generator matrix, which contains vectors that generate C as its columns; however, these vectors do not always form a basis, and we may not have a generator matrix in systematic form. We will illustrate and explain why next.

Example 3.1 Consider the linear codes

$$C_1 = \{(2a, 2b, a+b),\ a, b \in \mathbb{F}_3\},\ C_2 = \{(2a, 2b, a+b),\ a, b \in \mathbb{Z}_4\}.$$

The code over $\mathbb{F}_3$ has dimension 2, length $n = 3$, and contains 9 codewords

$$(0,0,0), (0,2,1), (0,1,2), (2,0,1), (2,2,2), (2,1,0), (1,0,2), (1,0,2), (1,1,1).$$

A generator matrix is

$$M = \begin{bmatrix} 2 & 0 \\ 0 & 2 \\ 1 & 1 \end{bmatrix}$$

since a codeword in the column form is this matrix multiplied by $\begin{bmatrix} a & b \end{bmatrix}^T$. Another generator matrix of C_1 is the reduced echelon form of M, obtained by multiplying both columns by 2:

$$R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 2 & 2 \end{bmatrix}.$$

The code C_2 over $\mathbb{Z}_4$ has length $n = 3$ and contains 8 codewords:

$$(0,0,0), (2,0,1), (0,0,2), (2,0,3), (0,2,1), (2,2,2), (0,2,3), (2,2,0).$$

The above matrix M is again a generator matrix for C_2; only this time, it is not possible to multiply or combine its columns to obtain $(1,0)$ and $(0,1)$ as first two rows. The vectors $(2,0,1)$ and $(0,2,1)$ do not form a basis, because a basis needs to satisfy linear independence. Here

$$\lambda_1(2,0,1) + \lambda_2(0,2,1) = 0$$

does not imply $\lambda_1 = \lambda_2 = 0$ since it could also be $\lambda_1 = \lambda_2 = 2$.
Now that we know what generator matrices are for linear codes, let us go back to generator matrices for the lattices obtained via Construction A.

Since C is a linear code, we saw above that each codeword $\mathbf{a} \in C$ can be written using a set of generators, say $\mathbf{a} = \sum_{i=1}^{l} a_i \mathbf{v}_i$, $\mathbf{v}_i = (v_{i1}, \ldots, v_{in})$ for $i = 1, \ldots, l$ (and $l = k$ for the case of a linear (n,k) code over $\mathbb{F}_p$). Now

$$\mathbf{a} = \sum_{i=1}^{l} a_i \mathbf{v}_i \in C \iff \rho^{-1}(\mathbf{a}) = \sum_{i=1}^{l} a_i \mathbf{v}_i + \sum_{i=1}^{n} q h_i \mathbf{e}_i \in \mathbb{R}^n$$

where $0 \leq a_i, v_{ij} \leq m-1$ for all i, j, $\mathbf{e}_i$, $i = 1, \ldots, n$ form the canonical basis of $\mathbb{R}^n$ and $h_1, \ldots, h_n \in \mathbb{Z}$. In words, $\rho^{-1}(\mathbf{a})$ is an integral linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_l, q\mathbf{e}_1, \ldots, q\mathbf{e}_n$. An expanded generator matrix B can thus be obtained as follows: stack all the column vectors in an $n \times (n+l)$ matrix. Now we would like to obtain a row echelon form for this matrix, except that because we are working with a lattice, only $\mathbb{Z}$-linear combinations are allowed, and we can only perform elementary operations on the columns which consist of additions and subtractions (divisions are not allowed, unlike for the echelon form). The notion of reduced echelon form is,

over $\mathbb{Z}$, formally replaced by that of *Hermite normal norm (HNF)* . We say that an integer matrix of full row rank is in (column) Hermite normal form if it is of the form $[H\ \mathbf{0}]$ with $H = (h_{ij})$ a square matrix and

1. $h_{ij} = 0$ for $i < j$, which means the matrix H will be lower triangular.
2. $0 \leq h_{ij} < h_{ii}$ for $i > j$, that is entries are nonnegative, and each row has a maximum entry on the diagonal.

Note that any matrix B with integer entries can be reduced to a column Hermite normal form, $B = [H\ \mathbf{0}]U$, where U is a square unimodular matrix. If B is full row rank as it is the case of the expanded generator matrix of Λ_C above, then H is also full rank. For algorithms that compute the HNF, see, e.g., [21, p. 67, 68; algorithm included]. Mathematical software packages such as Mathematica, Maple, MATLAB, Scilab, and Sage also have implemented algorithms. Usually those algorithms appear in the Hermite row form, so for the column form used here, it should be adapted via transposed matrices.

Proposition 3.3 *Let $\mathbf{v}_1, \ldots, \mathbf{v}_l$ be generators for the linear code C over $\mathbb{Z}_q$ and $\mathbf{e}_1, \ldots, \mathbf{e}_n$ be the canonical basis of $\mathbb{R}^n$. Then a generator matrix for the lattice $\rho^{-1}(C)$ is given by the $n \times n$ full rank matrix H obtained by computing the Hermite normal form $[H\ \mathbf{0}]$ of $[\mathbf{v}_1, \ldots, \mathbf{v}_l, q\mathbf{e}_1, \ldots, q\mathbf{e}_n]$. If the generator matrix of C can be put in systematic form*

$$\begin{bmatrix} \mathbf{I}_l \\ A \end{bmatrix},$$

(which, up to coordinate permutation, is always the case for $\mathbb{Z}_p = \mathbb{F}_p$ (and $l = k$) and may or may not be possible otherwise), then a generator matrix of Λ_C is

$$\begin{bmatrix} \mathbf{I}_l & \mathbf{0}_{l\times(n-l)} \\ A & q\mathbf{I}_{n-l} \end{bmatrix}.$$

Proof We already know from above that $\mathbf{v}_1, \ldots, \mathbf{v}_l, q\mathbf{e}_1, \ldots, q\mathbf{e}_n$ generate the lattice, we just need to extract a basis by computing the Hermite normal form out of the $n \times (n + l)$ matrix

$$\left[\mathbf{v_1}, \ldots, \mathbf{v}_l, q\mathbf{e}_1, \ldots, q\mathbf{e}_n\right],$$

which looks like $[H\ \mathbf{0}]$, and H clearly contains a basis. In the case C has a generator matrix in systematic form, then we need to compute a Hermite normal form out of

$$\begin{bmatrix} \mathbf{I}_l & q\mathbf{I}_l & \mathbf{0}_{l\times(n-l)} \\ A & \mathbf{0}_{(n-l)\times l} & q\mathbf{I}_{n-l} \end{bmatrix}.$$

Multiplying the first l columns by $-q$ and adding them to the next l columns give

$$\begin{bmatrix} \mathbf{I}_l & \mathbf{0}_l & \mathbf{0}_{l\times(n-l)} \\ A & -qA & q\mathbf{I}_{n-l} \end{bmatrix}.$$

Then multiplying the column containing the ith 1 of $\mathbf{I}_{n-l}$ in turn by a_{ij}, for $j = 1, \ldots, n-l$ and adding it to the corresponding column in $-qA$ will give the desired result.

Note that a generator matrix for Λ_C is obtained from $B = [\mathbf{v}_1, \ldots, \mathbf{v}_l, q\mathbf{e}_1, \ldots, q\mathbf{e}_n]$ when it is reduced to the form $[H\ \mathbf{0}]$ even if H does not satisfy all the requirements of the Hermite normal form, but the latter has a kind of canonical format similar to the reduced echelon form.

Example 3.2 For the codes C_1 and C_2 in Example 3.1, generator matrices for the lattices Λ_{C_1} and Λ_{C_2} can be obtained by considering the Hermite normal form of the matrices

$$B_1 = \begin{bmatrix} 2\,0\,3\,0\,0 \\ 0\,2\,0\,3\,0 \\ 1\,1\,0\,0\,3 \end{bmatrix} \text{ and } B_2 = \begin{bmatrix} 2\,0\,4\,0\,0 \\ 0\,2\,0\,4\,0 \\ 1\,1\,0\,0\,4 \end{bmatrix},$$

respectively, which are

$$H_1 = \begin{bmatrix} 1\,0\,0 \\ 0\,1\,0 \\ 2\,2\,3 \end{bmatrix} \text{ and } H_2 = \begin{bmatrix} 2\,0\,0 \\ 0\,2\,0 \\ 1\,1\,2 \end{bmatrix}.$$

Note also that H_1 is built from the generator matrix of the code C_1 in systematic form as described in the last proposition. As another example, consider the code C_3 in $\mathbb{Z}_6^3$ generated by the codeword $(1, 2, 3)$. Since it has a generator matrix in systematic form, $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$, a generator matrix of the lattice Λ_{C_3} in $\mathbb{R}^3$ is $\begin{bmatrix} 1\,0\,0 \\ 2\,6\,0 \\ 3\,0\,6 \end{bmatrix}$.

Example 3.3 Proposition 3.3 always provides a basis and a generator matrix for the lattice Λ_C associated with a code C. In some cases, other generator matrices can be derived from the Hermite matrices to better describe the lattice. For example, consider the code C over $\mathbb{Z}_5$ generated by $(1, 2)$, namely,

$$C = \langle (1,2) \rangle = \{(0,0), (1,2), (2,4), (3,1), (4,3)\} \subset \mathbb{Z}_5^2.$$

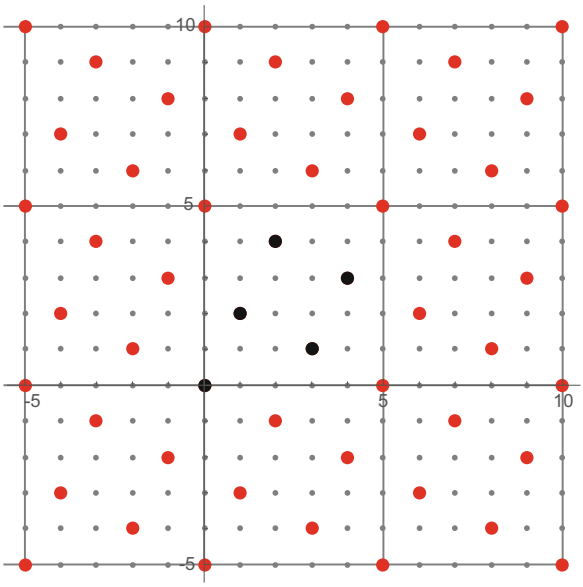

Fig. 3.3 The lattice constructed from the code $\langle(1,2)\rangle \subset \mathbb{Z}_5^2$

According to the above proposition, a basis for Λ_C is $\begin{bmatrix} 1 & 0 \\ 2 & 5 \end{bmatrix}$. One can verify using Theorem 2.2 that $\begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix}$ is also a generator matrix for this lattice, whose basis is Minkowski reduced (see Definition 2.15), geometrically revealing a square shape (see Fig. 3.3).

Example 3.4 Consider the linear code $C = \{(a_1, \ldots, a_{n-1}, \sum_{i=1}^{n-1} a_i),\ a_1, \ldots, a_{n-1} \in \mathbb{F}_2\}$ over $\mathbb{F}_2$. It has length n and dimension $n-1$. A systematic generator is

$$\begin{bmatrix} \mathbf{I}_{n-1} \\ 1 \ldots 1 \end{bmatrix}.$$

A generator matrix for Λ_C is thus

$$\begin{bmatrix} \mathbf{I}_{n-1} & \mathbf{0}_{(n-1)\times 1} \\ 1 \ldots 1 & 2 \end{bmatrix}.$$

This means that every vector $\mathbf{x} \in \rho^{-1}(C)$ is of the form $\mathbf{x} = (x_1, \ldots, x_{n-1}, \sum_{i=1}^{n-1} x_i + 2x_n)$, $x_i \in \mathbb{Z}$ for all i. This describes every vector which satisfies that the sum of its entries is even. Indeed, a constraint on the sum means that there are $n-1$ degrees of freedom in the first $n-1$ entries (they can be chosen to be anything), and to force the sum to be even no matter what is the choice of $x_1, \ldots, x_{n-1}$, the last component must contain $\sum_{i=1}^{n-1} x_i$. But then our constraint is just that the sum is even, so the

entry should be able to be anything as long as it is even; thus it is of the form $\sum_{i=1}^{n-1} x_i + 2x_n$ where x_n can take any value and $2x_n$ means any even value. This shows that we have just constructed the lattices

$$D_n = \{(x_1, \ldots, x_n), \ \sum_{i=1}^{n} x_i \text{ is even}\}$$

presented in Example 2.4.

3.2 Relevant Distances in Codes and Lattices

Since we are studying lattices with interesting parameters, one may wonder how distances defined over codes translate into parameters for lattices via Construction A. Distances are used in linear codes to characterize their error correction capability. We will consider here the widely used Hamming distance and the ℓ_p distances , $1 \leq p \leq \infty$, also called p-Lee distances. For $p = 1$, $p = 2$, and $p = \infty$, these are the well-known Lee, Euclidean, and the maximum or Chebyshev distances which are used in applications such as constrained and relay channels [38, 88, 101] ($p = 1$), physical layer networks [39] ($p = 2$), rank modulation, and flash memory [94] ($p = \infty$). General d_p distances $1 \leq p \leq \infty$ are considered in [19, 32, 45, 57, 85] and appear while studying the complexity of computational lattice problems [2, 82].

We recall the mathematical definition of a distance.

Definition 3.2 A *distance* or *metric* in a set A is a map $d : A \times A \to \mathbb{R}$ which satisfies the following three conditions :

i) $d(x, y) \geq 0$ and $d(x, y) = 0$ if and only if $x = y$.
ii) $d(x, y) = d(y, x)$, and
iii) $d(x, z) \leq d(x, y) + d(y, z)$, for every x, y, z in A.

In what follows, we treat the Hamming, Lee and p-distances for codes and lattices, and related concepts such as the minimum distance of a set and closed balls

$$B_d(x, R) = \{y \in A; d(y, x) \leq R\} \tag{3.1}$$

in these distances.

The Hamming Distance For $A = \mathbb{Z}_q^n$, particularly for $q = 2$, corresponding to binary codes, the commonly used distance is the *Hamming distance* d_H which counts the number of coordinates in which two codewords differ. For $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$,

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i; x_i \neq y_i\}|.$$

For example, in $\mathbb{Z}_2^4$,

$$d_H((1,0,1,1),(0,1,0,1)) = 3$$

and in $\mathbb{Z}_5^3$,

$$d_H((1,0,3),(1,2,0)) = 2.$$

The Minimum Hamming Distance For a linear code C in $\mathbb{Z}_q^n$, it is defined as the minimum of all distances between two different vectors in the code. Since $d_H(\mathbf{x},\mathbf{y}) = d_H(\mathbf{x}+\mathbf{k},\mathbf{y}+\mathbf{k})$, for every $\mathbf{x},\mathbf{y},\mathbf{k} \in \mathbb{Z}_q^n$, the minimum Hamming distance is the minimum of $d_H(\mathbf{x},\mathbf{0})$, $(\mathbf{x} \in C, \mathbf{x} \neq \mathbf{0})$, that is the minimum weight of a non-zero codeword.

For binary linear codes $C \subset \mathbb{Z}_2^n$, the minimum Hamming distance $d_H(C)$ is linked to the error correction capability. A code with minimum distance $d_H(C)$ can correct $R = \left\lfloor \frac{d_H(C)-1}{2} \right\rfloor$ errors. Geometrically this means that the Hamming balls of radius R centered at codewords do not intersect. Hence, any received vector in $\mathbb{Z}_2^n$ with no more than r different coordinates (errors) from that of a codeword will be located in just one of these balls and will be decoded as its center.

Definition 3.3 A binary linear code is *R-perfect* in the Hamming metric if the union of those balls centered in its codewords with the radius R is $\mathbb{Z}_2^n$.
The Hamming codes introduced by R.W. Hamming in 1950 and used in several applications are 1-perfect. In $\mathbb{Z}_2^7$, a 1-perfect code can be described as $C = \{(a_1,a_2,a_3,a_4,a_2+a_3+a_4,a_1+a_3+a_4,a_1+a_2+a_4), a_i \in \mathbb{Z}_2\}$.

The relation between the minimum Hamming distance of a code $C \subset \mathbb{Z}_2^n$ and the minimum norm (Euclidean distance) of its associated Construction A lattice Λ_C is described in the next proposition [60].

Proposition 3.4 *Let C be a linear binary code with minimum distance $d_H(C)$ and λ be the minimum norm (see (2.10)) of its associated lattice Λ_C. Then:*

i) If $d_H(C) < 4$, $\lambda = \sqrt{d}$ and the set of minimum norm vectors of Λ_C is composed by the codewords of C with weight d and the vectors obtained from these codewords by replacing one or more coordinates set to 1 by -1.
ii) If $d_H(C) = 4$, $\lambda = 2$ and the set of minimum norm vectors of Λ_C is composed by the codewords of C with weight equal to 4, the vectors obtained from these codewords by replacing one or more coordinates set to 1 by -1 and the vector which have ± 2 for their unique non-zero coordinate.
iii) If $d_H(C) > 4$, $\lambda = 2$ and the minimum norm vectors of Λ_C are the ones which have ± 2 for their unique non-zero coordinate.

This result is useful to detect the set of minimum norm vectors of special lattices which may be difficult to find in general. For example, consider the lattice E_8 (see Chap. 2). A lattice congruent to E_8 can be obtained via Construction A from the extended Hamming code in $\mathbb{Z}_2^8$ given by

$$C = \{(a_1,a_2,a_3,a_4,a_2+a_3+a_4,a_1+a_3+a_4,a_1+a_2+a_4,a_1+a_2+a_3), a_i \in \mathbb{Z}_2\}$$

(see [98, Chap. 5, 2.1]). The code C has minimum Hamming distance 4 and 14 of its codewords have this minimum distance (see Exercise 3.2). By the above proposition, considering all 2^4 possibilities of sign changes in each codeword of minimum distance plus the lattice vectors on the edges, we get that E_8 must have $14 \cdot 2^4 + 16 = 240$ vectors of minimum norm. This number (the kissing number of E_8) appears also in the theta series of this lattice (see the following section).

The Lee and the ℓ_p Distances Another distance used for $q-$ary codes is the Lee distance in $\mathbb{Z}_q^n$, introduced in [61] for non-binary codes. We consider here the set of integers modulo q in its typical representation, $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$. For a and b in $\mathbb{Z}_q$, it is the "circular" graph distance (see Fig. 3.4), defined by

$$d_{\text{Lee}}(a, b) = min\{|a - b|, q - |a - b|\}.$$

In the Cartesian product $\mathbb{Z}_q^n$, the Lee distance between $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ is defined as

$$d_{\text{Lee}}(\mathbf{a}, \mathbf{b}) = \sum_{i=1}^{n} d_{\text{Lee}}(a_i, b_i).$$

We remark (see Exercise 3.3) that for $q = 2$ and $q = 3$, the Lee and the Hamming distances in $\mathbb{Z}_q^n$ are the same for all pairs of vectors and these are the only values of

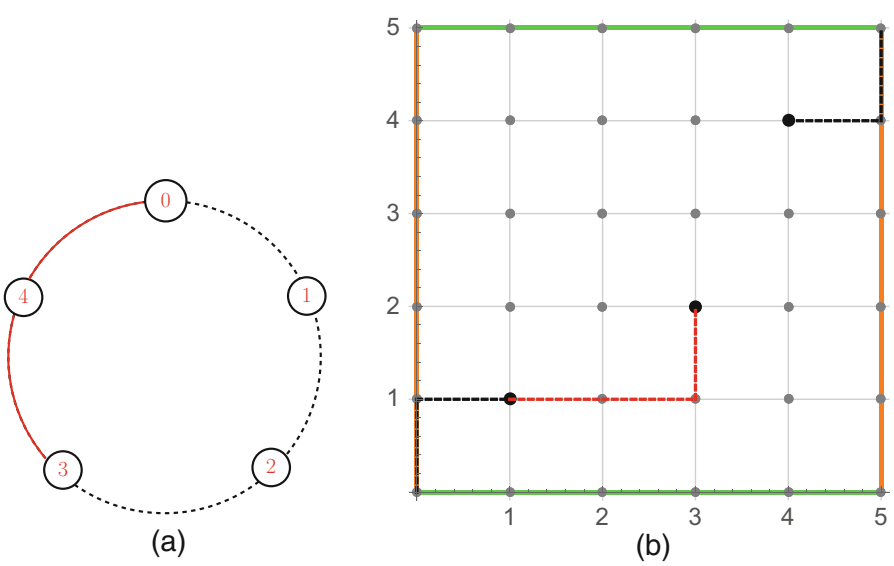

Fig. 3.4 (**a**) Lee distance in $\mathbb{Z}_5$: the smallest number of edges in the circular graph on the left (e.g., $d_{\text{Lee}}(0, 3) = 2$). (**b**) Lee distance in $\mathbb{Z}_5^2$: in the integer grid with the parallel board sides identified (flat torus), it is again the graph distance, that is the smallest number of edges connecting two pairs (e.g., $d_{\text{Lee}}((1, 1), (3, 2)) = 3$ (red path), $d_{\text{Lee}}((1, 1), (4, 4)) = 4$ (black path)

q for which both metrics coincide. For instance, in $\mathbb{Z}_5^3$ $d_{\text{Lee}}((1,0,3),(1,2,0)) = 5$ and $d_H((1,0,3),(1,2,0)) = 2$, as we have seen.

The Lee distance in $\mathbb{Z}_q^n$ can be seen as induced by the l_1 or Manhattan distance in $\mathbb{Z}^n$, $d_1(\mathbf{a},\mathbf{b}) = \sum_{i=1}^n |a_i - b_i|$, into the quotient $\mathbb{Z}^n/q\mathbb{Z}^n \simeq \mathbb{Z}_q^n$. We can also consider distances either in $\mathbb{Z}^n$ or in $\mathbb{Z}_q^n$ as the ones induced by the well-known l_p metrics in $\mathbb{R}^n$, which are defined for $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ in $\mathbb{Z}^n$ and $p \in \mathbb{N}$, $p \geqslant 1$,as

$$d_p(\mathbf{a},\mathbf{b}) = \left(\sum_{i=1}^n |a_i - b_i|^p\right)^{\frac{1}{p}}$$

and $d_\infty(\boldsymbol{a},\mathbf{b}) := \max\{|a_i - b_i|;\ i = 1,\ldots,n\}$. Note that for $p = 1$ and $p = 2$, we have the Lee distance and the standard Euclidean distance, respectively, whereas for $p = \infty$, this distance is also known as the maximum or Chebyshev metric. The correspondent induced ℓ_p- distance for $\mathbf{a}$ and $\mathbf{b}$ in $\mathbb{Z}^n/q\mathbb{Z}^n \simeq \mathbb{Z}_q^n$ (also called p-Lee distance) is given by [19]

$$d_p(\mathbf{a},\mathbf{b}) = \left(\sum_{i=1}^n (d_{\text{Lee}}(a_i,b_i))^p\right)^{\frac{1}{p}} \text{ for } p \in \mathbb{N}, p \geqslant 1,$$

and

$$d_\infty(\boldsymbol{a},\mathbf{b}) := \max\{d_{\text{Lee}}(a_i,b_i), i = 1,\ldots,n\}.$$

Example 3.5 For $\mathbf{a} = (1,1)$ and $\mathbf{b} = (4,4)$ in $\mathbb{Z}^2$, we have

$$d_1(\mathbf{a},\mathbf{b}) = 6,\ d_2(\mathbf{a},\mathbf{b}) = 6\sqrt{2},\ d_\infty(\mathbf{a},\mathbf{b}) = 3,$$

whereas for $\mathbf{a} = (1,1)$, $\mathbf{b} = (4,4)$ now considered in $\mathbb{Z}_5^2$,

$$d_1(\mathbf{a},\mathbf{b}) = d_{\text{Lee}}(\mathbf{a},\mathbf{b}) = 4,\ d_2(\mathbf{a},\mathbf{b}) = 4\sqrt{2},\ d_\infty(\mathbf{a},\mathbf{b}) = 2.$$

Like the Hamming distance, all the p-Lee distances in $\mathbb{Z}^n$ or $\mathbb{Z}_q^n$ are invariant by translations (Exercise 3.4):

$$d(\mathbf{a},\mathbf{b}) = d(\mathbf{a}+\mathbf{c},\mathbf{b}+\mathbf{c}).$$

As functions we have (see Exercise 3.5) that $d_1 \geq d_2 \geq \ldots \geq d_\infty$, which implies the inclusion reversal order for the closed balls of a fixed radius. For $p = 1$ (Lee) and $p = \infty$, the p-distances in $\mathbb{Z}^n$ or in $\mathbb{Z}_q^n$ are always integers, and there are closed form expressions for the number of points $\mu_p(n,R)$ in the closed balls of radius R in $\mathbb{Z}^n$, given by

$$\mu_1(n,R) = \sum_{i=0}^{\min\{n,R\}} 2^i \binom{n}{i}\binom{R}{i} \tag{3.2}$$

$$\mu_\infty(n, R) = (2R + 1)^n. \tag{3.3}$$

Note also that, for $2R + 1 \leq q$, the number of points in a closed ball of radius R in $\mathbb{Z}_q^n$ either in the Lee or in the infinity metric in $\mathbb{Z}_q^n$ is the same as in the ball in $\mathbb{Z}^n$ with the same radius.

Example 3.6 For $n = 2$, we have from the expressions above that $\mu_1(n, R) = R^2 + (R + 1)^2$ and $\mu_\infty(n, R) = (2R + 1)^2$. Thus a closed ball of radius 2 in the d_1 (Lee) distance either in $\mathbb{Z}^2$ or in $\mathbb{Z}_7^2$ has 13 points, whereas in the distance d_∞ a ball with the same radius has 25 points, since $2R+1 \leq q$. For the distance d_1, the closed balls with $R = 4$ in $\mathbb{Z}^2$ and in $\mathbb{Z}_7^2$ have 41 and 37 points, respectively. The balls of radius 4 for the distance d_∞ in $\mathbb{Z}^2$ and in $\mathbb{Z}_7^2$ have 81 and 49 points (since $d_\infty(\boldsymbol{a}, \mathbf{b}) \leq 3$, for all $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_7^2$), respectively.

The Minimum Distance $d_p(C)$ For a linear code C in $\mathbb{Z}_q^n$ or a lattice Λ in $\mathbb{Z}^n$, it is defined as the minimum of the ℓ_p distances between two different vectors in the code or in the lattice which, due to invariance under translation, is the same as the minimum ℓ_p-distance from a non-zero vector to the null vector (*minimum ℓ_p-norm*).

It should be remarked that for a large enough alphabet size, a code and its associated lattice via Construction A have the same minimum ℓ_p-distance [56, 89], since

$$d_p(\Lambda_C) = \min\left\{d_p(C), q\right\}. \tag{3.4}$$

Like in the Hamming metric, we may use the closest neighbor criterion under the p-distance for decoding by considering disjoint p-balls centered at codewords. We define the *d_p-packing radius* R of a code $C \subset \mathbb{Z}_q^n$ ($\Lambda \subset \mathbb{Z}^n$) as the greatest R such that the closed balls of radius R in the d_p metric centered at the distinct points of C are disjoint and there is at least one point of $\mathbb{Z}_q^n$ ($\mathbb{Z}^n$) at the boundary of these closed balls. Hence any received vector which is inside these balls will be univocally decoded as the codeword center of its ball.

For $p = 1$ and $p = \infty$, the packing radius of a linear code $C \subset \mathbb{Z}_q^n$ ($\Lambda \subset \mathbb{Z}^n$) is an integer given by the expression $R = \left\lfloor \frac{d_p(C)-1}{2} \right\rfloor$. For $1 < p < \infty$, a similar expression is not valid [19].

Similarly to the binary case with Hamming distance (recall Definition 3.3), we can consider closed balls (3.1) in $\mathbb{Z}_q^n$ or $\mathbb{Z}^n$ with respect to the ℓ_p metric and define:

Definition 3.4 If the union of disjoint closed balls of packing radius R in a p-metric covers $\mathbb{Z}_q^n$ (or $\mathbb{Z}^n$), we say that C (or Λ) is *R-perfect in this metric*.

For $R < \frac{q}{2}$, a necessary condition for a code to be R-perfect in the ℓ_p metric is that $|C|\, \mu_p(n, R) = q^n$. We may use the closed form expression for the number of closed ball points $\mu_p(n, R)$ in the cases $p = 1$ (3.2) and $p = \infty$ (3.3).

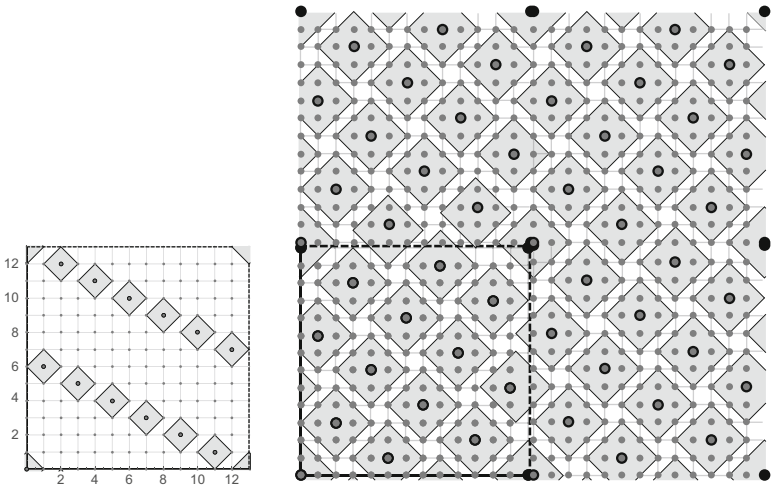

Fig. 3.5 Codes in $\mathbb{Z}_{13}^2$ with the Lee distance. On the left the code $C_1 = \langle (1,6) \rangle$ with its packing balls, on the right the perfect code $C_2 = \langle (2,3) \rangle$ represented inside its associated lattice Λ_{C_2}

Example 3.7 Consider the linear codes $C_1 = \langle (1,6) \rangle$ and $C_2 = \langle (2,3) \rangle$ in $\mathbb{Z}_{13}^2$ generated by the vectors $(2,3)$ and $(1,6)$, respectively. Both codes have 13 codewords, minimum distances in the Lee metric which are $d_1(C_1) = 3$ and $d_1(C_2) = 5$, and hence their packing radii are 1 and 2, respectively. The code C_2 is 2-perfect in the Lee distance since balls of radius 2 centered at its codewords are disjoint and cover $\mathbb{Z}_{13}^2$, whereas C_1 is not. Note also that, taking into account the above Example 3.6, the lattice Λ_{C_2} is also 2-perfect with respect to the l_1 distance (see Fig. 3.5). This relation between perfect codes and associated perfect lattices can be extended to all d_p distances.

Proposition 3.5 ([19]) *If $C \subset \mathbb{Z}_q^n$ is a perfect linear code in the ℓ_p-metric with packing radius $R < \frac{q}{2}$, then the lattice Λ_C is also perfect in this metric with the same radius.*

Example 3.8 Consider the perfect code given by $C_k = \langle (k, k+1) \rangle \subset \mathbb{Z}_h^2$, where $h = k^2 + (k+1)^2$, in the Lee metric with radius $R = k$ (see Exercise 3.6). Since $k < \frac{h}{2}$, the associated lattice Λ_C is also perfect in $\mathbb{Z}^2$. This provides, for $n = 2$, examples of perfect Lee lattices of any radius.

The result of the last example cannot be extended to dimension 3. This is a consequence of the so-called Golomb-Welch conjecture. Introduced in [46], it states that for $n \geq 3$, the unique Lee perfect lattices are the ones with radius $R = 1$. This long-standing conjecture is, up to now, only proved in particular cases and for $n \leq 11$ (see [50] and references therein). It is important to note that the condition $R < \frac{q}{2}$ in the last proposition cannot be removed. A counterexample

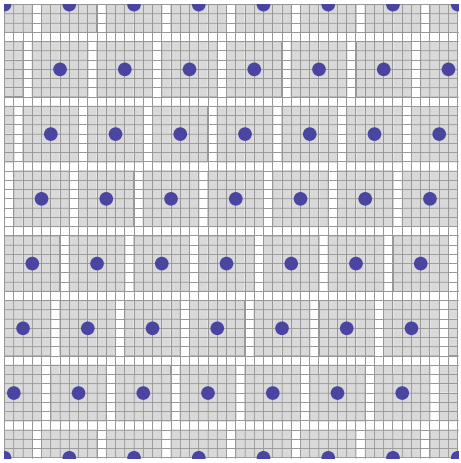

Fig. 3.6 The code $C = \langle (1, 7) \rangle \subset \mathbb{Z}_{49}^2$, which is perfect in the ℓ_∞ distance with its packing balls

can be given by the perfect binary code C with radius 7 in the Lee metric, $C = \{(0, 0, 0, 0, 0, 0, 0), (1, 1, 1, 1, 1, 1, 1)\} \subset \mathbb{Z}_2^7$ since Λ_C is not perfect in $\mathbb{Z}^7$ (see Exercise 3.7).

Note that the trivial codes $C = \{\mathbf{0}\}$ and $C = \mathbb{Z}_q^n$ may be considered perfect for any d_p distance. For $p = \infty$, the existence of perfect codes is fully characterized next.

Proposition 3.6 ([32]) *There are nontrivial perfect codes $C \subset \mathbb{Z}_q^n$ in the ℓ_∞ metric if and only if $q = bm$ with $b > 1$ an odd integer and $m > 1$ an integer.*

Example 3.9 Simple examples of perfect codes of packing radius R in the ℓ_∞ metric are, for $b = 2R + 1$, the Cartesian codes, $C = \sum_{i=1}^{n} \alpha_j b \mathbf{e}_\mathbf{i}, \subset \mathbb{Z}_{bm}^n$, $(\alpha_j = 0, 1, \ldots, m)$. An example of a non-Cartesian perfect code in the d_∞ metric is $C = \langle (1, 7) \rangle \subset \mathbb{Z}_{49}^2$ (see Fig. 3.6). Its packing radius is 3.

The next proposition shows that for each perfect code in the ℓ_∞ metric, there exists $p^* \geq 1$ such that this code is also perfect in the p-Lee metric for all $p \geq p^*$.

Proposition 3.7 ([32]) *Let $C \subseteq \mathbb{Z}_q^n$ be a perfect code in the ℓ_∞ metric with packing radius R. If $p > \frac{\ln(n)}{\ln\left(1+\frac{1}{R}\right)}$, then C is perfect in the ℓ_p metric, with radius $R_p = Rn^{1/p}$.*

Note that according to the above proposition the ℓ_∞-perfect code with packing radius 3, $C = \langle (1, 7) \rangle \subset \mathbb{Z}_{49}^2$, from Example 3.7 (Fig. 3.6) is also ℓ_p-perfect with packing radius $3.2^{\frac{1}{p}}$ for any $p \geq 3$.

It may be worth noting that the lattice distances discussed in this chapter were all related to the underlying code distances. Other distances may of course be of interest, e.g., the *p*roduct distance, discussed in the next chapter.

3.2.1 q-ary Lattice Decoding

We have discussed so far many connections between distances on codes and distances on their associated lattice via Construction A. We next give applications of these connections, in particular to the problem of lattice decoding. We recall (see also Chap. 2) that given a vector in $\mathbb{R}^n$ (obtained through transmission via for example a Gaussian channel), lattice decoding consists of finding a lattice vector which is closest to it. Without the setting of transmission via a communication channel, this becomes the closest vector problem (see Problem 2.2). The case of communication via a Gaussian channel corresponds to the Euclidean distance ($p = 2$). There is a huge amount of literature on this problem (e.g., [49, 109]). On the other hand, lattice-based cryptographic schemes are usually built upon q-ary lattices and are linked to the computational difficulty of the shortest (see Problem 2.1) and closest vector problems (Problem 2.2). While both problems are difficult in general, for q-ary lattices obtained from codes via Construction A, it is possible to solve them more efficiently by decoding the code.

In the next proposition and example, we denote by $\overline{\mathbf{x}}$ a codeword of a linear code $C \subset \mathbb{Z}_q^n$ and by $\mathbf{x}$ an associated vector in Λ_C. Since there is an isomorphism $\Lambda_C/q\mathbb{Z}^n \simeq C$, we do not distinguish elements of $\Lambda_C/q\mathbb{Z}^n \subseteq \mathbb{R}^n/q\mathbb{Z}^n$ from the codewords of C.

Proposition 3.8 ([32, 57]) *Let Λ_C be a q-ary lattice and $\boldsymbol{r} = (r_1, \ldots, r_n) \in \mathbb{R}^n$. Let $\overline{\boldsymbol{r}} \in \mathbb{R}^n/q\mathbb{Z}^n$ and $\overline{\boldsymbol{c}} \in C, \boldsymbol{c} = (c_1, \ldots, c_n)$, $0 \leq c_i < q$, a closest codeword to $\overline{\boldsymbol{r}}$ considering the d_p distance in $\mathbb{R}^n/q\mathbb{Z}^n$. An element $\boldsymbol{z} \in \Lambda_C$ which is closest to $\boldsymbol{r}$ considering the ℓ_p metric in $\mathbb{R}^n$ is $\boldsymbol{z} = (z_1, \cdots, z_n)$, where $z_i = c_i + qw_i$ and $w_i = \left\lceil \dfrac{r_i - x_i}{q} \right\rfloor$, for each $i = 1, \ldots, n$.*

Example 3.10 Consider the code $C = \langle(\bar{2}, \bar{3})\rangle \subset \mathbb{Z}_{13}^2$ and its associated lattice Λ_C. For the received vector $\mathbf{r} = (0, -6) \in \mathbb{R}^2$, the closest codeword from $\overline{\mathbf{r}} = (\bar{0}, \bar{7})$ is $\overline{\mathbf{x}} = (\overline{12}, \overline{8})$. The closest lattice point to $\mathbf{r}$ in the distance d_1 is $\mathbf{z} = (-1, -5)$.

3.3 Wiretap Coding and Theta Series

Let us look again at the lattice $\Lambda_C = \rho^{-1}(C)$ obtained from a linear code $C \subset \mathbb{Z}_q^n$ via Construction A geometrically. It is obtained by considering the lattice $q\mathbb{Z}^n$ and its translations by the codewords of C. As a first example, in Fig. 3.2b, $\rho^{-1}(C)$ is the union of $2\mathbb{Z}^2$ and $2\mathbb{Z}^2 + (1, 1)$. Also, for $C = \langle(1, 2)\rangle \subset \mathbb{Z}_5^2$ (Fig. 3.3), the lattice Λ_C is the union of $\Lambda = 5\mathbb{Z}^2$ with the four translations of Λ by the nonvanishing codewords of C, $(1, 2)$, $(2, 4)$, $(3, 1)$ and $(4, 3)$ (called gluing vectors). In other words, $\rho^{-1}(C)$ is the union of cosets of $q\mathbb{Z}^n$, and codewords of C form coset representatives. This makes Construction A particularly suitable for a coding strategy called *coset coding*, which we will explain next in the context of wiretap coding.

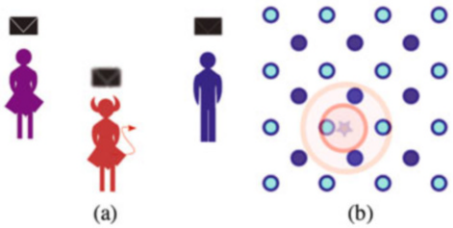

Fig. 3.7 Gaussian wiretap channel: channel and intuition. (**a**) A wiretap channel, where Alice and Bob want to exchange a confidential message in the presence of an eavesdropper Eve. (**b**) Bob's noise is such that it can decode the point transmitted via coset coding normally. Eve's noise is such that two points from the first coset and two points from the second coset are equally possible, and thus she has to decode one of the two at random

Let us consider Gaussian wiretap coding, and recall from (2.20) that transmission of a vector $\mathbf{x}$ over a Gaussian channel is of the form $\mathbf{y}_B = \mathbf{x} + \mathbf{n}_B$ where $\mathbf{n}_B$ is a random vector whose components are independent Gaussian random variables with mean 0 and variance σ_B^2. Suppose now that an eavesdropper (wiretapper) is listening to this transmission (see Fig. 3.7a). Then the eavesdropper will receive $\mathbf{y}_E = \mathbf{x} + \mathbf{n}_E$, where the noise $\mathbf{n}_E$ has variance σ_E^2. The subscripts B and E refer to Bob and Eve, the standard names of players when security is involved in a protocol. Now the Gaussian wiretap coding problem asks for reliability between the legitimate transmitter (Alice) and receiver (Bob), which is the Gaussian channel coding problem discussed in Chap. 2, but also confidentiality despite the presence of the eavesdropper Eve [62]. This is done via the introduction of randomness at the transmitter, and coset coding gives a practical way to handle this randomness. The secret information is encoded into cosets, while $\mathbf{x}$ is then chosen randomly within this coset. If we consider again the code $\{(0,0),(1,1)\} \subset \mathbb{Z}_2^2$ of Fig. 3.2b, one bit of secret can be transmitted using coset coding: to send 0, choose the coset $2\mathbb{Z}^2$, and to send 1, choose the coset $2\mathbb{Z}^2 + (1,1)$.

The idea behind wiretap coding is probably best understood in the scenario, called *wiretap II* [81], where Alice and Bob have a noiseless channel, and Eve receives μ symbols out of the n sent by Alice. Alice knows μ, but she does not know which μ positions are known to Eve. In the simplest case, say Alice sends $n = 2$ bits, and $\mu = 1$. Then Alice can achieve perfect confidentiality by sending $(b + r, r)$ where b is her secret bit, and r is a random bit, chosen uniformly at random. In the Gaussian case, the introduction of random bits is mimicked, but the intuition is different. Since Eve is supposed to have a stronger noise than Bob (as was already assumed in the wiretap II case since Bob has a noiseless channel), the geometric intuition is that when Bob receives a noisy codeword, his channel is such that in the radius around his received point, only the codeword that was sent is present, while Eve will find in her radius points from different cosets, such that each coset is equally likely to have been sent. This is illustrated in Fig. 3.7b. A practical example of the effect of coset coding is shown in Fig. 3.8, where an image has been transmitted, over a USRP testbed [65], using coset coding: on the right,

Fig. 3.8 The cameraman image transmitted by Alice and received by an eavesdropper: on the left, with no coset coding, in the middle with one bit of randomness, and on the right with two bits of randomness

one secret bit is mapped to a coset in $\mathbb{Z}_2$ ($\mathbb{Z}$ is partitioned into two cosets), and the coset representative is chosen with 2 bits of randomness. The technical settings of the experiments are found in [65].

Coset encoding uses two nested lattices $\Lambda_E \subset \Lambda_B$, where Λ_B is the lattice from which a signal constellation is carved for transmission to Bob, while Λ_E is the sublattice used to partition Λ_B. In the right picture of Fig. 3.8, $\Lambda_B = 2\mathbb{Z}$ and $\Lambda_E = \mathbb{Z}$. For a general Construction A, as explained above, Λ_B is partitioned using $\Lambda_E = q\mathbb{Z}^n$. This suggests two questions:

- Can we apply Construction A with other pairs of nested lattices? The answer is yes, and there are plenty of works and constructions following the same principle: instead of n copies of $\mathbb{Z}$, take n copies of some commutative ring R, and instead of $q\mathbb{Z}$, take an ideal I of this ring (see the introduction of the next chapter for a definition). Then use a linear code C which is a subset of $(R/I)^n$. See, e.g., [33, 59] and references therein.
- Would another choice of nested pairs of lattices $\Lambda_E \subseteq \Lambda_B$ bring more confidentiality, and what would be a design criterion for such a lattice? We will be discussing this criterion next.

As explained above, in wiretap coset coding, one message corresponds to one coset, here of a lattice, instead of one lattice point. Thus, mimicking the probability analysis of Chap. 2, the probability $P_{c,E}$ that Eve correctly decodes her received message is

$$P_{c,E} \leq \frac{1}{(\sqrt{2\pi}\sigma_E)^n} \sum_{\mathbf{t}\in\Lambda_E} \int_{\mathcal{V}_{\Lambda_B}(\mathbf{0})} e^{-\|\mathbf{u}+\mathbf{t}\|^2/2\sigma_E^2} \mathrm{d}\mathbf{u}.$$

It was shown in [80] that $P_{c,E}$ is bounded by

$$P_{c,E} \leq \frac{V(\Lambda_B)}{(\sqrt{2\pi}\sigma_E)^n} \sum_{\mathbf{t}\in\Lambda_E} e^{-||\mathbf{t}||^2/2\sigma_E^2} = \frac{V(\Lambda_B)}{(\sqrt{2\pi}\sigma_E)^n} \Theta_{\Lambda_E}\left(\frac{1}{2\pi\sigma_E^2}\right)$$

where we recall that $V(\Lambda_B)$ is the volume of Λ and Θ_Λ is the *theta series* of Λ [26] defined by

$$\Theta_\Lambda(z) = \sum_{\mathbf{x}\in\Lambda} q^{\|\mathbf{x}\|^2},\ q = e^{i\pi z}, \mathrm{Im}(z) > 0. \tag{3.5}$$

In the above upper bound, we set $y = -iz$ and thus consider $\Theta_\Lambda(y)$, for $y > 0$. In what follows, we will write $\Theta_\Lambda(q)$ whenever it does not matter whether we consider z or y. The theta series of an integral lattice keeps track of the different norms of lattice points. The coefficient $N(m)$ of q^m in this series tells how many points in the lattice are at squared distance m from the origin. This series always starts with 1, corresponding to the zero vector. The second term corresponds to the squared minimum norm λ^2 (see (2.10)), and thus the coefficient $N(\lambda^2)$ of q^{λ^2} is the kissing number of the lattice. The theta series of a general lattice is hard to compute, but in special cases, it can be expressed in terms of Jacobi theta functions [26, Chap. 4.1]. For example, it can be easily checked geometrically for $\mathbb{Z}^2$ that the first terms of its series are $\Theta_{\mathbb{Z}^2}(q) = 1 + 4q + 4q^2 + 4q^4 + 8q^5 + \ldots$. But it is not straightforward to see the coefficient attached to q^m, for big m in this series. A computation (that actually uses a Jacobi theta function) is shown in Example 3.11.

In Table 3.1 (extracted from [26]), the first non-zero coefficients of the theta series of the lattices $\mathbb{Z}^2$, A_2^*, $\mathbb{Z}^3$, FCC, BCC, and E_8 are given. Here A_2^* is the scaled version of the lattice A_2 (see Example 2.3), with minimum norm one, which is identified to the hexagonal lattice (Example 2.1).

Example 3.11 Let us compute the theta series of the lattice $\mathbb{Z}^n$:

$$\Theta_{\mathbb{Z}^n}(q) = \sum_{\mathbf{x}\in\mathbb{Z}^n} q^{||\mathbf{x}||^2} = \sum_{x_1\in\mathbb{Z}} q^{x_1^2} \cdots \sum_{x_n\in\mathbb{Z}} q^{x_n^2} = \left(\sum_{m\in\mathbb{Z}} q^{m^2}\right)^n$$

Table 3.1 First non-zero coefficients $N(m)$ of the Θ-series of some lattices studied in Chap. 2 [26, chap. 4]

$\mathbb{Z}^2$	m	0	1	2	4	5	8	9	10	13	16	17	18	20	25	26	29	32
	$N(m)$	1	4	4	4	8	4	4	8	8	4	8	4	8	12	8	8	4
A_2^*	m	0	1	3	4	7	9	12	13	16	19	21	25	27	28	31	36	37
	$N(m)$	1	6	6	6	12	6	6	12	6	12	12	6	6	12	12	6	12
$\mathbb{Z}^3$	m	0	1	2	3	4	5	6	8	9	10	11	12	13	14	16	17	18
	$N(m)$	1	6	12	8	6	24	24	12	30	24	24	8	24	48	6	48	36
FCC	m	0	2	4	6	8	10	12	14	16	18	20	22	24	26	30	32	34
	$N(m)$	1	12	6	24	12	24	8	28	6	36	24	24	24	72	48	12	48
BCC	m	0	3	4	8	11	12	16	18	19	24	27	31	35	36	40	43	44
	$N(m)$	1	8	6	12	24	8	6	24	24	24	32	12	48	30	24	24	24
E_8	m	0		2		4		6		8		10		12		14		16
	$N(m)$	1		240		2160		6720		17520		30240		60480		82560		140400

$$= (1 + 2q + 2q^4 + 2q^9 + \ldots)^n = \Theta_{\mathbb{Z}}(q)^n.$$

To evaluate the benefit of using a specific lattice Λ_E with respect to using $\Lambda_E = \nu\mathbb{Z}^n$ (ν is a scaling factor so that $\mathbb{Z}^n$ scaled to the same volume), we compare the behavior of the theta series of $\nu\mathbb{Z}^n$ with that of Λ_E and consequently define the notion of secrecy gain. This idea of defining a gain (here in terms of secrecy) by comparing the lattice $\mathbb{Z}^n$ and another lattice is fairly standard. In fact, we already mentioned it in the context of quantization (see the discussion on best quantizers at the end of Sect. 2.5.1).

Definition 3.5 The *(strong) secrecy gain* $\chi_{\Lambda,\text{strong}}$ of an n-dimensional lattice Λ is defined by

$$\chi_{\Lambda,\text{strong}} = \sup_{y>0} \frac{\Theta_{\nu\mathbb{Z}^n}(y)}{\Theta_{\Lambda}(y)}$$

defined for $y > 0$.
The role of the theta series Θ_{Λ_E} at the point $y = \frac{1}{2\pi\sigma_E^2}$ has been independently confirmed in [63], where it was shown for the mod-Λ Gaussian channel that the mutual information $I(\mathbf{S};\mathbf{Z})$, an information theoretic measure of the amount of information that Eve gets about the secret message $\mathbf{S}$ by receiving $\mathbf{Z}$, is bounded by a function that depends of the channel parameters and of $\Theta_{\Lambda_E}\left(\frac{1}{2\pi\sigma_E^2}\right)$.

The adjective "strong" in the definition of secrecy gain is motivated by the fact that the above quantity is hard to compute, while for unimodular lattices, the secrecy gain seems to correspond to a multiplicative symmetry point of the function $\frac{\Theta_{\nu\mathbb{Z}^n}(y)}{\Theta_{\Lambda}(y)}$, as illustrated in Fig. 3.9 (in log scale) for the E_8 lattice. The shape of the function is typical of that of a unimodular lattice. The "weak" secrecy gain thus corresponds to this symmetric point, conjectured to be the maximum of the function and thus the secrecy gain. As of now, this conjecture is still under investigation.

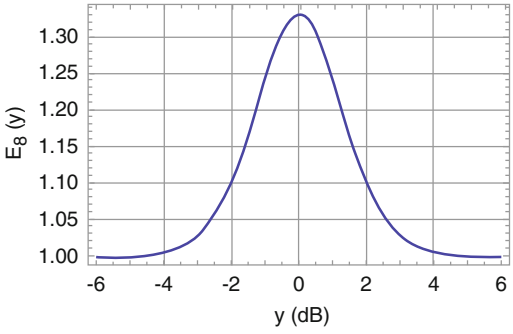

Fig. 3.9 The secrecy gain of the 8-dimensional unimodular lattice E_8 where the x-axis is in decibels ($10\log_{10}(y)$)

Exercises

Exercise 3.1 Show that for $S \subset \mathbb{Z}_q^n$, if $\rho^{-1}(S)$ is a lattice in $\mathbb{R}^n$, then S is a linear code.

Exercise 3.2 Show that the extended Hamming code in $\mathbb{Z}_2^8$ has minimum Hamming distance 4 and that 14 of its codewords have this minimum distance.

Exercise 3.3 Show that for $q = 2, 3$, the Lee distance is the same distance as the Hamming distance.

Exercise 3.4 Prove that the Hamming distance and the p-Lee distances are invariant by translation.

Exercise 3.5 Prove that for the Lee distances d_p, $d_1 \geq d_2 \geq \ldots \geq d_\infty$.

Exercise 3.6 As you can see in Figs. 3.3 and 3.5, the codes $\langle(1,2)\rangle \subset \mathbb{Z}_5^2$ and $\langle(2,3)\rangle \subset \mathbb{Z}_{13}^2$ are perfect in the Lee Metric. Prove that this result can be extended: Any code $C_k = \langle(k, k+1)\rangle \subset \mathbb{Z}_h^2$, where $h = k^2 + (k+1)^2$, is a perfect code in the Lee metric with packing radius $R = k$.

Exercise 3.7 Show that the condition $R < \frac{q}{2}$ in Proposition 3.5 cannot be removed by proving that $C = \{(0,0,0,0,0,0,0), (1,1,1,1,1,1,1)\} \subset \mathbb{Z}_2^7$ is perfect with radius 3 in the Lee metric but Λ_C is not perfect in $\mathbb{Z}^7$.