Chapter 5
Lattices and Spherical Codes

Lattices in $\mathbb{R}^n$ with sublattices which have an orthogonal basis are associated with spherical codes in $\mathbb{R}^{2n}$ generated by a finite commutative group of orthogonal matrices. They also can be used to construct homogeneous spherical curves for transmitting a continuous alphabet source over an AWGN channel. In both cases, the performance of the decoding process is related to the packing density of the lattices (see (2.13)). In the continuous case, the packing density of these curves relies on the search for projection lattices with good packing density. We present here a survey on this topic mainly based on [18, 31, 96, 105].

5.1 Spherical and Geometrically Uniform Codes

Consider the sphere of radius a in $\mathbb{R}^n$, $S^{n-1}(a) = \{\mathbf{x} \in \mathbb{R}^n; \|\mathbf{x}\| = a \geq 0\}$. A *spherical code* is a finite set of M points on this sphere. Usually we consider only spherical codes on the sphere of radius one, $S^{n-1} = S^{n-1}(1)$, and all the conclusions will be extended by similarity to a sphere of radius a. Two dual optimization (packing) problems regarding spherical codes, which have several applications in physics, chemistry, architecture, and signal processing, can be stated as:

Problem 1 Given a dimension n and an integer number $M > 0$, find a spherical code with M points such that the minimum distance between two points in the code is the largest possible.

Problem 2 Given a dimension n and a minimum distance $d > 0$, find a spherical code with the biggest number M of points such that each two of them are at distance at least d.

Codes which are solutions for one of these problems are called optimal spherical codes. In dimension 2, codes which are vertices of regular polygons inscribed in S^1 provide solutions for both problems. The solution of Problem 1 in dimension 3

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_5

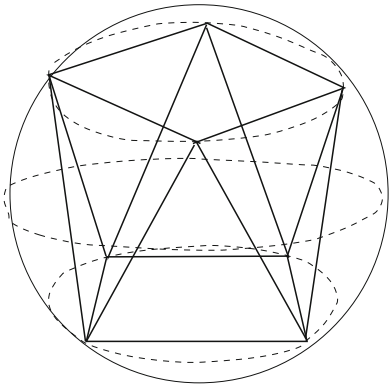

Fig. 5.1 Antiprism with eight vertices

is only known up to now for $1 \leq M \leq 12$ and for $M = 24$ [37]. As examples, for $M = 2$, 3, and 4, the optimal spherical codes in $\mathbb{R}^3$ are two antipodal points, the vertices of an equilateral triangle inscribed on an "equator" and the vertices of an inscribed regular tetrahedron in $S^2 \subset \mathbb{R}^3$, respectively. For $M = 8$ the optimal spherical code in $\mathbb{R}^3$ is given by the vertices, not of a cube as one could have possibly expected, but of a regular (with same length edges) antiprism with *eight* vertices (Fig. 5.1).

Other spherical codes known to be optimal for their minimum distances are the biorthogonal codes of $2n$ points in $\mathbb{R}^n$, obtained as all coordinate permutations of the vectors $(0, 0, \ldots, 0, \pm 1)$, and the simplex code which is the n-dimensional version of the triangle and tetrahedron vertices. It has $M = n+1$ points and can be described in the unit sphere in $\mathbb{R}^{n+1}$ as all permutations of the vector $\frac{1}{\sqrt{n+n^2}}(1, 1, \ldots, 1, -n)$. The distance between any two distinct points in this code is $\sqrt{\frac{2(n+1)}{n}}$.

Group codes as introduced by Slepian [97] and developed in subsequent articles [11, 16, 54, 64] are defined as finite sets on an n-dimensional sphere generated by the action of a group of orthogonal matrices. Geometrically uniform codes introduced by Forney [42] generalize this concept by considering also infinite sets of points in the Euclidean space having a transitive symmetry group. We consider this concept in the context of metric spaces [29]: for X a metric space, a signal set $S \subset X$ is a geometrically uniform code if and only if for s, t in S, there is an isometry f (depending on s, t) in X such that $f(s) = t$ and $f(S) = S$. Geometrically uniform codes capture the highly desirable properties that come from homogeneity: the same distance profile, congruent Voronoi regions in the same sense as defined for lattices, and the same error transmission probability for each codeword. One recurrent metric space considered here is the n-dimensional flat torus, obtained by identifying the opposite sides of an n-dimensional box and which can be defined as a quotient $T = \mathbb{R}^n/\Lambda$ where Λ is the group of translations generated by the n independent vectors which define this box (Λ is a lattice).

5.2 Flat Tori

A 2-dimensional flat torus can be visualized as a standard torus in the 3-dimensional space (Fig. 5.2), but it can be distinguished from the latter by being locally like a piece of plane (flat). One flat surface in $\mathbb{R}^3$ is a cylinder, obtained by identifying the boundaries of a rectangle. The flat torus can only be realized isometrically as a 2-dimensional surface in $\mathbb{R}^4$, and it is contained in a 3-dimensional sphere. For $\mathbf{c} = (c_1, c_2)$ with c_1, c_2 positive numbers such that $c_1^2 + c_2^2 = 1$, consider the map $\Phi_{\mathbf{c}} : \mathbb{R}^2 \to \mathbb{R}^4$, defined as $\Phi_{\mathbf{c}}(u_1, u_2) = (c_1 \cos(\frac{u_1}{c_1}), c_1 \sin(\frac{u_1}{c_1}), c_2 \cos(\frac{u_2}{c_2}), c_2 \sin(\frac{u_2}{c_2}))$. Observe that this map is doubly periodic, having identical images in the translates of the rectangle $[0, 2\pi c_1) \times [0, 2\pi c_2)$ by vectors $(k_1 2\pi c_1, k_2 2\pi c_2)$, k_i integers, and that its image is contained in a sphere of radius one in $\mathbb{R}^4$.

The parallel boundaries of each of these rectangles will be "glued" together and form a 2-dimensional surface with zero curvature – *the flat torus* $T_{\mathbf{c}}$. For each pair $\mathbf{c}$ under the above condition, we have a flat torus, and the sphere S^3 in $\mathbb{R}^4$ can be obtained as the union (foliation) of these tori. In Fig. 5.3 we can see for $\mathbf{c} = (0.8, 0.6)$, the tessellation of the plane given by the associated torus map. Note also that $\Phi_{\mathbf{c}}^{-1}(c_1, 0, c_2, 0)$ is the lattice given by the vertices of the rectangles. Spherical codes in $\mathbb{R}^4$ which are the image through a torus map of lattices in $\mathbb{R}^2$ with rectangular sublattices, as the one in the example of Fig. 5.3, present special homogeneous properties to be discussed in the next sections.

We next describe how any sphere in even dimensions $n = 2L$ can be considered as foliated by L-dimensional flat tori. Inequalities relating the distances on a flat torus in $\mathbb{R}^{2L}$ and on its associated hyperbox in $\mathbb{R}^L$ to be used in the next sections are also presented.

The unit sphere $S^{2L-1} \subset \mathbb{R}^{2L}$ can be foliated by flat tori (also called Clifford tori) as follows. For each unit vector $\mathbf{c} = (c_1, c_2, ..., c_L) \in S^{L-1}, c_i > 0, \sum_{i=1}^{L} c_i^2 = 1$, and $\mathbf{u} = (u_1, u_2, \ldots, u_L) \in \mathbb{R}^L$, let $\Phi_{\mathbf{c}} : \mathbb{R}^L \to \mathbb{R}^{2L}$ be defined as

$$\Phi_{\mathbf{c}}(\mathbf{u}) = \left(c_1 \cos\left(\frac{u_1}{c_1}\right), c_1 \sin\left(\frac{u_1}{c_1}\right), \ldots, c_L \cos\left(\frac{u_L}{c_L}\right), c_L \sin\left(\frac{u_L}{c_L}\right) \right). \tag{5.1}$$

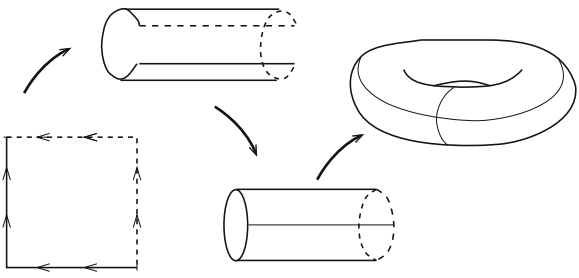

Fig. 5.2 A view of the 2-dimensional flat torus which only can be realized in $\mathbb{R}^4$

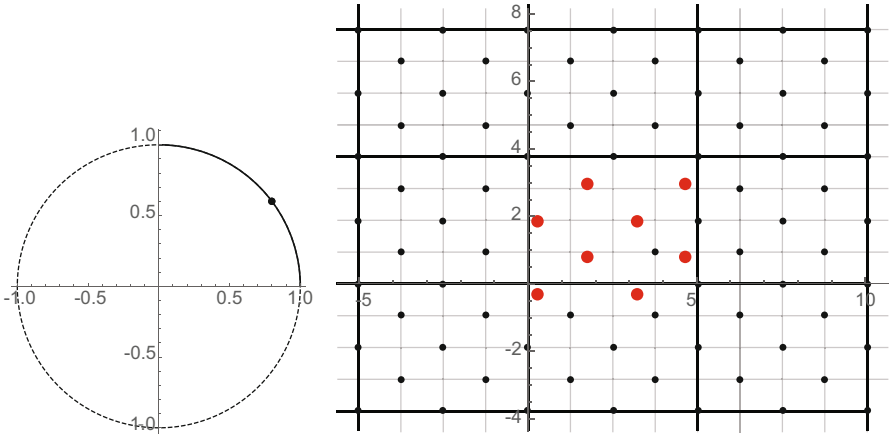

Fig. 5.3 The tessellation of the plane associated to $\mathbf{c} = (0.8, 0.6) \in S^1$, and a lattice Λ (black dots) which contains $2\pi c_1\mathbb{Z} \times 2\pi c_2\mathbb{Z}$ as a rectangular sublattice. In this case $\phi_{\mathbf{c}}(\Lambda)$ is a spherical code with $M = 8$

The image of this periodic map $\Phi_{\mathbf{c}}$ is the torus $T_{\mathbf{c}}$, a flat L-dimensional surface contained in the unit sphere S^{2L-1}, and $T_{\mathbf{c}}$ is also the image of an L-dimensional box $\mathscr{P}_{\mathbf{c}}$,

$$\mathscr{P}_{\mathbf{c}} = \{\mathbf{u} \in \mathbb{R}^L; 0 \leq u_i < 2\pi c_i, \;\; 1 \leq i \leq L\}. \tag{5.2}$$

The restriction of $\Phi_{\mathbf{c}}$ to $\mathscr{P}_{\mathbf{c}}$ is injective.

For $\mathbf{c} \in S^{L-1}$ and $c_i \geq 0$, if $c_i = 0$ for some $1 \leq i \leq L$, we may replace in (5.1) the coordinates related to c_i by 0 and obtain a degenerated flat torus $T_{\mathbf{c}}$, which is an embedding of a $(L-k)$-dimensional box in $\mathbb{R}^{2L}$, where k is the number of zero coordinates of $\mathbf{c}$.

The Gaussian curvature of a torus $T_{\mathbf{c}}$ is zero, and $T_{\mathbf{c}}$ can be cut and flattened into the box, $\mathscr{P}_{\mathbf{c}}$, just as a cylinder in $\mathbb{R}^3$ can be cut and flattened into a 2-dimensional rectangle [103]. Since the inner product $\langle \partial\Phi_{\mathbf{c}}/\partial u_i, \partial\Phi_{\mathbf{c}}/\partial u_j\rangle = \delta_{ij}$, where δ_{ij} is the Kronecker delta function, the application $\Phi_{\mathbf{c}}$ is a local isometry, which means that any measure of length, area, and volume up to dimension $L-k$ on $T_{\mathbf{c}}$ is the same of the corresponding pre-image in the box $\mathscr{P}_{\mathbf{c}}$.

We say that the family of flat tori $T_{\mathbf{c}}$ and their degenerations, with $\mathbf{c} = (c_1, c_2, ..., c_L)$, $\|\mathbf{c}\| = 1$, $c_i \geq 0$, defined above is a foliation on the unit sphere of $S^{2L-1} \subset \mathbb{R}^{2L}$. This means that any vector of S^{2L-1} belongs to one and only one of these flat tori.

The following results [105, 107] allow to relate the distances between two points in $\mathbb{R}^L$ and their spherical image on a flat tori in $\mathbb{R}^{2L}$.

Proposition 5.1 *[[105, 107]] Let $T_{\mathbf{b}}$ and $T_{\mathbf{c}}$ be two flat tori, defined by unit vectors* $\mathbf{b}$ *and* $\mathbf{c}$ *with nonnegative coordinates. The minimum distance $d(T_{\mathbf{c}}, T_{\mathbf{b}})$ between two points $\Phi_{\mathbf{c}}(\mathbf{u})$ and $\Phi_{\mathbf{c}}(\mathbf{v})$ on these flat tori is*

$$d(T_{\mathbf{c}}, T_{\mathbf{b}}) = \|\mathbf{c} - \mathbf{b}\| = \left(\sum_{i=1}^{L} (c_i - b_i)^2 \right)^{1/2}. \tag{5.3}$$

The distance between two points $\Phi_{\mathbf{c}}(\mathbf{u})$ and $\Phi_{\mathbf{c}}(\mathbf{v})$ on the same torus $T_{\mathbf{c}}$, defined by a vector $\mathbf{c} = (c_1, \cdots, c_L)$, is given by

$$||\Phi_{\mathbf{c}}(\mathbf{u}) - \Phi_{\mathbf{c}}(\mathbf{v})|| = 2\sqrt{\sum c_i^2 \sin^2\left(\frac{u_i - v_i}{2c_i}\right)} \tag{5.4}$$

and it is bounded according to the next proposition [105].

Proposition 5.2 ([106]) *Let* $\mathbf{c} = (c_1, c_2, ..., c_L) \in S^{2L-1}$, $c_i > 0$, $c_\xi = \min_{1 \le i \le L} c_i \neq 0$, $\Delta = \|\mathbf{u} - \mathbf{v}\|$ *for* $\mathbf{u}, \mathbf{v} \in \mathscr{P}_c$. *Suppose* $0 < \Delta \le c_\xi$, *then*

$$\frac{2\Delta}{\pi} \le \sin\left(\frac{\Delta}{2c_\xi}\right) 2c_\xi \le \|\Phi_{\mathbf{c}}(\mathbf{u}) - \Phi_{\mathbf{c}}(\mathbf{v})\| \le 2 \sin\frac{\delta}{2} \le \Delta.$$

Note that this last proposition shows that, for small values, the distance in $\mathbb{R}^{2L}$ between two points in a flat torus can be approached by the distance of the original points in the box $\mathscr{P}_c$ in half of the dimension.

The upcoming Sect. 5.3 is a strongly geometrical approach to commutative group codes presenting their connections with flat tori and quotient of lattices which allows the establishment of specific upper bounds on the number of points of those codes. Some results on constructions which may approach those bounds for optimal commutative group codes are discussed. Remarks on commutative group codes considered on graphs are also included. Section 5.4.1 summarizes a construction of spherical codes on layers of flat tori with some comparisons with well-known spherical codes. In Sect. 5.4.2 the homogeneous structure of flat tori and lattices come together again now in a coding scheme for transmitting continuous alphabet source over an AWGN channel. The search for projection lattices with good packing density plays a crucial role in this case.

5.3 Commutative Group Codes, Flat Tori, and Lattices

5.3.1 Commutative Group Codes

Let $\mathscr{O}_n$ be the multiplicative group of orthogonal $n \times n$ matrices and $\mathscr{G}_n(M)$ be the set of all order M commutative subgroups in $\mathscr{O}_n$.

A spherical *commutative group code* $\mathscr{C}$ is a set of M vectors which is the orbit of an initial vector $\mathbf{u}$ on the unit sphere $S^{n-1} \subset \mathbb{R}^n$ by a given finite group $G \in \mathscr{G}_n(M)$, i.e., $\mathscr{C} := G\mathbf{u} = \{g\mathbf{u}, g \in G\}$. Recalling the definition of *orthogonal matrix* in Sect. 2.1.1, one can see that starting from a vector in the sphere, all elements of $\mathscr{C}$ will be also in the sphere, and therefore $\mathscr{C}$ is indeed a spherical code.

The *minimum distance* in $\mathscr{C}$ is:

$$d := \min_{\substack{\mathbf{x},\mathbf{y} \in \mathscr{C} \\ \mathbf{x} \neq \mathbf{y}}} ||\mathbf{x} - \mathbf{y}|| = \min_{g_i \neq \mathbf{I} \in G} ||g_i\mathbf{x} - \mathbf{x}||,$$

where $||.||$ denotes the standard Euclidean norm.

A canonical form for a commutative group $G \in \mathscr{G}_n(M)$ can be obtained from the following result.

Proposition 5.3 ([43, p. 292]) *All the matrices O_i of a commutative group $\mathscr{O} = \{O_i\}_{i=1}^M$ of $n \times n$ orthogonal real matrices can simultaneously be put into a diagonal block canonical form through an orthogonal matrix Q:*

$$Q^T O_i Q = \left[\mathrm{Rot}\left(\frac{2\pi b_{i1}}{M}\right), \ldots, \mathrm{Rot}\left(\frac{2\pi b_{iq}}{M}\right), \mu_{2q+1}(i), \ldots, \mu_n(i) \right], \tag{5.5}$$

where b_{ij} are integers, the blocks $Rot(a)$ are the ones associated with 2-dimensional rotations by an angle of a radians:

$$\mathrm{Rot}(a) = \begin{bmatrix} \cos(a) & -\sin(a) \\ \sin(a) & \cos(a) \end{bmatrix},$$

and $\mu_l(i) = \pm 1$ with $l = 2q + 1, \ldots, n$.

The next proposition [28, 96] describes the geometric locus of a commutative group code. For even dimension this locus is always contained in a flat torus.

Proposition 5.4 *Every commutative group code of order M is, up to isometry, equal to a spherical code $\mathscr{X}$ whose initial vector is $\mathbf{u} = (u_1, \ldots, u_n)$, and its points have the form*

$$(\mathrm{Rot}(a_{i1})(u_1, u_2), \ldots, \mathrm{Rot}(a_{iq})(u_{2q-1}, u_{2q}), \mu_{2q+1}(i)u_{2q+1}, \ldots, \mu_n(i)u_n),$$

where $a_{ij} = \dfrac{2\pi b_{ij}}{M}$. Moreover,

1. *If $n = 2L$, $\mathscr{X}$ is contained in the flat torus $T_{\mathbf{c}}$, $\mathbf{c} = (c_1, \ldots, c_L)$ where $\mathbf{c}_i^2 = u_{2i-1}^2 + u_{2i}^2$.*
2. *If $n = 2L + 1$ and $\mathscr{X}$ is not contained in a hyperplane, $\mathscr{X} = \mathscr{X}_1 \cup \mathscr{X}_2$, where $\mathscr{X}_i$ is contained in the plane $\mathscr{P}_i = \{(x_1, \ldots, x_{2L+1}) \in \mathbb{R}^{2L+1}; x_{2L+1} = (-1)^i u_n\}$. Also, $\mathscr{X}_i$ is contained in the torus $T_{\mathbf{c}}$ of a sphere in $\mathbb{R}^{2L}$ with radius $(1 - u_n^2)^{1/2}$, where $\mathbf{c}_i^2 = u_{2i-1}^2 + u_{2i}^2$.*

5.3.2 Lattice Connections

We say that a $2L$-dimensional commutative group code is free from reflection blocks if its generator matrix group, considered as Proposition 5.3, satisfies $2L = 2q = n$. By reflection blocks, we refer to the 2-dimensional blocks

$$\pm \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix},$$

which appear in the canonical form when $2q < n$. Commutative group codes in even dimension, whose generator matrices are free from reflections blocks, are directly related to lattices.

For such commutative group codes $\mathscr{C} = G\mathbf{u}$, we may consider without loss of generality the initial vector as $\mathbf{u} = (c_1, 0, c_2, 0, \ldots, c_L, 0)$ where $\mathbf{c} = (c_1, c_2, ..., c_L)$ is a unit vector. We also will consider here $c_i > 0$, that is, codes that are not contained in a hyperplane of $\mathbb{R}^{2L}$. For the rotation angles $a_{ij} = (2\pi b_{ij})/M$, where $1 \leq i \leq M$, $1 \leq j \leq L$ as in Proposition 5.4, let $\mathbf{v}_i = (a_{i1}, \ldots a_{iL})$, $1 \leq i \leq M$ and the lattice Λ defined as the set of all integer combinations of $\mathbf{v}_i$. Note that Λ contains the rectangular lattice

$$\Lambda_{\mathbf{c}} = (2\pi c_1)\mathbb{Z} \times (2\pi c_1)\mathbb{Z} \times \cdots \times (2\pi c_L)\mathbb{Z}.$$

as a sublattice. The connection between these two lattices and the group code $\mathscr{C} = G\mathbf{u}$ is given next [96].

Proposition 5.5 *Let $\mathscr{C} = G\mathbf{u}$ with $\mathbf{u} = (c_1, 0, c_2, 0, \ldots, c_L, 0)$, $\mathbf{c} = (c_1, c_2, ..., c_L)$, $||c|| = 1$, $c_i > 0$ be a commutative group code in $\mathbb{R}^{2L}$, free from reflection blocks. The inverse image $\Phi_{\mathbf{c}}^{-1}$ by the torus mapping (5.1) is the lattice Λ defined as above. Moreover, the quotient of lattices $\dfrac{\Lambda}{\Lambda_{\mathbf{c}}}$ is isomorphic to the generator group G.*

Example 5.1 Let us consider the commutative group code $\mathscr{C}$ in $\mathbb{R}^4$ having G generated by the 4×4 matrix M with rotation blocks $[R(\frac{2\pi.1}{5}), R(\frac{2\pi.2}{5})]$ and initial vector $\mathbf{w} = (1/\sqrt{2}, 0, 1/\sqrt{2}, 0)$. Note that in this case we have $M = 5$ and a cyclic group of matrices, $G = \{\mathbf{I}, M, M^2, M^3, M^4\} \approxeq \mathbb{Z}_5$. In the notation of Proposition 5.3 $b_{i1} = i/5$, $b_{i2} = 2i/5$, and the code $\mathscr{C}$ of 5 words is obtained by multiplying $M^i\mathbf{w}$ ($\mathbf{w}$ in the column format). Then, for $\mathbf{c} = (c_1, c_2) = (1/\sqrt{2}, 1/\sqrt{2})$, the inverse image of the torus map $\Phi_{\mathbf{c}}$ of this code is the lattice $\Lambda \in \mathbb{R}^2$ generated by the vectors $\mathbf{v_1} = ((1/5)(2\pi c_1), (2/5)(2\pi c_2)$, $\mathbf{v_2} = ((-2/5)2\pi c_1, (1/5)2\pi c_2)$. Note also that if we consider the rectangular (square) sublattice $\Lambda_{\mathbf{c}}$ generated by $\mathbf{w_1} = (2\pi c_1, 0)$ and $\mathbf{w_1} = (0, 2\pi c_2)$, the quotient of lattices $\Lambda/\Lambda_{\mathbf{c}} \cong \mathbb{Z}_5$ and it is generated by $\bar{\mathbf{v}}_1$ (Fig. 5.4). It is interesting to note that this spherical code $\mathscr{C}$ is in fact the (optimal) simplex code in $\mathbb{R}^4$: any two of its five points are at a distance $\sqrt{5/2}$.

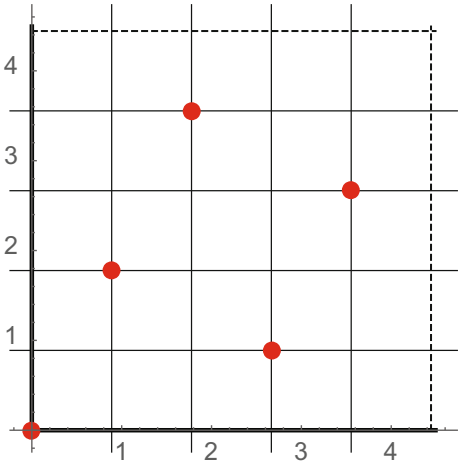

Fig. 5.4 The quotient of lattices linked to the simplex code in $\mathbb{R}^4$ with initial vector $(1/\sqrt{2}, 0, 1/\sqrt{2}, 0)$ and group of matrices generated by $[\mathrm{Rot}(\frac{2\pi.1}{5}), \mathrm{Rot}(\frac{2\pi.2}{5})]$

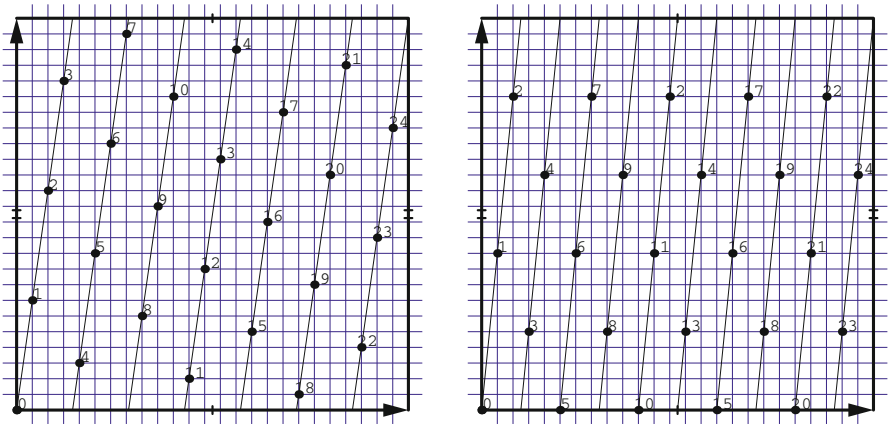

Fig. 5.5 Pre-images $\Phi_{\mathbf{c}}^{-1}$ of two cyclic group codes $\mathscr{C} = G\mathbf{u}$ of order $M = 25$ in $\mathbb{R}^4$. On the left, $G = \langle[\mathrm{Rot}(\frac{2\pi}{25}), Rot(\frac{2\pi 7}{25}]\rangle$, and the initial vector is $\mathbf{u} = (1/\sqrt{2}, 0, 1/\sqrt{2}, 0)$. On the right side, $G = \langle[\mathrm{Rot}(\frac{2\pi}{25}), \mathrm{Rot}(\frac{2\pi 10}{25}]\rangle$, and the initial vector is $\mathbf{u} = (\sqrt{0.54915}, 0, \sqrt{0.45085}, 0)$, which provides the best commutative group code of this order in $\mathbf{R}^4$[96]

Example 5.2 Figure 5.5 shows the inverse image of two commutative group codes. In both the group is cyclic ($\cong \mathbb{Z}_{25}$). Note that the lattice associated with the code on the left is equivalent to the square lattice with basis $\{(4, 3), (-3, 4)\}$ which is less dense than the lattice associated with the optimum code [106] on the right.

Proposition 5.6 ([96]) *Every commutative group code $\mathscr{C} = G\mathbf{u}$ of order M in $\mathbb{R}^{2L}$ free from 2×2 reflection blocks with initial vector $u = (u_1, \ldots, u_{2L})$ and minimum distance d satisfies*

$$M \leq \frac{\pi^L \Pi_{i=1}^{L} (u_{2i-1}^2 + u_{2i}^2)^{1/2} \Delta_{G\mathbf{u}}}{(\arcsin \frac{d}{4})^L} \leq \Delta_L \left(\frac{\pi}{(\arcsin \frac{d}{4}).L^{1/2}} \right)^L,$$

where $\Delta_{G\mathbf{u}}$ is the center density of the lattice Λ associated to the code and Δ_L is the maximum center density of a lattice packing in $\mathbb{R}^L$.

Remark 5.1 The inverse image through the torus mapping $\Phi_{\mathbf{c}}$ of a commutative group code of order M generated by matrices which may contain 2×2 reflection blocks ($2q < n$ in Proposition 5.4) not always is a quotient of lattices. However, from the L-periodicity of $\Phi_{\mathbf{c}}$ in $\mathbb{R}^L$,we can assert that for $\mathbf{u} = (u_1, \ldots, u_{2L})$, it is a periodic distribution of M points in the hyperbox $\mathscr{P}_{\mathbf{c}} \subset \mathbb{R}^L$, $c_i = \sqrt{u_{2i-1}^2 + u_{2i}^2}$ spanned by the lattice associated to this box. Therefore, for general commutative group in $\mathbb{R}^{2L}$, the lattice packing density in the last proposition can be replaced by the best periodical packing density in $\mathbb{R}^L$. Since any packing density in $\mathbb{R}^L$ can be approached by periodical packing densities as remarked in [22], we can also replace Δ_L in the last proposition for D_L, by the best center packing density in $\mathbb{R}^L$ [96]. Here it should be pointed out that for a general spherical code (not a group code), we have much bigger upper bounds and the codes may approach the packing density of $\mathbb{R}^{2L-1}$. The great advantages of commutative group codes are their homogeneity, easiness, and low cost of the encoding and decoding processes on flat tori [107]. Bounds for commutative group codes in odd dimensions, $n = 2L + 1$, can also be obtained [96] by observing that those codes must lie on two parallel hyperplanes and are formed by two equivalent copies of commutative group codes in $\mathbb{R}^{2L}$. Examples of such codes in $\mathbb{R}^3$ are the antiprisms. An interesting exercise is to describe the best spherical code of 8 points in $\mathbb{R}^3$, which is an antiprism with same size edges (Fig. 5.1), as a commutative group code described in Proposition 5.4.

The torus bounds given in the Proposition 5.6 and Remark 5.1 are tight in the following sense. Consider, for instance, the dual inequality of Proposition 5.2,

$$d \leq 2 \sin \left(\prod_{i=1}^{L} c_i D_L / M \right).$$

For big M the distance d must be small (from Proposition 5.2), and the inverse image of the ball of radius d in $\mathbb{R}^{2L}$ centered in a point of $T_{\mathbf{c}}$ will be arbitrarily close to the ball of same radius in $\mathbb{R}^L$. This means that the best packing in the flat torus will be approached by the best packing in its pre-image in the box $\mathscr{P}_{\mathbf{c}}$ and then the upper bounds of the above proposition and remark will be approached.

5.3.3 Approaching the Bound: Good and Optimum Commutative Group Codes

For small distances d or big M, good commutative group codes may be found on the search for orthogonal sublattices $\tilde{\Lambda}$ of a lattice Λ with good packing density. For each such sublattice, $\tilde{\Lambda}$ let $b_1, b_2, ..., b_n$ be length of the orthogonal basis vectors, $b = \left(\sum_{i=1}^{L} b_i^2 \right)^{\frac{1}{2}}$ the rescaled lattices $(1/b)\Lambda$ and $(1/b)\tilde{\Lambda}$. The commutative group

code $\mathscr{C}$ associated to the quotient $\frac{(1/b)\Lambda}{(1/b)\tilde{\Lambda}}$ on a flat torus $T_{\mathbf{c}}$ is a possible choice for a good code, particularly if Λ has the best packing density in its dimension.

The next proposition describes the spherical code in $\mathbb{R}^{2L}$ attached to a nested pair of lattices $\tilde{\Lambda} \subset \Lambda \subset \mathbb{R}^L$, $\tilde{\Lambda}$ orthogonal.

Proposition 5.7 *Let $\alpha = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ and $\beta = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n\}$ bases of lattices Λ_α and Λ_β, $\Lambda_\beta \subset \Lambda_\alpha$, and the associated generator matrices A_α, A_β. Then $A_\beta = A_\alpha H$, where H is an integer matrix. Suppose that β is composed by orthogonal vectors, and consider the frame in $\mathbb{R}^n$ given by the normalizations of these vectors. Let $b_i = \|\mathbf{w}_i\|$, $b = \left(\sum_{j=1}^n \|\mathbf{w}_j\|^2\right)^{\frac{1}{2}}$, $c_i = \frac{b_i}{b}$, $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ and $\phi_{\mathbf{c}}$ the torus map regarding in this frame. Then the normalized nested pair $(1/b)\Lambda_\beta \subset (1/b)\Lambda_\alpha$ of lattices is associated with a spherical code in $\mathbb{R}^{2n}$ with initial vector $(c_1, 0, c_2, 0, \ldots, c_n, 0)$ and generator group of matrices determined by the Smith normal decomposition of H.*

Proof As pointed out in Chap. 2, 2.2, by considering the Smith decomposition, $H = PDQ$, where P and Q are unimodular and D is the diagonal matrix with diagonal terms d_i, we have $A_\beta Q^{-1} = A_\alpha PD$, which implies that the columns $\mathbf{h}_i$ of the generator matrix $B_\beta = A_\beta Q^{-1}$ of Λ_β must be multiples of the columns $\mathbf{y}_i$ of the generator matrix of $B_\alpha = A_\alpha P$ of Λ_α, $\mathbf{h}_i = d_i \mathbf{y}_i$, and $i = 1, \ldots, n$. Since the expression $\mathbf{y}_i$ in terms of the original basis α is given by the matrix P, we have that for each $d_i \neq 1$, $\mathbf{y}_i$ represents a generator of the quotient of lattices with order d_j in terms of α, which implies that $\Lambda_\alpha/\Lambda_\beta \cong \mathbb{Z}_{\hat{d}_i} \oplus \ldots \oplus \mathbb{Z}_{\hat{d}_k}$, $\hat{d}_j \neq 1$. Then for each $d_j \neq 1$, it is associated the generator matrix $O_j = [Rot[2\pi p_{j1}/d_j], \ldots, Rot[2\pi p_{jn}/d_j]]$, where $M = |det(H)| = d_1 \ldots d_n$. The commutative group G composed by $M = |det(H)| = d_1 \ldots d_n$ orthogonal matrices will be the one generated by O_j, $j = 1, \ldots, k$. So in the Smith decomposition of H, the matrix D provides the group structure and the matrix P the rotation matrices involved.

Example 5.3 In the example of Fig. 5.3, we have, according to the notation used in the above proposition, $\alpha = \{\mathbf{v}_1, \mathbf{v}_2\}$, $\beta = \{\mathbf{w}_1, \mathbf{w}_2\}$, with $\mathbf{v}_1 = ((0.8)2\pi/4, 0)$, $\mathbf{v}_2 = ((0.8)2\pi/2, (0.6)2\pi/4)$,$\mathbf{w}_1 = ((0.8)2\pi, 0)$,$\mathbf{w}_2 = (0, (0.6)2\pi)$. Note this is an already normalized pair of lattices ($b = 1$). Since $\mathbf{w}_1 = 2\mathbf{v}_1$ and $\mathbf{w}_2 = 4\mathbf{v}_2 - 2\mathbf{v}_1$, we have:

$$H = \begin{bmatrix} 2 & -2 \\ 0 & 4 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \Longrightarrow \Lambda_\alpha/\Lambda_\beta = \mathbb{Z}_2 \oplus \mathbb{Z}_4.$$

Besides, the two generators of the quotient of lattices are the classes $\bar{\mathbf{v}}_1$ of order 2 and $\bar{\mathbf{v}}_1 - \bar{\mathbf{v}}_2$ of order 4 (note that in this case we could also choose $\bar{\mathbf{v}}_2$ as a generator of order 4 – see Fig. 5.3). The associated spherical code in $\mathbb{R}^4$ will have $(0.8, 0, 0.6, 0)$ for initial vector, as expected, and the group composed by eight matrices. $G = \{A^r.B^s, 0 \leq r \leq 1, 0 \leq s \leq 3$, where $A = [\text{Rot}[2\pi(1/2)], \text{Identity}]$ and $B = [\text{Rot}[2\pi(-1/4)], \text{Rot}[2\pi(1/4)]]$.

Table 5.1 Examples of commutative group codes in $\mathbb{R}^n$, $n = 4, 6, 8, 16$, constructed through the quotient of A_2, D_3, D_4, E_8 by "rectangular" sublattices

n	M	$d_{\min}$	Upper bound	Group
4	141,180	0.012706	0.0127061	$\mathbb{Z}_{141180}$
4	423,540	0.00733585	0.00733588	$\mathbb{Z}_{423540}$
6	32	1.1547	1.26069	$\mathbb{Z}_2 \oplus \mathbb{Z}_4^2$
6	2048	0.318581	0.320294	$\mathbb{Z}_8 \oplus \mathbb{Z}_{16}^2$
8	648	0.707107	0.736258	$\mathbb{Z}_3 \oplus \mathbb{Z}_6^3$
8	10,368	0.366025	0.369712	$\mathbb{Z}_6 \oplus \mathbb{Z}_{12}^3$
16	65,536	0.707107	0.780361	$\mathbb{Z}_2 \oplus \mathbb{Z}_4^6 \oplus \mathbb{Z}_8$
16	16777,216	0.382683	0.392069	$\mathbb{Z}_4 \oplus \mathbb{Z}_8^6 \oplus \mathbb{Z}_{16}$

Their minimum distances approach the upper bound Proposition 5.6

In [4] it is studied the existence of orthogonal sublattices of A_2, D_3,D_4, E_8, which (Chap. 2, 2.3) are the densest lattices in dimensions 2, 3, 4, and 8, and it is obtained the spherical codes in the double of these dimensions which approaches the bound of Proposition 5.3 particularly when M increases (Table 5.1).

In what follows, $\mathscr{C}(M, n, d)$ denotes a commutative group code $\mathscr{C}$ in $\mathbb{R}^n$ with M points and minimum distance equal to d. A $\mathscr{C}(M, n, d)$ is said to be *optimum* if d is the largest minimum distance for a fixed M and n.

As it is well-known, the minimum distance of a group code $\mathscr{C}$, generated by a finite group G, may vary significantly depending on the choice of the initial vector u. This problem still does not have a general solution, but have been studied in some important special cases, including reflection group codes [84] and permutation group codes [37]. Biglieri and Elia have shown in [11] that, for a fixed cyclic group code, the problem can be formulated as a linear programming problem. They also discussed the efficiency of some of these codes and remarked on the hardness of obtaining the best cyclic group code for a given cardinality M and dimension n.

In the search for the best commutative group code $\mathscr{C}(M, n, d)$, for fixed values of M and n, we must first find the set $G_n(M)$ of all commutative groups in $\mathscr{O}_n$ of order M and then the best initial vector for each one of those groups. An optimum code will be one which has the largest minimum distance in this set. The total number of $G_n(M)$ is related with the Euler number of divisors of M and is of order $\binom{M/2}{n/2}$. It is worth to remark that even isomorphic groups must be considered, since the resulting minimum distance may vary depending on which representation in $\mathscr{O}_n$ is taken for each group, i.e., two isomorphic groups may generate two non-isometric spherical codes, as illustrated in Fig. 5.5.

An approach to this problem is based on the association between commutative group codes and lattices described here. An important step of the algorithm derived in [106] is to reduce the number of cases to be analyzed by discarding isometric codes. This is done via the following proposition which consider generator matrices in the Hermite normal form (Chap. 3, 3.2).

Table 5.2 Some best commutative group codes of order M in $\mathbb{R}^6$ with $50 \leq M \leq 1000$, initial vector $\mathbf{c} = (c_1, 0, c_2, 0, c_3)$, generators (Gen) given by rotation blocks where b_{i1}, b_{i2}, b_{i3} as in Proposition 5.3 and bound from Proposition 5.6

M	$d_{\min}$	c_1	c_2	c_3	Group	Gen	Bound
50	0.9763	0.604	0.506	0.615	$\mathbb{Z}_{50}$	(7,6, 34)	1.091
250	0.6180	0.525	0.625	0.668	$\mathbb{Z}_5^2 \oplus \mathbb{Z}_{10}$	(50, 0, 0), (50, 50, 0), (25,25,25)	0.436
500	0.5046	0.577	0.577	0.577	$\mathbb{Z}_5 \oplus \mathbb{Z}_{10}^2$	(100, 0, 0), (50, 50, 0), (50, 0, 50)	0.5116
750	0.4367	0.587	0.549	0.594	$\mathbb{Z}_{750}$	(187,229,560)	0.5116
1000	0.3979	0.560	0.632	0.535	$\mathbb{Z}_{1000}$	(319,694,45)	0.4065

Proposition 5.8 ([106]) *Every commutative group code $\mathscr{C}(M, 2L, d)$, generated by a group $G \in \mathscr{O}_{2L}$ free of 2×2 reflection blocks, is isometric to a code obtained as image by $\Phi_{\mathbf{c}}$ of a lattice $\Lambda_G(\mathbf{c})$ which generator matrix T satisfies the following conditions:*

1. *T is in the Hermite Normal Form.*
2. $\det(T) = M^{L-1}$.
3. *There is a matrix W, with integer elements satisfying $WT = MI_L$, where I_L is the $L \times L$ identity matrix.*
4. *The elements of the diagonal of T satisfy $T(i,i) = \dfrac{M}{a_i}$ where a_i is a divisor of M and $(a_i)^i \cdot (a_{i+1} \cdots a_L) \leqslant M$, $\forall i = 1, \ldots, L$.*

As an example of application of the proposition above, let us consider $M = 128$. There are, up to isomorphism, only 4 abstract commutative groups or order 128: $\{Z_{128}, Z_2 \times Z_{64}, Z_4 \times Z_{32}, Z_8 \times Z_{16}\}$. However, for $n = 2L = \{4, 6, 8\}$, there are $\{2016, 41664, 635376\}$ distinct representations of them in $\mathscr{O}_n$. After discarding isometric codes by using Proposition 5.8, we must consider just $\{71, 2539, 55789\}$ representations, respectively [106]. Then the initial vector problem can be solved only for those cases.

In Table 5.2, it is shown some best commutative group codes in $\mathbb{R}^6$ [106].

5.3.4 Commutative Group Codes and Codes on Graphs

Commutative group codes can also be viewed as a graph or a coset code [40] on a flat torus with the graph distance (minimum number of edges from one vertex to another). They are also geometrically uniform in this context. This is the approach presented in [30]. As an example, consider the codes presented in Fig. 5.5 where each edge of the flat torus box is subdivided into $M = 25$ segments with the underlined grid associated to this subdivision. Considering also the boundary identification, those grids define a graph on each flat torus with vertices associated to the group Z_{25}^2. On the left we have the code C_1 generated by the element $(b_1, b_2) = (1, 7)$, which is a cyclic code in $Z_{25} \times Z_{25}$ of order $M = 25$ and minimum graph or

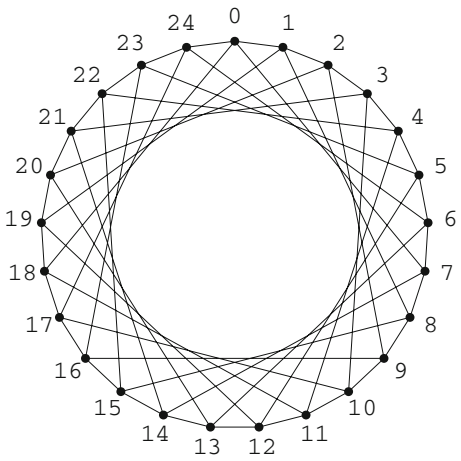

Fig. 5.6 The cyclic group code of Fig. 5.5 – left considered as generated by $(b_1, b_2) = (4, 3)$ and viewed as the circulant graph $C_{25}(1, 7)$

Lee distance equal to 7 and therefore a 3 – error correcting code (see Chap. 3, 3.2). Note that this code can also be generated by the element $(4, 3)$ and is a perfect code in $\mathbb{Z}_{25}^2$ (Chap. 3, Example 3.8). On the right of Fig. 5.5, we have the cyclic code C_2 generated by $(b_1, b_2) = (1, 10)$, which has a minimum graph distance 5. Thus, viewed as graph codes, the code on the left on Fig. 5.5 is better than the code on the right in opposition to the performance of their images as spherical codes in $\mathbb{R}^4$. To the code C_1 generated by $(4, 3)$, $C_1 = \{c_{1k} = k(4, 3) \text{ Mod } 25, k = 0, \cdots, 24\}$ (numbered in this order), it is associated the circulant graph $C_{25}(1, 7)$ (see Fig. 5.6). This circulant graph is equivalent to the graph given by the rotated squared grid defined by the elements of C_1. (Note that each point c_{1k} in this new graph is connected to c_{1j}, where $j = \pm 1$ Mod 25 or $j = \pm 7$ Mod 25.) This geometrical view through quotient of lattices may provide tools to analyze circulant and Cayley graphs which are used in parallel computing schemes [30].

5.4 Spherical Codes on Layers of Tori

5.4.1 Codes for the Gaussian Channel

Although commutative group codes discussed in the last section have applications based on their rich structure, those codes are not good in general for small distance concerning their trade-off between distance and number of points, since they are placed in just one torus of the sphere.

Flat tori layers can be used to construct spherical codes which combine the good structure of commutative group codes in each layer with a better packing density. A *torus layer spherical code (TLSC)* [105] can be generated by a finite set of orthogonal matrices and thus inherited group structure and homogeneity allowing efficient storage and decoding process, which is attached to lattices in the half of the code dimension.

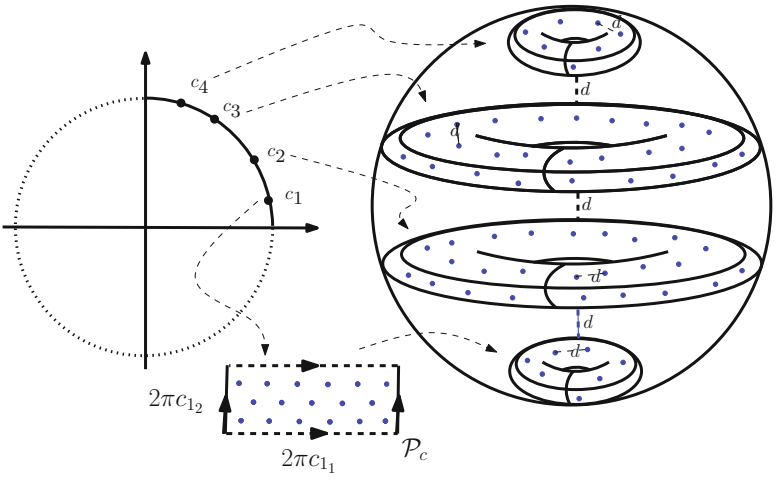

Fig. 5.7 An illustration of the construction of a four-dimensional torus layer spherical code

To design these codes, given a distance $d \in (0, \sqrt{2}]$, we first define a collection of tori in S^{2L-1} such that the minimum distance between any two of these tori is at least d. This can be done (Proposition 5.1) by designing a spherical code in $\mathbb{R}^L$ with minimum distance d and positive coordinates. Then, for each one of these tori, a finite set of points is chosen in $\mathbb{R}^L$ such that the distance between any two points, when embedded in $\mathbb{R}^{2L}$ by the standard parametrization (5.1), is greater than d, according to Proposition 5.2. This set of points may belong to a L-dimensional lattice, restricted to a hyperbox $\mathscr{P}_{\mathbf{c}}$ (5.2), chosen to approach a good packing density in $\mathbb{R}^L$ as described in Sect. 5.3. The $TLSC(2L, d)$ is the union of the commutative group codes associated to each one of the chosen tori. Figure 5.7 illustrates the construction of a $TLSC(4, d)$.

General spherical codes without any group structure, particularly for small distances and higher dimension, may present a much higher number of codewords for the same minimum distance since the packing density have greater bounds (attached to the packing density in the previous dimension). One advantage of the *TLSC* is regarding the simple coding/decoding processes. In [105], starting from a rectangular sublattice of the Leech lattice it is presented a *TLSC* in dimension 48 with more than 2^{113} points placed in 24 layers of flat tori with minimum distance 0.1. This code is generated by using just 12 matrices. For not very small distances (or non-asymptotic context), a torus layer spherical code may have comparable performance to other well-known spherical codes such as apple-peeling [35], wrapped [47], and laminated [48] codes, as illustrated in Table 5.3, and have the advantage of being constructive and homogeneous in each layer. For very small distance and higher dimension, the expected performance will decrease.

Table 5.3 Four-dimensional code sizes at various minimum distances

d	TLSC(4,d)	Apple-peeling	Wrapped	Laminated
0.5	172	136	*	*
0.4	308	268	*	*
0.3	798	676	*	*
0.2	2,718	2,348	*	*
0.1	22,406	19,364	17,198	16,976
0.01	2.27×10^7	1.97×10^7	2.31×10^7	2.31×10^7

*Unknown values

5.4.2 *Application: Coding for Continuous Alphabet Sources*

Curves on a sphere with good length, "distance," and structure are suitable to the following communication problem. A real value x (say, belonging to the interval $[0, 1]$) is to be transmitted over a power-constrained Gaussian channel of dimension n to a receiver. This can be achieved by first quantizing x, as in Sect. 2.5.1, and then encoding the quantized bits into a classical code. However, this "separated" approach necessarily incurs quantization errors and, ultimately, communication delay. Another possibility is to map the source, via a continuous (or piecewise continuous) function $\mathbf{s} : [0, 1) \to \mathbb{R}^L$, and then transmit it over the channel. Such a function is, indeed, a *curve* in $\mathbb{R}^n$. On the receiver side, a signal

$$\mathbf{y} = \mathbf{s}(x) + \mathbf{n}$$

is observed. The objective is to recover an estimate $\mathbf{x}$ of the sent value, attempting to minimize the mean square error (mse) $E[(x - \hat{x})^2]$ between the estimate and the true value.

The problem of building curves for such a transmission was first discussed by C. Shannon, pioneer of information theory in 1949 [91]. It is a remarkable result that if x has normal distribution and $n = 1$, the *optimal* distortion is achieved by the scaled identity mapping, i.e., $s(x) = \alpha x$ (e.g., [44]). For higher dimensions, however, the solution is not so simple. Perhaps surprisingly, the construction of continuous curves can be addressed by using lattices, a discrete structure. This relation is the subject of the next pages.

As a first example, consider the piecewise-linear mapping depicted in Fig. 5.8. If a receiver observes $\mathbf{y} = \mathbf{s}(x) + \mathbf{n}$, there are *two* possible types of errors:

1. *Small errors*: if the error is concentrated in a sufficiently small region, the closest curve value will be very close to the sent one.
2. *Large errors (or "jumps")*: in this case the noise is high enough so that the estimate "jumps" between two laps (or pieces) of the curve.

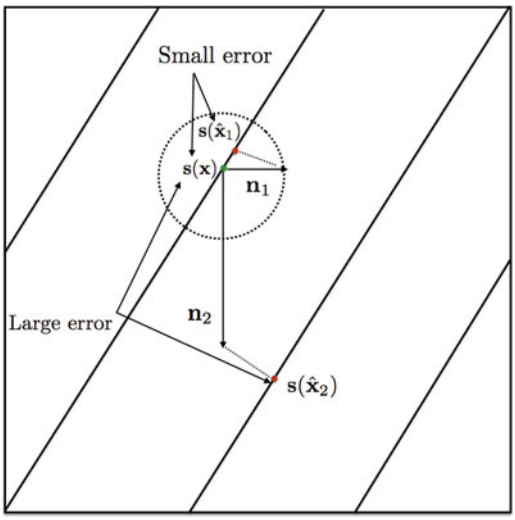

Fig. 5.8 Illustration of small and large errors

Large errors can be prevented by separating the laps apart, while for small errors it is desirable that the curve is as long as possible. These two objectives are, of course, contrary.

In the example of Fig. 5.8, the mapping $\mathbf{s} : [0, 1] \to \mathbb{R}^2$ can be defined as

$$\mathbf{s}(x) = (3x - \lfloor 3x \rceil, 2x - \lfloor 2x \rceil), \tag{5.6}$$

or if we denote the mod-1 operation by $x \bmod 1 = x - \lfloor x \rceil$, we can write, in a concise way, $\mathbf{s}(x) = (3x, 2x) \bmod 1$. Now the distance ρ_c between two pieces of this curve is the smallest distance between two integer translations of the straight line $(3x, 2x)$ or by homogeneity

$$\rho_c = \min_{u \in \mathbb{Z}^2} \min_{x \in \mathbb{R}} \|(3, 2)x - \mathbf{u}\| .$$

The first minimum is clearly obtained by projecting $\mathbf{u}$ onto the vector $(-2, 3)$ (orthogonal to $(3, 2)$). Therefore, we see that *the smallest distance between two laps of the curve is equal to the shortest vector of the projection of* $\mathbb{Z}^2$ *along* $(-2, 3)$.

This argument can be extended to any mapping of the form

$$\mathbf{s}(x) = \alpha(\mathbf{a}x(\bmod 1)),$$

where $\mathbf{a} \in \mathbb{Z}^L$, and α is a scaling factor chosen conveniently in order to satisfy the power constraint. Given a vector $\mathbf{a} \in \mathbb{Z}^L$, we may make a step further and consider the curves

$$\mathbf{s}(x) = \phi_{\mathbf{c}} \left(\frac{2\pi}{\sqrt{L}} \mathbf{a}x (\bmod 1) \right), \tag{5.7}$$

where $\mathbf{c} = \hat{\mathbf{e}} = (1/\sqrt{L})(1, \ldots, 1)$ (or we may consider different vectors) and ϕ is the torus mapping (5.1). These closed curves are contained on a flat torus T_c in the sphere of $\mathbb{R}^{2L}$ and are highly homogeneous (all their curvatures are constant [27]). From Proposition 5.1, the distance between the "laps" of the new curve is approximately the distance between two lines in the (mod 1) map. The length of the curve is given by $2\pi \|\mathbf{a}\| / \sqrt{L}$.

To summarize, good codes for continuous alphabet sources are related to curves that can be designed by choosing a vector $\mathbf{a} \in \mathbb{Z}^L$ such that:

1. The norm of $\mathbf{a}$ is large.
2. The projection of $\mathbb{Z}^L$ along the orthogonal hyperplane to $\mathbf{a}$ has large shortest vector.

As we will see next, these two objectives can be attained by finding projections of the cubic lattice $\mathbb{Z}^L$ with good packing density. In the next subsection, we consider the study of projections of lattices in a greater generality.

The problem of finding good projections of the cubic lattice (and thus curves for this communication problem) can be independently formulated as the "fat strut" [100] problem as follows. We want to find a point $\mathbf{a} \in \mathbb{Z}^L$ such that the cylinder anchored at the origin and $\mathbf{a}$ does not contain any other lattice point and has maximal volume.

Projections of Lattices The previous discussion motivates the study of *projections of lattices* along a vector space of $\mathbb{R}^L$. In fact, many notable lattices seen in Chap. 2 are naturally characterized through projections and intersections with hyperplanes. Furthermore, projections are strongly connected to the study of more advanced lattice structures, such as *laminated* and *perfect* lattices. The interested reader is invited to consult the references [26, Chap. 6] and [68] for a thorough account on these topics.

We need some preliminary definitions on the linear algebra of projections along subspaces of $\mathbb{R}^L$. Let V be a vector subspace of $\mathbb{R}^L$, for example, a plane in $\mathbb{R}^3$ or a hyperplane in $\mathbb{R}^L$. Denote by $V^\perp$ its orthogonal complement (in the case of a plane, it is a straight line, generated by one single vector). Any vector $\mathbf{x} \in \mathbb{R}^L$ can be decomposed in a unique way as $\mathbf{x} = \mathbf{v} + \mathbf{v}^\perp$, where $\mathbf{v} \in V$ and $\mathbf{v}^\perp \in V^\perp$. Given $\mathbf{x} \in \mathbb{R}^L$, we define the *orthogonal projection* of $\mathbf{x}$ in V (or along $V^\perp$) as $P_V(\mathbf{x}) = \mathbf{v}$ and $P_{V^\perp}(\mathbf{x}) = \mathbf{v}^\perp$. One can show (e.g., [70, p. 430]) that $P_{V^\perp}(\mathbf{x}) = P\mathbf{x}$, where

$$P = (I - V(V^t V)^{-1} V^t).$$

We call P the orthogonal *projector* (or projection matrix) onto $V^\perp$.

Let $\Lambda \subset \mathbb{R}^L$ be a lattice. The *projection* of Λ in $V^\perp$ is denoted by $P_{V^\perp}(\Lambda)$. If B is a generator matrix and P is the projection matrix above, we have

$$P_{V^\perp}(\Lambda) = \{P\mathbf{x} : \mathbf{x} \in \Lambda\} = \left\{PB\mathbf{u} : \mathbf{u} \in \mathbb{Z}^L\right\}. \tag{5.8}$$

The projection of lattice along a vector space is certainly closed under addition and subtraction. Perhaps more surprising is the fact that it need not be discrete, as seen in the next example.

Example 5.4 Let $\Lambda = \mathbb{Z}^2$ and $\mathbf{v} = (1, \sqrt{2})$. A projection matrix onto $\mathbf{v}^\perp$ is given by

$$P = \begin{pmatrix} \frac{2}{3} & -\frac{\sqrt{2}}{3} \\ -\frac{\sqrt{2}}{3} & \frac{1}{3} \end{pmatrix}.$$

Applying the orthogonal transformation defined by matrix

$$Q = \begin{pmatrix} \sqrt{\frac{2}{3}} & -\frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} & \sqrt{\frac{2}{3}} \end{pmatrix}$$

to the projection set (5.8), we have

$$P_{\mathbf{v}^\perp}(\mathbb{Z}^2)Q = \left\{QP\mathbf{x} : \mathbf{x} \in \mathbb{Z}^2\right\} = \frac{1}{\sqrt{3}}\left\{(\sqrt{2}x_1 + x_2, 0) : x_1, x_2 \in \mathbb{Z}\right\}.$$

It is an interesting exercise of combinatorics to use the pigeonhole principle to show that the above set is *not* discrete.
From the characterization of lattices as discrete sets (Theorem 2.1), it follows that the projection need not be a lattice. But as may be easily seen, there are examples in which the projection is indeed a lattice.

Example 5.5 The simplest example is the $\mathbb{Z}^L$ lattice. Its projection along the hyperplane orthogonal to any of the canonical vectors is equivalent to $\mathbb{R}^{L-1}$.
For a vector $\mathbf{v} \in \mathbb{R}^L$, we denote the hyperplane orthogonal to $\mathbf{v}$ by $\mathbf{v}^\perp$, i.e,

$$\mathbf{v}^\perp = \{\mathbf{x} \in \mathbb{R}^n : x_1 v_1 + \ldots + x_L v_L = 0\}.$$

The following proposition characterizes when the projection of a lattice is a discrete set and what does the new lattice "look like." Recall from Chap. 2 that a vector $\mathbf{x}$ in a lattice Λ is said to be *primitive* if it can be extended to a basis of Λ. The following proposition is rather well-known (an explicit proof can be found in [17]):

Proposition 5.9 *Let* $\mathbf{v}$ *be a primitive vector of a full-rank lattice* $\Lambda \subset \mathbb{R}^L$. *The following properties hold:*

(i) *The set* $P_{\mathbf{v}^\perp}(\Lambda)$ *is a lattice.*
(ii) *The volume of* $P_{\mathbf{v}^\perp}(\Lambda)$ *is given by*

$$V(P_{\mathbf{v}^\perp}(\Lambda)) = \frac{V(\Lambda)}{\|\mathbf{v}\|} \tag{5.9}$$

(iii) $P_{\mathbf{v}^\perp}(\Lambda)^* = \Lambda^* \cap \mathbf{v}^\perp$.

Item (ii) gives a very simple way of computing the discriminant of the projection, while item (iii) provides a simple characterization for its dual.

Example 5.6 Recall that A_L is defined in Sect. 2.4 as

$$A_L = \left\{\mathbf{x} \in \mathbb{Z}^{L+1} : x_1 + \cdots + x_L = 0\right\}.$$

In other words, if $\mathbf{v} = (1, \ldots, 1) \in \mathbb{Z}^{L+1}$, then $A_L = \mathbb{Z}^{L+1} \cap \mathbf{v}^{\perp}$. From the previous theorem, we have

$$A_L^* = P_{\mathbf{v}'}(\mathbb{Z}^{L+1}),$$

i.e., the dual of A_L is the projection of $\mathbb{Z}^{L+1}$ along $\mathbf{v}^{\perp}$.
Recalling the curve-packing problem in the previous subsection, we were to choose a vector $\mathbf{a} \in \mathbb{Z}^n$ such that:

1. The norm of $\mathbf{a}$ is large.
2. $P_{\mathbf{a}^{\perp}}(\mathbb{Z}^L)$ has a large shortest vector.

Or, having fixed the norm of $\mathbf{a}$, we would like maximize the minimum norm of $P_{\mathbf{a}^{\perp}}(\mathbb{Z}^L)$, say, $\lambda_1(\mathbf{a})$. Recalling the formula for the center density, and in light of Proposition 5.9, item (ii), this is equivalent to finding projections of $\mathbb{Z}^L$ with good packing density.

The Lifting Construction [100] gives a general solution for this problem. It is shown in [99] how to construct sequences of lattices which are, up to equivalence relations, similar to projections of $\mathbb{Z}^L$ and arbitrarily close to any target $(L-1)$-dimensional lattice.

Further Extensions

By using layers of tori, it is possible to generalize the construction in [108] as follows [18]. Let $T = \{T_1, \ldots, T_M\}$ be a collection of M tori in the unit sphere of $\mathbb{R}^{2L}$. For each one of these tori, consider closed curves of the form

$$\mathbf{s}_{T_c}(x) = \Phi_{\mathbf{c}}(x 2\pi \hat{\mathbf{u}}), \tag{5.10}$$

where $C = \operatorname{diag}(c_1, \ldots, c_L)$, $\hat{\mathbf{u}} = \mathbf{u}C = (c_1 u_1, \ldots, c_L u_L)$, $\Phi_{\mathbf{c}}$ is given by (5.1) and $x \in [0, 1]$.

Now let $\operatorname{Len} = \sum_{j=1}^{M} \operatorname{Len}_j$, where Len_j is the length of $\mathbf{s}_{T_j}$. We split the unit interval $[0, 1]$ into M pieces according to the length of each curve:

$$[0, 1) = I_1 \cup I_2, \ldots \cup I_M, \text{ where}$$

$$I_k = \left[\frac{\sum_{j=1}^{k-1} \operatorname{Len}_j}{\operatorname{Len}_j}, \frac{\sum_{j=1}^{k} \operatorname{Len}}{\operatorname{Len}}\right), \text{ for } k = 1, \ldots, M.$$

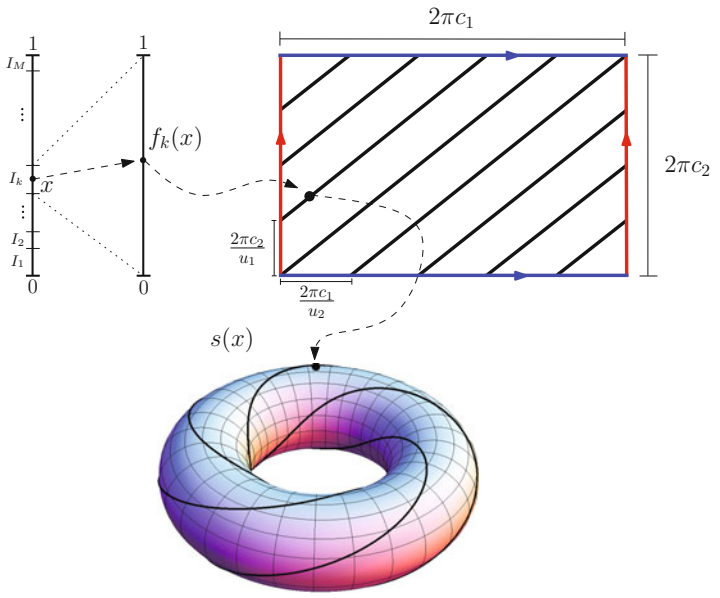

Fig. 5.9 Encoding process

and consider the bijective mapping

$$f_k : I_k \to [0, 1)$$
$$f_k(x) = \frac{x - \sum_{j=1}^{k-1} L_j/L}{l_k/L}.$$

Then the full encoding map $\mathbf{s}$ can be defined by

$$\mathbf{s}(x) := \mathbf{s}_{T_k}(f_k(x)), \text{ if } x \in I_k. \tag{5.11}$$

and is represented in Fig. 5.9. Finding a good collection of tori (i.e., such that each of them is separated at least a certain distance from each other) is related to finding a good spherical code of a given minimum distance, which can be approached through standard techniques (and even using layers of torus, as the construction presented in the previous section). On the other hand, finding good curves in each torus is equivalent to finding good projections of the rectangular lattice $c_1\mathbb{Z} \oplus \cdots \oplus c_L\mathbb{Z}$. In this case, it is possible to generalize the Lifting Construction and exhibit sequences of projections of $c_1\mathbb{Z} \oplus \cdots \oplus c_L\mathbb{Z}$ converging to any $(L-1)$-dimensional lattice, as in the later case. Through this, it is possible to meaningfully increase the length of the curves produced.

Discrete sets of points selected on a continuous closed curve on a flat torus as described in this section have also been used in [110] to approach good commutative group codes which are cyclic.