Lattices and Spherical Codes

Sueli I. R. Costa

University of Campinas
sueli@ime.unicamp.br

London-ish Lattice Coding & Crypto Meeting
January, 15th, 2018

Abstract

Lattices in $\mathbb{R}^n$ with orthogonal sublattices are associated with spherical codes in $\mathbb{R}^{2n}$ generated by a finite commutative group of orthogonal matrices. They can also 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. In the continuous case, the "packing density" of these curves relies on the search for projection lattices with good packing density. A brief survey and recent developments on this topic is presented here.

Summary

- Spherical and Geometrically Uniform Codes;
- Flat Tori;
- Commutative Group Codes, Flat Tori and Lattices;
- Lattice bounds: Good and optimum commutative group codes;
- Spherical codes in layers of flat tori;
- Codes for continuous alphabet sources;
- Recent developments/perspectives;

General References

- T. Ericson, V. Zinoviev, Codes on Euclidean Spheres, North Holland, 2001;
- S. Costa, F. Oggier, A. Campello, J-C. Belfiore, E. Viterbo, Lattices Applied to Coding for Reliable and Secure Communications, Springer, 2018.

Spherical and Geometrically Uniform Codes

Consider the sphere of radius a in $\mathbb{R}^n$,

$$\mathcal{S}^{n-1}(a) = \{\mathbf{x} \in \mathbb{R}^n;\ \|\mathbf{x}\| = a\}$$

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, $\mathcal{S}^{n-1} = \mathcal{S}^{n-1}(1)$ and all the conclusions will be extended by similarity to a sphere of radius a.

Spherical and Geometrically Uniform Codes

Two dual optimization (packing) problem, which have several applications in physics, chemistry, architecture and signal processing:

Problem 1: Given a dimension n and an integer number $M > 0$, to 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 $d > 0$, to find a spherical code with the biggest number M of points such that each two of them are at distance at least d.

Spherical and Geometrically Uniform Codes

Codes which are solutions for one of these problems are called *optimal spherical codes*.
In dimension 2: regular polygons.
In dimesion 3: the solution of Problem 1 is only known for $1 \leq M \leq 12$ and for $M = 24$.
For $M = 2, 3, 4$ (antipodal points, equilateral triangle at the equator, regular tetrahedron).
For $M = 8$:

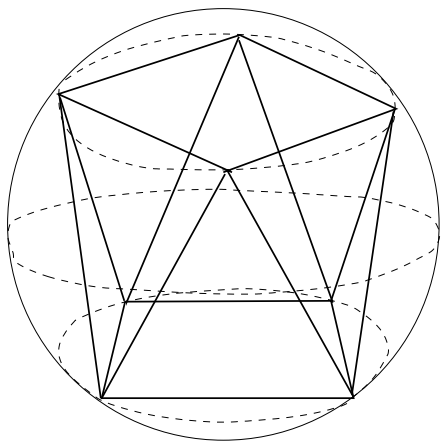


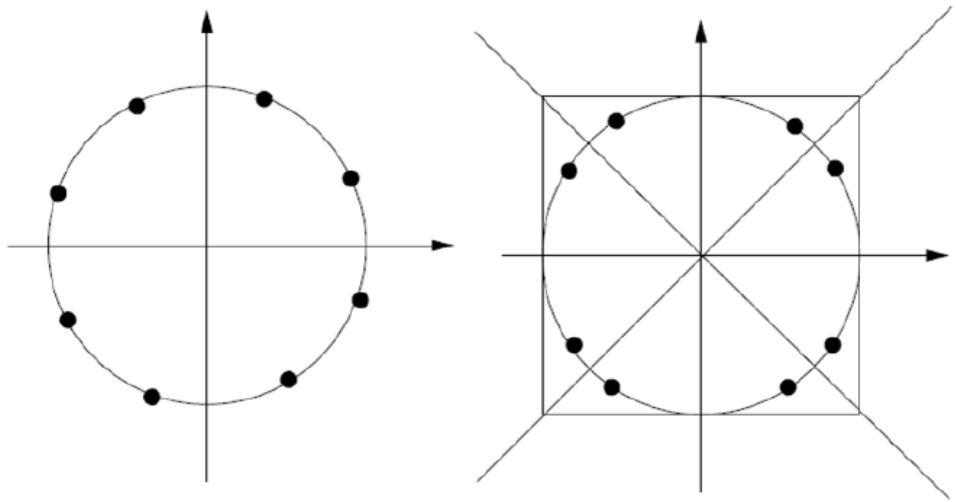
Figura: Antiprism with 8 vertices

- $M = 2n$ in $\mathbb{R}^n$: biorthogonal code (permutations of $(0, 0, ..., \pm 1)$);
- $M = n + 1$ in $\mathbb{R}^n$: simplex code ($\mathbf{y}_i$ permutations of $\frac{1}{\sqrt{n+n^2}}(1, 1, \ldots, 1, -n) \in \mathbb{R}^{n+1}$).
  $\sum_{j=1}^{n+1} y_{ij} = 0$ (hyperplane), $\sum_{j=1}^{n+1} y_{ij}^2 = n + n^2$.
  Normalize and rotate $\rightarrow$ squared distance between two code words $= 2 + \frac{2}{n}$;
- $\Lambda \subset \mathbb{R}^n$ a lattice, $\mathcal{C} \subset \Lambda \rightarrow$ lattice vectors of a fixed norm.

- Group Codes (Slepian 1958)
  Finite sets on an n-dimensional sphere generated by the action of a group of orthogonal matrices.
- Subsequent articles 70s – 90s: Biglieri, Elia, Loelinger, Caire, Ingemarsson
- Geometrically Uniform Codes (Forney 1991)
  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 $f(S) = S$.

Highly desirable properties that come from homogeneity: the same distance profile, congruent Voronoi regions (same error transmission probability) for each codeword.

Examples of group codes in S^1:



8-PSK

A rotation group on the left, a group of reflexitions on the right (the initial vector matters).

Lattices in $\mathbb{R}^n$ with orthogonal sublattices can be used to construct spherical codes in $\mathbb{R}^{2n}$ generated by commutative groups of orthogonal matrices.
Those codes will be contained on flat tori.

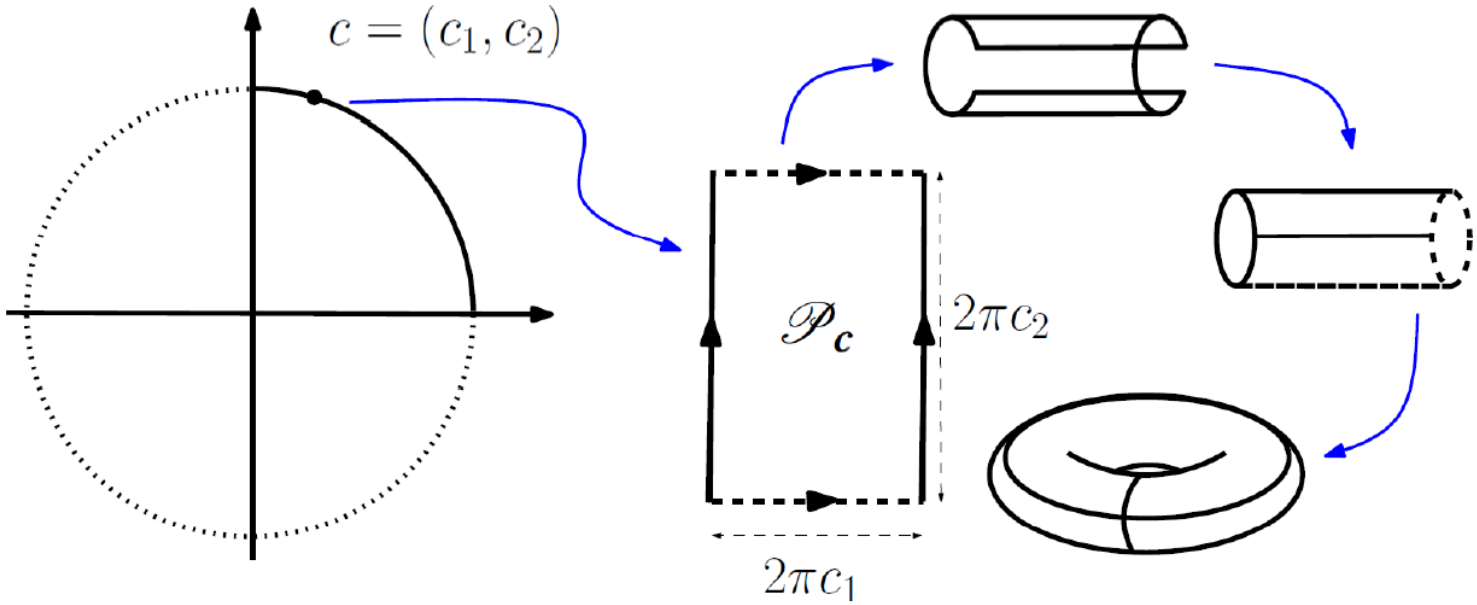
Flat Tori

A 2-dimensional flat torus.
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

$$\Phi_{\mathbf{c}}(u_1, u_2) = (c_1 \cos(\frac{u_1}{c_1}), c_1 \sin(\frac{u_1}{c_1}), c_2 \cos(\frac{u_2}{c_2}), c_2 \sin(\frac{u_2}{c_2})).$$

This is a doubly periodic map 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.

$$T_c = \Phi_c(\mathbb{R}^2) = \Phi_c([0, 2\pi c_1) \times [0, 2\pi c_2)).$$



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

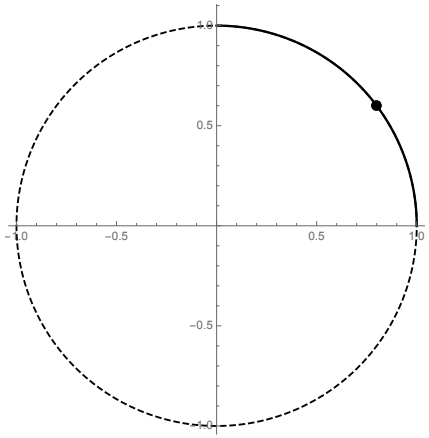
The unit sphere $S^{2L-1} \subset \mathbb{R}^{2L}$ can be foliated by flat tori (also called Clifford Tori): $\mathbf{c} = (c_1, c_2, .., c_L) \in \mathcal{S}^{L-1}, c_i > 0, \sum_{i=1}^{L} c_i^2 = 1$, and $\mathbf{u} = (u_1, u_2, \ldots, u_L) \in \mathbb{R}^L$, let $\Phi_{\mathbf{c}} : \mathbb{R}^L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

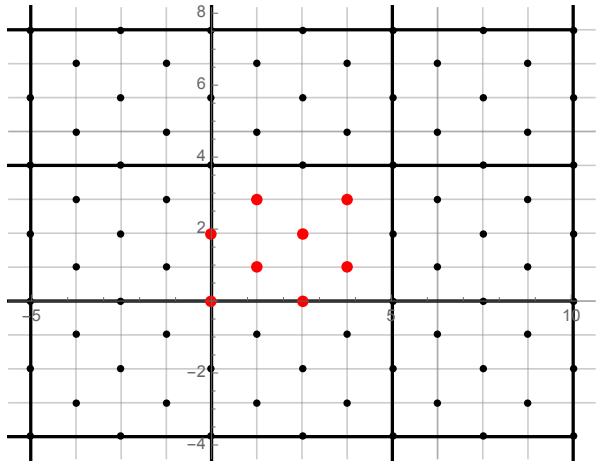
$$\Phi_{\mathbf{c}}(\mathbf{u}) = \left(c_1 \cos(\frac{u_1}{c_1}), c_1 \sin(\frac{u_1}{c_1}), \ldots, c_L \cos(\frac{u_L}{c_L}), c_L \sin(\frac{u_L}{c_L}) \right). \tag{1}$$

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

$$T_c = \phi_c(\mathbb{R}^l) = \phi_c(\mathcal{P}) \subset S^{2L-1}.$$

Any vector of $\mathcal{S}^{2L-1}$ belongs to one and only one of these flat tori.



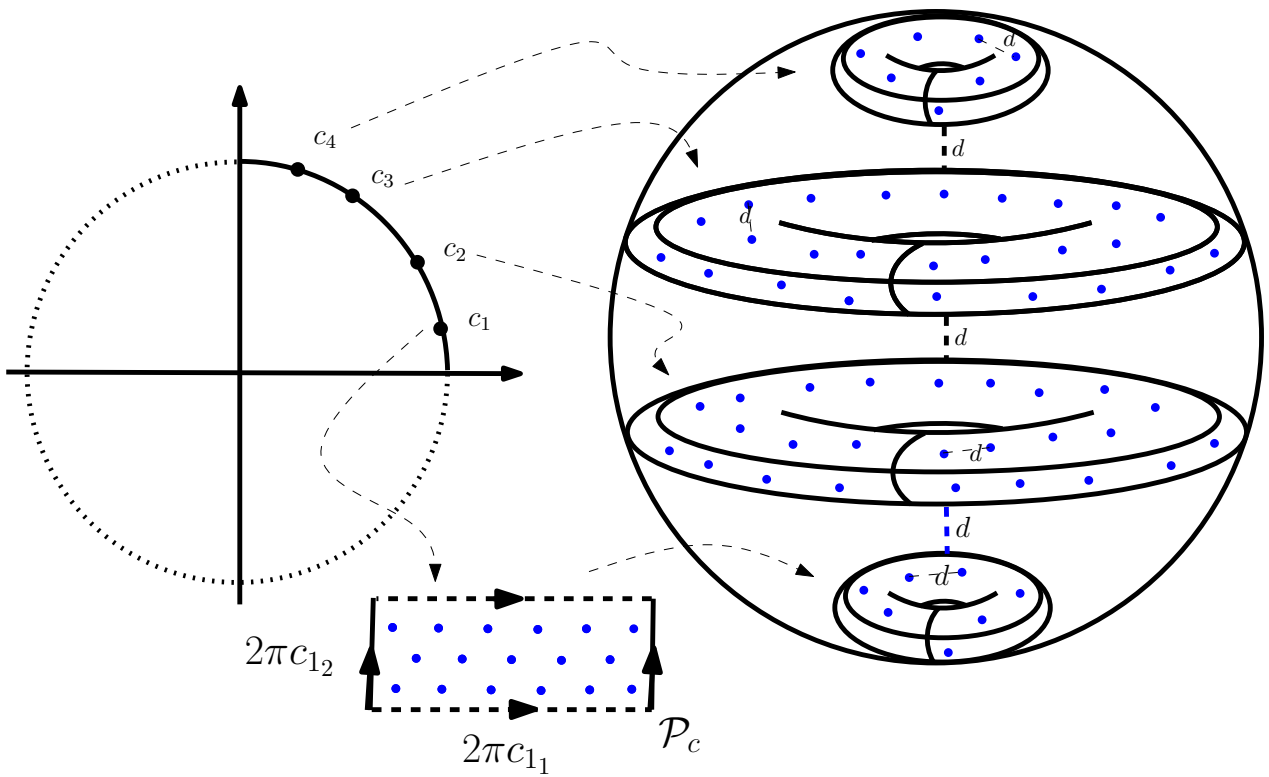


The tesselation of the plane associated to $\mathbf{c} = (0.8, 0.6) \in S^1$, and a lattice Λ (black dots) which contains $2\pi c_1\mathbb{Z} \times 2\pi c_2\mathbb{Z}$ as a rectangular sublattice. In this case $\phi_{\mathbf{c}}(\Lambda)$ is a spherical code in $S^3 \subset \mathbb{R}^4$ with $M = 8$.

Proposition

Let $T_{\mathbf{b}}$ and $T_{\mathbf{c}}$ be two flat tori, defined by unit vectors $\mathbf{b}$ and $\mathbf{c}$ with non negative 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

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



Distance between two points $\Phi_{\mathbf{c}}(\mathbf{u})$ and $\Phi_{\mathbf{c}}(\mathbf{v})$ on the same torus:

$$||\Phi_{\mathbf{c}}(\mathbf{u}) - \Phi_{\mathbf{c}}(\mathbf{v})|| = 2\sqrt{\sum c_i^2 \sin^2(\frac{u_i - v_i}{2c_i})} \tag{3}$$

Proposition

[VC03] Let $\mathbf{c} = (c_1, c_2, .., c_L) \in S^{L-1}$, $c_i > 0$, $c_\xi = \min_{1 \le i \le L} c_i \neq 0$, $\Delta = \|\mathbf{u} - \mathbf{v}\|$ *for* $\mathbf{u}, \mathbf{v} \in \mathcal{P}_c$. *Suppose* $0 < \Delta \le c_\xi$, *then*

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

Commutative Group Codes, Flat Tori and Lattices

Lattice bounds: Good and optimum commutative group codes

$\mathcal{O}_n =$ the multiplicative group of orthogonal $n \times n$ matrices
$\mathcal{G}_n(M) =$ the set of all order M commutative subgroups in $\mathcal{O}_n$.
A spherical *commutative group code* $\mathcal{C}$ is a set of M vectors which is the orbit of an initial vector $\mathbf{u}$ on the unit sphere $\mathcal{S}^{n-1} \subset \mathbb{R}^n$ by a given finite group $G \in \mathcal{G}_n(M)$:
$\mathcal{C} = G\mathbf{u} = \{g\mathbf{u}, g \in G\}$.
The *minimum distance* in $\mathcal{C}$ is:

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

A canonical form for a commutative group $G \in \mathcal{G}_n(M)$.

Proposition

All the matrices O_i of a commutative group $\mathcal{G} = \{O_i\}_{i=1}^{M}$ of $n \times n$ of orthogonal real matrices can simultaneously be put into a diagonal block canonical form through an orthogonal matrix Q:

$$Q^T O_i Q = \left[\mathrm{Rot}\left(\frac{2\pi b_{i1}}{M}\right), \ldots, \mathrm{Rot}\left(\frac{2\pi b_{iq}}{M}\right), \mu_{2q+1}(i), \ldots, \mu_n(i) \right], \tag{4}$$

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 geometric locus of a commutative group code:

Proposition

Every commutative group code of order M is, up to isometry, equal to a spherical code $\mathcal{X}$ 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 $n = 2L$, $\mathcal{X}$ 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 $\mathcal{X}$ is not contained in a hyperplane, $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$, where $\mathcal{X}_i$ is contained in the plane $\mathcal{P}_i = \{(x_1, \ldots, x_{2L+1}) \in \mathbb{R}^{2L+1}; x_{2L+1} = (-1)^i u_n\}$. Also, $\mathcal{X}_i$ is contained in the torus $T_{\mathbf{c}}$ of a sphere in $\mathbb{R}^{2L}$ with radius $(1 - u_n^2)^{1/2}$, where $\mathbf{c}_i^2 = u_{2i-1}^2 + u_{2i}^2$.

Lattice Connections

A $2L$-dimensional commutative group code is free from reflection blocks if its generator matrix group satisfies $2L = 2q = n$ as in the Proposition (no blocks

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

Commutative group codes in even dimension, whose generator matrices are free from reflections blocks, are directly related to lattices.

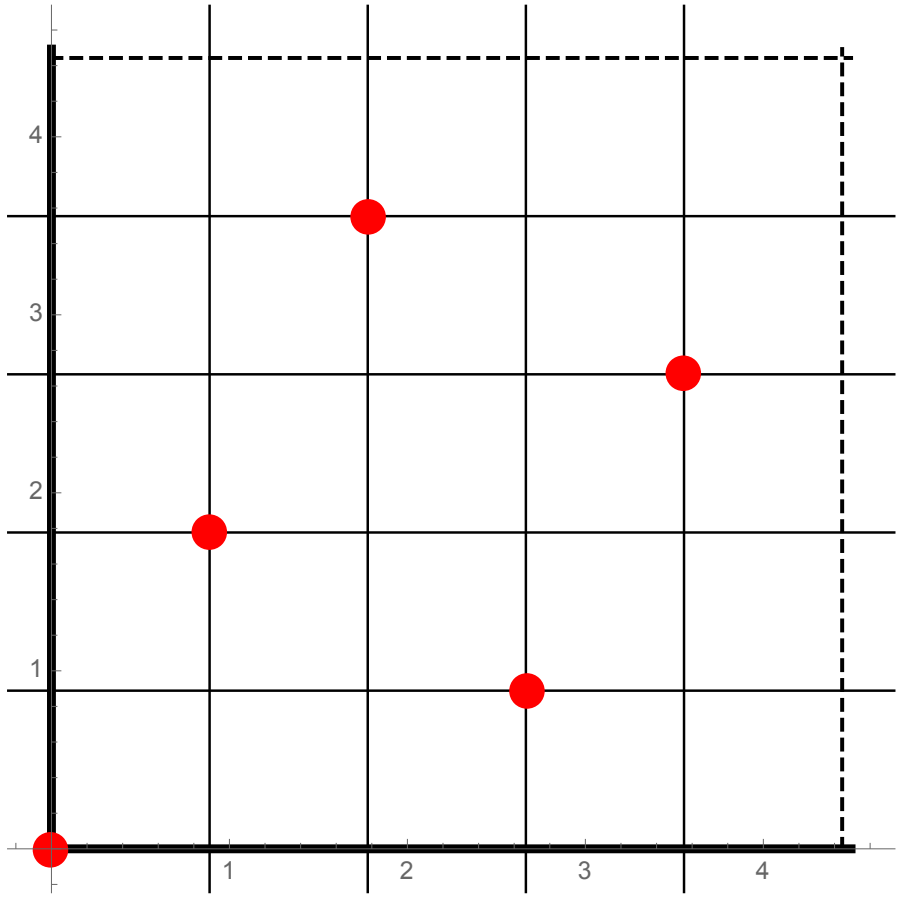
For such commutative group codes $\mathcal{C} = G\mathbf{u}$ we may consider $\mathbf{u} = (c_1, 0, c_2, 0, \ldots, c_L, 0)$ where $\mathbf{c} = (c_1, c_2, .., c_L) \in \mathcal{S}^{L-1}$, $c_i > 0$ rotation angles $a_{ij} = (2\pi b_{ij})/M$, $1 \leq i \leq M$, $1 \leq j \leq L$.
$\mathbf{v}_i = (a_{i1}, \ldots a_{iL})$, $1 \leq i \leq M$ and the lattice Λ with basis $\{\mathbf{v}_1, ..., \mathbf{v}_N\}$ which has the rectangular sublattice

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

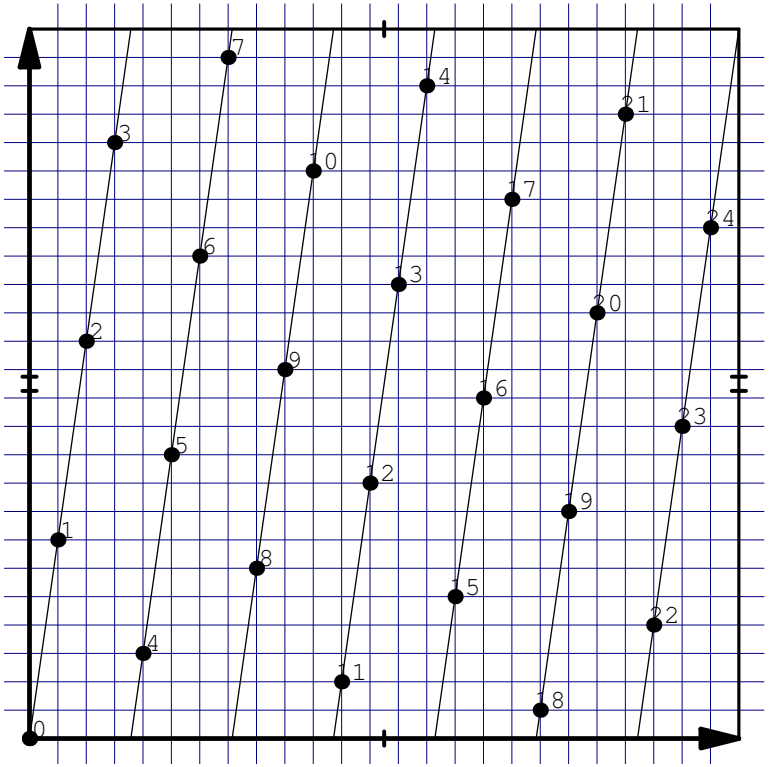
Proposition

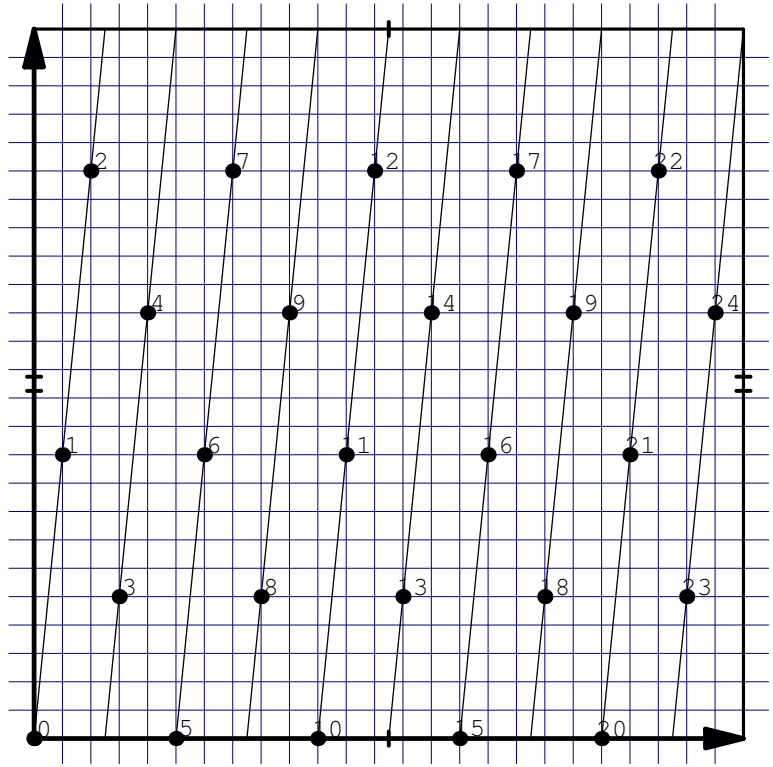
[SC08] Let $\mathcal{C} = G\mathbf{u}$ *with* $\mathbf{u} = (c_1, 0, c_2, 0, \ldots, c_L, 0)$, $\mathbf{c} = (c_1, c_2, .., c_L)$, $||c|| = 1$,$c_i > 0$ *be a commutative group code in* $\mathbb{R}^{2L}$, *free from reflection blocks. The inverse image* $\Phi_{\mathbf{c}}^{-1}$ *by the torus mapping (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.

Examples:



The quotient of lattices linked to the spherical code in $\mathbb{R}^4$ with initial vector $\mathbf{u} = (1/\sqrt{2}, 0, 1/\sqrt{2}, 0)$ and group $\mathcal{G}$ of matrices generated by $[\mathrm{Rot}(\frac{2\pi.1}{5}), \mathrm{Rot}(\frac{2\pi.2}{5})]$.
This code is a simplex code – squared distance between any two of its five points is $5/2$





Pre-images $\Phi_{\mathbf{c}}^{-1}$ of two cyclic group codes $\mathcal{C} = G\mathbf{u}$ 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 $\mathbf{u} = (\sqrt{0.54915}, 0, \sqrt{0.45085}, 0)$, what provides the best commutative group code of this order in $\mathbf{R}^4$. [TSCS15]

A lattice bound for commutative group codes

Proposition

[SC08] Every commutative group code $\mathcal{C} = G\mathbf{u}$ 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

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

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 $\mathbb{R}^L$.

Remarks

- The torus bounds given above are tight in the following sense.

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

  For big M, d is small and the distance in $T_{\mathbf{c}} \subset \mathbb{R}^{2L}$ is approached by its inverse image in $\mathbb{R}^L$;
- For general commutative groups in $\mathbb{R}^{2L}$ the lattice packing density in the last proposition can be replaced by the best packing density in $\mathbb{R}^L$;
- Bounds for commutative group codes in odd dimensions, $n = 2L + 1$, can also be obtained [SC08] by observing that those codes must lie on two parallel hyperplanes and are formed by two equivalent copies of commutative group codes in $\mathbb{R}^{2L}$.

Remarks

- For general spherical codes (not group codes) we have much bigger upper bounds and the codes may asymptotically approach the density of $\mathbb{R}^{2L-1}$ [HZ97]. Shannon (1959), Kabatianskii-Levenshtein (1979) (linear programming Delsarte72) bounds;
- The great advantage of commutative group codes are their homogeneity, easiness and low cost of the encoding and decoding processes on flat tori [VC03, TCV13].

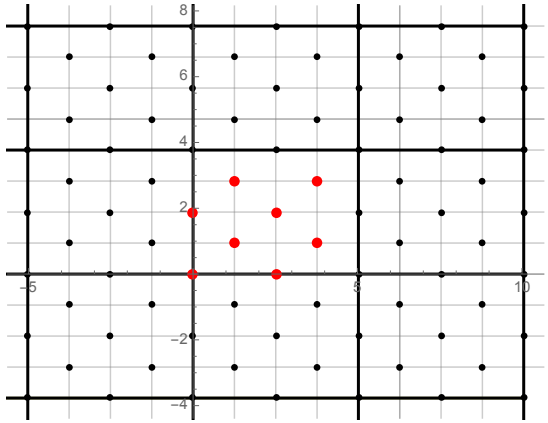
Approaching the Bound: Good and Optimum Commutative Group Codes

For small distances d or big M good commutative group codes may be found searching for orthogonal sublattices $\tilde{\Lambda}$ of a lattice Λ with good packing density.

Proposition

[AC13, COCBU18] Let $\alpha = \{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n\}$ *and* $\beta = \{\mathbf{w}_1, \mathbf{w}_2, ..., \mathbf{w}_n\}$ *bases of 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* $b_i = \|\mathbf{w}_i\|$, $b = \left(\sum_{j=1}^{n} \|\mathbf{w}_j\|^2\right)^{\frac{1}{2}}$, $c_i = \frac{b_i}{b}$, $\mathbf{c} = (c_1, c_2, ..., c_n)$ *and* $\phi_{\mathbf{c}}$ *the torus map regarding in this frame. Then to the normalized nested pair* $(1/b)\Lambda_\beta \subset (1/b)\Lambda_\alpha$ *of lattices it is associated a spherical code in* $\mathbb{R}^{2n}$ *with initial vector* $(c_1, 0, c_2, 0, ..., c_n, 0)$ *and generator group of matrices determined by the Smith normal decomposition of* H.

Example



According to the above proposition, $\alpha = \{\mathbf{v}_1, \mathbf{v}_2\}$, $\beta = \{\mathbf{w}_1, \mathbf{w}_2\}$, with $\mathbf{v}_1 = ((0.8)2\pi/2, 0)$, $\mathbf{v}_2 = ((0.8)2\pi/4, (0.6)2\pi/4)$, $\mathbf{w}_1 = ((0.8)2\pi, 0)$, $\mathbf{w}_2 = (0, (0.6)2\pi)$. $(b = 1)$. Since $\mathbf{w}_1 = 2\mathbf{v}_1$ and $\mathbf{w}_2 = 4\mathbf{v}_2 - 2\mathbf{v}_1$, we have:

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

Generators of the quotient of lattices: $\bar{\mathbf{v}}_1$ of order 2 and $-\bar{\mathbf{v}}_1 + \bar{\mathbf{v}}_2$ of order 4. The spherical code in $\mathbb{R}^4$ has $(0.8, 0, 0.6, 0)$ for initial vector, and $G = \{A^r.B^s, 0 \leq r \leq 1, 0 \leq s \leq 3$, where $A = [\mathrm{Rot}[2\pi(1/2)]$, Identity] and $B = [\mathrm{Rot}[2\pi(-1/4)], \mathrm{Rot}[2\pi(1/4)]]$.

Examples of good commutative group codes constructed from orthogonal sublattices of dense lattices

n	M	d_{min}	Upper bound	Group
4	141180	0.012706	0.0127061	$\mathbb{Z}_{141180}$
4	423540	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	10368	0.366025	0.369712	$\mathbb{Z}_6 \oplus \mathbb{Z}_{12}^3$
16	65536	0.707107	0.780361	$\mathbb{Z}_2 \oplus \mathbb{Z}_4^6 \oplus \mathbb{Z}_8$
16	16777216	0.382683	0.392069	$\mathbb{Z}_4 \oplus \mathbb{Z}_8^6 \oplus \mathbb{Z}_{16}$

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. Their minimum distances approach the upper bound [AC13].

The search for optimum commutative group codes

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

- For each $G \in \mathcal{G}_n(M)$ d varies depending on the initial vector;
- Isomorphic groups of matrices may produce spherical codes with different minimum distances for the same initial vector;
- Problem: Given m and n to find a optimal $\mathcal{C}(M, n, d) \rightarrow$ No general solution;
- Biglieri, Elia (1976): for a fixed cyclic group of order $M \rightarrow$ linear programming problem, total number of cases to be tested $\approx \binom{M/2}{n/2}$;

An approach based on the association between commutative group codes and lattices is presented next.

Proposition (TSCS15)

Every commutative group code $\mathcal{C}(M, 2L, d)$, generated by a group $G \in \mathcal{O}_{2L}$ 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 $W\,T = M\,I_L$, 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 $(a_i)^i \cdot (a_{i+1} \cdots a_L) \leqslant M$, $\forall i = 1, \ldots, L$.*

Example

For $M = 128$ there are, up to isomorphism, only 4 abstract commutative groups or order M:
$\{Z_{128}, Z_2 \times Z_{64}, Z_4 \times Z_{32}, Z_8 \times Z_{16}\}$., however for $n = 2L = \{4, 6, 8\}$ there are $\{2016, 41664, 635376\}$ distinct representations of them in $\mathcal{O}_n$.
After discarding isometric codes by using the above Proposition we must consider just $\{71, 2539, 55789\}$ representations, respectively.
The initial vector problem can then be solved only for those cases.

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

Some best commutative group codes of order M in $\mathbb{R}^6$ with $50 \leq M \leq 1000$, initial vector $\mathbf{c} = (c_1, 0, c_2, 0, c_3)$

Good commutative group code can be asymptotically reached through the following proposition.

Proposition (S18)

Let Λ *be a lattice with generator matrix* B *such that* $\mathrm{B}^* = (\mathrm{B}^T)^{-1}$ *has integer entries and* $\Lambda^\star_{w,\mathrm{P}}$ *a lattice with generator matrix* $\mathrm{B}^\star_{w,\mathrm{P}} = w\mathrm{B}^* + \mathrm{P}$, *where* P *has integer entries and* w *is integer. Then the lattice* $\Lambda_{w,\mathrm{P}}$ *with generator matrix* $\mathrm{adj}(\mathrm{B}^\star_{w,\mathrm{P}})$ *has* $\Lambda'_{w,\mathrm{P}} = \det(\Lambda^\star_{w,\mathrm{P}})\mathbb{Z}^n$ *as an orthogonal sublattice. Moreover*

$$\frac{1}{w}\Lambda^\star_{w,P} \longrightarrow \Lambda^*(w \to \infty)$$

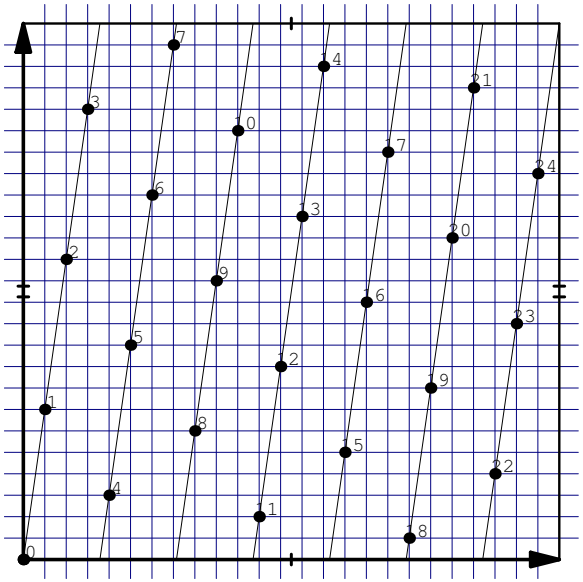
and by continuity of the matrix inversion process $\frac{1}{\det(\frac{1}{w}\mathrm{B}^\star_{w,\mathrm{P}})}\Lambda_{w,\mathrm{P}} \longrightarrow \Lambda(w \to \infty)$.

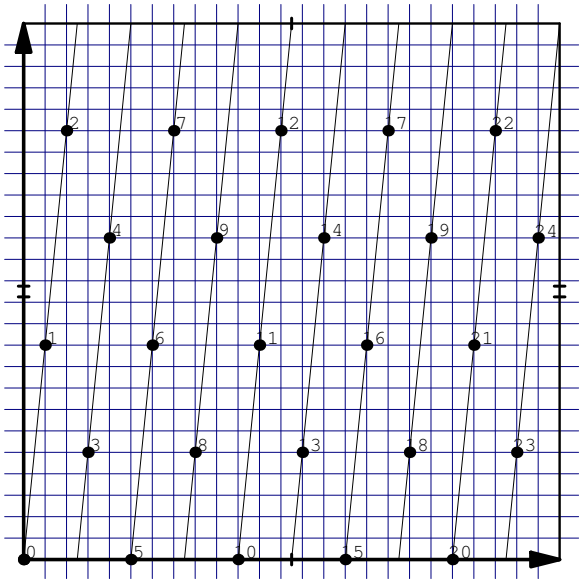
	$\mathrm{P}_{1,24}$		$\mathrm{P}_{1,24}$	
w	$\log_{10} M$	distance	$\log_{10} M$	distance
7	27.6113	0.177774	31.1194	0.128473
8	28.9791	0.156625	32.5112	0.112635
9	30.1901	0.139890	33.7389	0.100256
10	31.2763	0.126336	34.8371	0.0903175
11	32.2609	0.115147	35.8305	0.0821655
12	33.1610	0.105760	36.7374	0.0753593

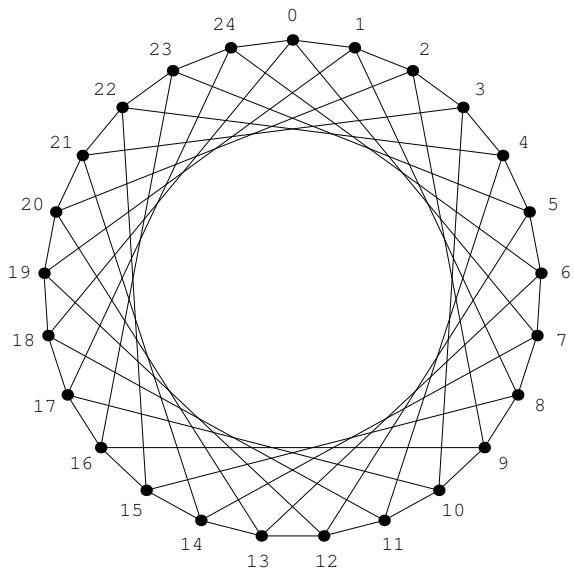
Performance of spherical commutative group codes in dimension 48 based in the last proposition.

Commutative group codes and codes on graphs

Commutative group codes can also be viewed as a graph or a coset code 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 [F91, CMAP04]. This is the approach presented in [CSAB10] which deals with Perfect Lee codes in $\mathbb{Z}_q^n$ (graph metric) and Cayley graphs (used in parallel computing).







The cyclic group code on left viewed as the circulant graph $C_{25}(1, 7)$.

Spherical codes in layers of tori

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)* [TCV13] can be generated by a finite set of orthogonal matrices and have efficient storage and decoding process, which is attached to lattices in the half of the code dimension.
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 by designing a spherical code in $\mathbb{R}^L$ with minimum distance d and positive coordinates. Then, for each one of these tori, a commutative group code based on lattices is derived.

Example

In [TCV13], 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.

Example

TLSC have the advantage of being constructive and homogeneous in each layer. For very small distance and higher dimension the expected performance will decrease.

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

Four-dimensional code sizes at various minimum distances, TLSC, apple-pilling [GHSW87], wrapped [HZ97] and laminated approaches [HZ97]. (*): unknown values.

Coding for continuous alphabet sources

Curves on a sphere with good length, large distance between its folds and structure are suitable to the 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. One 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 a curve in $\mathbb{R}^n$.

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

is observed. The objective is to recover an estimate $\mathbf{x}$, attempting to minimize the mean square error.
Building curves for such a transmission was discussed by C. Shannon, in his remarkable paper [S49]. If x has normal distribution and $n = 1$, the *optimal* distortion is achieved by the scaled identity mapping, i.e., $s(x) = \alpha x$. For higher dimensions, however, the problem is not so simple. One approach is related to flat tori and lattices. structure.

$$\mathbf{s}(x) = \phi_{\mathbf{c}} \left(\frac{2\pi}{\sqrt{n}} \mathbf{a} x (\text{mod } 1) \right), \tag{5}$$

where $\phi_{\mathbf{c}}$ is the tori map and usually $\mathbf{c} = (1/\sqrt{L})(1, \ldots, 1)$. 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 [C90]). From a previous proposition, the distance between the "laps" of the new curve is approximately the distance between two lines in the (mod 1) map. The curve's length, on the other hand, 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:

(i) The norm of $\mathbf{a}$ is large.

(ii) The projection of $\mathbb{Z}^L$ along the orthogonal hyperplane to $\mathbf{a}$ has large shortest vector.

These two objectives (trade-off) 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.

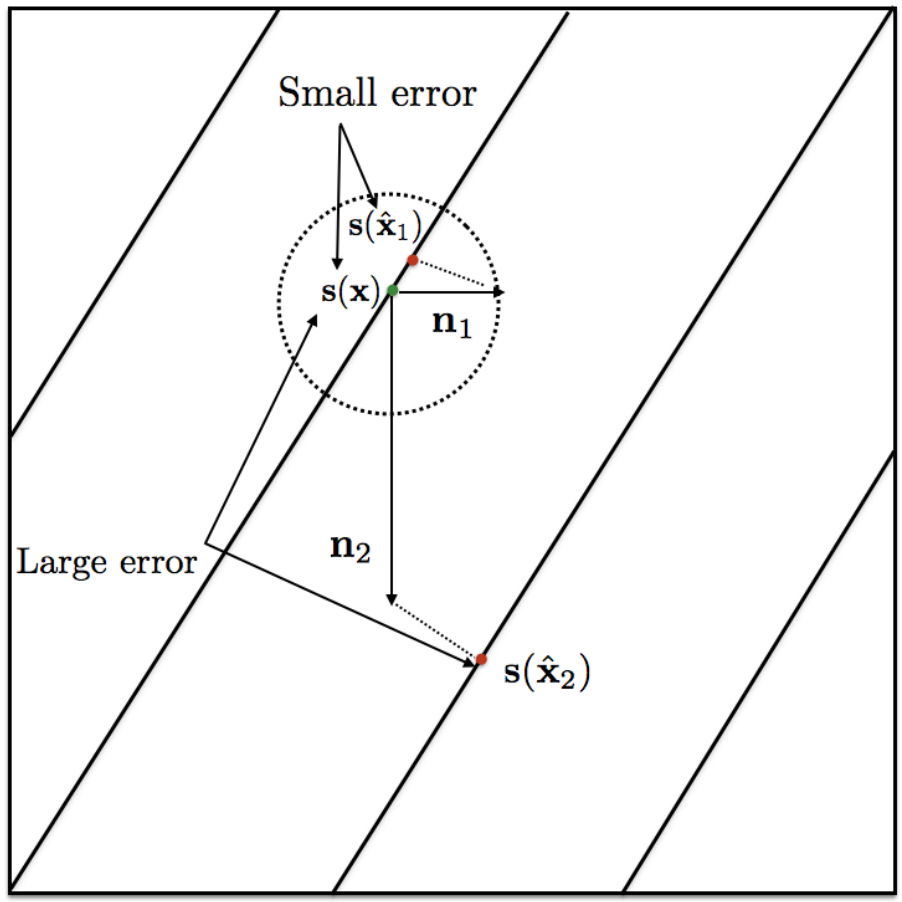
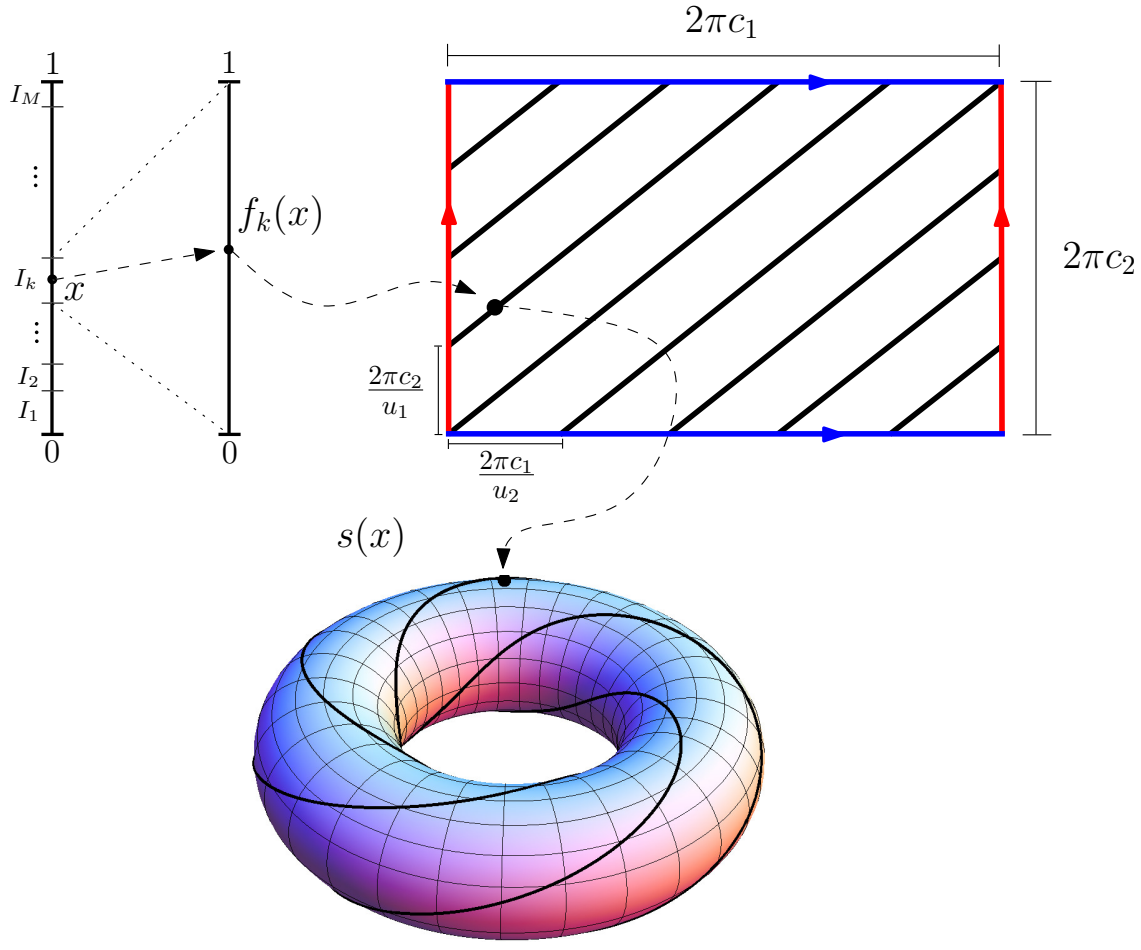
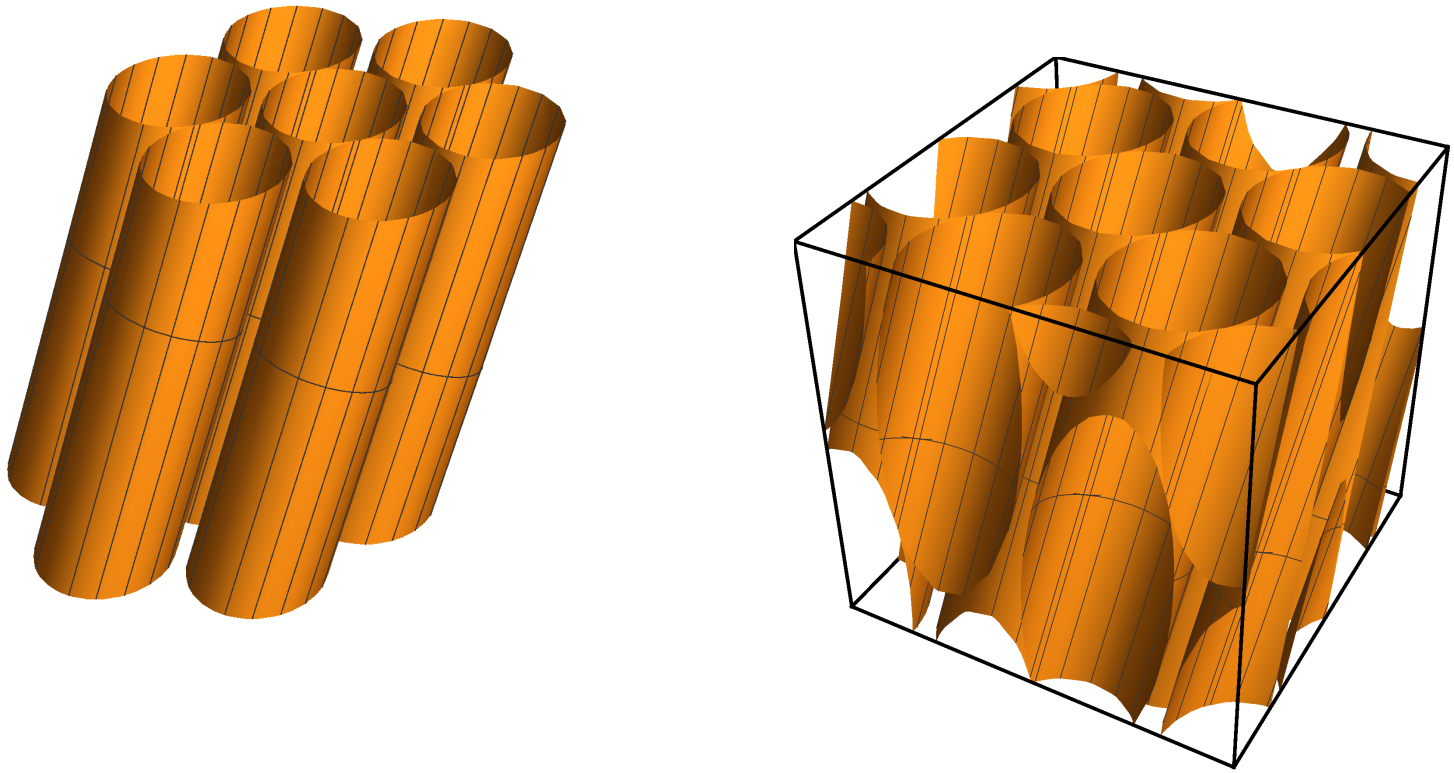


Illustration of small and large errors.



Encoding process



Packing of a curve in a Torus of $\mathbb{R}^6$, represented in a $3D$ box.

Advantage of these curves on flat tori: homogeneity and decoding process (flat torus decoding [VC03])

Projection of lattices

This topic is also connected to laminated and perfect lattices [CS99, M13].
Good curves on flat tori: Search for dense lattices in $\mathbb{R}^{2L-1}$ given as projections of the $2L$ dimensional integer lattice [VC03, SVC10].
A vector in a lattice Λ is said to be primitive if it can be extended to a basis of Λ.

Proposition

Let $\mathbf{v}$ *be a primitive vector of a full-rank lattice* $\Lambda \subset \mathbb{R}^n$. *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*

$$V(P_{\mathbf{v}^\perp}(\Lambda)) = \frac{V(\Lambda)}{\|\mathbf{v}\|} \tag{6}$$

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

Projection of lattices

We were to choose a vector $\mathbf{a} \in \mathbb{Z}^n$ such that

(i) The norm of $\mathbf{a}$ is large.

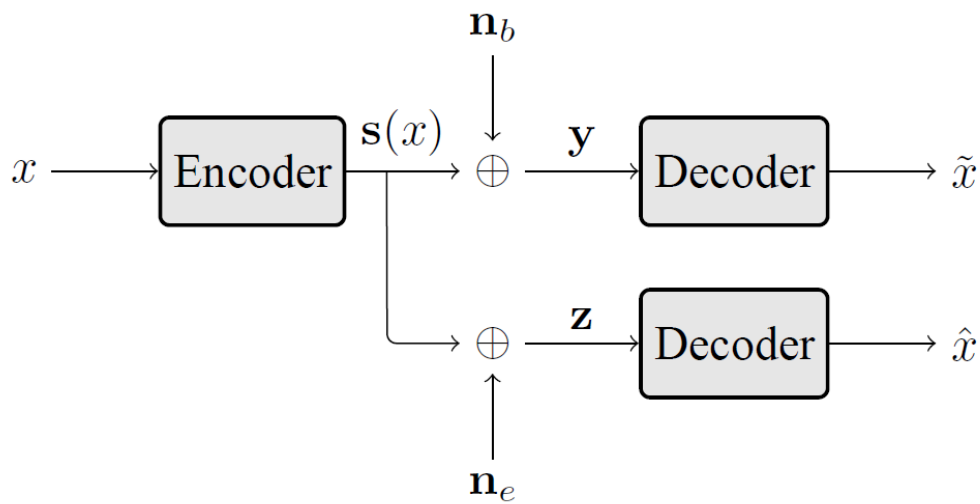
(ii) $P_{\mathbf{a}^\perp}(\mathbb{Z}^n)$ has a large shortest vector.

Or, having fixed the norm of $\mathbf{a}$ we would like maximize the minimum norm of $P_{\mathbf{a}^\perp}(\mathbb{Z}^n)$, say, $\lambda_1(\mathbf{a})$. This is equivalent to finding projections of $\mathbb{Z}^n$ with good packing density.
The Lifting Construction [SVC11] gives a general solution for this problem. Further extensions of this problem higher to projections from higher codimensions were presented in [CSC13].

- An interesting construction of asymptotically optimal (discrete) cyclic group codes from curves on tori is presented [ZTM17];
- Curves on flat torus layers for analog source coding are presented in [CTC2013]. As in the discrete case, for an estimate error correction (distance between "laps") a much bigger curve (homogeneous in each torus layers) can be provided

Continuous curves and secrecy

Schemes based on continuous curves on layers of flat tori can also be used to design a codes for wiretap channels with continuous input alphabets as presented in [ATB13].



The AWGN wiretap channel model.

Lattice topics in our research group: recent developments/ perspectives

- Still regarding spherical codes and lattices: Spherical codes inspired in the sphere Hopf fibration (recursive lattice construction); shaping gain: covering? quantization?
- Different metrics in lattices (Lee, Lp and maximum metric), Perfect and quasi-perfect codes [CJSC16,QC16, QCC18];
- Lattices from codes;
- Well rounded lattices;
- Algebraic lattices [JAC15] / Crypto connections RLWE [PR17];
- Lattice construction based on quaternion and octonion algebras [AB15, WBAC17];
- Lattice decoding in a distributed network setting (communication cost) [BVC17];

References

[AC2013] C. Alves and S. I.R. Costa. Commutative group codes in $\mathbb{R}^4$, $\mathbb{R}^6$, $\mathbb{R}^8$ and $\mathbb{R}^{16}$: approaching the bound. Discrete Mathematics, 313(16):1677 – 1687, 2013.

[AB15] C. Alves and J,-C. Belfiore, Lattices from maximal orders into quaternion algebras, J. Pure Appl. Algebra 219 (2015), 687–702.

[BOV04] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo. New algebraic constructions of rotated Zn- lattice constellations for the Rayleigh fading channel. IEEE Transactions on Information Theory, 50(4):702–714, 2004.

[BE76] E. Biglieri and M.Elia. Cyclic group codes for the Gaussian channel IEEE Transactions on Information Theory, 22(5):624 – 629, 1976.

[BVC17] M. Bollauf, V. Vaishampayan, S. I. R. Costa, On the communication cost of determining the nearest lattice point, IEEE ISIT 2017

References

[BVRB96] J. Boutros, E. Viterbo, C. Rastello, and J. C. Belfiore. Good lattice constellations for both rayleigh fading and gaussian channels. IEEE Transactions on Information Theory, 42(2):502–518, 1996.

[CB95] J. Caire and E. Biglieri. Linear block codes over cyclic groups. IEEE Transactions on Information Theory, 41(5):1246 –1256, 1995.

[CSCA16] A.Campello,G.C.Jorge,J.E.Strapasson, S.I.R.Costa.Perfect Codes in the lp metric. Eur. J. Comb., 53(C):72–85, 2016.

[CSC13] A. Campello, J. Strapasson, and S. I. R. Costa. On projections of arbitrary lattices. Linear Algebra and its Applications, 439(9):2577 – 2583, 2013.

[CTC13] A. Campello, C. Torezzan, and S. I. R. Costa. Curves on flat tori and analog source-channel codes. IEEE Transactions on Information Theory, 59(10):6646–6654, 2013.

[CE03] Cohn and N. Elkies. New upper bounds on sphere packings I. Annals of Mathematics, 157(2):689–714, 2003.

References

[CS99] J. H. Conway and N. J. A. Sloane. Sphere-packings, lattices, and groups. Springer-Verlag, New York, NY, USA, 1999.

[C90] S. I. R. Costa. On closed twisted curves. 109(1):205–214, 1990.

[CAMP04] S. I. R. Costa, E. Agustini, M. Muniz, and R. Palazzo. Slepian-type codes on a flat torus. IEEE ISIT 2000

[CAMP04] S. I. R. Costa, E. Agustini, M. Muniz, and R. Palazzo. Graphs, tessellations, and perfect codes on flat tori. IEEE Transactions on Information Theory, 50(10):2363 – 2377, 2004.

[CTCV13] S. I. R. Costa, C. Torezzan, A. Campello, and V. A. Vaishampayan. Flat tori, lattices and spherical codes. Information Theory and Applications Workshop (ITA), pages 1–8, 2013

[CSAC10] S.I.R. Costa, Strapasson J.E., M.M.S. Alves, and Carlos T.B. Circulant graphs and tessellations on flat tori. Linear Algebra and Its Applications, 432:369–382, 2010.

[CTCV13] S. I. R. Costa, C. Torezzan, A. Campello, and V. A. Vaishampayan. Flat tori, lattices and spherical codes. Information Theory and Applications Workshop (ITA), pp 1–8, 2013

References

[COCBV18] S.I R Costa, F. Oggier, A. Campello, J-C Belfiore, E. Viterbo, Lattices Applied to Coding for Reliable and Secure Communications, Springer 2018

[GHSW87] A. A. El Gamal, L. A. Hemachandra, Shperling I., and V. K. Wei. Using simulated anneling to design good codes. IEEE Transactions on Information Theory, IT-33 no 1:116–123, 1987.

[EZ01] T. Ericson and V. Zinoviev. Codes on Euclidean Spheres. North-Holland Mathematical Library, 2001.

[F91] G. D. Forney Jr. Geometrically uniform codes. IEEE Transactions on Information Theory, 37(5):1241 –1260, 1991.

[HZ97] J.Hamkins and K.Zeger, Asymptotically dense spherical codes.I. Wrapped spherical codes IEEE Transactions on Information Theory, 43(6):1774–1785, 1997.

[HZ97] J. Hamkins and K. Zeger. Asymptotically dense spherical codes II. Laminated spherical codes. IEEE Transactions on Information Theory, 43(6):1786–1798, 1997.

References

[I89] I.Ingemarsson, Group Codes for the Gaussian Channel. In Topics in Coding Theory volume 128 of Lecture Notes in Control and Information Sciences, pages 73–108. Springer Berlin Heidelberg, 1989.

[JAC15] G. C. Jorge, A. A. de Andrade, S. I. R. Costa, and J. E. Strapasson. Algebraic constructions of densest lattices. Journal of Algebra, 429:218 – 235, 2015.

[KL79] G. A. Kabatianskii and V. I. Levenshtein Bound for packing on a sphere and in space, Problems of Information Transmission, Vol. 14, N. 1, pp.

[L91] H.-A. Loeliger. Signal sets matched to groups. IEEE Transactions on Information Theory, 37(6):1675 –1682, 1991.

[M13] J. Martinet. Perfect Lattices in Euclidean Spaces. Springer, 2013.

[NG11] B. Nazer and M.Gastpar.Compute-and-Forward:Harnessing interference through structured codes. IEEE Transactions on Information Theory, 57(10):6463–6486, 2011

References

[OSB16] F. Oggier, P. Solé, and J. C. Belfiore. Lattice codes for the wiretap Gaussian channel: Construction and analysis. IEEE Transactions on Information Theory, 62(10):5690–5708 2016.

[OV04] F. Oggier and E. Viterbo. Algebraic number theory and code design for Rayleigh fading channels. Foundations and Trends in Communications and Information Theory, 1(3):333– 415, 2004.

[OW84] L. H. Ozarow and A. D. Wyner. Wire-tap channel II. AT&T Bell Laboratories Technical Journal, 63(10):2135–2157, 1984.

[P16] C. Peikert. A decade of lattice cryptography. Foundations and Trends in Theoretical Computer Science, 10(4):283–424, 2016.

[PR17] C. Peikert, O. Regev, N. Stephens-Davidowitz. Pseudorandomness of Ring-LWE for any ring and modulus, . Cryptology ePrint Archive, Report 258, 2017.

[PNF10] W.W. Peterson, J.B. Nation, and M.P. Fossorier. Reflection group codes and their decoding. IEEE Transactions on Information Theory, 56(12):6273 –6293, 2010.

References

[QC16]. C. Qureshi and S. I. R Costa. On perfect q-ary codes in the maximum metric. Information Theory and Applications Workshop (ITA), pages 1–4, Feb 2016.

[S59] C. E. Shannon, Probability of for error for optimal codes in a Gaussian channel, Bell Syst Techn J., Vol 38,pp. 611-656, 1959

[SC08] R.M.Siqueira and S.I.R.Costa, Flat tori, lattices and bounds for commutative group codes. Des. Codes Cryptography, 49(1-3):307–321, 2008.

[S68] D. Slepian. Group Codes for the Gaussian Channel. The Bell System Technical Journal, 47:575 – 602, 1968.

[SVC10] N.J.A. Sloane, V.A. Vaishampayan, and S.I.R. Costa. The lifting construction: A general solution for the fat strut problem. In IEEE ISIT pp 1037 –1041, 2010.

[SVC11] N. J. A. Sloane, Vinay A. Vaishampayan, and Sueli I. R. Costa. A note on projecting the cubic lattice. Discrete & Computational Geometry, 46(3):472–478, October 2011.

References

[SB13] P. Solé, J-C Belfiore, Constructive spherical codes near the Shannon bound, Desiigns Codes and Cryptography, Vol 66, 1-3, pp. 17-26, 2013

[TCV13]C.Torezzan, S.I.R.Costa and V.A.Vaishampayan., Constructive spherical codes on layers of flat. IEEE Transactions on Information Theory, 59(10):6655–6663, Oct 2013.

[S18] J. E. Strapasson, A note on orthogonal sublattices, Linear Algebra and Applications, To appear

[TMZ13] R. M. Taylor, L. Milli, A. Zaghloul, Packing tubes on tori: An efficient method for low SNR analog error correction, IEEE- ITW 2013

[TZM2017] R. M. Taylor Jr, A. Zaghloul, L. Mili. Structured spherical codes with asymptotically optimal distance distributions. In IEEE International Symposium on Information Theory, 2017.

[TSCS15] C. Torezzan, J. E. Strapasson, S. I. R. Costa, and R. M. Siqueira. Optimum tori commutative group codes. Designs, Codes and Cryptography, 74(2):379–394, 2015.

References

[VC03] V. A. Vaishampayan and S. I. R. Costa. Curves on a sphere, shift-map dynamics, and er- ror control for continuous alphabet sources. IEEE Transactions on Information Theory, 49(7):1658–1672, 2003.

[W09] J. Wang, Finding and Investigating Exact Spherical Codes, Experimental Mathematica, v.18-2, 249-256, 2009

[WABA17] C. Winki, C. Alves, N. Brasil, S. I. R. Costa, Algebraic Construction of Dense Lattices via Maximal Quaternion Orders (ArXiv, 2017)

[ZTM2017] A. Zaghloul,R. M. Taylor Jr, L. Mili. Structured spherical codes with asymptotically optimal distance distributions. In IEEE International Symposium on Information Theory, 2017.

[Z14] R.Zamir. Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation, and Multiuser Information Theory. Cambridge University Press, 2014.

References

[BZC18], M Bollauf, R. Zamir and S. I. R. Costa, Construction C* - An inter-level coded modulation of construction C, to be presented in the International Zurich Seminar on Information and Communication, Feb 2018

[QCC18] C. Qureshi, A. Campello, S. I. R. Costa, Non-existence of linear perfect Lee codes with radius 2 for infinitely many dimensions, IEEE Trans. Information Theory (to appear)

Thank you!