Four and Six-Dimensional Signal Constellations From Algebraic Lattices

J. Carmelo Interlando
Department of Mathematics
University of Notre Dame
Notre Dame, IN 46556-4618
USA

Michele Elia
Dipartimento di Elettronica
Politecnico di Torino
Corso Duca Degli Abruzzi 24
10129 Torino
Italy

Abstract

In this work we describe a procedure to construct finite signal constellations from lattices associated to rings of algebraic integers and their ideals. The procedure provides a natural way to label the constellation points by elements of a finite field. The labeling is proven to be linear which allows, at the receiver, a fast way to map a constellation point into a field element. The performance of four and six-dimensional constellations are determined in terms of minimum squared Euclidean distance and average energy, for rates from 1 up to 3.

1 Introduction

A lattice constellation $\mathcal{S}$ of dimension n consists of a set of M points, also called signals, in n-dimensional Euclidean space from a lattice of rank n. A given point $(x_1, \ldots, x_n) \in \mathcal{S}$ is associated to the signal $\sum_{i=1}^{n} x_i \phi_i(x)$, where $\{\phi_1(x), \ldots, \phi_n(x)\}$ is the signal orthonormal basis for the usual scalar product of functions over an interval $[0, T]$. Such constellations have proven to be an efficient means to transmit information over a Gaussian channel, see for example, [1], [3], [4], and [8].

A basic parameter guiding the design of such constellations is the *normalized minimum square distance*, given by $\kappa = \frac{d^2_{\min}}{E_{\text{av}}} \log_2 M$, where E_{av} is the average squared norm of the points of the constellation, and $d^2_{\min}$ is the minimum squared distance between points of the constellation [11]. For a given rate $R = \log_2 M/n$ bits per dimension, the best constellation is the one possessing the highest value of κ.

Another important aspect in the design of such constellations concerns the labeling of the constellation points. This is crucial at the receiver, when converting a constellation point

into a field element. One of the first works in that direction was [17], where Ungerboeck introduced the notion of mapping by set partitioning.

Our aim in this paper is to revisit a well-known method for constructing and labeling lattice constellations, and to apply it with a particular class of lattices, namely, the algebraic lattices. The result will be a systematic construction/labeling procedure. The basic idea of the old method is to select a sublattice $\Lambda' \subset \Lambda$, and to take the quotient Λ/Λ' of finite cardinality. The constellation then consists of the representatives of the cosets of Λ in Λ'. This general approach can be found in [4], [8], and [17].

The novelty introduced in the present paper is that the lattices being considered are algebraic lattices, that is, they are images in $\mathbb{R}^n$ of rings of algebraic integers or ideals in those rings. The lattice partitioning is then realized via Kummer's lemma, which is a constructive procedure to factor prime numbers in rings of algebraic integers. Moreover, Kummer's lemma provides us with a natural way to label the cosets of a sublattice by elements of a finite field $GF(q)$ to which Λ/Λ' is isomorphic. Finally, the linearity of the labeling speeds up decoding processes.

The procedure we derive from Kummer's lemma is systematic, in the sense that lattice constellations can be efficiently constructed and labeled in any dimension, in principle. Good constellations for the parameter κ can be obtained from good algebraic lattices, that is, lattices possessing a high center density. Two-dimensional constellations labeled by elements of a finite field were presented in [9], [10], and [13]. However, the techniques presented there do not allow an obvious generalization to higher dimensions.

This paper is organized as follows: in Section 2, a brief review of algebraic lattices and decomposition of primes in number fields is presented; in Section 3, the linear labeling of lattices is introduced along with a technique to effectively build signal constellations; in Section 4, the linear labeling technique is extended to sublattices of a lattice that is the image of a ring of integers; in Section 5, a concrete example of construction and labeling of a four dimensional constellation is worked out; in Section 6, a table of optimal constellations is presented; in Section 7, the conclusions are presented.

2 Algebraic Lattices and Ideal Decomposition in Number Fields

In this section we will present the essential concepts and results from algebraic number theory which lead to lattice construction and labeling of lattice points. For mathematical rigor and computational issues, the interested reader may consult [2], [12], and [14].

We say that $\mathbb{F} = \mathbb{Q}(\rho)$ is an algebraic number field of degree n if $\mathbb{F}$ is a finite extension field of $\mathbb{Q}$. Such extension field is obtained by adjoining to $\mathbb{Q}$ a root $\rho \in \mathbb{C}$ of $p(x)$, a polynomial in $\mathbb{Z}[x]$ of degree n. $\mathbb{F}$ can be seen as vector space over $\mathbb{Q}$ of dimension n, and one of its bases is $\{1, \rho, \ldots, \rho^{n-1}\}$.

There are exactly n embeddings of $\mathbb{F}$ into $\mathbb{C}$. These are homomorphisms $\phi : \mathbb{F} \to \mathbb{C}$ such

that $\phi(r) = r$, $\forall r \in \mathbb{Q}$. We will denote the n embeddings by $\sigma_1, \ldots, \sigma_n$. In fact, σ_i is completely defined by putting $\sigma_i(\rho) = \rho_i$, for $i = 1, \ldots, n$, where $\rho_1 = \rho, \rho_2, \ldots, \rho_n$ are the distinct roots of $p(x)$.

The set of all elements in $\mathbb{F}$ that are roots of monic polynomials in $\mathbb{Z}[x]$ forms a ring, called the ring of integers of $\mathbb{F}$, and denoted by $\mathfrak{O}_{\mathbb{F}}$. This ring is actually a $\mathbb{Z}$-module of rank n, so it admits a $\mathbb{Z}$-basis which we denote by $\{\omega_1, \ldots, \omega_n\}$.

Let us now order the σ_j such that $\sigma_j(x) \in \mathbb{R}$ for for $j = 1, \ldots, r_1$, and $\sigma_{j+r_2}(x)$ is the complex conjugate of $\sigma_j(x)$ for $j = r_1 + 1, \ldots, r_1 + r_2$. Note that $n = r_1 + 2r_2$. Then the *canonical embedding* $\sigma : \mathbb{F} \to \mathbb{R}^n$, defined by

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)).$$

is a $\mathbb{Q}$-algebra monomorphism, where $\Re(z)$ and $\Im(z)$ are, respectivelly, the real and imaginary parts of the complex number z.

Finally, the set $\{v_1, \ldots, v_n\}$, where

$$v_i = (\sigma_1(\omega_i), \ldots, \sigma_{r_1}(\omega_i), \Re\sigma_{r_1+1}(\omega_i), \Im\sigma_{r_1+1}(\omega_i), \ldots, \Re\sigma_{r_1+r_2}(\omega_i), \Im\sigma_{r_1+r_2}(\omega_i)),$$

forms a basis of a full-rank lattice Λ in $\mathbb{R}^n$. Given any nonzero ideal $\mathfrak{I}$ of $\mathfrak{O}_{\mathbb{F}}$, $\sigma(\mathfrak{I}) \subset \mathbb{R}^n$ is a sublattice of Λ, also of full-rank.

For the labeling of lattice points by elements of a finite field, we will need the following theorem, which is a special case of Theorem (2.27) [14, p. 390].

Theorem 2.1. *Let $\mathbb{F}$ be an algebraic number field with ring of integers $\mathfrak{O}_{\mathbb{F}}$. Let $\mathbb{F} = \mathbb{Q}(\rho), \rho \in \mathfrak{O}_{\mathbb{F}}$, and $m(x) \in \mathbb{Z}[x]$ be the minimal polynomial of ρ. Suppose p is a rational prime not dividing the index $f = [\mathfrak{O}_{\mathbb{F}} : \mathbb{Z}[\rho]]$ of ρ. The prime ideal $p\mathfrak{O}_{\mathbb{F}}$ decomposes into prime ideals of $\mathfrak{O}_{\mathbb{F}}$ in the following way: let $\overline{m}(x) = \overline{m_1}(x)^{e_1} \ldots \overline{m_r}(x)^{e_r}$ be the factorization of $m(x)$ into distinct monic irreducible polynomials of degree f_i $(1 \leq i \leq r)$ over $\mathbb{Z}_p[x]$, where $\bar{}$ denotes the residue class mapping $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$. Then $p\mathfrak{O}_{\mathbb{F}}$ has a* unique presentation

$$p\mathfrak{O}_{\mathbb{F}} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r},$$

as a power product of prime ideals in $\mathfrak{O}_{\mathbb{F}}$, where $\mathfrak{p}_i = \langle p, m_i(\rho) \rangle$ and $\mathfrak{O}_{\mathbb{F}}/\mathfrak{p}_i \cong GF(p^{f_i})$, for $1 \leq i \leq r$.

3 Linear Labeling of Lattice Constellations

Definition 3.1. *Let $\mathbb{F} = \mathbb{Q}(\rho)$ be a number field of degree n, where $\rho \in \mathfrak{O}_{\mathbb{F}}$, a $\mathbb{Z}$-module with basis $\{\omega_1, \ldots, \omega_n\}$. Let Λ be the lattice obtained from $\mathfrak{O}_{\mathbb{F}}$ via the canonical embedding σ. Given a rational prime p and a positive integer t, the mapping $\ell : \Lambda \to GF(p^t)$ is called a $GF(p^t)$-*linear labeling *if*

$$\ell(\sigma(x_1\omega_1 + \ldots + x_n\omega_n)) = x_1\ell(\sigma(\omega_1)) + \ldots + x_n\ell(\sigma(\omega_n)), \tag{3.1}$$

$\forall x_i \in \mathbb{Z}$, and $1 \leq i \leq n$.

Let p be a rational prime. Then, by Theorem 2.1, $p\mathfrak{O}_{\mathbb{F}} = \prod_{j=1}^{r} \mathfrak{p}_j^{e_j}$, where $\mathfrak{p}_j$ are distinct prime ideals in $\mathfrak{O}_{\mathbb{F}}$ given by $\mathfrak{p}_j = \langle p, m_j(\rho)\rangle$, and $\mathfrak{O}_{\mathbb{F}}/\mathfrak{p}_j \cong GF(q_j)$, with $q_j = p^{f_j}$. From this, and noting Definition 3.1, we have the following

Proposition 3.1. *Let φ be an isomorphism from $\mathfrak{O}_{\mathbb{F}}/\mathfrak{p}_j$ onto $GF(q_j)$, and let $\boldsymbol{pr}$ be the natural mapping from $\mathfrak{O}_{\mathbb{F}}$ onto $\mathfrak{O}_{\mathbb{F}}/\mathfrak{p}_j$. Then $\ell = \varphi \circ \boldsymbol{pr} \circ \sigma^{-1}$ is a linear $GF(q_j)$-labeling of Λ by $GF(q_j)$.*

Proof: Applying the basic properties of the mappings $\varphi, \boldsymbol{pr}$, and σ, we obtain:

$$\ell(\sigma(x_1\omega_1 + \ldots + x_n\omega_n)) = \varphi(\boldsymbol{pr}(\sigma^{-1}(\sigma(x_1\omega_1 + \ldots + x_n\omega_n)))) = \varphi(\boldsymbol{pr}(x_1\omega_1 + \ldots + x_n\omega_n)) =$$

$$\varphi(\boldsymbol{pr}(x_1\omega_1) + \ldots + \boldsymbol{pr}(x_n\omega_n)) = \varphi(\boldsymbol{pr}(x_1\omega_1)) + \ldots + \varphi(\boldsymbol{pr}(x_n\omega_n)) =$$

$$x_1\varphi(\boldsymbol{pr}(\omega_1)) + \ldots + x_n\varphi(\boldsymbol{pr}(\omega_n)) = \ell(\sigma(x_1\omega_1)) + \ldots + \ell(\sigma(x_n\omega_n)).$$

□

Remark 3.1. *Note that ℓ can be completely specified by setting $\ell(\sigma(\rho)) = r_0$, where r_0 is a root of the polynomial $m_j(x)$ over $GF(p)$.*

An immediate consequence of Proposition 1 is

Corollary 3.1. *$\ell(\sigma(x)) = \ell(\sigma(y))$ if and only if x and y are elements of the same coset of $\mathfrak{p}_j$ in $\mathfrak{O}_{\mathbb{F}}$.*

Algorithm for Constructing and Labeling a q_j-Point Constellation from Lattice $\sigma(\mathfrak{O}_{\mathbb{F}})$

Step 1) Choose one of the roots r_0 of the equation $m_j(x) = 0$ over $GF(p^{f_j})$;

Step 2) Set $\ell(\sigma(\rho)) = r_0$;

Step 3) Set $\ell(\sigma(\omega_i)) = \sum_{s=0}^{t} c_{i,s} r_0^s$, where $\omega_i = \sum_{s=0}^{t} c_{i,s}\rho^s$, for $1 \le i \le n$;

Step 4) For each one of p^{f_j} cosets of $\mathfrak{p}_j$ in $\mathfrak{O}_{\mathbb{F}}$, choose the respective coset leader as the element x^* such that $\sigma(x^*)$ is the closest to the origin. Finish.

In Step 4, the obtained set of coset leaders is the signal constellation we were seeking. At this point, it is worth mentioning the advantages of having a linear type of labeling:

1) The search for finite point constellations with p^f points is a systematic procedure consisting of partitioning a lattice $\Lambda = \sigma(\mathfrak{O}_{\mathbb{F}})$ into p^f cosets via an ideal $\mathfrak{p}$ of $\mathfrak{O}_{\mathbb{F}}$. The coset leaders having minimum energy are retained. Their labels are determined via the isomorphism between $\mathfrak{O}_{\mathbb{F}}/\mathfrak{p}$ and $GF(p^f)$;

2) At the receiver side, the decoder usually employs a two step procedure. First, given a received point $\boldsymbol{r} \in \mathbb{R}^n$, the nearest point $\boldsymbol{r}^*$ in the constellation is singled out. Secondly, the label of $\boldsymbol{r}^*$ can be quickly computed via Equation 3.1.

Next, we give an example to illustrate the labeling technique.

Example 3.1. *Consider $\mathbb{F} = \mathbb{Q}(\zeta_8)$, where ζ_8 is a primitive eighth root of unity. Its minimal polynomial is $m(x) = x^4 + 1$. The ring of integers is $\mathfrak{O}_{\mathbb{F}} = \mathbb{Z}[\zeta_8]$, a principal ideal domain. One can verify that $m(x) = (x-10)(x+10)(x-22)(x+22) \pmod{73}$. Thus,*

$$73\mathfrak{O}_{\mathbb{F}} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4,$$

where $\mathfrak{p}_1 = \langle 73, \zeta_8 - 10\rangle$, $\mathfrak{p}_2 = \langle 73, \zeta_8 + 10\rangle$, $\mathfrak{p}_3 = \langle 73, \zeta_8 - 22\rangle$, and $\mathfrak{p}_4 = \langle 73, \zeta_8 + 22\rangle$.

We have $\mathbb{Z}[\zeta_8]/\mathfrak{p}_1 \cong GF(73)$, and therefore $\zeta_8 \equiv 10 \pmod{\mathfrak{p}_1}$. From this, the following labeling results:

$$\ell(\sigma(x_0 + x_1\zeta_8 + x_2\zeta_8^2 + x_3\zeta_8^3)) = x_0 + 10x_1 + 27x_2 + 51x_3 \pmod{73},$$

$\forall x_i \in \mathbb{Z}$, and $0 \leq i \leq 3$.

4 Linear Labeling of Sublattices

Given a number field $\mathbb{F}$ and its ring of integers $\mathfrak{O}_{\mathbb{F}}$, let $\mathfrak{q}$ be a nonzero $\mathfrak{O}_{\mathbb{F}}$-ideal. If lattice $\sigma(\mathfrak{q})$ is denser than lattice $\sigma(\mathfrak{O}_{\mathbb{F}})$, then a signal constellation is generally built from $\mathfrak{q}$ instead of $\mathfrak{O}_{\mathbb{F}}$. If $\mathfrak{p}$ is also a nonzero $\mathfrak{O}_{\mathbb{F}}$-ideal, then $\mathfrak{O}_{\mathbb{F}}/\mathfrak{p} \cong \mathfrak{q}/\mathfrak{pq}$. In this direction, it would be convenient if we could label the cosets of $\mathfrak{pq}$ in $\mathfrak{q}$ utilizing the labeling adopted in $\mathfrak{O}_{\mathbb{F}}/\mathfrak{p}$, i.e., the elements of $\mathfrak{q}$ would receive the same label as they would receive in $\mathfrak{O}_{\mathbb{F}}$. At this point, however, some difficulties may arise. For example, consider the case where $\mathfrak{p} = \mathfrak{q}$. From the previous section, we know that $\ell(\sigma(x)) = 0, \forall x \in \mathfrak{p}$. Therefore, all the representatives of the cosets of $\mathfrak{p} \cdot \mathfrak{p}$ in $\mathfrak{p}$ will be labeled by 0, a property that is not desirable. To avoid this situation, we can resort to the following result [12, Corollary 3.28, p. 136].

Proposition 4.1. *Let $\mathfrak{p}, \mathfrak{q}$ be nonzero $\mathfrak{O}_{\mathbb{F}}$-ideals. Then:*

i) There is an isomorphism ϕ from the additive group of $\mathfrak{O}_{\mathbb{F}}/\mathfrak{p}$ onto the additive group of $\mathfrak{q}/\mathfrak{pq}$;

ii) There is always an $\mathfrak{O}_{\mathbb{F}}$-ideal $\mathfrak{a}$, relatively prime to $\mathfrak{q}$, such that $\mathfrak{aq}$ is principal. If γ is a generator of $\mathfrak{aq}$, then ϕ is specified by the mapping: $r + \mathfrak{p} \mapsto r\gamma + \mathfrak{pq}$.

Proposition 2 motivates the following

Definition 4.1. *Let $\mathfrak{O}_{\mathbb{F}}$ be the ring of integers of a number field $\mathbb{F}$, and let $\mathfrak{p}$ and $\mathfrak{q}$ be nonzero $\mathfrak{O}_{\mathbb{F}}$-ideals. Suppose ℓ is a linear labeling of $\Lambda = \sigma(\mathfrak{O}_{\mathbb{F}})$ by $GF(q)$, and r is any element of $\mathfrak{O}_{\mathbb{F}}$. Then we define the* label of $\sigma(x)$, for any x belonging to the coset $\overline{r\gamma}$ of $\mathfrak{pq}$ in $\mathfrak{q}$, *as $\lambda(\sigma(x)) := \ell(\sigma(r))$.*

Proposition 4.2. *The mapping λ is a linear labeling.*

Proof: Let r, s be any elements of $\mathfrak{O}_{\mathbb{F}}$, and define $x = r\gamma$, and $y = s\gamma$, where γ is as in Proposition 2. Then

$$\lambda(\sigma(x+y)) = \ell(\sigma(r+s)) = \ell(\sigma(r)) + \ell(\sigma(s)) = \lambda(\sigma(x)) + \lambda(\sigma(y)).$$

□

The next two examples illustrate this situation.

Example 4.1. *Let $\mathbb{F} = \mathbb{Q}(\zeta_8)$. Consider the ideal $\mathfrak{q} = \langle 1 - \zeta_8 \rangle$ of $\mathfrak{O}_{\mathbb{F}}$. It is easy to see that $N(\mathfrak{q}) = 2$ and $\sigma(\mathfrak{q})$ is the lattice denoted by D_4 in [4]. Let $\mathfrak{p} = \langle 4 - \zeta_8 \rangle$ be an ideal of $\mathfrak{O}_{\mathbb{F}}$. We have $N(\mathfrak{p}) = 257$; so $\mathbb{Z}[\zeta_8]/\mathfrak{p} \cong \mathbb{Z}_{257}$. On the other hand, $\mathbb{Z}[\zeta_8]/\mathfrak{p} \cong \mathfrak{q}/\mathfrak{p}\mathfrak{q}$. Therefore,*

$$\langle 1 - \zeta_8 \rangle / \langle 4 - 5\zeta_8 + \zeta_8^2 \rangle \cong \mathbb{Z}_{257}.$$

We have $\zeta_8 \equiv 4 \pmod{\mathfrak{p}}$. From this, the following labeling results:

$$\lambda(\sigma(x_0 + x_1\zeta_8 + x_2\zeta_8^2 + x_3\zeta_8^3)) = x_0 + 4x_1 + 16x_2 + 64x_3 \pmod{257},$$

$\forall\ x_0 + x_1\zeta_8 + x_2\zeta_8^2 + x_3\zeta_8^3 \in \langle 1 - \zeta_8 \rangle$.

Example 4.2. *As in the previous example, consider the ideal $\mathfrak{q} = \langle 2 - \zeta_8 \rangle$ of $\mathfrak{O}_{\mathbb{F}}$. Here, however, let $\mathfrak{p} = \mathfrak{q}$. Therefore,*

$$\langle 2 - \zeta_8 \rangle / \langle 4 - 4\zeta_8 + \zeta_8^2 \rangle \cong \mathbb{Z}_{17}.$$

Since $\zeta_8 \equiv 2 \pmod{\mathfrak{p}}$, then every $x_0 + x_1\zeta_8 + x_2\zeta_8^2 + x_3\zeta_8^3 \in \langle 2 - \zeta_8 \rangle$ receives the label 0, for:

$$\ell(x_0 + x_1\zeta_8 + x_2\zeta_8^2 + x_3\zeta_8^3) = x_0 + 2x_1 + 4x_2 + 8x_3 = 0 \pmod{17}.$$

Now, resorting to Proposition 2, and from $(y_0 + y_1\zeta_8 + y_2\zeta_8^2 + y_3\zeta_8^3) \cdot (2 - \zeta_8) = (x_0 + x_1\zeta_8 + x_2\zeta_8^2 + x_3\zeta_8^3)$, the following labeling results:

$$\lambda(\sigma(x_0 + x_1\zeta_8 + x_2\zeta_8^2 + x_3\zeta_8^3)) = \ell(y_0 + y_1\zeta_8 + y_2\zeta_8^2 + y_3\zeta_8^3) = y_0 + 2y_1 + 4y_2 + 8y_3 \pmod{17},$$

where: $x_0 = 2y_0 + y_3; x_1 = -y_0 + 2y_1; x_2 = -y_1 + 2y_2$; and $x_3 = -y_2 + 2y_3$, which implies

$$\lambda(\sigma(x_0 + x_1\zeta_8 + x_2\zeta_8^2 + x_3\zeta_8^3)) = 15x_0 + 13x_1 + 9x_2 + x_3 \pmod{17}.$$

5 A Four Dimensional Lattice Constellation

Using the techniques of the previous sections, here we will present a four dimensional lattice constellation $\mathcal{S}$ with 73 points linearly labeled by $GF(73)$. Its rate is $R = \log_2 73/4 = 1.5474$,

and its performance will be measured by the parameter $\kappa = \frac{d^2_{\min}}{E_{\text{av}}} \log_2 M$. For the same rate, the presented constellation compares favorably with spherical constellations [7].

The four dimensional lattice Λ associated to $\mathbb{Z}[\zeta_8]$ has a center density of 0.0625, whereas the sublattice Λ' associated to the ideal $(1-\zeta_8)\mathbb{Z}[\zeta_8]$ has a center density of 0.125. We will construct and label a 73-point constellation from Λ'.

The rational prime 73 splits in $\mathbb{Z}[\zeta_8]$ in prime ideals as $73\mathbb{Z}[\zeta_8] = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$, where $\mathfrak{p}_1 = \langle 10-\zeta_8\rangle$, $\mathfrak{p}_2 = \langle 63-\zeta_8\rangle$, $\mathfrak{p}_3 = \langle 22-\zeta_8\rangle$, and $\mathfrak{p}_4 = \langle 51-\zeta_8\rangle$. Hence,

$$\mathbb{Z}_{73} \cong \frac{\mathbb{Z}[\zeta_8]}{\mathfrak{p}_1} \cong \frac{\langle 1-\zeta_8\rangle}{\langle 1-\zeta_8\rangle\mathfrak{p}_1}.$$

Therefore,

$$\frac{\langle 1-\zeta_8\rangle}{\langle 10-11\zeta_8+\zeta_8^2\rangle} \cong \mathbb{Z}_{73}.$$

We have $\zeta_8 \equiv 10 \pmod{\mathfrak{p}_1}$. From this, the following linear labeling results:

$$\lambda(\sigma(x_0+x_1\zeta_8+x_2\zeta_8^2+x_3\zeta_8^3)) = x_0+10x_1+27x_2+51x_3 \pmod{73},$$

$\forall\ x_0+x_1\zeta_8+x_2\zeta_8^2+x_3\zeta_8^3 \in \langle 1-\zeta_8\rangle$.

Constellation $\mathcal{S}$ is identified in Table 1. The image via σ of an integer with coordinates (x_0,x_1,x_2,x_3) in the basis $\{1-\zeta_8, \zeta_8-\zeta_8^2, \zeta_8^2-\zeta_8^3, 1+\zeta_8^3\}$ (of the ideal $\langle 1-\zeta_8\rangle$) receives the label $\ell = x_0+10x_1+27x_2+51x_3 \bmod 73$. For $\mathcal{S}$, we have $\kappa = 3.1378$.

6 Some Optimal Constellations

In Table 2 we list some optimal constellations in dimensions from two through six. The constellations are described by their rate, minimum distance, and the parameter κ. We note that as the number of points grow, lattice constellations have a better performance in terms of κ, when compared to spherical constellations.

7 Conclusion

With q a power of a rational prime, finite lattice constellations of q points were constructed and labeled. The main idea was to choose a prime ideal $\mathfrak{p}$ of norm q in an algebraic number field $\mathbb{F}$, and then to consider the quotient $\mathfrak{O}_{\mathbb{F}}/\mathfrak{p}$ to realize the lattice partition. Proposition 3.1 and Definition 4.1 explain the labeling of the points in Λ, the lattice associated to $\mathfrak{O}_{\mathbb{F}}$ (or one of its ideals) by elements of $GF(q)$.

This method is a highly systematic procedure that allows the design of large constellations from complicated lattices in any dimension. Besides that, at the decoder, the generation of the decoded finite field symbol is very fast due to the linear labeling of the signal set. Nevertheless, once the constellation is generated and linearly labeled by elements of $GF(q)$,

ℓ	x_1	x_2	x_3	x_4	ℓ	x_1	x_2	x_3	x_4	ℓ	x_1	x_2	x_3	x_4
0	0	0	0	0	1	1	0	0	0	2	-2	-2	-1	1
3	-2	0	1	1	4	-1	0	1	1	5	0	0	1	1
6	1	1	-1	-1	7	0	-1	-1	-2	8	-1	-1	-2	0
9	-1	0	2	2	10	0	1	0	0	11	1	1	0	0
12	0	-1	0	-1	13	-1	-1	-1	1	14	-1	1	1	1
15	0	1	1	1	16	1	1	1	1	17	-2	-1	0	2
18	1	0	-1	-2	19	-1	1	2	2	20	-1	-2	-2	-1
21	-1	0	0	-1	22	0	0	0	-1	23	1	0	0	-1
24	-2	-2	-1	0	25	-1	-2	-1	0	26	-1	0	1	0
27	0	0	1	0	28	1	0	1	0	29	-2	-2	0	1
30	-1	-2	0	1	31	0	-1	-2	-1	32	0	1	0	-1
33	1	1	0	-1	34	2	1	0	-1	35	-1	-1	-1	0
36	0	-1	-1	0	37	0	1	1	0	38	1	1	1	0
39	-2	-1	0	1	40	-1	-1	0	1	41	0	-1	0	1
42	0	1	2	1	43	1	1	2	1	44	-2	-1	1	2
45	-1	0	-1	0	46	0	0	-1	0	47	1	0	-1	0
48	1	2	1	0	49	-2	0	0	1	50	-1	0	0	1
51	0	0	0	1	52	-1	-2	0	0	53	0	-1	-2	-2
54	-2	0	1	2	55	-1	0	1	2	56	0	0	1	2
57	-1	-1	-1	-1	58	0	-1	-1	-1	59	1	-1	-1	-1
60	1	1	1	-1	61	0	1	0	1	62	-1	-1	0	0
63	0	-1	0	0	64	0	1	2	0	65	-1	1	1	2
66	-2	-1	1	1	67	-1	-1	1	1	68	0	0	-1	-1
69	1	0	-1	-1	70	1	2	1	-1	71	-1	-2	-2	0
72	-1	0	0	0										

Table 1: 73-point constellation from $\mathbb{Z}[\zeta_8]$ labeled by $GF(73)$.

Code $[M,n]$	Description	$R=\frac{\log_2 M}{n}$	$d^2_{\min}$	K_{ira}
s $[6,5]$	Simplex [5]	0.50	2.4	6.204
$[5,3]$	multilevel [16]	0.77	2.143	4.975
s $[8,4]$	16-cell [5]	0.75	2.0	6.0
s $[4,2]$	Square	1.00	2.0	4.0
s $[16,4]$	Cyclic Polytope [6]	1.00	1.172	4.686
$[25,4]$	$\langle 21-55\zeta_{12}\rangle/(\mathfrak{p}_5\langle 21-55\zeta_{12}\rangle)$	1.16	1.040	4.837
s $[72,6]$	Ericson-Zinoviev [7]	1.03	1.0	6.170
s $[32,4]$	Ericson-Zinoviev [7]	1.25	0.667	3.330
$[37,4]$	$\langle 21-55\zeta_{12}\rangle/(\mathfrak{p}_{37}\langle 21-55\zeta_{12}\rangle)$	1.30	0.771	4.015
$[181,6]$	$\langle (1-\zeta_9)^2\rangle/(\mathfrak{p}_{181}\langle (1-\zeta_9)^2\rangle)$	1.25	0.628	4.710
s $[243,6]$	[7]	1.32	0.6	4.750
$[343,6]$	$\langle (1-\zeta_9)^2\rangle/(\mathfrak{p}_7\langle (1-\zeta_9)^2\rangle)$	1.40	0.560	4.720
s $[8,2]$	8-gon	1.50	0.586	1.760
$[73,4]$	$\langle 1-\zeta_8\rangle/(\mathfrak{p}_{73}\langle 1-\zeta_8\rangle)$	1.55	0.507	3.138
$[613,6]$	$\langle (1-\zeta_9)^2\rangle/(\mathfrak{p}_{613}\langle (1-\zeta_9)^2\rangle)$	1.54	0.431	3.990
s $[120,4]$	Schäfli $\{3,3,5\}$ [5]	1.73	0.309	2.130
$[157,4]$	$\langle 21-55\zeta_{12}\rangle/(\mathfrak{p}_{157}\langle 21-55\zeta_{12}\rangle)$	1.82	0.363	2.650
$[1459,6]$	$\langle (1-\zeta_9)^2\rangle/(\mathfrak{p}_{1459}\langle (1-\zeta_9)^2\rangle)$	1.75	0.312	3.280
s $[16,2]$	16-gon	2.00	0.152	0.610
$[16,2]$	16-QAM	2.00	0.4	1.600
$[241,4]$	$\langle 21-55\zeta_{12}\rangle/(\mathfrak{p}_{241}\langle 21-55\zeta_{12}\rangle)$	1.98	0.287	2.269
$[4051,6]$	$\langle (1-\zeta_9)^2\rangle/(\mathfrak{p}_{4051}\langle (1-\zeta_9)^2\rangle)$	1.99	0.232	2.780
$[64,2]$	64-QAM	3.00	0.095	0.571
$[4073,4]$	$\langle 1-\zeta_8\rangle/(\mathfrak{p}_{4073}\langle 1-\zeta_8\rangle)$	2.99	0.069	0.830

Table 2: Comparison between spherical group codes and lattice codes.

a general and fast way for picking out a constellation point, given a field element, is still missing. This operation is critical for transmission when large constellations are used.

Finally, although outside of the objectives of the present paper, another challenge in designing constellations having high rate, high minimum Euclidean distance, and low average signal power simultaneously, is to find rings of integers and ideals contained in them associated to very dense lattices [4].

References

[1] I. F. Blake, "The Leech lattice as a code for the Gaussian channel," *Information and Control*, **19** (1), pp. 66-74, August 1971.

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*. New York: Academic Press, 1966.

[3] A. R. Calderbank and N. J. A. Sloane, "New trellis codes based on lattices and cosets," *IEEE Trans. Inform. Theory,* vol. 33, No. 2, pp. 177-195, March 1987.

[4] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, New York: Springer-Verlag, 1988.

[5] H. S. M. Coxeter, *Regular Polytopes*. London: MacMillan, 1963.

[6] M. Elia, "Group codes and signal design for data transmission," *ISICT'87*, Campinas, Brazil, July 1987, pp. 235-254.

[7] T. Ericson and V. Zinoviev, *Codes on Euclidean Spheres*, North-Holland, 2001.

[8] G. D. Forney, Jr., M. D. Trott, and S.-Y. Chung, "Sphere-bound-achieving coset codes and multilevel coset codes," *IEEE Trans. on Inform. Theory*, vol. IT-46, pp. 820-850, May 2000.

[9] K. Huber, "Codes over Gaussian integers," *IEEE Trans. on Inform. Theory*, vol. 40, No. 1, pp. 207-216, January 1994.

[10] K. Huber, "Codes over Eisenstein-Jacobi integers," *AMS, Contemporary Mathematics*, vol. 158, pp. 165-179, 1994.

[11] I. Jacobs, "Comparisson of M-ary modulation systems," *Bell Syst. Tech. J.*, pp. 843-864, May-June 1967.

[12] R. A. Mollin, *Algebraic Number Theory*. Boca Raton: Chapman & Hall/CRC, 1999.

[13] T. P. da Nóbrega Neto, J.C. Interlando, O. M. Favareto, M. Elia, and R. Palazzo Jr., "Lattice constellations and codes from quadratic number fields," *IEEE Trans. on Inform. Theory*, vol. 42, No. 2, pp. 518-526, May 2001.

[14] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*. Cambridge University Press, 1989.

[15] N. J. A. Sloane, *Table of spherical codes*, published electronically at http://www.research.att.com/~njas/packings/index.html

[16] N. J. A. Sloane, R. H. Hardin, T. S. Duff, and J. H. Conway, "Minimal-energy clusters of hard spheres," *Discrete Computational Geom.*, 14 (1995), pp. 237-259.

[17] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Inform. Theory*, vol. IT-28, No. 1, pp. 55-67, January 1982.

[18] V.K. Wei, "q-ary turbo codes with QAM modulations," *5th IEEE Intern. Conf. on Universal Personal Communications*, vol. 2, pp. 814-817, September 1996, Cambridge, MA, USA.