Enabling multiplication in lattice codes via Construction A

Oggier, Frederique; Belfiore, Jean-Claude

2013

Frederique, O., & Jean-Claude, B. (2013). Enabling multiplication in lattice codes via Construction A. 2013 IEEE Information Theory Workshop (ITW), 1-5.

https://hdl.handle.net/10356/98610

https://doi.org/10.1109/ITW.2013.6691274

Enabling Multiplication in Lattice Codes via Construction A

Frédérique Oggier
Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University, Singapore
Email: frederique@ntu.edu.sg

Jean-Claude Belfiore
Dept of Communications & Electronics
Telecom ParisTech
Paris, France
Email: belfiore@telecom-paristech.fr

***Abstract*—As a first step towards distributed computations in a wireless network, we introduce ideal lattices, that is lattices built over an ideal of a ring of integers in a number field, as a tool for constructing lattice codes at the physical layer. These lattices are not only additive groups as all lattices, but they are also equipped with a multiplication, which enables polynomial operations at each node of the wireless network. In this paper, we show how some of these ideal lattices can be constructed from polynomial codes (generalization of cyclic codes) via Construction A, and illustrate how these lattices enable multiplication.**

I. Introduction

Connections between linear (N,k) codes, i.e., k-dimensional subspaces of $\mathbb{F}_q^N$, and lattices, i.e., discrete subgroups of $\mathbb{R}^N$, have been classically studied [1]. In the case of $q=2$, consider the projection $\rho : \mathbb{Z}^N \to \mathbb{F}_2^N$ where every component of N-dimensional integer vectors is reduced modulo 2. It is well known that

$$\Lambda_C := \frac{1}{\sqrt{2}}\rho^{-1}(C), \tag{1}$$

where C is a linear binary (N,k) code, is a lattice. This is referred to as Construction A. Furthermore, the lattice Λ_C is integral if and only if C is self-orthogonal, and Λ_C is unimodular if and only if C is self-dual. It is also known that the weight enumerator of C is closely related to the theta series of Λ_C.

There has been a recent renewed interest in these constructions of lattices from linear codes, motivated by lattice decoding and wiretap coding. In [2], the decoding of lattices obtained from a q-ary Construction A is considered, and a sphere decoder algorithm with respect to the Lee metric is proposed. In [3], an extension of Construction A, named Construction A', is introduced to construct Barnes-Wall lattices from linear codes over the polynomial ring $\mathbb{F}_2[u]/(u^m)$ for $m \geq 1$, though Construction A' does not always yield a lattice. Barnes-Wall lattices obtained that way enjoy an efficient decoding algorithm. In [4], connections between different constructions of lattices from codes, namely Construction D, Construction $\bar{D}$ and Construction A' are studied. In particular, it is shown that lattices from Construction $\bar{D}$ can be obtained from Construction A', which in turn gives a partial condition to decide when Construction A' provides a lattice.

Wiretap codes are codes designed to achieve both reliability and confidentiality between two legitimate users, in the presence of an eavesdropper. Wiretap encoding is performed using coset encoding, which can be implemented using Construction A. For wiretap fading channels, lattice codes are typically built from lattices obtained from number fields [5]. This motivated the study of Construction A in the context of number fields [6]. The construction goes as follows. Let K be a number field which is either totally real of CM, with ring of integers $\mathcal{O}_K$. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_K$ above $p \in \mathbb{Z}$. Let $\rho : \mathcal{O}_K^N \to (\mathcal{O}_K/\mathfrak{P}\mathcal{O}_K)^N$ be the group homomorphism that reduces componentwise modulo the ideal $\mathfrak{P}$. Since $\mathfrak{P}$ is prime, $\mathcal{O}_K/\mathfrak{P}\mathcal{O}_K$ is a finite field $\mathbb{F}$ of characteristic p. Let $C \subset \mathbb{F}^N$ be a linear code of length N. Then

$$\Lambda_C := \rho^{-1}(C)$$

is a lattice, that is a free $\mathbb{Z}$-module, with the symmetric bilinear form $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^N \mathrm{Tr}_{K/\mathbb{Q}}(\mathbf{x}_i \mathbf{y}_i)$, $\mathbf{x}, \mathbf{y} \in \mathcal{O}_K^N$, if K is totally real, or $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^N \mathrm{Tr}_{K/\mathbb{Q}}(\mathbf{x}_i \bar{\mathbf{y}}_i)$ if K is CM, with $\bar{\mathbf{y}}_i$ the complex conjugate of $\mathbf{y}_i$. Note that the bilinear form takes integral values (since $\mathbf{x}_i\mathbf{y}_i$ respectively $\mathbf{x}_i\bar{\mathbf{y}}_i$ belong to $\mathcal{O}_K$), and is positive definite. When C is a self-dual code, it is actually more natural to consider the normalized lattice

$$\Lambda_C := \frac{1}{\sqrt{p}}\rho^{-1}(C)$$

to study the classical connections between lattices and codes [6]. The construction described above is often written as

$$\Lambda_C = (\mathfrak{P}\mathcal{O}_K)^N + C \tag{2}$$

following [7]. Note that this notation does not make the scaling explicit. Let p be a prime, and ζ_p be a primitive pth root of unity. This construction generalizes the classical Construction A on the cyclotomic field $\mathbb{Q}(\zeta_p)$ [8], where $\mathfrak{P} = (1-\zeta_p)$. When $p=2$, this is the classical binary Construction A of (1). Note that constructions of lattices over number fields have been studied independently of their connections to linear codes, see e.g. [9], and because they can be extended to ideals, they are referred to as ideal lattices.

In this paper, we investigate the connection between linear codes and lattices from number fields, when $N=1$. Our motivation is however different. In [10], a transmission strategy

for wireless networks relying on lattice codes called "compute-and-forward" has been proposed, where relays decode a linear integral combination of the transmitted signals, treating the wireless channel as a natural computer. The motivation of [10] was to exploit interference to obtain a high so-called "computation rate" in the wireless network, which is the reason why compute-and-forward has been related to physical layer network coding.

We are however interested in the potential of the compute-and-forward scheme for not only linear but also non-linear distributed computations over a wireless network. This requires the existence of a multiplication in the lattice code. The contribution of this paper is to propose lattices over number fields to enable this multiplication, allowing, in a similar way as in [10], the computation of multivariate polynomial functions of lattice points.

A general construction is presented in Section II, where we propose a Construction A from a number field K with a totally ramified prime, which associates a lattice of rank $[K:\mathbb{Q}]$ to a polynomial code. Our approach is also compared to that of [11], which studied the problem of finding lattices with a multiplication for cryptographic applications. Section III illustrates this construction with the cyclotomic fields $\mathbb{Q}(\zeta_{2^m})$, $m \geq 3$, where ζ_{2^m} is a primitive 2^mth root of unity. The existence of a similar Construction A as proposed in Section II, however with a prime which is not totally ramified, is exhibited in Section IV. We conclude by illustrating in Section V how, by using a nested pair of these lattices (as in [10], one lattice serves for coding while the other one is for shaping), we get a natural structure of finite ring for the transmitted multidimensional constellation which enables local nonlinear computations at the relay level. Future reasearch directions are mentioned in the conclusion.

II. Construction A with a Totally Ramified Prime

Let K/F be an extension of number field of degree n, with respective rings of integers $\mathcal{O}_K$ and $\mathcal{O}_F$. Suppose that $p \in \mathbb{Z}$ is totally ramified in K, that is

$$p\mathcal{O}_K = \mathfrak{P}^{n[F:\mathbb{Q}]}$$

for some prime ideal $\mathfrak{P}$.

The quotient of $\mathcal{O}_K$ by $\mathfrak{P}^r$ is known [12], for any $r \leq n$.

Proposition 1: Let $p \in \mathbb{Z}$ be a prime which is totally ramified in K, and let $\mathfrak{P}$ denote the unique prime of $\mathcal{O}_K$ above p. Then

$$\mathcal{O}_K/\mathfrak{P}^r\mathcal{O}_K \simeq \mathbb{F}_p[X]/(X^r),$$

where $\mathbb{F}_p$ is the finite field with p elements.

Corollary 1: Suppose that 2 is totally ramified in K and that r is a power of 2. Then

$$\mathcal{O}_K/\mathfrak{P}^r\mathcal{O}_K \simeq \mathbb{F}_2[X]/(X^r+1).$$

Proof: Using Proposition 1, it is enough to show that

$$\mathbb{F}_2[X]/(X^r+1) \simeq \mathbb{F}_2[X]/(X^r).$$

Let $\phi : \mathbb{F}_2[X]/(X^r+1) \to \mathbb{F}_2[X]/(X^r)$ be the bijection defined by $\phi(\sum_{i=0}^{r-1} a_i X^i \pmod{X^r+1}) = \sum_{i=0}^{r-1} a_i (X+1)^i \pmod{X^r}$. That it is a ring homomorphism follows from the fact that

$$\begin{aligned} 1 &= \phi(X^r \mod X^r+1) \\ &= (X+1)^r \mod X^r \\ &= X^r+1 \mod X^r \\ &= 1 \mod X^r \end{aligned}$$

using that r is a power of 2. ∎

We denote by ψ the isomorphism

$$\mathcal{O}_K/\mathfrak{P}^r\mathcal{O}_K \simeq \mathbb{F}_p[X]/(X^r).$$

Since $\mathfrak{P}$ is an ideal of $\mathcal{O}_K$, $\mathfrak{P}\mathcal{O}_K/\mathfrak{P}^r\mathcal{O}_K$ is an ideal of $\mathcal{O}_K/\mathfrak{P}^r\mathcal{O}_K$, and $\psi(\mathfrak{P}\mathcal{O}_K/\mathfrak{P}^r\mathcal{O}_K)$ is an ideal of $\mathbb{F}_p[X]/(X^r)$.

Since $\mathbb{F}_p[X]/(X^r)$ is a principal ideal domain, every ideal, and thus in particular $\psi(\mathfrak{P}\mathcal{O}_K/\mathfrak{P}^r\mathcal{O}_K)$, is principal, generated by say the polynomial $g(X)$. To this ideal corresponds a polynomial code C formed by codewords $(c_0,\ldots,c_{r-1})$ where $\sum_{i=0}^{r-1} c_i X^i$ is a multiple of $g(X)$, called the generator polynomial of C.

Now $\mathfrak{P}\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}] = n[F:\mathbb{Q}]$, and it forms a lattice together with the symmetric bilinear form $\langle x,y\rangle = \mathrm{Tr}_{K/\mathbb{Q}}(xy)$ if K is totally real, and $\langle x,y\rangle = \mathrm{Tr}_{K/\mathbb{Q}}(x\bar{y})$ if K is CM, and $\bar{y}$ denotes the complex conjugation. When F is a principal ideal domain, $\mathcal{O}_K$ has an $\mathcal{O}_F$-basis, and we may instead consider $\mathfrak{P}\mathcal{O}_K$ with respectively $\langle x,y\rangle = \mathrm{Tr}_{K/F}(xy)$ or $\langle x,y\rangle = \mathrm{Tr}_{K/F}(x\bar{y})$.

We will denote by $\Lambda_{\mathfrak{P}}$ the lattice $(\mathfrak{P}\mathcal{O}_K, \mathrm{Tr}_{K/\mathbb{Q}})$, or also the lattice $(\mathfrak{P}\mathcal{O}_K, \mathrm{Tr}_{K/F})$, and, using the notation of (2), we have

$$\Lambda_{\mathfrak{P}} = \mathfrak{P}^r\mathcal{O}_K + C, \tag{3}$$

where C is the polynomial code corresponding to the ideal $\psi(\mathfrak{P}\mathcal{O}_K/\mathfrak{P}^r\mathcal{O}_K)$, and a possible scaling is not made explicit. Note how this construction relates to the traditional Construction A as described in (2):

- In this case, we consider $N=1$, that is only one copy of $\mathcal{O}_K$. This means that the lattice we consider is of rank $[K:\mathbb{Q}]$ instead of $N[K:\mathbb{Q}]$.
- In the usual Construction A, we choose a code C and $\rho^{-1}(C)$ defines a lattice, which is a sublattice of $\mathcal{O}_K^N$. Here, we are interested in the sublattice $\mathfrak{P}\mathcal{O}_K$ of $\mathcal{O}_K$, and we consider the whole of $\mathfrak{P}\mathcal{O}_K/\mathfrak{P}^r\mathcal{O}_K$ as a code, and do not look for a code inside $\mathfrak{P}\mathcal{O}_K/\mathfrak{P}^r\mathcal{O}_K$.

Having in mind applications to cryptographiy, Gentry introduced in [11] what he called "ideal lattices", which are lattices constructed by embedding ideals of the ring $\mathbb{Z}[X]/\phi(X)$ into $\mathbb{R}^n$, where $\phi(X)$ is a cyclotomic polynomial of degree n. The goal of [11] was to obtain lattices with a multiplication which are hard to decode. The schemes explicitly constructed were obtained by choosing $n=2^m$ and the cyclotomic polynomial $\phi(X) = X^{2^m}+1$ for some $m \geq 2$. The embedding of [11] is done as follows:

- Choose a polynomial $a(X) = \sum_{i=0}^{n-1} a_i X^i$ in $\mathbb{Z}[X]$ of degree at most $n-1$, and construct the corresponding vector $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$.
- For each $i = 1, 2, \ldots, n-1$, compute the polynomial

$$a^{(i)}(X) = X^i a(X) \pmod{\phi(X)} = \sum_{j=0}^{n-1} a_j^{(i)} X^j$$

and construct the corresponding vector $\mathbf{a}^{(i)} = (a_0^{(i)}, a_1^{(i)}, \ldots, a_{n-1}^{(i)})$.
- The matrix M whose i^{th} row is $\mathbf{a}^{(i+1)}$ with $\mathbf{a}^{(0)} = \mathbf{a}$ is a generator matrix of the ideal lattice generated by $a(X)$.

Though both the work of [11] and this paper aim at enabling multiplication in lattices, the actual lattice construction, and in particular (1) the way the lattices are embedded and (2) the properties that the lattices should fullfil, are very different. In this paper, we are interested in nested lattice codes, since nested lattice codes can achieve the capacity of the Gaussian channel with a power constraint [13]. Furthermore, ideal lattices for us will mean lattices obtained from the canonical embedding of an ideal of the ring of integers of some number field, and our design criterion will be ideal lattices which are good for coding in presence of Gaussian noise. These ideal lattices will be constructed from some polynomial codes, which are generalizations of cyclic codes.

III. Construction A from some Cyclotomic Fields

Let $\zeta := \zeta_{2^m}$ be a primitive 2^mth root of unity, $m \geq 3$, and consider the cyclotomic field $K = \mathbb{Q}(\zeta)$. Since the minimum polynomial of ζ is $X^{2^{m-1}} + 1 = \prod_{i=1}^{2^{m-1}} (X - \sigma(\zeta))$ where σ_i, $i = 1, \ldots, 2^{m-1}$ form the Galois group of K over $\mathbb{Q}$, we have, evaluating the polynomial in $X = 1$ that

$$2 = \prod_{i=1}^{2^{m-1}} (1 - \sigma_i(\zeta)),$$

showing that

$$2\mathcal{O}_K = (1-\zeta)^{2^{m-1}} \mathcal{O}_K.$$

Thus 2 is totally ramified in K, and we are in the framework of Section II, with $\mathfrak{P} = (1-\zeta)$.

A. Polynomial Code Construction

Using Corollary 1, we know that

$$\mathcal{O}_K/(1-\zeta)^r \mathcal{O}_K \simeq \mathbb{F}_2[X]/(X^r + 1)$$

for r a power of 2. Take $r = 2^{m-2}$. Since $\zeta^{2^{m-2}} = i$ is a primitive fourth root of unity, and $2\mathcal{O}_K = (1+i)(1-i)\mathcal{O}_K$, we have that

$$\begin{aligned} \mathcal{O}_K/(1-\zeta)^{2^{m-2}} \mathcal{O}_K &= \mathcal{O}_K/(1+i)\mathcal{O}_K \\ &\simeq \mathbb{F}_2[X]/(X^{2^{m-2}} + 1), \end{aligned}$$

where this isomorphism is denoted by ψ as in Section II. Now $(1-\zeta)\mathcal{O}_K/(1+i)\mathcal{O}_K$ is an ideal of $\mathcal{O}_K/(1+i)\mathcal{O}_K$, and

$$\psi((1-\zeta)\mathcal{O}_K/(1+i)\mathcal{O}_K) = (1+X)\mathbb{F}_2[X]/(X^{2^{m-2}} + 1).$$

The polynomial code C corresponding to the ideal $(1+X)\mathbb{F}_2[X]/(X^{2^{m-2}} + 1)$ of the ring $\mathbb{F}_2[X]/(X^{2^{m-2}} + 1)$ is found by using the generator polynomial $g(X) = 1 + X \pmod{X^{2^{m-2}} + 1}$. Multiples of $g(X)$ are of the form

$$\begin{aligned} & (a_0 + a_1 X + \ldots + a_{2^{m-2}-1} X^{2^{m-2}-1})(1+X) \\ = & \sum_{i=0}^{2^{m-2}-1} a_i X^i + \sum_{i=1}^{2^{m-2}} a_{i-1} X^i \\ = & \; a_0 + \sum_{i=1}^{2^{m-2}-1} (a_i + a_{i-1}) X^i + a_{2^{m-2}-1} X^{2^{m-2}}, \end{aligned}$$

with $a_i \in \mathbb{F}_2$, yielding the codeword

$$(a_0 + a_{2^{m-2}-1}, a_0 + a_1, a_1 + a_2, \ldots, a_{2^{m-2}-2} + a_{2^{m-2}-1}).$$

Since the sum of all the components but the last one is

$$a_0 + a_{2^{m-2}-1} + \sum_{i=1}^{2^{m-2}-2} (a_i + a_{i-1}) = a_{2^{m-2}-2} + a_{2^{m-2}-1},$$

we recognize that the code C is the $(2^{m-2}, 2^{m-2}-1)_{\mathbb{F}_2}$ parity check code, and using the notation introduced in (3), we get

$$\Lambda_{(1-\zeta)} = (1+i)\mathcal{O}_K + \left(2^{m-2}, 2^{m-2} - 1\right)_{\mathbb{F}_2}. \qquad (4)$$

B. Lattice Construction

Let us next look at the term $(1+i)\mathcal{O}_K$, and set $F = \mathbb{Q}(i)$. Since $K = \mathbb{Q}(\zeta)$, it is known that $\mathcal{O}_K = \mathbb{Z}[\zeta]$, and an integral basis is $\{1, \zeta, \zeta^2, \ldots, \zeta^{2^{m-1}-1}\}$. Since $\zeta^{2^{m-2}+l} = i\zeta^l$, we have that $\{1, \zeta, \zeta^2, \ldots, \zeta^{2^{m-2}-1}\}$ is a $\mathbb{Z}[i]$-basis of $\mathcal{O}_K$.

Lemma 1: The lattice $(\mathcal{O}_K, \frac{1}{2^{m-2}} \mathrm{Tr}_{K/\mathbb{Q}(i)})$ is isomorphic to $\mathbb{Z}[i]^{2^{m-2}}$.

Proof: It is immediate to compute that

$$\mathrm{Tr}_{K/\mathbb{Q}(i)}(\zeta^i \zeta^j) = \begin{cases} 0 & i+j \neq 2^m \\ 2^{m-2} & i+j = 0 \pmod{2^m} \end{cases}$$

thus

$$\mathrm{Tr}_{K/\mathbb{Q}(i)}(\zeta^i \bar{\zeta^j}) = \mathrm{Tr}_{K/\mathbb{Q}(i)}(\zeta^i \zeta^{-j}) = \begin{cases} 0 & i \neq j \\ 2^{m-2} & i = j \end{cases}$$

which shows that the lattice $(\mathcal{O}_K, \frac{1}{2^{m-2}} \mathrm{Tr}_{K/\mathbb{Q}(i)})$ is isomorphic to the lattice $\mathbb{Z}[i]^{2^{m-2}}$. ∎

Note that a generator matrix of this lattice is $\frac{1}{\sqrt{2^{m-2}}} B$, with B given by

$$B = \begin{bmatrix} \tau_1(1) & \tau_2(1) & \ldots & \tau_{2^{m-2}}(1) \\ \tau_1(\zeta) & \tau_2(\zeta) & \ldots & \tau_{2^{m-2}}(\zeta) \\ & & & \\ \tau_1(\zeta^{2^{m-2}-1}) & \tau_2(\zeta^{2^{m-2}-1}) & & \tau_{2^{m-2}}(\zeta^{2^{m-2}-1}) \end{bmatrix}$$

where the τ_i form the Galois group of K/F, and the corresponding Gram matrix is

$$\frac{1}{2^{m-2}} B B^H = \mathbf{I}_{2^{m-2}}.$$

We may alternatively write, keeping the notation of (3), that

$$\Lambda_{(1-\zeta)} = (1+i)\mathbb{Z}[i]^{2^{m-2}} + \left(2^{m-2}, 2^{m-2} - 1\right)_{\mathbb{F}_2} \qquad (5)$$

where the isomorphism $(1+i)\mathcal{O}_K \simeq (1+i)\mathbb{Z}[i]^{2^{m-2}}$ is understood.

C. Lattice Identification

As a last step, we will identify the lattice $\Lambda_{(1-\zeta)}$ as being the checkerboard lattice $D_{2^{m-1}}$. Recall [1] that D_n, for $n \geq 3$ is defined by

$$D_n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n,\ x_1 + \ldots + x_n \text{ even }\}. \qquad (6)$$

To best recognize the lattice $\Lambda_{(1-\zeta)}$, we will see it next as a real lattice.

Note first that $((1+i)\mathcal{O}_K, \frac{1}{2^{m-1}}\mathrm{Tr}_{K/\mathbb{Q}})$ is isomorphic to the lattice $\mathbb{Z}^{2^{m-1}}$. The proof is similar to that of Lemma 1. A generator matrix for the real lattice though is obtained slightly differently. Let $\sigma_1, \ldots, \sigma_{2^{m-1}}$ be the Galois group of $K/\mathbb{Q}$. Galois automorphisms come in pair of complex conjugates. Let us pick one automorphism per pair, and label them from σ_1 to $\sigma_{2^{m-2}}$. The generator matrix of the real lattice will be $\frac{1}{\sqrt{2^{m-1}}}B'$, with B' given by

$$\begin{bmatrix} \Re\sigma_1(1) & \Im\sigma_1(1) & \ldots & \Re\sigma_{2^{m-2}}(1) & \Im\sigma_{2^{m-2}}(1) \\ \Re\sigma_1(\zeta) & \Im\sigma_1(\zeta) & \ldots & \Re\sigma_{2^{m-2}}(\zeta) & \Im\sigma_{2^{m-2}}(\zeta) \\ & & & & \\ \Re\sigma_1(\zeta^{2^{m-1}-1}) & & \ldots & & \Im\sigma_{2^{m-1}}(\zeta^{2^{m-1}-1}) \end{bmatrix}$$

where $\Re$ and $\Im$ denote respectively the real and the imaginary part of their argument. The matrix B' describes exactly a $\mathbb{Z}$-basis of the lattice $(1+i)\mathcal{O}_K$ from (4), however it is not straightforward to identify the real lattice based on (4) and B'. We will thus instead work with (5), and assume that $(1+i)\mathbb{Z}[i]^r$, $r = 2^{m-2}$, is given in a canonical basis. Consider the vector $(1+i)(v_1, \ldots, v_r) + (b_1, \ldots, b_r) \in (1+i)\mathbb{Z}[i]^r + C$, where C is the $(r, r-1)_{\mathbb{F}_2}$ parity check code, and rewrite it by separating the real and imaginary part of every component $v_j = v_{j1} + iv_{j2}$, $v_{j1}, v_{j2} \in \mathbb{Z}$ to get

$$(v_{11} - v_{12} + b_1, v_{12} + v_{11}, \ldots, v_{r1} - v_{r2} + b_r, v_{r2} + v_{r1}) \in \mathbb{Z}^{2r}.$$

To show that the lattice obtained is $D_{2^{m-1}}$, it is enough (see (6)) to check that the sum of the components of this vector is even. This sum is given by

$$\begin{aligned} & \sum_{j=1}^{r}[(v_{j1} - v_{j2} + b_j) + v_{j1} + v_{j2}] \\ = & \sum_{j=1}^{r}[2v_{j1} + b_j] \\ = & \ 2\sum_{j=1}^{r} 2v_{j1} + \sum_{j=1}^{r} b_j. \end{aligned}$$

The second sum is even by definition of a parity check code, since b_r has the same parity as $\sum_{j=1}^{r-1} b_j$. This shows that

$$\Lambda_{(1-\zeta)} = (1+i)\mathbb{Z}[i]^{2^{m-2}} + \left(2^{m-2}, 2^{m-2} - 1\right)_{\mathbb{F}_2} \simeq D_{2^{m-1}}.$$

D. Example

We conclude this section by providing a worked out example.

Suppose that $m = 3$, and consider the cyclotomic field $K = \mathbb{Q}(\zeta_8)$, where $\zeta := \zeta_8$ is a primitive 8th root of unity. It is of degree 4 over $\mathbb{Q}$. Since $r = 2$, consider the ideal $(1-\zeta)^2\mathbb{Z}[\zeta]$. Since $(1+\zeta)(-\zeta+\zeta^2-\zeta^3) = (1-\zeta)$ and $i(1-i) = (1+i)$, we have that

$$(1-\zeta)^2\mathbb{Z}[\zeta] = (1-\zeta)(1+\zeta)\mathbb{Z}[\zeta] = (1-i)\mathbb{Z}[\zeta] = (1+i)\mathbb{Z}[\zeta],$$

so that

$$\mathbb{Z}[\zeta]/(1-\zeta)^2\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta]/(1+i)\mathbb{Z}[\zeta] \simeq \mathbb{F}_2[X]/(X^2+1)$$

is a ring with 4 elements, where the isomorphism $\psi : \mathbb{Z}[\zeta]/(1+i)\mathbb{Z}[\zeta] \to \mathbb{F}_2[X]/(X^2+1)$ is here given explicitly by

$$\begin{aligned} & \psi(a + b\zeta + c\zeta^2 + d\zeta^3 \pmod{1+i}) \\ = & \ (a+c) + (b+d)X \pmod{1+X^2}. \end{aligned}$$

Hence $\psi((1-\zeta)\mathbb{Z}[\zeta]/(1+i)\mathbb{Z}[\zeta]) = (1+X)\mathbb{F}_2[X]/(X^2+1)$. We next compute the polynomial code corresponding to the generator polynomial $g(X) = 1 + X$:

$$\begin{aligned} & (a_0 + a_1X)g(X) \\ = & \ (a_0 + a_1X)(1+X) \\ = & \ a_0 + X(a_0+a_1) + a_1X^2 \\ = & \ (a_0+a_1) + X(a_0+a_1) \pmod{X^2+1} \end{aligned}$$

showing that the codebook is

$$\{(a_0 + a_1, a_0 + a_1),\ a_0, a_1 \in \mathbb{F}_2\} = \{(00), (11)\}$$

which is the $(2,1)$ parity check code, which in fact is also the repetition code. $K = \mathbb{Q}(\zeta)$ has degree 4 over $\mathbb{Q}$, and ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_8]$, with integral basis $\{1, \zeta, \zeta^2, \zeta^3\} = \{1, \zeta, i, i\zeta\}$, and a $\mathbb{Z}[i]$-basis is $\{1, \zeta\}$. It is simpler to compute on this example that the generator matrix of this lattice is

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

and that

$$BB^H = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}.$$

Let $\sigma_1 : \zeta \mapsto \zeta$, $\sigma_2 : \zeta \mapsto -\zeta$, $\sigma_3 : \zeta \mapsto i\zeta$, $\sigma_4 : \zeta \mapsto -i\zeta$ be the four Galois automorphims of $K/\mathbb{Q}$. There are two pairs of Galois automorphisms: (σ_1, σ_4) and (σ_2, σ_3). By considering σ_1 and σ_2, and recalling that $\zeta = (1+i)/\sqrt{2}$, the generator matrix of the real lattice corresponding to $(1+i)\mathcal{O}_K$ is

$$B' = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & \sqrt{2} & 0 & -\sqrt{2} \\ -1 & 1 & -1 & 1 \\ -\sqrt{2} & 0 & \sqrt{2} & 0 \end{bmatrix}$$

and it is easy to check that $BB^T = 4\mathbf{I}_4$.

IV. Construction of E_8

The next construction illustrates that the requirement to work with a prime which is totally ramified is not necessary. Because of space constraints, this construction is much less detailed than that above.

Consider the cyclotomic field $K = \mathbb{Q}(\zeta_{24})$ of degree $\varphi(24) = 8$. Note that it contains $F = \mathbb{Q}(j)$ as a subfield, where $j = \zeta_3$, and K/F is of degree 4, with minimal

polynomial $\varphi(X) = X^4 + j$. The respective rings of integers are $\mathcal{O}_K = \mathbb{Z}[\zeta_{24}]$ and $\mathcal{O}_F = \mathbb{Z}[j]$. It can be computed that $\Lambda_{\mathcal{O}_K} = (\mathcal{O}_K, \mathrm{Tr}_{K/F}) \simeq A_2^4$. By noting that $\zeta_{24} = \zeta_8\zeta_3 = \zeta_8 j$, and by writing that $\mathbb{Q}(\zeta_{24})$ is the compositum of $\mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(j)$, this can be proven by using Lemma 1, and by computing the lattice obtained over $\mathcal{O}_F$.

We consider the prime $p = 3$. In $\mathbb{Z}[j]$, we have $3\mathbb{Z}[j] = -\sqrt{-3}\sqrt{-3}\mathbb{Z}[j] = \mathfrak{p}^2$ and in turn

$$\sqrt{-3}\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$$

where $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are principal. Take

$$\mathfrak{P}_1 = (j\zeta_{24}^2 + j\zeta_{24} - 1). \tag{7}$$

Since $\mathbb{Z}[j]/\mathfrak{p} \simeq \mathbb{F}_3$, we will build a polynomial code over the ring $\mathbb{F}_3[X]/(X^4+1)$, which means that the polynomial code that we will get is a negacyclic code. Recall that a negacyclic code is a linear code with the property that if $(c_1, \ldots, c_n)$ is a codeword, then so is $(-c_n, c_1, \ldots, c_{n-1})$. The generator polynomial $g(X)$ of the code is next obtained from (7) as

$$g(X) = X^2 + X - 1.$$

We recognize the generator polynomial of the tetracode over $\mathbb{F}_3$ [1]. It has length 4, dimension 2 and minimum Hamming distance 3.

To summarize

$$\begin{aligned}\Lambda_{\mathfrak{P}} &= (2+j)\mathbb{Z}[j]^4 + (4,2,3)_{\mathbb{F}_3} \\ &\simeq \sqrt{-3}A_2^4 + (4,2,3)_{\mathbb{F}_3},\end{aligned}$$

which corresponds to E_8 [1, Ex. 11b of Chap. 7].

V. Algebraic structure of the constellation

To conclude, we discuss how the algebraic structure that the ideal lattices inherit can be exploited for coding, or computing, over wireless relay networks.

To start with, the transmitted constellation is not the full ideal lattice $\Lambda_{\mathfrak{P}}$ as constructed above, but the set of coset representatives with smallest norms of the quotient group $\Lambda_{\mathfrak{P}}/\Lambda_s$ where $\Lambda_s \subset \Lambda_{\mathfrak{P}}$ is the shaping lattice [7]. Note that Λ_s will naturally be an ideal lattice as well. As a result, the quotient $\Lambda_{\mathfrak{P}}/\Lambda_s$ both has an additive as well as a multiplicative structure (it is a finite ring), enabling computations. This is illustrated next on the example developed in Subsection III-D.

Example 1: Let ζ be a primitive 8th root of unity and $K = \mathbb{Q}(\zeta)$. Recall that the lattice constructed was

$$\Lambda_{(1-\zeta)} = (1+i)\mathbb{Z}[i]^2 + (2,1) \simeq D_4,$$

that is

$$D_4 \simeq (1+\zeta)\mathcal{O}_K$$

where $\mathcal{O}_K = \mathbb{Z}[\zeta]$. Now, suppose that we want a $4-$dimensional constellation with 16 points and use the shaping lattice $2D_4 \simeq 2(1+\zeta)\mathcal{O}$. Then, the transmitted constellation will be

$$D_4/2D_4 \simeq \mathcal{O}_K/2\mathcal{O}_K \simeq \mathbb{F}_2[u]/(u^4)$$

since $(1+\zeta)^4\mathcal{O}_K = 2\mathcal{O}_K$. Thanks to the constellation $D_4/2D_4$, we are able to perform, at each node, any polynomial computation on the finite ring $\mathbb{F}_2[u]/u^4$ by mapping u to $1+\zeta_8$ through the canonical embedding of $\mathbb{Q}(\zeta_8)$.

VI. Conclusion

We proposed new constructions of lattices from codes, where lattices are built over the ring of integers of a number field, obtaining thus new Constructions A. This is motivated by the need to have lattices with not only an additive structure, but also with a multiplication, for application to nonlinear distributed computing over a wireless network. Future work involves providing more constructions, understanding the properties of these lattices better, and address the problem of evaluating the maximal rate at which such nonlinear computation can be done reliably.

Acknowledgment

The research of F. Oggier for this work is supported by the Nanyang Technological University under Research Grant M58110049.

References

[1] J.H. Conway, N.J.A. Sloane, "Sphere Packings, Lattices and Groups", *Springer*.

[2] A.C. Campello Jr., G.C. Jorge, S.I.R. Costa, "Decoding q-ary lattices in the Lee metric", *International Workshop on Information Theory (ITW)*, Paraty, 2011.

[3] J. Harshan, E. Viterbo, and J.-C. Belfiore, "Construction of Barnes-Wall lattices from linear codes over rings", *IEEE International Symposium on Information Theory (ISIT) 2012*, USA.

[4] W. Kositwattanarerk, F. Oggier, "On Construction D and Related Constructions of Lattices from Linear Codes", *International Workshop on Coding and Cryptography (WCC) 2013*, Norway.

[5] J.-C. Belfiore, F. Oggier, "Lattice Code Design for the Rayleigh Fading Wiretap Channel", *International Conference on Communications (ICC) 2011*, Kyoto.

[6] W. Kositwattanarerk, S.S. Ong, F. Oggier, "Wiretap Encoding of Lattices from Number Fields Using Codes over $\mathbb{F}_p$", *IEEE International Symposium on Information Theory (ISIT) 2013*, Turkey.

[7] G. D. Forney, "Coset Codes – Part I: Introduction and geometrical classification, " *IEEE Trans. on Inform. Theory*, vol. 34, No 5, Sep. 1988.

[8] W. Ebeling, "Lattices and Codes, A Course Partially Based on Lectures by Friedrich Hirzebruch", Series: Advanced Lectures in Mathematics, *Springer*.

[9] E. Bayer-Fluckiger, "Ideal Lattices", in the Proceedings of the conference in honor of Alan Baker, Number Theory and Diophantine Geometry, *Cambridge Univ. Press* (2002).

[10] B. Nazer and M. Gastpar, "Compute-and-Forward: Harnessing Interference Through Structured Codes," *IEEE Trans. on Inform. Theory*, vol. 57, no 10, Oct. 2011.

[11] C. Gentry, "Fully homomorphic Encryption using Ideal Lattices," *STOC'09*, 2009, Bethesda, Maryland.

[12] M. Elia, J.C. Interlando, R. Rosenbaum, "On the Structure of Residue Rings of Prime Ideals in Algebraic Number Fields - Part II: Ramified Primes", *International Mathematical Forum*, vol. 6, no. 12, 2011.

[13] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1+\mathsf{SNR})$ over the Additive White Gaussian Noise Channel with Lattice Encoding and Decoding", *IEEE Trans. on Inform. Theory*, vol. 50, No 10, Oct. 2004.