# Lattice Network Coding over Euclidean Domains

M. A. Vázquez-Castro, Frédérique Oggier

***Abstract*—We propose a novel approach to design and analyse lattice-based network coding. The underlying alphabets are carved from (quadratic imaginary) Euclidean domains with a known Euclidean division algorithm, due to their inherent algorithmical ability to capture analog network coding computations. These alphabets are used to embed linear $p$-ary codes of length $n$, $p$ a prime, into $n$-dimensional Euclidean ambient spaces, via a variation of the so-called Construction A of lattices from linear codes. A study case over one such Euclidean domain is presented and the nominal coding gain of lattices obtained from $p$-ary Hamming codes is computed for any prime $p$ such that $p \equiv 1 \pmod 4$.**

***Index Terms*—Euclidean Domains, Network Coding, Lattices.**

## I. Introduction

Lattice codes are the Euclidean space counterparts of linear codes over finite fields. They have been extensively studied in communications and networking, for transmission over continuous channels.

Lattice codes provide a classical information theoretic way to obtain achievable rates for point-to-point Gaussian channels (e.g. [1], [2], and [3]), and it is known that rates up to $(1/2)\log(1+SNR)$ can be achieved using nested lattices together with the minimum-mean square error (MMSE) estimator. From a coding point of view, codes for Gaussian channels are sphere packings, and lattices yielding dense sphere packings have been identified (see [4]) in small dimensions (4, 5, 6, 7, and 8). In particular, linear codes can be used as a mean to get good lattice sphere packings, via the so-called Construction A [4]: for example, in dimension 8 the best known packing is the Gosset lattice $E_8$, obtained by Construction A using a length 8 Hamming code, and in dimension 24, the optimal packing is the Leech lattice, which can also be obtained from a linear code.

Lattice codes have started to play a role in networking with the advent of physical-layer network coding (PNC). PNC was first introduced in [5] and early subsequent research focused on three different aspects: PNC as a modulation-demodulation technique (e.g. [6]), joint design of PNC and channel coding, and its use in wireless networks (primarily for simple relay networks e.g. [7] or [8]). Later works merged these aspects as in the information theoretical work [9], where the relaying mechanism compute and forward (CF) is introduced by which the receiver noise is completely removed before forwarding while analog computing is retrieved by appropriate mappings. Such a mechanism is translated into coding strategies in [10], where an algebraic approach relying on nested lattices over Principal Ideal Domains (PIDs) is proposed, together with instances of coding and decoding schemes. Practical approaches are available in [11] where suboptimal lattice decoding schemes are analyzed and in [12] where a practical integer forcing precoder (IFP) is presented.

The objective of this paper is to obtain lattice codes in the Euclidean space that enable to map the physical layer analog computing to arithmetics in Euclidean spaces. Our contributions can be summarized as follows:

- We propose quadratic imaginary Euclidean domains with a known Euclidean division algorithm as privileged underlying alphabets for lattice-based network coding.
- We explicit maps from lattices to finite fields and back, relying on the Euclidean division algorithm.
- We compute the nominal coding gain of lattices obtained from $p$-ary Hamming codes over the Euclidean domain of Gaussian integers, for any prime $p$ such that $p \equiv 1 \pmod 4$.

This document is organized as follows. Section II provides the necessary mathematical background on Euclidean domains, together with two division algorithms (in Subsection II-A), while the relevance of quadratic imaginary Euclidean domains to physical layer network coding is justified in Subsection II-B. The actual method for the construction of physical layer alphabets over quadratic imaginary Euclidean domains, with explicit maps allowing to go from the lattice to finite fields and back are detailed in Section III. These alphabets are used to embed linear $p$-ary of length $n$ codes into $n$-dimensional ambient Euclidean spaces, as explained in Section IV, where the case of lattices built from $p$-ary Hamming codes is treated.

## II. Quadratic Imaginary Euclidean Domains

Consider the following five sets:

$$\mathbb{Z}[\rho] = \{a + b\rho,\ a, b \in \mathbb{Z}\},$$

with

$$\rho = \sqrt{D}, \qquad D \in \{-1, -2\} \tag{1}$$

$$\rho = \tfrac{1+\sqrt{D}}{2}, \quad D \in \{-3, -7, -11\}. \tag{2}$$

They are *integral domains*, that is, by definition, commutative rings with identity $1 \neq 0$ where $xy = 0$ implies $x = 0$ or $y = 0$ for any two elements $x, y$.

These five integral domains have several things in common: firstly, they have a $\mathbb{Z}$-basis given by $\{1, \rho\}$ (they are called *quadratic* because the $\mathbb{Z}$-basis contains two elements), and they are *imaginary* (contained in $\mathbb{C}$ but not in $\mathbb{R}$). Next, for $z \in \mathbb{Z}[\rho]$, its conjugate $\bar{z}$ is defined to be

$$\bar{z} = a + b\bar{\rho}$$

M. A. Vázquez-Castro is with the Dpt. of Telecommunications and Systems Engineering of Universitat Autònoma de Barcelona, Spain. Frédérique Oggier is with the Division of Mathematical Sciences School of Physical and Mathematical Sciences at Nanyang Technological University, Singapore.

with

$$\bar{\rho} = \begin{cases} -\sqrt{D}, & D \in \{-1,-2\} \\ \frac{1-\sqrt{D}}{2} & D \in \{-3,-7,-11\} \end{cases}$$

with which one may define a *norm* function $N$, such that

$$N(z) := z\overline{z} = \begin{cases} a^2 - Db^2 & \text{if } D = -1,-2 \\ a^2 + ab + \frac{1-D}{4}b^2 & \text{if } D = -3,-7,-11. \end{cases}.$$

Note that $a^2 - Db^2 \in \mathbb{Z}$, but so does $a^2 + ab + b^2\frac{1-D}{4}$ since $-3, -7$ and $-11$ are all congruent to $1 \pmod 4$. This norm $N$ happens to coincide with the Euclidean norm, that is

$$N(z) = \begin{cases} N(a + b\sqrt{D}) = |a + ib\sqrt{D}|^2 & \text{(3a)} \\ N(a + b\frac{1+\sqrt{D}}{2}) = |a + \frac{b}{2} + i\frac{b\sqrt{D}}{2}|^2. & \text{(3b)} \end{cases}$$

The cases of $D = -1$ and $D = -3$ are the famous Gaussian integers and Eisenstein-Jacobi (EJ) integers respectively. Gaussian integers form a square lattice while EJ integers form a lattice with hexagonal symmetry.

Finally, the five of them are *Euclidean domains*, which explains the term *quadratic imaginary Euclidean domains*.

*Definition 1:* A *Euclidean domain* is an integral domain $R$ for which there exists a function $d : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ with the property that for any $x, y \in R$ with $y \neq 0$, we can write

$$x = qy + r$$

with either $r = 0$ or $d(r) < d(y)$.

The five integral domains above are furthermore said to be *norm-Euclidean* because $d = N$, the Euclidean norm, in their case. The concept of Euclidean domain generalizes that of division in $\mathbb{Z}$ to some other rings.

### A. Euclidean Division Algorithms

It is important for our application to physical network coding to have an explicit *division algorithm*, which outputs $r$ on the input $(x, y)$. Such an algorithm is known for these five quadratic imaginary Euclidean domains, though it is worth noting that there are integral domains known to be Euclidean, with no explicit division algorithm [13].

*Proposition 1:* The integral domain $\mathbb{Z}[\rho]$, for $\rho = \sqrt{D}$, $D \in \{-1,-2\}$ and $\rho = \frac{1+\sqrt{D}}{2}$, for $D \in \{-3,-7,-11\}$, are norm-Euclidean domains.

We provide these well-known proofs, not only for the sake of completeness, but also because they provide algorithms to perform a norm-Euclidean division.

*Proof:* Note first that

$$\begin{aligned} N(r) < N(y) &\iff N(x - yq) < N(y) \\ &\iff N(\tfrac{x-yq}{y}) < 1 \\ &\iff N(\tfrac{x}{y} - q) < 1 \end{aligned}$$

for $x, y, q$ in $R$, using the multiplicativity of the norm.

**Case I:** $\rho = \sqrt{D}$ with $D = -1, -2$.

Using the above remark, it is enough to show that for every $\alpha \in \mathbb{Q}(\rho)$, there exists a $\beta \in \mathbb{Z}[\rho]$ such that $N(\alpha - \beta) < 1$.

Take $\alpha = a_1 + a_2\rho \in \mathbb{Q}(\rho)$ and $\beta = b_1 + b_2\rho \in \mathbb{Z}[\rho]$, where $b_1$ (resp. $b_2$) is the integer nearest to $a_1$ (resp. $a_2$), that is

$$|b_1 - a_1| \leq \frac{1}{2},\ |b_2 - a_2| \leq \frac{1}{2}.$$

We are left to compute

$$\begin{aligned} N(\alpha - \beta) &= N(a_1 + a_2\rho - b_1 - b_2\rho) \\ &= (a_1 - b_1)^2 - D(a_2 - b_2)^2 \leq \frac{1-D}{4} \end{aligned}$$

which is indeed strictly smaller than one when $D \in \{-1,-2\}$.

**Case II:** $\rho = \frac{1+\sqrt{D}}{2}$ with $D = -3, -7, -11$.

It is again enough to show that for every $\alpha \in \mathbb{Q}(\sqrt{D})$, there exists a $\beta \in \mathbb{Z}[\rho]$ such that $N(\alpha - \beta) < 1$. Take $\alpha = a_1 + a_2\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, and $\beta = b_1 + b_2\frac{1+\sqrt{D}}{2} \in \mathbb{Z}[\rho]$, where $b_2$ is an integer such that $b_2/2$ is as close as possible to $a_2$, that is

$$|\tfrac{b_2}{2} - a_2| \leq \frac{1}{4},$$

and $b_1$ is an integer such that $b_2/2 + b_1$ is as close as possible to $a_1$, that is

$$|\tfrac{b_2+2b_1}{2} - a_1| \leq \frac{1}{2}.$$

We are left to compute

$$\begin{aligned} N(\alpha - \beta) &= N(a_1 + a_2\sqrt{D} - b_1 - b_2\tfrac{1+\sqrt{D}}{2}) \\ &= (a_1 - b_1 - \tfrac{b_2}{2})^2 - D(a_2 - \tfrac{b_2}{2})^2 \leq \frac{1}{4} - \frac{D}{16} \end{aligned}$$

which is indeed strictly smaller than one when $D \in \{-3,-7,-11\}$. ∎

*Example 1:* To divide $3 + i$ by $2 + i$ in $\mathbb{Z}[i]$, compute

$$\alpha = \frac{3+i}{2+i} = \frac{7}{5} + i\frac{-1}{5}$$

thus $q = 1$ and

$$3 + i = (2 + i) + 1,\ N(1) = 1 < N(2 + i) = 5.$$

### B. Relevance to Physical Layer Network Coding

The connection between the above Euclidean division and physical layer network coding is done via congruence classes. Let $x, y$ be two elements in $R$ a Euclidean domain. By definition

$$r \equiv x \pmod y \iff x = yq + r$$

for $r, q$ in $R$, and we say that $x$ is *congruent* to $r$ modulo $y$. The congruence relation induces a partition of $R$ into *residue classes* modulo $y$. For $x \in R$, we denote its residue class as

$$[x]_y = \{r \in R,\ r \equiv x \pmod y\}. \quad (4)$$

*Example 2:* Let us continue Example 1, with $y = 2 + i$. Then

$$[3 + i]_{2+i} = \{r \in \mathbb{Z}[i],\ r \equiv 3 + i \pmod{2 + i}\} = [1]_{2+i}.$$

Also $[0]_{2+i} = [2 + i]_{2+i}$, and a partition of $\mathbb{Z}[i]$ is given by

$$[0]_{2+i},\ [1]_{2+i}, [i]_{2+i}\ [1 + i]_{2+i},\ [2]_{2+i},$$

where $0, 1, i, 1 + i, 2$ are remainders of the norm-Euclidean division, since their norm is smaller than 5.

The set of congruence classes in $R$ is a ring, called quotient ring, and often denoted by $R/(y)$, where $(y)$ represents the set of multiples of $y$ in $R$. For the five cases of interest here, it is known [13] that $R/(y)$ has a field structure whenever $y$ is prime, and its cardinality is the Euclidean norm $N(y)$ [13]. This is illustrated in the above example.

The quotient ring $R/(y)$ inherits some of the structure of $R$. Hence, the selection of $R$ to construct the physical layer alphabet depends on the structure that is required for network coding computations.

There are several (infinitely many in fact) elements of $R$ that are mapped to one residue class, however, the Euclidean division gives a natural candidate, its remainder. It has the advantage of being of small norm, here in fact, of small Euclidean norm, which is valuable in terms of constellation shaping, as will be elaborated and illustrated in the next section.

This justifies why quadratic imaginary Euclidean domains form a natural algebraic framework for the construction of physical layer alphabets. First, alphabets coming from imaginary quadratic Euclidean domains are naturally represented in the complex plane. Second, the existence of a known explicit division algorithm makes the construction of physical layer alphabets and physical network coding computations algorithmically feasible: we map "nature" computation to componentwise modular arithmetics (mod operation), which is also used at transmitter, intermediate and receiver nodes.

Note that the five cases considered are the only imaginary quadratic fields known to be Euclidean domains (see [13]). They are particular cases of those considered in [10], where a theoretical physical layer networking piece of work was developed solely based on structural (not algorithmic) properties.

## III. Alphabet Design for Physical Layer Network Coding

Let $\mathbb{Z}[\rho]$ be the imaginary quadratic norm-Euclidean domains considered above. Let $p \in \mathbb{Z}$ and $\pi$ a prime number in $\mathbb{Z}[\rho]$ . Then it is known [13] that $p = \pi\bar{\pi}$ in $\mathbb{Z}[\rho]$, when

$$p \equiv \begin{cases} 1 \pmod 4 & \text{if } D=-1 \\ 1,3 \pmod 8 & \text{if } D=-2 \\ 1 \pmod 6 & \text{if } D=-3 \\ 1,2,4 \pmod 7 & \text{if } D=-7 \\ 1,3,4,5,9 \pmod{11} & \text{if } D=-11. \end{cases}$$

The set of congruence classes $\mathbb{Z}[\rho]/(\pi)$ for these primes $\pi$ is a field and its cardinality is $N(\pi) = p$ (since $N(p) = p^2$), as discussed above. Thus $R/(\pi)$ is isomorphic to the finite field $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ with $p$ elements.

*Example 3:* In $\mathbb{Z}[i]$, $5 = (2+i)(2-i)$. Take $\pi = 2+i$. We computed a set of congruence classes in Example 2. Notice that $i = (2+i)(-1+i)+3$, $i+1 = (2+i)(-1+i)+4$ thus $[i]_\pi = [3]_\pi$, $[1+i]_\pi = [4]_\pi$, so that

$$[0]_\pi,\ [1]_\pi,\ [3]_\pi,\ [4]_\pi,\ [2]_\pi,$$

is the same set of congruence classes with different representatives, which illustrates that it is isomorphic to $\mathbb{F}_5$.

We next proceed with the construction of alphabets within the framework established so far, distinguishing our algorithmic construction from the structural constructions known so far [10].

*Definition 2:* Given one of the five quadratic imaginary Euclidean domain $\mathbb{Z}[\rho]$, and a prime $p \in \mathbb{Z}$ such that $p = \pi\bar{\pi}$, a *physical layer alphabet* for network coding is chosen to be

$$\mathcal{A}_\pi = \{x \in \mathbb{Z}[\rho],\ N(x) < N(\pi) = p\}$$

where we recall that this algebraic norm corresponds to the Euclidean one.

We have $|\mathcal{A}_\pi| = N(\pi) = \pi\overline{\pi} = p$.

The norm Euclidean division provides a way to map an arbitrary element $x \in \mathbb{Z}[\rho]$ to $\mathcal{A}_\pi$. Recall that when dividing $x \in \mathbb{Z}[\rho]$ by $\pi$, we get

$$x = \begin{cases} \pi[\frac{x\bar{\pi}}{p}] + r, & D \in \{-1,-2\} \\ \pi[[\frac{x\bar{\pi}}{p}]] + r, & D \in \{-3,-7,-11\}, \end{cases}$$

where $[a+ib] := [a] + i[b]$ and $[a]$ for $a$ in $\mathbb{Q}\left(\sqrt{D}\right)$ means the closest integer from $a$. Also $[[a+ib]] := [[a]] + i[[b]]$ is a notation that we introduce: $[[b]]$ for $b$ in $\mathbb{Q}\left(\sqrt{D}\right)$ means the closest half-integer from $b$, after which $[[a]]$ is obtained by finding the integer $a'$ such that $[[b]] + a'$ is the closest to $a \in \mathbb{Q}\left(\sqrt{D}\right)$. Hence, $[\frac{x\bar{\pi}}{p}]$ and $[[\frac{x\bar{\pi}}{p}]]$ are in $\mathbb{Z}[\rho]$ by definition.

Define the natural map $\varphi_\pi : \mathbb{Z}[\rho] \to \mathcal{A}_\pi$, such that

$$\varphi_\pi(x) = \begin{cases} x - \pi[\frac{x\bar{\pi}}{p}], & D \in \{-1,-2\} \\ x - \pi[[\frac{x\bar{\pi}}{p}]], & D \in \{-3,-7,-11\}. \end{cases}$$

### A. From Complex Alphabets to Finite Fields and Back

Let $\mathbb{Z}[\rho]$ be one of the 5 norm-Euclidean domains defined in (1) and (2), and let $p$ be a prime such that $p = \pi\bar{\pi}$ in $\mathbb{Z}[\rho]$. Recall from the previous subsection that $\mathbb{Z}[\rho]/(\pi) \simeq \mathbb{F}_p$.

Define the map $\mu_\pi : \mathbb{F}_p \to \mathcal{A}_\pi$, such that

$$\alpha \overset{\mu_\pi}{\longmapsto} r = \begin{cases} \alpha - \pi[\frac{\alpha\bar{\pi}}{p}], & D \in \{-1,-2\} \\ \alpha - \pi[[\frac{\alpha\bar{\pi}}{p}]], & D \in \{-3,-7,-11\}. \end{cases} \tag{5}$$

The map $\mu_\pi^{-1} : \mathcal{A}_\pi \to \mathbb{F}_p$ given by

$$\mu_\pi^{-1}(r) = \bar{r}u\pi + rv\bar{\pi} \pmod p,$$

is the inverse of $\mu_\pi$, for $u, v$ such that $1 = u\pi + v\bar{\pi}$. They exist because $\pi$ and $\bar{\pi}$ are coprime, and there is a Euclidean division (thus a Bezout identity). Indeed, write $\alpha \in \mathbb{F}_p$ as $\alpha = r + a\pi$ for $a \in \mathbb{Z}[\rho]$, and notice that $\bar{\alpha} = \bar{r} + \bar{a}\bar{\pi}$ must be equal to $\alpha$ (since $\alpha \in \{0, \ldots, p-1\}$). Then

$$\begin{aligned} & \bar{r}u\pi + rv\bar{\pi} \pmod p \\ = \ & (\bar{\alpha} - \bar{a}\bar{\pi})u\pi + (\alpha - a\pi)v\bar{\pi} \pmod p \\ = \ & \bar{\alpha}u\pi + \alpha v\bar{\pi} \pmod p \\ = \ & \alpha \pmod p. \end{aligned}$$

The maps are summarized below:

| | | |
|---|---|---|
| $x = \pi\lvert\frac{x\bar{\pi}}{p}\rvert + r \in \mathbb{Z}[\rho]$ | $\xrightarrow{\varphi_\pi}$ | $\varphi_\pi(x) = x - \pi\lvert\frac{x\bar{\pi}}{p}\rvert$ |
| $= r \in \mathcal{A}_\pi$ | $\xrightarrow{\mu_\pi^{-1}}$ | $\mu_\pi^{-1}(r) = \bar{r}u\pi + rv\bar{\pi}$ |
| $\mu_\pi(\alpha) = \alpha - \pi\lvert\frac{\alpha\bar{\pi}}{p}\rvert$ | $\xleftarrow{\mu_\pi}$ | $= \alpha \in \mathbb{F}_p$ |

where $|.|$ stands for $[.]$ when $D = -1, -2$ and for $[[.]]$ when $D = -3, -7, -11$ as previously defined. The map $\mu_\pi$ and its inverse have been studied in the particular cases of $D = -1$ and $D = -3$ in [14], [15], [16].

Figure 1 shows the obtained alphabet and labelling in the 2-dimensional Euclidean space for $D = -1$ and prime $p = 73$.

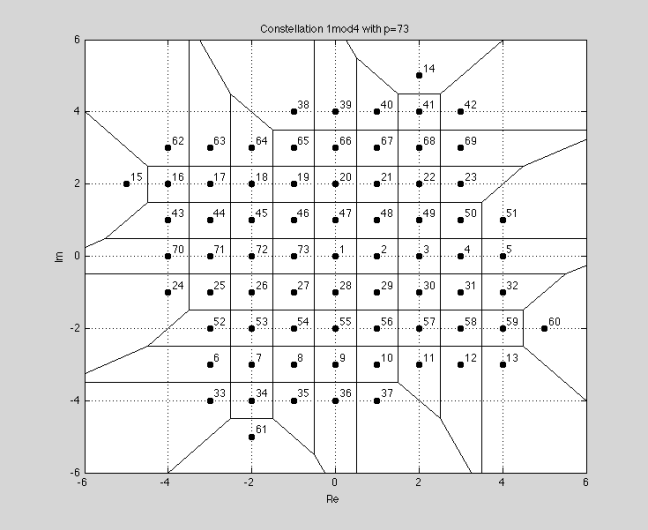


Figure 1. Example of alphabets obtained from $\mathbb{Z}[i]$ for $p = 73$.

### B. Packing Gains

The physical layer alphabet $\mathcal{A}_\pi$ is carved from $\mathbb{Z}[\rho]$, which forms a 2-dimensional lattice. The Voronoi region of this lattice $\mathbb{Z}[\rho]$ corresponds to the decision regions around each of the constellation symbols. The volume of the Voronoi region is the volume of the lattice.

*Definition 3:* The *volume* of a lattice is the volume of its fundamental parallelotope, given by $|\det(G)|$, where $G$ is a matrix containing the basis vectors of the lattice.

The volume (or area for a 2-dimensional lattice) for the five values of $D$ considered are shown in the second row of Table I, and are easily computed from the basis given in the first row of Table I. The third row shows the *packing gain*, that is the ratio between the area of a classic QAM constellation, and that of the lattice $\mathbb{Z}[\rho]$. It is observed that the packing for $D = -3$ is the best ($10\log_{10}(1.155) = 0.625$ dB) as expected, since this corresponds to the hexagonal lattice, a lattice known to be dense.

| $D$ | $-1$ | $-2$ | $-3$ | $-7$ | $-11$ |
|---|---|---|---|---|---|
| a basis of the lattice $\mathbb{Z}[\rho]$ | $(1,0)$, $(0,1)$ | $(1,0)$, $(0,\sqrt{2})$ | $(1,0)$, $(\frac{1}{2},\frac{\sqrt{3}}{2})$ | $(1,0)$, $(\frac{1}{2},\frac{\sqrt{7}}{2})$ | $(1,0)$, $(\frac{1}{2},\frac{\sqrt{11}}{2})$ |
| $vol(\mathbb{Z}[\rho])$ | 1 | $\sqrt{2}$ | $\sqrt{3}/2$ | $\sqrt{7}/2$ | $\sqrt{11}/2$ |
| $1/vol(\mathbb{Z}[\rho])$ | 1 | 0.707 | 1.155 | 0.756 | 0.603 |

Table I
PACKING GAIN OVER QAM.

Note that the shape and size of the constellation is determined by the selected prime.

## IV. Lattices over Euclidean Domains

We next use the Euclidean alphabets obtained above to embed linear $p$-ary codes into the $n$-dimensional Euclidean space.

### A. Euclidean Lattices for Networking

Let $\mathcal{C}[k,n,d_H]_p$ be a linear block code of length $n$, dimension $k$ over $\mathbb{F}_p$, minimum Hamming distance $d_H$ and generator matrix $\left[\begin{array}{cc} \mathbb{I}_k & B \end{array}\right]$. The Euclidean image of the linear block code $\mathcal{C}[k,n,d_H]_p$ in $\mathcal{A}_\pi^n$ is obtained by applying $\mu_\pi$ componentwise on every codeword of $\mathcal{C}[k,n,d_H]_p$. By abuse of notation, we will next use $\mu_\pi$ and similarly $\varphi_\pi^{-1}$ componentwise.

Furthermore, we obtain a version of Construction A [4]:.

*Proposition 2:* The preimage $\varphi_\pi^{-1}(\mu_\pi(\mathcal{C}[k,n,d_H]_p))$ forms a lattice over $\mathbb{Z}[\rho]$, that is all linear combinations with coefficients in $\mathbb{Z}[\rho]$ of some set of linearly independent vectors in a Euclidean space. This lattice has a generator matrix

$$G = \left[\begin{array}{cc} \mathbb{I}_k & B \\ 0 & \pi\mathbb{I}_{n-k} \end{array}\right] \tag{6}$$

containing basis vectors.

*Proof:* The proof is similar to known Constructions A (e.g. [17]). That $\varphi_\pi^{-1}(\mu_\pi(\mathcal{C}[k,n,d_H]_p))$ forms a lattice follows since $\mathcal{C}[k,n,d_H]_p$ is a group, and $\varphi_\pi$ componentwise is a group homomorphism. Indeed if $x = \pi[\frac{x\bar{\pi}}{p}] + r$ and $y = \pi[\frac{y\bar{\pi}}{p}] + s$, then $x+y = \pi([\frac{x\bar{\pi}}{p}]+[\frac{y\bar{\pi}}{p}]) + r + s$ and $\varphi_\pi(x+y) = x+y \pmod{\pi} = r+s$ which is equal to $\varphi_\pi(x)+\varphi_\pi(y) = x \pmod{\pi} + y \pmod{\pi} = r+s$, which is enough. For the claim on a generator matrix, compute a lattice point $\mathbf{x}$ using $G$, show that ${\mu_\pi}^{-1}\varphi_\pi(\mathbf{x})$ is in $\mathcal{C}[k,n,d_H]_p$ and conclude using a volume argument (see [17] for similar computations). ■

We are next interested in the properties of this lattice, in particular its Hermite parameter.

*Definition 4:* The *Hermite parameter* or *nominal coding gain* of a lattice $\Lambda$

$$\gamma_c(\Lambda) = \frac{\lambda(\Lambda)}{vol(\Lambda)^{1/n}}$$

measures the normalized density of the lattice, where

$$\lambda(\Lambda) = \min\{\|\mathbf{v}\|,\ \mathbf{v} \in \Lambda \setminus \{0\}\}$$

is the *minimum distance* of the lattice $\Lambda$, given by the length of the shortest nonzero lattice vector.

In the case of a lattice obtained via Construction A described above, its Hermite parameter depends not only on the encoding linear block code $\mathcal{C}[k,n,d_H]_p$ but also on the specific Euclidean domain $\mathbb{Z}[\rho]$ and selected prime number $p$. An example is provided in the next subsection.

Note that the shaping region is naturally given by the canonical projection $\varphi_\pi$ that defines the signal constellation.

### B. The Hamming Euclidean Lattice

We consider the lattice obtained when $\mathcal{C}[k,n,d_H]_p$ is a $p$-ary Hamming code, defined as follows.

*Definition 5:* Given an integer $r \geq 2$, the $p$-ary *Hamming code* $Ham(r,p)$ over the finite field $\mathbb{F}_p$ with $n = \frac{p^r-1}{p-1}$ is an $[n, n-r, 3]$ linear code defined by a parity check matrix whose columns form a list of nonzero vectors satisfying the condition that no two vectors are scalar mutliples of each other.

*Example 4:* We use the Hamming code $Ham(2,5)$ with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 0 & 4 & 3 \\ 0 & 0 & 1 & 0 & 4 & 2 \\ 0 & 0 & 0 & 1 & 4 & 1 \end{bmatrix}$$

over the Gaussian integers with $p = 5$ (see Example 3). We show in Figure 2 the $625 \times 625$ matrix of crossed distances between the constellation symbols $\mu_{2+i}\left(\mathcal{C}\left[4,6,3\right]_5\right) \in \mathcal{A}_{2+i}^6 \subset \mathbb{Z}\left[i\right]^6$ where some symmetry properties can be appreciated.

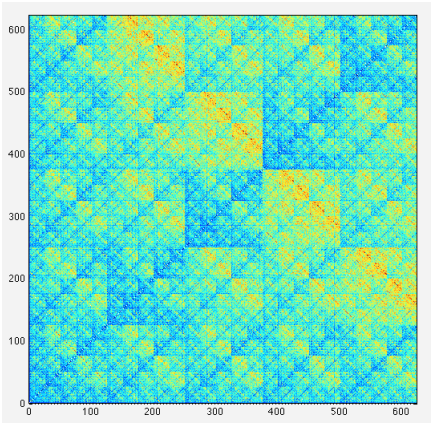


Figure 2. Visualization of $\mu_{2+i}\left(\mathcal{C}\left[4,6,3\right]_5\right)$ in terms of crossed distances between constellation symbols.

We now compute the nominal coding gain of the lattice obtained from the $p$-ary Hamming code.

*Theorem 1:* The nominal coding gain of a $p$-ary Hamming lattice $\Lambda$ over a quadratic Euclidean domain $\mathbb{Z}\left[\rho\right]$ with $\rho = \sqrt{-1}$, for a Hamming code $Ham(r,p)$ for any $p \equiv 1 \pmod 4$ equals

$$\gamma_c(\Lambda) = \frac{3}{p^{r/n}}.$$

*Proof:* From (6), the volume of this lattice $\Lambda$ is $vol(\Lambda) = p^r$, $r = n-k$, thus

$$\gamma_c(\Lambda) = \frac{\lambda(\Lambda)}{p^{r/n}},$$

and the minimum Euclidean distance of the constellation is 3. Hence, the result follows. ■

Figure 3 plots this nominal coding gain, showing the well known fact that $p$-ary Hamming codes are not asymptotically optimal, i.e, the minimum Hamming distance does not grow linearly with the block length. However, they can still yield sufficiently good performance for low signal-to-noise ratios.

## V. Acknowledgments

The research of F. Oggier for this work is supported by the Nanyang Technological University under Research Grant M58110049. Part of the work was done while F. Oggier was visiting the Dept. of Telecommunications and Systems Engineering of Universitat Autònoma de Barcelona.

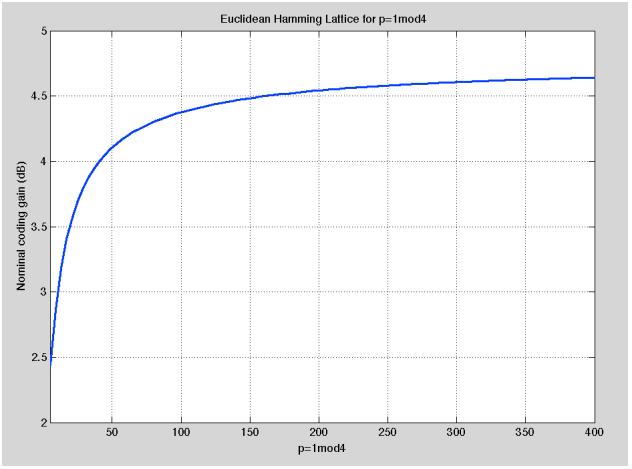


Figure 3. Nominal coding gain of lattices obtained from $Ham(r,p)$ over $\mathbb{Z}\left[\rho\right]$ with $\rho = \sqrt{-1}$, r=2 and for any $p = 1 \pmod 4$ .

## References

[1] G. Polytrev, "On coding without restrictions for the AWGN channel," *IEEE Trans. Inform. Theory*, vol. 40, pp. 409-417, 1994.
[2] H. Loeliger, "Averaging bounds for lattices and linear codes", *IEEE Trans. Inform. Theory*, vol. 43, no. 6, pp. 1767-11773, 1997.
[3] U. Erez and R. Zamir, "Lattice coding can achieve log(1 + SNR) on the AWGN channel using nested codes", *IEEE Trans. Inform. Theory*, vol. 50, no. 10, pp. 2293-2314, 2004.
[4] J. H. Conway , N. J. A. Sloane, Sphere packings, lattices and groups, Springer-Verlag, 3rd edition, New York, 1998.
[5] S. Zhang, S. C. Liew, and P. P. Lam, "Hot topic: Physical layer network coding," in Proc. ACM MOBICOM , 2006.
[6] S. Zhang, S.-C. Liew, "Channel coding and decoding in a relay system operated with physical-layer network coding", *IEEE Journal on Selected Areas in Communications*, vol. 27, no 5, pp. 788–796, 2009.
[7] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, J. Crowcroft, "XORs in the air: practical wireless network coding", *IEEE/ACM Transactions on Networking*, vol. 16, no 3, pp. 497–510, 2008.
[8] K. Lu, S. Fu, Y. Qian, H.-H. Chen, "On capacity of random wireless networks with physical-layer network coding.", *IEEE Journal on Selected Areas in Communications*, vol 27, no 5, pp. 763–772, 2009.
[9] B. Nazer and M. Gastpar, "Reliable physical layer network coding," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 438 –460, march 2011.
[10] C. Feng, D. Silva, and F. Kschischang, "An algebraic approach to physical layer network coding", *IEEE Trans. on Information Theory*, vol. 59, no . 11, pp. 7576-7596, 2013.
[11] A. Mejri, G. Rekaya-Ben Othman, J.-C. Belfiore, "Lattice decoding for the compute-and-forward protocol", *Third Int. Conference on Communications and Networking*, ComNet 2012.
[12] S. Gupta, M. A. Vázquez-Castro, "Physical-layer network coding based on integer-forcing precoded compute and forward", *Second Int. Workshop on Vehicular Communications and Networking*, VECON 2012.
[13] Yu. I. Manin, A. A. Panchishkin, "Introduction to modern number theory", Second Edition, Springer 2004.
[14] K. Huber. "Codes Over Gaussian Integers", *IEEE Trans on Information Theory*, vol. 40, no. 1, pp. 207- 216, 1994.
[15] S. I. R. Costa, M. Muniz, E. Agustini and R . Palazzo, "Graphs, tessellations, and perfect codes on flat tori", *IEEE Trans. on Information Theory*, vol. 50, no . 10, pp. 2363-2377, 2004.
[16] T. P. da Nóbrega, J. C. Interlando, O. Milaré, M. Eliaand R. Palazzo, "Lattice constellations and codes from quadratic number fields", *IEEE Trans. on Information Theory*, vol 47, no 4, pp. 1514-1527, 2001.
[17] W. Kositwattanarerk, S. S. Ong, F. Oggier, "Wiretap encoding of lattices from number fields using codes over $\mathbb{F}_p$", in the proceedings of the *IEEE International Symposium on Information Theory (ISIT)*, 2013.