Construction-A Full-Diversity Lattices

Joseph J. Boutros
Texas A&M University at Qatar
boutros@tamu.edu

Jean-Claude Belfiore
Huawei, France
jean.claude.belfiore@huawei.com

***Abstract*—Lattices from Construction A and non-binary codes are considered. These lattices are built from number fields as coset codes of the ring of integers $O_{\mathbb{K}}$ modulo an ideal $\mathcal{I}$. Diversity of a Construction-A lattice Λ on block-fading channels is guaranteed by the chain $\mathcal{I}^m \subset \Lambda \subset O_{\mathbb{K}}^m$. We study how the code alphabet size should be chosen in order to avoid error floors on the Gaussian channel due to the sublattice $\mathcal{I}^m$. Our aim is to get Construction-A lattices that are good for both Gaussian and block-fading channels.**

I. Construction A and Codes on Graphs

Low-density lattices codes [19] brought new tools from modern coding theory to the theory of lattices in Euclidean spaces. Such modern tools combined to integer lattices from Construction A proposed by Leech and Sloane [16] produce very efficient ensembles of lattices. The recent success in building high-dimensional fast-decodable LDA and GLD lattices [10], [7], [11], motivated us to investigate methods for building full-diversity lattices via Construction A. On the Gaussian channel, in absence of fading, LDA lattices can achieve Shannon capacity under lattice decoding [11]. LDA lattices [10] and some of their cousins in the GLD family [7] are built by Construction A:

$$\Lambda = \Phi(C[n,k]_p) + p\mathbb{Z}^n. \tag{1}$$

Here, the lattice Λ has rank n in $\mathbb{R}^n$, p is a prime integer, and $C[n,k]_p$ is a linear code of length n and dimension k, $0 < k < n$, defined over the finite field $\mathbb{F}_p$. If C is a low-density parity-check (LDPC) code over $\mathbb{F}_p$ [14], [9], then Λ is referred to as an LDA lattice. If C is a generalized low-density (GLD) code over $\mathbb{F}_p$ [8], then Λ is referred to as a GLD lattice. The map $\Phi : \mathbb{F}_p \to \mathbb{Z}/p\mathbb{Z} \subset \mathbb{Z}$ is a group homomorphism that embeds $\mathbb{F}_p$ in $\mathbb{Z}$.

For Construction-A lattices, two sufficient conditions should be met for finite lattice constellations in order to attain Shannon capacity [12], [22]: 1- Gaussian goodness which is equivalent to lattices attaining Poltyrev limit given by the highest noise variance $\sigma^2_{max} = \frac{vol(\Lambda)^{2/n}}{2\pi e}$ [17], and 2- Covering goodness which is equivalent to spherically shaped constellations in high dimensions. In all cases, the prime p increases as n^λ where λ admits a lower bound that depends on the coding rate $R = k/n$ of C. For random lattices built from random non-binary codes $C[n,k]_p$, we have $\lambda > (1+R)^{-1}$, see Theorem 2 in [11]. For LDA lattices where C is a non-binary LDPC code whose Tanner graph has an expansion factor of D, λ is to be greater than $\frac{1}{1-R}$, see Theorem 3 in [11]. In practice, the symbol error rate of LDA lattices is close enough to Poltyrev limit under iterative message-passing decoding (Belief Propagation). In some cases, for GLD lattices, a spectral thinning is proven, i.e. the symbol error probability scales as $1/n$ similar to standard Turbo codes based on convolutional codes. Also, the value of p implemented in practical iterative decoders is not as high as n^λ. We believe that proofs in [12] and [11] could be improved to yield a smaller prime p but the huge proof length is an obstacle. Under iterative decoding, the value of p is selected large enough to guarantee that Λ in (1) is not perturbed by its sublattice $p\mathbb{Z}^n$. In other words, the distance inside a coset should be larger than the distance between two cosets labeled by C. The next section investigates how the alphabet size p should be selected to guarantee a good performance of the sublattice $p\mathbb{Z}^n$.

II. Alphabet size without diversity

The error probability of the one-dimensional integer lattice $p\mathbb{Z}$ is given by the following Lemma.

Lemma 1: Let $\Lambda \subset \mathbb{R}^n$ be a real lattice built via Construction A as in (1). Then, its sublattice $p\mathbb{Z}^n$ has the following error probability per dimension (per lattice coordinate) on a Gaussian channel

$$P_e(p\mathbb{Z}) = 2Q\left(\sqrt{\Delta\frac{\pi e}{2}p^{2R}}\right), \tag{2}$$

where $\Delta \geq 1$ is the SNR-distance to Poltyrev limit and $Q(x)$ is the Gaussian tail function [1].

Proof: In the one-dimensional lattice $p\mathbb{Z}$, the minimum Euclidean distance is p and each point has 2 neighbors. Then,

$$P_e(p\mathbb{Z}) = 2Q\left(\frac{p}{2\sigma}\right) = 2Q\left(\sqrt{\frac{p^2}{4\sigma^2}}\right). \tag{3}$$

But $\sigma^2 = \sigma^2_{max}/\Delta = \frac{vol(\Lambda)^{2/n}}{\Delta\times 2\pi e}$. Notice that the noise level affecting $p\mathbb{Z}$ is identical to that affecting the lattice Λ. From Construction A, the fundamental volume of Λ is $vol(\Lambda) = p^{n-k} = p^{n(1-R)}$ which yields $\frac{1}{\sigma^2} = \Delta \times 2\pi e/p^{2(1-R)}$. Substituting the expression of $\frac{1}{\sigma^2}$ in (3) gives the error probability $P_e(p\mathbb{Z})$ stated by this lemma. ■

The distance to Poltyrev limit is usually expressed in decibels, $\Delta(dB) = 10\log_{10}(\Delta)$. The error probability per lattice point on a Gaussian channel, where additive noise is independent and identically distributed from one dimension to another, satisfies

$$P_e(p\mathbb{Z}^n) = 1 - (1 - P_e(p\mathbb{Z}))^n \leq nP_e(p\mathbb{Z}). \tag{4}$$

Figure 1 shows the variation of the alphabet size p based on expressions (2) and (4). It is surprising to see that small values of p are good enough, e.g. $p = 11$ or $p = 13$ for $R = 1/3$ used at $n = 1$ million in GLD lattices under iterative decoding [7]. If lattice decoding is to be considered, the current theory established for LDA lattices yields huge values, e.g. for $R = 1/3$ we get $p > n^{1.5}$ [11].

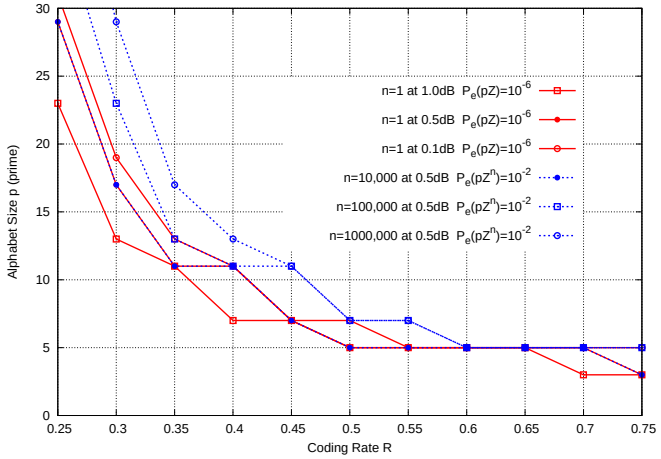

Figure 1. Performance of the integer cubic lattice $p\mathbb{Z}^n$ as a sublattice of $\Lambda = C[n,k]_p + p\mathbb{Z}^n$. The plot shows the alphabet size p versus the coding rate R for a fixed error probability per lattice coordinate ($P_e(p\mathbb{Z})$) and a fixed error probability per lattice point ($P_e(p\mathbb{Z}^n)$). The distance to Poltyrev limit is taken to be $\Delta(dB) = 0.1, 0.5, 1.0dB$ for $P_e(p\mathbb{Z}) = 10^{-6}$ and $\Delta(dB) = 0.5dB$ for $P_e(p\mathbb{Z}^n) = 10^{-2}$.

Furthermore, at $P_e(p\mathbb{Z}) = 10^{-6}$ and $P_e(p\mathbb{Z}^n) = 10^{-2}$, $p_{min} = \lim_{R\to 1}(p) = 3$. Hence, binary codes for Construction A cannot reach this level of performance. Ternary codes (at least) are necessary at high coding rate. Note that LDA lattices require $R > \frac{1}{2}$ to achieve Shannon capacity of the Gaussian channel in the proof given in [11]. Finally, we complete this section with a proposition describing the behavior of p^{2R} as logarithmic in the lattice dimension when the performance constraint is on the point error probability. A constraint on the symbol error probability (per coordinate) does not need p to increase with n. The proof of the following proposition is based on (2) & (4), $x = \sqrt{\Delta \frac{\pi e}{2} p^{2R}} \geq 2$, and the inequality $Q(x) > \frac{x}{(1+x^2)\sqrt{2\pi}} e^{-x^2/2}$ [1].

Proposition 1: Let $\Lambda \subset \mathbb{R}^n$ be a real lattice built via Construction A as in (1). Assume that its point error probability $P_e(\Lambda)$ is bounded above by 10^{-2}. Then the alphabet size satisfies (necessary condition)

$$p^{2R} > \frac{4}{\Delta\pi e}[-\log(1-(1-10^{-2})^{\frac{1}{n}}) + \log(x)] \quad (5)$$

$$\approx \frac{4}{\Delta\pi e}[\log(n) - \log(10^{-2})], \quad (6)$$

where log is the natural logarithm function.

III. Construction A from number fields

Lattices built from (1) have no diversity; there exists a lattice point with a unique non-zero coordinate making the diversity order equal to 1. This lack of diversity is the result of $p\mathbb{Z}^n \subset \Lambda$. Instead of building Λ as a coset code from the partition chain $\mathbb{Z}^n/\Lambda/p\mathbb{Z}^n$, we may use $\Lambda_{O_\mathbb{K}}^m/\Lambda/\Lambda_\mathcal{I}^m$ where $\Lambda_{O_\mathbb{K}} = \sigma(O_\mathbb{K}) \subset \mathbb{R}^{[\mathbb{K}:\mathbb{Q}]}$ is a lattice built from the ring of integers $O_\mathbb{K}$ of a number field $\mathbb{K} = \mathbb{Q}(\theta)$ of degree $[\mathbb{K}:\mathbb{Q}]$, $\Lambda_\mathcal{I} = \sigma(\mathcal{I})$ is a lattice associated to an ideal $\mathcal{I}$ of $O_\mathbb{K}$ such that the quotient ring has order $|O_\mathbb{K}/\mathcal{I}| = p$, and $m = n/[\mathbb{K}:\mathbb{Q}]$. Construction A from a number field becomes

$$\Lambda = \Phi(C[m,k]_p) + \Lambda_\mathcal{I}^m. \quad (7)$$

In the above expression, $\Lambda \subset \mathbb{R}^n$ has rank n, the code $C[m,k]_p \subset \mathbb{F}_p^m$ has dimension k, $0 < k < m$, and the homomorphism $\Phi : \mathbb{F}_p \to \Lambda_{O_\mathbb{K}} \subset \mathbb{R}^{[\mathbb{K}:\mathbb{Q}]}$ embeds the prime field $\mathbb{F}_p$ in the real space $\mathbb{R}^{[\mathbb{K}:\mathbb{Q}]}$. The canonical embedding $\sigma : O_\mathbb{K} \to \mathbb{R}^{[\mathbb{K}:\mathbb{Q}]}$ converts the ring of integers $O_\mathbb{K}$ and its ideals into lattices of dimension $[\mathbb{K}:\mathbb{Q}]$, see [18] and [4] for more details. Examples will be given below for quadratic number fields.

The Construction-A lattice Λ in (7) has the same diversity as $\Lambda_{O_\mathbb{K}}$ and $\Lambda_\mathcal{I}$ because of the chain $\Lambda_\mathcal{I}^m \subset \Lambda \subset \Lambda_{O_\mathbb{K}}^m$. This diversity is $L = r_1 + r_2$ [4], where (r_1, r_2) is the signature of $\mathbb{K} = \mathbb{Q}(\theta)$, i.e. the minimal polynomial $\mu_\theta(x)$ of θ has degree $[\mathbb{K}:\mathbb{Q}] = r_1 + 2r_2$, it has r_1 real roots and $2r_2$ complex roots. Of course, any finite constellation carved from Λ will also have a diversity $L \geq r_1 + r_2$. Another way to get diversity $L \geq 2$ is to utilize root-LDPC codes [6] in Construction A. For a root-LDPC code $C[n,k]_p$, diversity is guaranteed by root checknodes for an alphabet not exceeding p values per real dimension. This does not guarantee that Λ in (1) has diversity $L \geq 2$ but a well-chosen finite constellation may attain that diversity order as in the case of root-LDA lattices [21]. In the current paper, we are interested by the intrinsic diversity of the lattice itself.

Let us show a simple example for $p = 11$ and $[\mathbb{K}:\mathbb{Q}] = 2$. Consider the real quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ for $d \geq 2$. Its ring of integers is $O_\mathbb{K} = \mathbb{Z}[\phi]$ where $\{1, \phi\}$ is an integral basis. Let $\mu_\phi(x) = x^2 + \mu_1 x + \mu_0$ be the minimal polynomial of ϕ. If $d \neq 1 \ mod \ 4$ then $\phi = \sqrt{d}$, its conjugate is $\bar{\phi} = -\sqrt{d}$, and $\mu_\phi(x) = x^2 - d$. If $d = 1 \ mod \ 4$ then $\phi = (1+\sqrt{d})/2$, its conjugate is $\bar{\phi} = (1-\sqrt{d})/2$, and $\mu_\phi(x) = x^2 - x - (d-1)/4$. Let $\mathcal{I} = gO_\mathbb{K}$ be a principal ideal with generator g. Then, $N(\mathcal{I}) = |O_\mathbb{K}/\mathcal{I}|$ is equal to the algebraic norm $|N(g)|$ of g (in absolute value). Assume $g = g_0 + g_1\phi$ then $N(g) = (g_0 + g_1\phi)(g_0 + g_1\bar{\phi})$ and g should satisfy $|N(g)| = p$. The code $C[m,k]_p$ can now select a sequence of m cosets in the quotient ring $O_\mathbb{K}/\mathcal{I}$ to make a lattice point in real dimension $n = 2m$. More precisely, the $\mathbb{Z}$-module $O_\mathbb{K}$ is converted into a bidimensional lattice via $\sigma : O_\mathbb{K} \to \mathbb{R}^2$, where $\sigma(a + b\phi) = (a + b\phi, \quad a + b\bar{\phi})$ for $a, b \in \mathbb{Z}$. The lattice $\Lambda_{O_\mathbb{K}} = \sigma(O_\mathbb{K})$ has a generator matrix (in row convention):

$$G_{O_\mathbb{K}} = \begin{pmatrix} 1 & 1 \\ \phi & \bar{\phi} \end{pmatrix}. \quad (8)$$

The sublattice $\Lambda_{\mathcal{I}} = \sigma(\mathcal{I})$ has a generator matrix:

$$G_{\mathcal{I}} = \begin{pmatrix} g & \bar{g} \\ g\phi & \bar{g}\bar{\phi} \end{pmatrix} \quad (9)$$
$$= \begin{pmatrix} g_0 + g_1\phi & g_0 + g_1\bar{\phi} \\ -g_1\mu_0 + (g_0 - g_1\mu_1)\phi & -g_1\mu_0 + (g_0 - g_1\mu_1)\bar{\phi} \end{pmatrix}$$

In the special case of real quadratic number fields, the fundamental volume of $\Lambda_{\mathcal{I}}$ is given by [18] [4]:

$$vol(\Lambda_{\mathcal{I}}) = |\det(G_{\mathcal{I}})| = N(\mathcal{I}) \times |\det(G_{O_{\mathbb{K}}})| = p\sqrt{d_{\mathbb{K}}}, \quad (10)$$

where the field discriminant is $d_{\mathbb{K}} = d$ if $d = 1 \ mod \ 4$ and $d_{\mathbb{K}} = 4d$ if $d \neq 1 \ mod \ 4$.

Take $d = 5$ and $g = -1+3\phi$. We get $|O_{\mathbb{K}}/\mathcal{I}| = p = 11$, the minimum squared Euclidean distance of $\Lambda_{\mathcal{I}}$ is $d^2_{Emin}(\mathcal{I}) = 23$ and its Hermite constant γ_I is

$$\gamma_I = \frac{d^2_{Emin}(\mathcal{I})}{vol(\Lambda_{\mathcal{I}})} = \frac{23}{11\sqrt{5}} \approx 0.9351. \quad (11)$$

Take $d = 14$ and $g = 5 + \phi$. We get $|O_{\mathbb{K}}/\mathcal{I}| = p = 11$, $d^2_{Emin}(\mathcal{I}) = 78$, and

$$\gamma_I = \frac{39}{11\sqrt{14}} \approx 0.9476. \quad (12)$$

Both lattices from $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{14})$ have a Hermite constant less than 1. The Hermite constant is also known as the fundamental gain of a lattice [13]. Recall that $p\mathbb{Z}$ has a fundamental gain equal to 1. The loss in fundamental gain for $\Lambda_{\mathcal{I}}$ is small when $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ or $\mathbb{K} = \mathbb{Q}(\sqrt{14})$. Unfortunately, in the next section, we will see that an extra loss is due to the degree $[K : Q]$ itself (the fact that $m = n/2$). We complete this section with the illustration of $\Lambda_{O_{\mathbb{K}}}$ and $\Lambda_{\mathcal{I}}$ for $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ and $I = (-1+3\phi)O_{\mathbb{K}}$ as shown in Figure 2. Points of $\Lambda_{O_{\mathbb{K}}}$ are plotted in red and points of $\Lambda_{\mathcal{I}}$ are in blue. Integers a and b show lattice points $\sigma(a+b\phi)$. Circles at three special shells of $\Lambda_{O_{\mathbb{K}}}$ are drawn, those at squared radius 2, 3, and 7. The 11 points of $\Lambda_{O_{\mathbb{K}}}$ on these three shells represent the quotient ring $O_{\mathbb{K}}/\mathcal{I}$. Each of these points is the image via the homomorphism Φ of an element from $\mathbb{F}_{11}$.

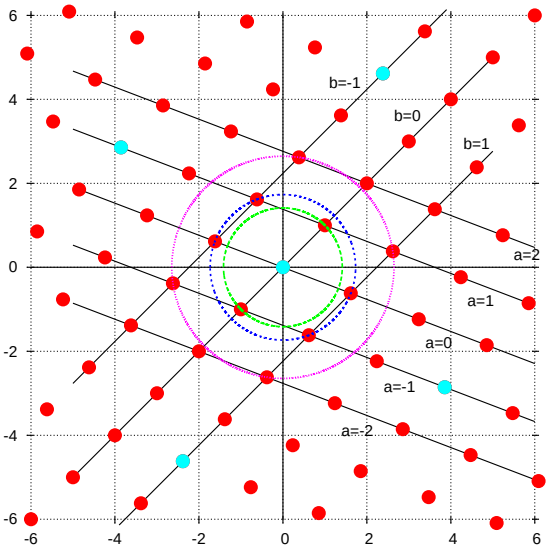

Figure 2. The bidimensional double-diversity lattices $\Lambda_{O_{\mathbb{K}}}$ and $\Lambda_{\mathcal{I}}$ built from the field $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ and $O_{\mathbb{K}}/\mathcal{I}$ shown on the first three shells.

IV. Alphabet size with double diversity

As a continuation of the previous section, we limit our study to real quadratic number fields $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, $d \geq 2$. Distance inside the coset $\Lambda_{\mathcal{I}}$ should be large enough to avoid error floors on a Gaussian channel. Similarly to Lemma (1), we state the following lemma for $O_{\mathbb{K}}$-lattices defined by (7).

Lemma 2: Let $\Lambda \subset \mathbb{R}^n$ be a real lattice built via Construction A as in (7). Then, its sublattice $\Lambda^m_{\mathcal{I}}$ has an error probability $P_e(\Lambda_{\mathcal{I}})$ per two dimensions ($[\mathbb{K} : \mathbb{Q}] = 2$) on a Gaussian channel that admits the following lower and upper bounds

$$2Q\left(\sqrt{\Delta\frac{\pi e}{2}\gamma_I \ p^R}\right) \leq P_e(\Lambda_{\mathcal{I}}), \quad (13)$$

$$P_e(\Lambda_{\mathcal{I}}) \leq 2Q\left(\sqrt{\Delta\frac{\pi e}{2}\gamma_I \ p^R}\right) + \sum_{\ell=2}^{3} 2Q\left(\sqrt{\Delta\frac{\pi e}{2}\frac{d^2_\ell(\mathcal{I}) \ p^R}{vol(\Lambda_{\mathcal{I}})}}\right),$$

where $R = \frac{k}{m} = \frac{k}{n/2}$ is the coding rate of C, Δ is the SNR-distance to Poltyrev limit, the Hermite constant is $\gamma_I = d^2_{Emin}(\mathcal{I})/vol(\Lambda_{\mathcal{I}})$ with $vol(\Lambda_{\mathcal{I}}) = N(\mathcal{I})\sqrt{d_{\mathbb{K}}}$ and $d^2_{Emin}(\mathcal{I})$ being the minimal squared Euclidean distance of the lattice $\Lambda_{\mathcal{I}}$. The second term in the upper bound involves $d^2_{Emin}(\mathcal{I}) = d^2_1(\mathcal{I}) \leq d^2_2(\mathcal{I}) \leq d^2_3(\mathcal{I})$, where $d^2_\ell(\mathcal{I})$ for $\ell = 1 \ldots 3$ correspond to the squared Euclidean norms of the six closest lattice points to the origin.

Proof: In the bidimensional lattice $\Lambda_{\mathcal{I}}$, consider a point x_ℓ at distance $d_\ell(\mathcal{I})$ from the origin 0. Assuming 0 is transmitted over a Gaussian channel, the error probability with respect to x_ℓ, known as the pairwise error probability, is given by

$$P_e(\ell) = Q\left(\frac{d_\ell(\mathcal{I})}{2\sigma}\right). \quad (14)$$

Notice that the noise level affecting $\Lambda_{\mathcal{I}}$ is identical to that affecting the lattice Λ. The noise variance is $\sigma^2 = \sigma^2_{max}/\Delta = \frac{vol(\Lambda)^{2/n}}{\Delta \times 2\pi e}$. By its definition (7), the lattice fundamental volume is $vol(\Lambda) = vol^m(\Lambda_{\mathcal{I}})/p^k$ so we get

$$\frac{1}{\sigma^2} = \frac{\Delta \ 2\pi e}{vol(\Lambda_{\mathcal{I}})} \ p^R.$$

Substituting the expression of $\frac{1}{\sigma^2}$ in (14) gives the final expression of $P_e(\ell)$

$$P_e(\ell) = Q\left(\sqrt{\Delta\frac{\pi e}{2}\frac{d^2_\ell(\mathcal{I}) \ p^R}{vol(\Lambda_{\mathcal{I}})}}\right). \quad (15)$$

For $\ell = 1$, $P_e(1) = Q\left(\sqrt{\Delta\frac{\pi e}{2}\gamma_I \ p^R}\right)$ and $2P_e(1)$ is a lower bound to $P_e(\Lambda_{\mathcal{I}})$ because of the Voronoi facets corresponding to points x_1 and $-x_1$. This proves the lower bound to $P_e(\Lambda_{\mathcal{I}})$.

For the upper bound, one should notice that the number of Voronoi facets cannot exceed 6 in dimension 2. Then we obtain $P_e(\Lambda_{\mathcal{I}}) \leq 2P_e(1) + 2P_e(2) + 2P_e(3)$.

■

It is clear from Lemma 2 that a good choice of $\Lambda_{\mathcal{I}}$, for a given finite field size p, is to maximize its Hermite constant γ_I. Of course, dropping the constraint $N(\mathcal{I}) = p$ will allow us to build the densest bidimensional lattice $\Lambda_{\mathcal{I}} = A_2$ [3] with Hermite constant $\gamma_I = 2/\sqrt{3} = 0.62dB$. Unfortunately, attaining $\Lambda_{\mathcal{I}} = A_2$ leads to huge ideal norms for $d \geq 7$. For $\mathbb{Q}(\sqrt{3})$, the construction of the hexagonal lattice A_2 can be made as follows with a non-prime alphabet size $N(\mathcal{I})$:

$$I = \ell(3+\sqrt{3})\mathbb{Z}[\sqrt{3}], \quad N(\mathcal{I}) = 6\ell^2, \quad \forall \ell \in \mathbb{Z}^*. \tag{16}$$

Construction π_A proposed by Huang and Narayanan [15] works with an alphabet which is equal to the product of distinct primes. It is not so simple to build non-binary codes over an alphabet of size $6k^2$ and keep $\Lambda_{\mathcal{I}} = A_2$. Plugging back the constraint $N(\mathcal{I}) = p$, we look for ideals in real quadratic fields with the highest possible γ_I. Table I shows such ideals for $p = 11, 13, 17$ and 31. Ideals from $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{14})$ considered in the previous section are also listed for reference in Table I. The first six terms of the Theta series of these lattices are found in Table II.

p	d	$d_{\mathbb{K}}$	g	$d^2_{Emin}(\mathcal{I})$	$\gamma_I(dB)$
11	5	5	$-1+3\phi$	23	-0.29
11	14	56	$5+\phi$	78	-0.23
11	341	341	$26+3\phi$	231	0.56
13	127	508	$\pm 34+3\phi$	326	0.46
17	973	973	$-338+21\phi$	578	0.37
31	341	341	$44+5\phi$	651	0.56

Table I
PARAMETERS FOR LATTICES $\sigma(\mathcal{I})$ WHERE $\mathcal{I} = gO_{\mathbb{K}}$ IS A PRINCIPAL IDEAL IN THE RING OF INTEGERS $O_{\mathbb{K}}$ OF QUADRATIC NUMBER FIELDS $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. THE IDEAL NORM $N(\mathcal{I}) = p$, THE DISCRIMINANT $d_{\mathbb{K}}$, THE GENERATOR g, THE MINIMUM EUCLIDEAN DISTANCE, AND HERMITE CONSTANT $\gamma_I(dB) = 10\log_{10}(\gamma_I)$ ARE GIVEN.

p	d	$\theta_{\Lambda_{\mathcal{I}}}(z)$
11	5	$1+2q^{23}+2q^{27}+2q^{42}+2q^{58}+2q^{92}+\ldots$
11	14	$1+2q^{78}+2q^{100}+2q^{114}+2q^{242}+2q^{284}+\ldots$
11	341	$1+4q^{231}+2q^{242}+2q^{682}+4q^{715}+4q^{924}+\ldots$
13	127	$1+2q^{326}+2q^{338}+2q^{352}+2q^{976}+2q^{1018}+\ldots$
17	973	$1+2q^{578}+2q^{599}+2q^{667}+2q^{1687}+2q^{1891}+\ldots$
31	341	$1+4q^{651}+2q^{682}+2q^{1922}+4q^{2015}+4q^{2604}+\ldots$

Table II
THETA SERIES FOR $\Lambda_{\mathcal{I}} = \sigma(\mathcal{I})$ OF LATTICES GIVEN IN TABLE I.

The Euclidean distances d_1, d_2, d_3 required for the lower and upper bounds in Lemma 2 are easily determined from Table II. Notice that $\mathbb{Q}(\sqrt{341})$ reaches $\gamma_I = 0.56dB$ (very close to A_2) for $p = 11$ and $p = 31$. The kissing number is 4 in these two cases. We plotted the error probability of the ideal in Figure 3 versus the coding rate R. Depending on the kissing number τ, we plotted $2P_e(1)$ if $\tau = 2$ and $P_e(1) + P_e(2) = 4P_e(1)$ if $\tau = 4$. Indeed, $\tau P_e(1)$ is a very accurate approximation for $P_e(\Lambda_{\mathcal{I}})$ at low error rates. From the results in Figure 3, we conclude that the error floor due to $\Lambda^m_{\mathcal{I}}$ can be guaranteed to be less than 10^{-6} by choosing a large enough coding rate, e.g. $R \geq 0.69$ for $p = 11$ and $R \geq 0.48$ for $p = 31$.

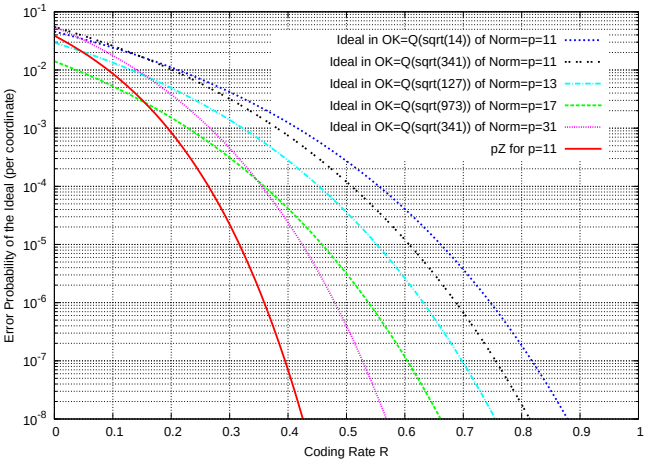

Figure 3. Performance of best found ideals $\mathcal{I} = gO_{\mathbb{K}}$ in $O_{\mathbb{K}}$ in real quadratic fields $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. The plot shows the point error probability (in two dimensions) versus the coding rate R of Construction A, at $\Delta = 0dB$ from Poltyrev limit.

To understand how p^{2R} in Lemma 1 switches down to p^R in Lemma 2, let us rewrite the expression of $P_e(1)$ for any diversity $L = r_1 + r_2 \geq 2$ and $[\mathbb{K} : \mathbb{Q}] \geq 2$. Since $n = m \cdot [\mathbb{K} : \mathbb{Q}]$, the normalized volume becomes $[vol(\Lambda)]^{\frac{2}{n}} = [vol(\Lambda_{\mathcal{I}})]^{\frac{2}{[\mathbb{K}:\mathbb{Q}]}}/p^{\frac{2R}{[\mathbb{K}:\mathbb{Q}]}}$ and $\frac{d^2_{Emin}(\mathcal{I})}{[vol(\Lambda_{\mathcal{I}})]^{\frac{2}{[\mathbb{K}:\mathbb{Q}]}}} = \gamma_I$. The general expression is

$$P_e(1) = Q\left(\sqrt{\Delta \frac{\pi e}{2} \gamma_I \; p^{\frac{2R}{[\mathbb{K}:\mathbb{Q}]}}}\right). \tag{17}$$

The lattice diversity produced by the number field comes with a drawback. The price to pay for $L \leq [\mathbb{K} : \mathbb{Q}]$ is a factor of $1/[\mathbb{K} : \mathbb{Q}]$ in the exponent of p.

V. CONSTRUCTION A FOR HIGHER DIVERSITY AND NON-PRIME FIELDS

As revealed by (17), p should be enlarged to $p^{[\mathbb{K}:\mathbb{Q}]}$ in order to get back to the factor p^{2R} found in Lemma 1. For simplicity, we limit our study here to totally real number fields and to lattices as modules over $\mathbb{Z}$. Most of the constructions and results can be extended from $\mathbb{Z}$-modules to modules over the Gaussian integers [10] or Eisenstein integers [20]. We discuss below three constructions for diversity orders $L \geq 2$ and non-prime finite fields.

- **Construction over a non-prime finite field**. Consider the ideal $\mathcal{I} = pO_{\mathbb{K}}$ of $O_{\mathbb{K}}$ where p is inert in $\mathbb{K}$. Then, $N(\mathcal{I}) = p^L$, where $L = [\mathbb{K} : \mathbb{Q}] \geq 2$ is the diversity order. Also, $O_{\mathbb{K}}/\mathcal{I}$ is isomorphic to $\mathbb{F}_{p^L}$. In this case, Construction A can utilize a linear code $C[m,k]_{p^L}$ of length $m = n/L$ over the non-prime field $\mathbb{F}_{p^L}$. From a performance point of view, this is similar to a Construction A with a prime field

of order close to p^L. But the non-prime field may help in finding faster decoding algorithms for C. Finally, in a slightly different construction, it is possible to consider $N(\mathcal{I}) = p^\ell$, $\ell < L$, and look for the ideal $\mathcal{I}$ with the highest γ_I.

• **Construction with p totally split**. Consider again the ideal $\mathcal{I} = pO_\mathbb{K}$ where p is totally split in $\mathbb{K}$. Then, $\mathcal{I} = \prod_{j=1}^{L} \mathcal{I}_j$ is the product of L ideals with $O_\mathbb{K}/\mathcal{I}_j$ isomorphic to $\mathbb{F}_p$. In this case, the lattice Λ is built from a linear code of length n over $\mathbb{F}_p$. There is no need for a non-prime field. However, the Hermite constant of $O_\mathbb{K}$ should be maximized which may reduce the freedom while looking for an adequate number field. In this method, for example, $\mathbb{Q}(\sqrt{5})$ is the best candidate for $L = 2$. For $L > 2$, a number field with a ring $O_\mathbb{K}$ of acceptable Hermite constant should be chosen. Recall that $\gamma_{O_\mathbb{K}}$ and γ_I can never exceed the Hermite constant of the densest lattice in real dimension $[\mathbb{K} : \mathbb{Q}]$. So, even if the performance is dominated by the factor $p^{2R/[\mathbb{K}:\mathbb{Q}]}$, a ring $O_\mathbb{K}$ with bad density should be avoided.

• **Naive construction with rotated cubic lattices**. Number fields for this method were well studied in [5], [2]. Let $\mathbb{Z}_L$ be a rotated version of diversity L of the integer cubic lattice $\mathbb{Z}^L$. In this case, $\mathbb{Z}_L = \sigma(\mathcal{I})$ for a specific ideal $\mathcal{I}$ in $O_\mathbb{K}$ and the generator matrix G_I is orthogonal. The quotient $\mathbb{Z}_L/p\mathbb{Z}_L$ has order p^L. Construction A becomes $\Lambda = C[m,k]_{p^L} + p\mathbb{Z}_L^m$, where $m = n/L$. But $\mathbb{Z}_L/p\mathbb{Z}_L = G_I \cdot (\mathbb{Z}/p\mathbb{Z})^L$, this allows us to go back to $\mathbb{F}_p$. Let Γ be a $n \times n$ orthogonal matrix built by m copies of G_I placed on its main diagonal. The naive construction is

$$\Lambda = \Gamma \cdot (C[n,k]_p + p\mathbb{Z}^n)\,. \tag{18}$$

The performance is now given by Lemma 1. Assuming C is a sparse code (LDPC or GLD), decoding can be made via belief propagation on a factor graph that includes the checknodes of C and the $L \times L$-rotation checknodes. In this method, the best choice of $\mathbb{Z}_L$ is not known yet. In [5], [2], the $L \times L$ rotation yields the maximal product distance, or a high product distance if the maximum cannot be attained. The best $\mathbb{Z}_L$ by itself does not necessarily lead to the best Construction A. This behavior was already observed in GLD lattices where a good component lattice may degrade the larger Construction-A GLD lattice.

VI. Conclusions and Perspectives

Two decades ago, small-dimensional lattices that are good for both Gaussian and Rayleigh fading channels were constructed [4]. In large dimensions, Construction A with non-binary codes is one of the most successful recent tools for building lattices. This paper proposed methods to build Construction-A lattices that are good for both Gaussian and fading channels. The alphabet size p of the inherent non-binary linear code should be large enough (reasonable values are found) in order to avoid error floors generated by the sublattice $p\mathbb{Z}^n$ or $\Lambda_\mathcal{I}^m$. In the last section, three methods for high diversity orders were described. Our future work will be dedicated to these methods, the study of their lattice parameters, their performance analysis under lattice decoding and iterative decoding, and their practical implementation.

Acknowledgment

The work of Joseph J. Boutros was supported by the Qatar National Research Fund (QNRF), a member of Qatar Foundation, under NPRP project 6-784-2-329.

References

[1] M. Abramowitz and I.A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*. National Bureau of Standards, Applied Mathematics Series, June 1964, 10th printing, December 1972.

[2] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo, "New Algebraic Constructions of Rotated $\mathbb{Z}^n$-Lattice Constellations for the Rayleigh Fading Channel," *IEEE Trans. on Inf. Theory*, vol. 50, no. 4, pp. 702-714, April 2004.

[3] E. Bayer-Fluckiger and G. Nebe, "On the Euclidean minimum of some real number fields," *Journal de Théorie des Nombres de Bordeaux*, Tome. 17, no. 2, pp. 437-454, 2005.

[4] J.J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channels," *IEEE Trans. on Inf. Theory*, vol. 42, no. 2, pp. 502-518, March 1996.

[5] J.J. Boutros and E. Viterbo, "Signal Space Diversity: a power and bandwidth efficient diversity technique for the Rayleigh fading channel," *IEEE Trans. on Inf. Theory*, vol. 44, no. 4, pp. 1453-1467, July 1998.

[6] J.J. Boutros, A. Guillén i Fàbregas, E. Biglieri, and G. Zémor, "Low-Density Parity-Check Codes for Nonergodic Block-Fading Channels," *IEEE Trans. on Inf. Theory*, vol. 56, no. 9, pp. 4286-4300, Sept. 2010.

[7] J.J. Boutros, N. di Pietro, and Y. C. Huang, "Spectral thinning in GLD lattices," *2016 Information Theory and Applications Workshop (ITA)*, La Jolla, CA, pp. 1-9, Feb. 2015.

[8] J.J. Boutros, O. Pothier, and G. Zémor, "Generalized low density (Tanner) codes," *IEEE Intern. Conf. on Comm. (ICC)*, vol. 1, pp. 441-445, Vancouver, June 1999.

[9] M.C. Davey and D.J.C MacKay, "Low Density Parity Check Codes over GF(q)," *IEEE Communications Letters*, vol. 2, pp. 165-167, June 1998.

[10] N. di Pietro, J.J. Boutros, G. Zémor, and L. Brunel, "Integer low-density lattices based on Construction A," *Proc. of the 2012 IEEE Inf. Theory Workshop*, pp. 422-426, Lausanne, Sep. 2012.

[11] N. di Pietro, G. Zémor, and J.J. Boutros, "LDA lattices without dithering achieve capacity on the Gaussian channel," submitted to the *IEEE Trans. on Inf. Theory*, March 2016. http://arxiv.org/pdf/1603.02863v1.

[12] U. Erez and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Trans. on Inf. Theory*, vol. 51, no. 10, pp. 3401-3416, Oct. 2005.

[13] G. D. Forney, "Coset codes I: introduction and geometrical classification,", *IEEE Trans. on Inf. Theory*, vol. 34, no. 5, pp. 1123-1151, 1988.

[14] R. G. Gallager. *Low-density parity-check codes*, PhD thesis, Massachusetts Institute of Technology Press, 1963.

[15] Y.-C. Huang and K.R. Narayanan, "Construction π_A and π_D Lattices: Construction, Goodness, and Decoding Algorithms," June 2015. http://arxiv.org/pdf/1506.08269v1.

[16] J. Leech and N.J.A. Sloane, "Sphere packing and error-correcting codes," *Canadian Journal of Mathematics*, no. 23, pp. 718-745, 1971.

[17] G. Poltyrev, "On coding without restrictions for the AWGN channel," *IEEE Trans. on Inf. Theory*, vol. 40, no. 2, pp. 409-417, March 1994.

[18] P. Samuel, *Théorie Algébrique des Nombres*. Hermann, Paris, 1967. English translation, *Algebraic Number Theory*, Houghton Mifflin, New York, 1975.

[19] N. Sommer, M. Feder, and O. Shalvi, "Low-density lattice codes," *IEEE Trans. on Inf. Theory*, vol. 54, no. 4, pp. 1561-1585, April 2008.

[20] N.E. Tunali, Y.-C. Huang, J.J. Boutros, and K.R. Narayanan, "Lattices over Eisenstein Integers for Compute-and-Forward," *IEEE Trans. on Inf. Theory*, vol. 61, no. 10, pp. 5306-5321, Oct. 2015.

[21] P.-C. Wang, Y.-C. Huang, K.R. Narayanan, and J.J. Boutros, "Physical-layer network-coding over block fading channels with Root-LDA lattice codes," *IEEE Intern. Conf. on Comm. (ICC)*, Kuala Lumpur, May 2016.

[22] R. Zamir, *Lattice coding for signals and networks.* Cambridge University Press, 2014.