Non-Binary GLD Codes and their Lattices

Nicola di Pietro, Nour Basha, and Joseph J. Boutros
Texas A&M University at Qatar
c/o Qatar Foundation, Education City, 23874, Doha, Qatar
{nicola.dipietro, nour.basha, joseph.boutros}@qatar.tamu.edu

***Abstract*—The recently discovered family of generalized low-density (GLD) lattices brings new mathematical challenges to coding theorists and practitioners. Given the excellent performance of integer GLD lattices in high dimensions and motivated by the simple lattice structure used for fast iterative decoding, this paper is a first attempt to analyze GLD lattices for asymptotically large dimensions. Firstly, we describe non-binary GLD codes and show their asymptotic goodness in terms of minimum Hamming distance. Secondly, we consider a GLD lattice ensemble built via Construction A from non-binary GLD codes, and analyze their goodness with respect to Poltyrev limit on the Gaussian channel. Finally, at large dimensions and using a large code alphabet, we prove that infinite GLD lattice constellations attain Poltyrev capacity limit under maximum likelihood decoding.**

I. Introduction

Coding theory includes the study of mathematical structures to protect information in its digital or analog form. Among those structures, point lattices in the Euclidean space are an interesting tool for both source coding and channel coding. In [1], a new family of generalized low-density (GLD) lattices was proposed. The key idea is to build a new lattice in high dimensions from the intersection of two or more interleaved direct sums of a small-dimensional lattice. A special situation occurs if the small lattice itself is built from a non-binary Construction A. In such a case, the GLD lattice itself is derived from a non-binary GLD code via Construction A. Binary GLD codes proposed more than a decade ago in [3], [4] are based on the intersection of two binary codes. GLD codes are another example of mathematical structures (in a finite field) useful in coding and information theory. In this paper, we consider non-binary GLD codes in order to build integer GLD lattices.

We show the asymptotic goodness property of GLD codes over the finite field $\mathbb{F}_p$ under some conditions on the codes' parameters. This property is used in a second step to find a decoding gap to Poltyrev limit on the Gaussian channel [17]. These two main results are found in (7) and Theorem 2. As a consequence, when the GLD code approaches the Varshamov-Gilbert bound at a vanishing rate and a large p, the GLD lattice ensemble attains Poltyrev limit (cf. Corollary 1). The main motivation for this first attempt in analyzing GLD lattices came from the excellent performance observed under iterative decoding [2]. Currently, there are no complete or accurate mathematical tools to understand iterative decoding for non-binary fields and the real field. Hence our study considers minimum distance and ML decoding for GLD codes and lattices respectively.

II. Non-Binary GLD Codes

Generalized low-density codes have many interesting aspects, based on their matrix and graph representations as reported for the binary case in [3], [4]. A non-binary GLD ensemble has a representation identical to its binary counterpart, but binary variables are replaced by symbols belonging to the finite field $\mathbb{F}_p$. We restrict our study to prime fields, i.e. p is a prime integer.

Let C_1 and C_2 be two codes of length N and dimension K defined over $\mathbb{F}_p$. At the price of a lower coding rate, a code C with a better error-correction capability is built from the intersection of C_1 and C_2,

$$C = C_1 \cap C_2. \tag{1}$$

We say that $p-$ary code symbols have degree $J = 2$ because they belong to two check nodes defined by C_1 and C_2 respectively. As a simple example, let C_1 be a binary BCH code with parameters $[15, 11, t = 1]_2$ whose generator polynomial is $g_1(x) = x^4 + x + 1$. Let C_2 be a binary BCH code with same parameters $[15, 11, t = 1]_2$ and generator polynomial $g_2(x) = x^4 + x^3 + x^2 + x + 1$. It is straightforward to prove that $C = C_1 \cap C_2$ is a double error-correcting BCH code [5] with parameters $[15, 7, t = 2]_2$. In order to handle a very large code length N, it is important to introduce an elementary code C_0 of length n and dimension k. Then, C_1 is taken to be a direct sum of L versions of C_0, i.e. $C_1 = C_0^{\oplus L}$, where $L = N/n$. The second big check C_2 is taken to be a permuted version of C_1, i.e. $C_2 = \pi(C_1)$, where π is a permutation of size N. The standard GLD code definition becomes

$$C = C_0^{\oplus L} \cap \pi(C_0^{\oplus L}). \tag{2}$$

The structure of the parity-check matrix of C is illustrated in Figure 1. A GLD code with a higher degree J can be built if the intersection involves J codes with $J - 1$ permutations. If $R_0 > (J - 1)/J$ is the rate of C_0, the rate of the GLD code C is for almost all permutations equal to

$$R = 1 - J(1 - R_0) > 0 \tag{3}$$

Now, we generalize the ensemble performance found in [3], [4] to the non-binary case in order to find a condition that guarantees that non-binary GLD codes are asymptotically good. In the sequel, given a GLD ensemble, the expression of a certain $B(\omega)$ is determined as a function of the parameters p, J, n, and k. The positivity of this $B(\omega)$ near the origin will imply that the ensemble is asymptotically good. Let

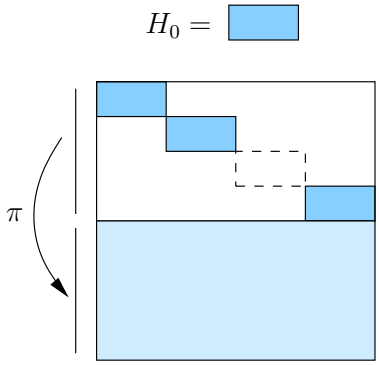

Figure 1. Structure of the GLD parity-check matrix for symbols of degree $J = 2$, where H_0 is the parity-check matrix of an elementary code C_0 and π is a column permutation.

$g(s) = A_0(e^s)/p^k$ be the moment generating function of C_0, where $A_0(x)$ is the weight enumerator polynomial [5] of C_0. Then, the moment generating function of $C_1 = C_0^{\oplus L}$ is $G(s) = g(s)^L = \sum_\ell Q(\ell)e^{\ell s}$. The number of codewords in C_1 of Hamming weight ℓ is $N_1(\ell) = p^{kL}Q(\ell)$. Let us suppose that π_1 is the identity and that $\pi_2, \pi_3, \ldots, \pi_J$ are some random permutations of $\{1, 2, \ldots, N\}$. Then, the probability that a vector of weight ℓ belongs to $C = \cap_{j=1}^{J} \pi_j(C_0^{\oplus L})$ is

$$P(\ell) = \left(\frac{N_1(\ell)}{\binom{N}{\ell}(p-1)^\ell} \right)^J. \tag{4}$$

The average number of codewords in C having weight ℓ is

$$N(\ell) = \binom{N}{\ell}(p-1)^\ell \times P(\ell) = \frac{p^{JkL}Q(\ell)^J}{\left(\binom{N}{\ell}(p-1)^\ell\right)^{J-1}}. \tag{5}$$

After upper bounding $Q(\ell)$ by $G(s)e^{-\ell s}$, based on the argument found in [4], we find

$$N(\ell) = \Theta(\exp(-NB(\omega))), \tag{6}$$

where Θ refers to the Bachmann-Landau notation and $\omega = \ell/N$ is the normalized Hamming weight, such that $\omega \in [0, 1]$. Further details are omitted due to lack of space. In addition, let $\mu(s) = \log(g(s))$ and $H(x) = -x\log(x) - (1-x)\log(1-x)$, where $H(x)$ is the natural entropy function. The function $B(\omega)$, found in (6), is expressed as follows:

$$\begin{aligned} B(\omega) = {} & (J-1)\left(H(\omega) + \omega\log(p-1)\right) \\ & - \frac{J}{n}(\mu(s) + k\log(p)) + Js\omega. \end{aligned} \tag{7}$$

Let $\mathrm{d}_{\mathrm{H}_{\min}}(C)$ be the minimum Hamming distance of C. From (6) and (7), when $N \to \infty$, the normalized minimum Hamming distance $\Delta = \mathrm{d}_{\mathrm{H}_{\min}}(C)/N$ is lower bounded by the largest ω_0 satisfying $B(\omega) > 0$ for $\omega \in]0, \omega_0[$. Figure 2 shows the lower bound of Δ for three GLD ensembles with $J = 2$ and different coding rates and compares it to the Varshamov-Gilbert bound [7]. The illustrated results are $\Delta \geq 0.1136$ for $C_0[24, 18]_{11}$, $\Delta \geq 0.3732$ for $C_0[16, 10]_{11}$, and $\Delta \geq 0.6454$ for $C_0[20, 11]_{11}$.

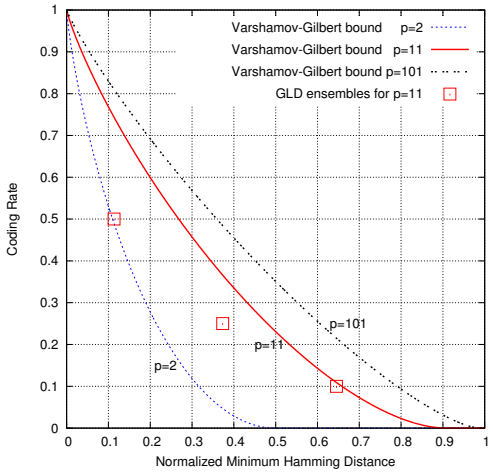

Figure 2. Lower bound on minimum Hamming distance for GLD ensembles with $J = 2$ for $p = 11$ and three different coding rates.

III. Notation for Lattices

An *N-dimensional lattice* Λ is a discrete additive subgroup of $\mathbb{R}^N$ identified by a *basis* of N linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_N$. By definition,

$$\Lambda = \left\{ \mathbf{x} \in \mathbb{R}^N : \mathbf{x} = \sum_{i=1}^{N} z_i \mathbf{b}_i,\ z_i \in \mathbb{Z} \right\}. \tag{8}$$

The matrix G with the $\mathbf{b}_i$'s as rows is called a *generator matrix* of the lattice and, synthetically, we write $\Lambda = \mathbb{Z}^N G$. The *volume* of a lattice is defined as $\mathrm{Vol}(\Lambda) = |\det(G)|$ and is independent from the choice of a lattice basis. A classical reference for learning more about lattices is [16].

Definition 1: Let p be a prime number and consider a linear code $C = C[N, K]_p$ over $\mathbb{F}_p$ of length N, dimension K, and rate $R = K/N$. The lattice Λ obtained by *Construction A* from C is defined as

$$\Lambda = \{\mathbf{x} \in \mathbb{R}^N : \mathbf{x} \equiv \mathbf{c} \bmod p,\ \exists \mathbf{c} \in C\} = C + p\mathbb{Z}^N. \tag{9}$$

Construction A lattices are very useful for many theoretical and practical reasons and have been very often employed in the literature concerning lattice coding (see for example [1], [8]–[15]). More details about Construction A can be found in [16]. A well-known property of Construction A lattices, which will be used later in this paper, is [6]

$$\mathrm{Vol}(\Lambda) = p^{N-K} = p^{N(1-R)}. \tag{10}$$

IV. Poltyrev Capacity for the Gaussian Channel

In this paper we deal with (infinite) lattices as codes for the transmission of information over the unconstrained Additive White Gaussian Noise (AWGN) channel. A message is a lattice point $\mathbf{x}$ and the channel output is $\mathbf{y} = \mathbf{x} + \mathbf{w} \in \mathbb{R}^N$, where $\mathbf{w}$ is the random noise and the w_i's are i.i.d. random variables, independent from the channel input. For every i, the random w_i follows a Gaussian distribution with mean value 0 and variance σ^2.

Infinite lattice constellations have infinite energy and their performance can be analyzed by the means of *Poltyrev capacity*. We summarize Poltyrev's results as follows [17]:

Theorem 1 (Poltyrev): Given the unconstrained AWGN channel with channel noise variance σ^2, there exists a sequence of N-dimensional lattices of constant volume V for which the decoding probability can be made as small as wanted for a sufficiently large value of N, if and only if $V^{\frac{2}{N}} > 2\pi e\sigma^2$. As a consequence, given a family of lattices with volume V, we can hope that a lattice in the family can be decoded with vanishing error probability only if the channel noise obeys

$$\sigma^2 < \sigma^2_{\max} = \frac{V^{\frac{2}{N}}}{2\pi e}. \tag{11}$$

$\sigma^2_{\max}$ is often referred to as *Poltyrev capacity*. We say that a lattice family with volume V is *Poltyrev-capacity-achieving* if a random element of the family has a vanishing error decoding probability for every value of $\sigma^2 < \sigma^2_{\max}$.

To conclude this section, we recall that the weak law of large numbers implies:

Lemma 1 (Typical norm of the AWG noise): Consider N i.i.d. random variables $X_1, \ldots, X_N$, each of them following a Gaussian distribution of mean 0 and variance σ^2. Let $\rho = \sqrt{\sum_{i=1}^N X_i^2}$; then, for every $\varepsilon > 0$,

$$\lim_{N\to\infty} \mathcal{P}\left\{\rho \leq \sigma\sqrt{N}\,(1+\varepsilon)\right\} = 1. \tag{12}$$

V. GLD Lattices And Poltyrev Capacity

Generalized low-density (GLD) lattices were defined for the first time in [1]. We recall that their definition traces the one given in Section II for GLD codes: given an n-dimensional lattice Λ_0, a natural number $L = N/n$ and $J-1$ different permutations $\pi_2, \pi_3, \ldots, \pi_J$ of $\{1, 2, \ldots, N\}$, an nL-dimensional GLD lattice Λ is defined by:

$$\Lambda = \Lambda_0^{\oplus L} \cap \pi_2\left(\Lambda_0^{\oplus L}\right) \cap \cdots \cap \pi_J\left(\Lambda_0^{\oplus L}\right). \tag{13}$$

In this paper, we will only deal with GLD lattices for which Λ_0 is built by Construction A from a code C_0 of length n. In this case, the GLD lattice Λ is actually a Construction A lattice, too, and

$$\Lambda = C + p\mathbb{Z}^N, \tag{14}$$

where C is the GLD code obtained from C_0 with the same π_i's and the same parameters n, L, and J of the GLD lattice.

A. The random ensemble

We would like to investigate the problem of achieving Poltyrev capacity with GLD lattices under maximum likelihood decoding. Our main results about this problem are contained in Theorem 2 and Corollary 1 and are obtained for a particular random ensemble of GLD lattices. The used techniques are very similar to the ones applied in [13], [14] for proving analogous results for low-density Construction A lattices (LDA).

Our GLD lattice ensemble is obtained by Construction A from a GLD code ensemble that contains randomness in two different senses. Firstly, the π_i's are chosen independently and uniformly at random amongst all the permutations of $\{1, 2, \ldots, N\}$. Secondly, $C_0^{\oplus L}$ is the direct sum of L random i.i.d. random codes. Each one of the random C_0's is defined by its $(n-k)\times n$ parity-check matrix (with $k/n = R_0 > (J-1)/J$), whose entries are i.i.d. random variables, uniformly taking values in $\{0, 1, \ldots, p-1\}$.

B. Some classical useful lemmas

Lemma 2 provides a useful upper bound for the binomial coefficient. Its proof can be found in [5, Ch. 10 - Lemma 7]. The proof of (16) can be found in [14, Lemma 2.3], while (17) is classical and directly comes from Stirling's formula.

Lemma 2: Let N be a natural number and let $0 \leq \theta \leq 1$ be any rational number such that θN is natural. Then:

$$\binom{N}{\theta N} \leq \frac{1}{\sqrt{2\pi N\theta(1-\theta)}} e^{NH(\theta)}, \tag{15}$$

where $H(\theta)$ is once again the natural entropy function.

Lemma 3: Let $B_{\mathbf{c},N}(\rho) = \{\mathbf{x} \in \mathbb{R}^N : \|\mathbf{x}-\mathbf{c}\|^2 \leq \rho^2\}$ be the N-dimensional ball centered at $\mathbf{c}$ of radius ρ. Then

$$|\mathbb{Z}^N \cap B_{\mathbf{c},N}(\rho)| \leq \mathrm{Vol}\left(B_{\mathbf{c},N}(\rho)\right)\left(1 + \frac{\sqrt{N}}{2\rho}\right)^N \tag{16}$$

and

$$\mathrm{Vol}(B_{\mathbf{c},N}(\rho)) \sim \frac{1}{\sqrt{\pi N}}\left(\frac{\sqrt{2\pi e}\rho}{\sqrt{N}}\right)^N. \tag{17}$$

C. The main results

As we have already mentioned, Theorem 2 and Corollary 1 concern the possibility of achieving Poltyrev capacity with GLD lattices under ML decoding. For infinite lattice constellations, ML decoding consists in looking for the closest lattice point to the channel output. If this point is equal to the channel input, then we have decoded well; otherwise, an error occurs.

Despite its random nature, every lattice in our GLD ensemble deterministically contains $p\mathbb{Z}^N$, as defined by the properties of Construction A (see (14)). This suggests that the points of $p\mathbb{Z}^N$ have to be treated individually when we probabilistically analyze the decoding of a GLD lattice. The following lemma will be used for this purpose in order to prove Theorem 2, and shows that, asymptotically, the points of $p\mathbb{Z}^N$ cannot lead to errors under ML decoding. Its proof is omitted due to a lack of space, but it can be found in [14, Lemma 3.1].

Lemma 4: Let $\Lambda \subseteq \mathbb{R}^N$ be a Construction A lattice, let $\mathbf{0} \in \Lambda$ be the lattice point to be sent over the AWGN channel and let $\mathbf{w}$ be the random noise vector. Furthermore, suppose that the noise variance per dimension is equal to $\sigma^2 = \sigma^2_{\max}(1-\delta)^2$, for some constant $0 < \delta < 1$ and $\sigma^2_{\max} = p^{2(1-R)}/2\pi e$, where R is the rate of the code underlying Construction A (cf. (10) and (11)). Then, for every $\mathbf{z} \in p\mathbb{Z}^N \setminus \{\mathbf{0}\}$, provided that $p \geq N^\lambda$ for some $\lambda > 0$,

$$\lim_{N\to\infty} \mathcal{P}\{\|\mathbf{w}\|^2 \geq \|\mathbf{w}-\mathbf{z}\|^2\} = 0. \tag{18}$$

And now, the main result of this paper:

Theorem 2: Consider the random ensemble described in Section V-A and suppose that $p \geq N^{\lambda}$ for some $\lambda > 0$. Moreover, suppose that the minimum Hamming distance of the random GLD codes underlying the GLD lattices is lower bounded by ΔN for some constant $\Delta > 0$. Then, for every $0 < \delta < 1$, such that

$$\frac{e^{\frac{H(\Delta)}{\Delta}}}{\sqrt{\Delta}}(1-\delta) < 1, \tag{19}$$

a random lattice of the family can be ML decoded with vanishing error probability for every channel noise variance $\sigma^2 = \sigma^2_{\max}(1-\delta)^2$.

Proof: Let Λ be a random lattice of our ensemble. Due to the lattice's symmetry and the independence of random noise from channel input, we can assume that the point of Λ transmitted over the channel is the point $\mathbf{0}$. The AWG noise vector is $\mathbf{w} = (w_1, w_2, \ldots, w_N)$, the channel output is $\mathbf{y} = \mathbf{w}$, and the channel noise variance is $\sigma^2 = \sigma^2_{\max}(1-\delta)^2$, where $\sigma^2_{\max}$ is the noise variance value that corresponds to Poltyrev capacity according to (11).

Lemma 1 states that, when N is very large, the vector $\mathbf{y}$ tends to lie within a distance of a little bit more than $\sigma\sqrt{N}$ to $\mathbf{0}$. Given $\varepsilon > 0$, let us call the *decoding ball* the N-dimensional ball $\mathcal{B} = B_{\mathbf{y},N}(\sigma\sqrt{N}(1+\varepsilon))$ centered at $\mathbf{y}$. When N goes to infinity, the point $\mathbf{0}$ is inside the decoding ball with probability tending to 1; if this occurs, the probability of making a decoding error under ML decoding is smaller than the probability that one or more lattice points different from $\mathbf{0}$ lie inside the ball. If $\mathbf{0}$ is the only lattice point in $\mathcal{B}$, then lattice decoding gives the correct answer; otherwise, an error will possibly occur. Furthermore, Lemma 4 guarantees that the possible presence of points of $p\mathbb{Z}^N$ inside the decoding ball does not actually impede good ML decoding.

Summarizing, it is sufficient to show that, if $\mathcal{N}$ is the random variable that counts the number of lattice points inside $\mathcal{B}$ that do not belong to $p\mathbb{Z}^N$, then $\lim_{N\to\infty} \mathcal{P}\{\mathcal{N} = 0\} = 1$.

In order to do this, for every integer point $\mathbf{x} \in \mathcal{B} \cap \mathbb{Z}^N$, consider the random variables

$$X_{\mathbf{x}} = \begin{cases} 1, & \text{if } \mathbf{x} \in \Lambda \\ 0, & \text{if } \mathbf{x} \notin \Lambda \end{cases} \quad \text{and} \quad \mathcal{N} = \sum_{\mathbf{x} \in \mathbb{Z}^N \cap \mathcal{B} \smallsetminus p\mathbb{Z}^N} X_{\mathbf{x}}; \tag{20}$$

to prove our result it is sufficient to show that

$$\lim_{N\to\infty} \mathbb{E}[\mathcal{N}] = \lim_{N\to\infty} \sum_{\mathbf{x} \in \mathbb{Z}^N \cap \mathcal{B} \smallsetminus p\mathbb{Z}^N} \mathcal{P}\{\mathbf{x} \in \Lambda\} = 0. \tag{21}$$

We use the fact that

$$\mathcal{P}\{\mathbf{x} \in \Lambda\} = \mathcal{P}\{\mathbf{x} \bmod p \in C\} = \left(\mathcal{P}\{\mathbf{x} \bmod p \in C_0^{\oplus L}\}\right)^J.$$

The latter equality holds true because the permutations defining C are completely random. Let H_1 be the parity-check matrix of $C_1 = C_0^{\oplus L}$ and let $\mathbf{h}$ be any of its rows, representing a parity-check equation. By construction, we know that $\mathbf{h}$ has exactly n (random) non-zero entries and $N-n$ (deterministic) zero entries (see the upper part of the matrix in Figure 3). We define the *support* of $\mathbf{x} \in \mathbb{R}^N$ as the set

$$\operatorname{Supp}(\mathbf{x}) = \{i : x_i \not\equiv 0 \bmod p\}, \tag{22}$$

and we say that the *weight* of $\mathbf{x}$ is $|\operatorname{Supp}(\mathbf{x})|$. Similarly, the *support* of $\mathbf{h}$ is

$$\operatorname{Supp}(\mathbf{h}) = \{i : h_i \text{ is a random variable}\}. \tag{23}$$

Then, for every $\mathbf{x} \in \mathbb{Z}^N \cap \mathcal{B} \smallsetminus p\mathbb{Z}^N$,

$$\mathcal{P}\{\mathbf{h}\mathbf{x}^T \equiv 0 \bmod p\} = \begin{cases} 1, & \text{if } \operatorname{Supp}(\mathbf{h}) \cap \operatorname{Supp}(\mathbf{x}) = \emptyset \\ p^{-1}, & \text{otherwise} \end{cases}.$$

The i.i.d. random choice of n entries of each row of H_1 makes the events $\{\mathbf{h}\mathbf{x}^T = 0 \bmod p\}_{\mathbf{h}}$ mutually independent. Therefore, if t is the number of rows of H_1 with which a certain $\mathbf{x}$ shares its support, then

$$\mathcal{P}\{\mathbf{x} \in \Lambda\} = \left(\mathcal{P}\{\mathbf{x} \bmod p \in C_0^{\oplus L}\}\right)^J = p^{-tJ}. \tag{24}$$

Recall that the only entries of H_1 that can be non-zero are its random entries. They are grouped into L blocks of dimension $(n-k) \times n$, that we will call the H_0-blocks of H_1. Then, as soon as $\mathbf{x}$ and $\mathbf{h}$ have some common support, the same will occur for all other $n-k-1$ parity-check equations corresponding to the same H_0-block as $\mathbf{h}$. This implies that t is equal to $n-k$ times the number of H_0-blocks of H_1, with whose equations $\mathbf{x}$ shares the support. For an $\mathbf{x}$ of fixed weight ℓ, this number is greater than or equal to ℓ/n, therefore

$$\mathcal{P}\{\mathbf{x} \in \Lambda\} \leq p^{-(n-k)\frac{\ell}{n}J} = p^{-J\ell(1-R_0)}, \tag{25}$$

where R_0 is the rate of the code C_0. By hypothesis, there exists $\Delta > 0$ such that $|\operatorname{Supp}(\mathbf{x})| \geq \Delta N$ for all $\mathbf{x} \in \Lambda \smallsetminus p\mathbb{Z}^N$. Thus,

$$\begin{aligned} \mathbb{E}[\mathcal{N}] &= \sum_{\ell=\lceil \Delta N \rceil}^{N} \sum_{\substack{\mathbf{x} \in \mathbb{Z}^N \cap \mathcal{B} \smallsetminus p\mathbb{Z}^N \\ |\operatorname{Supp}(\mathbf{x})| = \ell}} \mathcal{P}\{\mathbf{x} \in \Lambda\} \\ &\leq \sum_{\ell=\lceil \Delta N \rceil}^{N} M_\ell p^{-J\ell(1-R_0)}, \end{aligned} \tag{26}$$

where $M_\ell = |\{\mathbf{x} \in \mathbb{Z}^N \cap \mathcal{B} \smallsetminus p\mathbb{Z}^N : |\operatorname{Supp}(\mathbf{x})| = \ell\}|$. For $S \subseteq \{1, 2, \ldots, N\}$, let $\mathbf{x}_S = (x_s)_{s\in S}$ be the subvector of $\mathbf{x}$ made only of the coordinates of $\mathbf{x}$ indexed by elements of S. Moreover, let us call $P = \{i \mid x_i \equiv 0 \bmod p, x_i \neq 0\}$. If $S = \operatorname{Supp}(\mathbf{x})$, then, up to a coordinate reordering, $\mathbf{x}$ is partitioned like that: $\mathbf{x} = (0, \ldots, 0 \mid \mathbf{x}_P \mid \mathbf{x}_S)$. If $|P| = m$, then $\|\mathbf{x}_P\|^2 \geq mp^2$. Hence, recalling formulae (3), (10), and (11) and that the decoding ball $\mathcal{B}$ has radius $\rho = \sigma_{\max}(1-\delta)\sqrt{N}(1+\varepsilon)$, we can deduce that for every $\mathbf{x} \in \mathcal{B} \cap \mathbb{Z}^N$, the cardinality of P has to obey the condition:

$$\begin{aligned} mN^{2\lambda} \leq mp^2 \leq \rho^2 &= \frac{p^{2J(1-R_0)}}{2\pi e}(1-\delta)^2 N(1+\varepsilon)^2 \\ &\leq \frac{(1-\delta)^2(1+\varepsilon)^2}{2\pi e} N^{1+\lambda 2J(1-R_0)} < N^{1+\lambda 2J(1-R_0)}. \end{aligned}$$

This means that $m < N^{1-2\lambda(1-J(1-R_0))} = N^{\eta}$, for some $\eta = 1 - 2\lambda(1 - J(1 - R_0)) < 1$ because $1 - J(1 - R_0) > 0$ (see (3)). Hence, using Lemma 3 for (27):

$$\begin{aligned} M_\ell &\leq \binom{N}{\ell} |\mathbb{Z}^\ell \cap B_{\mathbf{y},\ell}(\rho)| + \\ &\quad + \sum_{m=1}^{\lfloor N^\eta \rfloor} \binom{N}{\ell} \binom{N-\ell}{m} |p\mathbb{Z}^m \cap B_{\mathbf{y},m}(\rho)||\mathbb{Z}^\ell \cap B_{\mathbf{y},\ell}(\rho)| \\ &\lesssim \binom{N}{\ell} |\mathbb{Z}^\ell \cap B_{\mathbf{y},\ell}(\rho)| \; + \binom{N}{\ell} N^{N^\eta} |\mathbb{Z}^\ell \cap B_{\mathbf{y},\ell}(\rho)| \cdot \\ &\qquad \cdot \sum_{m=1}^{\lfloor N^\eta \rfloor} \left(\frac{\sqrt{2\pi e}}{\sqrt{m}} \frac{\rho}{p} \left(1 + \frac{\sqrt{m}p}{2\rho} \right) \right)^m \qquad (27) \\ &= \binom{N}{\ell} |\mathbb{Z}^\ell \cap B_{\mathbf{y},\ell}(\rho)| O\left(N^{2N^\eta} \right) \end{aligned}$$

We can go back to (26) and deduce a bound for its general addendum with the help of Lemma 2 and Lemma 3:

$$\begin{aligned} \frac{M_\ell}{p^{J\ell(1-R_0)}} &\lesssim \frac{\binom{N}{\ell} |\mathbb{Z}^\ell \cap B_{\mathbf{y},\ell}(\rho)| O\left(N^{2N^\eta} \right)}{p^{J\ell(1-R_0)}} \\ &\leq \binom{N}{\ell} \frac{\mathrm{Vol}\left(B_{\mathbf{y},\ell}(\rho) \right)}{p^{J\ell(1-R_0)}} \left(1 + \frac{\sqrt{\ell}}{2\rho} \right)^\ell O\left(N^{2N^\eta} \right) \\ &\lesssim \left(\frac{e^{\frac{N}{\ell} H\left(\frac{\ell}{N}\right)}}{p^{J(1-R_0)}} \frac{\sqrt{2\pi e}\rho}{\sqrt{\ell}} \left(1 + \frac{\sqrt{\ell}}{2\rho} \right) \right)^\ell O\left(N^{2N^\eta} \right) \\ &\lesssim \left(e^{\frac{N}{\ell} H\left(\frac{\ell}{N}\right)} \sqrt{\frac{N}{\ell}} (1-\delta)(1+\varepsilon) \right)^\ell T(N), \end{aligned}$$

where the term

$$T(N) = \left(1 + \frac{O(1)}{N^{\lambda J(1-R_0)}} \right)^N O\left(N^{2N^\eta} \right) \qquad (28)$$

does not grow faster than sub-exponentially in N. Our aim is to show (21); given (26) and the previous asymptotic bound, (21) is true if we can show that

$$\left(e^{\frac{N}{\ell} H\left(\frac{\ell}{N}\right)} \sqrt{\frac{N}{\ell}} (1-\delta)(1+\varepsilon) \right)^\ell \qquad (29)$$

decreases to 0 exponentially fast in N for every $\Delta N \leq \ell \leq N$. It can be shown that

$$f\left(\frac{\ell}{N} \right) = e^{\frac{N}{\ell} H\left(\frac{\ell}{N}\right)} \sqrt{\frac{N}{\ell}} (1-\delta)(1+\varepsilon) \qquad (30)$$

is decreasing. Hence, $f\left(\frac{\ell}{N}\right) \leq f(\Delta) < 1$ by hypothesis (19), since we can take ε as small as wanted. This is enough to assure the exponential decrease of (29) and conclude. ■

Corollary 1: Consider the random ensemble described in Section V-A and suppose that $p \geq N^\lambda$ for some $\lambda > 0$. Suppose also that the minimum Hamming distance of the random GLD codes underlying the GLD lattices is lower bounded by ΔN for some Δ that approaches 1 asymptotically in N. As a result, this ensemble achieves Poltyrev capacity.

Proof: The proof comes directly from Theorem 2 since (19) is satisfied for every δ when Δ is close enough to 1. ■

VI. Conclusion

Motivated by some satisfactory numerical results, we have carried out a theoretical analysis of the decoding performance of the newborn family of GLD lattices. Firstly, we have generalized some results of non-binary GLD codes concerning their asymptotic goodness. Secondly, in Theorem 2, we have shown that a particular ensemble of GLD lattices can be reliably ML decoded for every channel noise variance up to a well defined distance to Poltyrev limit, which is described as a function of the minimum Hamming distance of the underlying GLD codes. Finally, Corollary 1 states the condition under those GLD lattice ensembles can achieve Poltyrev capacity.

Acknowledgment

The research work presented in this paper on GLD codes and lattices is supported by QNRF, a member of Qatar Foundation, under NPRP project 5-597-2-241.

References

[1] J.J. Boutros, N. di Pietro, and N. Basha, "Generalized low-density (GLD) lattices," *Proc. of the 2014 IEEE Inf. Theory Workshop*, pp. 15-19, Hobart, Nov. 2014.

[2] N. di Pietro, J.J. Boutros, and Y. C. Huang, "Spectral thinning in GLD lattices," *Proc. of the 2015 IEEE Inf. Theory and Applications Workshop*, Ja Jolla, Feb. 2015.

[3] O. Pothier, L. Brunel, and J.J. Boutros, "A low complexity FEC scheme based on the intersection of interleaved block codes," *IEEE Veh. Tech. Conf.*, vol. 1, pp. 274-278, Houston, May 1999.

[4] 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.

[5] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.

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

[7] W.W. Peterson and E.J. Weldon. *Error-Correcting Codes*. The MIT Press, 2nd edition, 1972.

[8] H.-A. Loeliger, "Averaging bounds for lattices and linear codes," *IEEE Trans. on Inf. Theory*, vol. 43, no. 6, pp. 1767-1773, Nov. 1997.

[9] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1+\mathrm{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Trans. on Inf. Theory*, vol. 50, no. 10, pp. 2293-2314, Oct. 2004.

[10] 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.

[11] O. Ordentlich and U. Erez, "A simpler proof for the existence of good pairs of nested lattices," 2012. Available at http://arxiv.org/abs/1209.5083.

[12] 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.

[13] N. di Pietro, G. Zémor, and J.J. Boutros "New results on Construction A lattices based on very sparse parity-check matrices," *Proc. of the 2013 IEEE Intern. Symp. on Inf. Theory (ISIT)*, pp. 1675-1679, July 2013.

[14] N. di Pietro, "On infinite and finite lattice constellations for the additive white gaussian noise channel," PhD thesis, Univ. Bordeaux, Jan. 2014.

[15] C. Ling and J.-C. Belfiore, "Achieving AWGN channel capacity with lattice Gaussian coding," *IEEE Trans. on Inf. Theory*, vol. 60, no. 10, pp. 5918-5929, Oct. 2014.

[16] J.H. Conway and N.J.A. Sloane. Sphere Packings, Lattices and Groups. Springer-Verlag, New York, 3rd edition, 1999.

[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.