New Bounds for GLD Lattices and Codes

Maiara F. Bollauf, Joseph J. Boutros, and Nordine Mir
Texas A&M University at Qatar
Education City, 23874 Doha, Qatar
Email: {maiara.bollauf, joseph.boutros, nordine.mir}@qatar.tamu.edu

***Abstract*—We prove that the ensemble of random Generalized Low-Density (GLD) lattices can attain the Poltyrev limit for an alphabet size increasing polylogarithmically with the lattice dimension. Our main theorem imposes no constraints on the normalized minimum distance of the code associated to the lattice ensemble, any asymptotically good code is suitable. This is a great improvement with respect to the first theorem on Poltyrev goodness of GLD lattices (2015). Our new bound is based on a new method referred to as the *buckets approach* where we employ the asymptotics of the restricted compositions of the Hamming weight. The new bound has applications in many coding areas beyond the specific lattice ensemble considered in this paper.**

I. Introduction

Error-correcting codes [12] [15] are special mathematical structures based on finite fields, while point lattices live in a Euclidean space [4]. Both codes and lattices play an important role in Information Theory, Computer Science, and many related areas. Lately in Mathematics, researchers showed that the densest sphere packings in $\mathbb{R}^8$ and $\mathbb{R}^{24}$ are lattice packings from the Gosset and the Leech lattices respectively [18] [3].

A more recent advance by di Pietro et al. and Vatedka et al. concerns capacity-achieving Low-Density Construction A (LDA) lattices which are built from non-binary LDPC codes (sparse codes [12]) via Construction A [4]. A new family of lattices, known as Generalized Low-Density (GLD) lattices, was introduced in 2014 following a similar construction in finite fields [1]. In 2015, the performance of GLD lattices at high signal-to-noise ratio (SNR) was studied to prove spectral thinning [2] and their Poltyrev goodness was proven in [6]. As stated by Erez and Zamir [9], Poltyrev goodness is a condition to attain channel capacity. It relates to the quality of an infinite lattice constellation that admits a vanishing error probability under closest-point decoding for a noise variance as close as possible to the highest limit established by Poltyrev [16].

In this paper, we describe a new method to analyze GLD codes and better take into account the embedded permutations. This method, called the *buckets approach*, is presented in Section III. It handles each component code $\mathcal{C}_0$ as a bucket randomly receiving apples (i.e. non-zero coordinates) from a point with a given Hamming weight. Section IV recalls three important results where the last lemma about integer points with coordinates in $p\mathbb{Z}$ is refined. Finally, by combining all previous results, Section V presents a new Poltyrev goodness theorem stronger that the previous theorem published in [6]. A brief overview of GLD lattices is provided in the next section. The positive integer p is a prime number throughout this paper.

II. An overview of GLD lattices

The key idea of a GLD construction is to improve a lattice, e.g. increase its Hermite constant, by making intersections of two or more sub-lattices. Moreover, in order to get low-complexity decoding algorithms and be able to analyze the structure, the intersecting lattices are made of the direct sum of a small-dimensional lattice $\Lambda_0 \subset \mathbb{R}^{n_0}$.

Definition 1. *(General GLD) A GLD lattice $\Lambda_{gld} \subset \mathbb{R}^n$ is defined by the intersection of J sub-lattices,*

$$\Lambda_{gld} = \bigcap_{i=1}^{J} \pi_i \left(\Lambda_0^{\oplus L}\right), \tag{1}$$

where $L = n/n_0$ and $\{\pi_i\}_{i=1}^J$ are random permutations (interleavers) uniformly selected from the symmetric group $\mathcal{S}_n$.

Definition 2. *(Construction-A GLD) Let $\Lambda_0 = \mathcal{C}_0[n_0, k_0]_p + p\mathbb{Z}^{n_0}$ be a real integer lattice built via Construction A from a code $\mathcal{C}_0$ of length n_0 and dimension k_0 defined over the prime field $\mathbb{F}_p$. The GLD lattice Λ_{gld} derived from Λ_0 is*

$$\Lambda_{gld} = \bigcap_{i=1}^{J} \pi_i \left(\mathcal{C}_0^{\oplus L}\right) + p\mathbb{Z}^n = \mathcal{C}_{gld} + p\mathbb{Z}^n. \tag{2}$$

Figure 1 depicts the parity-check matrix of a GLD code $\mathcal{C}_{gld} = \cap_{i=1}^{J} \pi_i \left(\mathcal{C}_0^{\oplus L}\right)$ with $J = 3$, π_1 is the identity, π_2 and π_3 are random. H_0 is the $(n_0 - k_0) \times n_0$ parity-check matrix of $\mathcal{C}_0$. The main structural difference of GLD codes compared to LDPC codes lies on the fact that each $[n_0, n_0 - 1, 2]_p$ check node of the latter is replaced by $[n_0, k_0, d_0]_p$ code in the former. In the special case when $k_0 = n_0 - 1$, LDA lattices [7] become a class of GLD lattices [1].

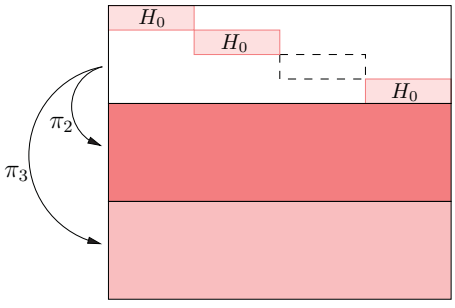

Fig. 1. Parity-check matrix of a GLD code with $J = 3$ direct sums.

The rate of a GLD code R is directly related to the rate $R_0 = k_0/n_0$ of the code $\mathcal{C}_0$ via $R = 1 - J(1 - R_0)$.

978-1-5386-6900-6/19/$31.00 ©2019 IEEE

The fundamental volume of a Construction A GLD lattice is calculated by

$$Vol(\Lambda_{gld}) = p^{n-k} = p^{n(1-R)}. \tag{3}$$

Poltyrev [16] introduced an alternative to analyze the performance of an infinite lattice constellation without a power constraint over the Gaussian channel, referred to as *Poltyrev capacity or limit*. Given the channel noise variance σ^2, there exists a sequence of n-dimensional lattices of constant volume V for which the probability of decoding error can be made as small as possible for a sufficiently large value of n, if and only if

$$\sigma^2 < \sigma^2_{\max} = \frac{V^{2/n}}{2\pi e}. \tag{4}$$

In the sequel, for $\delta > 0$, the noise variance will be related to the limit $\sigma^2_{\max}$ by

$$\sigma^2 = \sigma^2_{max}(1-\delta)^2 = \frac{p^{2(1-R)}}{2\pi e}(1-\delta)^2. \tag{5}$$

The 2015 theorem by di Pietro et al. [6] showing that GLD lattices are Poltyrev-capacity achieving is recalled below:

Theorem 1. *(GLD lattices achieving Poltyrev limit) Consider a random ensemble and suppose that $p = n^\lambda$ for some $\lambda > 0$. Admit that the minimum Hamming distance of the random GLD codes underlying GLD lattices is lower bounded by Δn, for some $0 < \Delta \leq 1$. Then for every $0 < \delta < 1$ such that*

$$f(\Delta) = \frac{e^{\frac{H(\Delta)}{\Delta}}}{\sqrt{\Delta}}(1-\delta) < 1, \tag{6}$$

where $\Delta = d_{H_{\min}}(\mathcal{C})/n$, a random lattice of the family can be decoded under maximum likelihood (ML) decoding with vanishing error probability for every channel noise variance $\sigma^2 = \sigma^2_{max}(1-\delta)^2$.

In practice, it is possible to see that there are a few choices for Δ, i.e., $\Delta > 0.98$ such that the inequality in (6) holds. Moreover, when $\delta \to 0$, it immediately follows that $\Delta \to 1$ and in conclusion, the only reasonable codes to be considered are repetition codes, which is very constraining and would make the construction of high-rate finite constellations fail.

In order to improve this drawback and to take better advantage of the GLD code structure that underlies the lattice construction (mainly the J permutations), we propose in the upcoming sections an innovative approach to the Poltyrev-achieving capacity GLD lattices.

III. The buckets approach for permutations

Consider n/n_0 shallow buckets each of capacity n_0 apples, $n_0 \geq 1$. The position of apples inside a bucket is taken into account. Imagine that ℓ apples are randomly thrown towards the n/n_0 buckets and no apples are falling outside, where $1 \leq \ell \leq n$. Assume that an apple falls in any of the buckets with equal probability. A bucket is said to be active if, after throwing the ℓ apples, it contains at least one apple.

Let B be the number of active buckets. B is a discrete random variable taking values in the range $[b_{\min}, b_{\max}]$, with $b_{\min} = \lceil \frac{\ell}{n_0} \rceil$ corresponds to $b-1$ buckets being 100% full. Obviously $b_{\max} = \min\{\frac{n}{n_0}, \ell\}$. In the ensemble of GLD codes considered in next sections, we shall have $b_{\max} = \frac{n}{n_0}$ because of the asymptotic goodness property $\ell > \frac{n}{n_0}$ proven in the last section of this paper. An illustration is given in Figure 2 for $\ell = 5$, $b = 2$ active buckets, and a total of $n/n_0 = 3$ buckets.

Our objective in this section is to determine $\mathcal{P}\{B = b\}$ after randomly throwing the ℓ apples into the n/n_0 buckets. For b active buckets, the integer ℓ can be written as the sum of b integers,

$$\ell = \sum_{i=1}^{b} \ell_i, \qquad \ell_i \in [1, n_0], \tag{7}$$

where ℓ_i is the number of apples in the ith active bucket. The sum in (7) is a restricted composition of the positive integer ℓ with a fixed number of parts, see Chapter 3 in [14] for more details on compositions.

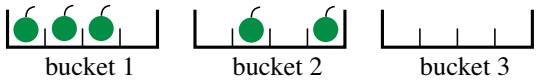

Fig. 2. One configuration of five apples in three shallow buckets. $\ell = 5$, $n_0 = 4$, $n/n_0 = 3$, and $b = 2$ active buckets.

• What is the number of restricted compositions given $B = b$? Let $f(t) = \sum_{j=1}^{n_0} t^j$ be the enumerator polynomial for one active bucket, i.e. t^k corresponds to k apples inside the bucket. Denote by $c(\ell, b, n, n_0)$ the number of restricted compositions of ℓ apples when $B = b$ for a total of n/n_0 buckets each containing up to n_0 apples. Since n and n_0 are well defined in the context of this paper, we drop them to simplify the notations and we write $c(\ell, b)$ for the number of restricted compositions.

At finite n and ℓ, $c(\ell, b)$ is given by [14] [8]

$$c(\ell, b) = [t^\ell]\,(f(t))^b = [t^\ell](t + t^2 + \ldots + t^{n_0})^b, \tag{8}$$

where the notation $[t^k]h(t)$ denotes the coefficient of t^k of the polynomial $h(t)$. The number of integer compositions of ℓ with b parts restricted to $[1, n_0]$ can be linked to ordinary binomial coefficients via a formula established in [11]. A more recent alternative proof is based on the application of Theorem 1 in [8] which yields

$$c(\ell, b) = \sum_{j=0}^{b} (-1)^j \binom{b}{j} \binom{\ell - jn_0 - 1}{b-1}. \tag{9}$$

The sum in (9) should be evaluated with $\binom{n}{k} = 0$ for $n \leq 0$. For example, for $n_0 = 4$, $c(5, 2) = 4$ because we can only write $5 = 1+4 = 4+1 = 2+3 = 3+2$, and $c(10, 3) = 6$ because $10 = 2+4+4 = 3+3+4$ and their permutations.

For asymptotic values $n \gg 1$ and $\ell \gg 1$, the number of restricted integer compositions of ℓ with b parts is determined

via the Daniels-Good theorem as proposed in [10] for computing the asymptotics of the entropy density function. Daniels-Good theorem was proved by I.J. Good in 1957 [13] with some improvement with respect to the previous version of H.E. Daniels [5]. In the sequel, we adapt the notation to our study to get the following lemma:

Lemma 1. *(Asymptotics of the Number of Restricted Compositions) Let $\ell \geq b \gg 1$. The number of compositions of ℓ with b parts where each part is restricted to $[1, n_0]$ is*

$$c(\ell, b) = \frac{f(t_0)^b}{t_0^\ell \sqrt{2\pi b \kappa_2(t_0)}} \times \left\{1 + O\left(\frac{1}{b}\right)\right\} \tag{10}$$

where $f(t) = \sum_{j=1}^{n_0} t^j$, $\kappa_2(t) = \frac{f''(t)}{f(t)} - \left(\frac{f'(t)}{f(t)}\right)^2 + \frac{f'(t)}{tf(t)}$, and t_0 is the unique non-negative real solution of the equation

$$tf'(t) = \frac{\ell}{b}\, f(t). \tag{11}$$

Proof: Let us apply Good's Theorem 6.1 [13] after checking that all its conditions are satisfied. From $b_{\min} = \lceil \frac{\ell}{n_0} \rceil$ and $b_{\max} = \min\{\frac{n}{n_0}, \ell\}$ we derive that the ratio $\frac{\ell}{b}$ is held inside the constant interval $[1, n_0]$. The convergence radius of $f(t)$ is infinity and all its coefficients are equal to 1. Thus, the main conditions of Good's theorem are all satisfied.

Now, define a new real variable

$$r = \frac{\ell}{b} \in [1, n_0]. \tag{12}$$

The parameter t_0 is solution of $tf'(t) = rf(t)$, or equivalently, it is root of the following equation,

$$\sum_{j=1}^{n_0} (j - r) t_0^{j-1} = 0. \tag{13}$$

Since the real r varies in the interval $[1, n_0]$, the coefficients of the polynomial in (13) make a unique change in sign, so (13) has a unique positive real root thanks to Descartes' rule of signs for $r > 1$, and $t_0 = 0$ for $r = 1$. The application of Theorem 6.1 from [13] gives (10). ∎

The variable $r = \ell/b$ shall be used in the next sections of this paper. From (11), we get an expression for r,

$$r = \frac{tf'(t)}{f(t)} = \frac{\sum_{j=1}^{n_0} j t^j}{\sum_{j=1}^{n_0} t^j}, \tag{14}$$

yielding $r = (n_0 + 1)/2$ if $t_0 = 1$, and

$$r = \frac{n_0 t_0^{n_0+1} - (n_0 + 1) t_0^{n_0} + 1}{(1 - t_0)(1 - t_0^{n_0})}, \quad \text{for } t_0 \neq 1. \tag{15}$$

To summarize how $c(\ell, b)$ behaves versus r: $r = 1$ corresponds to $t_0 = 0$ and $c(\ell, b) = 1$ (because $\ell = b$ has a unique restricted composition), $r \to n_0$ corresponds to $t_0 \to +\infty$ and $c(\ell, b) = 1$ (also, $\ell = bn_0$ has a unique restricted composition), and finally (10) gives $c(\ell, b)$ for $1 < r < n_0$.

• Now we are ready to determine $\mathcal{P}\{B = b\}$. Given the number of apples $\ell = \sum_{i=1}^{b} \ell_i$ and the number of active buckets b, there exist $\binom{n_0}{\ell_i}$ different configurations for the ith bucket. For b selected buckets, the total number of configurations becomes

$$\sum_{\{\ell_i\}: \sum_{i=1}^{b} \ell_i = \ell} \prod_{i=1}^{b} \binom{n_0}{\ell_i}, \tag{16}$$

where the above sum has $c(\ell, b)$ terms. The ℓ apples may fall into a total of $n_0 \times n/n_0 = n$ positions and b buckets should be selected among n/n_0, so we get

$$\mathcal{P}\{B = b\} = \frac{\binom{n/n_0}{b}}{\binom{n}{\ell}} \sum_{\substack{\{\ell_i\}: \\ \sum_{i=1}^{b} \ell_i = \ell}} \prod_{i=1}^{b} \binom{n_0}{\ell_i}, \tag{17}$$

for $b \in [b_{\min}, b_{\max}]$. Next, a bound on $\mathcal{P}\{B = b\}$ is derived.

Corollary 1. *(Upper Bound of the Probability of Active Buckets) The probability of b active buckets after throwing ℓ apples is bounded from above as*

$$\mathcal{P}\{B = b\} \leq \frac{\binom{n/n_0}{b}}{\binom{n}{\ell}} \times c(\ell, b) \times \min\{n_0^\ell, n_0^{bn_0 - \ell}\}. \tag{18}$$

Proof: The sum over the $\{\ell_i\}$ has $c(\ell, b)$ terms and the binomial coefficients satisfy $\binom{n_0}{\ell_i} \leq \min\{n_0^{\ell_i}, n_0^{n_0 - \ell_i}\}$. Then the announced bound is straightforward. ∎

Lemma 1 could be used for finite but large values of ℓ. For the main result of this paper at asymptotic dimensions, we only need to bound $c(\ell, b)$ from above in the expression of the probability $\mathcal{P}\{B = b\}$.

Proposition 1. *(Upper Bound for the Composition Factor) Consider the factor $c(\ell, b)^{1/\ell}$. According to Lemma 1 for $\ell \geq b \gg 1$, $c(\ell, b)^{1/\ell} \sim C(t_0, r)$ where*

$$C(t_0, r) = \frac{f(t_0)^{1/r}}{t_0}. \tag{19}$$

The composition factor satisfies $C(t_0, r) \leq 2$ for $1 \leq r \leq n_0$.

Proof: Recall that $c(\ell, b) = 1$ for $r = 1$ and $r = n_0$. Now consider $1 < r < n_0$. The sub-exponential terms in (10) are dropped when $\ell \gg 1$. To demonstrate that $C(t_0, r) = \frac{f(t_0)^{1/r}}{t_0} \leq 2$ it is equivalent to $C(t_0, r)^r \leq 2^r$. For a fixed r and a general $t > 0$, we have that

$$\frac{\partial C(t, r)^r}{\partial t} = \frac{tf'(t) - rf(t)}{t^{r+1}} = 0 \Leftrightarrow t = t_0, \tag{20}$$

from the hypothesis and the extreme point is unique. It still remains to show that t_0 is a global minimum. One can notice that

$$\lim_{t \to 0} \frac{\partial C(t, r)^r}{\partial t} = -\infty \quad \text{and} \quad \lim_{t \to +\infty} \frac{\partial C(t, r)^r}{\partial t} = +\infty. \tag{21}$$

Therefore, t_0 is a minimum of $C(t, r)^r$ and as a consequence, for all $t > 0$, $C(t_0, r)^r \leq C(t, r)^r$. Suppose the special choice of $t = \frac{1}{2}$, then $C\left(\frac{1}{2}, r\right)^r = f\left(\frac{1}{2}\right) \times 2^r \leq 2^r$ because $f\left(\frac{1}{2}\right) \leq 1$. and in particular, $C(t_0, r)^r \leq C\left(\frac{1}{2}, r\right)^r \leq 2^r$, as we wanted to prove. ∎

IV. Preliminary bounds and inequalities

This section collects three relevant results from the literature that are useful to describe our contributions and make this paper almost self-contained. However, Lemma 4 about integer points to be excluded is an improvement to similar results found in [6] [7]. The first lemma below shall define the radius of the decoding ball on a Gaussian channel.

Lemma 2. *[7, Lemma 1] (Typical Norm of the Gaussian 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 $\rho = \sqrt{X_1^2 + \cdots + X_n^2}$. Then, for every $\varepsilon > 0$:*

$$\lim_{n\to\infty} \mathcal{P}\left\{\rho \leq \sigma\sqrt{n}(1+\varepsilon)\right\} = 1. \tag{22}$$

The next result is about the number of $\mathbb{Z}^n$ points located inside a ball of radius ρ.

Lemma 3. *[7, Lemmas 2&3] (Number of Integer Points in an $n-$Dimensional Ball) Let $\mathcal{B}_{c,n}(\rho)$ denotes the $n-$dimensional ball centered at c of radius ρ. Then,*

$$|\mathbb{Z}^n \cap \mathcal{B}_{c,n}(\rho)| \leq \frac{1}{\sqrt{\pi n}} \left(\frac{\sqrt{2\pi e}\rho}{\sqrt{n}} \left(1 + \frac{\sqrt{n}}{2\rho}\right)\right)^n. \tag{23}$$

Consider an additive white Gaussian noise channel. Assume that the transmitted lattice point is the all-zero point. Then, the channel output is $y = \mathbf{0} + w \in \mathbb{R}^n$, where w is a Gaussian vector with i.i.d $\mathcal{N}(0, \sigma^2)$ components and σ^2 defined by (5). We define the decoding ball $\mathcal{B} = \mathcal{B}_{y,n}(\rho)$ as the n-dimensional ball centered on y with radius ρ. In the sequel, we take ρ as

$$\rho = \sigma\sqrt{n}(1+\varepsilon) = \frac{p^{J(1-R_0)}}{\sqrt{2\pi e}}\sqrt{n}(1-\delta)(1-\varepsilon). \tag{24}$$

As proved in [7], points belonging to $p\mathbb{Z}^n \setminus \{\mathbf{0}\}$ do not compete with the transmitted point $\mathbf{0}$ inside the decoding ball $\mathcal{B}$, i.e. $\mathcal{P}\{\|w - \mathbf{0}\|^2 \geq \|w - z\|^2\} \to 0$. Here, we make a similar proof but valid for any point in $\mathbb{Z}^n$ where one of its non-zero components is a multiple of p.

Lemma 4. *(Integer Points to be Excluded) Let $z = (z_1, \ldots, z_n) \in \mathbb{Z}^n$ such that $z_i \in p\mathbb{Z} \setminus \{0\}$ for some i. Then*

$$\lim_{n\to\infty} \mathcal{P}\{\|w\|^2 \geq \|w - z\|^2\} = 0. \tag{25}$$

Proof: Force to zero all components of z which are not multiple of p to get $\tilde{z} \in p\mathbb{Z}^n \setminus \{\mathbf{0}\}$. We have,

$$\mathcal{P}\{\|w\|^2 \geq \|w - z\|^2\} \leq \mathcal{P}\{\|w\|^2 \geq \|w - \tilde{z}\|^2\}. \tag{26}$$

Now, in a standard fashion [7, Eq. (28)], after using (5), the right term in the above inequality can be bounded from above by $2nQ\left(\frac{p}{2\sigma}\right) \leq 2n\exp\left(\frac{\pi e p^{2R}}{4(1-\delta)^2}\right)$, where $Q(x) \leq \exp(-x^2/2)$ is the Gaussian tail function. The upper bound decreases to 0 if $p = n^\lambda$ for $\lambda > 0$. ∎

Note that (25) is also true for $p = (\log n)^a$ if $2aR \geq 1$.

V. Improved bounds for GLD lattices

The GLD lattices ensemble considered in this section is similar to the ensemble of LDA lattices in [7] and GLD lattices in [6]. We follow the model Λ_{gld} of (2) where the J direct sums are randomly permuted with respect to each others. The instances of $\mathcal{C}_0$ in a direct sum are independent and randomly selected via their $(n_0 - k_0) \times n_0$ parity-check matrix H_0. In each instance, the entries of H_0 are random variables uniformly distributed in $\mathbb{F}_p$. Finally, the GLD lattices ensemble is a Construction A of the GLD codes ensemble.

Closest-point decoding is performed over an additive white Gaussian noise channel. This decoding is also referred to as Lattice Decoding in Information Theory, or Maximum-Likelihood (ML) Decoding in Communication Theory. Lemma 2 and ρ in (24) guarantee that the $\mathbf{0}$ transmitted point is inside the decoding ball $\mathcal{B}$. Lemma 4 tells us that, despite their presence or not inside $\mathcal{B}$, integer points with at least one component multiple of p do not induce any decoding error. A decoding error may occur if a non-zero point of $\mathbb{Z}^n$ inside $\mathcal{B}$ belongs to Λ_{gld}. Let $\mathcal{P}_e$ be the probability of error. Then, we have

$$\mathcal{P}_e \leq \sum_{x \in \mathbb{Z}^n \cap \mathcal{B}} \mathcal{P}\{x \in \Lambda_{gld}\}. \tag{27}$$

The summation in the above inequality should not consider integer points excluded by Lemma 4 (they have no incidence on decoding errors). The main result of this paper is to prove that $\mathcal{P}_e$ vanishes when $n \to \infty$ for any $\sigma^2 < \sigma^2_{\max}$ and p increasing with n, without any extra constraint on normalized minimum distance $\Delta > 0$. In [6], the technique consisted of expressing the bound of the error probability as $\sum_{\ell=\Delta n}^{n} F(\omega)^\ell$, where $\omega = \ell/n$, and to show that this upper bounding function goes to zero. Nevertheless, the special structure of the GLD code was not fully taken into account, so the key idea is to establish a new upper bound of the form $\sum_{\ell=\Delta n}^{n} [\sum_{b=b_{\min}}^{b_{\max}} F_p(\omega, r)^\ell]^J$, with $r = \frac{\ell}{b}$ defined in (12).

Theorem 2. *(GLD Lattices Achieve Poltyrev Limit with $a > 0$ and any $\Delta > 0$) Consider the random GLD lattices ensemble described previously. Suppose that $p = (\log n)^a$ for some exponent $a > \frac{1}{2R}$. Moreover, assume 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 $0 < \delta < 1$, 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: The proof is based on Corollary 1, Proposition 1, Lemma 3, and (27). We start by splitting the sum in (27) according to the Hamming weight $W(x)$ of $x \bmod p$. The total number of apples in all buckets shall be $\ell = W(x)$.

$$\mathcal{P}_e \leq \sum_{\ell=\lceil \Delta n \rceil}^{n} \sum_{\substack{x \in \mathbb{Z}^n \cap \mathcal{B}: \\ W(x) = \ell}} \mathcal{P}\{x \in \Lambda_{gld}\}. \tag{28}$$

From Definition 2, x is a lattice point if and only if $x \bmod p$ belongs to the GLD code, which is equivalent to $x \bmod p$

belonging to the J permuted direct sums $\mathcal{C}_0^{\oplus L}$. We obtain

$$\mathcal{P}\{x \in \Lambda_{gld}\} = (\mathcal{P}\{x \bmod p \in \mathcal{C}_0^{\oplus L}\})^J. \quad (29)$$

Now, we use the buckets approach to take into account the random permutations in the ensemble. Conditioning on b active buckets, i.e. b elementary codes $\mathcal{C}_0$ are receiving a non-zero weight, then $\mathcal{P}\{x \bmod p \in \mathcal{C}_0^{\oplus L}\} = (p^{-(n_0-k_0)})^b$. After summing over all values of b, where $b_{\min}$, $b_{\max}$, and $\mathcal{P}\{B=b\}$ depend on ℓ, we reach

$$\mathcal{P}\{x \bmod p \in \mathcal{C}_0^{\oplus L}\} = \sum_{b=b_{\min}}^{b_{\max}} \mathcal{P}\{B=b\} \left(\frac{1}{p^{(n_0-k_0)}}\right)^b \quad (30)$$

and combining (28), (29), with the above equation, it leads to

$$\mathcal{P}_e \leq \sum_{\ell=\lceil \Delta n \rceil}^{n} \sum_{\substack{x \in \mathbb{Z}^n \cap \mathcal{B}: \\ W(x)=\ell}} \left(\sum_{b=b_{\min}}^{b_{\max}} \frac{\mathcal{P}\{B=b\}}{p^{b(n_0-k_0)}} \right)^J$$

$$\leq \sum_{\ell=\lceil \Delta n \rceil}^{n} \binom{n}{\ell} |\mathbb{Z}^\ell \cap \mathcal{B}_{y,\ell}(\rho)| \left(\sum_{b=b_{\min}}^{b_{\max}} \frac{\mathcal{P}\{B=b\}}{p^{b(n_0-k_0)}} \right)^J. \quad (31)$$

We use Corollary 1 and Proposition 1 to bound $\mathcal{P}\{B=b\}$, and Lemma 3 to count integer points inside the ℓ-dimensional ball (due to $W(x)=\ell$). The binomial coefficients $\binom{n}{\ell}$ and $\binom{n/n_0}{b}$ are bounded via the famous inequalities from Lemma 7, Chapter 10 in [15]. After some algebraic manipulations and after dropping sub-exponential terms, the final bound becomes

$$\sum_{\ell=\Delta n}^{n} \left[\sum_{b=b_{\min}}^{b_{\max}} \left(\underbrace{\frac{e^{\frac{H(\omega n_0/r)}{\omega n_0}} C(t_0,r) \min\left\{n_0, n_0^{\frac{n_0}{r}-1}\right\}}{p^{(n_0-k_0)\left(\frac{1}{r}-\frac{1}{n_0}\right)} \omega^{\frac{1}{2J}} e^{\frac{H(\omega)}{\omega}\frac{J-1}{J}}} \kappa}_{F_p(\omega,r)} \right)^{\ell} \right]^J$$

where $\kappa = (1-\delta)(1-\varepsilon)$ and $\omega = \ell/n$. $F_p(\omega,r)$ is the fraction without the exponent ℓ and not including the κ factor. $F_1(\omega,r)$ shall denote $F_p(\omega,r)$ at $p=1$. In the trivial case $\omega=1$, $F_1(1,n_0)$ is 1: the bound of $\mathcal{P}_e$ includes $(1-\delta)$ inside κ which guarantees a vanishing $\mathcal{P}_e$ for any $\sigma^2 < \sigma^2_{\max}$ ($\delta > 0$).

For $\Delta \leq \omega < 1$, we claim that $F_1(\omega, n_0)$ is always less than 1. Indeed,

$$F_1(\omega,n_0) = \left[\sqrt{\omega} \exp\left(\frac{H(\omega)}{\omega} (J - 1 - \frac{J}{n_0}) \right) \right]^{-1/J}. \quad (32)$$

Except for $n_0 = 3$ ($J=2$ and $k_0=2$) where Δ should be greater than 0.16036, all other admissible values of the GLD code parameters (i.e. $R = 1 - J(1-R_0) > 0$) yield $F_1(\omega,n_0) < 1$ for any $\Delta > 0$. This condition allows to have $F_1(\omega,r) < 1$ in a range $r_c(\omega) < r \leq n_0$. Hence, $\mathcal{P}_e$ vanishes when $n \to \infty$ for r in this high range near n_0 and $\Delta \leq \omega < 1$.

For $r \leq r_c(\omega)$ and $\Delta \leq \omega < 1$, we use the fact that $F_1(\omega,r)$ is bounded from above by a constant. The reader may easily check that $F_1(\omega,r) \leq \exp(\frac{1}{\Delta n_0}) \times 2 \times n_0/\Delta^{1/2J}$. In this case, the increasing p in the denominator and $\ell \to \infty$ will push $\mathcal{P}_e$ towards 0. An alphabet size p increasing polylogarithmically in n can do the job by forcing $F_p(\omega,r)$ to be less than 1. ■

VI. Conclusions

GLD lattices built via Construction A over the ring $\mathbb{Z}$ with p-ary GLD codes are considered in this paper. We present an innovative method to compute the probability of active elementary codes within the GLD code. The buckets approach utilizes restricted compositions of an integer to find the distribution of active elementary codes. Asymptotics are found via the Daniels-Good theorem. The new upper bound on the probability of error of a GLD lattice ensemble is established in the proof of Theorem 2. Besides the gain at high weight due to J (number of intersecting direct sums), our new bound includes a power of the alphabet size allowing the ensemble to attain Poltyrev capacity with a polylogarithmic growth. The new theorem corresponds to reasonable values of the normalized minimum distance Δ for practical applications. Extensions of this buckets approach to other cases in Coding and Information Theory are very promising.

Acknowledgment

The authors would like to thank Texas A&M University at Qatar and Qatar Foundation for the Responsive Research Seed Grant 2018-2019, which funded the current work.

References

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

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

[3] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko, and M. Viazovska, "The sphere packing problem in dimension 24," *Ann. Math*, vol. 185, no. 3, pp. 1017-1033, Apr. 2017.

[4] J. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. 3rd ed., New York (NY), USA: Springer-Verlag, 1999.

[5] H.E. Daniels, "Saddle-point approximations in statistics," *Annals of Mathematical Statistics*, vol. 25, no. 4, pp. 631-650, Dec. 1954.

[6] N. di Pietro, N. Basha, and J.J. Boutros, "Non-Binary GLD Codes and their Lattices," *Proc. of the 2015 IEEE Information Theory Workshop*, Jerusalem, Israel, Apr. 2015.

[7] N. di Pietro, G. Zémor, and J.J. Boutros, "LDA lattices without dithering achieve capacity on the Gaussian channel," *IEEE Trans. on Inf. Theory*, vol. 64, no. 3, pp. 1561-1594, Mar. 2018.

[8] S. Eger, "Restricted weighted integer compositions and extended binomial coefficients," *Journal of Integer Sequences*, vol. 16, pp. 1-25, Jan. 2013.

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

[10] N.E. Fahssi, "Polynomial Triangles Revisited," arXiv:1202.0228 [math.CO], Jul. 2012.

[11] D.C. Fielder and C.O. Alford, *Pascal's triangle: top gun or just one of the gang?*, in G. E. Bergum, A. N. Philippou, and A. F. Horadam, eds., Applications of Fibonacci Numbers, Kluwer, pp. 77-90, 1991.

[12] R.G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.

[13] I.J. Good, "Saddle-point methods for the multinomial distribution," *The Annals of Statistics*, vol. 28, no. 4, pp. 861-881, Dec. 1957.

[14] S. Heubach and T. Mansour, *Combinatorics of Compositions and Words*. Boca Raton, FL: CRC Press, 2009.

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

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

[17] S. Vatedka and N. Kashyap, "Some goodness properties of LDA lattices," *Problems of Information Transmission*, vol. 53, no. 1, pp. 1-29, Jan. 2017.

[18] M. Viazovska, "The sphere packing problem in dimension 8," *Ann. Math*, vol. 185, no. 3, pp. 991-1015, Apr. 2017.