Spectral Thinning in GLD Lattices

Joseph J. Boutros
ECE Department
Texas A&M University at Qatar
Education City, 23874 Doha, Qatar
boutros@ieee.org

Nicola di Pietro
ECE Department
Texas A&M University at Qatar
Education City, 23874 Doha, Qatar
nicola.dipietro@qatar.tamu.edu

Yu-Chih Huang
ECE Department
Texas A&M University
College Station, TX 7784-3128, USA
cyeekk51@tamu.edu

***Abstract*—This paper deals with generalized low-density (GLD) lattices which have been recently shown to be an excellent family of lattices for communication over the Gaussian channel. Under iterative decoding, numerical results for GLD lattices show an error rate per lattice coordinate extremely close to Poltyrev theoretical limit of an infinite constellation. These results are found for GLD ensembles with degree-2 variable nodes. In the error floor region, the probability of error per lattice coordinate decreases when the lattice dimension grows. This phenomenon is similar to spectral thinning in parallel concatenated convolutional codes (Turbo codes) also known as interleaving gain. The present work aims to give the theoretical explanation of this error floor decay as a function of the lattice dimension. Namely, we show how spectral thinning applies to codes on graphs associated with GLD lattices. This stands on the proof that the number of cycles of small length in random bipartite graphs follows a Poisson distribution. Our theorem on cycles is an adaptation of a theorem by Béla Bollobás to irregular bipartite graphs.**

I. Introduction

Random graphs theory [1] is nowadays used in many areas in science and engineering. In coding theory [2], graph representation of error-correcting codes started its golden era with the pioneering work by Tanner [3]. Graph theory also played an important role in Euclidean codes, mainly in point lattices [4]. The recent family of generalized low-density lattices [5] [6] has a simple graph structure that allows decoding in high dimensions (e.g. 10^6). The GLD graph is suitable for applying iterative belief propagation (BP) decoding [7] to decode lattice points over an additive white Gaussian noise (AWGN) channel. It is also suitable to make a theoretical analysis under the assumption of maximum-likelihood (ML) decoding.

Codes on graphs have a special behavior at finite length. An extensive finite-length study for low-density parity-check codes (LDPC) and turbo codes can be found in [7]. In general, for turbo-like and LDPC-like codes, the error rate performance plot can be divided into two regions: a waterfall region which is due to large decoding failures and an error floor region which is due to small failures. For example, some of the first analyses of the ML performance of turbo codes concluded that the bit error rate decreases as $1/n$ in the error floor region for a turbo interleaver of size n. This $1/n$ enhancement factor in the bit error rate was referred to as *interleaving gain* [11] or *spectral thinning* [12]. See Lemma 6.52 on page 358 in [7] for more details about the error floor of turbo codes under ML decoding. Similarly, LDPC codes exhibit a $1/n$ spectral thinning behavior under ML decoding over the AWGN channel with binary input (BI-AWGN). See Lemma 4.177 on page 258 in [7]. Unfortunately, little is known about the error floor scaling under BP decoding over the BI-AWGN channel. The BP error floor is higher than the ML error floor for LDPC codes because of the presence of pseudo-codewords. For turbo codes, BP decoding performs very close to ML decoding. Hence, the BP error floor shows a $1/n$ spectral thinning as predicted by the ML analysis.

In all codes on graphs, the error floor small failures are produced by short-length cycles. The code graph has variables nodes that represent code symbols and check nodes that represent the code constraints. Under ML decoding, we are interested in codewords whose supports are cycles. As proved by Bollobás [9] for non-bipartite graphs, dominant configurations are those without shackles, i.e. it is enough to consider primitive cycles [7]. Consequently, variable nodes with degree 3 or higher should be excluded from these graph configurations. In LDPC codes, only degree-2 bit nodes are considered. Degree-2 bit nodes can be replaced by simple edges, which leads to a non-bipartite check-node-only graph. In standard turbo codes, all bit nodes have degree 2.

When analyzing cycles, variables nodes with degree 3 or higher should also be excluded from GLD graph configurations. We will see in the next section that a GLD ensemble with degree-2 variable nodes shall give rise to a bipartite check-node-only graph. This situation does not occur in LDPC-like and turbo-like codes. Thus, GLD ensembles require the generalization of known results for non-bipartite graphs to bipartite graph configurations.

The analysis of GLD lattices on the AWGN channel is not as simple as analyzing BP decoding of LDPC codes on the binary erasure channel. Thus, after presenting GLD lattices in Section II, their spectral thinning is defined under ML decoding in Section III. In Section IV we generalize Bollabás theorem [9] to bipartite graphs with irregular left and right degree distributions. At asymptotic dimension n, for GLD ensembles with an elementary lattice of minimum Hamming weight 2, our theorem states that the GLD bipartite graph has Poisson distributed cycles up to a length that does not exceed $\log n$. The Poisson parameter is given as a function of the left and right degree distributions. Section V includes computer simulation results in dimensions 10^3, 10^4, 10^5, and 10^6. They reveal a spectral thinning behavior where the error rate per lattice coordinate is inversely proportional to the lattice dimension at high signal-to-noise ratio. Spectral thinning in GLD lattices is observed despite iterative BP decoding.

In this paper, we assume that the reader has enough familiarity with lattices as algebraic structures and as infinite constellations for the digital transmission of information over the AWGN channel. In case of need, the reader should refer to textbooks [4] and [8].

II. GLD Lattices and their Graphs

In this section we recall the definition of *Generalized Low-Density (GLD)* lattices and their graphical representation. GLD lattices were proposed for the first time in [5] and are the transposition to the real Euclidean space $\mathbb{R}^n$ of GLD codes [13], [14] defined over finite fields. Their capability of achieving Poltyrev limit [15], with asymptotically vanishing maximum likelihood decoding error probability of an infinite constellation, was shown in [6]. We give below two definitions for GLD lattices.

Definition 1: Let $\Lambda_1, \ldots, \Lambda_J \subseteq \mathbb{R}^n$ be J real lattices of rank n in $\mathbb{R}^n$. A *Generalized Low-Density (GLD)* lattice is defined as [5] [6]

$$\Lambda = \bigcap_{j=1}^{J} \Lambda_j. \tag{1}$$

A GLD lattice coordinate belongs to J component lattices, i.e. it has degree J in the graph representation. Then, the integer J is referred to as the *degree* of variable nodes. In practice, we usually consider component lattices with a sparse graph representation. The second definition restricts the GLD family to a sub-family built from an elementary lattice Λ_0 by taking $\Lambda_j = \pi_j(\Lambda_0^{\oplus L})$ where $\Lambda_0^{\oplus L}$ is the direct sum of L copies of the elementary lattice.

Definition 2: Let $\Lambda_0 \subseteq \mathbb{R}^{n_0}$ be a lattice of small dimension n_0, let L be a natural number, and let us call $n = n_0 L$. Given J permutations $\pi_1 = \mathrm{id}, \pi_2, \ldots, \pi_J$ of $\{1, 2, \ldots, n\}$, a *Generalized Low-Density (GLD)* lattice is defined as [5] [6]

$$\Lambda = \bigcap_{j=1}^{J} \pi_j \left(\Lambda_0^{\oplus L}\right) \subseteq \mathbb{R}^n, \tag{2}$$

where $\pi_j(x_1, x_2, \ldots, x_n) = \left(x_{\pi_j(1)}, x_{\pi_j(2)}, \ldots, x_{\pi_j(n)}\right)$.

In the sequel, we use this second definition for GLD lattices. As mentioned in the previous section, degree-2 variable nodes are the only variable nodes involved in the analysis of short cycles. From this point, we study the special case $J = 2$. We write $\pi_2 = \pi$ so we have the following simple expression for a GLD lattice

$$\Lambda = \Lambda_0^{\oplus L} \bigcap \pi(\Lambda_0^{\oplus L}). \tag{3}$$

In GLD ensembles studied in this paper, we consider Λ_0 built from a non-binary Construction A,

$$\Lambda_0 = C_0[n_0, k_0]_p + p\mathbb{Z}^{n_0}, \tag{4}$$

where p is a prime number, C_0 is a linear code of length n_0 and dimension k_0 defined over the finite field $\mathbb{F}_p$. C_0 is called the elementary code. Here, we assumed an injective mapping from $\mathbb{F}_p$ into $\mathbb{Z}$ that assigns elements of $\mathbb{F}_p$ to elements of the integer set $\{-\frac{p-1}{2}, \ldots, -1, 0, +1, \ldots, +\frac{p-1}{2}\}$. The expression $\Lambda_0 = C_0 + p\mathbb{Z}^{n_0}$ is an abuse of notation where C_0 is the real image of the code defined over the field $\mathbb{F}_p$. The combination of (3) and (4) gives

$$\Lambda = C_0^{\oplus L} \bigcap \pi(C_0^{\oplus L}) + p\mathbb{Z}^n = C_{\mathrm{GLD}} + p\mathbb{Z}^n, \tag{5}$$

where C_{GLD} is a linear GLD code [13] [14].

The GLD graph representation uses a standard notation from coding theory as illustrated in Figure 1. A lattice coordinate, known as a variable node, is represented by a circle. The local constraint given by the elementary lattice Λ_0 is drawn as a square and is called a check node. An edge connects a variable node to a check node if x_i is the coordinate of a point that belongs to Λ_0. In that case, the point modulo p is a codeword of C_0. Hence, it is equivalent to refer to the check node by the notation C_0.

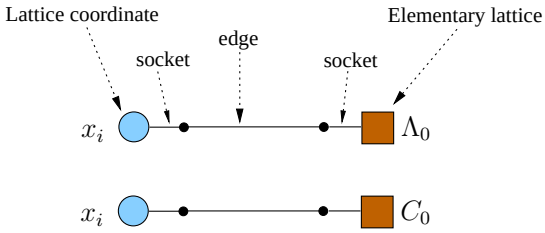

Figure 1. Notation for GLD graphs. The variable node x_i connects to a check node C_0 when it is a coordinate of a point of Λ_0.

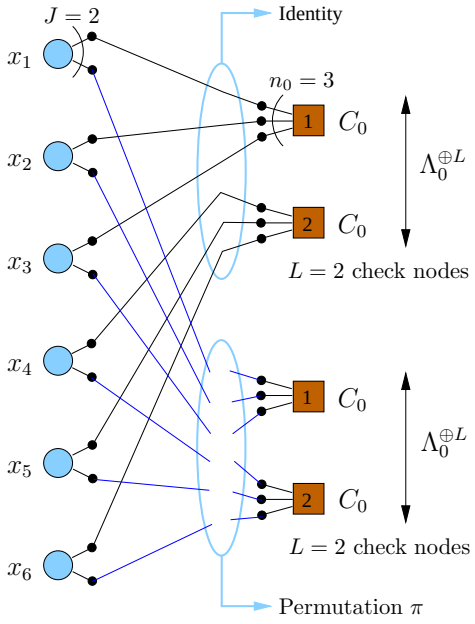

Figure 2. Tanner graph representation of a GLD ensemble including variable nodes of degree $J = 2$ and check nodes of degree n_0. Direct sum length is $L = 2$. The elementary code C_0 has parameters $[n_0 = 3, k_0]_p$ and $\Lambda_0 = C_0 + p\mathbb{Z}^n$. The GLD lattice dimension is $n = n_0 L = 6$.

An example in dimension $n = 6$ is shown in Figure 2. It represents a GLD lattice as defined by (3). Parameters are $n_0 = 3$ and $L = 2$. Notice how this GLD ensemble is different from an LDPC ensemble [7]. In our case, the matching between left sockets and right sockets involves a random permutation of size n, while an LDPC ensemble with the same degree distribution has a random permutation of size $2n$. Also, in the GLD ensembles, we have two classes of check nodes because Λ is the intersection of two direct sums. The first class of check nodes is connected to all variable nodes via an identity matching as shown in Figure 2. Now, since all variable nodes have degree 2, they can be dropped and implicitly included in the edge connecting a check node from the first class to a check

node in the second class. Consequently, a bipartite check-node-only graph for GLD ensembles can be constructed. It includes L check nodes on each side as depicted in Figure 3.

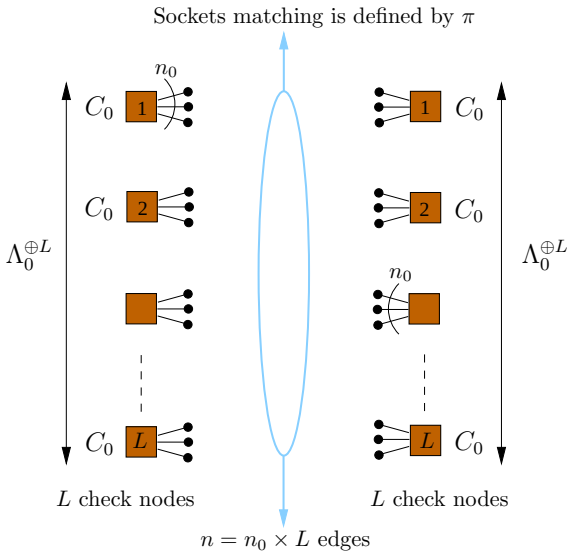

Figure 3. Bipartite graph representation of a GLD ensemble including check nodes only, valid for $J = 2$. The GLD ensemble has a total of $2L$ check nodes. Lattice coordinates are associated to the edges.

III. Spectral Thinning under ML decoding

There exist no tools for the theoretical analysis of iterative BP decoding in the non-binary case, as for non-binary LDPC codes. It is even more difficult to consider iterative BP decoding of a lattice with integer or real coordinates. The analysis in this section assumes ML decoding of a lattice on the AWGN channel. Nevertheless, the predicted $1/n$ ML spectral thinning is also observed under BP decoding of GLD lattices as revealed in Section V. In the following, $G(\Lambda)$ is the bipartite check-node-only graph of Λ as described in the previous section.

Definition 3: Let $\mathbf{x} \in \Lambda$ be a non-zero lattice point. The *graphical support* of $\mathbf{x}$, denoted $\mathrm{Supp}(\mathbf{x})$, is the set of edges of $G(\Lambda)$ assigned to non-zero variable nodes x_i.

The above definition is directly related to C_{GLD} in (5). Indeed, $|\mathrm{Supp}(\mathbf{x} \bmod p)| = \omega$ is the Hamming weight of the corresponding codeword in C_{GLD}. For a fixed GLD lattice Λ, let $\Theta_\Lambda(z)$ be the theta series of Λ as defined in [4] ($q = e^{i\pi z}$),

$$\Theta_\Lambda(z) = \sum_{\mathbf{x}\in\Lambda} q^{\|\mathbf{x}\|^2} = \sum_{d\geq 0} \tau(d) q^{d^2}, \tag{6}$$

where $\tau(d)$ is the number of lattice points located at Euclidean distance d from the origin. On the additive white Gaussian noise channel with noise variance σ^2, a union bound on the point error probability P_e is derived from the theta series [16]:

$$P_e \leq \sum_{\mathbf{x}\in\Lambda\setminus\{\mathbf{0}\}} Q\left(\frac{\|\mathbf{x}\|}{2\sigma}\right) \leq (\Theta_\Lambda(z) - 1), \tag{7}$$

where $q = e^{-d^2/(2\sigma^2)}$. For infinite GLD lattice constellations, signal-to-noise ratio is defined by the ratio $\mathrm{Vol}(\Lambda)^{2/N}/\sigma^2 = p^{2(1-R_{\mathrm{GLD}})}/\sigma^2$ [5] since average energy per point is infinite.

Upper bound (7) is useful when the theta series of Λ can be determined. The method for estimating $\Theta_\Lambda(z)$ or at least get an expression of its expected value over the GLD ensemble is not known yet, especially in high dimensions. In the following, we suggest to modify the upper bound on P_e in order to decouple the effect of C_{GLD} from the influence of $p\mathbb{Z}^n$. Consider a lattice point $\mathbf{x} = \mathbf{c} + p\mathbf{z}$, where $\mathbf{c} = (c_1, \ldots, c_n) \in C_{\mathrm{GLD}}$ and $\mathbf{z} = (z_1, \ldots, z_n) \in \mathbb{Z}^n$, see (5). Denote by $w_H(c_i)$ the Hamming weight of c_i. The squared norm of $\mathbf{x}$ is lower-bounded as

$$\begin{aligned}
\|\mathbf{x}\|^2 &= \sum_{i=1}^{n} (c_i + z_i p)^2 \\
&= \sum_{i=1}^{n} \left[c_i^2 + z_i^2 p^2 + 2 c_i z_i p\right] \\
&\geq \sum_{i=1}^{n} \left[w_H(c_i) + z_i^2 p^2 - p(p-1)|z_i|\right] \\
&= \omega + p^2\|\mathbf{z}\|^2 - p(p-1)\|\mathbf{z}\|_1,
\end{aligned} \tag{8}$$

where $\omega = w_H(\mathbf{c}) = |\mathrm{Supp}(\mathbf{x} \bmod p)|$, $\|\mathbf{z}\|^2 = \sum_{i=1}^n z_i^2$, and $\|\mathbf{z}\|_1 = \sum_{i=1}^n |z_i|$. The number of edges in $G(\Lambda)$ associated to non-zero symbols in $\mathbf{c}$ is ω. Given (7) and (8), and the well-known inequality $Q(x) \leq \exp(-x^2/2)$ [16], the union bound on the error probability per lattice coordinate becomes

$$\begin{aligned}
P_{es} &\leq \sum_{\mathbf{x}\in\Lambda\setminus\{\mathbf{0}\}} \frac{|\mathrm{Supp}(\mathbf{x})|}{n} Q\left(\frac{\|\mathbf{x}\|}{2\sigma}\right) \\
&\leq \sum_{(\omega,\mathbf{z})\neq(0,\mathbf{0})} \frac{|\mathrm{Supp}(\mathbf{x})|}{n} e^{-\left(\omega + p^2\|\mathbf{z}\|^2 - p(p-1)\|\mathbf{z}\|_1\right)/8\sigma^2} \\
&\leq A + B + A_0 B.
\end{aligned} \tag{9}$$

The contribution of the cubic lattice $p\mathbb{Z}^n$ to errors is given by

$$B = \sum_{\mathbf{z}\in\mathbb{Z}^n\setminus\{\mathbf{0}\}} \exp\left(\frac{-p^2\|\mathbf{z}\|^2 + p(p-1)\|\mathbf{z}\|_1}{8\sigma^2}\right). \tag{10}$$

The contribution of the linear code C_{GLD} to errors is given by

$$A = \sum_{\omega=\omega_{\min}}^{n} \frac{\omega}{n} \tau(\omega) \exp\left(-\frac{\omega}{8\sigma^2}\right). \tag{11}$$

$\tau(\omega)$ is the number of codewords of weight ω. Notice that we used $|\mathrm{Supp}(\mathbf{x})| \leq w + w_H(\mathbf{z})$ and $w_H(\mathbf{z}) \leq n$. Finally,

$$A_0 = \sum_{\omega=\omega_{\min}}^{n} \tau(\omega) \exp\left(-\frac{\omega}{8\sigma^2}\right). \tag{12}$$

Now the actions of C_{GLD} and $p\mathbb{Z}^n$ being decoupled, we use (9) for a noise variance far enough from Poltyrev limit (in the error floor region), where $\sigma^2 < p^{2(1-R_{\mathrm{GLD}})}/(2\pi e)$ [15]. We prove below that the mean error term $\mathbb{E}[A]$ decreases as $1/n$ when the elementary code C_0 has minimum Hamming weight $d_{H\min}(C_0) = 2$ and the GLD ensemble has $J = 2$ edges per variable node. We also show that $B = o(\mathbb{E}[A])$. For a well chosen p, thanks to the decoupling, we are able to study cycles in $G(\Lambda)$ without the interference of the graphical support of points from $p\mathbb{Z}^n$. The spectral thinning does not appear in GLD ensembles if $d_{H\min}(C_0) \geq 3$ or $J \geq 3$.

Theorem 1: Consider a GLD ensemble with lattice instances $\Lambda = C_0^{\oplus L} \bigcap \pi(C_0^{\oplus L}) + p\mathbb{Z}^n = C_{\rm GLD} + p\mathbb{Z}^n$. Assume the elementary code C_0 has minimum Hamming weight 2. Let $p = \beta \log n$, where $\beta > \max\{1, 16\sigma^2\}$. For σ^2 small enough, we have

$$n\mathbb{E}[P_{es}] = O\left(1\right) \quad \text{for } n \gg 1, \tag{13}$$

i.e. the expected error probability per lattice coordinate decreases as $1/n$ at high signal-to-noise ratio. Expectation is made over all permutations π of the GLD ensemble.

Proof: Notation is simplified by dropping the floor function when converting reals into integers, e.g. $\omega = \lfloor \log n \rfloor$ is written $\omega = \log n$. We start the proof by developing A given in (11). For some ε small enough, let $\omega_{\max} = (\log n)^{1-\varepsilon}$ be the maximum cycle length to which applies Theorem 2 of Section IV. Again, to make the proof more readable, we drop the ε in the sequel.

The summation is cut into two parts, $A = A_1 + A_2$, where

$$A_1 = \sum_{\omega=\omega_{\min}}^{\omega_{\max}} \frac{\omega}{n} \tau(\omega) \exp\left(-\frac{\omega}{8\sigma^2}\right). \tag{14}$$

$\omega_{\min} = 4$ because graphs with length-2 cycles are expurgated from the ensemble, i.e. cycles in $G(\Lambda)$ have length greater than or equal to 4. A_1 includes low-weight codewords of $C_{\rm GLD}$ which are given by short cycles, all of even length. Let $\mathcal{C}_k$ be the set of all cycles in $G(\Lambda)$ of length k. $|\mathcal{C}_k| = X_k$ (same notation as in Section IV). Denote by $\mathcal{S}$ the power set of the set of cycles $\mathcal{C}_k$, for $k = \omega_{\min}, \ldots, \omega_{\max}$,

$$\mathcal{S} = 2^{\{\mathcal{C}_4, \mathcal{C}_6, \ldots, \mathcal{C}_{\log n}\}}.$$

Low-weight codewords counted in A_1 are given by the following set

$$\mathcal{C} = \{\mathbf{c} \in \mathcal{S} : |\operatorname{Supp}(\mathbf{c})| \leq \omega_{\max}\}.$$

For example, weight-10 codewords in $\mathcal{C}$ are built by union of many cycles such that the final graphical support in $G(\Lambda)$ has 10 edges. The number of weight-10 codewords is

$$\tau(10) = X_{10} + X_4 X_6.$$

Of course, there are many other partitions of 10 such as $10 = 5 + 5$. But partitions with odd integers and those involving 2 are not counted in $\mathcal{C}$, which is equivalent to $X_2 = 0$ and $X_k = 0$ for odd weight k. Let $\mathcal{P}(\omega)$ be the set of all partitions of the integer ω. For any ω in the range $[\omega_{\min}, \omega_{\max}]$, we have

$$\tau(\omega) = \sum_{\{k_i\} \in \mathcal{P}(\omega)} \prod_i X_{k_i}. \tag{15}$$

From Theorem 2 in Section IV, we know that the X_k are independent and Poisson distributed with mean $\mathbb{E}[X_k] = \lambda_k$ given by (32). In the simple regular GLD ensemble defined in the previous section, we have

$$\lambda_k = \frac{(n_0 - 1)^k}{k}. \tag{16}$$

Hence, we get

$$\mathbb{E}[\tau(\omega)] = \sum_{\{k_i\} \in \mathcal{P}(\omega)} \prod_i \lambda_{k_i} \leq \eta(\omega/2)\lambda_\omega, \tag{17}$$

where $\eta(\omega)$ is the Hardy-Ramanujan-Rodemacher partition function [17]. From (14) and (17), the expected value of A_1 over all permutations defining the GLD ensemble satisfies

$$n\mathbb{E}[A_1] \leq \sum_{\omega=4}^{\log n} \omega \eta(\omega/2) \lambda_\omega \exp\left(-\frac{\omega}{8\sigma^2}\right). \tag{18}$$

Let us show that the right term series in (18) converges. At large ω, the partition function behaves like [17]

$$\eta(\omega) \sim \frac{1}{4\omega\sqrt{3}} \exp\left(\pi\sqrt{\frac{2w}{3}}\right). \tag{19}$$

The general term of the series decreases like

$$\exp\left(\sqrt{\omega}\right) \exp\left[-\omega\left(\frac{1}{8\sigma^2} - \log(n_0 - 1)\right)\right].$$

We conclude that, for $\sigma^2 < 1/8\log(n_0 - 1)$, we have

$$n\mathbb{E}[A_1] = O(1). \tag{20}$$

Our second step in this proof is to show that $n\mathbb{E}[A_2] = O(1)$.

$$\mathbb{E}[A_2] = \sum_{\omega=\log n}^{n} \frac{\omega}{n} \mathbb{E}[\tau(\omega)] \exp\left(-\frac{\omega}{8\sigma^2}\right). \tag{21}$$

The expected number of codewords $\mathbb{E}[\tau(\omega)]$ cannot be determined via (17) because Theorem 2 is valid up to $\omega_{\max} = (\log n)^{1-\varepsilon}$ only. We may be tempted to assume a binomial weight distribution [18] [19] by taking the expected value to be $\mathbb{E}[\tau(\omega)] = \binom{n}{\omega}(p-1)^\omega / p^{n-k}$. Unfortunately, $\log n$ is not sufficient to have the weight distribution well approximated by a binomial. We will proceed by upper-bounding without any approximation.

Let $g(s)$ be the moment generating function of the elementary code C_0,

$$g(s) = \frac{1 + a_2 e^{2s} + \ldots + a_{n_0} e^{n_0 s}}{p^{k_0}}. \tag{22}$$

In a way similar to [13] [14], the average weight distribution for a non-binary GLD code satisfies [6]:

$$\mathbb{E}[\tau(\omega)] \leq \frac{\left(p^{k_0} g(s)\right)^{2L} e^{-2\omega s}}{\binom{n}{\omega}(p-1)^\omega}. \tag{23}$$

We obtain

$$\mathbb{E}[A_2] \leq \sum_{\omega=\log n}^{n} \frac{\omega}{n} \frac{\left(p^{k_0} g(s)\right)^{2L} e^{-2\omega s}}{\binom{n}{\omega}(p-1)^\omega} \exp\left(-\frac{\omega}{8\sigma^2}\right). \tag{24}$$

The right term of the above inequality is analyzed in three different intervals for ω.

1) The weight ω is in $[\log n, \beta_1 \log n]$, for some real $\beta_1 \geq 1$. Indeed, for $\omega/n \ll 1$, we fix $s = -\frac{1}{2}\log n$ so $\left(p^{k_0} g(s)\right)^{2L}$ converges to e^{2a_2/n_0}. The term in the summation in (24) behaves like

$$\frac{\omega}{n} \exp\left(\omega \log\left(\frac{\omega}{p-1}\right) - \frac{\omega}{8\sigma^2}\right).$$

Then $\log n \leq \omega \leq p-1$ guarantees that $\mathbb{E}[A_2]$ vanishes with n. The alphabet size is taken to be $p = \beta_1 \log n + 1$. At $\omega = \log n$, the summation term in (24) is $O(1/n^{1+\log\beta_1 + 1/8\sigma^2})$.

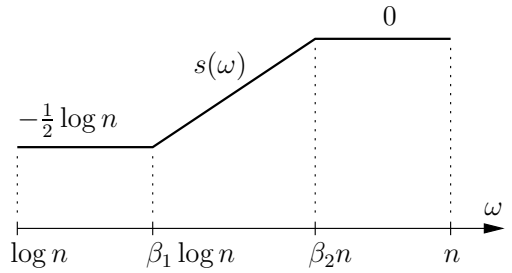

Figure 4. Illustrative sketch for a choice of the function $s(\omega)$ that guarantees convergence for high-weight codewords, i.e. $n\mathbb{E}[A_2] = O(1)$.

2) The weight ω is in $[\beta_2 n, n]$, for some real $\beta_2 \leq 1$. For $s = 0$, at $\omega = \beta_2 \log n$, the summation term in (24) behaves like

$$\exp\left(n\left[\frac{2k_0}{n_0}\log p - \beta_2 \log(p-1) - \frac{\beta_2}{8\sigma^2}\right]\right).$$

The signal-to-noise ratio should satisfy

$$\frac{1}{8\sigma^2} > \frac{2k_0/n_0}{\beta_2}\log p - \log(p-1)$$

to make $\mathbb{E}[A_2]$ vanish. This inequality is valid in the whole range $[\beta_2 n, n]$. It also requires that $1/\sigma^2$ increases as $\log\log n$. When the difference between the two sides of the inequality is $\log(n)/n$ then we get $n\mathbb{E}[A_2] = O(1)$.
3) In this third case, we have $\omega \in [\beta_1 \log n, \beta_2 n]$. As illustrated in Figure 4, a linear function from $-\frac{1}{2}\log n$ to 0 is sufficient to have $n\mathbb{E}[A_2] = O(1)$. In fact, by taking $\beta_1 = \beta_2 = 1$, all cases are merged into a unique case and no convergence condition on $\frac{1}{8\sigma^2}$ is needed anymore. At this point of the proof, for high-weight codewords, we have

$$n\mathbb{E}[A_2] = O(1). \tag{25}$$

From (20) and (25), it is found that $n\mathbb{E}[A] = O(1)$. Our third step in this proof is to show that $nB = o(1)$.

In a way similar to how the theta series of $\mathbb{Z}^n$ is expressed with the Jacobi theta function $\theta_3(z)$ of $\mathbb{Z}$ (see [4]), we rewrite the summation in (10) to get

$$B = \left(\sum_{z_1\in\mathbb{Z}} \exp\left(\frac{-p^2 z_1^2 + p(p-1)|z_1|}{8\sigma^2}\right)\right)^n - 1$$
$$= \left(1 + 2\ \exp\left(\frac{-p}{8\sigma^2}\right) + 2\ \exp\left(\frac{-2p^2-2p}{8\sigma^2}\right) + \ldots\right)^n - 1.$$

Now take $p = \beta \log n$ with $\beta > 16\sigma^2$. For this choice of p, B tends to zero like $2n^{-\beta/8\sigma^2+1}$ so we obtain

$$nB = o(1).$$

The method used for A to prove $n\mathbb{E}[A] = O(1)$ can also be applied to the error term A_0 to prove that $\mathbb{E}[A_0] = O(1)$. Finally, from (9), given that B is not involved in the expectation over the GLD ensemble, P_{es} satisfies

$$n\mathbb{E}[P_{es}] \leq n\mathbb{E}[A] + nB + \mathbb{E}[A_0]nB = O(1).$$

■

IV. Distribution of Cycles in Random Bipartite Graphs

We prove here Theorem 2, which is an adaptation to bipartite graphs of some results that Bollobás provided for random graphs in [9]. Notice that this section is self-consistent and can be read independently from the rest of the paper. Theorem 2 is used in the proof of Theorem 1 to derive $n\mathbb{E}[A_1] = O(1)$ for spectral thinning. The reader should note that σ in this section denotes the union of groups in a bipartite configuration and the integer k here is the length of a cycle in the bipartite graph. We tried to adopt as much as possible the notation used in [9].

Lemma 1: Suppose that $k = o(\log n)$ and consider a sequence of constant $\{a_i\}_{i=1}^n \subseteq \mathbb{N}^*$ such that $M = \max_i\{a_i\}$. Then,

$$k!\left(\sum_{\substack{S\subseteq\{1,2,\ldots,n\}\\|S|=k}}\prod_{i\in S} a_i\right) \sim \left(\sum_{i=1}^n a_i\right)^k,$$

where the asymptotic relation has to be intended with respect to n.

Proof: We will find the result by induction on k. The base case $k = 1$ is a trivial equality. Then, let us suppose that the lemma is true for a general k and show it for the case $k+1$: first of all, notice that

$$(k+1)!\left(\sum_{\substack{S\subseteq\{1,2,\ldots,n\}\\|S|=k+1}}\prod_{i\in S} a_i\right) \leq \left(\sum_{i=1}^n a_i\right)^{k+1}. \tag{26}$$

Then, using the induction step in (27), we have

$$\begin{aligned}
\left(\sum_{i=1}^n a_i\right)^{k+1} &= \left(\sum_{i=1}^n a_i\right)\left(\sum_{i=1}^n a_i\right)^k \\
&\sim k!\left(\sum_{i=1}^n a_i\right)\left(\sum_{\substack{S\subseteq\{1,2,\ldots,n\}\\|S|=k}}\prod_{i\in S} a_i\right) \qquad (27)\\
&= k!\Bigg(a_1\left(\sum_{\substack{S\subseteq\{1,2,\ldots,n\}\\|S|=k}}\prod_{i\in S} a_i\right) + \ldots + \\
&\quad + a_n\left(\sum_{\substack{S\subseteq\{1,2,\ldots,n\}\\|S|=k}}\prod_{i\in S} a_i\right)\Bigg) \\
&= k!\Bigg((k+1)\left(\sum_{\substack{S\subseteq\{1,2,\ldots,n\}\\|S|=k+1}}\prod_{i\in S} a_i\right) + \\
&\quad + \sum_{i=1}^n a_i\left(a_i \sum_{\substack{S\subseteq\{1,2,\ldots,n\}\setminus\{i\}\\|S|=k-1}}\prod_{j\in S} a_j\right)\Bigg) \\
&\leq (k+1)!\left(\sum_{\substack{S\subseteq\{1,2,\ldots,n\}\\|S|=k+1}}\prod_{i\in S} a_i + \right.
\end{aligned}$$

$$+\frac{\sum_{i=1}^n a_i^2}{k+1}\left(\sum_{\substack{S\subseteq\{1,2,\dots,n\}\\|S|=k-1}}\prod_{j\in S}a_j\right)\Bigg)$$

$$\leq (k+1)!\left(\sum_{\substack{S\subseteq\{1,2,\dots,n\}\\|S|=k+1}}\prod_{i\in S}a_i\right)\left(1+\frac{nM^2\binom{n}{k-1}M^{k-1}}{(k+1)\binom{n}{k+1}}\right)$$

$$\sim (k+1)!\left(\sum_{\substack{S\subseteq\{1,2,\dots,n\}\\|S|=k+1}}\prod_{i\in S}a_i\right)\left(1+\frac{M^{k+1}}{(k+1)n}\right). \quad (28)$$

(26) and (28) are enough to conclude. ∎

Let $G=(V,P,E)$ be an undirected bipartite graph: V is the set of left vertices, P the set of right vertices and $E\subseteq V\times P$ is the set of edges. Moreover, let d_i^V (resp. d_j^P) be the degree of node $i\in V$ (resp. $j\in P$). Suppose also that $|V|=n_V$ and $|P|=n_P=\alpha n_V$ for some rational constant α. Without loss of generality, suppose that $\Delta^V=d_1^V\geq d_2^V\geq\dots d_{n_V}^V\geq 2$ and $\Delta^P=d_1^P\geq d_2^P\geq\dots d_{n_P}^P\geq 2$ and let us call $\Delta=\max\{\Delta^V,\Delta^P\}$. The total number of vertices in the graph is $n=n_V+n_P$. All the asymptotic relations provided below are meant to be for n tending to infinity.

We are interested in studying random bipartite graphs when the two sequences $\mathbf{d}^V=\{d_i^V\}_i$ and $\mathbf{d}^P=\{d_j^P\}_j$ are fixed for given n_V and n_P. More precisely, we would like to describe the asymptotic distribution of cycles of even length k in a random bipartite graph with fixed degree sequences and we focus our attention on $k=o(\log n)$. We will derive this distribution from the study of its analogue in *bipartite configurations*:

Definition 4: A *bipartite configuration* is a triplet $F=(W,Q,D)$, in which $W=\cup_{i=1}^{n_V}W_i$ and $Q=\cup_{j=1}^{n_P}Q_j$ are unions of *groups* and D is the set of *edges*. Every group W_i (resp. Q_j) is a set of d_i^V (resp. d_j^P) vertices. An edge in D is a couple of two vertices, one in W and one in Q, and all edges are pairwise disjoint. In other words, the degree of a vertex of a configuration is always 1, while a group W_i (resp. Q_j) has total degree d_i^V (resp. d_j^P).

From now on, let $k\in 2\mathbb{N}$ be such that $k=o(\log n)$. It should be clear from the notion of a cycle in a graph what a k-cycle of a configuration is. Formally:

Definition 5: A *k-cycle* (or a cycle of *length* k) of a bipartite configuration is given by k groups $W_{i_1},W_{i_2},\dots,W_{i_{k/2}},Q_{j_1},Q_{j_2},\dots,Q_{j_{k/2}}$ and k edges $e_1,e_2,\dots,e_k$ such that for every $l=1,2,\dots,k/2$ the edge e_{2l-1} connects the groups W_{i_l} and Q_{j_l} and the edge e_{2l} connects the groups Q_{j_l} and $W_{i_{l+1}}$ (with $W_{i_{k/2+1}}=W_{i_1}$).

Let $\sigma=\sigma_W\cup\sigma_Q$ be the union of two unions of groups of a bipartite configuration, both of them made of $k/2$ groups and such that $\sigma_W\subseteq W$ and $\sigma_Q\subseteq Q$. We denote by $|\sigma_W|$ (resp. $|\sigma_Q|$) the number of groups that compose σ_W (resp. σ_Q) and we define $w(\sigma_W)=\prod_{i:W_i\subseteq\sigma_W}d_i^V(d_i^V-1)$ (resp. $w(\sigma_Q)=\prod_{j:Q_j\subseteq\sigma_Q}d_j^P(d_j^P-1)$). Then, consider the quantity

$$C_k(\mathbf{d}^V,\mathbf{d}^P)=\frac{1}{k}(k/2)!^2\sum_{\substack{\sigma=\sigma_W\cup\sigma_Q\\|\sigma_W|=|\sigma_Q|=\frac{k}{2}}}(w(\sigma_W)w(\sigma_Q)).$$

$C_k(\mathbf{d}^V,\mathbf{d}^P)$ is exactly the number of k-sets of pairs of vertices that can be a cycle of length k in a bipartite configuration. Moreover, for a given number $q\in 2\mathbb{N}$, let us define $\mathbf{d}^V-q/2$ (resp. $\mathbf{d}^P-q/2$) to be the sequence $\{0,0,\dots,0,d_{q/2+1}^V,d_{q/2+2}^V,\dots,d_{n_V}^V\}$ (resp. $\{0,0,\dots,0,d_{q/2+1}^P,d_{q/2+2}^P,\dots,d_{n_P}^P\}$). We have the following property:

Lemma 2: For asymptotically large $n=n_V+n_P$, for any fixed $q\in 2\mathbb{N}$, for $\Delta=O(\log n)$, and for $k=o(\log n)$,

$$C_k(\mathbf{d}^V,\mathbf{d}^P)\sim\frac{2^k}{k}\left(\sum_{i=1}^{n_V}\binom{d_i^V}{2}\right)^{k/2}\left(\sum_{j=1}^{n_P}\binom{d_j^P}{2}\right)^{k/2} \quad (29)$$

and

$$C_k(\mathbf{d}^V,\mathbf{d}^P)\sim C_k\left(\mathbf{d}^V-\frac{q}{2},\mathbf{d}^P-\frac{q}{2}\right). \quad (30)$$

Proof: By definition, one has

$$\begin{aligned}C_k(\mathbf{d}^V,\mathbf{d}^P)&=\frac{1}{k}(k/2)!^2\sum_{\substack{\sigma=\sigma_W\cup\sigma_Q\\|\sigma_W|=|\sigma_Q|=\frac{k}{2}}}(w(\sigma_W)w(\sigma_Q))\\&=\frac{1}{k}(k/2)!^2\left(\sum_{\substack{\sigma_W\subseteq W\\|\sigma_W|=\frac{k}{2}}}2^{k/2}\prod_{i:W_i\subseteq\sigma_W}\binom{d_i^V}{2}\right)\cdot\\&\quad\cdot\left(\sum_{\substack{\sigma_Q\subseteq Q\\|\sigma_Q|=\frac{k}{2}}}2^{k/2}\prod_{j:Q_j\subseteq\sigma_Q}\binom{d_j^P}{2}\right)\\&\sim\frac{2^k}{k}\left(\sum_{i=1}^{n_V}\binom{d_i^V}{2}\right)^{k/2}\left(\sum_{j=1}^{n_P}\binom{d_j^P}{2}\right)^{k/2},\end{aligned}$$

by Lemma 1; this proves (29). For (30), let $A=\cup_{i=q/2+1}^{n_V}W_i$ and $B=\cup_{j=q/2+1}^{n_P}Q_j$; we have:

$$\begin{aligned}&C_k\left(\mathbf{d}^V-\frac{q}{2},\mathbf{d}^P-\frac{q}{2}\right)=\\&=\frac{1}{k}(k/2)!^2\sum_{\substack{\sigma=\sigma_W\cup\sigma_Q\subseteq A\cup B\\|\sigma_W|=|\sigma_Q|=\frac{k}{2}}}(w(\sigma_W)w(\sigma_Q))\\&=\frac{1}{k}(k/2)!^2\left(\sum_{\substack{\sigma_W\subseteq A\\|\sigma_W|=\frac{k}{2}}}w(\sigma_W)\right)\left(\sum_{\substack{\sigma_Q\subseteq B\\|\sigma_Q|=\frac{k}{2}}}w(\sigma_Q)\right)\\&=C_k(\mathbf{d}^V,\mathbf{d}^P)+\\&\quad-\frac{1}{k}(k/2)!^2\left(\sum_{\substack{\sigma_W\subseteq W\\\exists W_i\subseteq W\setminus A\\|\sigma_W|=\frac{k}{2}}}w(\sigma_W)\right)\left(\sum_{\substack{\sigma_Q\subseteq B\\|\sigma_Q|=\frac{k}{2}}}w(\sigma_Q)\right)+\\&\quad-\frac{1}{k}(k/2)!^2\left(\sum_{\substack{\sigma_W\subseteq A\\|\sigma_W|=\frac{k}{2}}}w(\sigma_W)\right)\left(\sum_{\substack{\sigma_Q\subseteq Q\\\exists Q_j\subseteq Q\setminus B\\|\sigma_Q|=\frac{k}{2}}}w(\sigma_Q)\right)+\\&\quad-\frac{1}{k}(k/2)!^2\left(\sum_{\substack{\sigma_W\subseteq W\\\exists W_i\subseteq W\setminus A\\|\sigma_W|=\frac{k}{2}}}w(\sigma_W)\right)\left(\sum_{\substack{\sigma_Q\subseteq Q\\\exists Q_j\subseteq Q\setminus B\\|\sigma_Q|=\frac{k}{2}}}w(\sigma_Q)\right)\end{aligned}$$

$$= C_k(\mathbf{d}^V, \mathbf{d}^P)\,(1 - f(n))\,.$$

for a certain $f(n)$ which is the sum of the three big terms above, divided by $C_k(\mathbf{d}^V, \mathbf{d}^P)$. The proof is concluded because $f(n) = o(1)$:

$$\begin{aligned} f(n) &\le \frac{kq\binom{n_V - q/2}{k/2-1}\Delta_V^k \binom{n_P - q/2}{k/2}\Delta_P^k}{4\binom{n_V}{k/2}\binom{n_P}{k/2}} + \\ &+ \frac{\binom{n_V - q/2}{k/2}\Delta_V^k kq\binom{n_P - q/2}{k/2-1}\Delta_P^k}{4\binom{n_V}{k/2}\binom{n_P}{k/2}} + \\ &+ \frac{k^2q^2\binom{n_V - q/2}{k/2-1}\Delta_V^k \binom{n_P - q/2}{k/2-1}\Delta_P^k}{8\binom{n_V}{k/2}\binom{n_P}{k/2}} \\ &\le \frac{kq\Delta^{4k}}{4n_V} + \frac{kq\Delta^{4k}}{4n_P} + \frac{k^2q^2\Delta^{4k}}{16n_Vn_P} = o(1). \end{aligned}$$

■

For simplicity, in the process of counting the number of cycles in a random configuration we would like to have a nice correspondence between the number of cycles and the number of involved edges. More precisely, we would like to be able to say that, if we consider t_2 2-cycles, t_4 4-cycles, ..., t_k k-cycles in a configuration, then these cycles correspond to $q = \sum_{i=2,4,\dots,k} it_i$ different edges and q different groups. This is true if we restrict our analysis only to configurations without *r-shackles*:

Definition 6: An r-shackle is a set of $l + 1 \le r + 1$ edges that connect vertices of some l different groups.

Attention: in [9], Bollobás calls *shackles* some particular cases of 2-shackles. We do not need to deal with them here and for us a *shackle* is simply a general r-shackle for which we do not need to specify r.

Let us call m the total number of edges of a bipartite configuration. $m = \sum_{i=1}^{n_V} d_i^V = \sum_{j=1}^{n_P} d_j^P$. Notice that

$$2\min\{n_V, n_P\} \le m \le n\Delta, \tag{31}$$

which means that m grows at least linearly fast in n. There are exactly $m!$ different bipartite configurations for given degree sequences $\mathbf{d}^V$ and $\mathbf{d}^P$. More generally, if we fix q edges of a configuration, we define N_q as the number of different configurations that contain those edges. Thus, $N_q = (m-q)!$.

Lemma 3: Given a set of q edges $\{e_1, e_2, \dots, e_q\}$ that do not contain an r-shackle, let $N^*(e_1, e_2, \dots, e_q)$ be the number of configurations that contain these edges and at least one r-shackle; moreover, let N_q^* be the maximum of $N^*(e_1, e_2, \dots, e_q)$ over all the possible choices of q different edges. Then, if $\Delta = O(\log n)$, and for every fixed q and r,

$$N_q^* = o(N_q).$$

Proof: We will prove this lemma by induction on r. In bipartite configurations, since edges always go from right to left (or vice versa), there cannot exist 1-shackles. For this reason, we start treating the base case $r = 2$. A 2-shackle is formed by two groups (one in W and one in Q) connected by three (parallel) edges. Then, when we fix q edges without shackles, there are two possible ways of adding at least a shackle to the configuration:

1) either the shackle involves (at least) one of the already fixed q edges: there are at most $q(\Delta_V - 1)(\Delta_P - 1)N_{q+1}$ configurations that satisfy this hypothesis;
2) or the shackle involves only other edges than the fixed ones: there do not exist more than $3!n_Vn_P\binom{\Delta_V}{3}\binom{\Delta_P}{3}N_{q+3}$ configurations that satisfy this second possibility.
Merging the two cases and recalling (31):

$$\frac{N_q^*}{N_q} \le \frac{q\Delta^2}{m-q} + \frac{3!n^2\Delta^6}{(m-q-2)^3} = o(1).$$

We are ready to treat the induction step for a more general r. Observe that we can divide r-shackles into two different categories: the ones which are also l-shackles for some $l < r$ and the ones which are not. For the first category, the result is proved by the induction hypothesis; hence, let us focus on $N_q^*(r)$, the number of configurations with q fixed edges (without shackles) that contain at least one r-shackle which is not an l-shackle for every $l < r$. In the rest of the proof, let us call the latter a *proper* r-shackle. We are left to show that $N_q^*(r) = o(N_q)$.

First of all, consider an r-shackle that involves only one vertex in one of its groups. If we take out from the shackle that vertex and the corresponding edge, then we obtain an $(r-1)$-shackle. This proves that a proper shackle involves at least two vertices in every group that it contains.

Now, as for the case $r = 2$, two different situations can be considered:
1) if the proper r-shackle does not involve the q already fixed edges: we treat this case only for even r (the odd case basically corresponding to the same computation and being easily deducible); the number of configurations satisfying this hypothesis is at most

$$\binom{n_V}{r/2}\binom{n_P}{r/2}\frac{r^2}{4}\,(r/2)!^2\Delta^{2(r+1)}N_{q+r+1}.$$

This bound can be explained as follows: the binomial coefficients come from the choice of the r groups forming the shackle. By definition, all the groups have to be connected; the fact that the configuration is bipartite and that by hypothesis there is no group of degree 1 implies that there must exist a connected path through all the groups (which means fixing $r-1$ edges): this can be done in at most $(r/2)!^2\Delta^{2(r-1)}$ different ways. Finally, we have to fix the two remaining edges, that must involve the initial and final group of the fixed path (because they cannot have degree 1): this can be done in at most $\Delta^4r^2/4$ different ways.
2) If the proper r-shackle involves at least one of the q already fixed edges: an argument similar to the previous one (again, for even r, but easily generalizable) tells that in this case the number of possible configurations is bounded by

$$q\binom{n_V}{(r-2)/2}\binom{n_P}{(r-2)/2}\frac{r^2}{4}\,((r-2)/2)!^2\Delta^{2r}N_{q+r}.$$

When we put together the two previous cases, we obtain that

$$\frac{N_q^*(r)}{N_q} \le \frac{n^rr^2\,(r/2)!^2\Delta^{2(r+1)}}{4(m-q-r)^{r+1}} + \frac{qn^{r-2}r^2\,((r-2)/2)!^2\Delta^{2r}}{4(m-q-r+1)^r},$$

in which both addenda are $o(1)$. ■

We are finally ready to state and prove the main theorem of this section:

Theorem 2: Consider a random bipartite graph $G = (V, P, E)$ with m edges. Suppose that the degree sequences $\mathbf{d}^V = \{d_i^V\}_i$ and $\mathbf{d}^P = \{d_j^P\}_j$ are fixed for given n_V and n_P, with $\Delta = O(\log n)$. For every even $k = o(\log n)$, the number of cycles of length k in the random graph follows a Poisson distribution with parameter

$$\lambda_k \sim \frac{1}{k} \left(\sum_{i=1}^{n_V} \binom{d_i^V}{2} \right)^{k/2} \cdot \left(\sum_{j=1}^{n_P} \binom{d_j^P}{2} \right)^{k/2} \cdot \left(\frac{m}{2} \right)^{-k}. \quad (32)$$

Proof: Let $\mathcal{G}$ be the set of all bipartite graphs $G = (V, P, E)$, let Φ be the set of all bipartite configurations $F = (W, Q, D)$, let $\Phi_0 \subseteq \Phi$ be the set of all bipartite configurations without r-shackles, and let Ω be the set of bipartite configurations without parallel edges between two groups. We turn all of this sets into probability spaces with uniform distribution.

Consider the map $\varphi : \Omega \to \mathcal{G}$ that assigns to every configuration $F \in \Omega$ the graph G that has an edge between $i \in V$ and $j \in P$ if and only if there is an edge in the configuration between W_i and Q_j. For a random G, let $X_l(G)$ be the random variable describing the number of l-cycles in G, for $l \in 2\mathbb{N}$ and $l \geq 4$. If $X_l(F)$ is the analog random variable for a configuration F, the map φ shows that $X_l(G)$ and $X_l(F)$ have the same distribution over $\mathcal{G}$ as over Ω. Therefore, our job is done if we show that over Ω the $X_l(F)$ asymptotically follow a Poisson distribution with parameter λ_k and in (32).

Let $\mathbb{E} = \mathbb{E}_{\Phi_0}[t_2, t_4, \ldots, t_l]$ be the expectation over Φ_0 of the number of t-tuples that consist of t_2 2-cycles, t_4 4-cycles, ..., t_l l-cycles (for $l = o(\log n)$), with $t = \sum_{k=2,4,\ldots,l} t_k$. Because of the absence of r-shackles (we can suppose r to be big enough), these cycles contain $q = \sum_{k=2,4,\ldots,l} k t_k$ different edges (and q different groups: $q/2$ in W and $q/2$ in Q). Then, using the notation N_q^* as in Lemma 3 and defining $M_q = N_q - N_q^*$, we have

$$\mathbb{E} = \mathbb{E}_{\Phi_0}[t_2, t_4, \ldots, t_l] \leq \left(\prod_{k=2,4,\ldots,l} \binom{C_k(\mathbf{d}^V, \mathbf{d}^P)}{t_k} \right) \frac{N_q}{M_0}$$

and

$$\mathbb{E} \geq \left(\prod_{k=2,4,\ldots,l} \binom{C_k(\mathbf{d}^V - q/2, \mathbf{d}^P - q/2)}{t_k} \right) \frac{M_q}{M_0}.$$

Now, Lemma 3 implies that $M_q = N_q - N_q^* \sim N_q = (m-q)!$. Applying this and Lemma 2 to the previous inequalities, we obtain that

$$\mathbb{E} \sim \prod_{k=2,4,\ldots,l} \frac{C_k(\mathbf{d}^V, \mathbf{d}^P)^{t_k}}{t_k!} m^{-k t_k} = \prod_{k=2,4,\ldots,l} \frac{\lambda_k^{t_k}}{t_k!}, \quad (33)$$

where

$$\lambda_k = C_k(\mathbf{d}^V, \mathbf{d}^P) m^{-k}.$$

Again, we use Lemma 2 to derive

$$\lambda_k \sim \frac{1}{k} \left(\sum_{i=1}^{n_V} \binom{d_i^V}{2} \right)^{k/2} \cdot \left(\sum_{j=1}^{n_P} \binom{d_j^P}{2} \right)^{k/2} \cdot \left(\frac{m}{2} \right)^{-k}.$$

Note that the right hand side of (33) is the binomial moment of a joint Poisson distribution with parameters $\lambda_2, \lambda_4, \ldots, \lambda_l$. Theorem C.33 in [7, p. 497] and Theorem 1.23 in [1, p. 26] imply that asymptotically the random variables $X_2(F), X_4(F), \ldots, X_l(F)$ follow independent Poisson distributions with $X_k(F)$ having mean λ_k. Since by Lemma 3 $|\Phi_0| \sim |\Phi|$, the $X_k(F)$ have the same distribution over Φ and, repeating the argument for $t_2 = 0$, the distribution is the same over Ω, too. This ends the proof. ■

V. Computer Simulations

Consider the non-binary elementary code C_0 of length $n_0 = 3$ and dimension $k_0 = 2$ defined over the field $\mathbb{F}_{11}$ by the parity-check matrix $(4 \;\; 5 \;\; 10)$. Its moment generating function is $g(s) = (1 + 30e^{2s} + 90e^{3s})/121$. The finite field is mapped to the integer set $\{-5, \ldots, +5\}$ as described in Section II. The small lattice is

$$\Lambda_0 = [3, 2]_{11} + 11\mathbb{Z}^3.$$

Finally, a lattice instance from the GLD lattice ensemble is $\Lambda = \Lambda_0^{\oplus L} \bigcap \pi(\Lambda_0^{\oplus L})$, where π is a randomly chosen permutation of size $n = n_0 L = 3L$. For Monte Carlo simulations, we took $n = 10^3 - 1$, $10^4 - 1$, $10^5 - 1$, and $10^6 - 1$. A GLD instance is decoded via message passing (or belief propagation [7]) on its bipartite graph. At the check node level, incoming messages are processed by an 11-state trellis forward-backward algorithm [20] to produce soft output messages. One decoding iteration corresponds to the decoding of all $2L$ check nodes. We allow up to 400 decoding iterations per lattice point.

As shown in Figure 5, the error probability per lattice coordinate decreases as $1/n$ in the error floor region. For dimension 10^6, the error floor can be improved by taking $p = 13$ instead of 11. We deliberately considered an elementary code with a weak minimum Hamming distance in order to attain a waterfall performance at 0.3 dB only from Poltyrev limit.

VI. Conclusions

Generalized low-density lattice ensembles with variable nodes of degree 2 and an elementary code of minimum weight 2 are studied in this paper. Our first theorem states that the error floor decreases as $1/n$. The proof of this theorem is based on a new decoupling technique. Our second theorem, an improvement of a well-known theorem proved by Bollobás, states that the length of short cycles in bipartite random graphs is Poisson disributed and gives the expression of its mean. Our result is valid for cycles with length up to $\log(n)^{1-\varepsilon}$.

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] B. Bollobás. *Random Graphs*. Cambridge University Press, UK, 2nd edition, 2001.

[2] R.E. Blahut. Theory and practice of error control codes. Reading, MA: Addison-Wesley, 1984.

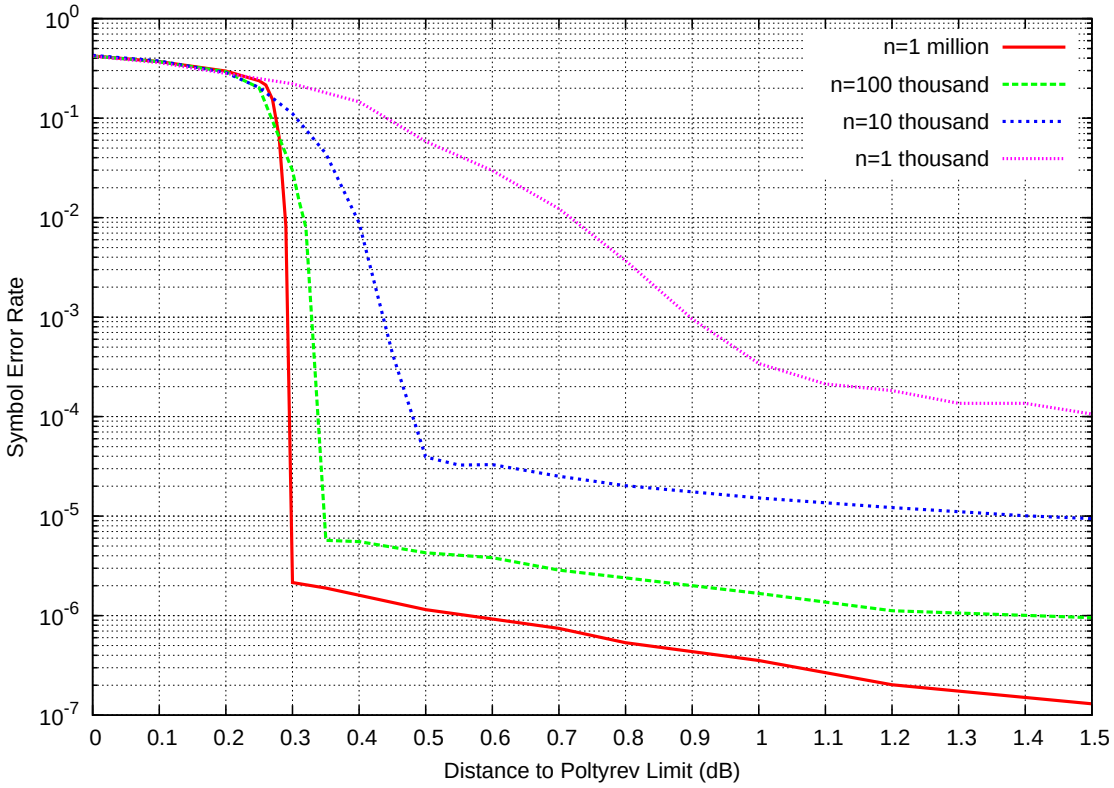

Figure 5. Ensemble performance of GLD lattices for dimensions $n = 1000$, 10000, 100000, and 1000000. Error rate is measured after BP decoding. The number of decoding iterations does not exceed 400 per lattice point. We measured 100 erroneous points at each signal-to-noise ratio level.

[3] R.M. Tanner,"A recursive approach to low complexity codes," *IEEE Trans. on Inf. Theory*, vol. IT-27, no. 5, pp. 533-547, Sept. 1981.

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

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

[6] N. di Pietro, J. J. Boutros, and N. Basha, "Non-binary GLD codes and their lattices," *2015 IEEE Information Theory Workshop*, Jerusalem, April 2015.

[7] T. Richardson and R. Urbanke. *Modern Coding Theory*. Cambridge University Press, 2008.

[8] R. Zamir. Lattice Coding for Signals and Networks. Cambridge University Press, 2014.

[9] B. Bollobás, "A probabilistic proof of an asymptotic formula for the number of labelled regular graphs," *Europ. J. Combinatorics*, vol. 1, no. 4, pp. 311-316, Dec. 1980.

[10] B.D. McKay, N.C. Wormald, and B. Wysocka, "Short Cycles in Random Regular Graphs," *The Electronic Journal of Combinatorics*, vol. 11, no. 1, 2004.

[11] S. Benedetto and G. Montorsi, "Unveiling turbo-codes: some results on parallel concatenated coding schemes," *IEEE Trans. on Inf. Theory*, vol. 42, no. 2, pp. 409-429, March 1996.

[12] L.C. Perez, J. Seghers, and D.J. Costello, "A distance spectrum interpretation of turbo codes," *IEEE Trans. on Inf. Theory*, vol. 42, no. 6, pp. 1698-1709, Nov. 1996.

[13] 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.

[14] 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.

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

[16] J.G. Proakis and M. Salehi. *Digital Communications*. McGraw-Hill, 5th edition, 2008.

[17] J.H. Conway and R.K. Guy. *The Book of Numbers*. New York: Springer-Verlag, pp. 94-96, 1996.

[18] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, eight impression (1991), North-Holland, 1977.

[19] V. M. Sidelnikov, "The spectrum of weights of binary BoseChaudhuri-Hocquenghem codes," Probl. Pered. Inform., vol. 7, no. 1, pp. 1422, 1971.

[20] L. R. Bahl, J. Cocke, F. Jelinek and J. Raviv, "Optimal decoding for linear codes for minimizing symbol error rate," *IEEE Trans. on Inf. Theory*, vol. 20, no. 2, pp. 284-287, March 1974.