New Results on Low-Density Integer Lattices

Nicola di Pietro*†, Joseph J. Boutros‡, Gilles Zémor†, and Loïc Brunel*

*Mitsubishi Electric R&D Centre Europe, Rennes, France
Email: {n.dipietro, l.brunel}@fr.merce.mee.com
†Institut de Mathmatiques, UMR 5251, Université de Bordeaux, France
Email: {nicola.di.pietro, gilles.zemor}@math.u-bordeaux1.fr
‡Texas A&M University at Qatar, Doha, Qatar
Email: boutros@tamu.edu

***Abstract*—A new family of integer lattices built from Construction A and non-binary low-density parity-check (LDPC) codes has been proposed by the authors in 2012. Lattices in this family are referred to as LDA lattices. Previous experimental results revealed excellent performance which clearly single out LDA lattices among the strongest candidates for potential applications in digital communications and networks, such as network coding and information theoretic security at the physical layer level. In this paper, we show that replacing random codes by LDPC codes in Construction A does not induce any structural loss. More precisely, our main theorem states that LDA lattices can achieve Poltyrev capacity limit on an additive white Gaussian noise channel. We present here the detailed proof and its consequences on the lattice dimension, the finite field size, and the parameters of the LDPC ensemble. The latter has a row weight that increases logarithmically in the code length. In a more recent work, it is proved that the Poltyrev limit is attained by a different LDA ensemble having a small constant row weight.**

I. Introduction

More than a century ago, significant works by mathematicians have been accomplished on quadratic forms and lattices. In the recent era, besides the extensive research on advanced topics related to quadratic forms, Leech and Sloane [1] made an elegant relationship between Euclidean lattices [2] and error-correcting codes [3], see also chap. 5 in [2]. Mainly, linear error-correcting codes defined on a finite field $\mathbb{F}_p$ can be used to construct lattices over the ring of relative integers $\mathbb{Z}$, the ring of Gaussian integers $\mathbb{Z}[i]$, and the ring of Eisenstein integers $\mathbb{Z}[\omega]$. These three rings are the best candidates for digital transmission at the physical layer in data networks where communication links are real or complex.

Among these algebraic constructions of lattices from error-correcting codes, we cite the so-called Constructions A,B, and D [2, chap.5] [4]. Construction A produces a lattice out of a unique code. Construction B has two nested codes, the larger being a single parity-check code. Construction D is based on multiple nested lattices. Many of the famous lattice sphere packings in small dimensions (less than 32) are found by these algebraic constructions. Obviously, linear binary codes played a great role in those constructions. Famous lattices like the Gosset lattice E_8, the Leech lattice Λ_{24}, and the Barnes-Wall family BW_n are built via binary codes. A few constructions with non-binary codes can be found in [2] (including complex constructions for E_8 and Λ_{24}). Furthermore, powerful lattices such those proposed in [5] [6] and [7] are made of nested binary codes, LDPC and Turbo codes respectively. They suffer from the small number of nested codes due to the limited complexity. Also, analysis of Construction D lattices is not very tractable where the Turbo or the LDPC ensemble should be taken into account. The recent family of low-density lattice codes [8] breaks from previous constructions by not relying on underlying error-correcting codes, its lattice generator matrix is obtained by directly inverting a sparse matrix: this new approach has structural appeal but decoding is somewhat unwieldy.

Construction A with linear random non-binary codes has been studied by Loeliger [9]. For a lattice dimension n and an alphabet size p, $n \to \infty$ and $p \to \infty$, it has been shown that random codes based on Construction A can achieve the maximum noise level σ^2_{max}, see Section III and [12]. Attaining the Poltyrev limit σ^2_{max} would automatically imply that a rate up to $\frac{1}{2}\log(\text{SNR})$ can be reached by a finite constellation under lattice decoding. The addition of an MMSE factor and the proof of covering goodness extends this result to the capacity $\frac{1}{2}\log(1+\text{SNR})$ as proved by Erez and Zamir [10]. Unfortunately, the presence of random coding within Construction A is a main drawback making such a lattice ensemble too far from any practicality.

Gaborit and Zémor proposed a lattice family of high fundamental gain (i.e. Hermite constant) obtained by Construction A with random non-binary codes [11]. They used codes defined by double circulant generator matrices. Similar to the case of fully random p-ary codes, we do not know how to decode these lattices in moderate and large dimensions (beyond 100).

A new approach was proposed by the present authors in [13] [14] relying on Construction A together with p-ary LDPC codes [15] [16]. Experiments with reasonable values of p, such as $p = 11$ and $p = 41$, showed excellent results with those lattices, referred to as LDA lattices. The decoder is iterative [17] with an acceptable complexity being able to decode in dimensions up to 10000. Error rate performance for large dimensions are very good and estimated Hermite constants at small dimensions via LLL [18] show that most LDA lattices have a high packing density.

In this paper, we show that replacing random codes by LDPC codes in Construction A does not induce any structural

loss. More precisely, our main theorem states that LDA lattices can achieve Poltyrev capacity limit on an additive white Gaussian noise channel, under lattice decoding. The simplified statement is given in Theorem 1 in Section III and the full statement is found in Theorem 4 in Section IV-C.

II. Lattices and Construction A

Let $C[n,k]_p$ be a linear block code of length n and dimension k over $\mathbb{F}_p$. When needed we write $C[n,k,d_H]_p$ for a code with minimum Hamming distance d_H. From multilevel coded modulation point of view [19], Construction A has two levels only, the first is protected by $C[n,k]_p$ and the second is uncoded. A lattice Λ is a discrete sub-group of rank n of $\mathbb{R}^n$. Construction A defines Λ via the expression

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

In the above expression, we abuse notation by identifying $\mathbb{F}_p$ with one of its natural embeddings in $\mathbb{Z}$. For example, we have $E_8 = [8,4,4]_2 + 2\mathbb{Z}^8$, where $[n,k,d_H]$ is used as shorthand for a code with parameters n, k, d_H. The E_8 lattice can also be obtained by an equivalent complex Construction B, $E_8 = [4,1,4]_2 + (1+i)[4,3,2]_2 + (1+i)^2\ \mathbb{Z}[i]^4$, and by another complex Construction A, $E_8 = [4,2,3]_3 + i\sqrt{3}\ \mathbb{Z}[\omega]^4$. E_8 is an extremal case for its Euclidean distance. Indeed, the squared Euclidean distance in $[8,4,4]_2$ is 4, it is equal to the squared Euclidean distance in the coset $2\mathbb{Z}^8$. Improving C won't improve the Euclidean distance of E_8 because $p=2$. This simple example shows us that avoiding Construction D with multiple nested binary codes is possible by using a more powerful code C and a larger finite field size p. Hence, LDA lattices [13] refer to the Construction A case where C is an LDPC code and $p>2$.

In the sequel, we restrict the study to LDA lattices built as $\mathbb{Z}$-modules. Its generalization to lattices over $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ should be straightforward.

III. LDA Lattices and Lattice Decoding

First of all, let us recall what the AWGN channel is and how a lattice is used for the transmission of information. Let $\Lambda \subseteq \mathbb{R}^n$ be an LDA lattice with generator matrix G. In this scenario, uncoded information is represented by an integer vector $z \in \mathbb{Z}^n$, which is coded into the lattice point $x = zG \in \Lambda$. This point is sent over the AWGN channel, which adds to x some random noise. The channel output is then the real n-dimensional point $y = x + \eta$, where $\eta = (\eta_1, \ldots, \eta_n)$ and the η_i's are n i.i.d. normally distributed random variables of variance σ^2:

$$\eta_i \sim \mathcal{N}(0, \sigma^2). \tag{2}$$

By definition, a *lattice code* is the intersection of a lattice with a bounded *shaping region* and properly only this finite subset of the lattice consists of the codewords used for communication (see for example [8]). As it is done by other authors (for example [8], [6], [5] and [7]), in this paper we treat the case of *lattice decoding* or decoding of the *infinite lattice*. This means that the decoder makes no assumption on the shaping region and the boundaries of the code; equivalently, we could say that the whole unbounded lattice makes up the codebook. In this setting, the decoder only looks for the lattice point which is the closest to the channel output y. Given a lattice code, this method is equivalent to maximum likelihood (ML) decoding for all the points that are far from the boundaries of the shaping region, while it is reduced to a suboptimal solution for all the points close to them. For an infinite lattice, lattice decoding is optimal. Lattice decoder is simply a *quantizer*, which finds $\hat{x} \in \Lambda$ such that $y = \hat{x} + v$, for some $v \in \mathcal{V}$, the Voronoi region of the origin. Of course, y is correctly decoded if and only if $\hat{x} = x$. We define the *error probability* P_e as

$$P_e = \mathcal{P}\{\hat{x} \neq x\}. \tag{3}$$

By the symmetry of the lattice, this probability is the same for every x in Λ and coincides with the average error probability.

In [12], Poltyrev adapted the concept of capacity to this scenario. When the codebook is unbounded, usual capacity loses its sense. Poltyrev proposed the notion of *generalized capacity*, which concretely implies that there exists a lattice in big enough dimension n that can be decoded with arbitrary small decoding probability P_e if and only if the noise variance of the channel is

$$\sigma^2 < \frac{\mathrm{Vol}(\Lambda)^{\frac{2}{n}}}{2\pi\,\mathrm{e}} =: \sigma^2_{max}. \tag{4}$$

We refer the reader to [12] for all the details. Notice that, for a lattice obtained by Construction A from a k-dimensional code in $\mathbb{F}_p^n$, $\mathrm{Vol}(\Lambda) = p^{(n-k)}$ and $\sigma^2_{max} = p^{2(1-k/n)}/2\pi\,\mathrm{e}$.

With a little abuse of language, we call *Poltyrev capacity* the upper bound for acceptable noise variance in (24). We will henceforth say that a lattice family *achieves* Poltyrev capacity if a random lattice in the family can be decoded with error probability as small as wanted in big enough dimension.

This paper is dedicated to the proof of the following result:

Theorem 1: There exists a Poltyrev-capacity-achieving family of LDA lattices $\Lambda = C[n,k] + p\mathbb{Z}^n$, such that the rows of the parity-check matrices of the underlying LDPC codes have degree logarithmic in n.

This theorem will be a straightforward consequence of Theorem 4 in Section IV-C, which expresses the same result with some more technical details due to specific construction of the LDA lattices family.

IV. LDA lattices achieve Poltyrev capacity

A. Random LDA lattices ensemble

First of all, let us specify the random LDA lattices ensemble we deal with. Let p be a prime number and let H be a matrix of size $n \times n(1-R)$, for some $0 < R < 1$ with entries in $\{0, 1, \ldots, p-1\}$. More precisely, let each row of the matrix be a random vector, built independently from each other as follows. Let $0 \leq \Delta \leq n$ be an integer. For a given row of H, let us choose, following a uniform random distribution, exactly Δ coordinates. We assign to these coordinates a value, chosen uniformly at random in $\{0, 1, \ldots, p-1\}$; furthermore, we impose that all the other $n - \Delta$ coordinates are deterministically

equal to 0. What we obtain is a matrix in which every row contains exactly $n-\Delta$ zeros and Δ random entries, placed in random positions.

This matrix can be viewed as the parity-check matrix of a k-dimensional random code $C = C[n,k]_p \subseteq {\mathbb{F}_p}^n$, for which all parity-check equations have at most Δ non-zero coefficients. This implies that the rate of C it at least R, but it may also be bigger. Notice that, if Δ is small with respect to n, C is an LDPC code. We will take into account the set of all LDA lattices $\Lambda = C + p\mathbb{Z}^n \subseteq \mathbb{Z}^n$ such that C is built at random as we have just described.

B. Preliminary lemmas

Before stating our main theorem, we prove here two classical lemmas that will be useful in the following.

Lemma 2: Let $B_{n,c}(\rho) := \{x \in \mathbb{R}^n \mid ||x-c||^2 \leq \rho^2\}$ be the sphere centered at c of radius $\rho = \rho(n)$. Let $N := |\mathbb{Z}^n \cap B_{n,c}(\rho)|$. Then

$$N \leq \mathrm{Vol}\left(B_{n,c}\left(\rho\right)\right)\left(1+\frac{\sqrt{n}}{2\rho}\right)^n. \tag{5}$$

Proof: Consider, for every $z \in \mathbb{Z}^n$, the cube $\mathcal{C}_z$ centered at z and of edge (and volume) equal to 1. Let

$$\mathcal{U} := \bigcup_{z \in \mathbb{Z}^n \cap B_{n,c}(\rho)} \mathcal{C}_z \tag{6}$$

and let $\mathcal{S}$ be the sphere circumscribed to $\mathcal{U}$ (which contains $B_{n,c}(\rho)$, too). Since the diagonal of any $\mathcal{C}_z$ measures $\sqrt{n}$, we have

$$\mathrm{Vol}(\mathcal{S}) \leq \mathrm{Vol}\left(B_{n,c}\left(\rho+\frac{\sqrt{n}}{2}\right)\right). \tag{7}$$

Hence

$$N = |\{z \mid \mathcal{C}_z \subseteq \mathcal{U}\}| = \mathrm{Vol}(\mathcal{U}) \leq \mathrm{Vol}(\mathcal{S}) \leq \tag{8}$$

$$\leq \mathrm{Vol}\left(B_{n,c}\left(\rho+\frac{\sqrt{n}}{2}\right)\right) = \tag{9}$$

$$= \mathrm{Vol}\left(B_{n,c}(1)\right)\left(\rho+\frac{\sqrt{n}}{2}\right)^n = \tag{10}$$

$$= \mathrm{Vol}\left(B_{n,c}(1)\right)\rho^n\left(1+\frac{\sqrt{n}}{2\rho}\right)^n = \tag{11}$$

$$= \mathrm{Vol}\left(B_{n,c}\left(\rho\right)\right)\left(1+\frac{\sqrt{n}}{2\rho}\right)^n, \tag{12}$$

which is what we were looking for.

Lemma 3: 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 $\varepsilon > 0$,

$$\mathcal{P}\left\{\rho \leq \sigma\sqrt{n}\left(1+\varepsilon\right)\right\} \longrightarrow 1, \text{ as } n \to \infty. \tag{13}$$

Proof: It is known that, since $X_i \sim \mathcal{N}(0,\sigma^2)$, $i = 1,\ldots,n$, then X_i^2 has a gamma distribution and $\mathbb{E}[X_i^2] = \sigma^2$, $\mathrm{Var}(X_i^2) = 2\sigma^4$. Consequently, by the independence of the X_i,

$$\mathbb{E}[\rho^2] = n\sigma^2, \ \mathrm{Var}(\rho^2) = 2n\sigma^4. \tag{14}$$

Given a random variable Y and any $\tau > 0$, Chebyshev's inequality states that

$$\mathcal{P}\left\{|Y - \mathbb{E}[Y]| > \tau\right\} \leq \frac{\mathrm{Var}(Y)}{\tau^2}. \tag{15}$$

Then, choose any $\kappa > 0$ and fix $Y = \rho^2$ and $\tau = \kappa\sqrt{2n}\sigma^2$; we have

$$\mathcal{P}\left\{|\rho^2 - n\sigma^2| > \kappa\sqrt{2n}\sigma^2\right\} \leq \frac{1}{\kappa^2}. \tag{16}$$

If we choose $\kappa = \kappa(n)$ such that $\lim_{n\to\infty}\kappa = +\infty$, than

$$\mathcal{P}\left\{|\rho^2 - n\sigma^2| \leq \kappa\sqrt{2n}\sigma^2\right\} \longrightarrow 1, \text{ as } n \to \infty. \tag{17}$$

Equivalently,

$$\mathcal{P}\left\{\rho^2 \leq \sigma^2 n\left(1+\kappa\sqrt{\frac{2}{n}}\right)\right\} \longrightarrow 1, \text{ as } n \to \infty. \tag{18}$$

Taking for example $\kappa = \log n$, we have that $\lim_{n\to\infty}\kappa\sqrt{2/n} \to 0$ and for every $\varepsilon > 0$, we can conclude that

$$\mathcal{P}\left\{\rho \leq \sigma\sqrt{n}\left(1+\varepsilon\right)\right\} \longrightarrow 1, \text{ as } n \to \infty, \tag{19}$$

which proves the lemma.

C. The main result

We are now ready to state our main theorem.

Theorem 4: Let n be a positive integer and let R be a real number such that $0 < R < 1$. Let $p = n^\lambda$ be a prime number for some $\lambda > 0$. Let $\Delta = \beta \log n$ be an integer number, for some $\beta \in \mathbb{R}$. If

$$\lambda > \frac{1}{2R} \quad \text{and} \quad \frac{n}{\log n} \geq \beta > \lambda + \frac{3}{2(1-R)}, \tag{20}$$

then there exists a family of n-dimensional LDA lattices $\Lambda = C + p\mathbb{Z}^n$ that achieves Poltyrev capacity and such that the row degree in the parity-check matrix of C is at most Δ, the rate of C is at least R.

Proof: The family of LDA lattices that we consider is the random ensemble described in Section IV-A. Let Λ be a lattice of this family. Because of the lattice symmetry, we can suppose that the point of Λ transmitted over the channel is the point 0. $\eta = (\eta_1, \ldots, \eta_n)$ is the AWG noise vector and the channel output is $y = \eta$. We suppose that the channel noise variance is $\sigma^2 = \sigma^2_{\max}(1-\delta)^2$ for some $0 < \delta < 1$ that can be as small as wanted.

Lemma 3 states that, when n is very large, the vector y tends to lie within a sphere of radius a bit greater than $\sigma\sqrt{n}$ and centered at 0.

Let us consider the sphere $\mathcal{B} := B_{n,y}(\sigma\sqrt{n}(1+\varepsilon))$ centered at y, with $\varepsilon > 0$ chosen such that

$$\varepsilon < \frac{\delta}{1-\delta}; \tag{21}$$

this last condition will be useful in the following.

When n grows, the point 0 is inside the sphere with probability tending to 1; the probability of error P_e is smaller than the probability that one or more lattice points different

from 0 lie inside the sphere: if 0 is the only point in $\mathcal{B} := B_{n,y}(\sigma\sqrt{n}(1+\varepsilon))$, then lattice decoding gives the correct answer; otherwise, an error will very likely come out.

For every integer point $x \in \mathcal{B} \cap \mathbb{Z}^n$, let X_x be the random variable defined by

$$X_x = \begin{cases} 1, \text{ if } x \in \Lambda \\ 0, \text{ if } x \notin \Lambda \end{cases} . \tag{22}$$

Since $p\mathbb{Z}^n$ is contained in any LDA lattice, $X_x = 1$ for any $x \in p\mathbb{Z}^n$, independently from Λ. That is, in order to imply that 0 is the only point of $p\mathbb{Z}^n$ which lies in $\mathcal{B}$ (with very high probability when n is big enough), we impose the prime p to be bigger than the diameter of the sphere. In this way, the values that a coordinate of an integer point inside $\mathcal{B}$ may take, are contained in a set of representatives of the classes modulo p and, in particular, each class is represented at most once. This implies that $|p\mathbb{Z}^n \cap \mathcal{B}| \leq 1$ and, if 0 is inside $\mathcal{B}$, there will not be in it any other points of $p\mathbb{Z}^n$.

Formally, the condition on p is the following:

$$p > 2\sigma\sqrt{n}(1+\varepsilon). \tag{23}$$

We want it to be satisfied for every $\sigma < \sigma_{\max}$, therefore, taking into account the upper bound

$$\sigma < \frac{p^{(1-R)}}{\sqrt{2\pi\,\mathrm{e}}} \tag{24}$$

and the fact that $p = n^\lambda$, it becomes:

$$n^\lambda > \sqrt{\frac{2}{\pi e}}(1+\varepsilon)n^{\lambda(1-R)+\frac{1}{2}}.$$

This justifies the condition $\lambda > 1/2R$ in the hypothesis of the theorem, which makes (at least asymptotically) true the previous inequality.

Now, let $\mathcal{N}$ be the random variable that counts the number of lattice points inside $\mathcal{B}$ that do not belong to $p\mathbb{Z}^n$. We will show that

$$\lim_{n\to\infty} \mathcal{P}\{\mathcal{N} = 0\} = 1. \tag{25}$$

By definition,

$$\mathcal{N} = \sum_{x \in \mathbb{Z}^n \cap \mathcal{B} \setminus p\mathbb{Z}^n} X_x. \tag{26}$$

We prove the theorem if we prove (25). It is sufficient to show that

$$\lim_{n\to\infty} \mathbb{E}[\mathcal{N}] = 0. \tag{27}$$

Notice that

$$\mathbb{E}[\mathcal{N}] = \sum_{x \in \mathbb{Z}^n \cap \mathcal{B} \setminus p\mathbb{Z}^n} \mathbb{E}[X_x] = \sum_{x \in \mathbb{Z}^n \cap \mathcal{B} \setminus p\mathbb{Z}^n} \mathcal{P}\{x \in \Lambda\}. \tag{28}$$

If H is the parity-check matrix of C,

$$\mathcal{P}\{x \in \Lambda\} = \mathcal{P}\{Hx^T \equiv 0 \bmod p\} \tag{29}$$

$$= \left(\mathcal{P}\{hx^T \equiv 0 \bmod p\}\right)^{n(1-R)}, \tag{30}$$

where h represents any randomly built row of H (all rows of H are i.i.d.). Then,

$$\mathbb{E}[\mathcal{N}] = \sum_{x \in \mathbb{Z}^n \cap \mathcal{B} \setminus p\mathbb{Z}^n} \left(\mathcal{P}\{hx^T \equiv 0 \bmod p\}\right)^{n(1-R)}. \tag{31}$$

Given an integer point $x \in \mathbb{Z}^n \setminus p\mathbb{Z}^n$, suppose that $|\operatorname{Supp}(x)| = s > 0$, for some integer $1 \leq s \leq n$. We define *support* of the random vector $h = (h_1, \ldots, h_n)$ the set of indices of the Δ coordinates of h that are not deterministically equal to 0. If $I = \{i \in \operatorname{Supp}(x) \cap \operatorname{Supp}(h)\}$, we have

$$\mathcal{P}\{hx^T \equiv 0 \bmod p\} = \tag{32}$$

$$\mathcal{P}\{hx^T \equiv 0 \bmod p \mid |I| = 0\}\mathcal{P}\{|I| = 0\} + \tag{33}$$

$$+ \mathcal{P}\{hx^T \equiv 0 \bmod p \mid |I| \neq 0\}\mathcal{P}\{|I| \neq 0\} = \tag{34}$$

$$= 1 \cdot \mathcal{P}\{|I| = 0\} + \frac{1}{p} \cdot \mathcal{P}\{|I| \neq 0\} \leq \tag{35}$$

$$\leq \mathcal{P}\{|I| = 0\} + \frac{1}{p}. \tag{36}$$

There are two different situations:

- If $1 \leq s \leq n - \Delta$,

$$\mathcal{P}\{|I| = 0\} = \frac{\binom{n-s}{\Delta}}{\binom{n}{\Delta}} = \tag{37}$$

$$= \frac{n-\Delta}{n} \cdot \frac{n-1-\Delta}{n-1} \cdots \frac{n-s+1-\Delta}{n-s+1} = \tag{38}$$

$$= \left(1 - \frac{\Delta}{n}\right) \cdot \left(1 - \frac{\Delta}{n-1}\right) \cdots \left(1 - \frac{\Delta}{n-s+1}\right) \leq \tag{39}$$

$$\leq \left(1 - \frac{\Delta}{n}\right)^s = \left(1 - \frac{\beta \log n}{n}\right)^s \leq \tag{40}$$

$$\leq \frac{1}{n^{\beta s/n}}. \tag{41}$$

The previous inequality comes from the fact that

$$\left(1 - \frac{\beta \log n}{n}\right)^s \leq \frac{1}{n^{\beta s/n}} \Leftrightarrow \tag{42}$$

$$\Leftrightarrow \log\left(1 - \frac{\beta \log n}{n}\right) \leq \log \frac{1}{n^{\beta/n}} = -\frac{\beta \log n}{n}, \tag{43}$$

$$\tag{44}$$

which is true because

$$\log(1-x) \leq -x \text{ for all } x < 1. \tag{45}$$

Notice that for n big enough $\log(1 - \beta \log n/n)$ is well-defined and $0 < \beta \log n/n < 1$.

- If instead $n - \Delta < s \leq n$, $\mathcal{P}\{|I| = 0\} = 0$.

Therefore, if n is big enough, putting together (31), (36) and what we have just shown, recalling that $p = n^\lambda$, we get

$$\mathbb{E}[\mathcal{N}] = \sum_{x \in \mathbb{Z}^n \cap \mathcal{B} \smallsetminus p\mathbb{Z}^n} \left(\mathcal{P}\{hx^T \equiv 0 \bmod p\}\right)^{n(1-R)} \tag{46}$$

$$\leq \sum_{s=1}^{n-\Delta} \sum_{\substack{x \in \mathbb{Z}^n \cap \mathcal{B} \smallsetminus p\mathbb{Z}^n \\ |\operatorname{Supp}(x)|=s}} \left(\frac{1}{n^{\beta s/n}} + \frac{1}{n^\lambda}\right)^{n(1-R)} + \tag{47}$$

$$+ \sum_{s=n-\Delta+1}^{n} \sum_{\substack{x \in \mathbb{Z}^n \cap \mathcal{B} \smallsetminus p\mathbb{Z}^n \\ |\operatorname{Supp}(x)|=s}} \left(\frac{1}{n^\lambda}\right)^{n(1-R)}. \tag{48}$$

First of all, let us show that (48) goes to 0 when n grows. We will use the following definition: we say that a function $f(n)$ is asymptotic to $g(n)$ (denoted $f(n) \sim g(n)$), if $\lim_{n\to\infty} f(n)/g(n) = 1$. Let $\Gamma(\cdot)$ be the Euler Gamma function, then:

$$\sum_{s=n-\Delta+1}^{n} \sum_{\substack{x \in \mathbb{Z}^n \cap \mathcal{B} \smallsetminus p\mathbb{Z}^n \\ |\operatorname{Supp}(x)|=s}} \left(\frac{1}{n^\lambda}\right)^{n(1-R)} \leq \tag{49}$$

$$\leq \sum_{x \in \mathbb{Z}^n \cap \mathcal{B}} \left(\frac{1}{n^\lambda}\right)^{n(1-R)} = \tag{50}$$

$$= |\mathbb{Z}^n \cap \mathcal{B}| \left(\frac{1}{n^\lambda}\right)^{n(1-R)} \leq \tag{51}$$

$$\leq \operatorname{Vol}(\mathcal{B}) \left(1 + \frac{1}{2(1+\varepsilon)\sigma}\right)^n \left(\frac{1}{n^\lambda}\right)^{n(1-R)} = \tag{52}$$

$$= \frac{(\sqrt{\pi}\sigma\sqrt{n}(1+\varepsilon))^n}{\Gamma\left(\frac{n}{2}+1\right)} \left(1 + \frac{1}{2(1+\varepsilon)\sigma}\right)^n \left(\frac{1}{n^\lambda}\right)^{n(1-R)} \sim \tag{53}$$

$$\sim \frac{(\sigma\sqrt{2\pi\,\mathrm{e}}(1+\varepsilon))^n}{\sqrt{\pi n}} \left(1 + \frac{1}{2(1+\varepsilon)\sigma}\right)^n \left(\frac{1}{n^\lambda}\right)^{n(1-R)} = \tag{54}$$

$$= \frac{((1-\delta)(1+\varepsilon))^n}{\sqrt{\pi n}} \left(1 + \frac{\sqrt{2\pi\,\mathrm{e}}}{2(1+\varepsilon)(1-\delta)n^{\lambda(1-R)}}\right)^n. \tag{55}$$

Notice that in (52) we have used Lemma 2, (54) follows by Stirling approximation and (55) from the fact that $\sigma = (1-\delta)\sigma_{\max}$. Now, one can show that the term in the big parenthesis is either asymptotic to a constant or, at worst, subexponential (i. e. asymptotic to $\exp(Cn^\mu)$, for some constants C and $0 < \mu < 1$); hence the dominating term in (55) is $((1-\delta)(1+\varepsilon))^n$. But $(1-\delta)(1+\varepsilon) < 1$, thanks to condition (21):

$$(1-\delta)(1+\varepsilon) < 1 \Leftrightarrow \varepsilon < \frac{1}{1-\delta} - 1 = \frac{\delta}{1-\delta}. \tag{56}$$

This implies that (55) tends to 0 as n tends to infinity and the same holds for (48).

At this point, we only have to study the behavior of (47). In order to do it, we will separate the analysis in three subcases: let

$$1 < a < 1 + \frac{2}{3 + 2\lambda(1-R)} \tag{57}$$

be a constant such that $a\lambda/\beta < 1$. We will consider separately:

1) $1 \leq s \leq \lambda n/\beta$;
2) $\lambda n/\beta < s < a\lambda n/\beta$;
3) $a\lambda n/\beta \leq s \leq n - \Delta$.

Note that $a\lambda n/\beta$ is really less than $n - \Delta$ if n is big enough.

First case : $1 \leq s \leq \lambda n/\beta$ (that is, $\lambda \geq \beta s/n$). First of all, recall that $B_{n,c}(\rho)$ is the n-dimensional sphere of radius ρ, centered at c. Notice that

$$|\{x \in \mathbb{Z}^n \cap \mathcal{B} \smallsetminus p\mathbb{Z}^n \mid |\operatorname{Supp}(x)| = s\}| \leq \tag{58}$$

$$\leq |\{x \in \mathbb{Z}^n \cap \mathcal{B} \mid |\operatorname{Supp}(x)| = s\}| \leq \tag{59}$$

$$\leq \binom{n}{s} |\mathbb{Z}^n \cap B_{s,y}(\sigma\sqrt{n}(1+\varepsilon))| \leq \tag{60}$$

$$\leq n^s |\mathbb{Z}^n \cap [-\sigma\sqrt{n}(1+\varepsilon), \ldots, \sigma\sqrt{n}(1+\varepsilon)]^s| \leq \tag{61}$$

$$\leq n^s (2\sigma\sqrt{n}(1+\varepsilon) + 1)^s. \tag{62}$$

This will be useful in the following:

$$\sum_{s=1}^{\lfloor \lambda n/\beta \rfloor} \sum_{\substack{x \in \mathbb{Z}^n \cap \mathcal{B} \smallsetminus p\mathbb{Z}^n \\ |\operatorname{Supp}(x)|=s}} \left(\frac{1}{n^{\beta s/n}} + \frac{1}{n^\lambda}\right)^{n(1-R)} \leq \tag{63}$$

$$\leq \sum_{s=1}^{\lfloor \lambda n/\beta \rfloor} n^s (2\sigma\sqrt{n}(1+\varepsilon) + 1)^s \left(\frac{2}{n^{\beta s/n}}\right)^{n(1-R)} \leq \tag{64}$$

$$\leq \sum_{s=1}^{\lfloor \lambda n/\beta \rfloor} \left(C_1 n^{\lambda(1-R)+3/2-\beta(1-R)}\right)^s, \tag{65}$$

where C_1 is a constant. The last inequality is obtained recalling that $\sigma = \sigma_{\max}(1-\delta) = n^{\lambda(1-R)}(1-\delta)/\sqrt{2\pi\,\mathrm{e}}$. We conclude by pointing out that the previous sum is a geometric series and it tends to 0 because the exponent of n is negative, thanks to condition (20).

Second case : $\lambda n/\beta < s < a\lambda n/\beta$ (and $\beta s/n < a\lambda$). First of all, notice that, if we bound $\binom{n}{s}$ with 2^n instead of n^s in (61), we have

$$|\{x \in \mathbb{Z}^n \cap \mathcal{B} \smallsetminus p\mathbb{Z}^n \mid |\operatorname{Supp}(x)| = s\}| \leq \tag{66}$$

$$\leq 2^n (2\sigma\sqrt{n}(1+\varepsilon) + 1)^s \leq \tag{67}$$

$$\leq 2^n (C_2 n^{1/2+\lambda(1-R)}), \tag{68}$$

where C_2 is a constant. This implies that

$$\sum_{s=\lfloor \lambda n/\beta \rfloor + 1}^{\lfloor a\lambda n/\beta \rfloor} \sum_{\substack{x \in \mathbb{Z}^n \cap \mathcal{B} \smallsetminus p\mathbb{Z}^n \\ |\operatorname{Supp}(x)|=s}} \left(\frac{1}{n^{\beta s/n}} + \frac{1}{n^\lambda}\right)^{n(1-R)} \leq \tag{69}$$

$$\leq \sum_{s=\lfloor \lambda n/\beta \rfloor + 1}^{\lfloor a\lambda n/\beta \rfloor} \sum_{\substack{x \in \mathbb{Z}^n \cap \mathcal{B} \smallsetminus p\mathbb{Z}^n \\ |\operatorname{Supp}(x)|=s}} \left(\frac{1}{n^{\beta s/n}}\right)^{n(1-R)} \cdot \tag{70}$$

$$\cdot \left(1 + n^{\frac{\beta s}{n} - \lambda}\right)^{n(1-R)} \leq \tag{71}$$

$$\leq 2^n \left(1 + n^{\lambda(a-1)}\right)^{n(1-R)} \cdot \tag{72}$$

$$\cdot {C_2}^n \sum_{s=\lfloor \lambda n/\beta \rfloor + 1}^{\lfloor a\lambda n/\beta \rfloor} \left(n^{1/2+\lambda(1-R)-\beta(1-R)}\right)^s, \tag{73}$$

for some constant C_2.

Let $\gamma := 1/2 + \lambda(1-R) - \beta(1-R)$. The summation is a (partial) geometric series and it is equal to:

$$\frac{1-n^{\gamma(\lfloor a\lambda n/\beta\rfloor+1)}}{1-n^{\gamma}} - \frac{1-n^{\gamma(\lfloor \lambda n/\beta\rfloor+1)}}{1-n^{\gamma}} = \tag{74}$$

$$\frac{n^{\gamma(\lfloor \lambda n/\beta\rfloor+1)} - n^{\gamma(\lfloor a\lambda n/\beta\rfloor+1)}}{1-n^{\gamma}} \sim \tag{75}$$

$$\sim n^{\gamma(\lfloor \lambda n/\beta\rfloor+1)}, \tag{76}$$

since γ is negative by hypothesis (20) and $a > 1$.

This implies that (69) is bounded by a function which is asymptotic to

$$(2C_2)^n n^{n(\lambda(a-1)(1-R)+\gamma(\lfloor \lambda/\beta\rfloor+1/n))} \leq \tag{77}$$

$$n(2C_2)^n n^{n(\lambda(a-1)(1-R)+\gamma\lambda/\beta)}, \tag{78}$$

which goes to 0 if $(\lambda(a-1)(1-R)+\gamma\lambda/\beta)$ is negative. Let us check that this is true:

$$\lambda(a-1)(1-R)+\gamma\lambda/\beta = \tag{79}$$

$$= \lambda(a-1)(1-R) + \left(\frac{1}{2} + \lambda(1-R) - \beta(1-R)\right)\frac{\lambda}{\beta} < 0 \Leftrightarrow \tag{80}$$

$$\Leftrightarrow \beta > \frac{\lambda}{2-a} + \frac{1}{2(2-a)(2-R)}. \tag{81}$$

This is true thanks to hypothesis (20) and the condition $a < 1 + 2/(3 + 2\lambda(1-R))$, which imply

$$\lambda + \frac{3}{2(1-R)} > \frac{\lambda}{2-a} + \frac{1}{2(2-a)(2-R)}. \tag{82}$$

All of this allows us to conclude that (78) and (69) tend to 0 when n grows.

Third case : $a\lambda n/\beta \leq s \leq n - \Delta$. We have

$$\sum_{s=\lfloor a\lambda n/\beta\rfloor+1}^{n-\Delta} \sum_{\substack{x\in\mathbb{Z}^n\cap\mathcal{B}\setminus p\mathbb{Z}^n \\ |\operatorname{Supp}(x)|=s}} \left(\frac{1}{n^{\beta s/n}} + \frac{1}{n^{\lambda}}\right)^{n(1-R)} \leq \tag{83}$$

$$\leq \sum_{x\in\mathbb{Z}^n\cap\mathcal{B}} \left(\frac{1}{n^{\lambda}}\right)^{n(1-R)} \left(1 + \frac{1}{n^{\beta s/n-\lambda}}\right)^{n(1-R)} = \tag{84}$$

$$= \left(|\mathbb{Z}^n\cap\mathcal{B}| \left(\frac{1}{n^{\lambda}}\right)^{n(1-R)}\right) \left(1 + \frac{1}{n^{\beta s/n-\lambda}}\right)^{n(1-R)}. \tag{85}$$

We know that the left term is (asymptotically) bounded by (55) and goes to 0 exponentially; we show now that the right term is at most subexponential in n. Recalling that $s \geq a\lambda n/\beta$, it is bounded as follows:

$$\left(1 + \frac{1}{n^{\beta s/n-\lambda}}\right)^{n(1-R)} \leq \tag{86}$$

$$\left(1 + \frac{1}{n^{\lambda(a-1)}}\right)^{n(1-R)} \sim \exp\left(n^{1-\lambda(a-1)}(1-R)\right), \tag{87}$$

with $a > 1$ by hypothesis. Then, also (83) is bounded by a quantity in which the dominating term is $((1+\varepsilon)(1-\delta))^n$, which goes to 0 as n tends to infinity.

This ends the proof of (27), which is enough to conclude that the theorem is true.

V. Conclusions and future work

LDA lattices are obtained from Construction A with a non-binary LDPC code. We proved in this paper that the LDA lattice ensemble attain Poltyrev limit. This completes previous experimental results based on iterative factor graph decoding of LDA lattices. In a more recent work, it is proved that Poltyrev limit is attained by a different LDA ensemble having a small constant row weight. Our next step is to prove that both LDA lattice ensembles can achieve $\frac{1}{2}\log(1+\text{SNR})$ for finite constellations.

References

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

[2] J.H. Conway and N.J.A. Sloane, *Sphere packings, lattices and groups*, third edition, Springer-Verlag, 1999.

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

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

[5] M.-R. Sadeghi, A. H. Banihashemi, and D. Panario, "Low-density parity-check lattices: construction and decoding analysis," *IEEE Trans. on Inf. Theory*, vol. 52, no. 10, pp. 4481-4495, Oct. 2006.

[6] I. J. Baik and S. Y. Chung, "Irregular low-density parity-check lattices," in *Proc. of IEEE Int. Symp. on Inf. Theory*, pp. 2479-2483, July 2008.

[7] A. Sakzad, M.-R. Sadeghi, and D. Panario, "Turbo lattices: construction and performance analysis," available on arxiv.org, 2011.

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

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

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

[11] P. Gaborit and G. Zémor, "On the construction of dense lattices with a given automorphisms group," *Ann. de l'Institut Fourier*, vol. 57, no. 4, pp. 1051-1062, 2007.

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

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

[14] N. di Pietro, L. Brunel, J.J. Boutros, and G. Zémor, "Integer low-density lattices," *Information Theory and Applications*, San Diego, Feb. 2012.

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

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

[17] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge, U.K., Cambridge Univ. Press, 2008.

[18] A. K. Lenstra, H. W. Lenstra and L. Lovász, "Factoring polynomials with rational coefficients," *Math. Ann.*, 261(3) pp. 515–534, 1982.

[19] U. Wachsmann, R.F.H. Fischer, and J.B. Huber, "Multilevel codes: theoretical concepts and practical design rules," *IEEE Trans. Inform. Theory*, vol. 45, no. 5, pp. 1361–1391, July 1999.