New results on Construction A Lattices based on Very Sparse Parity-Check Matrices

Nicola di Pietro*[†], Gilles Zémor[†], Joseph J. Boutros[‡],

*Mitsubishi Electric R&D Centre Europe, Rennes, France
Email: n.dipietro@fr.merce.mee.com
[†]Institut de Mathématiques, 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*—We address the problem of transmission of information over the AWGN channel using lattices. In particular, we will deal with previously introduced LDA lattices which are obtained by Construction A from LDPC codes over the finite field $\mathbb{F}_p$. We will show how to build a particular ensemble of LDA lattices related to bipartite graphs with good expansion properties. We investigate the quality of this family under lattice decoding and show that a random member in it can be reliably decoded for any value of the channel noise variance up to Poltyrev limit. Values of p and the parameters for which optimal performance is guaranteed under lattice decoding are in accordance with the optimal parameters found experimentally under iterative decoding.**

I. Introduction

We are interested in a family of integer lattices suitable for decoding in high dimensions that are obtained from non-binary LDPC codes and Construction A and called accordingly *LDA* lattices. These lattices were first envisaged in [6] and reintroduced in [4] where an efficient iterative decoder was proposed: their performance has been encouraging, being in a number of contexts at least as good as all other families of lattices decodable with reasonable complexity.

The question we address in the present paper is how good the intrinsic quality of the LDA family is under full lattice decoding. We will show that with a proper choice of the underlying LDPC codes, LDA lattices can be reliably decoded for any value of the AWGN channel noise variance, up to Poltyrev limit [12], which is the maximum possible when the decoder is unaware of the shaping region. This analysis is motivated also by the well-known results in [11] and [7] about Construction A lattices and constitutes the natural continuation of the work started in [5]. One important feature of the lattice family we build, is that the parity-check matrices of the underlying LDPC codes have bounded row and column degrees. This result contrasts sharply with its analog for binary LDPC codes. Indeed, binary LDPC codes with parity-check equations of bounded weight have been known not to achieve capacity since Gallager [10]. Previous studies, of non-binary LDPC codes for modulo additive channels [8] and of LDA lattices [5], require parity-check equations with weight tending to infinity to achieve capacity.

The structure of the paper will be as follows: in Section II we give some background on lattices in general and the construction of LDA lattices in particular. In Section III we state and discuss our main result and its implications for practical decoding. In Section IV we introduce a particular family of bipartite graphs and specify some technical expansion properties that characterise it. These graphs will serve to define the skeleton of the LDPC code parity-check matrix, i.e. the underlying binary matrix. Finally, in Section V we relate these graphs to a random LDA lattice ensemble and prove that the latter achieves the Poltyrev limit.

II. LDA Lattices

We start with a brief introduction to lattices and set some notation. Then we recall Construction A [3] and the definition of the family of *LDA lattices* [4].

Let B be a set of n linearly independent vectors of $\mathbb{R}^n$; an n-dimensional lattice $\Lambda \subset \mathbb{R}^n$ is the set of all linear combinations with integer coefficients of the vectors of the *basis* $B = \{B_1, \dots, B_n\}$:

$$\Lambda = \left\{ \sum_{i=1}^{n} z_i B_i, z_i \in \mathbb{Z} \right\}. \tag{1}$$

The matrix G of size $n \times n$ whose rows are the vectors of a basis, is called a *generator matrix* for Λ. The volume of a lattice is defined as $\mathrm{Vol}(\Lambda) := |\det(G)|$. For detailed background on lattices we refer the reader to [3].

We now recall Construction A, which is a practical way to build a lattice from a linear code. More precisely, let C be a linear code of length n over the finite field $\mathbb{F}_p$. Codewords of C may be identified with integer points in the cube $[0, \dots, p)^n$. Using this identification, we say that Λ is obtained by Construction A from C if

$$\begin{aligned} \Lambda = C + p\mathbb{Z}^n &= \{x = c + pz, c \in C, z \in \mathbb{Z}^n\} && (2) \\ &= \{x \in \mathbb{R}^n \mid \exists c \in C,\ x \equiv c \mod p\}. && (3) \end{aligned}$$

Note that this is Construction A in a restricted sense. It can be generalized by replacing $p\mathbb{Z}^n$ with other lattices [3]. The

LDA definition in [4] uses a more general version of Construction A, but in the present work we stay with Construction A in the narrow sense. A *Low-Density-construction-A lattice* or, briefly, an *LDA lattice* is a lattice obtained by Construction A from a code C with the peculiarity that C is an LDPC code, that is, its parity-check matrix is sparse [10].

III. Lattice Decoding of LDA Lattices

A. AWGN Channel and Lattice Decoding

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, whose output is the real n-dimensional point $y = x+\eta$, with $\eta = (\eta_1, \dots, \eta_n)$. The η_i's are n i.i.d. normally distributed random variables of variance σ^2.

Following other authors (e.g. [16], [1], [14] and [15]), we treat the case of *lattice decoding* (or decoding of the *infinite lattice*). This means that the the set of codewords makes up the whole lattice. The *lattice decoder* simply finds the lattice point $\hat{x} \in \Lambda$ closest to the received point y. Of course, y is correctly decoded if and only if $\hat{x} = x$. We define the *error probability* as $P_e = \mathcal{P}\{\hat{x} \neq x\}$. By the symmetry of the lattice, this probability is the same for every $x \in \Lambda$ and coincides with the average error probability.

In [12], Poltyrev adapted the concept of capacity to this setting. When the set of codewords 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 arbitrarily small decoding error 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 details. Notice that, for an LDA lattice, $\sigma^2_{max} = p^{2(1-k/n)}/2\pi e$ if k is the dimension over $\mathbb{F}_p$ of the LDPC code.

We shall say, with a slight abuse of language, that a family of n-dimensional lattices Λ_n *achieves Poltyrev capacity* if, for every value of the channel noise variance smaller than σ^2_{max}, a random lattice of the family of big enough dimension n can be decoded with an arbitrarily small error probability.

B. The Main Result

Our main result reads:

Theorem 1. *There exists a Poltyrev-capacity-achieving family of LDA lattices $\Lambda_n = C_n + p\mathbb{Z}^n$ such that the parity-check matrix of the codes C_n has row and column degrees bounded from above by constants.*

One should ask what practical values of the constants we can achieve. Also of importance is the value of the prime number p relative to the lattice dimension n. When proving theoretical results on lattices obtained from Construction A, the size of p can be difficult to control and results in large values of p, namely $p > n$, that we would wish to avoid for practical decoding. This phenomenon occurs, for example, in [7] and [9]. We manage to achieve the Poltyrev limit with $p = n^\lambda$, $\lambda < 1$. Experiments reported in [4] tend to indicate that optimum results under iterative decoding are obtained for $p \approx n^{1/2}$: we have been able to confirm that for $p \approx n^{1/2}$ lattice decoding can go all the way to the Polyrev limit.

Furthermore, it is remarkable that the constants involved in the Theorem are definitely realistic; for example, for codes of rate $1/2$ and $p \approx n^{1/2}$, the required column degree of the parity-check matrix needed to guarantee that the LDA lattices achieve capacity is only 7. The detailed result leading to Theorem 1 and that enables one to compute constants and values of λ for $p = n^\lambda$ will be given in Theorem 3 below.

IV. Graph-theoretic Tools

We will require our LDPC codes to have Tanner graphs ([13], pag. 51) with expansion properties. In this section we state the, somewhat non-standard, expansion properties of bipartite random graphs that we need.

Let $\mathcal{G} = (V, P, E)$ be an undirected bipartite graph; $V \cup P$ is its set of vertices and E its set of edges. Later, V and P will stand for the sets of variable and check nodes respectively. Let $|V| = n$, $|P| = n(1-R)$, for some $0 < R < 1$. By now, parallel edges are accepted, that is, there might be two or more edges connecting the same two vertices.

If S is a subset of V, then we define $N(S)$ to be the *neighbourhood* of S, i.e. the set of vertices of P incident to a vertex of S. The neighbourhood $N(T)$ is similarly defined for a subset T of P.

From now on, we will consider only graphs with the following variation of the *biregularity* property: the number of edges incident to any single vertex of V (resp. P) has constant cardinality Δ_V (resp. Δ_P). Consequently, the neighbourhood of any single vertex of V (resp. P) has cardinality at most Δ_V (resp. Δ_P). If the graph has no parallel edges, these cardinalities are exactly Δ_V and Δ_P and the graph is biregular, according to the standard definition. Denote by $\mathcal{F}(n, R, \Delta_V, \Delta_P)$ the family of graphs just defined. Note that biregularity implies the relations:

$$n \times \Delta_V = n(1-R) \times \Delta_P \quad \text{and} \quad \Delta_P = \frac{\Delta_V}{(1-R)}. \tag{5}$$

We are interested in some particular expansion properties of this kind of graphs. Let $h(\cdot)$ be the *binary entropy function*: for all $0 < u < 1$, $h(u) = -u\log_2 u - (1-u)\log_2(1-u)$ and $h(1) = h(0) := 0$. Let α and A be two constants such that

$$1 < \alpha \leq A < \Delta_V - 1. \tag{6}$$

We say that a graph is (α, A)-*good* if there exist β and ε

satisfying

- $$\frac{1}{(1-R)} < \beta < \frac{2}{(1-R)}, \tag{7}$$
- $$0 < \varepsilon \leq \min\left\{\frac{(1-R)}{2A}, \frac{(1-R)(\Delta_V - A - 1)}{\Delta_V + R - 2}\right\}, \tag{8}$$
- $$\Delta_V > \frac{(1-R)h\left(\frac{A\varepsilon}{(1-R)}\right) + h(\varepsilon)}{h(\varepsilon) - \frac{A\varepsilon}{(1-R)}h\left(\frac{(1-R)}{A}\right)} \tag{9}$$

and for which

1. If $S \subseteq V$ and $|S| \leq \lceil \varepsilon n \rceil$, then $|N(S)| \geq A|S|$. (10)
2. If $S \subseteq V$ and $|S| \leq \left\lceil \frac{n(1-R)}{2\alpha} \right\rceil$, then $|N(S)| \geq \alpha|S|$. (11)
3. If $T \subseteq P$ and $|T| \leq \frac{n(1-R)}{2}$, then $|N(T)| \geq \beta|T|$. (12)

All three conditions above mean in quantitatively different ways that all "small enough" subsets of V or P have "big enough" sets of neighbours.

We have set the necessary notation to state the following lemma:

Lemma 2. *Let $n, \Delta_V \in \mathbb{N}$, with $\Delta_V \geq 2$. Let $0 < R < 1$ and let $\mathcal{G}$ be a graph in $\mathcal{F}(n, R, \Delta_V, \Delta_P)$, chosen uniformly at random in the family. Fix α and A satisfying (6). Furthermore, suppose that*

$$\Delta_V > \max\left\{\frac{(1-R) + h\left(\frac{1-R}{2\alpha}\right)}{h\left(\frac{1-R}{2\alpha}\right) - \frac{1}{2}h\left(\frac{(1-R)}{\alpha}\right)}, \frac{2\alpha^2 + 2\alpha + R - 2}{2\alpha - 1}\right\}. \tag{13}$$

Then

$$\lim_{n\to\infty} \mathcal{P}\{\mathcal{G} \text{ is not } (\alpha, A)\text{-good}\} = 0. \tag{14}$$

Due to lack of space, we do not provide here a proof of the previous lemma, that can be obtained with similar techniques to the ones used in [2]. Nevertheless, the proof has to be derived from scratch because the results of [2] are not precise enough for our purposes.

V. LDA Lattices Achieve Poltyrev Capacity

First, we precisely describe the family of LDA lattices we consider. Then we will state and sketch the proof of our main result, Theorem 3 below, which is the technical version of Theorem 1 presented at the end of Section III-B.

A. Random LDA Lattice Ensemble

Let $\mathcal{G}$ be any (α, A)-good graph, in the sense specified in the previous section. A priori, it may contain parallel edges. Let us identify them and call again $\mathcal{G}$ the new graph, with at most one edge between any two vertices. It is still an (α, A)-good bipartite graph and represents also the Tanner graph of an LDPC code. Let H be the *binary* parity-check matrix with Tanner graph $\mathcal{G}$. Let p be a prime number and let us associate a label to every edge of $\mathcal{G}$, independently of each other and chosen uniformly at random in the set $\{0, 1, 2, \ldots, p-1\}$ of the representatives of classes modulo p. Equivalently, we are choosing a parity-check matrix $\mathbf{H}$ of elements in $\mathbb{F}_p$. Let $C = C[n, k]_p \subseteq \mathbb{F}_p$ be the k-dimensional linear code over the finite field $\mathbb{F}_p$ with parity-check matrix $\mathbf{H}$. The actual Tanner graph of $\mathbf{H}$ is a subgraph of $\mathcal{G}$ which may differ from the whole graph $\mathcal{G}$ if some random coordinates are chosen to be equal zero. Notice also that, for the same reason, the rate k/n of C may be greater than R. The binary matrix H may be thought of the *skeleton* of the random matrix $\mathbf{H}$.

Every $i \in P$ represents a parity-check equation of C and a row of $\mathbf{H}$, while a $j \in V$ is a coordinate of a codeword $c \in C$. If Δ_V is small with respect to n, the code is an LDPC code and column (resp. row) weights are bounded from above by Δ_V (resp. Δ_P).

Let $\Lambda = C + p\mathbb{Z}^n$ be the random LDA lattice obtained by Construction A from C. We will investigate the behaviour of Λ for the transmission of information over the AWGN channel.

B. The Main Theorem

Theorem 3. *Let n be a positive integer number and let $0 < R < 1$. Let $p = n^\lambda$ be a prime number for some $\lambda > 0$ and let α, A and $3 - R < \Delta_V \in \mathbb{N}$ be three constants that obey conditions (6) and (13). If*

$$\lambda > \max\left\{\frac{1}{2(\alpha - 1 + R)}, \frac{3}{2(A - 1 + R)}\right\}, \tag{15}$$

then there exists a Poltyrev-capacity-achieving family of LDA lattices $\Lambda_n = C_n + p\mathbb{Z}^n$ such that the rate of C_n is at least R and the row degree in the parity-check matrix of C_n is at most $\Delta_V/(1-R)$.

To obtain the family of LDA lattices we will deal with, we first choose pairs $(n, p = n^\lambda)$. A typical value of λ that we target is $\lambda = 1/2$. We then choose (α, A) satisfying (15) and so as to minimize the lower bound (13) on Δ_V in Lemma 2. Lemma 2 then gives us the existence of an (α, A)-good graph which is then used to define the LDA ensemble of Section V-A. We show below that this particular ensemble of lattices achieves Poltyrev capacity.

C. Proof of Theorem 3 (Sketch)

We say that a function $f(n)$ is *asymptotical* to $g(n)$ (denoted $f(n) \sim g(n)$), if $\lim_{n\to\infty} f(n)/g(n) = 1$. In the proof of Theorem 3 we will deal with some spheres in $\mathbb{R}^n$ and we will have to count the number of integer points that they contain. We will use the following lemmas:

Lemma 4. *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*

$$N \leq \mathrm{Vol}\left(B_{n,c}(\rho)\right)\left(1 + \frac{\sqrt{n}}{2\rho}\right)^n. \tag{16}$$

Lemma 5. *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 $\xi > 0$, $\mathcal{P}\left\{\rho \leq \sigma\sqrt{n}\left(1 + \xi\right)\right\} \to 1$, as $n \to \infty$.*

These lemmas are classical and their proofs are omitted.

In order to prove Theorem 3, we evaluate the probability of decoding error, averaged over all LDA lattices built at random following the model described in Section V-A. So, let $\mathcal{G}$ be a bipartite graph chosen at random in $\mathcal{F}(n, R, \Delta_V, \Delta_P)$; we know by Lemma 2 that, if n is big enough, $\mathcal{G}$ is an (α, A)-good graph. Let $\Lambda = C + p\mathbb{Z}^n$ be a random LDA lattice associated to $\mathcal{G}$, and suppose we use Λ for communication.

First of all, because of the lattice symmetry, we can suppose that the point of Λ sent over the channel is the point 0. The AWG noise vector is $\eta = (\eta_1, \dots, \eta_n)$ and the channel output is $y = \eta$. Let us suppose that the noise variance per dimension is $\sigma^2 = \sigma_{\max}^2(1-\delta)^2 < \sigma_{\max}^2$, for some $0 < \delta < 1$.

Let us consider the sphere $\mathcal{B} := B_{n,y}(\sigma\sqrt{n}(1+\xi)) \subseteq \mathbb{R}^n$ centered at y, of radius $\sigma\sqrt{n}(1+\xi)$, with $\xi > 0$ chosen such that

$$\xi < \frac{\delta}{1-\delta}; \tag{17}$$

Lemma 5 states that, when n is very large, the point 0 is inside the sphere with probability tending to 1.

We first argue that

Claim 6. *With probability tending to* 1*, all non-zero vectors of* $p\mathbb{Z}^n$ *in* $\mathcal{B}$ *will be further away from the received vector* y *than the transmitted (zero) vector.*

Proof: (Sketch) Recall that we have $\sigma \approx p^{1-R}$. Therefore, with probability almost 1, all coordinates of y have magnitude not exceeding p^β with $1 - R < \beta < 1$. Every coordinate of y is therefore closer to 0 than any non-zero multiple of p.

We are therefore only concerned with ensuring that the decoder does not return $\hat{x} \not\equiv 0 \bmod p$. To this end let us introduce the random variable $\mathcal{N}$ that counts the number of lattice points inside the sphere and not belonging to $p\mathbb{Z}^n$. Our goal is to show that $\mathbb{E}[\mathcal{N}] \to 0$: this will prove the desired result.

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

$$X_x = \begin{cases} 1, & \text{if } x \in \Lambda \\ 0, & \text{if } x \notin \Lambda \end{cases} . \tag{18}$$

We have

$$\mathcal{N} = \sum_{x \in (\mathbb{Z}^n \cap \mathcal{B}) \smallsetminus p\mathbb{Z}^n} X_x \tag{19}$$

and

$$\mathbb{E}[\mathcal{N}] = \sum_{x \in (\mathbb{Z}^n \cap \mathcal{B}) \smallsetminus p\mathbb{Z}^n} \mathcal{P}\{x \in \Lambda\} \tag{20}$$

An integer point x belongs to Λ if and only if $\mathbf{H}x^T \equiv 0 \bmod p$. Remember that $\mathbf{H}$ is a sparse matrix so, if some of the coordinates of x are equal to 0 (in $\mathbb{F}_p$), some parity-check equations will be trivially satisfied, no matter what its random coefficients are. More precisely: let H_i be the i-th row of the binary skeleton matrix H of $\mathbf{H}$ (see Section V-A). We have that if the supports of x and H_i have empty intersection then $\mathcal{P}\{\mathbf{H}x^T \equiv 0 \bmod p\} = 1$. On the other hand, if the supports of x and H_i intersect in at least one coordinate, then we see that $\mathcal{P}\{\mathbf{H}x^T \equiv 0 \bmod p\} = 1/p$.

For a fixed x, let $T_x := \{i \mid \operatorname{Supp}(H_i) \cap \operatorname{Supp}(x) \neq \emptyset\}$. Notice that T_x is the neighbourhood in $\mathcal{G}$ of $\operatorname{Supp}(x)$. Now let $t = |T_x|$ be the number of parity-check equations that are not trivially satisfied by x: then $\mathcal{P}\{x \in \Lambda\} = p^{-t}$, because the coefficients that define the parity-check equations are chosen independently and therefore the events $\{x \text{ satisfies the } i\text{-th parity-check}\}$ are independent. This means that

$$\mathbb{E}[\mathcal{N}] = \sum_{x \in (\mathbb{Z}^n \cap \mathcal{B}) \smallsetminus p\mathbb{Z}^n} \frac{1}{p^t} = \sum_{t=1}^{n(1-R)} \sum_{\substack{x \in (\mathbb{Z}^n \cap \mathcal{B}) \smallsetminus p\mathbb{Z}^n \\ |T_x| = t}} \frac{1}{p^t} \tag{21}$$

In order to clarify our strategy, suppose for a moment that $|T_x| = n(1-R)$ for all x, which is false in general. The summation would become

$$\sum_{x \in (\mathbb{Z}^n \cap \mathcal{B}) \smallsetminus p\mathbb{Z}^n} \frac{1}{p^{n(1-R)}} \leq \frac{|\mathbb{Z}^n \cap \mathcal{B}|}{p^{n(1-R)}} \leq \tag{22}$$

$$\leq \frac{\operatorname{Vol}(\mathcal{B})}{p^{n(1-R)}} \left(1 + \frac{1}{2(1+\xi)\sigma}\right)^n \text{(by Lemma 4)} \sim \tag{23}$$

$$\sim \frac{1}{\sqrt{\pi n}} \left((1+\xi)\frac{\sqrt{2\pi e}\sigma}{p^{(1-R)}}\right)^n \left(1 + \frac{1}{2(1+\xi)\sigma}\right)^n, \tag{24}$$

where the asymptotic expression is obtained by Stirling's approximation of the volume of the sphere. One can show that the term in the right parentheses is at worst subexponential (i. e. asymptotical to $\exp(an^\mu)$, for some constants a and $0 < \mu < 1$); hence the dominating term in (24) is the central one. Our goal being to show that $\mathbb{E}[\mathcal{N}] \to 0$, we would be done, since (24) goes to 0 when n grows, because the base of the dominating exponential is smaller than 1 (recall that $\sigma_{\max} = p^{(1-R)}/\sqrt{2\pi\,\mathrm{e}}$ for an LDA lattice):

$$(1+\xi)\frac{\sqrt{2\pi e}\sigma}{p^{(1-R)}} < 1 \Leftrightarrow \sigma = \sigma_{\max}(1-\delta) < \frac{\sigma_{\max}}{1+\xi} \tag{25}$$

$$\Leftrightarrow \xi < \frac{\delta}{1-\delta}, \tag{26}$$

which is condition (17).

What happens in the more general case, when $|T_x| < n(1-R)$? A priori, the power of p in (24) is not sufficient to guarantee the convergence to 0; this clearly happens, for example, when $|T_x|$ is a constant with respect to n. We need a more detailed analysis, based on an efficient estimation of $|\{x \in (\mathbb{Z}^n \cap \mathcal{B}) \smallsetminus p\mathbb{Z}^n \mid |T_x| = t\}|$, which exploits the properties of (α, A)-good graphs.

We begin by cutting the summation in (21) into three different parts; given a small positive constant ε, such that condition (10) holds for $\mathcal{G}$, we will consider the three cases: $t < A\lceil\varepsilon n\rceil$, $A\lceil\varepsilon n\rceil \leq t < n(1-R)/2$ and $n(1-R)/2 < t \leq n(1-R)$.

One can see that, according to the choice of ε, $t < A\lceil\varepsilon n\rceil$ implies that $|\operatorname{Supp}(x)| \leq \lceil\varepsilon n\rceil$ and, because of (10), $t \geq A|\operatorname{Supp}(x)|$. As a consequence, recalling that $B_{n,y}(\rho)$ is the

n-dimensional sphere centered at y of radius ρ, $\forall t < A\lceil \varepsilon n \rceil$ we have:

$$\begin{aligned}
&|\{x \in (\mathbb{Z}^n \cap \mathcal{B}) \smallsetminus p\mathbb{Z}^n \mid |T_x| = t\}| \leq && (27)\\
&\leq |\{x \in (\mathbb{Z}^n \cap \mathcal{B}) \smallsetminus p\mathbb{Z}^n \mid |\operatorname{Supp}(x)| \leq t/A\}| \leq && (28)\\
&\leq \binom{n}{\lfloor t/A \rfloor} |\mathbb{Z}^{\lfloor t/A \rfloor} \cap B_{\lfloor t/A \rfloor, y}(\sigma\sqrt{n}(1+\xi))| \leq && (29)\\
&\leq n^{t/A} |\mathbb{Z}^{\lfloor t/A \rfloor} \cap \mathcal{C}_{\lfloor t/A \rfloor}(2\sigma\sqrt{n}(1+\xi))| \leq && (30)\\
&\leq n^{t/A}(2\sigma\sqrt{n}(1+\xi)+1)^{t/A}, && (31)
\end{aligned}$$

where $\mathcal{C}_{\lfloor t/A \rfloor}(2\sigma\sqrt{n}(1+\xi))$ is the $\lfloor t/A \rfloor$-dimensional cube of edge $2\sigma\sqrt{n}(1+\xi)$. Then,

$$\begin{aligned}
&\sum_{t=1}^{A\lceil \varepsilon n \rceil - 1} \sum_{\substack{x \in (\mathbb{Z}^n \cap \mathcal{B}) \smallsetminus p\mathbb{Z}^n \\ |T_x| = t}} \frac{1}{p^t} = && (32)\\
&= \sum_{t=1}^{A\lceil \varepsilon n \rceil - 1} \frac{|\{x \in (\mathbb{Z}^n \cap \mathcal{B}) \smallsetminus p\mathbb{Z}^n \mid |T_x| = t\}|}{p^t} \leq && (33)\\
&\leq \sum_{t=1}^{A\lceil \varepsilon n \rceil - 1} \frac{n^{t/A}(2\sigma\sqrt{n}(1+\xi)+1)^{t/A}}{p^t} < && (34)\\
&< \sum_{t=1}^{A\lceil \varepsilon n \rceil - 1} \left(D^{1/A} n^{(3/2A + \lambda(1-k/n)/A - \lambda)}\right)^t, && (35)
\end{aligned}$$

where D is a constant term. The last inequality holds because $p = n^\lambda$ and $\sigma < \sigma_{\max} = n^{\lambda(1-k/n)}/\sqrt{2\pi\,\mathrm{e}}$ (see (4)); k is the dimension of the code C over $\mathbb{F}_p$ and $k/n \geq R$). Now, (35) is a geometric series and its limit for n going to infinity is 0 if the exponent of n is negative; it is, thanks to hypothesis (15).

Very similar arguments show that

$$\begin{aligned}
&\lim_{n\to\infty} \sum_{t=A\lceil \varepsilon n \rceil}^{n(1-R)/2-1} \sum_{\substack{x \in (\mathbb{Z}^n \cap \mathcal{B}) \smallsetminus p\mathbb{Z}^n \\ |T_x| = t}} \frac{1}{p^t} = && (36)\\
&= \lim_{n\to\infty} \sum_{t=n(1-R)/2}^{n(1-R)} \sum_{\substack{x \in (\mathbb{Z}^n \cap \mathcal{B}) \smallsetminus p\mathbb{Z}^n \\ |T_x| = t}} \frac{1}{p^t} = 0. && (37)
\end{aligned}$$

Condition (11) and (12) are necessary to obtain (36) and (37) respectively, in the same way as (10) leads to (35).

Putting together what we have just shown and recalling (21), we get that $\lim_{n\to\infty} \mathbb{E}[\mathcal{N}] = 0$. This is enough to conclude that $\lim_{n\to\infty} \mathcal{P}\{x \in p\mathbb{Z}^n \mid x \in \mathcal{B} \cap \Lambda\} = 1$, which implies (by Claim 6) that $\lim_{n\to\infty} \mathcal{P}\{\hat{x} = 0\} = 1$.

This is the end of the proof of Theorem 3.

VI. Conclusion

Encouraged by the experimental results of [4], we have analysed the behaviour of LDA lattices for the transmission of information over the AWGN channel. More precisely, we have shown that there exists a Poltyrev-capacity-achieving family of LDA lattices associated to very sparse p-ary parity-check matrices. Specifically, the number of non-zero entries per matrix-row or per column is a (typically small) constant. This is in constrast to what is known about the binary LDPC case, for which families of codes with bounded-weight parity-check equations cannot achieve capacity. Ideally, we would like the constants under which we can guarantee optimal performance to be even smaller, and coincide with the constant $\Delta_V = 2$ used in [4] and that has experimentally also emerged as a good choice for non-binary LDPC codes used on binary-input channels ([17] and references therein). We do not believe the constants obtained here to be the best possible, though it is presently unclear to us whether Δ_V can be reduced all the way to $\Delta_V = 2$.

Finally, we note that the smallest values of p predicted to achieve capacity are in surprisingly close accordance with the optimal values of p obtained experimentally with decoders based on iterative decoding techniques [4]. This is arguably the most satisfying conclusion of the present contribution.

Acknowledgements

The authors would like to thank the French Research and Development Centre of Mitsubishi Electric (Rennes, France) for financial support.

References

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

[2] L. A. Bassalygo, M. S. Pinsker, "Complexity of an optimum nonblocking switching network without reconnections", in *Problems Inform. Transmission*, vol. 9, pp. 64–66, 1974.

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

[4] N. di Pietro, J. J. Boutros, G. Zémor and L. Brunel, "Integer low-density lattices based on construction A," *Proc. of the IEEE Inform. Theory Workshop (ITW), 2012*, pp.422-426, 3-7 Sept. 2012.

[5] N. di Pietro, J. J. Boutros, G. Zémor and L. Brunel, "New results on low-density integer lattices," *Information Theory and Applications Workshop (ITA), 2013*, 10-15 Feb. 2013.

[6] U. Erez, *Coding with known interference and some results on lattices for digital communication*, Ph.D. dissertation, Tel-Aviv Univ., 2002.

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

[8] U. Erez and G. Miller, "The ML decoding performance of LDPC ensembles over $\mathbb{Z}_q$," *IEEE Trans. on Inf. Theory*, vol. 51, no. 5, pp. 1871–1789, May 2005.

[9] 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.

[10] R. G. Gallager. *Low-density parity-check codes*, Ph.D. dissertation, Massachussets Institute of Technology Press, 1963.

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

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

[13] T. Richardson and R. Urbanke, *Modern coding theory*, Cambridge University Press, 2008.

[14] 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.

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

[16] 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.

[17] P. Suthisopapan, K. Kasai, A. Meesomboon, V. Imtawil and K. Sakaniwa, "Simple low-rate non-binary LDPC coding for relay channels," 2011, available at http://arxiv.org/abs/1108.3285.