From LDPC Codes to LDA Lattices: A Capacity Result

Nicola di Pietro
Texas A&M University at Qatar
c/o Qatar Foundation, Education City
P.O. Box 23874, Doha, Qatar
nicola.ndp@gmail.com

Gilles Zémor
IMB, Université de Bordeaux
351, cours de la Libération
F-33405, Talence Cedex, France
zemor@math.u-bordeaux.fr

Joseph J. Boutros
Texas A&M University at Qatar
c/o Qatar Foundation, Education City
P.O. Box 23874, Doha, Qatar
boutros@ieee.org

***Abstract*—This paper contains a summary of the arguments used to show how to achieve capacity of the AWGN channel with Voronoi constellations of LDA lattices under lattice decoding. No dithering is required in the tranmission scheme and capacity is achievable with LDA lattices whose parity-check matrices have constant row and column degrees. Although most of the technical details of the proof cannot be treated here, the reader is introduced to the fundamentals and novelties of the authors' approach to the problem. The random capacity-achieving LDA ensemble is presented and the definition of D-goodness of a bipartite graph is given. As an example of the power of this tool for investigating LDA lattices, a lemma about their minimum Hamming distance is provided.**

I. Introduction

This paper addresses the problem of communication over the Additive White Gaussian Noise (AWGN) channel with lattice codes and *lattice decoding*. This decoding strategy is suboptimal with respect to the maximum likelihood (ML) decoder, but its easier algorithmic nature makes it appealing for both theoretical analysis and practical implementation.

Erez and Zamir [11], [18] were the first to provide a full proof that capacity can be achieved in this context. Their solution is based on the Modulo-Lattice Additive Noise (MLAN) channel and Voronoi constellations with Construction A lattices. More recently, Belfiore and Ling [15] proposed a solution that involves a non-uniform distribution on the channel inputs and a probabilistically finite codebook.

Once the theoretical problem of non-constructively achieving capacity was solved, it left the place to the challenge of designing some constructive families of lattices adapted to iterative decoding with close-to-capacity performance. Most of the proposed families are inspired by LDPC and turbo codes [1], [21]–[23] and an interesting work about lattices based on polar codes exists [25]; the latter are also shown to be capacity-achieving.

The authors of this paper have contributed to this research domain with the introduction of two lattice families: the most recent are the *Generalized Low-Density (GLD) lattices* [3], [4]. They show great performance under iterative decoding and numerical simulations have been run in remarkably high dimensions (up to one million). Moreover, [10] provides a theoretical analysis about the possibility of achieving the so called Poltyrev capacity with infinite GLD-lattice constellations.

The second family is the one of *Low-Density Construction A (LDA) lattices*, to which this paper is entirely devoted. LDA lattices put together the strength of Construction A and LDPC codes, and their corresponding parity-check matrix is sparse. This is the key idea to reconduct their decoding to well-performing, implementable LDPC decoding algorithms. LDA lattices were referred to with this name by di Pietro *et al.* [6], who also proposed an efficient iterative decoding algorithm which yields very good performance. A theoretical analysis of the Poltyrev-capacity-achieving qualities of infinite LDA constellations was carried on by the same authors [7], [8], whereas the "goodness" properties of LDA lattices are studied in [24]. The problem of attaining capacity of the AWGN channel with finite LDA constellations was approached and solved in [9]. The main purpose of this work is to recall and partially improve the latter result. Defoliated of all technical hypotheses, our main accomplishment can be stated as follows:

Theorem 1. *For every* $\mathrm{SNR} > 1$*, there exists a random ensemble of LDA lattices that achieves capacity of the AWGN channel under lattice encoding and decoding.*

Notice that the restriction $\mathrm{SNR} \leq 1$ is not very constraining: for very small SNR there is no need of using lattice constellations for communications over the AWGN channel and classical coded binary modulations are already known to work in a more than satisfactory way [20].

For lack of space, this paper cannot contain the technical proofs that lead to our result. Its aim is only to depict the strategies and the theoretical tools that underlie them. A longer and detailed version of this paper will be published soon and a substantial part of this work is contained in [9].

A. Structure of the paper

Section II recalls some definitions about lattice constellations. Section III presents the D-goodness of bipartite graphs. Our LDA ensemble is depicted in Section IV, which also describes the information transmission scheme. Section V is a summary of the main features of the proof that LDA lattices are capacity-achieving. It also contains a lemma on their minimum Hamming distance.

B. Notation

A crucial parameter of our analysis is the prime number p that underlies Construction A. We are interested in describing its growth as a function of the lattice dimension n. For this reason, p is defined as $p = n^\lambda$ for some positive constant λ. Clearly, this is a slight abuse of notation that means, without any undesired consequence, that $p = p(\lambda)$ is the closest prime number to n^λ.

II. Lattice constellations for the AWGN channel

We assume that the reader is familiar with lattices as mathematical objects and constellations for the transmission of information; excellent references are [5], [26]. We repeat here some definitions, mainly for fixing our notation.

We exclusively deal with real lattices, i.e. discrete additive subgroups of the Euclidean vector space $\mathbb{R}^n$. Also, we suppose that they are always full-rank and n indicates both the lattice dimension and the dimension of the Euclidean space. The *Voronoi region* of a point $\mathbf{x}$ of a lattice Λ is the set

$$\mathcal{V}(\mathbf{x}) = \{\mathbf{y} \in \mathbb{R}^n : \|\mathbf{y} - \mathbf{x}\| \leq \|\mathbf{y} - \mathbf{z}\|,\ \forall \mathbf{z} \in \Lambda \setminus \{\mathbf{x}\}\}.$$

We call Voronoi region of the lattice, and denote it $\mathcal{V}(\Lambda)$, the Voronoi region of $\mathbf{0}$. The *volume* of Λ is $\mathrm{Vol}(\Lambda) = \mathrm{Vol}\left(\mathcal{V}(\Lambda)\right)$ and its *effective radius* is the radius of the ball whose volume is equal to $\mathrm{Vol}(\Lambda)$. Consider two lattices Λ and Λ_f; we say that they are *nested* if $\Lambda \subseteq \Lambda_f$. We call *Voronoi constellation* [12] of two nested lattices the lattice code $\mathcal{C} = \Lambda_f \cap \mathcal{V}(\Lambda)$. In this context, Λ is often called the *shaping lattice* and Λ_f the *fine lattice*. We can deduce that the Voronoi constellation has cardinality $\mathrm{Vol}(\Lambda)/\mathrm{Vol}(\Lambda_f)$; its elements are the represantatives of the congruence classes of Λ_f/Λ with minimum norm.

Definition 1. *Let $C = C[n,k]_p \subseteq \mathbb{F}_p^n$ be a p-ary linear code of length n and dimension k and let us naturally embed C into $\mathbb{Z}^n$. If H is a parity-check matrix of C, we say that the lattice $\Lambda \subseteq \mathbb{R}^n$ is built with* Construction A *from C when*

$$\Lambda = C + p\mathbb{Z}^n = \{\mathbf{x} \in \mathbb{Z}^n : H\mathbf{x}^T \equiv \mathbf{0}^T \bmod p\}.$$

H is called a parity-check matrix *of Λ as well. Λ is called a* Low-Density Construction A *(or briefly* LDA*) lattice if it is built with Construction A from an LDPC code.*

We recall that LDPC codes are linear codes whose parity-check matrix has a great majority of zero entries [14], [20].

Definition 2. *Let $\mathbf{C}$ be the capacity of our channel. A family of lattice codes is* capacity-achieving *if for every $\delta > 0$ and for every $\varepsilon > 0$ there exists a lattice code in the family with rate at least $\mathbf{C} - \delta$ and decoding error probability at most ε.*

Let $\mathbf{x}$ be the AWGN channel input and let $\mathbf{y} = \mathbf{x} + \mathbf{w}$ be its random output, then the *Wiener coefficient* is $\alpha = \arg\min_{\beta \in \mathbb{R}} \mathbb{E}[\|\mathbf{x} - \beta\mathbf{y}\|^2]$. The minimum in the previous formula is usually called *Minimum Mean Squared Error* and the Wiener coefficient is also called *MMSE coefficient*. It is well known that, if $\mathbb{E}[\|\mathbf{x}\|^2] = nP$ and $w_i \sim \mathcal{N}(0, \sigma^2)$ for every i, then $\alpha = \frac{P}{P+\sigma^2}$. We denote $Q_\Lambda(\cdot)$ the *quantizer* of a lattice Λ associated with $\mathcal{V}(\Lambda)$: $Q_\Lambda(\mathbf{y}) = \arg\min_{\mathbf{x} \in \Lambda} \|\mathbf{y} - \mathbf{x}\|$.

Definition 3. *A* MMSE lattice decoder *returns $\hat{\mathbf{x}} = Q_\Lambda(\alpha\mathbf{y})$ as the channel input guess.*

Multiplication by α is essential for us to achieve capacity with a lattice decoder, as it was for Erez and Zamir [11], [18]. We will give a geometrical explanation of this in Section V.

III. Expansion properties of bipartite graphs

Let $\mathcal{G} = (V_L, V_R, E)$ be an undirected bipartite graph; $V_L \cup V_R$ is its set of (left and right) vertices and E its set of edges. Let $|V_L| = n$ and $|V_R| = fn$, for some constant non-zero fraction $f \in \mathbb{Q}$ (that can be bigger than 1). If S is a subset of vertices of a graph $\mathcal{G}$, its *neighborhood* $N(S)$ is defined as the set of vertices of the graph that are incident to a vertex of S. In a bipartite graph, $N(S) \subseteq V_R$ for every $S \subseteq V_L$ and, vice versa, $N(T) \subseteq V_L$ for every $T \subseteq V_R$. We will consider only *biregular* graphs: the neighborhood of any vertex of V_R (resp. V_L) has cardinality exactly Δ (resp. $f\Delta$). Let us denote by $\mathcal{F}(n, f, \Delta)$ the family of graphs just defined.

Definition 4. *Let D be a positive constant. A graph of $\mathcal{F}(n, f, \Delta)$ is* D-good from left to right *if*

$$\forall S \subseteq V_L \text{ s.t. } |S| \leq \frac{n}{D+1},\ \text{then } |N(S)| \geq fD|S|. \quad (1)$$

Analogously, it is D-good from right to left *if*

$$\forall T \subseteq V_R \text{ s.t. } |T| \leq \frac{fn}{D+1},\ \text{then } |N(T)| \geq \frac{D|T|}{f}.$$

We say that a graph of $\mathcal{F}(n, f, \Delta)$ is D-good *if it is good both from left to right and from right to left.*

Lemma 1. *Let $\mathcal{G}$ be a graph chosen uniformly at random in $\mathcal{F}(n, f, \Delta)$, and let $h(\cdot)$ be the binary entropy function. If $D \geq 1$ and*

$$\Delta > \max\left\{ \left(1 + \frac{1}{f}\right)\left(1 - \frac{Dh\left(\frac{1}{D}\right)}{(D+1)h\left(\frac{1}{D+1}\right)}\right)^{-1}, D^2 + \frac{1}{f}, \frac{D^2}{f} + 1 \right\},$$

then $\lim_{n\to\infty} \mathcal{P}\{\mathcal{G} \text{ is } \ D\text{-good}\} = 1$.

The proof of the previous lemma uses the same main ideas that Bassalygo applies in [2]. The reader may also be interested in comparing this lemma with Theorem 8.7 of [20, p. 431] and reading therein about the construction of *expander codes*.

The D-goodness of the Tanner graphs [20] associated with LDA lattices plays an essential role in the proof of Lemma 3 and Theorem 2. The way it is exploited to adapt some random-coding arguments to the LDA case is definitely one of the most novel tools of this work.

IV. The random LDA ensemble and the transmission scheme

Our lattice codes are given by Voronoi constellations of nested LDA lattices. First, let us fix two constants R and R_f such that $0 < R < R_f < 1$. Also, let us fix the constant

Δ_P, which is the number of non-zero entries per row of the LDPC parity-check matrices. Our random shaping lattice Λ is the LDA lattice generated by the following p-ary parity-check matrix of dimension $n(1-R)\times n$:

$$\mathbf{H}=\left(\frac{\mathbf{H}'}{\mathbf{H}_f}\right).$$

Its lower submatrix $\mathbf{H}_f$, formed by its last $n(1-R_f)$ rows, is the parity-check matrix of the random LDA fine lattice Λ_f. By construction, we impose that $\mathbf{H}$ has exactly Δ_P random entries per row and $\Delta_V=\Delta_P(1-R)$ random entries per column. Also, each column of $\mathbf{H}_f$ has exactly $\Delta_P(1-R_f)$ random entries per column. All the other entries are deterministically fixed to 0 and their position is fixed once for all, as well. The random entries of $\mathbf{H}$ are i.i.d. random variables with equiprobable values in $\mathbb{F}_p$. Of course, $\Lambda\subseteq\Lambda_f$ and the random Voronoi constellation is given by Λ_f/Λ. Lemma 1 guarantees that the Tanner graph associated with the fine LDA lattice Λ_f is D-good for every $D\geq 1$ such that:

$$\Delta_P>\max\left\{\frac{2-R_f}{1-R_f}\left(1-\frac{Dh\left(\frac{1}{D}\right)}{(D+1)h\left(\frac{1}{D+1}\right)}\right)^{-1},\ \frac{D^2}{1-R_f}+1\right\}. \tag{2}$$

It can be shown that (2) suffices to claim that the graph associated with the shaping LDA lattice Λ is D-good, too.

The points of the LDA-lattice constellation are indexed by the $p^{n(R_f-R)}$ different syndromes of the form $(s_1,s_2,\ldots,s_{n(R_f-R)},0,\ldots,0)$ associated with the matrix $\mathbf{H}$, with $s_i\in\mathbb{F}_p$. More explicitly, let $\mathbb{F}_p^{(R_f-R)}$ be the set of the messages; the bijection

$$\begin{aligned}\varphi\colon \Lambda_f\cap\mathcal{V}(\Lambda)&\to\mathbb{F}_p^{n(R_f-R)}\\ \mathbf{x}&\mapsto\mathbf{H}'\mathbf{x}^T \bmod p\end{aligned}$$

makes a constructive encoding possible. Our transmission scheme works as follows: the sender pairs up a message and a syndrome and transmits $\mathbf{x}$, the corresponding constellation point obtained via φ^{-1}, over the AWGN channel. The receiver gets the channel output $\mathbf{y}=\mathbf{x}+\mathbf{w}$; by MMSE lattice decoding of $\mathbf{y}$, he gets $\hat{\mathbf{x}}=Q_{\Lambda_f}(\alpha\mathbf{y})$. The decoded message is the one associated with $\varphi(\hat{\mathbf{x}})$. For every $\mathbf{s}'\in\mathbb{F}_p^{n(R_f-R)}$, let $\mathbf{x}\in\Lambda_f$ be any solution of the linear system $H'\mathbf{x}^T\equiv\mathbf{s}'^T \bmod p$. Then, $\varphi^{-1}(\mathbf{s}')=\mathbf{x}-Q_\Lambda(\mathbf{x})$ and encoding can be done substantially thanks to a lattice decoder, too.

Notice that our scheme differs from the others traditionally proposed in the literature about lattices. We do not transform the AWGN into a MLAN channel [11], [18] and, in particular, we do not assume that the sender and the receiver share the common randomness known as *dither*. The possibility of avoiding dithering in this context had already been pointed out by Forney [13], but no proof had ever been provided, to the best of our knowledge. Furthermore, we keep an a priori uniform disitribution on the lattice constellations and do not introduce the random Gaussian coding proposed in [15], [25].

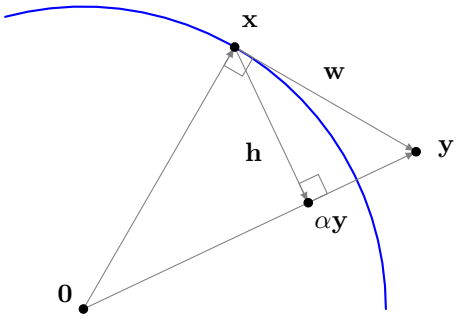

Figure 1. Geometric interpretation: $\mathbf{x}$ is the channel input; $\|\mathbf{x}\|^2=nP$. The AWG noise is $\mathbf{w}$, with norm $\|\mathbf{w}\|^2=n\sigma^2$. The channel output is $\mathbf{y}=\mathbf{x}+\mathbf{w}$. The Wiener coefficient $\alpha=\frac{P}{P+\sigma^2}$ is used for the MMSE scaling of $\mathbf{y}$ and $\alpha\mathbf{y}$ is the lattice decoder input. $\mathbf{h}$ is the effective noise after MMSE scaling.

V. Overview and discussion on our proof

We give here a general description of our proof, by the means of a heuristic argument that does not take into account all the probabilistic and asymptotic aspects of the rigorous demonstration. With the use of the adverb "typically", we will mean "with probability tending to 1 when n tends to infinity".

Our result is based on the following facts: first, the points of the LDA constellation typically lie very close to the surface of a sphere whose radius is essentially the effective radius of the shaping LDA lattice. Then, the AWG noise is typically almost orthogonal to the sent vector, in the sense that, if $\mathbf{x}$ is our transmitted constellation point and $\mathbf{w}$ is the noise, then $|\mathbf{x}\mathbf{w}^T|$ is "small enough". Furthermore, the "effective noise" due to MMSE scaling and the sent point are not decorrelated. Consequently, it is not possible to show that MMSE lattice decoding works independently of the sent point. Nevertheless, Theorem 2 is based on the fact that the number of points for which this does not happen is not big enough to perturb the average error probability of the family. Finally, we look for lattice points inside a sphere centered at the MMSE-scaled channel output with a very specific radius. Basically, there will be no decoding error if the only lattice point in this *decoding sphere* is the transmitted one.

Now, let us try to understand the geometric sense of the elements that we have just listed. So, suppose that the channel input is a point $\mathbf{x}$ whose norm is fixed to be $\|\mathbf{x}\|=\sqrt{nP}$, for some $P>0$ (Lemma 3 specifies this value). Suppose also that $\mathbf{x}\mathbf{w}^T=0$ (this is a stronger hypothesis than what the actual noise allows to assume, but it helps to understand the more general scenario); if $\mathbf{y}=\mathbf{x}+\mathbf{w}$ is the channel output, then $\|\mathbf{y}\|^2=\|\mathbf{x}\|^2+\|\mathbf{w}\|^2$. We call σ^2 the Gaussian noise variance per dimension. Basic Euclidean geometry (see Figure 1) tells us that multiplying $\mathbf{y}$ by the Wiener coefficient α helps in bringing the decoder input closer to the sent point.

The receiver decodes $\alpha\mathbf{y}$ and there is no decoding error if the closest lattice point to $\alpha\mathbf{y}$ is $\mathbf{x}$. We can show that this typically happens if $\mathrm{SNR}=\frac{P}{\sigma_2}>1$ and $\|\alpha\mathbf{y}-\mathbf{x}\|^2<np^{2(1-R_f)}/(2\pi e)$. Notice that the latter bound defines what we called the *decoding sphere* before. It concretely means

that our constellation tolerates an effective noise after MMSE scaling whose variance per dimension is less than $\sigma^2_{\mathrm{Pol}} = p^{2(1-R_f)}/(2\pi e)$. This value is far from being fortuitous: it is precisely the so called *Poltyrev limit* or *Poltyrev capacity* of the random infinite constellation Λ_f [9], [16], [19]. We intuitively understand that this is the good condition on the maximum bearable noise, admitting that no problem comes from the fact that the effective noise and the sent point $\mathbf{x}$ are not decorrelated (this would be the case if we used dithering).

The condition on the signal-to-noise ratio can be simply understood with the following argument: let us call $\mathbf{h} = \alpha\mathbf{y} - \mathbf{x}$ and suppose that it takes the maximum value allowed by the Poltyrev limit: $\|\mathbf{h}\|^2 = n\sigma^2_{\mathrm{Pol}}$ (which also can be shown to correspond to the rate of the constellation that equals capacity). If we want good decoding, we need $\alpha\mathbf{y}$ to be closer to $\mathbf{x}$ than to $\mathbf{0}$, because the latter deterministically belongs to any lattice; in other terms, it is necessary that $\|\alpha\mathbf{y}\|^2 > \|\mathbf{h}\|^2$. An easy computation based on Figure 1 shows that this holds true if and only if $P > \sigma^2$ or, equivalently, $\mathrm{SNR} > 1$. This gives a first explanation why we do not treat the case $\mathrm{SNR} \leq 1$.

We prove that MMSE decoding works by a probabilistic approach, showing that almost always the only lattice point inside the *decoding sphere* $\mathcal{B}$ centered at $\alpha\mathbf{y}$ is the sent point $\mathbf{x}$. The average argument that we apply leads to the estimation of (a more elaborated version of) the following sum: $\sum_{\mathbf{z}\in\mathcal{B}\setminus\{\mathbf{x}\}} \mathcal{P}\{\mathbf{z} \in \Lambda_f \mid \mathbf{x} \in \Lambda_f\}$. Decoding without errors corresponds to a sum which converges to 0. The easiest situation to deal with is when the two events $\{\mathbf{z} \in \Lambda_f\}$ and $\{\mathbf{x} \in \Lambda_f\}$ are independent, but they may not be, because the multiplication by α adds some correlation between $\mathbf{x}$ and the effective noise $\alpha\mathbf{y} - \mathbf{x}$. Erez and Zamir's dithering technique is a method to eliminate this correlation. In our case, there is a priori some $\mathbf{x}$ for which the probability in the previous sum turns out to be "bigger" than desired, while at the same time we need to show that the whole sum is "small". The originality of our analysis consists of deducing that the proportion of this kind of points in the constellation is very small.

Some considerable difficulties in estimating $\mathcal{P}\{\mathbf{z} \in \Lambda_f \mid \mathbf{x} \in \Lambda_f\}$ arise because the parity-check matrices of LDA lattices are sparse. These difficulties have to be treated with much care and the D-goodness of the associated Tanner graphs is of great help. As an example of the techniques used in the proofs of Lemma 3 and Theorem 2, we propose the following lemma:

Lemma 2. *Let Λ_f be our random n-dimensional LDA fine lattice with $p = n^\lambda$, $D > (1-R_f)^{-1}$, and $\lambda > (D(1-R_f)-1)^{-1}$. Suppose also that* (2) *holds true. For every $\mathbf{x} \in \Lambda_f$, let $w(\mathbf{x}) = |\{i : x_i \neq 0\}|$. Then, for every constant $\delta < D(1-R_f)/(D+1)$,*

$$\lim_{n\to\infty} \mathcal{P}\left\{\mathbf{x} \in \Lambda_f \setminus p\mathbb{Z}^n \middle| w(\mathbf{x}) \leq \delta n\right\} = 0.$$

Hence, the minimum Hamming distance of the LDPC code underlying Λ_f is typically lower bounded by $\frac{D(1-R_f)}{(D+1)}n - o(1)$.

Proof: Let $\Lambda_f = C_f + p\mathbb{Z}^n$, where C_f is the random LDPC code defined by $\mathbf{H}_f$. For $\mathbf{x} \in \mathbb{F}_p^n \setminus \{\mathbf{0}\}$, consider the random variables

$$X_{\mathbf{x}} = \begin{cases} 1, & \text{if } \mathbf{x} \in C_f \\ 0, & \text{otherwise} \end{cases} \quad \text{and} \quad X = \sum_{\substack{\mathbf{x}\in\mathbb{F}_p^n \\ 1\leq w(\mathbf{x})\leq\delta n}} X_{\mathbf{x}}.$$

Thus, X counts the number of points of C_f of Hamming weight $1 \leq w(\mathbf{x}) \leq \delta n$. To conclude, it suffices to prove that

$$\lim_{n\to\infty} \mathbb{E}[X] = \lim_{n\to\infty} \sum_{\substack{\mathbf{x}\in\mathbb{F}_p^n \\ 1\leq w(\mathbf{x})\leq\delta n}} \mathcal{P}\{\mathbf{x} \in C_f\} = 0.$$

We will split the previous sum into two smaller sums and show that both of them converge to 0.

Case 1: $w(\mathbf{x}) \leq n/(D+1)$**.** If $\mathrm{Supp}(\mathbf{x}) = \{x_j \neq 0\}$ and $N(\mathrm{Supp}(\mathbf{x}))$ is its neighborhood in the Tanner graph associated with $\mathbf{H}_f$, notice that

$$\mathcal{P}\{\mathbf{x} \in C_f\} = \mathcal{P}\left\{\mathbf{H}_f\mathbf{x}^T \equiv \mathbf{0}^T \bmod p\right\} \overset{\text{(a)}}{\leq} \left(\frac{1}{p}\right)^{|N(\mathrm{Supp}(\mathbf{x}))|} \overset{\text{(b)}}{\leq} \left(\frac{1}{p}\right)^{D(1-R_f)|\,\mathrm{Supp}(\mathbf{x})|};$$

(a) comes from the fact that for every parity-check equation $\mathbf{h}_i$ with $i = 1, 2, \ldots, n(1-R_f)$, the events $\{\mathbf{h}_i\mathbf{x}^T \equiv \mathbf{0}^T \bmod p\}_i$ are independent; moreover, parity-check equations connected to only-0 variables are trivially satisfied. (b) is a consequence of the D-goodness of the Tanner graph: simply apply (1) to $S = \mathrm{Supp}(\mathbf{x})$ with $f = 1 - R_f$. Therefore,

$$\begin{aligned}
&\sum_{\substack{\mathbf{x}\in\mathbb{F}_p^n \\ 1\leq w(\mathbf{x})\leq n/(D+1)}} \mathcal{P}\{\mathbf{x} \in C_f\} \\
&\qquad \leq \sum_{w=1}^{\lfloor n/(D+1)\rfloor} \sum_{\substack{\mathbf{x}\in\mathbb{F}_p^n \\ w(\mathbf{x})=w}} \left(\frac{1}{p}\right)^{D(1-R_f)w} \\
&\qquad \leq \sum_{w=1}^{\lfloor n/(D+1)\rfloor} \binom{n}{w} \left(\frac{p-1}{p^{D(1-R_f)}}\right)^w \\
&\qquad \leq \sum_{w=1}^{\lfloor n/(D+1)\rfloor} \left(n^{1-\lambda(D(1-R_f)-1)}\right)^w \to 0,
\end{aligned}$$

because of the conditions on λ and D.

Case 2: $n/(D+1) < w(\mathbf{x}) \leq \delta n$**.** Applying (1) to any $S \subseteq \mathrm{Supp}(\mathbf{x})$ of size $n/(D+1)$, the D-goodness of the Tanner graph implies that $|N(\mathrm{Supp}(\mathbf{x}))| \geq \frac{D(1-R_f)}{D+1}n$. Therefore,

$$\begin{aligned}
&\sum_{\substack{\mathbf{x}\in\mathbb{F}_p^n \\ n/(D+1)<w(\mathbf{x})\leq\delta n}} \mathcal{P}\{\mathbf{x} \in C_f\} \\
&\qquad \leq \sum_{w=\lfloor n/(D+1)\rfloor+1}^{\lfloor\delta n\rfloor} \binom{n}{w}(p-1)^w \left(\frac{1}{p}\right)^{\frac{D(1-R_f)n}{(D+1)}} \\
&\qquad \leq n2^n p^{n\left(\delta - \frac{D(1-R_f)}{(D+1)}\right)} \to 0,
\end{aligned}$$

because $\delta < D(1-R_f)/(D+1)$ by hypothesis. ∎

A. Our two main results

The next lemma formally states that our Voronoi LDA constellation points have a very precise typical norm or, similarly, that our LDA shaping lattice has a "spherical" Voronoi region.

Lemma 3. *Consider a non-zero syndrome* $\mathbf{s}$ *associated with a constellation point:* $\mathbf{s} = (s_1, s_2, \ldots, s_{n(R_f-R)}, 0, \ldots, 0)$. *Suppose that* $p = n^\lambda$ *for some* $\lambda > 0$ *and let* $0 < \omega < 1$. *Fix the constant* D *to be* $D > \max\left\{(1-R_f)^{-1}, 2\right\}$ *and suppose that* (2) *holds true. Let* ρ_{eff} *denote the effective radius of the shaping LDA lattice* Λ. *If* $\mathbf{x}$ *is the random LDA constellation point whose syndrome is* $\mathbf{s}$ *and if*

$$\lambda > \max\left\{\frac{1}{D(1-R_f)-1}, \frac{1}{2R}, \frac{1}{1-R}, \frac{1}{D-2}, \left(1-\frac{1}{D^2-1}-\frac{1}{D(1-R)}\right)^{-1}\right\},$$

then

$$\lim_{n\to\infty} \mathcal{P}\left\{\rho_{\text{eff}}\left(1-\frac{1}{n^\omega}\right) \le \|\mathbf{x}\| \le \rho_{\text{eff}}\left(1+\frac{1}{n^\omega}\right)\right\} = 1.$$

Theorem 2. *Suppose that* $1 > R_f > R > \frac{1}{2}$. *Fix* $D > (1-R_f)^{-1}$ *and* Δ_P *that satisfies* (2). *If* $p = n^\lambda$, *with*

$$\lambda > \max\left\{\frac{1}{D(1-R_f)-1}, \frac{1}{1-R_f}, \left(1-\frac{1}{D^2-1}-\frac{1}{D(1-R_f)}\right)^{-1}\right\},$$

then the random ensemble of nested LDA lattices presented in Section IV achieves capacity of the AWGN channel under MMSE lattice decoding, when $\text{SNR} > 1$.

We emphasize the fact that Δ_P, D, R, and R_f are constant, therefore the parity-check matrices associated with our LDA lattices have constant row and column degree. For binary LDPC codes to achieve capacity of the binary symmetric channel, logarithmic row degrees are required [14], [17]. Surprisingly, in our LDA scenario this hypothesis can be relaxed.

VI. Conclusion

We have stated the capacity-achieving properties of a particular ensemble of LDA lattices based on non-binary LDPC lattices. Our solution is innovative because it does not require the tools of the MLAN channel and of dithering. Furthermore, it is based on Voronoi lattice constellations and we do not need to introduce Gaussian coding, keeping an a priori uniform distribution over the lattice constellation.

Also, the row and column degree of the parity-check matrices that underlie our construction are reasonably small constants. The Tanner graphs associated with these matrices have some particular expansion properties that, qualitatively speaking, say that all "small enough" sets of nodes have "big enough" neighborhoods. These properties turn out to be one of the most important theoretical pillars of our analysis.

Acknowledgment

The research work presented in this paper on LDA lattices is supported by QNRF, a member of Qatar Foundation, under NPRP project 6-784-2-329.

References

[1] I.-J. Baik and S.-Y. Chung, "Irregular low-density parity-check lattices," in *Proc. ISIT*, Toronto, Canada, 2008, pp. 2479-2483.

[2] L. A. Bassalygo, "Asymptotically optimal switching circuits," *Problems of Inf. Transmission*, vol. 17, no. 3, pp. 206-211, 1981.

[3] J. J. Boutros, N. di Pietro, and N. Basha, "Generalised low-density (GLD) lattices," in *Proc. ITW*, Hobart, Australia, 2014, pp.15-19.

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

[5] J. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*. 3rd ed., New York (NY), USA: Springer-Verlag, 1999.

[6] N. di Pietro, J. J. Boutros, G. Zémor, and L. Brunel, "Integer low-density latices based on Construction A," in *Proc. ITW*, Lausanne, Switzerland, 2012, pp.422-426.

[7] N. di Pietro, J. J. Boutros, G. Zémor, and L. Brunel, "New results in low-density integer lattices," in *Proc. ITA Workshop*, San Diego (CA), USA, 2013, pp.1-6.

[8] N. di Pietro, J. J. Boutros, G. Zémor "New results on Construction A lattices based on very sparse parity-check matrices," in *Proc. ISIT*, 2013, Istanbul, Turkey, pp.1675-1679.

[9] N. di Pietro, "On infinite and finite lattice constellations for the additive white Gaussian noise channel," Ph.D. dissertation, Inst. de Math., Univ. de Bordeaux, Bordeaux, France, 2014.

[10] N. di Pietro, N. Basha, and J. J. Boutros, "Non-binary GLD codes and their lattices," in *Proc. ITW*, Jerusalem, Israel, 2015, pp.1-5.

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

[12] G. D. Forney, Jr., "Multidimensional constellations. II. Voronoi constellations," *IEEE J. Sel. Areas Commun.*, vol. 7, no. 6, pp. 941-958, Aug. 1989.

[13] G. D. Forney, Jr., "On the role of MMSE estimation in approaching the information-theoretic limits of linear Gaussian channels: Shannon meets Wiener," in *Proc. Commun., Control, and Computing, 2003 41st Annu. Allerton Conf. on*, Monticello (IL), USA, 2003, pp. 1-14.

[14] R. G. Gallager, *Low-density parity-check codes*. Cambridge (MA), USA: MIT Press, 1963.

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

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

[17] D. J. C. MacKay, "Good error correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 399-431, Mar. 1999.

[18] O. Ordentlich and U. Erez, "A simple proof for the existence of "good" pairs of nested lattices," in *Proc. IEEEI*, Eilat, Israel, 2012, pp. 1-12.

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

[20] T. Richardson and R. Urbanke, *Modern coding theory*. New York, USA: Cambridge University Press, 2008

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

[22] A. Sakzad, M.-R. Sadeghi, and D. Panario, "Turbo lattices: construction and error decoding performance," Aug. 2011. Available: http://arxiv.org/abs/1108.1873

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

[24] S. Vatedka and N. Kashyap, "Some "goodness" properties of LDA lattices," in *Proc. ITW*, Jerusalem, Israel, 2015, pp. 1-5.

[25] Y. Yan, L. Liu, C. Ling, and X. Wu, "Construction of capacity-achieving lattice codes: polar lattices," Nov. 2014. Available: http://arxiv.org/abs/1411.0187

[26] R. Zamir, *Lattice coding for signals and networks*. Cambridge, United Kingdom: Cambridge University Press, 2014.