Integer Low-Density Lattices based on Construction A

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

*Mitsubishi Electric R&D Centre Europe, Rennes, France
Email: {n.dipietro, l.brunel}@fr.merce.mee.com
†Institut de Mathématiques, UMR 5251, Université Bordeaux 1, 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 describe a new family of integer lattices built from construction A and non-binary LDPC codes. An iterative message-passing algorithm suitable for decoding in high dimensions is proposed. This family of lattices, referred to as LDA lattices, follows the recent transition of Euclidean codes from their classical theory to their modern approach as announced by the pioneering work of Loeliger (1997), Erez, Litsyn, and Zamir (2004-2005). Besides their excellent performance near the capacity limit, LDA lattice construction is conceptually simpler than previously proposed lattices based on multiple nested binary codes and LDA decoding is less complex than real-valued message passing.**

I. Introduction

Coding over finite alphabet for the AWGN channel has undergone a huge effort to achieve capacity with efficient decoding, and while this quest is arguably reaching its conclusion, the similar problem for infinite alphabet coding has received much less attention and has been picking up some momentum only lately. It has been known for some time that lattices, the equivalent of linear codes, achieve (non-constructively) capacity [13] [5] [6], but not many practical lattice coding schemes have been put forward that have a chance of approaching capacity. For large dimensions, the more promising lattices are inspired by LDPC coding. Among existing propositions we find [17] [2] [18] that use lattices with an underlying binary code structure: the binary code is chosen to be amenable to iterative decoding techniques, i.e. it belongs to the LDPC or turbo-code families. We also find Sommer et al.'s Low-Density Lattice Codes (LDLCs) that do not have an embedded binary code, but are constructed directly so as to be decodable by a scheme inspired by the LDPC techniques.

In the present work we try a somewhat different approach to constructing efficiently decodable families of lattices. We again rely on an underlying finite-alphabet code structure, but depart from the binary alphabet and use LDPC codes over non-binary alphabets. We shall call upon the celebrated construction A technique [4] to obtain lattices from linear codes over finite alphabets. Note that construction A is not in itself a very restrictive scheme for lattice construction since it has been used, relying on codes over large alphabets, to produce (non-constructively) capacity-achieving lattices [5]. Construction A also yields some of the best asymptotic sphere-packing densities [7].

In principle, non-integer lattices could be constructed with the scheme presented below: we shall stay with integer lattices however (hence the title), because it is unlikely that practically usable non-integer lattices will realistically outperform integer lattices. The underlying LDPC code will be chosen to be over a prime field: LDPC codes over non-binary alphabets have been mostly experimented with over fields of characteristic 2, but there are no theoretical obstacles to working with prime fields and these are the ones most suitable for our purposes. Decoding complexity will be, as is usual in the area of iterative decoding, essentially linear in the lattice dimension, though it will also grow with the finite field size.

The paper is organized as follows: in Section II we shall recall what we need from construction A in a somewhat generalized setting. In Section III we specify our particular construction and the channel and capacity we will be working with. In Section IV we describe and discuss the lattice decoder. In Section V we discuss specifics and the choice of parameters; we also discuss simulation results. Finally, Section VI gives concluding comments.

II. Lattices and Construction A

We will consider n-dimensional lattices $\Lambda = \mathbb{Z}^n G$ with $n \times n$ generator matrices G and basis $(b_1, \ldots, b_n)$ written as row vectors. The *volume* of the lattice is defined as $\mathrm{vol}(\Lambda) := |\det(G)|$. For any $x \in \Lambda$, its *Euclidean norm* is $||x|| := \sqrt{x_1^2 + \ldots + x_n^2}$ and we denote the lattice *minimum distance* as $d_{\min}(\Lambda) := \min_{x \in \Lambda \setminus 0} ||x||$. The *fundamental gain* of a lattice Λ is defined as

$$\gamma(\Lambda) := \frac{d_{\min}^2(\Lambda)}{\mathrm{vol}(\Lambda)^{2/n}}. \quad (1)$$

Let L be a lattice of small dimension Δ and let L' be a sublattice of L such that the quotient L/L' is finite of prime cardinality p. The additive group L/L' injects naturally into the finite field $\mathbb{F}_p$ through an additive group isomorphism, and we assume identification of the two abelian groups. We may define a lattice Λ of dimension $n = \Delta\ell$ in the following way, which is the general setting for construction A in Conway and Sloane's terminology [4]. Let C be an $\mathbb{F}_p$-linear code of length ℓ, dimension k and *rate* $R = k/\ell$: let $\Pi : L^\ell \to (L/L')^\ell$ be the natural projection, the lattice Λ is defined as:

$$\Lambda = \{x \in L^\ell \mid \Pi(x) \in C\}.$$

Our strategy is to design efficiently decodable lattices through the above construction when the code C is taken to be an LDPC code over $\mathbb{F}_p$ and decoded through appropriately calibrated message-passing.

We shall focus mainly on two simple cases, namely when $(L, L') = (\mathbb{Z}, p\mathbb{Z})$ and $(L, L') = (\mathbb{Z}[i], \phi\mathbb{Z}[i])$ where $(\phi) = (a + bi)$ is a prime ideal of $\mathbb{Z}[i]$ of norm $a^2 + b^2 = p$.

In the first case, which is one of the more classical forms of construction A [4], it is well known that a generator matrix for Λ has the form

$$G = \begin{pmatrix} I_k & \Phi(B) \\ 0 & pI_{n-k} \end{pmatrix} \tag{2}$$

where $(I_k\ B)$ is a $k \times \ell$ generator matrix in systematic form for the code C and where $\Phi\ : \mathbb{F}_p \to \mathbb{Z}$ is a natural embedding of $\mathbb{F}_p$ into $\mathbb{Z}$, typically with $\Phi(\mathbb{F}_p) = [-(p-1)/2, (p-1)/2]$. We have $\mathrm{vol}(\Lambda) = p^{n-k} = p^{n(1-R)}$, with $\ell = n$.

In the second, Gaussian integer case, taking for C an $\mathbb{F}_p$-linear code of length ℓ and dimension k of generator matrix $(I_k\ B)$, we have similarly, that Λ can be seen as a $\mathbb{Z}[i]$-module generated by the $\ell \times \ell$ matrix

$$G' = \begin{pmatrix} I_k & \Phi(B) \\ 0 & \phi I_{\ell-k} \end{pmatrix} \tag{3}$$

where Φ is an embedding of $\mathbb{F}_p$ into a suitable region of $\mathbb{Z}[i]$ via the isomorphism $\mathbb{F}_p \xrightarrow{\sim} \mathbb{Z}[i]/(\phi)$: in other words, $\Phi(\mathbb{F}_p)$ is a set of representatives for $\mathbb{Z}[i]/(\phi)$. To obtain a generator matrix for the real lattice Λ of dimension $n = 2\ell$, simply apply the transformation $x + iy \mapsto \left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right)$ to every coordinate of G'. In this case we have $\mathrm{vol}(\Lambda) = p^{\ell-k} = p^{\frac{1}{2}n(1-R)}$. Figure 1 shows a suitable representation $\Phi(\mathbb{F}_{41})$ of $\mathbb{Z}[i]/(4 + 5i)$ as a constellation of $\mathbb{Z}[i] = \mathbb{Z}^2$: a family of LDPC codes over $\mathbb{Z}[i]/(4+5i)$ and their associated lattices will be experimented with in the sequel.

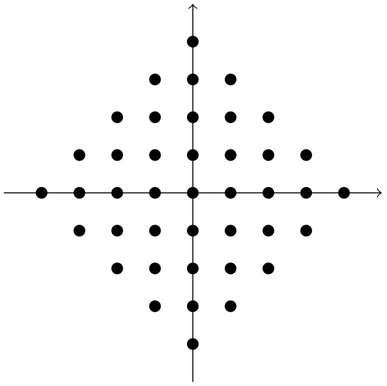

Figure 1. A system of representatives for $\mathbb{Z}[i]/(4 + 5i)$

Note that replacing $\mathbb{Z}[i]$ by the Eisenstein integers yields a similar construction.

III. LDA Lattices and the Gaussian channel

It is now the time to define the new family of lattices we will deal with. By means of Construction A (see Section II), any linear code $C \subseteq \mathbb{F}_p^n$ can be used to build a lattice. For our particular construction, we will take C to be a Low-Density Parity-Check (LDPC) code [8] and we will refer to the resulting lattices as Integer *Low-Density A* (LDA) lattices.

In our scenario, the information to be transmitted is represented by integer vectors $z \in \mathbb{Z}^n$. The uncoded system is then the lattice $\mathbb{Z}^n$ of all integer points in the n-dimensional space. Now, let Λ be an LDA lattice with generator matrix G; its points are the *codewords* to be sent through the channel and z is encoded to $x = zG \in \Lambda$. We are interested in the behaviour of Λ under the *additive white Gaussian noise* (AWGN) channel, that is, the channel output is

$$y = x + \eta, \text{ with } \eta_i \sim \mathcal{N}(0, \sigma^2),\ i = 1, \ldots, n. \tag{4}$$

Following other authors, we will perform *infinite lattice decoding*, that is, our decoder makes no assumption on the shaping region and decodes as if all points of the lattice where good candidates to be the sent codeword. In this scenario, since a lattice has infinite energy, the usual concept of capacity loses its sense. Poltyrev introduced in [14] the notion of *generalized capacity*, which is the maximum value C_∞ such that we can construct a lattice with *normalized logarithmic density* smaller than C_∞ and arbitrarily small decoding error probability. In concrete terms, it implies that there exists a lattice in big enough dimension n for which the decoding is possible with arbitrary small error probability if and only if

$$\sigma^2 < \frac{\mathrm{vol}(\Lambda)^{\frac{2}{n}}}{2\pi e} =: \sigma^2_{max}. \tag{5}$$

We have

$$\sigma^2_{max} = \begin{cases} \frac{1}{2\pi e} p^{2(1-R)}, & \text{for } (L, L') = (\mathbb{Z}, p\mathbb{Z}), \\ \frac{1}{2\pi e} p^{(1-R)}, & \text{for } (L, L') = (\mathbb{Z}[i], \phi\mathbb{Z}[i]). \end{cases} \tag{6}$$

In Section V, we will evaluate the performance of LDA lattices as a function of the noise variance: the best lattices are the ones which attain small symbol error rates for values of the noise variance that are close to σ^2_{max}.We will speak of distance from capacity, meaning the distance of the channel noise variance from σ^2_{max}.

IV. LDA Lattice Decoder

In small dimensions, typically less than 100, Sphere Decoding of Λ is feasible after computing the Gram matrix from (2) or (3) [20] [3]. For high dimensions ($n \geq 1000$), there is no method to handle lattice decoding besides iterative message passing algorithms [17] [18] [19]. The complexity of iterative message passing is linear in n. The critical parameter in our case is the size p of the finite field. Indeed, the p-ary LDPC code C defining Λ can be decoded via belief propagation (BP) or min-sum decoding [16]. Results shown in Section V are obtained with BP. Decoding of an LDPC checknode in C is made via the forward-backward algorithm on the syndrome trellis [1]. The trellis has p^2 transitions in its largest section.

For large p, checknode decoding should be done via Fast Fourier Transform [9]. We describe below the factor graph of Λ and the messages propagating on its edges.

A. Factor graph for Construction A

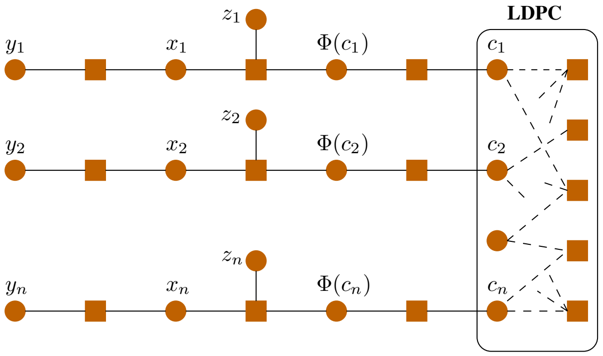

Figure 2. Factor graph of a lattice from Construction A.

The factor graph [12] is derived from the lattice structure given in Section II. Messages and constraints are given for a $\mathbb{Z}$-lattice transmitted over a memoryless AWGN channel. It is straightforward to extend to $\mathbb{Z}[i]$-lattices and other types of memoryless channels. As shown in Figure 2, the constraints are:

- The channel where the output conditional distribution is $y_i \sim \mathcal{N}(x_i, \sigma^2)$, $i = 1, \ldots, n$.
- The lattice constraint given by Construction A, i.e. Λ is the union of cosets of $p\mathbb{Z}^n$. We have $x_i = \Phi(c_i) + pz_i$, where $z_i \in \mathbb{Z}$, $c_i \in \mathbb{F}_p$, and $c = (c_1, c_2, \ldots, c_n) \in C$.
- The embedding Φ of $\mathbb{F}_p$ into the Euclidean space. For $(L, L') = (\mathbb{Z}, p\mathbb{Z})$ and $\ell = n$, the isomorphism $\Phi(c_i)$ is simply defined as the element of $[-(p-1)/2, (p-1)/2]$ that projects onto c_i modulo p. We will write c_i instead of $\Phi(c_i)$ in order to simplify the notation.
- The LDPC constraint given by $cH_C^t = 0$, where H_C is a sparse $(n-k) \times n$ parity-check matrix.

B. Probabilistic messages for Construction A

Now, let us find the expressions of messages propagating left to right in the factor graph. The left-to-right message produced by x_i is

$$P(x_i|y_i) \propto \exp\left(-\frac{(y_i - x_i)^2}{2\sigma^2}\right), \quad \forall x_i \in \mathbb{Z}. \tag{7}$$

Since we have $x_i = c_i + pz_i \equiv c_i \mod p$, the left-to-right message received by c_i is

$$P(c_i|y_i) = \sum_{x_i \in \mathbb{Z} | x_i \equiv c_i} P(x_i|y_i). \tag{8}$$

Now we describe messages propagating right to left. The right-to-left message produced by c_i is the LDPC extrinsic information $P(c_i|C, y\backslash\{y_i\})$ determined by multiplying all messages from its neighbouring checknodes [16]. The outgoing message from z_i is 1 in the absence of *a priori* information. As shown later for our practical implementation, there is a hidden constraint producing an *a priori* information $\pi(z_i)$. Thus, the right-to-left message received by x_i would be

$$P(x_i|C, y\backslash\{y_i\}) \propto \pi(z_i) \cdot P(c_i|C, y\backslash\{y_i\}) \tag{9}$$

From the above description and the fact that the *a posteriori* probability (APP) of a variable node v is determined by the product of the two messages in the two opposite directions on any edge connected to v (belief propagation on an a cyclic graph [16]), we can state the following lemma.

Lemma 1. *Let $\Lambda = C[n,k]_p + p\mathbb{Z}^n$ be an LDA lattice and $x = (x_1, x_2, \ldots, x_n)$ be a lattice point. A message passing decoder should maximize $APP(x_i)$, for $i = 1, \ldots, n$, where the* a posteriori *probability for a lattice component is given by*

$$APP(x_i) \propto P(x_i|y_i)\pi(z_i)P(c_i|C, y\backslash\{y_i\}). \tag{10}$$

C. Implementation

The summation over $\mathbb{Z}$ in (8) decays very quickly around y_i because of the exponential behaviour given in (7). Consider the real interval $\mathcal{W}_i = [y_i - m\sigma, y_i + m\sigma]$ where σ^2 is the noise variance from (4) and $m \in \mathbb{R}^+$. We choose m such that the probability of the transmitted x_i being outside $\mathcal{W}_i$ is less than ε, i.e. $2Q(m) < \varepsilon$ where $Q()$ is the Gaussian tail function. For example, $m = 6.467$ and $\varepsilon = 10^{-10}$. The observation for a code symbol becomes

$$P(c_i|y_i) \approx \sum_{x_i \in \mathcal{W}_i | x_i \equiv c_i} P(x_i|y_i). \tag{11}$$

Limiting the search for a lattice component $x_i = c_i + pz_i$ to $\mathcal{W}_i$ brings an *a priori* on z_i. For a given symbol value c_i and a given channel observation y_i, the search for the unknown z_i is now restricted to $[(y_i - c_i - m\sigma)/p, (y_i - c_i + m\sigma)/p]$. The number of admissible integer translations z_i is $\mu_i(y_i, c_i)$ given by

$$\mu_i(y_i, c_i) := |\{x_i \in \mathcal{W}_i | x_i \equiv c_i \mod p\}|. \tag{12}$$

Consequently, the prior on z_i is given by $\pi(z_i) = 1/\mu_i(y_i, c_i)$. The implementation can be further simplified if p is large enough. Indeed, taking $2m\sigma \leq p$ yields $\mu_i(y_i, c_i) = 1$, for all y_i and all c_i. The latter condition is satisfied when $2m\sigma_{max} \leq p$, where σ_{max}^2 is given by (6), which translates into $p^R \geq 2m/\sqrt{2\pi e}$.

Summarizing, we decode an LDA $\mathbb{Z}$-lattice point coordinatewise as follows, for a fixed index $i = 1, \ldots, n$:

- *Initialisation*: compute $P(x_i|y_i)$ (7) for all $x_i \in \mathcal{W}_i$ and add them as described in (11) to get the p values of $P(c_i|y_i)$.
- *Iterations*: apply Belief Propagation with input $P(c_i|y_i)$ to compute the p values of $P(c_i|C, y\backslash\{y_i\})$.
- *Final decision*: for every $x_i \in \mathcal{W}_i$, compute the product in (10) and find the $x_i = \hat{x}_i$ that maximizes it.

An alternative strategy for the final decision consists in taking as $\hat{x}_i$ the closest to y_i representant of the class modulo p that maximizes the extrinsic probability $P(c_i|C, y\backslash\{y_i\})$.

Notice that, when p is large enough (or when the noise is weak enough, too), the width of the window $\mathcal{W}_i$ is smaller than p itself and the classes modulo p are represented by at most one integer around y_i, as anticipated before, and the two different strategies for the final decision eventually coincide.

V. Optimization and decoding performance

In this section, we present some details on the choice of the LDPC codes for the construction of the LDA lattices that we have tested; after that, we conclude with some simulation results and the comparison with the performance of already known lattice families.

The core of the lattice is of course the p-ary LDPC code and its choice may be optimized. In the classical binary setting, an LDPC code is identified by its parity-check matrix and, equivalently, by the associated Tanner graph. When the entries of the parity-check matrix are non-binary, the Tanner graph is built as usual, and in addition, a label is associated to every edge; this label is equal to the corresponding non-zero entry in the parity-check matrix of the code (see for example [19]).

Optimizing the choice of the p-ary code coincides with optimizing the related labeled Tanner graph. In the binary case, this is often reduced to choosing a graph without small cycles. In the case of p-ary LDPC codes, we also choose in a clever way the non-zero p-ary entries of the parity-check matrix (that is, the p-ary labels of the graph edges). This aspect has a significant impact on iterative decoding and has not been previously considered. The "non-triviality" of the graph labels guarantees the existence of better codes with respect to their binary equivalents, resulting in a more powerful and improved Construction A.

A. Choice of the coefficients for the parity-check equations

In order to make a good choice for the coefficients of the parity-check matrix H_C of the LDPC code, we investigate the *single parity-check (SPC) code* defined by each parity-check equation (the rows of H_C). Formally, we define

$$C_{SPC} := \{x = (x_1, \ldots, x_s) \in \mathbb{F}_p^s \mid a_1x_1 + \ldots + a_sx_s = 0\}$$

as the SPC code associated with the *non-zero* coefficients $a_1, \ldots, a_s \in \mathbb{F}_p \smallsetminus \{0\}$ of a row of H_C. We say that this row has *degree* equal to s.

Note that the message-passing decoder applies MAP decoding to the individual SPC codes. Contrary to the binary case, there are many choices for an SPC code and they may have a strong influence over MAP decoding. In particular, (7) shows that the minimum *Euclidean* distance of the SPC code will be an important parameter and we choose to optimize it. The Euclidean minimum distance is defined as

$$d_{\min}(C_{SPC}) := \min_{x \in C_{SPC} \smallsetminus \{0\}} ||\Phi(x)||$$

(where Φ is defined in Section II). Experiments confirm that coefficients a_i's that maximize $d_{\min}(C_{SPC})$ yield a significantly improved performance over random a_i's for construction A with $(L, L') = (\mathbb{Z}, p\mathbb{Z})$.

We will focus for a moment on this kind of lattice and show how to implement the good choice of the coefficients in the particular case for which we show the simulation results in the next subsection. With this parameters, one can see that $d_{\min}(C_{SPC})$ cannot be greater than $\sqrt{3}$. The condition $d_{\min}(C_{SPC}) \neq 1$ is an immediate consequence of the fact that all the a_i's are non-zero. We can find how to avoid a Euclidean minimum distance of $\sqrt{2}$ as follows: let $(x_1, \ldots, x_s)$ be a point of C_{SPC} of smallest Euclidean norm;

$$\begin{aligned} d_{\min}(C_{SPC}) = \sqrt{2} &\iff \sqrt{x_1^2 + \ldots + x_s^2} = \sqrt{2} \\ &\iff x_i, x_j = \pm 1, \ \exists\ i, j \in \{1, \ldots, s\} \\ &\qquad \text{and } x_k = 0\ \forall k \neq i, j. \end{aligned}$$

$(x_1, \ldots, x_s)$ must satisfy the parity-check equation, that becomes

$$\pm a_i \pm a_j = 0, \ a_i = \pm a_j.$$

This means that the condition

$$a_i \neq \pm a_j, \ \forall i, j \in \{1, \ldots, s\} \tag{13}$$

suffices to impose $d_{\min}(C_{SPC}) > \sqrt{2}$.

Our simulations have directed us towards the choice $s = 5$: in this case the first value of p for which we may have $d_{\min} > \sqrt{2}$ is $p = 11$ and experimentally, this has turned out to be the optimum choice of p for regular LDPCs.

B. Tanner graph construction

Generally, random graphs give good performance, provided that one manually removes all 4-cycles and guarantees a girth of at least 6. We have anyway preferred to use LDPC codes whose corresponding graph is built by means of the Progressive Edge-Growth algorithm (PEG) [10]. This algorithm builds the graph edge by edge, in an iterative manner that locally maximizes the current girth of the graph during construction. Experimentally, we have seen that PEG-obtained graphs allow to reach better symbol error rates (SER), thanks to a "deeper" error floor region with respect to random graphs. At the same time, in the waterfall region of random graphs, PEG-obtained graphs have very similar performance.

C. Simulation results

We will show here some simulation results and compare them with what is known in the literature about other families of lattices used for the transmission of information.

In Figure 3, the distance from capacity is represented as mentioned at the end of Section III. The values of the parameters that we fix in the following are the ones that experimentally have given the best results till now. The number of decoding iterations has been fixed to at most 200 in all simulations.

Let us start with an LDA lattice obtained by classical p-ary Construction A. We have only investigated regular LDPC codes and similarly to the case of binary LDPC's constructed as binary images of q-ary LDPCs [15], we have found that a degree 2 per variable node yields the best results. As

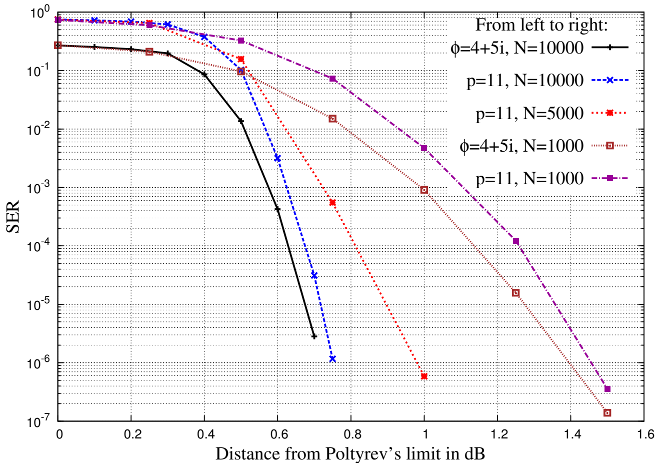

Figure 3. Symbol error rate versus distance to Poltyrev limit for LDA lattices.

mentioned before, the most interesting case to come up was that of a $(2,5)$-regular code with $p = 11$.

As described in Section V-B, the graph is built using the PEG algorithm, with the slight modification with respect to [10] that the check nodes degree distribution is fixed, too. The non-zero entries of the parity-check equation are chosen as described in Section V-A. Fig. 3 shows that for $n = 1000$, we attain a SER of less than 10^{-6} at 1.5 dB from capacity. This corresponds to an improvement of about 0.2 dB better with respect to the performance of LDLC [19] at a SER of 10^{-5}.

With a similar lattice in dimension $n = 5000$, we attain a SER of less than 10^{-6} at 1 dB from capacity, which corresponds to an improvement of more than 0.2 dB with respect to Irregular LDPC lattices and of about 0.8 dB with respect to Regular LDPC lattices (see [2]).

In dimension $n = 10000$, our LDA $\mathbb{Z}$-lattice provides a SER of 10^{-6} at 0.75 dB from capacity, which is better than what LDLC do [19].

An even more interesting result is given by the performance of LDA $\mathbb{Z}[i]$-lattices (construction A with $(L, L') = (\mathbb{Z}[i], \phi\mathbb{Z}[i])$. As in the previous examples, the Tanner graph is $(2,5)$-regular, while the prime ideal used for the modulo operation is $(4+5i)$, corresponding to $p = 41$. In (real) dimension $n = 1000$ ($\ell = 500$), a SER of about 10^{-5} is attained at 1.25 dB from capacity, equalling the performance of Turbo lattices [18], while, for $n = 10000$ ($\ell = 5000$), the same SER is attained at about 0.7 dB from capacity.

VI. Conclusion and Future Work

In this paper, we considered LDA lattices built from Construction A with p-ary low-density parity-check codes. The LDA factor graph and a simple iterative decoding algorithm have been described. Computer simulations for LDA lattices over the rings $\mathbb{Z}$ and $\mathbb{Z}[i]$ showed a close-to-capacity performance that exceeds or matches previous propositions for moderate dimensions ($n = 1000, 10000$). Also, LDA decoding utilizes belief propagation to infer integer lattice components. A direct extension would be the construction of LDA lattices represented by the union of cosets of a well selected ideal in the ring of Eisenstein integers $\mathbb{Z}[\omega]$.

Construction A is a special case of multilevel coded modulations [11] [21]. For LDA lattices, it has one coded level with the p-ary LDPC code and one uncoded level given by $p\mathbb{Z}^n$ with its infinite cardinality. Comparison to coded modulations with finite constellations should be done later after building and shaping finite LDA constellations.

The main application of LDA lattices in this paper was error correction on a Gaussian channel, but other numerous potential applications exist such as physical layer network coding and physical layer security.

References

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

[2] 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.

[3] L. Brunel and J. J. Boutros, "Lattice decoding for joint detection in direct-sequence CDMA systems," *IEEE Trans. on Inf. Theory*, vol. 49, no. 4, pp. 1030–1037, April 2003.

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

[5] 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.

[6] U. Erez, S. Litsyn and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Trans. on Inf. Theory*, vol. 51, no. 10, pp. 3401–3416, Oct. 2005.

[7] 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.

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

[9] C. R. P. Hartmann and L. D. Rudolph, "An optimum symbol-by-symbol decoding rule for linear codes," *IEEE Trans. on Inf. Theory*, vol. 22, no. 5, pp. 514–517, Sept. 1976.

[10] X.-Y. Hu, E. Eleftheriou and D. M. Arnold, "Regular and irregular progressive edge-growth tanner graphs," *IEEE Trans. on Inf. Theory*, vol. 51, no. 1, pp. 386–398, Jan. 2005.

[11] H. Imai and S. Hirakawa, "A new multilevel coding method using error-correcting codes," *IEEE Trans. on Information Theory*, vol. 23, no. 3, pp. 371–377, May 1977.

[12] F. Kschischang, B. Frey and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 498–519, Feb. 2001.

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

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

[15] C. Poulliat, M. Fossorier, and D. Declercq, "Design of non binary LDPC codes using their binary image: algebraic properties," *Proc. of IEEE Intern. Symp. of Inf. Theory 2006*, pp. 93–97, July 2006.

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

[17] 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.

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

[19] 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.

[20] E. Viterbo and J. J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. on Inf. Theory*, vol. 45, no. 5, pp. 1639–1642, July 1999.

[21] 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.