

Generalized Low-Density (GLD) Lattices

Joseph J. Boutros, Nicola di Pietro, and Nour Basha
 Texas A&M University at Qatar
 Education City, 23874, Doha, Qatar
 {joseph.boutros, nicola.dipietro, nour.basha}@qatar.tamu.edu

Abstract—We propose the construction of a new family of lattice sphere packings. Given a small-dimensional lattice, we start by building a first lattice in a large dimension by the direct sum of the small lattice. Then, the coordinates of the first large lattice are permuted to yield a second large-dimensional lattice. Finally, our generalized low-density (GLD) lattice is the intersection of the first and the second lattice. We restrict our construction in this paper to integer lattices. GLD lattices are the result of mixing classical lattice theory with modern coding theory. They are potential candidates not only for channel coding as coded modulations, but also for physical-layer network coding and for secure digital communications.

I. INTRODUCTION

Lattice constellations are known to be good codebooks for source coding, channel coding, and data transmission in networks. In recent times, analysis of lattice constellations and efficient lattice families have been proposed for the purpose of channel coding. A non-exhaustive list of publications on the subject is [5]–[19], [21]. In this paper, we deal with a new family of lattices for coding over channels with additive white Gaussian noise. This family is referred to as *Generalized Low-Density (GLD) Lattices*. The idea of introducing GLD lattices comes from two main intentions:

- 1) Adapting to real lattices the construction of *Generalized Low Density (Tanner) Codes* based on linear binary BCH codes [3] [4].
- 2) Extending the work on *Low-Density Lattice Codes* [13] to other lattice families, still basing their strength on sparse *parity-check matrices*.

GLD lattices considered in this paper are integer (i.e. contained in \mathbb{Z}^N) and have a sparse rectangular parity-check matrix. These two features are the most important for the design of a suitable iterative decoding algorithm and represent the solid foundations of the GLD family. Also, interesting mathematical problems arise from the GLD lattice definition.

The following sections give algebraic and graphical descriptions of GLD lattices in a tutorial-like manner suitable for both mathematicians and engineers. Section II briefly defines a lattice in \mathbb{R}^N . Section III gives a matrix representation of GLD lattices. The corresponding graph representation is found in Section IV. Iterative decoding of GLD lattices is briefly discussed in Section VI. Section V shows how to select the component small-dimensional lattice in the GLD lattices family. The paper ends with a section revealing numerical results of the performance of GLD lattices in dimension 1000 on a Gaussian channel.

II. LATTICES

The main subject of this paper is *real lattices*. Mathematically, a lattice is a \mathbb{Z} -module of the Euclidean vector space \mathbb{R}^N . Concretely, it is simply a discrete, additive subgroup of \mathbb{R}^N , according to the following definition [1]:

Definition 1: Given M and N two natural numbers, $M \leq N$, and given a set of M linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_M \in \mathbb{R}^N$, an M -dimensional lattice Λ is defined as the set of all integer linear combinations of the \mathbf{b}_i 's:

$$\Lambda = \left\{ \mathbf{x} \in \mathbb{R}^N : \mathbf{x} = \sum_{i=1}^M z_i \mathbf{b}_i, z_i \in \mathbb{Z} \right\}. \quad (1)$$

The \mathbf{b}_i 's are called a *basis* of the lattice Λ and we say that they *generate* it. M is called the *rank* of the lattice and we say that the lattice has *full rank* if $M = N$. The $M \times N$ matrix G whose rows are the \mathbf{b}_i 's is called the *generator matrix* associated with that basis and

$$\Lambda = \{ \mathbf{x} \in \mathbb{R}^N : \mathbf{x} = \mathbf{z}G, \mathbf{z} \in \mathbb{Z}^M \} = \mathbb{Z}^M G. \quad (2)$$

When $M = N$ and G is square, we define the *volume* of the lattice as $\text{Vol}(\Lambda) = |\det(G)|$.

Given a rank- N lattice $\Lambda \subseteq \mathbb{R}^N$, any generator matrix G of Λ is square and has full rank; then, let $H = G^{-1}$. A definition of Λ equivalent to (1) and (2) is

$$\Lambda = \{ \mathbf{x} \in \mathbb{R}^N : \mathbf{x}H \text{ is an integer vector} \}. \quad (3)$$

Extending to lattices the terminology of linear codes, H can be viewed as a *parity-check matrix* defining Λ .

III. ALGEBRAIC CONSTRUCTION

Now, let the space dimension N be fixed. The first ingredient for the construction of a GLD lattice in \mathbb{R}^N is an n -dimensional lattice $\Lambda_0 \subseteq \mathbb{R}^n$, for some small n dividing N . Let G_0 be its generator matrix and $H_0 = G_0^{-1}$. Let $L = N/n$ and consider the $N \times N$ matrix

$$H_1 = \begin{pmatrix} H_0 & 0 & \dots & 0 \\ 0 & H_0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & H_0 \end{pmatrix}; \quad (4)$$

its diagonal blocks are L copies of the matrix H_0 defining Λ_0 . Therefore, H_1 defines the lattice

$$\Lambda_1 = \Lambda_0^{\oplus L}, \quad (5)$$

where the exponent $\oplus L$ denotes the direct sum of L summands all equal to Λ_0 . Now, let π be a permutation of $\{1, 2, \dots, N\}$ and let

$$\Lambda_2 = \{(x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(N)}) : (x_1, x_2, \dots, x_N) \in \Lambda_1\}.$$

A parity-check matrix for Λ_2 is clearly obtained by permuting with π the rows of H_1 , that is, if Π is the permutation matrix representing π , $H_2 = \Pi H_1$. We call Λ_2 the lattice generated by the parity-check matrix H_2 and we emphasize the relation between Λ_1 and Λ_2 with the notation

$$\Lambda_2 = \pi(\Lambda_1) = \pi(\Lambda_0^{\oplus L}). \quad (6)$$

Definition 2 (GLD lattice): Given Λ_1 and Λ_2 built as described before, we call *Generalized Low-Density (GLD) lattice* the lattice

$$\Lambda = \Lambda_1 \cap \Lambda_2 = \Lambda_0^{\oplus L} \cap \pi(\Lambda_0^{\oplus L}). \quad (7)$$

Notice that a (non-square, $N \times 2N$) parity-check matrix H for the GLD lattice Λ is

$$H = \begin{pmatrix} H_1 & H_2 \end{pmatrix}. \quad (8)$$

H is rectangular, so in particular it is not invertible and we cannot say that its inverse generates Λ . Nevertheless, it is a parity-check matrix in the sense that it defines Λ as in (3). Clearly, since we are in an N -dimensional space, the $2N$ columns of H (or, equivalently, the $2N$ corresponding parity-check equations) cannot generate a lattice of dimension bigger than N . It means that at least N of these columns are redundant or, more mathematically, at least N of them are linearly dependent on the others. Nevertheless, this matrix will be our favorite for representing GLD lattices and it will be directly used in iterative decoding of GLD lattice codes. Its main feature, hence the adjective *Low-Density*, is that it is sparse, provided that n is small compared to N . Namely, by construction, it has row degree at most $2n$ and column degree at most n .

Before going on, let us make a small example to make this construction explicit. Let $n = 2$, $L = 2$, and $N = 4$; let

$$\pi : (a, b, c, d) \rightarrow (d, b, a, c) \quad (9)$$

be the permutation of four elements that sends the first element to the third position, the second element to the second position, and so on according to (9); hence

$$\Pi = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (10)$$

Then, let

$$H_0 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \quad (11)$$

$$\text{and } H_2 = \begin{pmatrix} 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad (12)$$

with $H_2 = \Pi H_1$. The corresponding GLD lattice is then defined by the parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 1 & 1 \end{pmatrix}. \quad (13)$$

IV. GRAPHICAL REPRESENTATIONS

As we have already anticipated, our main goal is to design lattices that are suitable for channel coding and iterative decoding. For the latter, we also need to associate a graph with our lattice structure. Similar to the case of linear codes (and in particular LDPC codes), we can associate a *Tanner graph* [2] with a parity-check matrix of a GLD lattice Λ . This is a bipartite graph, built as follows:

- One set of nodes represents the variables x_1, x_2, \dots, x_N .
- The other set of nodes represents parity-check equations (the columns \mathbf{h}_j of H , $j = 1, 2, \dots, 2N$).
- There is an edge between a variable node x_i and a parity-check node \mathbf{h}_j if and only if the entry $h_{i,j}$ of H is different from 0.

In order to better understand this, let us build the Tanner graph for the GLD lattice of the example of the previous section. This lattice is identified by H in (13) and the corresponding Tanner graph is depicted in Figure 1.

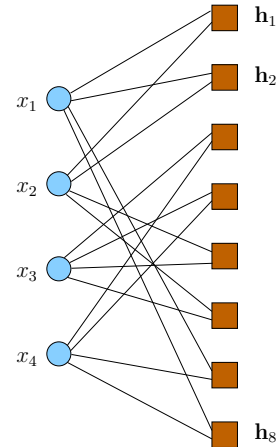


Figure 1. Tanner graph of the lattice defined by H in (13). Variable nodes x_1, x_2, x_3, x_4 are on the left, check nodes $\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_8$ are on the right.

For a general GLD lattice, a Tanner graph has N variable nodes and $2N$ check nodes. Instead of considering columns of H as separate check nodes, given definition (7), we build a more compact Tanner graph having $2N/n = 2L$ check nodes. This graph is called *generalized Tanner graph* in the sequel. It is more efficient for iterative decoding by message passing [2]. Each of its check nodes represents on its own n columns of H and corresponds to a lattice copy of Λ_0 . Let us illustrate

this graph through our previous example in (13). The left half part of H has $L = 2$ copies of H_0 , i.e. the direct sum $\Lambda_0^{\oplus 2}$. The right half part has also two copies of H_0 where point coordinates are reordered according to π , i.e. $\pi(\Lambda_0^{\oplus 2})$. As depicted in Figure 2-(a), the Tanner graph has four generalized check nodes and represents $\Lambda = \Lambda_0^{\oplus 2} \cap \pi(\Lambda_0^{\oplus 2})$.

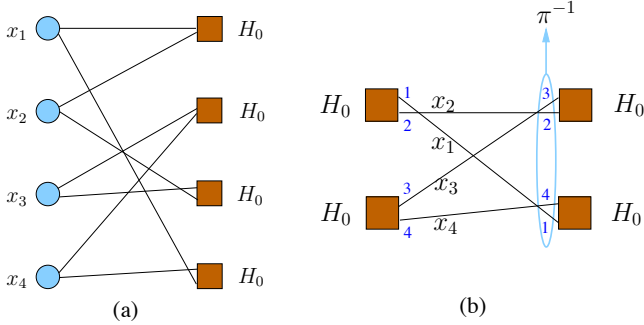


Figure 2. The generalized Tanner graph associated with the GLD lattice defined by H in (13), where $\Lambda = \Lambda_1 \cap \Lambda_2 = \Lambda_0^{\oplus 2} \cap \pi(\Lambda_0^{\oplus 2})$.

By GLD construction $\Lambda = \Lambda_1 \cap \Lambda_2$, i.e. intersection of two lattices, variable nodes representing lattice coordinates all have degree 2 in the generalized Tanner graph. Hence, the graph can be further simplified by moving the first L check nodes to the left and assigning coordinates to edges. This transformation in the example $n = L = 2$ and dimension $N = 4$ converts the graph in Figure 2-(a) into the simpler graph of Figure 2-(b). For a GLD lattice Λ of rank $N = nL$, as depicted in Figure 3, the generalized Tanner graph has L check nodes on the right and L check nodes on the left. A check node has degree n ; it represents a local constraint defined by Λ_0 . The total number of edges is $N = nL$. One lattice coordinate is assigned to one graph edge.

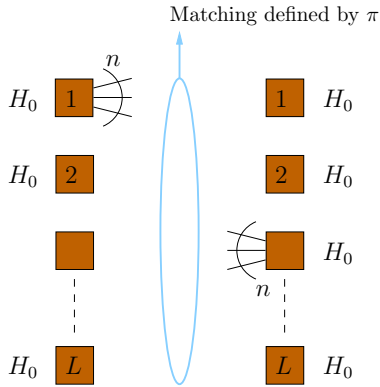


Figure 3. The generalized Tanner graph associated with a GLD lattice Λ of rank $N = nL$, where $\Lambda = \Lambda_0^{\oplus L} \cap \pi(\Lambda_0^{\oplus L})$.

V. CHOICE OF THE COMPONENT LATTICE Λ_0

The choice of the n -dimensional lattice Λ_0 is crucial for the construction of good GLD lattices. Indeed, it can make the difference between having a useless, trivial intersection $\Lambda_0^{\oplus L} \cap \pi(\Lambda_0^{\oplus L}) = \{\mathbf{0}\}$ or a more significant GLD lattice of full rank N . In other words, the presence of some kind of

symmetry in Λ_0 is necessary if we want the GLD construction to produce non-trivial new lattices.

For this reason, from now on we restrict our analysis to GLD lattices for which Λ_0 is obtained by *Construction A*:

Definition 3 (Construction A (see also [1])): Let p be a prime number and let $C_0 = C_0[n, k, d_H]_p$ be a linear code over \mathbb{F}_p of length n , dimension k , rate $R = k/n$, and minimum Hamming distance d_H . The lattice Λ_0 obtained by *Construction A* from C_0 is defined as:

$$\Lambda_0 = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} \equiv \mathbf{c} \pmod{p}, \exists \mathbf{c} \in C_0\}. \quad (14)$$

A compact way of expressing the previous formula is to write Λ_0 as a coset code [20]:

$$\Lambda_0 = C_0 + p\mathbb{Z}^n. \quad (15)$$

One simple consideration about a Construction A lattice Λ_0 is that

$$p\mathbb{Z}^n \subseteq \Lambda_0 \subseteq \mathbb{Z}^n, \quad (16)$$

from which we directly obtain:

$$p\mathbb{Z}^N \subseteq \Lambda_0^{\oplus L} \subseteq \mathbb{Z}^N \quad \text{and} \quad p\mathbb{Z}^N \subseteq \pi(\Lambda_0^{\oplus L}) \subseteq \mathbb{Z}^N. \quad (17)$$

Finally,

$$p\mathbb{Z}^N \subseteq \Lambda = \Lambda_0^{\oplus L} \cap \pi(\Lambda_0^{\oplus L}) \subseteq \mathbb{Z}^N. \quad (18)$$

These simple inclusions yield the first, essential consequence of building Λ_0 with Construction A: independently from the choice of the permutation π , the corresponding GLD lattice is automatically 1) integer; 2) of full rank N . The first property is very useful to implement the decoding algorithm, in which messages will not need to be probability density functions (as in [13]), but discrete distributions instead. The second property is a guarantee of consistency of the construction itself.

While in the general case it is hard to find and describe the intersection of a lattice with a permuted version of itself, our particular choice of Λ_0 allows us to analyze in the GLD setting two of the main lattice parameters: the volume and the *minimum squared (Euclidean) distance*, defined as $d_\Lambda^2 = \min_{\mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}} \|\mathbf{x}\|^2$:

Proposition 1: In the notation of this section, if Λ is a GLD lattice with Λ_0 obtained by Construction A, then

$$\min(p^2, d_H) \leq d_\Lambda^2 \leq p^2 \quad (19)$$

and

$$p^{(1-R)N} = p^{(n-k)L} \leq \text{Vol}(\Lambda) \leq p^N. \quad (20)$$

Proof: The inclusion $p\mathbb{Z}^N \subseteq \Lambda$ implies the following inequalities: $\text{Vol}(\Lambda) \leq \text{Vol}(p\mathbb{Z}^N) = p^N$ and $d_\Lambda^2 \leq p^2$. Moreover, (15) directly implies that $d_{\Lambda_0}^2 \geq \min(p^2, d_H)$ and the inclusion $\Lambda \subseteq \Lambda_0^{\oplus L}$ implies that $d_\Lambda^2 \geq d_{\Lambda_0^{\oplus L}}^2 = d_{\Lambda_0}^2$. Putting all of this together, we conclude that $\min(p^2, d_H) \leq d_\Lambda^2 \leq p^2$, which is (19).

Passing to the proof of (20), we notice that $\Lambda \subseteq \Lambda_0^{\oplus L}$ also implies that

$$\text{Vol}(\Lambda) \geq \text{Vol}(\Lambda_0^{\oplus L}) = \text{Vol}(\Lambda_0)^L.$$

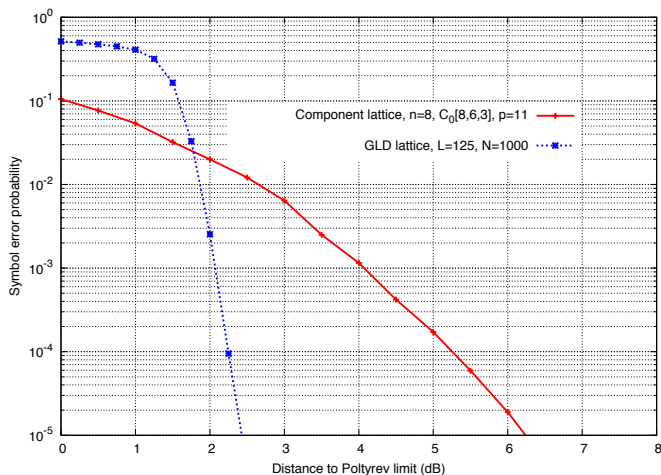


Figure 4. Error rate performance as a measure for the goodness of a GLD lattice over the Gaussian channel, $\Lambda_0 = [8, 6, 3]_{11} + 11\mathbb{Z}^8$, $N = 1000$.

The error probability per lattice coordinate, usually called *symbol error probability*, is plotted in Figure 4 versus the gap to Poltyrev's limit. The symbol error probability has been estimated via Monte Carlo method where at least 200 erroneous lattice points are measured. Message passing in the generalized Tanner graph did at most 200 decoding iterations. Despite the good structure of Λ_0 , the GLD lattice is more than 2dB away from Poltyrev's limit. This weakness is mainly due to a relatively small value of $L = N/n = 125$.

A second GLD lattice of dimension $N = 1000$ has been built from $C_0[4, 3, 2]_{11}$ with smaller but more check nodes, $n = 4$ and $L = 250$. The linear code C_0 is a single parity-check over F_{11} . The generator matrix of Λ_0 is

$$G_0 = \begin{pmatrix} 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 11 \end{pmatrix}. \quad (26)$$

Under similar conditions as the first GLD lattice, this one performs closer to the theoretical limit on the Gaussian channel as shown in Figure 5. This performance is comparable to that of the best lattices known in the current literature.

ACKNOWLEDGMENT

The research work presented in this paper on GLD lattices is supported by QNRF, a member of Qatar Foundation, under NPRP project 5-597-2-241.

REFERENCES

- [1] J.H. Conway and N.J.A. Sloane. Sphere Packings, Lattices and Groups. Springer-Verlag, New York, 3rd edition, 1999.
- [2] T. Richardson and R. Urbanke. Modern Coding Theory. Cambridge University Press, New York, 2008.
- [3] O. Pothier, L. Brunel, and J.J. Boutros, "A low complexity FEC scheme based on the intersection of interleaved block codes," *IEEE Veh. Tech. Conf.*, vol. 1, pp. 274-278, Houston, May 1999.
- [4] J.J. Boutros, O. Pothier, and G. Zémor, "Generalized low density (Tanner) codes," *IEEE Intern. Conf. on Comm. (ICC)*, vol. 1, pp. 441-445, Vancouver, June 1999.
- [5] G. Poltyrev, "On coding without restrictions for the AWGN channel," *IEEE Trans. on Inf. Theory*, vol. 40, no. 2, pp. 409-417, March 1994.

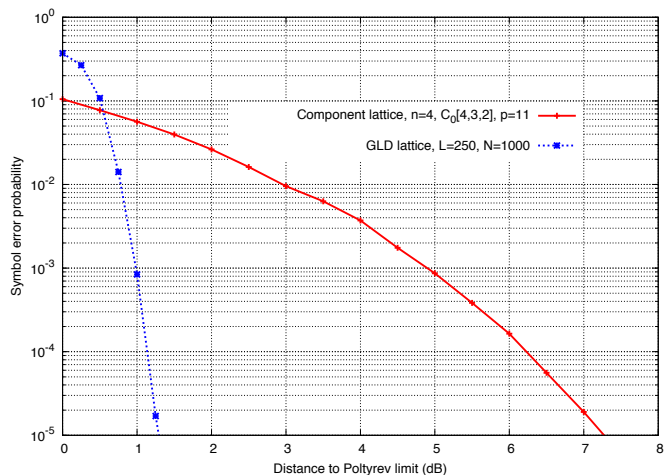


Figure 5. Error rate performance as a measure for the goodness of a GLD lattice over the Gaussian channel, $\Lambda_0 = [4, 3, 2]_{11} + 11\mathbb{Z}^4$, $N = 1000$.

- [6] H.-A. Loeliger, "Averaging bounds for lattices and linear codes," *IEEE Trans. on Inf. Theory*, vol. 43, no. 6, pp. 1767-1773, Nov. 1997.
- [7] 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.
- [8] O. Ordentlich and U. Erez, "A simpler proof for the existence of good pairs of nested lattices," 2012. Available at <http://arxiv.org/abs/1209.5083>.
- [9] C. Ling and J.-C. Belfiore, "Achieving the AWGN channel capacity with lattice Gaussian coding," *IEEE Intern. Symp. on Inf. Theory Proceedings (ISIT)*, pp. 1416-1420, July 2013.
- [10] A. Ingber, R. Zamir, and M. Feder, "Finite-dimensional infinite constellations," *IEEE Trans. on Inf. Theory*, vol. 59, no. 3, pp. 1630-1656, March 2013.
- [11] P. Gaborit and G. Zémor, "On the construction of dense lattices with a given automorphism group," *Annales de l'Institut Fourier*, vol. 57, no. 4, pp. 1051-1062, 2007.
- [12] I.-J. Baik and S.-Y. Chung, "Irregular low-density parity-check lattices," *IEEE Intern. Symp. on Inf. Theory (ISIT)*, pp. 2479-2483, 2008.
- [13] 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.
- [14] A. Sakzad, M.-R. Sadeghi, and D. Panario, "Turbo lattices: Construction and error decoding performance," 2012. Available at <http://arxiv.org/abs/1108.1873v3>.
- [15] M.-R. Sadeghi and A. Sakzad, "On the performance of 1-level LDPC lattices," *Iran Workshop on Comm. and Inf. Theory (IWCIT)*, pp. 1-5, 2013.
- [16] Y. Yan, C. Ling, and X. Wu, "Polar lattices: Where Arikan meets Forney," *IEEE Intern. Symp. on Inf. Theory (ISIT)*, pp. 1292-1296, July 2013.
- [17] 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.
- [18] N. di Pietro, G. Zémor, and J.J. Boutros, "New results on Construction A lattices based on very sparse parity-check matrices," *Proc. of the 2013 IEEE Intern. Symp. on Inf. Theory (ISIT)*, pp. 1675-1679, July 2013.
- [19] N. di Pietro, "On Infinite and Finite Lattice Constellations for the Additive White Gaussian Noise Channel," PhD thesis, Université de Bordeaux, Jan. 2014.
- [20] G. D. Forney, "Coset codes I: introduction and geometrical classification," *IEEE Trans. on Inf. Theory*, vol. 34, no. 5, pp. 1123-1151, 1988.
- [21] 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.
- [22] J.J. Boutros, N. Gresset, L. Brunel, and M. Fossorier, "Soft-input soft-output lattice sphere decoder for linear channels," *IEEE Glob. Comm. Conf.*, vol. 3, pp. 1583-1587, Dec. 2003.
- [23] 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.