Convolutional Lattices

J.J. Boutros and N. di Pietro
Texas A&M University at Qatar
boutros@tamu.edu

F. Jardel
Nokia Bell Labs, Stuttgart
fanny.jardel@nokia.com

C. Kourtellaris
University of Cyprus
kourtellaris.christos@ucy.ac.cy

***Abstract*—Real convolutional lattices over the ring of integers $\mathbb{Z}$ are considered in this paper. We study the stability of convolutional lattices under sphere decoding. A new stable family of time-alternating convolutional lattices is proposed. The structure, the parameters, and a performance example are shown for time-alternating convolutional lattices. These lattices can be used as constituent blocks in concatenated coded modulations for control and communication.**

I. Introduction

Lattices are the real Euclidean counterpart of error-correcting codes. They are discrete additive subgroups of $\mathbb{R}^n$. Lattices are used to process information in many scientific areas such as channel coding, source coding, and cryptography [1][2][3]. Lattices in this paper are real, they are modules over the ring of integers $\mathbb{Z}$ [4]. Construction over the ring of Gaussian integers or any other complex ring are not considered here. See [1] for an extensive list of lattices and their mathematical properties.

Why are we considering convolutional lattices? Their main interesting property is causality. Convolutional lattices allow for causal encoding and causal decoding, hence they are suited to control applications where feedback should be produced almost in real time. Convolutional lattices, also named *Signal Codes*, were first introduced in [5]. Signal Codes are defined over complex fields and the authors were not interested in causality, mainly at the decoder side. Also, a recent work on turbo-like codes based on complex lattices appeared in [6] for low spectral efficiency. Our goal is to build high spectral efficiency coded modulations (based on lattices) for control and communication systems. Time-alternating convolutional lattices described in this paper are a first step towards this goal.

In asymptotic dimensions, sufficient conditions are known for lattice codes to achieve the capacity of the additive white Gaussian noise channel. Under Construction A, a finite constellation can achieve the capacity of the Gaussian channel if two conditions are met: Poltyrev goodness and Covering goodness [2]. For lattices in finite (small) dimensions, the design relies on the packing goodness. Indeed, in a way similar to error-correcting codes where the Minimum Hamming distance is a main parameter for code optimization at short length, the packing density is the main parameter for lattices in non-asymptotic dimensions. The packing density of a n-dimensional lattice $\Lambda \subset \mathbb{R}^n$ is usually measured by its *Hermite constant* γ, also referred to as its *fundamental gain* [7], given by the following ratio

$$\gamma = \frac{d^2_{Emin}}{vol(\Lambda)^{2/n}}, \tag{1}$$

where d^2_{Emin} is the minimum squared Euclidean distance of Λ and $vol(\Lambda)$ is its fundamental volume. Hermann Minkowski gave a non-constructive proof that good lattices exist [8]. At large n, Minkowski's bound is expressed as

$$\frac{n}{2\pi e} \lesssim \gamma. \tag{2}$$

Kabatiansky and Levenshtein gave an upper bound to the packing density [9], a bound expressed as

$$\gamma \lesssim \frac{1.744\ n}{2\pi e}. \tag{3}$$

From the bounds (2) and (3), it can be stated that dense lattices should satisfy $\gamma = \Theta(n)$. This paper aims at designing dense (but not very dense) convolutional lattices with $\gamma = \Theta(n^\kappa)$, $\kappa < 1$.

The paper is structured as follows. Convolutional lattices are defined in the next section. Stability of sphere decoding and unstable convolutional lattices are considered in sections III and IV respectively. Stable time-alternating lattices are described in Section V before the conclusions.

II. Causal and Convolutional Lattices

Let G be a $n \times n$ generator matrix of a lattice Λ of rank n in the real n-dimensional space $\mathbb{R}^n$. Row convention is assumed. The Gram matrix is a positive definite symmetric matrix Γ defined as follows:

$$\Gamma = G \cdot G^t, \tag{4}$$

where G^t is the transpose of G. In other words, Γ contains all scalar products of basis vectors, a basis of Λ is represented by the rows of G. The following well-known result can be found from matrix properties in Linear Algebra.

Theorem 1. *Any lattice Λ of rank n in $\mathbb{R}^n$ admits a lower triangular generator matrix.*

There are many ways to prove the above theorem. Hermite Normal Form reduction generates a lower triangular matrix for any integer lattice [10]. For general real lattices, apply the QR decomposition to G^t [11][12] and write it as $G^t = Q \cdot R$, where Q is orthogonal and R is upper triangular. Then,

$G = R^t \cdot Q^t$, i.e. R^t is a lower triangular generator matrix of Λ. It is important to note that the lower triangular matrix is obtained from an original non-triangular matrix by rotating the lattice in $\mathbb{R}^n$ via Q. A proof based on Cholesky decomposition [11][12] would be made by writing $\Gamma = L \cdot L^t$ which leads directly to a lower triangular generator matrix L. The n-dimensional rotation is found by $Q = L \cdot G^{-1}$.

Let $x = z \cdot G$ be a lattice point, where $z \in \mathbb{Z}^n$. Assume G is already lower triangular. Suppose that discrete time advances from n backward to 1, so the information source is producing z_n, followed by z_{n-1}, then z_{n-2}, and so on till z_1. From $x = z \cdot G$, we deduce that

$$x_j = g_{jj} z_j + \sum_{i=j+1}^{n} g_{ij} z_i, \tag{5}$$

for $j = 1, \ldots, n$. The lattice coordinate at time j is computed from input at time j and previous inputs. Consequently, this lattice encoding is causal. From Theorem 1, we get that any lattice Λ admits a causal encoding via a lower triangular generator matrix.

Consider a channel output $y = (y_1, \ldots, y_n)$ received in a time ordered fashion: y_n, then y_{n-1}, etc., up to y_1. A causal lattice decoder is a decoder capable of decoding, at time instant j based on $(y_j, y_{j+1}, \ldots, y_n)$, all lattice coordinates x_i, for $i \geq j$. A causal lattice decoder is not asked to be optimal in the global Maximum Likelihood (ML) sense. Its main task is to get a quick estimate (without delay) of the transmitted point coordinates.

Definition 1. *A lattice Λ is said to be causal if it admits a causal encoder and a causal decoder.*

Convolutional lattices are a special class of causal lattices. In theory, they admit a causal decoder, but it is not sure whether the decoder is feasible with a reasonable complexity.

Definition 2. *Λ is a convolutional lattice with memory $L-1$ if G is lower triangular and has L non-zero diagonals. In this case, G is called a convolutional generator matrix.*

The $n \times n$ real matrices $G = [g_{ij}]$ defined below generate convolutional lattices in $\mathbb{R}^n$ of memory 1 and memory 2 respectively:

$$g_{ij} = \delta_{ij} + \frac{1}{2}\delta_{ij+1}, \qquad i,j = 1 \ldots n, \tag{6}$$

$$g_{ij} = \delta_{ij} + \frac{1}{2}\delta_{ij+1} + \frac{1}{4}\delta_{ij+2}, \qquad i,j = 1 \ldots n, \tag{7}$$

where δ_{ij} is the Kronecker delta.

The main diagonal (referred to as the *first diagonal*) and the sub-diagonals in both matrices given above have constant elements. A convolutional lattice Λ is said to be time-invariant if $g_{j+\ell-1,j}$ does not depend on j for all ℓ and for all j, where $1 \leq \ell \leq L$ and $1 \leq j \leq n - L + 1$. The two time-invariant convolutional lattices defined by (6) and (7) exhibit a very weak Hermite constant due to rows of small norm in the generator matrix. A first approach for building good convolutional lattices is to make the diagonals time-variant via a log-normal distribution. The following construction of G with $L = 2$, referred to as the *KB construction*, yields a good packing density with a fundamental volume close to unity:

- Generate n instances $\exp(a_i)$ of a r.v. $\exp(\mathcal{N}(0, \sigma^2_{KB}))$. Sort $\{\exp(a_i)\}_{i=1}^n$ by decreasing order and put on the first diagonal.
- Generate $n-1$ instances $\exp(b_i)$ of a r.v. $\exp(\mathcal{N}(0, \sigma^2_{KB}))$. Sort $\{\exp(b_i)\}_{i=1}^n$ by increasing order and put on the second diagonal.

From the law of large numbers, the Hermite constant denominator satisfies $vol^{2/n} = \exp(2\sum_i a_i/n) \to 1$. The minimum Euclidean distance in the convolutional KB construction is guaranteed to be high enough thanks to the opposite sorting on the first and the second diagonal.

Figure 1 shows the performance of a convolutional KB lattice versus the distance to Poltyrev limit at $n = 64$. The highest noise variance that an infinite lattice constellation can sustain with a vanishing error probability is given by Poltyrev limit, $\sigma^2_{max} = 1/(2\pi e)$ [13]. The distance to Poltyrev limit, expressed in dB, becomes $10\log_{10}(\sigma^2_{max}/\sigma^2)$, where σ^2 is the noise variance on the Gaussian channel. For reference, Figure 1 also shows a union bound to the error rate based on the first elements in the estimated Theta series of the KB lattice, the Leech lattice performance in dimension 24, and that of the integer lattice $\mathbb{Z}^{64}$. The reader should not be surprised. The KB lattice performance is wrong due to instability. This issue is discussed in the next section.

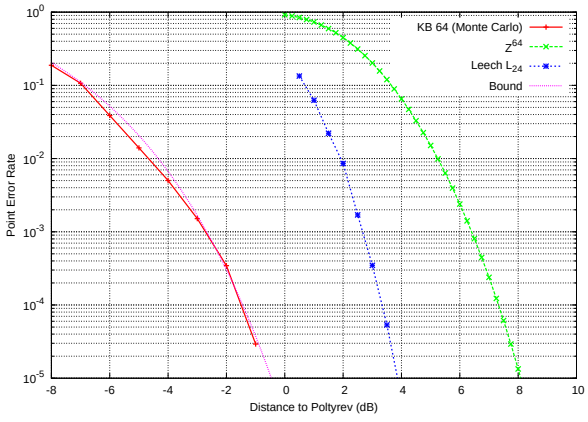

Figure 1. Performance of the unstable KB64 convolutional lattice ($L = 2$). Detection of any overflow of z was not activated while applying a 32-bit implementation of sphere decoding. The point error rate is wrongly beating Poltyrev limit (0 dB).

III. Stability of Sphere Decoding

For real dimensions up to $n = 100$, sphere decoding can be used to perform ML decoding of convolutional lattices (with failure if the search radius is too small). Notice that such small-dimensional lattices are well suited to control applications where delay has to be minimized. Nevertheless, convolutional lattices would be interesting at large n, e.g. $n = 10000$ or more, for other applications in Information Theory and Coding Theory. Sphere decoding is not causal since it is a block-oriented decoding. However, because it is equivalent to a tree search, sphere decoding may become causal after relaxing its ML optimality. In this section, we consider the optimal (ML up to a radius failure) sphere decoder.

Sphere decoding is known to be implemented in two different methods [14]: 1- Pohst enumeration where points are enumerated inside a sphere of a well selected radius. The nearest point is kept as the best candidate. The sphere may be empty if the radius is too small. 2- Schnorr-Euchner enumeration where parallel hyperplanes are enumerated, then points inside those hyperplanes. In all cases, the inverse matrix G^{-1} is required to perform lattice decoding.

If G is ill-conditioned, then sphere decoding won't be possible because G^{-1} cannot be numerically determined with an acceptable accuracy. Indeed, the condition number of a matrix G is

$$\mathrm{cond}(G) = \mathrm{cond}(G^{-1}) = \|G\| \times \|G^{-1}\| \geq 1, \quad (8)$$

where $\|\cdot\|$ can be any matrix norm such as $\|\cdot\|_1$, $\|\cdot\|_2$, or $\|\cdot\|_\infty$. A matrix that is not invertible has condition number equal to infinity. The generator matrix G of Λ is always considered to be non-singular (non-zero fundamental volume). If the condition number is close to one, the matrix is well conditioned which means its inverse can be computed with good accuracy. If the condition number is very large, then the matrix is said to be ill-conditioned (nearly singular). The computation of the inverse of an ill-conditioned matrix is prone to large numerical errors. These errors may lead to direct failure of sphere decoding.

Definition 3. *Let Λ be a lattice defined by its $n \times n$ generator matrix. We say that sphere decoding of Λ is unstable if G is ill-conditioned, i.e.* $\mathrm{cond}(G) \gg 1$. *By abuse of vocabulary, we will say that the lattice Λ is unstable if* $\mathrm{cond}(G) \gg 1$.

In all its versions, on a Gaussian channel, the sphere decoder as an instance of ML decoding (with failure if the search radius is too small) looks for the vector $\hat{z}$ in $\mathbb{Z}^n$ that minimizes

$$\|y - \hat{z} \cdot G\|^2. \quad (9)$$

So the search made by the decoder is on z, not on x. For a given lattice point x, we have the trivial relation

$$z = x \cdot G^{-1}. \quad (10)$$

Again, we can see any potential instability of sphere decoding by looking at (10). When $\mathrm{cond}(G) \gg 1$, some of the entries of G^{-1} become very large in absolute value. For a lattice point x near the origin, the corresponding z may be extremely far from the origin. A 32-bit or even a 64-bit implementation of sphere decoding will fail for very ill-conditioned matrices. From a geometrical point of view, the condition number measures the amount of distortion of the unit sphere (or any other region like the lattice Voronoi region, in the corresponding vector norm used to define the matrix norm) under the transformation by the matrix. The larger $\mathrm{cond}(G)$, the more distorted the unit sphere becomes when transformed by G. In practice, this generates an overflow of z when the decoder is looking for the nearest lattice point.

Figure 1 shows a wrong performance of the KB lattice because its generator matrix is very ill-conditioned. The sphere decoder, or its implementation, was not set to detect that z_i was flipping around the 32-bit limit and so the decoder was too optimistically decoding the all-0 lattice point.

IV. Unstable Convolutional Lattices

We show in this section some simple examples that illustrate how the inverse of an apparently innocuous matrix, but with a large condition number, can be numerically very unstable. First of all, recall that the inverse of a matrix $M \in \mathrm{Mat}^{n\times n}(\mathbb{R})$ (if it exists) is equal to

$$M^{-1} = \frac{1}{\det(M)} \mathrm{Adj}(M); \quad (11)$$

$\mathrm{Adj}(M)$ is the so called adjoint matrix of M, whose (i, j)-th entry is equal (up to a sign change) to the (j, i)-th minor of M, which is the determinant of the $(n - 1) \times (n - 1)$ matrix obtained from M by eliminating its j-th row and i-th column.

Now, consider the $n \times n$ double-diagonal real generator matrix G of a convolutional lattice ($L = 2$):

$$G = \begin{pmatrix} g_{1,1} & 0 & 0 & \cdots & 0 \\ g_{2,1} & g_{2,2} & 0 & \cdots & 0 \\ 0 & g_{3,2} & \ddots & \cdots & 0 \\ \vdots & 0 & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & g_{n-1,n-1} & 0 \\ 0 & \cdots & 0 & g_{n,n-1} & g_{n,n} \end{pmatrix} \quad (12)$$

and let us call $H = G^{-1}$ its inverse. Applying (11), one can easily show the following proposition.

Proposition 1. *The (i, j)-th entry h_{ij} of $H = G^{-1}$, where G is double-diagonal, is equal to*

$$0, \quad \text{if } j > i, \quad (13)$$

$$g_{i,i}^{-1}, \quad \text{if } i = j. \quad (14)$$

For $j < i$, h_{ij} is given by the expression

$$\frac{(-1)^{i+j}}{\det(G)} \prod_{k=1}^{j-1} g_{k,k} \prod_{k=j+1}^{i} g_{k,k-1} \prod_{k=i+1}^{n} g_{k,k}. \quad (15)$$

Formula (15) can take very huge values, even if the entries of G are small. Expressions similar to (13)-(15) can be established for $L > 2$. Consider the following example:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 2 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 2 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 2 & 1 & 0 \\ 0 & \cdots & 0 & 0 & 2 & 1 \end{pmatrix}; \quad (16)$$

the determinant of G is equal to 1, all its entries are equal 1 or 2, but the $(n,1)$-th entry of its inverse is equal to 2^{n-1}. As another example, consider G in which the main diagonal contains only 1, while the second diagonal contains the numbers from 1 to $n-1$:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 2 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & n-2 & 1 & 0 \\ 0 & \cdots & 0 & 0 & n-1 & 1 \end{pmatrix}. \quad (17)$$

Whereas the biggest entry of this matrix is equal to n, the $(n,1)$-th entry of its inverse equals $(n-1)!$. The two convolutional matrices given in (6) and (7) are stable but their Hermite constant is poor. On the contrary, the KB construction with good (estimated) packing density turned to be unstable. Thus, while constructing good convolutional lattices, one should make a trade-off between packing-density and generator matrix stability.

A final example of an unstable convolutional lattice in $\mathbb{R}^{18}$ is given below. The generator matrix has 3 non-zero entries per column (except for the last two columns) that are cyclically shifted from one row to another. The first diagonal is given by the sequence

$$6, \frac{1}{16}, 3, 6, \frac{1}{16}, 3, \ldots, 6, \frac{1}{16}, 3. \quad (18)$$

The second diagonal has the sequence

$$3, 6, \frac{1}{16}, 3, 6, \frac{1}{16}, \ldots, \frac{1}{16}, 3, 6. \quad (19)$$

Finally the third diagonal includes

$$\frac{1}{16}, 3, 6, \frac{1}{16}, 3, 6, \ldots, 3, 6, \frac{1}{16}. \quad (20)$$

The generator matrix of the above 18-dimensional lattice is ill-conditioned. Its inverse includes rational numbers with huge integers and cannot be entirely shown in this paper. We show in (21) the first column of the matrix $H = G^{-1}$.

$$\begin{array}{c} \frac{1}{6} \\ -8 \\ \frac{4607}{288} \\ \frac{105985}{27648} \\ -\frac{990529}{576} \\ \frac{4564251647}{1327104} \\ \frac{104980331521}{127401984} \\ -\frac{981316647745}{2654208} \\ \frac{4521802132477439}{6115295232} \\ \frac{104003968574937601}{587068342272} \\ -\frac{972189978010605889}{12230590464} \\ \frac{4479747414704296998911}{28179280429056} \\ \frac{103036686633444629477377}{2705210921189376} \\ -\frac{963148190256669653268289}{56358560858112} \\ \frac{443808382401610031763079833 5}{12985012421709004 8} \\ \frac{102078400832849509976615818753}{12465611924840644608} \\ -\frac{954190495043940770961729099073}{259700248434180096} \\ \frac{439680772276164622308167107270963 1}{598349372392350941184} \end{array} \quad (21)$$

The inverse matrix in (21) was found via a special number theory software, Pari/gp, developed by the Mathematics Institute at Bordeaux, France. Mathematica by Wolfram fails in finding the exact inverse. MatLab by MathWorks displays a failure message.

From (15) and its generalization to $L > 2$, we deduce that the expression of $h_{i,j}$ includes products of terms belonging to the same diagonal in G. A stable G in large dimensions should include entries that compensate each other on the same diagonal. It is not clear how to select those elements and whether the best choice is to consider time-invariant or time-variant convolutional matrices. Nevertheless, we will show in the next section a convolutional structure that is sufficiently stable and exhibiting a positive fundamental gain.

V. Time-Alternating Stable Convolutional Lattices

We propose now an explicit construction of a stable n-dimensional convolutional lattice. The ℓ-th diagonal of its generator matrix, for $1 \leq \ell \leq L$, contains the elements

$$(n^{\alpha_\ell}, n^{-\alpha_\ell}, n^{\alpha_\ell}, n^{-\alpha_\ell}, \cdots, n^{(-1)^{n+2-\ell}\alpha_\ell}). \quad (22)$$

This lattice is named *time-alternating convolutional* lattice because the exponent alternates its sign along a diagonal. The generator matrix of a time-alternating

convolutional lattice looks like, for $n = 6$ and $L = 3$,

$$\begin{pmatrix} n^{\kappa_1} & 0 & 0 & 0 & 0 & 0 \\ n^{\kappa_2} & n^{-\kappa_1} & 0 & 0 & 0 & 0 \\ n^{\kappa_3} & n^{-\kappa_2} & n^{\kappa_1} & 0 & 0 & 0 \\ 0 & n^{-\kappa_3} & n^{\kappa_2} & n^{-\kappa_1} & 0 & 0 \\ 0 & 0 & n^{\kappa_3} & n^{-\kappa_2} & n^{\kappa_1} & 0 \\ 0 & 0 & 0 & n^{-\kappa_3} & n^{\kappa_2} & n^{-\kappa_1} \end{pmatrix}.$$

A time-alternating convolutional lattice has the following interesting features:

- It is completely determined by the *generating sequence* $(\kappa_1, \kappa_2, \ldots, \kappa_L)$.
- Its volume, for n even, is equal to 1 when no trellis termination is applied. Indeed, in order to avoid the first $L-1$ rows, the encoder and decoder consider $z_1 = z_2 = \ldots = z_{L-1} = 0$. This is equivalent to deleting the first $L-1$ rows from G because they have weak norm. This operation is named *trellis termination*. After trellis termination, the new Gram matrix satisfies $vol^{2/n} = (\det\ \Gamma)^{1/n} \to 1$ for large n.
- The product of an even number of consecutive elements on the same diagonal is equal to 1.
- Numerical simulations show that, for reasonable choices of the κ_ℓ, the lattice is stable. Namely, we considered $\kappa_\ell = \kappa_1 + (\ell - 1) \times \Delta$. For example, at $n = 64$ and $L = 5$, a good choice is $\kappa_1 = 0.8$ and $\Delta = 0.0775$ leading to a fundamental gain (Hermite constant) of 4.93 dB. The performance is shown in Figure 2. Intuitively, we can understand that stability comes from the fact that all the elements of the inverse of the generator matrix come from some generalization of (15). Since our particular construction keeps under control the product of consecutive elements on a diagonal, stability can be obtained.
- In every row, the exponents of n have alternate positive and negative sign. This avoids rows to have too big or too small norm with respect to other rows and helps obtaining a good fundamental gain for the lattice.

It can be shown that, in order to find a reliable estimation of the minimum distance of the lattice, it is sufficient to investigate the Theta series (up to a certain layer via Pohst enumeration) of a lattice generated by L consecutive rows of G. Furthermore, the shortest vector satisfies the following.

Theorem 2. *Let the shortest vector of a time-alternating convolutional lattice be $x_0 = z_0 G$ and let $\kappa_\ell = \kappa_1 + (\ell-1) \times \Delta$, where $0 < \kappa_1 < \kappa_2 < \ldots < \kappa_L$. For $L \geq 3$ and n large enough, if $\Delta < \frac{1}{\log_2(n)}$ then the Hamming weight of z_0 is greater than 1.*

VI. Conclusions

Convolutional lattices in the Euclidean space are a good imitation of binary convolutional codes. Stability is an important issue when building convolutional lattices. We proposed time-alternating convolutional lattices to render a good packing density with stable sphere decoding. Besides sphere decoding, for reasonable constraint length L, convolutional lattices also admit message-passing (belief propagation) decoding. Time-alternating convolutional lattices are dense enough at small dimensions but not too dense. They are good constituents for building new turbo lattices.

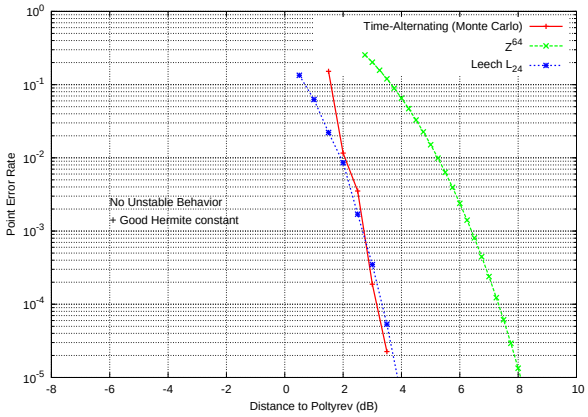

Figure 2. Performance of the time-alternating stable convolutional lattice, at dimension $n = 64$, constraint length $L = 5$, exponent $\kappa_1 = 0.08$, and step $\Delta = 0.0775$.

Acknowledgment

This work was supported by the Qatar National Research Fund (QNRF), a member of Qatar Foundation, under NPRP project 6-784-2-329.

References

[1] J.H. Conway and N.J.A. Sloane. *Sphere packings, lattices and groups*. Springer-Verlag, New York, 3rd edition, 1999.

[2] R. Zamir, *Lattice coding for signals and networks.* Cambridge University Press, 2014.

[3] D. Micciancio and S. Goldwasser, *Complexity of lattice problems: a cryptographic perspective.* Springer, 2002.

[4] S. Lang, *Algebra.* 3rd edition, Springer, 2005.

[5] O. Shalvi, N. Sommer, and M. Feder, "Signal codes: Convolutional lattice codes," *IEEE Trans. on Inf. Theory*, vol. 57, no. 8, pp. 5203–5225, Aug. 2011.

[6] P. Mitran and H. Ochiai, "Parallel Concatenated Convolutional Lattice Codes With Constrained States," *IEEE Trans. on Comm.*, vol. 63, no. 4, pp. 1081-1090, April 2015.

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

[8] H. Minkowski, Diskontinuitäsbereich für arithmetische Aequivallenz, J. Reine Angew. Math., 129, 1905, 220–274.

[9] G.A. Kabatiansky and V.I. Levenshtein, "Bounds for packings on a sphere and in space," *Problems of Information Transmission*, PPI 14:1, pp. 1-17, 1978.

[10] H. Cohen, *A course in computational algebraic number theory*, 3rd ed., Berlin, Heidelberg, Germany: Springer-Verlag, 1996.

[11] R.A. Horn and C.R. Johnson. *Matrix analysis*. Cambridge, 1985.

[12] A. Bjorck. *Numerical methods for least squares problems*. SIAM Publications, Philadelphia, PA, 1996.

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

[14] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Trans. on Inf. Theory*, vol. 48, no. 8, pp. 2201-2214, Aug. 2002.