Trellis Detection for Random Lattices

Francisco A. Monteiro[1,3] and Frank R. Kschischang[2]

[1] *The Computer Laboratory, University of Cambridge, UK*
[2] *Dept. of Electrical and Computer Eng., University of Toronto, Canada*
[3] *Instituto de Telecomunicações, Instituto Universitário de Lisboa (ISCTE-IUL), Portugal*
fatbnm2@cam.ac.uk , frank@comm.utoronto.ca

Abstract— **In general, lattice problems are simple to describe but rather hard to solve optimally. Several suboptimal solutions have been proposed for the closest vector problem (CVP), which is central in multiple-input multiple-output (MIMO) communication systems. It is known that some lattices have a trellis representation, however, those lattices require very particular geometries that are not found in lattices randomly generated. In this paper we show that for the typical number of dimensions used in MIMO communication, with high probability, there exists a synthetic lattice that is a member of the family of lattices that have a trellis representation and which is sufficiently close to any given random lattice. For that purpose we present a method to find a trellis-oriented basis for a given random lattice. The basis vectors of the synthetic lattice and the basis vectors of the original lattice are close and for finite alphabets the two lattices are roughly the same in the region of interest. Therefore, the optimal decision (Voronoi) regions of both lattices chiefly overlap. A linear transformation then focuses the original lattice onto the synthetic one, known to have a trellis representation. This minimizes the distortion of the Voronoi regions associated with maximum-likelihood detection and therefore the performance attained in the MIMO-CVP is close to optimal.**

Keywords: *Lattices with trellis, quotient group, rectangular sublattices, cosets, closest vector problem.*

I. Introduction

The regularity of a lattice lends itself for the representation of problems where signals are interpreted as a point in a multidimensional space defined in some basis. One of the most important lattice problems is the closest vector problem (CVP) [1], which consists in finding the point that is the one at the shortest distance from a given off-lattice target point.

Forney's pioneering work [2] showed that some lattices can be described by a trellis, where each segment of the trellis is associated with the coordinates of the lattice points in each dimension of the space. The lattices for which a trellis exists, can be said to constitute a *family* of lattices, denoted by $\mathcal{L}_R$.

These properties have been used in coding theory for detecting lattice codes [3]. However, this approach requires a rather restricted type of lattice allowing a trellis representation. Some well known lattices belong to $\mathcal{L}_R$ (such as A_2, D_4, E_8, or the Leech lattice in $\mathbb{R}^{24}$) [4] but others are constructed imposing a specific geometrical structure during the design of the code. Maximum likelihood detection (MLD) can in those cases be attained through trellis detection, and therefore the CVP is in those cases solved with the Viterbi algorithm. This circumvents the exponential complexity of MLD (measuring the distance from the given point to all the points in the lattice). The complex lattice associated with a MIMO link with N_T transmit antennas and a M-QAM modulation will have M^{N_T} complex points within its border.

Clearly, the trellis detection approach cannot be extended to any random lattice. However, one should ask the question, for any given lattice, can one find a lattice that is sufficiently "similar" or "close" to it, and yet is simultaneously a member of the family of lattices with a trellis representation, $\mathcal{L}_R$. This paper deals with that question. As lattices are defined by generator matrices, the problem can be seen as a *matrix nearness problem* [5]; as in many other matrix nearness problems, the one we formulate also does not seem to have an analytical solution and therefore we take an algorithmic approach. To the best of our knowledge the approximation of a random lattice by a lattice in $\mathcal{L}_R$ is a new approach to MIMO detection. In [6] the authors use a trellis detector but their approach is clearly sub-optimal, as it is based on a transformation of a tree data structure (associated with a sphere decoder) into a trellis data structure, and ends up losing many of the branches.

In MIMO, one has to detect a vector $\mathbf{x}$ from a real vector $\mathbf{y}$ obtained after a channel $\mathbf{H}$ and perturbed by the additive noise vector $\mathbf{n}$, that is, $\mathbf{y} = \mathbf{Hx} + \mathbf{n}$.

In this paper we derive the property that makes a lattice a member of $\mathcal{L}_R$ and presents an algorithm to find such a lattice which is "nearby" a given random lattice. Then the paper presents results for typical detection in MIMO spatial multiplexing, comparing the results with the most important sub-optimal receivers and MLD.

II. Lattices

Lattices are discrete subgroups in $\mathbb{C}^n$. The most common manner to specify a lattice Λ is based on on a set of vectors which are the columns of a *generator matrix* $\mathbf{H}$:

$$\Lambda = \left\{ \mathbf{y} \in \mathbb{C}^n : \mathbf{y} = \sum_{i=1}^{n} \mathbf{h}_i x_i = \mathbf{H} \cdot \mathbf{x} \,, \quad x_i \in \mathbb{Z} \right\}. \qquad (1)$$

The coordinates of the lattice points are thus integer combinations of the columns of the complex generator matrix $\mathbf{H}$ (some authors prefer to span the row space though).

Hereafter, we assume a real-valued model, obtained by stacking the real and imaginary components of the equivalent model of complex lattices as described, e.g., in [7].

The *dual lattice* of a real *primal lattice* is generated by the dual basis $\mathbf{H}^{(D)} = (\mathbf{H}^{-1})^T$ and $\mathrm{vol}(\Lambda_D) = (\mathrm{vol}(\Lambda))^{-1}$ [8].

The region of space whose points are closer to the origin than to any other point of the lattice is called the Voronoi region. This is the most interesting fundamental region amid the infinite number of other possible tilings of the space.

III. Focusing Onto the $\mathcal{L}_R$ Family

We call $\mathcal{M}$ the set of all possible lattices in $\mathbb{R}^n$. Hence, $\mathbb{Z}^n$ is just one particular lattice in $\mathcal{M}$ (see Figure 1). Moreover, all lattices with a trellis representation are also members of that $\mathcal{M}$ and we say that they constitute the $\mathcal{L}_\mathrm{R}$ family of lattices.

It is well known that the simplest way of solving the CVP amounts to the least-squares solution given by the Moore-Penrose pseudo-inverse of the generator matrix. In the MIMO context this is known as the zero-forcing (ZF) solution. Geometrically, this type of linear receiver applies a linear transformation that takes the received lattice Λ and transforms it back into the original $\mathbb{Z}^n$. We will call this procedure a *focusing* of the received lattice Λ onto $\mathbb{Z}^n$, and we propose to generalize this concept of focusing by means of a linear transformation $\mathcal{F}$. The ZF focusing approach presents the lowest complexity among all sub-optimal receivers but also results in the poorest performance (in terms of erroneous decisions). The poor performance is a direct consequence of the potentially huge mismatch between the optimal decision regions in MLD and the decision regions associated with focusing onto $\mathbb{Z}^n$. These decision regions are nothing but linear transformations of *n*-dimensional hypercubes. Note that the convenience of the ZF receiver comes from the fact that the destination lattice is $\mathbb{Z}^n$, which allows detection by means of a simple slicer.

We argue that it is possible to perform a linear transformation from any received lattice Λ onto other lattices in $\mathcal{M}$ which also lend themselves to another convenient detection method, namely, the Viterbi algorithm. Figure 1 depicts the set of all lattices, including the particular $\mathcal{L}_\mathrm{R}$ family. Any given lattice may be closer to one lattice in $\mathcal{L}_\mathrm{R}$ than to $\mathbb{Z}^n$, as those are infinitely many more. Again, notice that ZF would focus any received lattice always onto $\mathbb{Z}^n$, regardless the distance to it.

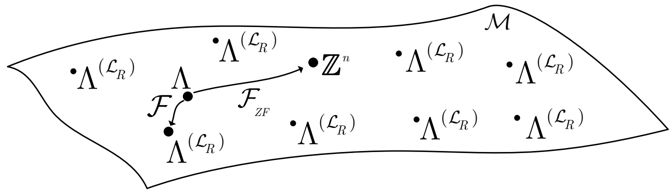
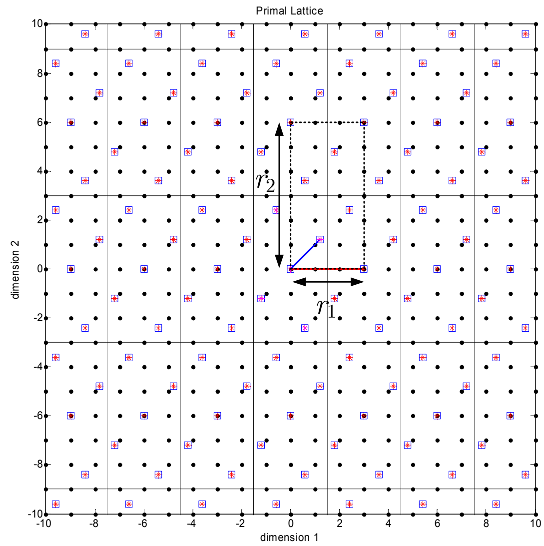


Figure 1. The set of lattices and the focusing operator. A received lattice Λ can be focused onto the nearest member of $\mathcal{L}_R$ or onto $\mathbb{Z}^n$.

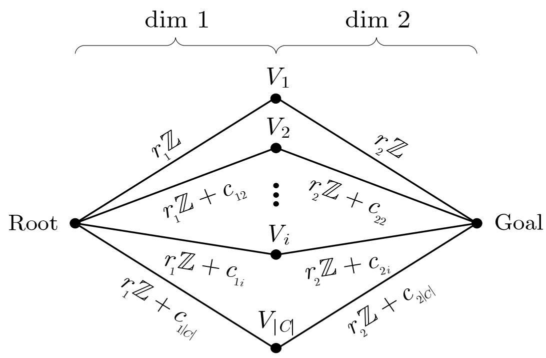
When the distance between lattices is reduced, then the matching (or coverage [7]) between their decision regions is maximized, which minimizes the distortion created by linearly transforming one lattice onto another one. If there is a member of $\mathcal{L}_\mathrm{R}$ nearby Λ (i.e. very "similar" to Λ), then *i)* its MLD regions will mach closely the ones of the original lattice and *ii)* the distortion involved in the focusing operation will be small.

IV. The $\mathcal{L}_R$ Family of Lattices

A lattice has a trellis if it can be written as the union of a *rectangular sublattice* Λ_R and translated versions of it. As noticed by Forney [2], such a lattice is given by $\Lambda = \Lambda_R + [\Lambda/\Lambda_R]$, where $[\Lambda/\Lambda_R]$ is a "system of coset representatives" for the cosets of Λ_R in Λ or, equivalently, for the elements of the quotient group Λ/Λ_R. As Λ_R is a rectangular lattice, by definition it can be expressed by a Cartesian product, i.e., $\Lambda_R = r_1\mathbb{Z} \times \cdots \times r_n\mathbb{Z}$.



(a) Rectangular sub-lattice in a lattice that has a trellis representation.



(b) Trellis of the 2D lattice.

Figure 2. A rectangular sub-lattice in a random lattice and the trellis representation of the lattice.

Figure 2 shows an example of a lattice in $\mathbb{Z}^2$ and its representation by a trellis. It is possible to observe the rectangular quotient group and its translated versions.The lattice is then the union of the cosets of Λ_R in Λ . For the case in Figure 2 , the index of Λ_R in Λ is $|C|=|\Lambda/\Lambda_R|=5$. In general,

$$\left|C\right| = \frac{\det(\Lambda_R)}{\det(\Lambda)}. \tag{2}$$

Using the origin as a representative of Λ_R, the set constituted by the origin together with all the other points with coordinates (c_{1i}, c_{2i}), i=1,2....$|C|$, that are inside the central rectangular region are the *coset representatives* of the quotient group. The whole lattice can now be seen as a tiling of the space using that fundamental region. The coefficients $r_1, r_2, \cdots r_n$ have now a simple geometrical interpretation as they define the lengths of the fundamental hyper-rectangle.

There is a strong connection between the way the trellis of binary block codes and group codes are obtained from a trellis-oriented generator matrix [3], [9] , and how the trellis of a lattice is obtained from the basis of a lattice in $\mathcal{L}_R$, [2], [10]. The n-dimensional orthogonal sublattice has its basis vectors along one-dimensional subspaces W_i, i=1,...,n. From these we can define the sequence of spaces $\{\mathbf{0}\} \subset V_0 \subset V_1 \subset \cdots \subset V_n = \mathbb{R}^n$ and each W_i, is the 1-D orthogonal complement of V_{i-1} to V_i. We denote the projections onto V_i and W_i respectively by P_i and the P_{W_i} and define the intersection lattices $\Lambda_i = \Lambda \cap V_i$ and the one-dimensional lattices $\Lambda_{W_i} = \Lambda \cap W_i$.

Using these definitions, the state space of a trellis of a lattice in the coordinate system $\{W_i\}_{i=1}^n$ is $P_i(\Lambda) / \Lambda_1$ and the label group for the trellis branches is $P_{W_i}(\Lambda) / \Lambda_{W_i}$ [11], [12] [13].

V. Orthogonal Sublattices

We are interested in finding what properties a generator matrix must have so that it generates a lattice $\Lambda \in \mathcal{L}_R$.

A. Properties of the generator matrix

A lattice can only be written as in the form $\Lambda = \Lambda_R + [\Lambda/\Lambda_R]$ if and only if it contains a rectangular sublattice. Given a lattice, to find if a rectangular sublattice in it is believed to be itself an NP-hard problem. Micciancio calls it the *quasi orthogonal set problem* [8] that we may appropriately call it the *quasi orthogonal sublattice problem* (QOSP). This problem deserved virtually no attention in the literature, apparently due to lack of applications.

In addition to the problem of discovering a rectangular sublattice we add an additional constraint: we want to find the rectangular sublattice that minimizes the index number of the quotient group in order to minimize the number of trellis paths. The problem does not seem to have an analytical solution; consequently, we revert to an algorithmic approach.

Let us consider a random rational lattice defined by a rational $\mathbf{H}$ with entries $h_{ij}=n_{ij}/d_{ij}$ and whose inverse is the rational matrix $\mathbf{W}=\mathbf{H}^{-1}$ with entries p_{ij}/q_{ij}. For lattice points, because $\mathbf{x} = \mathbf{H}^{-1}\mathbf{y}$ (no noise), one should force

$$\begin{bmatrix} x_1 \\ \vdots \\ x_i \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \frac{p_{11}}{q_{11}} & \frac{p_{12}}{q_{12}} & \cdots & \frac{p_{1n}}{q_{1n}} \\ \frac{p_{21}}{q_{21}} & \frac{p_{22}}{q_{22}} & \cdots & \frac{p_{2n}}{q_{2n}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{p_{n1}}{q_{n1}} & \frac{p_{n2}}{q_{n2}} & \cdots & \frac{p_{nn}}{q_{nn}} \end{bmatrix} \cdot \begin{bmatrix} kr_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{p_{11}}{q_{11}} kr_1 \\ \frac{p_{21}}{q_{21}} kr_1 \\ \vdots \\ \frac{p_{n1}}{q_{n1}} kr_1 \end{bmatrix} \tag{3}$$

for $k \in \mathbb{Z}$. As $\mathbf{x} \in \mathbb{Z}$, then $\frac{p_{i1}}{q_{i1}} kr_1 \in \mathbb{Z} \Rightarrow \frac{r_1}{q_{i1}} \in \mathbb{Z}$ and thus $q_{i1} \left| r_1 \right.$, where $q_{i1} \left| r \right.$ denotes that q_{i1} divides r . Hence,

$$r_1 = \operatorname{lcm}\left(q_{11}, q_{21}, \cdots, q_{n1}\right), \tag{4}$$

where lcm stands for *lowest common multiple*. Applying the same reasoning to each dimension one gets the rule $r_i = \operatorname{lcm}\left(q_{1i}, q_{2i}, \cdots, q_{ni}\right)$. Finally, we can interpret the property in terms of the columns of $\mathbf{H}^{(D)}$, the generator matrix of the dual lattice (henceforth called the *dual matrix*). In conclusion, the sublattice Λ_R of $\Lambda \in \mathcal{L}_R$ in the original system of coordinates is completely defined by the denominators q_{ij} of the dual lattice, so that

$$r_i = \operatorname{lcm}\left(q_{i1}, q_{i2}, \cdots, q_{in}\right),\ i = 1, 2, \ldots n. \tag{5}$$

B. Algorithm

Given rule (5) for the dual matrix and noting that the lattice equivalence problem is untreatable [1], we reduce the problem to finding a similar lattice to the problem of finding a close (in the Frobenius sense) dual generator matrix. For that purpose, one starts by applying a QR decomposition to the dual matrix, reducing it to the upper triangular (u.t) form via a rigid rotation of the lattice, $\mathbf{Q}$. To make the elements in this matrix shorter, we *i)* LLL-reduce this rotated dual lattice and then *ii)* find rational approximations for the matrix elements via a greedy algorithm. (Notice that the Diophantine approximation problem is itself a NP-hard problem, solvable by mapping it onto another CVP [14]). The algorithm finds an approximated (or *synthetic*) dual lattice:

$$\tilde{\mathbf{H}}^{(D)} = \left(\mathbf{h}_1^{(D)}\ \mathbf{h}_2^{(D)} \cdots \mathbf{h}_n^{(D)}\right) = \begin{pmatrix} \frac{p_{11}}{r_1} & \frac{p_{12}}{r_1} & \cdots & \frac{p_{1n}}{r_1} \\ 0 & \frac{p_{22}}{r_2} & \cdots & \frac{p_{2n}}{r_2} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \frac{p_{nn}}{r_n} \end{pmatrix}. \tag{6}$$

ALGORITHM 1: SYNTHESIS OF A LATTICE IN $\mathcal{L}_R$
Input: Generator $\mathbf{H}$, Admissible numb. of paths Γ.
Output: Approximation $\tilde{\mathbf{H}} \in \mathcal{L}_R$; number of cosets $|C|$.
$\mathbf{H}_{\text{red}}^{(D)}, \mathbf{M} \leftarrow \text{LLL}\{(\mathbf{H}^{-1})^T\}$, $\mathbf{M}$ unimodular
Sort columns by increasing norm
$\mathbf{Q}, \widehat{\mathbf{H}}_{\text{red}}^{(D)}, \mathbf{J} \leftarrow QR\left(\text{sort}(\mathbf{H}_{\text{red}}^{(D)})\right)$; $\mathbf{J}$ permutation, $\widehat{\mathbf{H}}_{\text{red}}^{(D)}$ u.t.
Do until $\left|C\right| < \Gamma$
Obtain $\tilde{\mathbf{H}}_{\text{red}}^{(D)}$: for each row *i*, obtain rational approximation of each q_{ij} using a common denominator r_i and with maximum error δ
$\mathbf{P}, \mathbf{R} \leftarrow \tilde{\mathbf{H}}_{\text{red}}^{(D)}$; as in expression (8)
$\left|C\right| = \prod_{i=1}^{n} p_i$
increment δ
end loop
$\tilde{\mathbf{H}} = \mathbf{Q}^T \left((\tilde{\mathbf{H}}_{\text{red}}^{(D)} \cdot \mathbf{J}^{-1})^{-1}\right)^T \mathbf{M}^{-1}$

C. Geometrical interpretation: distortion vs number of cosets

The number of cosets in a quotient group is

$$\left|\frac{\tilde{\Lambda}}{\Lambda_R}\right| = \frac{\text{Vol}\left(\Lambda_R\right)}{\text{Vol}\left(\tilde{\Lambda}\right)} = \frac{\prod_{i=1}^{n} r_i}{\det\left(\tilde{\mathbf{H}}\right)} = \prod_{i=1}^{n} r_i \cdot \det\left(\tilde{\mathbf{H}}_D\right). \quad (7)$$

In order to calculate $\det(\tilde{\mathbf{H}}_D)$ one should observe that (6) is uniquely defined by two matrices: one is $\mathbf{P}$, comprising the denominators of $\tilde{\mathbf{H}}_D$, and the other we call $\mathbf{R}$, with the numerators of $\tilde{\mathbf{H}}_D$, and both matrices are u.t.:

$$\mathbf{P} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ 0 & p_{22} & \cdots & p_{21} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p_{nn} \end{bmatrix} \text{ and } \mathbf{R} = \begin{bmatrix} r_1 & r_1 & \cdots & r_1 \\ 0 & r_2 & \cdots & r_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & q_n \end{bmatrix}. \quad (8)$$

Note that the non-zero elements of $\mathbf{R}$ in each row are forced to be equal. The determinant of $\tilde{\mathbf{H}}_D$ is then

$$\det\left(\tilde{\mathbf{H}}_D\right) = \prod_{i=1}^{n} \frac{p_{ii}}{r_i} = \underbrace{\prod_{i=1}^{n} p_{ii}}_{\substack{\text{product diagonal} \\ \text{numerators}}} \cdot \underbrace{\prod_{i=1}^{n} \frac{1}{r_i}}_{\substack{\text{volume of} \\ \text{quantization grid}}} \quad (9)$$

and (7) comes as

$$\left|\frac{\tilde{\Lambda}}{\Lambda_R}\right| = \prod_{i=1}^{n} r_i \cdot \prod_{i=1}^{n} p_i \cdot \prod_{i=1}^{n} \frac{1}{r_i} = \prod_{i=1}^{n} p_i . \quad (10)$$

The number of cosets is thus solely determined by $\text{diag}(\mathbf{P})$. Geometrical insight into the problem can now be given from:

$$\left|\frac{\Lambda}{\Lambda_R}\right| = \frac{\text{Vol}\left(\Lambda_R\right)}{\text{Vol}\left(\tilde{\Lambda}\right)} = \text{Vol}\left(\Lambda_R\right)\text{Vol}\left(\tilde{\Lambda}_D\right)$$

$$= \prod_{i=1}^{n} r_i \cdot \text{Vol}\left(\tilde{\Lambda}_D\right) = \text{Vol}\left(\tilde{\Lambda}_D\right) \Big/ \frac{1}{\prod_{i=1}^{n} r_i} = \frac{\text{Vol}\left(\tilde{\Lambda}_D\right)}{\text{Vol}(\varepsilon_q)}. \quad (11)$$

The denominator $\left(\prod_{i=1}^{n} r_i\right)^{-1}$ corresponds to the volume of the elementary quantization grid (see Figure 3).

In order to reduce the number of paths in the trellis of a lattice in $\mathcal{L}_R$, one wants to keep low value entries in $\text{diag}(\mathbf{P})$, while at the same time, a good approximation that minimizes $\left\|\mathbf{H}^{(D)} - \tilde{\mathbf{H}}^{(D)}\right\|_F$, implies having larger r_i values (as these ratios are fixed, this constitutes another constraint into the problem).

Algorithm 1 outputs $\tilde{\Lambda}(\tilde{\mathbf{H}})$ and, by construction, the shape of the Voronoi regions of this lattice are similar to the ones of the original Λ. Using the concept introduced in Section III, the focusing linear transformation is

$$\mathcal{F}(\mathbf{H}, \tilde{\mathbf{H}}) = \tilde{\mathbf{H}} \cdot \mathbf{H}^{-1}, \quad (12)$$

with $\mathcal{F}$ close to the identity matrix, i.e., $\left\|\mathcal{F} - \mathbf{I}\right\|_F < \varepsilon$. By allowing an increasing number of cosets, ε can be reduced towards zero.

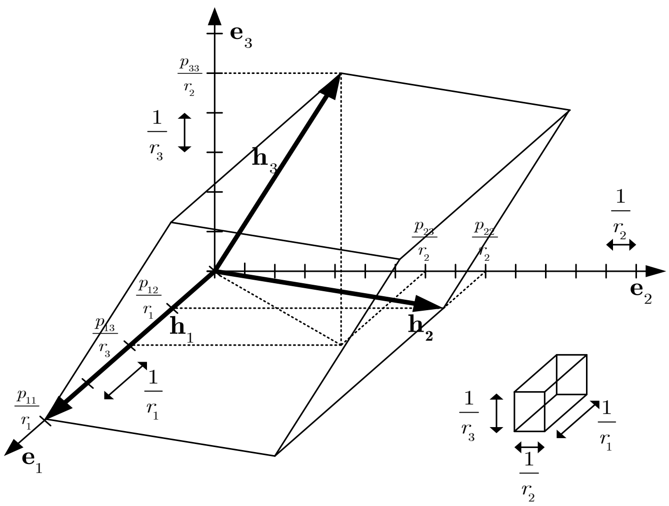


Figure 3. Approximation versus number of cosets: the dilemma of the approximation in the dual lattice (example in a 3D space).

VI. RESULTS AND DISCUSSION

We have assessed the proposed receiver using lattices which arise in MIMO communications under Rayleigh flat fading channel and compared its performance with the one of lattice-reduction-aided receivers (with ZF and with ordered successive interference cancellation (OSIC) schemes), which are well known for capturing the full diversity provided by MLD [15]. The performances of linear ZF, linear minimum mean square error (MMSE) and OSIC without lattice-reduction are also included in the results presented in Figure 4. The proposed trellis-based detection also attains full diversity while reducing the gap between lattice reduction and MLD and the required number of cosets needed to achieve quasi-optimum detection is surprisingly small. Algorithm 1 searches for an approximate lattice with a specified maximum number of cosets Γ (i.e., paths in a trellis). However, their average number is about half of the specified Γ. Figure 4 shows the performance for a typical benchmarking MIMO configuration (4×4 antennas with 64 QAM). Limiting the admissible number of cosets to Γ=100, we observe that an average of 38 paths is enough to synthesise good approximated lattices in $\mathcal{L}_R$ to achieve a performance about 1.2 dB away from ML, coinciding with the performance of LLL-OSIC-ZF. With an average of 506 cosets, the gap shortens to 0.6 dB. The complexity in Algorithm 1 is dominated by the LLL reduction, $\mathcal{O}(n^4)$, added to $\mathcal{O}(n^3)$ in the QR decomposition, and the complexity of the iterations for rational approximation, dominated by a continued fractions algorithm, $\mathcal{O}(n^3)$ [16] . Sphere decoding is well known to have a random number of branch expansions during the exploration of the tree (unless fixed complexity sphere decoding is used [17]). That number varies each time a received vector is decoded, and is highly dependent on the noise power. We note that, while in the proposed detector the number of cosets is also a random variable, it only affects the pre-processing stage. Then, the complexity remains constant over the coherence time of that lattice instance. For 2×2 configuration with 64-QAM, an average of 20 cosets have been found to assure the same performance as MLD and for the 3×3 setup, the performance is 0.2 dB away from MLD with 34 cosets on average.

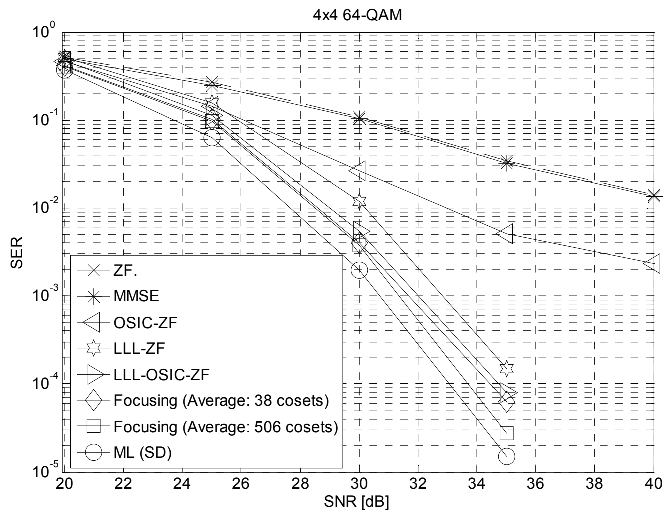


Figure 4. Symbol error probability when detecting in a lattice with n=8 real dimensions (4×4 MIMO configuration) with 64-QAM.

The number of cosets needed for near-optimal performance diminishes for smaller alphabets (smaller M). This happens because the distortion between the received lattice and the approximated lattice in $\mathcal{L}_R$ increases as one gets further away from the origin. It should also be noticed that, by construction, the number of trellis paths is an upper bound on the number of trellis states. Finally, note that the length of the trellises (number of segments) is determined by the dimensionality of the lattice (n=2N_R) and therefore, for the typical number of antennas in MIMO, these trellises are rather short.

ACKNOWLEDGMENTS

Francisco Monteiro was funded for this research with grants from the Royal Academy of Engineering, the Cambridge Philosophical Society, The Computer Lab., and Fitzwilliam College (UK) and with scholarships from the Gulbenkian Foundation and the Foundation for Science and Technology (Portugal). Francisco Monteiro is thankful to Oded Regev for discussions on the *quasi orthogonal sublattice problem.*

REFERENCES

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

[2] G. D. Forney Jr., "Coset codes-part II: binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. 34, no. 5, pp. 1152-1187, Sep. 1988.

[3] F. R. Kschischang and V. Sorokine, "On the trellis structure of block codes," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1924-1937, Nov. 1995.

[4] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, New York, USA: Springer, 1999.

[5] N. H. Higham, "Matrix nearness problems and applications," in *Applications of Matrix Theory*, M. J. C. Gover and S. Barnett, Eds. Oxford, UK: Oxford University Press, 1989, pp. 1-27.

[6] J. Lee and S.-C. Park, "MIMO Detector Based on Trellis," *IEICE Trans. on Communications*, vol. E91-B, no. 3, pp. 951-954, March 2008.

[7] K. Su and F. R. Kschischang, "Coset-based lattice detection for MIMO systems," in *Proc. of ISIT'07 - IEEE Inter. Symp. on Information Theory*, Nice, France, June 2007, pp. 1941 - 1945.

[8] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems - A Cryptographic Perspective*. Norwell, Massachusetts, USA: Kluwer Academic Publishers, 2002.

[9] A. Vardy, "Trellis Structure of Codes," in *Handbook of Coding Theory*, Vera Pless and W. Cary Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, ch. 24, pp. 1989-2117.

[10] G. D. Forney Jr., "Density / length profiles and trellis complexity of lattices," *IEEE Trans. Inform. Theory*, vol. 40, no. 6, pp. 1753-1772, Nov. 1994.

[11] A. H. Banihashemi, "Decoding complexity and trellis structure of lattices," PhD thesis, University of Waterloo, Ontario, Canada, 1997.

[12] A. H. Banihashemi and F. R. Kschischang, "Tanner graphs for group block codes and lattices: construction and complexity," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 822-834, Feb. 2001.

[13] H. Kan and H. Shen, "The bases associated with trellis of a lattice," *IEICE Trans. on Fundamentals*, vol. E88, no. 7, pp. 2030-2033, July 2005.

[14] L. Lovász, *An Algorithmic Theory of Numbers, Graphs and Convexity*. Philadelphia, Pennsylvania, USA: Society for Industrial and Applied Mathematics (SIAM), 1986, ch. 1, pp. 15-38.

[15] Mahmoud Taherzadeh, Amin Mobasher, and Amir K. Khandani, "LLL reduction achieves the receive diversity in MIMO decoding," *IEEE Trans. on Inf. Theory*, vol. 53, no. 12, pp. 4801-4805, Dec. 2007.

[16] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press, 2010, ch. 5, p. 230.

[17] L. G. Barbero and J. S. Thompson, "Fixing the complexity of the sphere decoder for MIMO detection," *Trans. Wireless Commun*, vol. 7, no. 6, pp. 2131-2142, June 2008.