International Symposium on Information Theory and its Applications, ISITA2004
Parma, Italy, October 10–13, 2004

A Very Efficient Lattice Reduction Tool on Fast Fading Channels

Ghaya Rekaya[†], Jean-Claude Belfiore[†] and Emanuele Viterbo[‡]

[†] École Nationale Supérieure des Télécommunications
46, rue Barrault
75013 Paris - FRANCE
Emails: rekaya,belfiore@enst.fr

[‡] Politecnico di Torino
C.so Duca degli Abruzze, 24
10129 Torino - ITALY
Email: viterbo@polito.it

Abstract

We present a very efficient lattice reduction tool for algebraic lattices by using the matrix representation of units in number fields. This algorithm requires a careful study of the so-called "logarithmic lattice". From this algorithm, very efficient suboptimal decoders can be derived on fast fading channels.

1. Introduction

Orthogonal or unitary linear precoders are known to bring diversity to a communication system on a fast fading channel. This kind of diversity is known as "modulation diversity" [1]. In order to decode such a system, we need a lattice decoder [2]. But this decoder can become very complex to implement when the dimension of the precoder increases. In order to simplify it, one may use lattice reduction for fast fading channels [3] as well as for MIMO channels [4]. The most popular of all reduction algorithms is the so-called LLL algorithm [5]. This algorithm may be used for every lattice. We specialize to the case of algebraic lattices constructed from number fields and present a new reduction algorithm, with a huge reduction in complexity when compared to the LLL.

2. Notations, assumptions and system model

2.1. Notations

Our system uses QAM (complex case) or PAM (real case) constellations. Each QAM (resp. PAM) signal is denoted x_i. The vector of QAM (PAM) signals has length n and is denoted $\mathbf{x} = (x_1, x_2, \cdots, x_n)^\top$. We do not consider, in this paper, the shaping problems which can be solved by, for example, with mod Λ precoding [6]. So, we assume that the transmitter sends a point $\mathbf{x}$ of $\mathbb{Z}[i]^n$ in the complex case or $\mathbb{Z}^n$ in the real case. We use a linear transform Φ to introduce diversity, which is a unitary matrix (for the complex case) or an orthogonal one (for the real case). The channel matrix is assumed to be a diagonal *i.i.d.* matrix,

$$\mathbf{H} = \text{diag}\,[h_1, h_2, \ldots, h_n] \tag{1}$$

known at the receiver (perfect CSI). Finally, the noise is an $n-$dimensional vector $\mathbf{b}$ of *i.i.d* Gaussian variables. To summarize, the received signal is

$$\mathbf{y} = \mathbf{H} \cdot \Phi \cdot \mathbf{x} + \mathbf{b} \tag{2}$$

2.2. Number theory bases

In all the paper, $\mathbb{Q}$ is the field of rationals with its ring of integers $\mathbb{Z}$, $\mathbb{Q}(i) = \{p + iq | p, q \in \mathbb{Q}\}$ ($i = \sqrt{-1}$) is the field of rational complexes with its ring of Gaussian integers $\mathbb{Z}[i]$. In the real case, we use $\mathbb{F} = \mathbb{Q}$ as the base field and in the complex case, we use $\mathbb{F} = \mathbb{Q}(i)$ as the base field.

Now, let θ be an algebraic number of degree n on $\mathbb{F}$. Let $\mathbb{K} = \mathbb{F}(\theta)$ be the smallest field containing $\mathbb{F}$ and θ. $Gal_{\mathbb{K}/\mathbb{F}}$ is the Galois group of automorphisms on $\mathbb{K}$ with elements denoted $\sigma_i, i = 1, \ldots, N$. We assume in the following that the extension $\mathbb{F}(\theta)$ is Galois, which means that $N = n$.

$\mathcal{O}_\mathbb{K}$ is the ring of integers of $\mathbb{K}$ and for each $\alpha \in \mathbb{K}$ we define two quantities

- The trace of α, $\text{Tr}_{\mathbb{K}/\mathbb{F}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \in \mathbb{F}$
- The norm of α, $N_{\mathbb{K}/\mathbb{F}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \in \mathbb{F}$

Units of $\mathcal{O}_\mathbb{K}$ are algebraic integers which are invertible in $\mathcal{O}_\mathbb{K}$. Then, their norms are units in $\mathcal{O}_\mathbb{F}$. For example, if $\mathbb{F} = \mathbb{Q}$, then units of $\mathbb{F}$ are 1 and -1.

2.3. The structure of matrix Φ

We assume, in this paper, that $\mathbf{\Phi} = [\phi_{i,j}]$ is an algebraic unitary (orthogonal) matrix (see [7, 8] for details). That means that this matrix is constructed with algebraic numbers in $\mathbb{K}$. In fact, all elements $\phi_{i,j}$ are algebraic integers,

$\phi_{i,j} \in \mathcal{O}_{\mathbb{K}}$. The structure of $\mathbf{\Phi}$ is the following,

$$\mathbf{\Phi} = \frac{1}{\sqrt{n}} \begin{bmatrix} \sigma_1(\theta_1) & \sigma_1(\theta_2) & \cdots & \sigma_1(\theta_n) \\ \sigma_2(\theta_1) & \sigma_2(\theta_2) & \cdots & \sigma_2(\theta_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\theta_1) & \sigma_n(\theta_2) & \cdots & \sigma_n(\theta_n) \end{bmatrix} \quad (3)$$

where $\theta_1, \theta_2, \ldots, \theta_n \in \mathcal{O}_{\mathbb{K}}$ are linearly independent on $\mathbb{F}$.

3. The matrix representation of an algebraic number

3.1. Example: Matrix representation of the complex numbers

We can see the field of complex numbers as an extension of degree 2 on $\mathbb{R}$. That means that $\mathbb{C} = \mathbb{R}(i)$ and i has minimal polynomial X^2+1. A complex number $z = x+iy$ has norm $N_{\mathbb{C}/\mathbb{R}}(z) = x^2 + y^2 = z \cdot \overline{z}$. Now, each complex number can be represented as a real matrix. For example, we have the association

$$x + iy \longmapsto \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

and we get

$$N_{\mathbb{C}/\mathbb{R}}(z) = x^2 + y^2 = \det \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

3.2. Generalization

This matrix representation can be generalized [9]. If $\mathbb{K}$ is an extension of degree n on $\mathbb{F}$, then to each element $\alpha \in \mathbb{K}$, we can associate a matrix $\mathbf{T}_\alpha \in \mathcal{M}_n(\mathbb{F})$ with determinant,

$$\det \mathbf{T}_\alpha = N_{\mathbb{K}/\mathbb{F}}(\alpha)$$

Moreover, if $\alpha \in \mathcal{O}_{\mathbb{K}}$, then $\mathbf{T}_\alpha \in \mathcal{M}_n(\mathcal{O}_{\mathbb{F}})$.

For example, take

- $\mathbb{F} = \mathbb{Q}(i)$; so $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[i]$
- $\theta = e^{i\frac{\pi}{4}} = \frac{1}{\sqrt{2}}(1+i)$; so $n = 2$ and we get $\sigma_1(\theta) = \theta, \sigma_2(\theta) = -\theta$

The matrix

$$\mathbf{T}_z = \begin{bmatrix} x & iy \\ y & x \end{bmatrix} \in \mathcal{M}_2(\mathbb{F})$$

is associated to a number $z = x + y\theta$ with $x, y \in \mathbb{F}$.

4. Transforming fading into a basis change

Now, assume that the received signal $\mathbf{y}$ is as in eq. (2) with the $\mathbf{\Phi}$ matrix satisfying (3). A reduction algorithm tends to transform the lattice basis into another lattice basis whose vectors have minimal length. It also tends to orthogonalize the basis. In other words, the reduction algorithm tends to find a new basis as close as possible to the canonical basis of a $\mathbb{Z}^n$ lattice . Matrix $\mathbf{H}$ can be expressed as

$$\mathbf{H} = \left(\prod_{i=1}^{n} h_i\right)^{\frac{1}{n}} \cdot \operatorname{diag}[a_1, a_2, \ldots, a_n] \quad (4)$$

with $\prod_{i=1}^{n} a_i = 1$. Assume that the vector $(|a_1|, |a_2|, \ldots, |a_n|)$ is composed by the modules of conjugates of some unit u in $\mathcal{O}_{\mathbb{K}}$, i.e., $a_k = e^{i\beta_k}\sigma_k(u), \forall k$ with $\beta_k = \arg a_k - \arg \sigma_k(u)$. The received signal can then be expressed as

$$\mathbf{y} = \left(\prod_{i=1}^{n} h_i\right)^{\frac{1}{n}} \cdot \operatorname{diag}\left[e^{i\beta_1}\sigma_1(u), \ldots, e^{i\beta_n}\sigma_n(u)\right] \cdot \mathbf{\Phi} \cdot \mathbf{x} + \mathbf{b}$$

Since $\mathbf{\Phi}$ has the structure of (3), then,

$$\mathbf{y} = \left(\prod_{i=1}^{n} h_i\right)^{\frac{1}{n}} \cdot \mathbf{\Psi} \cdot \mathbf{\Phi} \cdot \mathbf{T}_u \cdot \mathbf{x} + \mathbf{b}$$

with $\mathbf{\Psi} = \operatorname{diag}\left[e^{i\beta_1}, e^{i\beta_2}, \ldots, e^{i\beta_n}\right]$. Let $\mathbf{T}_u$ be the matrix representation of the unit u.

Denote $\mathbf{z} = (1/\prod_{i=1}^{n} h_i)^{\frac{1}{n}} \cdot \mathbf{\Phi}^\dagger \cdot \mathbf{\Psi}^\dagger \cdot \mathbf{y}$, then

$$\mathbf{z} = \mathbf{T}_u \cdot \mathbf{x} + \mathbf{w}$$

where $\mathbf{w} = (1/\prod_{i=1}^{n} h_i)^{\frac{1}{n}} \cdot \mathbf{\Phi}^\dagger \cdot \mathbf{\Psi}^\dagger \cdot \mathbf{b}$ remains an *i.i.d.* noise vector. Now, since $|\det \mathbf{T}_u| = 1$, (u is a unit), then it is a unimodular matrix. So,

$$\mathbf{T}_u \cdot \mathcal{O}_{\mathbb{F}}^n = \mathcal{O}_{\mathbb{F}}^n$$

with $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}$ or $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[i]$. A ML lattice decoder is now obvious as it is a symbol by symbol threshold detector followed by multiplication by the matrix $\mathbf{T}_u^{-1}$. This inverse matrix is easy to find, due to the structure of units in $\mathcal{O}_{\mathbb{K}}$ [9].

5. The reduction algorithm

Now, we have all the necessary tools to present the reduction algorithm.

5.1. The logarithmic lattice

Dirichlet's theorem [9] gives the structure of units in $\mathcal{O}_{\mathbb{K}}$.

Theorem 1 *Let $\mathbb{K}$ be an extension of $\mathbb{Q}$ with signature (r,s) (with degree $r+2s$). Then there exists $r+s-1$ units named "fundamental units" $u_1, u_2, \ldots, u_{r+s-1}$ such that any unit u can be expressed as*

$$u = \epsilon \cdot \prod_{i=1}^{r+s-1} u_i^{k_i} \tag{5}$$

where ϵ is a complex number with modulus equal to 1 and $k_i \in \mathbb{Z}$.

Now from a unit u, construct the vector

$$\mathbf{u} = \left(\ln|\sigma_1(u)|, \ldots, \ln|\sigma_{r+s}(u)|\right)^{\top}$$

Then vector $\mathbf{u}$ lies in a hyperplane with equation

$$\sum_{i=1}^{r+s} x_i = 0$$

Moreover, in this hyperplane, (5) implies that all vectors of type $\mathbf{u}$ are in a lattice named the logarithmic lattice, with generator matrix,

$$\begin{bmatrix} \ln|\sigma_1(u_1)| & \ln|\sigma_2(u_1)| & \cdots & \ln|\sigma_{r+s}(u_1)| \\ \ln|\sigma_1(u_2)| & \ln|\sigma_2(u_2)| & \cdots & \ln|\sigma_{r+s}(u_2)| \\ \vdots & \vdots & \ddots & \vdots \\ \ln|\sigma_1(u_{r+s-1})| & \ln|\sigma_2(u_{r+s-1})| & \cdots & \ln|\sigma_{r+s}(u_{r+s-1})| \end{bmatrix}$$

5.2. Logarithmic lattice decoding and reduction

Now, the objective is to approximate the vector $\left(e^{-i\beta_1}a_1, \ldots, e^{-i\beta_n}a_n\right)$ with the vector $(\sigma_1(u), \sigma_2(u), \ldots, \sigma_n(u))$ where u is some unit. This is done by performing a decoding of the logarithmic lattice. But this decoding is quite easy to do since:

1. A suboptimal decoding is enough.
2. The logarithmic lattice is fixed, since it only depends on $\mathbf{\Phi}$. All the preprocessing steps to decode that lattice are done once and only once.

Once this step has been processed, a unit u is found corresponding to a unimodular matrix $\mathbf{T}_u$ such that

$$\mathbf{T}_u = \frac{1}{n}\begin{bmatrix} \mathrm{Tr}(u) & \mathrm{Tr}(u\theta) & \cdots & \mathrm{Tr}(u\theta^{(n-1)}) \\ \mathrm{Tr}(u\theta^{-1}) & \mathrm{Tr}(u) & \cdots & \mathrm{Tr}(u\theta^{(n-2)}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(u\theta^{-(n-1)}) & \mathrm{Tr}(u\theta^{-(n-2)}) & \cdots & \mathrm{Tr}(u) \end{bmatrix}$$

where Tr is for $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}(i)}$. This matrix *is* the reduction matrix.

6. Simulation results

We present here simulation results in conjunction with a linear detector for the lattice. We present here some simple complex cases where the lattice is seen as a $\mathbb{Z}[i]$ lattice. All unitary matrices are from [7].

6.1. The 2-dimensional complex case

The unitary matrix $\mathbf{\Phi}$ is as in eq. (3) with $\theta_k = \exp\left(\frac{i(k-1)\pi}{4}\right)$. There is one fundamental unit, $1+i-e^{\frac{i\pi}{4}}$ and the logarithmic lattice is $\Lambda \cong \mathbb{Z}$.

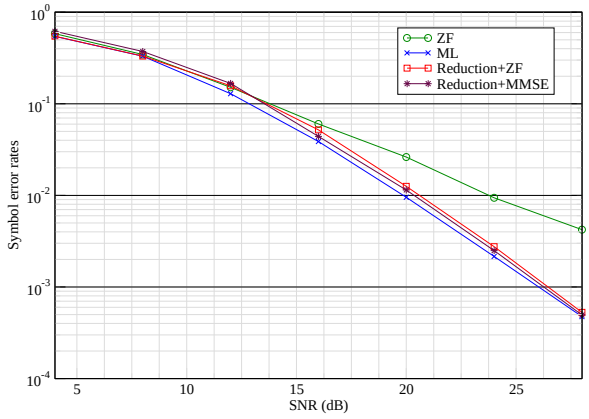

Figure 1: Lattice decoding - Dimension 2

6.2. The 4-dimensional complex lattice

The unitary matrix $\mathbf{\Phi}$ is as in (3) with $\theta_k = \exp\left(\frac{i(k-1)\pi}{8}\right)$. There are 3 fundamental units, $-1+i-i\theta^2$, $1+i\theta^2+\theta^3$ and $-1-i\theta+\theta^2+(1+i)\theta^3$ with $\theta = \exp\left(\frac{i\pi}{8}\right)$. This leads to the logarithmic lattice generated by

$$\begin{bmatrix} -0.88 & 0.88 & -0.88 & 0.88 \\ 0.56 & -0.16 & -1.44 & 1.04 \\ 1.04 & 0.56 & -0.16 & -1.44 \end{bmatrix}$$

6.3. Structure of the decoder

Let

$$\varepsilon = \frac{1}{\left(\prod_{i=1}^{n} h_i\right)^{\frac{1}{n}}} \cdot \mathbf{H} \cdot \left(\mathbf{\Psi} \cdot \mathrm{diag}\left[\sigma_1(u), \sigma_2(u), \ldots, \sigma_n(u)\right]\right)^{-1} - \mathbf{I}_n$$

represent the approximation error, where $\mathbf{I}_n$ is the identity matrix. After reduction, (2) becomes,

$$\mathbf{y} = \left(\prod_{i=1}^{n} h_i\right)^{\frac{1}{n}} \cdot \mathbf{\Psi} \cdot (I_n + \varepsilon) \cdot \mathbf{\Phi} \cdot \mathbf{T}_u \cdot \mathbf{x} + \mathbf{b}$$

Then a linear ZF or MMSE detection can be performed which gives the results of Figs. 1 and 2. Note how the sub-optimality of the decoder does not compromise the diversity gain of the code.

7. Conclusion

A novel lattice reduction algorithm is given for algebraic precoders. The complexity of our algorithm is much lower than the one of the LLL algorithm and gives excellent results as it preserves the diversity order of the linear precoder even when it is followed by a ZF detector. A more detailed analysis of this algorithm will follow in a forthcoming paper.

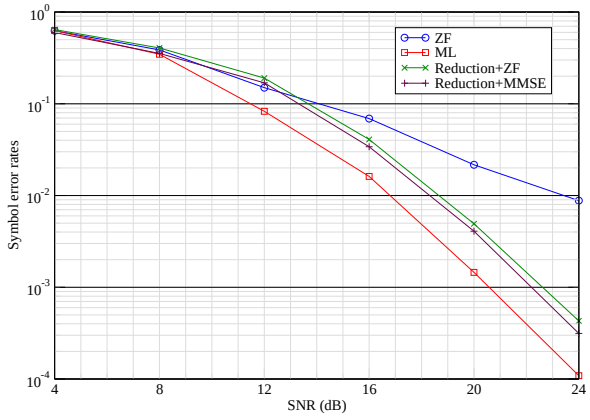

Figure 2: Lattice decoding - Dimension 4

References

[1] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good Lattice Constellations for both Rayleigh fading and Gaussian channels," *IEEE Trans. Inform. Theory*, vol. 42, pp. 502–518, March 1996.

[2] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1639–1642, July 1999.

[3] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Trans. Inform. Theory*, vol. 48, pp. 2201–2214, August 2002.

[4] H. Yao and G. W. Wornell, "Achieving the full MIMO diversity-multiplexing frontier with rotation-based space-time codes," in *Proceedings Allerton Conf. Commun., Cont., and Computing, (Illinois)*, October 2003.

[5] M. Grötschel, L. Lovász, and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*. New York: Springer-Verlag, 1988.

[6] C. Windpassinger and R. F. H. Fischer, "Low-complexity near-maximum-likelihood detection ...," in *Proceedings of the ITW*, pp. 345–348, *IEEE*, April 2003.

[7] X. Giraud, E. Boutillon, and J.-C. Belfiore, "Algebraic tools to build modulation schemes for fading channels," *IEEE Trans. Inform. Theory*, vol. 43, pp. 938–952, May 1997.

[8] E. Viterbo and J. J. Boutros, "Signal space diversity: a power- and bandwidth-efficient diversity technique for the rayleigh fading channel," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1453–1467, July 1998.

[9] H. Cohn, *Advanced Number Theory*. Dover Publications Inc. New York, 1980.