Augmented Lattice Reduction for MIMO Decoding

Laura Luzzi, Ghaya Rekaya-Ben Othman, *Member, IEEE,* and Jean-Claude Belfiore, *Member, IEEE*

***Abstract*—Lattice reduction algorithms, such as the Lenstra-Lenstra-Lovasz (LLL) algorithm, have been proposed as preprocessing tools in order to enhance the performance of suboptimal receivers in multiple-input multiple-output (MIMO) communications. A different approach, introduced by Kim and Park, allows to combine right preprocessing and detection in a single step by performing lattice reduction on an "augmented channel matrix". In this paper we propose an improvement of the augmented matrix approach which guarantees a better performance. We prove that our method attains the maximum receive diversity order of the channel. Simulation results evidence that it significantly outperforms LLL reduction followed by successive interference cancellation (SIC) while requiring a moderate increase in complexity. A theoretical bound on the complexity is also derived.**

***Index Terms*—Lattice reduction-aided decoding, LLL algorithm, right preprocessing.**

I. Introduction

Multiple-input multiple-output (MIMO) systems can provide high data rates and reliability over fading channels. In order to achieve optimal performance, maximum likelihood decoders such as the Sphere Decoder may be employed; however, their complexity grows prohibitively with the number of antennas and the constellation size, posing a challenge for practical implementation.

On the other hand, suboptimal receivers such as zero forcing (ZF) or successive interference cancellation (SIC) do not preserve the diversity order of the system [10]. Right preprocessing using *lattice reduction* has been proposed in order to enhance their performance [19, 4, 8]. In particular, the classical Lenstra-Lenstra-Lovasz (LLL) algorithm for lattice reduction, whose average complexity is polynomial in the number of antennas[1], has been proven to achieve the optimal receive diversity order in the spatial multiplexing case [17]. Very recently, it has also been shown that combined with regularization techniques such as minimum mean square error generalized decision-feedback equalizer (MMSE-GDFE) left preprocessing, lattice reduction-aided decoding is optimal in terms of the diversity-multiplexing tradeoff [7]. However, the shift between the error probability of maximum likelihood (ML) detection and LLL-ZF (respectively, LLL-SIC) detection increases greatly for a large number of antennas [12].

Recently a new lattice reduction-aided decoding technique combining the right preprocessing stage and the detection stage in a single step was proposed in [11]. This technique, called *Improved Lattice Reduction*, consists in LLL-reducing an augmented lattice which is a function of the channel matrix and of the received signal. An estimate of the transmitted message can then be recovered directly from the change of basis matrix. Improved Lattice Reduction is equivalent to LLL-SIC decoding in terms of probability of error.

In this paper we present a different kind of augmented lattice reduction decoding which significantly enhances its performance by carefully choosing the augmented lattice parameters. In the coherent case, MIMO decoding amounts to solving an instance of the *closest vector problem* (CVP) in a finite subset of the lattice generated by the channel matrix[2]. Following an idea of Kannan [9], our strategy is to reduce the CVP to the *shortest vector problem* (SVP) by embedding the n-dimensional lattice generated by the channel matrix into an $(n+1)$-dimensional lattice. We show that for a suitable choice of the embedding, the transmitted message can be recovered directly from the coordinates of the shortest vector of the augmented lattice with provably high probability.

In general, the LLL algorithm is not guaranteed to solve the SVP; however, it certainly finds the shortest vector in the lattice in the particular case where the minimum distance is exponentially smaller than the other successive minima. Equivalently, we can say that "the LLL algorithm is an *SVP-oracle* when the lattice gap is exponential in the lattice dimension" [16]. An appropriate choice of the embedding ensures that this condition is satisfied.

Thanks to this property, we can prove that our method also achieves the receive diversity of the channel. Numerical simulations evidence that augmented lattice reduction significantly outperforms LLL-SIC detection while requiring a moderate increase in complexity. A theoretical (albeit pessimistic) bound on the complexity is also derived.

This paper is organized as follows: in Section II we introduce the system model and basic notions concerning lattice reduction, and summarize the existing lattice reduction-aided decoding schemes. In Section III we describe augmented lattice reduction decoding, and in Sections IV and V we analyze its performance and complexity, both theoretically and through numerical simulations.

II. Preliminaries

A. System model and notation

We consider a MIMO system with M transmit and N receive antennas such that $M \leq N$ using spatial multiplexing.

Manuscript received January 8, 2010; revised May 6, 2010; accepted July 4, 2010. The associate editor coordinating the review of this paper and approving it for publication was N. Sagias.

The authors are with Télécom-ParisTech, 46 Rue Barrault, 75013 Paris, France (e-mail: {luzzi, rekaya, belfiore}@telecom-paristech.fr).

This work has been supported by the Institut Carnot TELECOM-EURECOM.

Digital Object Identifier 10.1109/TWC.2010.072210.100023

[1]Note that the *worst-case* number of iterations of the LLL algorithm applied to the MIMO context is unbounded, as has been proved in [8]. However, the tail probability of the number of iterations decays exponentially, so that in many cases high complexity events can be regarded as negligible with respect to the target error rate (see [7], Theorem 3).

[2]Actually, LLL-ZF and LLL-SIC suboptimal decoding correspond to two classical techniques for finding approximate solutions of the CVP, due to Babai: the *rounding algorithm* and *nearest plane algorithm* respectively [1].

The complex received signal is given by

$$\mathbf{y}_c = \mathbf{H}_c\mathbf{x}_c + \mathbf{w}_c, \tag{1}$$

where $\mathbf{x}_c \in \mathbb{C}^M$, $\mathbf{y}_c$, $\mathbf{w}_c \in \mathbb{C}^N$, $\mathbf{H}_c \in M_{N\times M}(\mathbb{C})$. The transmitted vector $\mathbf{x}_c$ belongs to a finite constellation $\mathcal{S} \subset \mathbb{Z}[i]^M$; the entries of the channel matrix $\mathbf{H}_c$ are supposed to be i.i.d. complex Gaussian random variables with zero mean and variance per real dimension equal to $\frac{1}{2}$, and $\mathbf{w}_c$ is the Gaussian noise with i.i.d. entries of zero mean and variance N_0. We consider the coherent case where $\mathbf{H}_c$ is known at the receiver.

Separating the real and imaginary part, the model can be rewritten as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{w}, \tag{2}$$

in terms of the real-valued vectors

$$\mathbf{y} = \begin{pmatrix}\Re(\mathbf{y}_c)\\ \Im(\mathbf{y}_c)\end{pmatrix} \in \mathbb{R}^n, \quad \mathbf{x} = \begin{pmatrix}\Re(\mathbf{x}_c)\\ \Im(\mathbf{x}_c)\end{pmatrix} \in \mathbb{Z}^m$$

and of the equivalent real channel matrix

$$\mathbf{H} = \begin{pmatrix}\Re(\mathbf{H}_c) & -\Im(\mathbf{H}_c)\\ \Im(\mathbf{H}_c) & \Re(\mathbf{H}_c)\end{pmatrix} \in M_{n\times m}(\mathbb{R}).$$

Here $n = 2N$, $m = 2M$.

The maximum likelihood decoded vector is given by

$$\hat{\mathbf{x}}_{\mathrm{ML}} = \underset{\hat{\mathbf{x}}_c\in\mathcal{S}}{\operatorname{argmin}} \|\mathbf{H}_c\hat{\mathbf{x}}_c - \mathbf{y}_c\| = \underset{\hat{\mathbf{x}}_c\in\mathcal{S}}{\operatorname{argmin}} \|\mathbf{H}\hat{\mathbf{x}} - \mathbf{y}\|,$$

where $\|\cdot\|$ denotes the Euclidean norm, and $\hat{\mathbf{x}} = \begin{pmatrix}\Re(\hat{\mathbf{x}}_c)\\ \Im(\hat{\mathbf{x}}_c)\end{pmatrix}$.

B. Lattice reduction

An m-dimensional real lattice in $\mathbb{R}^n$ is the set of points

$$\mathcal{L}(\mathbf{H}) = \{\mathbf{H}\mathbf{x} \mid \mathbf{x} \in \mathbb{Z}^m\},$$

where $\mathbf{H} \in M_{n\times m}(\mathbb{R})$. We denote by $d_{\mathbf{H}}$ the *minimum distance* of the lattice, that is the smallest norm of a nonzero vector in $\mathcal{L}(\mathbf{H})$. More generally, for all $1 \le i \le m$ one can define the *i-th successive minimum* of the lattice as follows:

$$\lambda_i(\mathbf{H}) = \inf\{r > 0 \mid \exists \mathbf{v}_1,\ldots,\mathbf{v}_i \text{ linearly independent in } \mathcal{L}(\mathbf{H}) \text{ s.t. } \|\mathbf{v}_j\| \le r \quad \forall j \le i\} \tag{3}$$

We recall that two matrices $\mathbf{H}, \mathbf{H}'$ generate the same lattice if and only if $\mathbf{H}' = \mathbf{H}\mathbf{U}$ with $\mathbf{U} \in M_{m\times m}(\mathbb{R})$ unimodular, that is, $\mathbf{U}$ has integer entries and $\det(\mathbf{U}) = \pm 1$.

Lattice reduction algorithms allow to find a new basis $\mathbf{H}'$ for a given lattice $\mathcal{L}(\mathbf{H})$ such that the basis vectors are shorter and nearly orthogonal. Orthogonality can be measured by the absolute value of the coefficients $\mu_{i,j} = \frac{\langle \mathbf{h}_i, \mathbf{h}_j^*\rangle}{\|\mathbf{h}_j^*\|^2}$ in the Gram-Schmidt orthogonalization (GSO) of the basis.

We recall the following useful property of GSO: the length of the smallest of the Gram-Schmidt vectors $\mathbf{h}_i^*$ is always less or equal to the minimum distance $d_{\mathbf{H}}$ of the lattice [15]. In other words,

$$d_{\mathbf{H}} \ge a(\mathbf{H}) \doteqdot \min_{1\le i\le m} \|\mathbf{h}_i^*\|. \tag{4}$$

A basis $\mathbf{H}$ is said to be *LLL-reduced* [14] if its Gram-Schmidt coefficients $\mu_{i,j}$ and Gram-Schmidt vectors satisfy the following properties:

1) *Size reduction:*

$$|\mu_{k,l}| \le \frac{1}{2}, \quad 1 \le l < k \le m,$$

2) *Lovasz condition:*

$$\left\|\mathbf{h}_k^* + \mu_{k,k-1}\mathbf{h}_{k-1}^*\right\|^2 \ge \delta \left\|\mathbf{h}_{k-1}^*\right\|^2, \quad 1 < k \le m,$$

where $\delta \in \left(\frac{1}{4}, 1\right)$ (a customary choice is $\delta = \frac{3}{4}$).

The LLL algorithm is summarized in Algorithms 1 and 2. Given a full-rank matrix $\mathbf{H} \in M_{n\times m}(\mathbb{R})$, it computes an LLL-reduced version $\mathbf{H}_{\mathrm{red}} = \mathbf{H}\mathbf{U}$, with $\mathbf{U} \in M_{m\times m}(\mathbb{Z})$ unimodular, and outputs the columns $\{\mathbf{h}_i\}$ and $\{\mathbf{u}_i\}$ of $\mathbf{H}_{\mathrm{red}}$ and $\mathbf{U}$ respectively.

Algorithm 1: The LLL algorithm

$\mathbf{U} = \mathbf{I}_m$
Compute the GSO of $\mathbf{H}$
$k \leftarrow 2$
while $k \le m$ **do**
  RED(k,k-1)
  if $\left\|\mathbf{h}_k^* + \mu_{k,k-1}\mathbf{h}_{k-1}^*\right\|^2 < \delta\left\|\mathbf{h}_{k-1}^*\right\|^2$ **then**
    swap $\mathbf{h}_k$ and $\mathbf{h}_{k-1}$
    swap $\mathbf{u}_k$ and $\mathbf{u}_{k-1}$
    update GSO
    $k \leftarrow \max(k-1, 2)$
  end
  else
    for $l = k-2, \ldots, 1$ **do**
      RED(k,l)
    end
    $k \leftarrow k+1$
  end
end

Algorithm 2: Size reduction RED(k,l)

if $|\mu_{k,l}| > \frac{1}{2}$ **then**
  $\mathbf{h}_k \leftarrow \mathbf{h}_k - \lfloor \mu_{k,l} \rceil \mathbf{h}_l$
  $\mathbf{u}_k \leftarrow \mathbf{u}_k - \lfloor \mu_{k,l} \rceil \mathbf{u}_l$
  for $j = 1, \cdots, l-1$ **do**
    $\mu_{k,j} \leftarrow \mu_{k,j} - \lfloor \mu_{k,l} \rceil \mu_{l,j}$
  end
  $\mu_{k,l} \leftarrow \mu_{k,l} - \lfloor \mu_{k,l} \rceil$
end

We list here some properties of LLL-reduced bases that we will need in the sequel. First of all, the LLL algorithm finds at least one basis vector whose length is not too far from the minimum distance $d_{\mathbf{H}}$ of the lattice. The following inequality holds for any m-dimensional LLL-reduced basis $\mathbf{H}$ [3]:

$$\|\mathbf{h}_1\| \le \alpha^{\frac{m-1}{2}} d_{\mathbf{H}}, \tag{5}$$

where $\alpha = \frac{1}{\delta - 1/4}$ ($\alpha = 2$ if $\delta = \frac{3}{4}$). Moreover, the first basis vector cannot be too big compared to the Gram-Schmidt vectors $\{\mathbf{h}_i^*\}$:

$$\|\mathbf{h}_1\| \le \alpha^{\frac{i-1}{2}} \|\mathbf{h}_i^*\|, \qquad \forall 1 \le i \le m.$$

In particular, if $j = \operatorname{argmin}_{1 \leq i \leq m} \|\mathbf{h}_i^*\|$,

$$d_{\mathbf{H}} \leq \|\mathbf{h}_1\| \leq \alpha^{\frac{j-1}{2}} \left\|\mathbf{h}_j^*\right\| = \alpha^{\frac{j-1}{2}} a(\mathbf{H}) \leq \alpha^{\frac{m-1}{2}} a(\mathbf{H}). \quad (6)$$

C. Lattice reduction-aided decoding

In this section we briefly review existing detection schemes which use the LLL algorithm to preprocess the channel matrix, in order to improve the performance of suboptimal decoders such as ZF or SIC [19, 18, 4].

Let $\mathbf{H}_{\text{red}} = \mathbf{H}\mathbf{U}$ be the output of the LLL algorithm on $\mathbf{H}$. We can rewrite the received vector as $\mathbf{y} = \mathbf{H}_{\text{red}}\mathbf{U}^{-1}\mathbf{x} + \mathbf{w}$.

- The *LLL-ZF decoder* outputs

$$\hat{\mathbf{x}}_{LLL-ZF} = Q_{\mathcal{S}}\left(\mathbf{U}\left(\left\lfloor \mathbf{H}_{\text{red}}^{\dagger}\mathbf{y}\right\rceil\right)\right),$$

  where $\mathbf{H}_{\text{red}}^{\dagger} = (\mathbf{H}_{\text{red}}^T\mathbf{H}_{\text{red}})^{-1}\mathbf{H}_{\text{red}}^T$ is the Moore-Penrose pseudoinverse of $\mathbf{H}_{\text{red}}$, $\lfloor \cdot \rceil$ denotes component-wise rounding to the nearest integer and $Q_{\mathcal{S}}$ is a quantization function that forces the solution to belong to the constellation $\mathcal{S}$.
- The *LLL-SIC decoder* performs the QR decomposition $\mathbf{H}_{\text{red}} = \mathbf{Q}\mathbf{R}$, computes $\widetilde{\mathbf{y}} = \mathbf{Q}^T\mathbf{y}$, finds by recursion $\widetilde{\mathbf{x}}$ defined by

$$\tilde{x}_m = \left\lfloor \frac{\tilde{y}_m}{r_{mm}} \right\rceil,$$
$$\tilde{x}_i = \left\lfloor \frac{\tilde{y}_i - \sum_{j=i+1}^{m} r_{ij}\tilde{x}_j}{r_{ii}} \right\rceil, \qquad i = m-1, \ldots, 1,$$

  and finally outputs $\hat{\mathbf{x}}_{LLL-SIC} = Q_{\mathcal{S}}\left(\mathbf{U}\widetilde{\mathbf{x}}\right)$.

D. Improved lattice reduction

Recently, Kim and Park [11] have proposed a new decoding technique based on the LLL algorithm, called *Improved lattice reduction*, which allows to estimate the transmitted message directly from the unimodular reduction matrix.

Let $\mathbf{y}$ be the (real) received vector in the model (2). Consider the $(n+1) \times (m+1)$ augmented matrix

$$\widetilde{\mathbf{H}} = \begin{pmatrix} \mathbf{H} & -\mathbf{y} \\ \mathbf{0}_{1\times m} & t \end{pmatrix} = \begin{pmatrix} h_{1,1} & \cdots & h_{1,m} & -y_1 \\ \vdots & & & \vdots \\ h_{n,1} & \cdots & h_{n,m} & -y_n \\ 0 & \cdots & 0 & t \end{pmatrix} \quad (7)$$

where $t > 0$ is a parameter to be determined.

Let $\widetilde{\mathbf{H}}_{\text{red}} = \widetilde{\mathbf{H}}\widetilde{\mathbf{U}}$ be the output of the LLL algorithm on $\widetilde{\mathbf{H}}$.

- The *Improved lattice reduction decoder* outputs

$$\hat{\mathbf{x}}_{ILR} = Q_{\mathcal{S}}(\widetilde{u}_{1,m+1}, \ldots, \widetilde{u}_{m,m+1})^T \quad (8)$$

In [11], the parameter t is chosen such that $t > r_{m,m}$, where $\mathbf{R} = (r_{i,j})$ is the upper triangular matrix in the the QR decomposition $\mathbf{H}_{\text{red}} = \mathbf{Q}\mathbf{R}$. This ensures that the Lovasz condition on the last column of the augmented matrix $\widetilde{\mathbf{H}}$ is always verified. Therefore, LLL-reducing $\widetilde{\mathbf{H}}$ amounts to LLL-reducing the submatrix $\mathbf{H}$ and then performing a final round of size reduction without swaps on the last column.

Although not explicitly stated in [11], the performance of improved lattice reduction is exactly the same as LLL-SIC. In fact, it is not hard to prove by induction that

$$Q_{\mathcal{S}}(\widetilde{\mathbf{u}}_{m+1}) = Q_{\mathcal{S}}\begin{pmatrix} \sum_{i=1}^{n} \widetilde{x}_i\mathbf{u}_i \\ 1 \end{pmatrix} = \begin{pmatrix} \hat{\mathbf{x}}_{LLL-SIC} \\ 1 \end{pmatrix}$$

where $\mathbf{u}_i$ and $\widetilde{\mathbf{u}}_i$ are the columns of $\mathbf{U}$ and $\widetilde{\mathbf{U}}$ respectively.

III. Augmented Lattice Reduction

We introduce here a different decoder based on the augmented matrix (7) which, by carefully choosing the parameter t, greatly enhances the performance with respect to Improved lattice reduction.

Observe that the points of the augmented lattice $\mathcal{L}(\widetilde{\mathbf{H}})$ are of the form $\begin{pmatrix} \mathbf{H}\mathbf{x}' - q\mathbf{y} \\ qt \end{pmatrix}$, $\mathbf{x}' \in \mathbb{Z}^m,\ q \in \mathbb{Z}$. In particular, the vector $\mathbf{v} = \begin{pmatrix} \mathbf{H}\mathbf{x} - \mathbf{y} \\ t \end{pmatrix} = \begin{pmatrix} \mathbf{w} \\ t \end{pmatrix}$ belongs to the augmented lattice. We will show that for a suitable choice of t, and supposing that the noise is small enough, $\mathbf{v}$ is the shortest vector in the lattice and the LLL algorithm finds this vector. That is, $\pm\mathbf{v}$ is the first column of $\widetilde{\mathbf{H}}_{\text{red}} = \widetilde{\mathbf{H}}\widetilde{\mathbf{U}}$, the output of LLL algorithm on $\widetilde{\mathbf{H}}$. Clearly, since $\widetilde{\mathbf{H}}$ is full-rank with probability 1, in this case the first column of the change of basis matrix $\widetilde{\mathbf{U}}$ is $\begin{pmatrix} \pm\mathbf{x} \\ \pm 1 \end{pmatrix}$. Thus we can "read" the transmitted message directly from the change of basis matrix $\widetilde{\mathbf{U}}$.

To summarize, in order to decode we can perform the LLL algorithm on $\widetilde{\mathbf{H}}$, and given the output $\widetilde{\mathbf{H}}_{\text{red}} = \widetilde{\mathbf{H}}\widetilde{\mathbf{U}}$, we can choose

$$\hat{\mathbf{x}} = Q_{\mathcal{S}}\left(\left\lfloor \frac{1}{\widetilde{u}_{m+1,1}}(\widetilde{u}_{1,1}, \ldots, \widetilde{u}_{m,1})^T \right\rceil\right), \quad (9)$$

where $\widetilde{\mathbf{U}} = (\widetilde{u}_{i,j})$. (Division by $\widetilde{u}_{m+1,1}$ is needed because under the previous assumptions, $\widetilde{u}_{m+1,1} = \pm 1$ and $(\widetilde{u}_{1,1}, \ldots, \widetilde{u}_{m,1})^T = \pm\mathbf{x}$.)

The previous decoder can be improved by including all the columns of $\widetilde{\mathbf{H}}_{\text{red}}$ in the search for the vector $\mathbf{v}$. Let

$$\mathbf{s}_k = \frac{1}{\widetilde{u}_{m+1,k}}(\widetilde{u}_{1,k}, \ldots, \widetilde{u}_{m,k})^T, \quad k = 1, \ldots, m.$$

If $\exists k \in \{1, \ldots, m\}$ such that $|\widetilde{u}_{m+1,k}|$=1, we define

$$k_{\min} = \operatorname*{argmin}_{k \text{ s.t. } |\widetilde{u}_{m+1,k}|=1} \|\mathbf{H}\mathbf{s}_k - \mathbf{y}\|,$$

otherwise $k_{\min} = 1$. Then the *Augmented Lattice Reduction decoder* outputs

$$\hat{\mathbf{x}}_{\text{ALR}} = Q_{\mathcal{S}}\left(\lfloor \mathbf{s}_{k_{\min}} \rceil\right). \quad (10)$$

IV. Performance Analysis and Simulation Results

A. Diversity of augmented lattice reduction

In this paragraph we will investigate the performance of augmented lattice reduction. We begin by proving that our method, like LLL-ZF and LLL-SIC, attains the maximum receive diversity gain of N, for an appropriate choice of the parameter t in (7). The diversity gain d of a decoding scheme is defined as follows:

$$d = -\lim_{\rho\to\infty} \frac{\log(P_e)}{\log(\rho)},$$

where ρ denotes the signal to noise ratio and P_e is the error probability.

Proposition 1. *If the augmented lattice reduction is performed using $t = \varepsilon a(\mathbf{H}_{\mathrm{red}})$, where $a(\mathbf{H}_{\mathrm{red}})$ is the length of the smallest vector in the GSO of $\mathbf{H}_{\mathrm{red}}$, and $\varepsilon \leq \frac{1}{2\sqrt{2}\alpha^{\frac{m}{2}}}$, then it achieves the maximum receive diversity N.*

Remark. It is essential to use $a(\mathbf{H}_{\mathrm{red}})$ in place of $a(\mathbf{H})$. In fact, for general bases $\mathbf{H}$ that are not LLL-reduced, there is no lower bound of the type (6) limiting how small the smallest Gram-Schmidt vector can be. For $a(\mathbf{H}_{\mathrm{red}})$, putting together the bounds (4) and (6), we obtain

$$\frac{d_{\mathbf{H}}}{\alpha^{\frac{m-1}{2}}} \leq a(\mathbf{H}_{\mathrm{red}}) \leq d_{\mathbf{H}} \tag{11}$$

Note that the LLL reduction of $\mathbf{H}$ does not entail any additional complexity, since it is the same as the LLL reduction on the first m columns of $\widetilde{\mathbf{H}}$. In fact the parameter t can be chosen during the LLL reduction of $\widetilde{\mathbf{H}}$, after carrying out the LLL algorithm on the first m columns.

In order to prove the previous Proposition, we will show that in the $(m+1)$-dimensional lattice $\mathcal{L}(\widetilde{\mathbf{H}})$ there is an exponential gap between the first two successive minima. Then, using the estimate (5) on the norm of the first vector in an LLL-reduced basis, one can conclude that in this particular case the LLL algorithm finds the shortest vector in the lattice $\mathcal{L}(\widetilde{\mathbf{H}})$ with high probability. This, in turn, allows to recover the closest lattice vector $\mathbf{Hx}$ to $\mathbf{y}$ in $\mathcal{L}(\mathbf{H})$ supposing that the noise $\mathbf{w}$ is small enough.

The following definition makes the notion of "gap" more precise:

Definition. *Let $\mathbf{v}$ be a shortest nonzero vector in the lattice $\mathcal{L}(\mathbf{H})$, and let $\gamma > 1$. $\mathbf{v}$ is called γ-*unique *if $\forall \mathbf{u} \in \mathcal{L}(\mathbf{H})$,*

$$\|\mathbf{u}\| \leq \gamma \|\mathbf{v}\| \Rightarrow \mathbf{u} \textit{ is an integer multiple of } \mathbf{v}.$$

Note that if $\mathbf{v}$ is a γ-unique shortest vector, there is a gap between the first two successive minima of the lattice $\mathcal{L}(\mathbf{H})$ defined in equation (3): $\lambda_2(\mathbf{H}) > \gamma\lambda_1(\mathbf{H}) = \gamma d_{\mathbf{H}}$. We now prove the existence of such a gap under suitable conditions:

Lemma 1. *Let $\widetilde{\mathbf{H}}$ be the matrix defined in (7), and let $t = \varepsilon a(\mathbf{H}_{\mathrm{red}})$, with $\varepsilon \leq \frac{1}{2\sqrt{2}\alpha^{\frac{m}{2}}}$.*

Suppose that $\|\mathbf{w}\| = \|\mathbf{y} - \mathbf{Hx}\| \leq \frac{\varepsilon}{\alpha^{\frac{m-1}{2}}} d_{\mathbf{H}}$.

Then $\mathbf{v} = \begin{pmatrix} \mathbf{Hx} - \mathbf{y} \\ t \end{pmatrix}$ is an $\alpha^{\frac{m}{2}}$-unique shortest vector of $\mathcal{L}(\widetilde{\mathbf{H}})$.

Remark. Observe that the hypothesis on $\|\mathbf{w}\|$ implies in particular that $\|\mathbf{w}\| < \frac{d_{\mathbf{H}}}{2}$ and $\mathbf{Hx}$ is indeed the closest lattice point to $\mathbf{y}$.

Proof: We need to show that any vector $\mathbf{u} \in \mathcal{L}(\widetilde{\mathbf{H}})$ that is not a multiple of $\mathbf{v}$ must have length greater than $\alpha^{\frac{m}{2}} \|\mathbf{v}\|$.

By contradiction, suppose that $\exists \mathbf{u} = \begin{pmatrix} \mathbf{Hx}' - q\mathbf{y} \\ qt \end{pmatrix} \in \mathcal{L}(\widetilde{\mathbf{H}})$ linearly independent from $\mathbf{v}$ such that $\|\mathbf{u}\| \leq \alpha^{\frac{m}{2}} \|\mathbf{v}\|$. Since $\|\mathbf{u}\| \geq |q|\, t$,

$$|q| \leq \frac{\|\mathbf{u}\|}{t} \leq \frac{\alpha^{\frac{m}{2}} \|\mathbf{v}\|}{t}.$$

On the other side, $\|\mathbf{u}\| \leq \alpha^{\frac{m}{2}} \|\mathbf{v}\|$ implies that also $\|\mathbf{Hx}' - q\mathbf{y}\| \leq \alpha^{\frac{m}{2}} \|\mathbf{v}\|$. Consider

$$\begin{aligned} &\|\mathbf{Hx}' - q\mathbf{Hx}\| \leq \|\mathbf{Hx}' - q\mathbf{y}\| + \|q\mathbf{y} - q\mathbf{Hx}\| \leq \\ &\leq \alpha^{\frac{m}{2}} \|\mathbf{v}\| + |q|\, \|\mathbf{y} - \mathbf{Hx}\| \leq \alpha^{\frac{m}{2}} \|\mathbf{v}\| + \frac{\alpha^{\frac{m}{2}} \|\mathbf{v}\|}{t} \|\mathbf{w}\| \leq \\ &\leq \alpha^{\frac{m}{2}} t \sqrt{\frac{1 + \|\mathbf{w}\|^2}{t^2}} \left(1 + \frac{\|\mathbf{w}\|}{t}\right) \end{aligned} \tag{12}$$

The bound (11) on $a(\mathbf{H}_{\mathrm{red}})$ implies

$$\frac{\varepsilon}{\alpha^{\frac{m-1}{2}}} d_{\mathbf{H}} \leq t \leq \varepsilon d_{\mathbf{H}}, \quad \|\mathbf{w}\| < t$$

Using these inequalities, we can bound the expression (12) with

$$\alpha^{\frac{m}{2}} \varepsilon d_{\mathbf{H}} 2\sqrt{2} < d_{\mathbf{H}}.$$

Thus $\|\mathbf{Hx}' - q\mathbf{Hx}\| < d_{\mathbf{H}}$. But this is a contradiction because $\mathbf{Hx}' - q\mathbf{Hx} \in \mathcal{L}(\mathbf{H})$ and is nonzero since $\mathbf{v}$ and $\mathbf{u}$ are linearly independent. Therefore $\mathbf{v}$ is $\alpha^{\frac{m}{2}}$-unique. (Since the last coordinate of $\mathbf{v}$ in the basis $\widetilde{\mathbf{H}}$ is 1, $\mathbf{v}$ cannot be a nontrivial multiple of another lattice vector.) □

Lemma 2. *Under the hypotheses of Lemma 1, the augmented lattice reduction methods (9) and (10) correctly decode the transmitted signal* $\mathbf{x}$.

Proof: Let $\widetilde{\mathbf{H}}_{\mathrm{red}} = \widetilde{\mathbf{H}}\widetilde{\mathbf{U}}$ denote the output of the LLL reduction of $\widetilde{\mathbf{H}}$, and let $\hat{\mathbf{h}}_1 = \widetilde{\mathbf{H}} \begin{pmatrix} \mathbf{x}' \\ q \end{pmatrix} = \begin{pmatrix} \mathbf{Hx}' - q\mathbf{y} \\ qt \end{pmatrix}$ be its first column. The property (5) of LLL reduction in dimension $m+1$ entails that $\left\|\hat{\mathbf{h}}_1\right\| \leq \alpha^{\frac{m}{2}} d_{\widetilde{\mathbf{H}}}$. But since $\mathbf{v} = \begin{pmatrix} \mathbf{Hx} - \mathbf{y} \\ t \end{pmatrix}$ has been shown to be $\alpha^{\frac{m}{2}}$-unique in the previous Lemma, it means that $\hat{\mathbf{h}}_1$ is an integer multiple of $\mathbf{v}$: $\exists a \in \mathbb{Z} \setminus \{0\}$ such that $\hat{\mathbf{h}}_1 = a\mathbf{v}$. In particular $at = qt$, so $a = q$ and $\hat{\mathbf{h}}_1 = q\mathbf{v}$. Then by definition of $\widetilde{\mathbf{H}}$, $\hat{\mathbf{h}}_1 = \widetilde{\mathbf{H}} \begin{pmatrix} q\mathbf{x} \\ q \end{pmatrix}$. This means that the first column of the reduction matrix $\widetilde{\mathbf{U}}$ is $\begin{pmatrix} q\mathbf{x} \\ q \end{pmatrix}$, and so $\hat{\mathbf{x}}_{\mathrm{ALR}} = Q_{\mathcal{S}}(\lfloor \mathbf{u}_1 \rceil) = Q_{\mathcal{S}}(q\mathbf{x}/q) = \mathbf{x}$ and the augmented lattice reduction methods (9) and (10) correctly decode the transmitted message.
(Observe that this is possible only if $|q| = 1$, since $\det(\widetilde{\mathbf{U}})$ is also a multiple of q and $\widetilde{\mathbf{U}}$ is unimodular.) □

Thus for any channel realization $\mathbf{H}$, we have the following bound on the error probability for the augmented lattice reduction method:

$$P_{e,\mathrm{ALR}}(\mathbf{H}) \leq P\{\|\mathbf{w}\| > \varepsilon' d_{\mathbf{H}}\},$$

with $\varepsilon' = \frac{\varepsilon}{\alpha^{\frac{m-1}{2}}}$. To conclude the proof of Proposition 1, we need to show that

$$\lim_{\rho \to \infty} \frac{-\log P\{\|\mathbf{w}\| > \varepsilon' d_{\mathbf{H}}\}}{\log \rho} \geq N$$

This turns out to be true. In fact, it has been shown in [17] (Proof of Theorem 2), that for any constant c_M depending only on the number of transmit antennas, there exist two constants

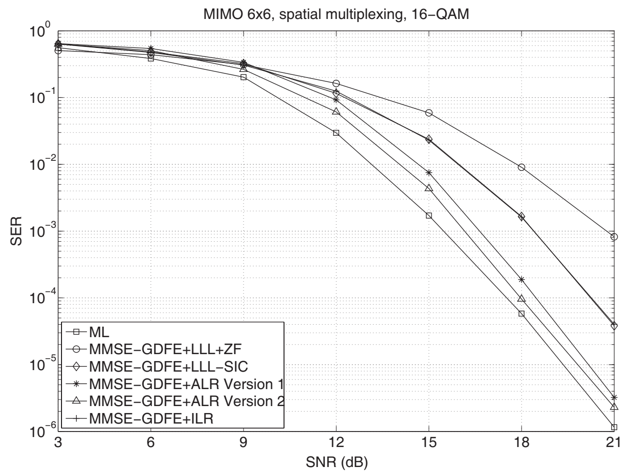

Fig. 1. Performance comparison of augmented lattice reduction with LLL-ZF, LLL-SIC and Improved Lattice Reduction with MMSE-GDFE preprocessing for a 6×6 uncoded MIMO system using 16-QAM. The LLL algorithm is performed using $\delta = \frac{3}{4}$.

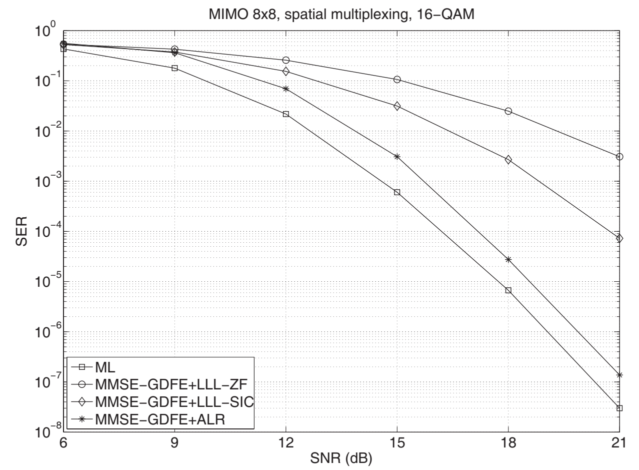

Fig. 2. Performance comparison of augmented lattice reduction with LLL-ZF and LLL-SIC detection with MMSE-GDFE preprocessing for a 8×8 uncoded MIMO system using 16-QAM.

$C_1, C_2 > 0$ depending on c_M, M and N such that[3],

$$P\{\|\mathbf{w}\| > c_M d_{\mathbf{H}}\} \leq \frac{C_1(\ln(\rho))^{N+1}}{\rho^N} \qquad \text{for } N = M,$$

$$P\{\|\mathbf{w}\| > c_M d_{\mathbf{H}}\} \leq \frac{C_2}{\rho^N} \qquad \text{for } N > M.$$

Thus augmented lattice reduction achieves the maximum receive diversity N with the choice $t = \varepsilon a(\mathbf{H}_{\text{red}})$.

B. Simulation results

Figure 1 shows the comparison of augmented lattice reduction with LLL-SIC detection, both using MMSE-GDFE preprocessing. The simulations refer to an uncoded 6×6 MIMO system using 16-QAM (quadrature amplitude modulation) constellations. The improved decoder defined in (10) is used for augmented lattice reduction.

Two versions of augmented lattice reduction with different values of the parameter ε are compared. Clearly it is preferable to choose ε as big as possible in order to minimize the probability $P\left\{\|\mathbf{w}\| > \frac{\varepsilon}{\alpha^{\frac{m-1}{2}}} d_{\mathbf{H}}\right\}$. Version 1 corresponds to the choice $\varepsilon = \frac{1}{2\sqrt{2}\alpha^{\frac{m}{2}}}$, the highest value of ε that verifies the hypothesis of Proposition 1. At the symbol error rate (SER) of $1 \cdot 10^{-4}$, its performance is within $0.8\,\text{dB}$ from ML decoding and gains $1.9\,\text{dB}$ with respect to LLL-SIC decoding.

Version 2 corresponds to a value of ε optimized by computer search (experimentally, this is around $2^{-\frac{m}{4}}$), whose performance is within only $0.4\,\text{dB}$ of ML decoding at the SER of $1 \cdot 10^{-4}$. From now on, we will always consider this optimized version. For higher values of ε, we are not able to prove that the LLL algorithm finds the shortest lattice vector in $\mathcal{L}(\widetilde{\mathbf{H}})$. However, it is well-known that the LLL algorithm performs much better on average than the theoretical bounds predict.

The gain with respect to LLL-SIC decoding increases with the number of antennas: it is $3.5\,\text{dB}$ for an 8×8 MIMO system, at the SER of 10^{-4}. On the other side, augmented lattice reduction is still within $0.8\,\text{dB}$ from ML performance (see Fig. 2).

V. Complexity Analysis and Simulation Results

In this section we propose to estimate the additional complexity required by augmented lattice reduction with respect to LLL-ZF and LLL-SIC decoding. We are interested in the complexity order as a function of the number of transmit and receive antennas. For the sake of simplicity, we consider the case $n = m$.

A. Theoretical bounds

The complexity of LLL reduction of a Gaussian matrix $\mathbf{H}$ has been studied in [8] and [13]. As we have seen in Section II, every instance of the LLL-SIC (respectively LLL-ZF) decoder consists of three main phases: GSO, the main body of the LLL algorithm and detection.

The full GSO which is performed at the beginning of the LLL algorithm requires $O(m^3)$ elementary operations. The number $K(\mathbf{H})$ of iterations (Lovasz tests) in the main body of the LLL algorithm for a fixed realization $\mathbf{H}$ of the channel is bounded by [5, 13, 8]

$$K(\mathbf{H}) \leq m^2 \log_{\frac{1}{\sqrt{\delta}}} \left(\frac{A(\mathbf{H})}{a(\mathbf{H})} \right) + m, \tag{13}$$

where $A(\mathbf{H})$ and $a(\mathbf{H})$ denote respectively the maximum and minimum norm of the Gram-Schmidt vectors of $\mathbf{H}$. For general $\mathbf{H}$, $K(\mathbf{H})$ can be arbitrarily large. However, it was shown in [13] and [8] that $\mathbb{E}(K(\mathbf{H})) \sim O\left(m^2 \ln m\right)$.

Each iteration of the classical LLL algorithm requires $O(m^2)$ elementary operations. However, this estimate can be reduced to $O(m)$ by considering a weaker version of the algorithm, called *effective LLL reduction*, which has been proposed in [13]. It consists in removing the size reduction operations RED(k,l) for $l = k-2, \ldots, 1$ (lines 13-15 in Algorithm 1). As shown in [13], effective LLL reduction outputs the same Gram-Schmidt vectors as the standard LLL reduction. Therefore, SIC decoding using effective LLL reduction has the

[3]This result was used in [17] in order to prove that the LLL-ZF decoder achieves the receive diversity order. The proof in [17] actually refers to the complex model (1), but the statement also holds for the real model since $d_{\mathbf{H}} = d_{\mathbf{H}_c}$, $\|\mathbf{w}\| = \|\mathbf{w}_c\|$.

same performance as LLL-SIC. In the case of ZF decoding, a final cycle of size-reduction, requiring $O(m^3)$ operations, has to be performed on the effectively LLL-reduced basis.

Since LLL reduction outputs the GSO of $\mathbf{H}_{\mathrm{red}}$, its QR decomposition is easily obtained and so the complexity of *SIC detection* is negligible. The QR decomposition can be also used to perform *ZF detection*, by back substitution using $\mathbf{R}$.

In conclusion, the average complexity of LLL-SIC and LLL-ZF detection is of the order $O\left(m^4 \ln m\right)$ if using the standard LLL algorithm and $O\left(m^3 \ln m\right)$ for effective LLL.

For fixed $\mathbf{H}$, we can use the estimate (13) to obtain a bound of the number of iterations of the LLL reduction of $\widetilde{\mathbf{H}}$. The GSO of $\widetilde{\mathbf{H}}$ yields

$$\begin{pmatrix} \mathbf{h}_1^* & \cdots & \mathbf{h}_m^* & \mathbf{0}_{m\times 1} \\ 0 & \cdots & 0 & t \end{pmatrix}.$$

Therefore $a(\widetilde{\mathbf{H}}) \geq \min(t, a(\mathbf{H})) = \min(\varepsilon a(\mathbf{H}_{\mathrm{red}}), a(\mathbf{H}))$. LLL reduction increases the minimum of the Gram-Schmidt vectors [5], so $a(\mathbf{H}_{\mathrm{red}}) \geq a(\mathbf{H})$, and $a(\widetilde{\mathbf{H}}) \geq \varepsilon a(\mathbf{H})$. On the other side $t < a(\mathbf{H}_{\mathrm{red}}) \leq A(\mathbf{H}_{\mathrm{red}}) \leq A(\mathbf{H})$ and so $A(\widetilde{\mathbf{H}}) = \max(t, A(\mathbf{H})) = A(\mathbf{H})$. Then

$$K(\widetilde{\mathbf{H}}) \leq (m+1)^2 \log_{\frac{1}{\sqrt{\delta}}} \left(\frac{A(\widetilde{\mathbf{H}})}{a(\widetilde{\mathbf{H}})}\right) + m + 1 \leq$$
$$\leq \frac{(m+1)^2}{c} \ln \left(\frac{A(\mathbf{H})}{\varepsilon a(\mathbf{H})}\right) + m + 1$$

where $c = \log \frac{1}{\sqrt{\delta}}$. Following [8], we can estimate the average $\mathbb{E}[K(\widetilde{\mathbf{H}})]$, recalling that $\frac{A(\mathbf{H})}{a(\mathbf{H})} \leq k(\mathbf{H})$, the condition number of $\mathbf{H}$, and that [2]

$$\mathbb{E}[\ln k(\mathbf{H})] \leq \ln m + 2.24.$$

We thus obtain

$$\mathbb{E}[K(\widetilde{\mathbf{H}})] \leq \frac{(m+1)^2}{c} \left(-\ln \varepsilon + \mathbb{E}[\ln k(\mathbf{H})]\right) + m + 1 \leq$$
$$\leq \frac{(m+1)^2}{c} \left(-\ln \varepsilon + \ln m + 2.24\right) + m + 1. \quad (14)$$

For the choice $\varepsilon = \frac{1}{2\sqrt{2}\alpha^{\frac{m}{2}}}$, the average number of iterations of the main loop of the LLL algorithm using augmented lattice reduction is at most of the order of $O(m^3)$. This yields a complexity bound of $O(m^5)$ operations using standard LLL reduction and $O(m^4)$ operations using effective LLL followed by a final cycle of size reduction. (The latter is necessary to obtain the best performance for the improved decoder (10)).

B. Simulation results

Our complexity simulations evidence the fact that the upper bounds (13) and (14) on the average number of iterations of the LLL algorithm for LLL-aided linear decoding and the augmented lattice reduction method are both quite pessimistic. The number of iterations for both methods appears in fact to be quadratic in practice, see Fig. 3.

Augmented lattice reduction and LLL-SIC appear to have the same complexity order but augmented lattice reduction requires roughly 1.5 times the number of flops[4] as LLL-SIC, at least for small values of m (Fig. 4).

Our simulations are performed for $\delta = \frac{3}{4}$. Two versions of augmented lattice reduction are considered, one using standard LLL, the other using effective LLL followed by a final cycle of size reduction. As was shown also in [13], for small dimensions ($N < 10$) effective LLL reduction doesn't offer a real complexity advantage with respect to standard LLL.

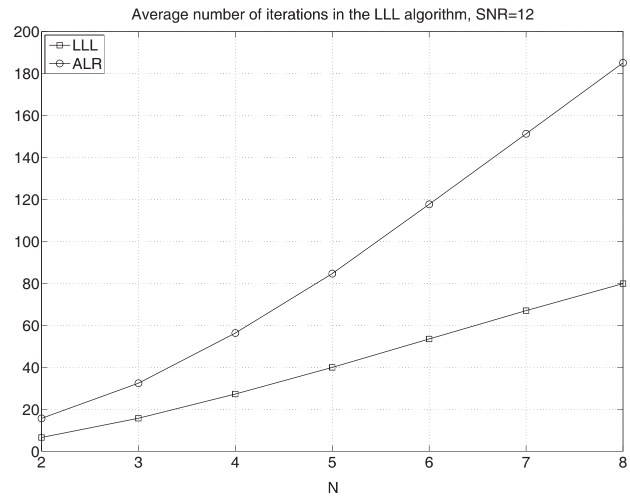

Fig. 3. Average number of steps of the LLL algorithm as a function of the number N of transmit and receive antennas.

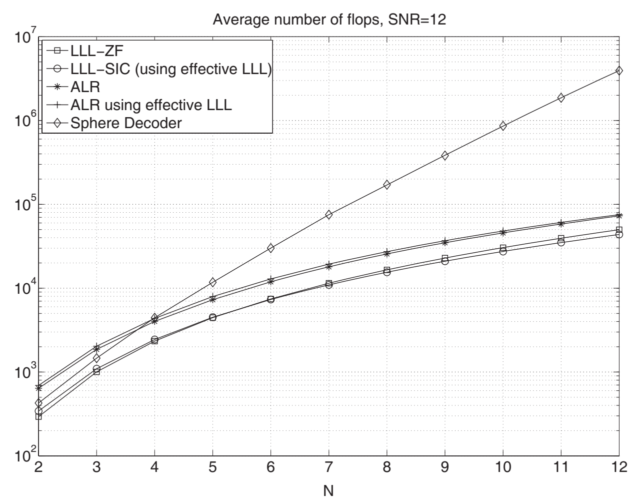

Fig. 4. Complexity comparison (expressed in flops, in logarithmic scale) of augmented lattice reduction with LLL-ZF, LLL-SIC and sphere decoding as a function of the number N of transmit and receive antennas, at $\mathrm{SNR} = 12$, using 16-QAM constellations.

C. Case of slow fading channels

If the channel matrix $\mathbf{H}$ varies so slowly that it can be considered constant during the transmission of several frames, the complexity of LLL-SIC and LLL-ZF decoding is greatly reduced since lattice reduction needs to be performed only once. In the case of augmented lattice reduction, the matrix $\widetilde{\mathbf{H}}$ depends also on the received vector $\mathbf{y}$, so an update of the

[4]Here we define a "flop" as any floating-point operation (addition, multiplication, division or square root).

LLL algorithm will still be required for each frame. However, a significant complexity gain will be achieved, since in many cases of interest, LLL-reducing the first m columns roughly accounts for $\frac{2}{3}$ of the total complexity, as suggested by Fig. 4.

D. Complex LLL reduction

A generalization of the LLL algorithm to complex lattices has been applied to MIMO decoding in [6]. It has been show experimentally in [6] that the complex versions of LLL-ZF and LLL-SIC decoding have essentially the same performance of their real counterparts but with substantially reduced complexity.

A complex version of the augmented lattice reduction can be implemented by LLL-reducing the $(N+1)\times(M+1)$-dimensional matrix

$$\widetilde{\mathbf{H}}_{\mathrm{c}} = \begin{pmatrix} \mathbf{H}_{\mathrm{c}} & -\mathbf{y}_{\mathrm{c}} \\ \mathbf{0}_{1\times N} & t \end{pmatrix},$$

and allows to save about 40% of computational costs without any change in performance.

VI. CONCLUSIONS

In this paper, we have presented a low-complexity decoding method for MIMO systems based on augmented lattice reduction, which improves a previous technique introduced in [11].

Simulation results evidence that our augmented lattice reduction technique has a substantial performance gain with respect to the classical LLL-ZF and LLL-SIC decoders, while having approximately the same complexity order.

ACKNOWLEDGEMENTS

We wish to thank Cong Ling for helpful discussions. We also would like to thank the three anonymous reviewers for their valuable suggestions and comments that helped to improve the quality of this paper, in particular concerning the complexity analysis.

REFERENCES

[1] L. Babai, "On Lovasz' lattice reduction and the nearest lattice point problem," *Combinatorica*, vol. 6, no. 1, pp. 1–13, 1986.

[2] C. Chen and J. J. Dongarra, "Condition numbers of Gaussian random matrices," *SIAM J. Matrix Analysis and Applications*, vol. 27, no. 3, 2005, 603–620, 2005.

[3] H. Cohen, "A course in computational algebraic number theory," *Graduate Texts in Mathematics*, Springer, 2000.

[4] M. O. Damen, H. El Gamal, and G. Caire, "On maximum-likelihood detection and the search for the closest lattice point," *IEEE Trans. Inf. Theory*, vol. 49, pp. 2389–2402, 2003.

[5] H. Daudé and B. Vallée, "An upper bound on the average number of iterations of the LLL algorithm," *Theoretical Computer Science*, vol. 123, no. 1, 95–115, 1994.

[6] Y. H. Gan, C. Ling, and W. H. Mow, "Complex lattice reduction algorithm for low-complexity MIMO detection," *IEEE Trans. Signal Process.*, vol. 57, no. 7, 2009.

[7] J. Jaldén and P. Elia, "DMT optimality of LR-aided linear decoders for a general class of channels, lattice designs, and system models," submitted to *IEEE Trans. Inf. Theory*.

[8] J. Jaldén, D. Seethaler, and G. Matz, "Worst- and average-case complexity of LLL lattice reduction in MIMO wireless systems," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2008, pp. 2685–2688.

[9] R. Kannan, "Minkowski's convex body theorem and integer programming," *Math. Oper. Res.* vol. 12, pp. 415–440, 1987.

[10] K. Raj Kumar, G. Caire, and A. L. Moustakas, "Asymptotic performance of linear receivers in MIMO fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, 2009.

[11] N. Kim and H. Park, "Improved lattice reduction aided detections for MIMO systems," *Vehicular Technology Conference*, 2006.

[12] C. Ling, "On the proximity factors of lattice reduction-aided decoding," submitted for publication. Preprint version available online: http://arxiv.org/abs/1006.1666.

[13] C. Ling and N. Howgrave-Graham, "Effective LLL reduction for lattice decoding," *IEEE International Symposium on Information Theory*, 2007, Nice, France.

[14] A. K. Lenstra, J. H. W. Lenstra, and L. Lovasz, "Factoring polynomials with rational coefficients," *Math. Ann.*, vol. 261, pp. 515-534, 1982.

[15] J. C. Lagarias, H. W. Lenstra Jr., and C. P. Schnorr, "Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice," *Combinatorica*, vol. 10, no. 4, pp. 333–348, 1990.

[16] P. Q. Nguyen and J. Stern, "Lattice reduction in cryptology: an update," in *Algorithmic Number Theory, Lecture Notes in Computer Science*, Springer, 2006

[17] M. Taherzadeh, A. Mobasher, and A. K. Khandani, "LLL reduction achieves the receive diversity in MIMO decoding," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4801–4805, 2007.

[18] C. Windpassinger and R. Fischer, "Low-complexity near-maximum likelihood detection and precoding for MIMO systems using lattice reduction," in *Proc. IEEE Information Theory Workshop*, 2003, pp. 345–348.

[19] H. Yao and G. W. Wornell, "Lattice-reduction-aided detectors for MIMO communication systems," in *Proc. Global Telecommunications Conference*, 2002, vol. 1, pp. 424–428.

Laura Luzzi was born in Pavia, Italy, in 1980. She received the degree (Laurea) in Mathematics from the University of Pisa, Italy, in 2003 and the Ph.D. degree in Mathematics for Technology and Industrial Applications from Scuola Normale Superiore, Pisa, Italy, in 2007. During the completion of this work, she was a postdoctoral fellow at the Department of Communications and Electronics at TELECOM ParisTech, Paris, France. Her research interests include algebraic space-time coding and decoding, and continued fractions.

Ghaya Rekaya-Ben Othman was born in Tunis, Tunisia, in 1977. She received the degree in electrical engineering from ENIT, Tunisia, in 2000 and the Ph.D. degree from the Ecole Nationale Supérieure des Télécommunications (ENST) Paris, France, in 2004. Since 2005, she has been with the Department of Communications and Electronics, TELECOM ParisTech, Paris, France, as Assistant Professor. Her research interests are in space-time coding and lattice reduction and decoding.

Jean-Claude Belfiore received the Diplôme d'ingénieur (Eng. degree) from Supelec in 1985, the doctorat (PhD) from Ecole Nationale Supérieure des Télécommunications (ENST Paris) in 1989 and the "Habilitation à diriger des Recherches" (HdR) from Université Pierre et Marie Curie (UPMC) in 2001. He was enrolled in Alcatel in 1985 and then in 1989 in ENST, Paris where he is now a full professor. He is carrying out research at the "Laboratoire de Traitement et Communication de l'Information" (LTCI), joint research laboratory between ENST and the "Centre National de la Recherche Scientifique" (CNRS), UMR 5141, where he is in charge of research activities in the fields of wireless communications, coding for wireless networks and space-time coding. Jean-Claude Belfiore has made pioneering contributions on signal design for wireless communication systems, space-time coding, cooperative and multi-user communications.