WORST- AND AVERAGE-CASE COMPLEXITY OF LLL LATTICE REDUCTION IN MIMO WIRELESS SYSTEMS

Joakim Jaldén[†]*, Dominik Seethaler*[‡]*, and Gerald Matz*[†]

[†] Institute of Communications and Radio-Frequency Engineering,
Vienna University of Technology,
Gusshausstrasse 25/389, A-1040 Vienna, Austria.
email: {jjalden,gmatz}@nt.tuwien.ac.at

[‡] Communication Technology Laboratory,
ETH Zürich,
Sternwartstrasse 7, CH-8092 Zürich, Switzerland.
email: seethal@nari.ee.ethz.ch

ABSTRACT

Lattice reduction by means of the LLL algorithm has been previously suggested as a powerful preprocessing tool that allows to improve the performance of suboptimal detectors and to reduce the complexity of optimal MIMO detectors. The complexity of the LLL algorithm is often cited as polynomial in the dimension of the lattice. In this paper we argue that this statement is not correct when made in the MIMO context. Specifically, we demonstrate that in typical communication scenarios the worst-case complexity of the LLL algorithm is not even finite. For i.i.d. Rayleigh fading channels, we further prove that the average LLL complexity is polynomial and that the probability for an atypically large number of LLL iterations decays exponentially.

Index Terms— LLL, lattice reduction, MIMO, decoding, precoding, complexity.

1. INTRODUCTION

Lattice reduction (LR) techniques have become increasingly important tools in the design of transceivers for multiple input-multiple output (MIMO) communication systems. It was first demonstrated in [1] that augmenting traditional linear MIMO detectors with LR techniques yields new (LR aided) detectors with favorable performance. LR has also been used to reduce the complexity of optimal detectors such as the sphere decoder [2, 3] and to improve broadcast precoding schemes [4].

LR in MIMO systems amounts to reducing a lattice basis that corresponds to the MIMO channel matrix, which itself is usually modeled in a stochastic manner. The most popular solution to this problem (see e.g. [2, 4, 5]) has been the basis reduction algorithm of Lenstra, Lenstra, and Lovász (LLL) [6]. The LLL algorithm operates iteratively and terminates as soon as a reduced basis is obtained. The number of iterations required, denoted K, depends strongly on the original lattice basis. For practical implementations of LR in MIMO systems, it is thus of utmost importance to characterize the statistics of K for a given stochastic MIMO channel model.

A well-known result regarding the number of LLL iterations states that for n-dimensional lattices with integer input basis vectors of bounded length B, the LLL algorithm terminates after at most $O(n^2 \log B)$ iterations [6]. This results was used in [6] to prove that the complexity (defined as the number of bit operations) of the LLL algorithm is polynomial in the size of the input (defined as the number of bits required to describe the lattice basis). However, the complexity analysis of [6] does *not* apply to the MIMO context since the stochastic channel models typically adopted do not result in integer basis vectors of bounded length (e.g., in the i.i.d. Rayleigh fading scenario the lattice basis has i.i.d. Gaussian elements, which results in real-valued basis vectors of arbitrary large length). Furthermore, contrary to [6] most of the MIMO literature measures complexity in terms of arithmetic operations on *real-valued* numbers, whose size can not be measured in bits. In spite of these deviations from the assumptions in [6], that paper is often incorrectly used to claim polynomial complexity of the LLL algorithm when applied to MIMO systems (see e.g. [4, 5, 7]).

In this paper, we present a detailed complexity analysis of the LLL algorithm when applied to MIMO channels:

- For MIMO channel models that allow for arbitrarily poorly conditioned channel matrices (e.g., the i.i.d. Rayleigh fading model), we demonstrate that for any given k there exist channel realizations that require $K \geq k$ LLL iterations, i.e., in this case, there is no universal upper bound on the number of LLL iterations (even for fixed lattice dimension).
- By extending [8] to i.i.d. Rayleigh fading MIMO channels, we show that the *average* number of LLL iterations is upper bounded by a polynomial in the dimension of the lattice. A similar result was independently obtained in [9], although by a slightly different approach. The result therein is however for a real-valued Gaussian channel model and fails to apply to the broadcast precoding case
- We establish that the tail probability of K in the i.i.d. Rayleigh fading case decays at least exponentially.

The rest of the paper is organized as follows. The LLL algorithm is outlined in Section 2.1 and its application to MIMO systems is briefly reviewed in Section 2.2. The main contributions of this work are found in Section 3, where we rigorously establish the claims made above.

2. BACKGROUND AND MOTIVATION

In order to put the statements of Section 3 into context, we provide some background on the LLL algorithm, its use for MIMO detection, and the stochastic lattice models arising in that context.

For $m \geq n$, an n-dimensional lattice $\mathcal{L}$ in m-dimensional Euclidean space is a discrete subset of $\mathbb{R}^m$ given by

$$\mathcal{L} \triangleq \left\{ \mathbf{B}\mathbf{x} \,|\, \mathbf{x} \in \mathbb{Z}^n \right\}. \qquad (1)$$

Here $\mathbb{Z}$ denotes the set of integers and $\mathbf{B} = [\mathbf{b}_1 \ldots \mathbf{b}_n] \in \mathbb{R}^{m \times n}$ denotes the *generator matrix* of $\mathcal{L}$ and consists of n linearly independent lattice *basis vectors* $\mathbf{b}_1, \ldots, \mathbf{b}_n$. For a given lattice $\mathcal{L}$, the

This work was supported by the STREP project No. IST-026905 (MASCOT) within the Sixth Framework Programme of the European Commission.

1-4244-1484-9/08/$25.00 ©2008 IEEE

Table 1 The LLL algorithm

```
1:  $l \leftarrow 2$
2:  repeat
3:      $\mathbf{b}_l \leftarrow \mathbf{b}_l - \lceil \mu_{l\,l-1} \rfloor \mathbf{b}_{l-1}$                    (translate)
4:      if $\|\hat{\mathbf{b}}_{l-1}\|^2 > t^2 \|\hat{\mathbf{b}}_l + \mu_{l\,l-1}\hat{\mathbf{b}}_{l-1}\|^2$ then
5:          $\mathbf{b}_l \leftrightarrow \mathbf{b}_{l-1}$                                          (swap)
6:          $l \leftarrow \max(l-1, 2)$
7:      else
8:          for $j = l-2$ to $1$ do
9:              $\mathbf{b}_l \leftarrow \mathbf{b}_l - \lceil \mu_{lj} \rfloor \mathbf{b}_j$                (translate)
10:         end for
11:         $l \leftarrow l+1$
12:     end if
13: until $l > n$
```

generator matrix is not unique. In fact, if $\mathbf{B}$ is a generator matrix for $\mathcal{L}$, then any matrix $\mathbf{B}' = \mathbf{B}\mathbf{U}$, where $\mathbf{U}$ is unimodular (i.e., $\mathbf{U} \in \mathbb{Z}^{n \times n}$ and $\det(\mathbf{U}) = \pm 1$) is also a generator matrix for $\mathcal{L}$. Given a generator matrix $\mathbf{B}$, the task of LR algorithms is to find another generator matrix $\mathbf{B}'$ that has improved properties according to specific criteria.

2.1. LLL Lattice Reduction

For a given a generator matrix $\mathbf{B} = [\mathbf{b}_1 \ldots \mathbf{b}_n]$, let $\hat{\mathbf{b}}_1, \ldots, \hat{\mathbf{b}}_n$ denote the vectors obtained by Gram-Schmidt orthogonalization:

$$\hat{\mathbf{b}}_i \triangleq \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \hat{\mathbf{b}}_j \qquad \text{with} \quad \mu_{ij} \triangleq \frac{\mathbf{b}_i^{\mathrm{T}} \hat{\mathbf{b}}_j}{\|\hat{\mathbf{b}}_j\|^2}\,. \tag{2}$$

A lattice basis is *Lovász t-reduced* if it satisfies the Lovász condition

$$\|\hat{\mathbf{b}}_{i-1}\|^2 \leq t^2 \|\hat{\mathbf{b}}_i + \mu_{i\,i-1}\hat{\mathbf{b}}_{i-1}\|^2 \quad \text{for} \quad 1 < i \leq n\,, \tag{3}$$

and in addition is *size-reduced*, i.e.,

$$|\mu_{ij}| \leq \tfrac{1}{2} \quad \text{for} \;\; 1 \leq j < i \leq n\,. \tag{4}$$

The real parameter t may be chosen anywhere in the range $(1, 2)$ but is typically chosen as $t = 2/\sqrt{3}$. The basis vectors of any Lovász t-reduced basis are relatively short and nearly orthogonal [6], which is desirable in many applications.

The LLL algorithm, stated in Table 1 for convenience, transforms a given basis into a Lovász t-reduced basis through a sequence of *swaps* and *translations* of the basis vectors ($\lceil \cdot \rfloor$ denotes rounding to the closest integer). The algorithm uses an index l (initialized to $l = 2$) and repeatedly tests the Lovász condition (cf. line 4)

$$\|\hat{\mathbf{b}}_{l-1}\|^2 \leq t^2 \|\hat{\mathbf{b}}_l + \mu_{l\,l-1}\hat{\mathbf{b}}_{l-1}\|^2\,. \tag{5}$$

If (5) is violated, the basis vectors $\mathbf{b}_l$ and $\mathbf{b}_{l-1}$ are swapped (line 5) and the index l is decremented (provided $l > 2$). If (5) is satisfied, the basis is size-reduced through a sequence of integer translations (lines 8–10) and l is incremented. The algorithm terminates as soon as $l > n$. At this stage, the basis is guaranteed to satisfy both (3) and (4). The original basis is overwritten with the reduced one. It should also be understood that $\hat{\mathbf{b}}_i$, $1 \leq i \leq n$, and μ_{ij}, $1 \leq j < i \leq n$, need to be updated according to (2) whenever the basis is changed (this happens in lines 3, 5, and 9).

2.2. LR-Aided MIMO Detection

We briefly summarize the application of LR in MIMO systems. Further details and additional motivation can be found in [1–4].

We consider the specific case of an equivalent complex baseband model for a MIMO system with N transmit and $M \geq N$ receive antennas, assuming a flat-fading MIMO channel. Here, the received vector $\mathbf{r} \in \mathbb{C}^M$ is given by

$$\mathbf{r} = \mathbf{H}\mathbf{s} + \mathbf{v}\,, \tag{6}$$

where $\mathbf{H} \in \mathbb{C}^{M \times N}$ is the channel matrix containing complex fading coefficients and $\mathbf{v} \in \mathbb{C}^N$ is additive white Gaussian noise. For simplicity, we assume that the transmitted symbols $\mathbf{s}$ are points in $\mathbb{Z}_{\mathbb{C}}^N$, where $\mathbb{Z}_{\mathbb{C}} = \mathbb{Z} + i\mathbb{Z}$ denotes the complex integers (this assumption is often satisfied in practice after proper scaling and translation of the symbol constellation [3]).

The model (6) is formulated in the complex domain but can be easily transformed into an equivalent real-valued model

$$\mathbf{y}_r = \mathbf{H}_r \mathbf{s}_r + \mathbf{v}_r, \tag{7}$$

where $\mathbf{H}_r \in \mathbb{R}^{m \times n}$ (with $n = 2N$ and $m = 2M$) is given by

$$\mathbf{H}_r \triangleq \begin{bmatrix} \Re\{\mathbf{H}\} & -\Im\{\mathbf{H}\} \\ \Im\{\mathbf{H}\} & \Re\{\mathbf{H}\} \end{bmatrix} \tag{8}$$

($\Re\{\cdot\}$ and $\Im\{\cdot\}$ respectively denote the real and imaginary part) and where the vectors $\mathbf{y}_r$, $\mathbf{s}_r$, and $\mathbf{v}_r$ are defined accordingly. Since $\mathbf{s}_r \in \mathbb{Z}^n$, the matrix $\mathbf{H}_r$ may be seen as the generator matrix of a lattice, and $\mathbf{y}_r$ as a lattice point perturbed by noise. The decoding problem amounts to finding a lattice point close to $\mathbf{y}_r$ [2, 3].

LR-aided detection is motivated by the fact that the performance and complexity of many detectors (e.g. the zero forcing detector) depends crucially on the condition number of the generator matrix (channel) $\mathbf{H}_r$. The key idea is to rewrite (7) as

$$\mathbf{y}_r = \mathbf{H}_r' \, \mathbf{s}_r' + \mathbf{v}_r, \tag{9}$$

where $\mathbf{H}_r' = \mathbf{H}_r \mathbf{U}$ with $\mathbf{U}$ unimodular is an improved generator matrix and $\mathbf{s}_r' = \mathbf{U}^{-1} \mathbf{s}_r$ is *again* in $\mathbb{Z}^n$. An estimate of $\mathbf{s}_r$ can be obtained by applying any conventional detector to the model (9) and transforming the resulting intermediate solution back to the original domain via the relation $\mathbf{s}_r = \mathbf{U}\,\mathbf{s}_r'$. The aim of LR is to select $\mathbf{U}$ such that the columns of $\mathbf{H}_r'$ are as orthogonal as possible since this is favorable for detector performance and/or complexity. This task can be accomplished using the LLL algorithm. Indeed, it has recently been shown that LR-aided zero-forcing detection using the LLL algorithm achieves full receive diversity in i.i.d. Rayleigh fading [5].

2.3. Stochastic Lattice Models

In the following, we will assume a MIMO channel with i.i.d. Rayleigh fading and consider two corresponding stochastic lattice models. In the first case, referred to as *primal Rayleigh model*, the generator matrix equals $\mathbf{B}_{\mathcal{P}} \triangleq \mathbf{H}_r$ (cf. (8)). Here, $\mathbf{B}_{\mathcal{P}}$ consists of two deterministically related blocks (the first N columns and the last N columns) whose elements are separately i.i.d. Gaussian.

With the second case, the LLL algorithm is applied to the dual basis, which is preferable in some situations [5]. The generator matrix of the dual basis is given by $\mathbf{B}_{\mathcal{D}} \triangleq (\mathbf{H}_r^{\dagger})^{\mathrm{T}}$, where $\mathbf{H}_r^{\dagger} = (\mathbf{H}_r^{\mathrm{T}}\mathbf{H}_r)^{-1}\mathbf{H}_r^{\mathrm{T}}$ denotes the Moore-Penrose pseudo inverse of $\mathbf{H}_r$. Using the matrix inversion lemma, it can be shown that $\mathbf{B}_{\mathcal{D}} \triangleq (\mathbf{H}_r^{\dagger})^{\mathrm{T}}$ features exactly the same block structure as $\mathbf{H}_r$ in (8). This case will referred to as the *dual Rayleigh model* and also arises naturally in the precoding context (e.g. [4]).

3. LLL COMPLEXITY

This section provides an analysis of the worst- and average-case complexity of the LLL algorithm when used in MIMO systems. Complexity will be measured in terms of the the number K of LLL iterations, defined as the number "repeat" loops entered by the LLL algorithm (more precisely, the number of Lovász tests (line 4 in Table 1) performed by the algorithm). We emphasize that all results hold true for arbitrary values of t in the range $(1, 2)$.

3.1. Impact of Condition Number

For an arbitrary basis $\mathbf{B} = [\mathbf{b}_1 \dots \mathbf{b}_n]$ define

$$a \triangleq \min_{1\le i\le n} \|\hat{\mathbf{b}}_i\| \quad \text{and} \quad A \triangleq \max_{1\le i\le n} \|\hat{\mathbf{b}}_i\| \tag{10}$$

where $\hat{\mathbf{b}}_1, \dots, \hat{\mathbf{b}}_n$ are the Gram-Schmidt vectors corresponding to $\mathbf{B}$ (cf. (2)). It was shown in [8] that the number of iterations K required to LLL-reduce $\mathbf{B}$ is upper bounded according to

$$K \le n^2 \log_t \frac{A}{a} + n\,. \tag{11}$$

As an immediate consequence of the bound (11), the LLL algorithm is guaranteed to terminate for any given real-valued basis. Our subsequent analysis will replace (11) with a less tight bound, which is, however, more tractable within our stochastic lattice models. To this end, note that $\sigma_1 \ge A$ and $a \ge \sigma_n$ where $\sigma_1 \ge \dots \ge \sigma_n$ are the singular values of the generator matrix $\mathbf{B}$ [10]. This implies $A/a \le \kappa(\mathbf{B})$ where $\kappa(\mathbf{B}) \triangleq \sigma_1/\sigma_n$ is the condition number of $\mathbf{B}$. The number of LLL iterations is thus upper bounded according to

$$K \le n^2 \log_t \kappa(\mathbf{B}) + n\,. \tag{12}$$

Based on (12) it is seen that the number of LLL iterations K can become large only for poorly conditioned generator matrices (i.e., small $\kappa(\mathbf{B})$ implies small K). The bound (12) has the advantage that it is useful for both the primal and dual Rayleigh models since

$$\kappa(\mathbf{B}_{\mathcal{P}}) = \kappa(\mathbf{B}_{\mathcal{D}}) = \kappa(\mathbf{H})\,,$$

which may be seen by noting that $\mathbf{H}$, $\mathbf{H}_r$, and $(\mathbf{H}_r^\dagger)^{\mathrm{T}}$ all have the same condition number [10]. Since the primal and dual Rayleigh model impose no constraint on the condition number $\kappa(\mathbf{H})$, the right-hand side of (12) is in these cases not bounded from above. This suggests that here the number of LLL iterations can be arbitrarily large. The next section will make this statement more precise.

3.2. Worst-Case Analysis

Proposition 1 *For any integers k, n, m such that $2 \le n \le m$, there exist real-valued bases for n-dimensional lattices in $\mathbb{R}^m$ such that their LLL reduction requires at least k iterations (i.e., $K \ge k$).*

Before discussing the implications of this result for MIMO systems, we provide a constructive proof inspired by the analysis of the related Gauss' algorithm in [11]. That the worst-case complexity of the Gauss algorithm is infinite is also noted in [1].

Proof: It is sufficient to prove the case $n = 2$ by constructing bases $[\mathbf{b}_1\, \mathbf{b}_2]$, whose LLL reduction requires at least k iterations. The general case $n > 2$ follows simply by considering lattice bases whose first two basis vectors are $\mathbf{b}_1$ and $\mathbf{b}_2$.

Consider two linearly independent real-valued vectors $\mathbf{u}, \mathbf{v} \in \mathbb{R}^m$ that satisfy

$$\|\mathbf{u}\| > 2\|\mathbf{v}\|\,, \tag{13}$$

but are arbitrary otherwise. The basis $[\mathbf{u}\,\mathbf{v}]$ generates a two-dimensional lattice $\mathcal{L}$ in $\mathbb{R}^m$and is necessarily size-reduced since (13) implies that

$$\frac{|\mathbf{v}^{\mathrm{T}}\mathbf{u}|}{\|\mathbf{u}\|^2} < \frac{1}{2}\,. \tag{14}$$

For an arbitrary integer r, $|r| \ge 3$, let $\mathbf{w}$ be given by

$$\mathbf{w} \triangleq r\mathbf{u} + \mathbf{v}\,.$$

Then, $[\mathbf{b}_1\mathbf{b}_2] = [\mathbf{w}\,\mathbf{u}] = [\mathbf{u}\,\mathbf{v}]\,\mathbf{M}$ with

$$\mathbf{M} \triangleq \begin{bmatrix} r & 1 \\ 1 & 0 \end{bmatrix} \tag{15}$$

forms another basis for $\mathcal{L}$ since $\mathbf{M}$ is unimodular. Furthermore, the basis $[\mathbf{b}_1\mathbf{b}_2] = [\mathbf{w}\,\mathbf{u}]$ is also size-reduced since

$$\|\mathbf{w}\| \ge |r|\|\mathbf{u}\| - \|\mathbf{v}\| > 2\|\mathbf{u}\|\,, \tag{16}$$

which implies

$$\mu_{21} = \frac{\mathbf{b}_2^{\mathrm{T}}\hat{\mathbf{b}}_1}{\|\hat{\mathbf{b}}_1\|^2} = \frac{\mathbf{b}_2^{\mathrm{T}}\mathbf{b}_1}{\|\mathbf{b}_1\|^2} = \frac{\mathbf{u}^{\mathrm{T}}\mathbf{w}}{\|\mathbf{w}\|^2} < \frac{1}{2}\,. \tag{17}$$

Consider now the LLL reduction of $[\mathbf{b}_1\mathbf{b}_2] = [\mathbf{w}\,\mathbf{u}]$, starting with $l = 2$. Due to (17), $\lceil\mu_{21}\rfloor = 0$ and line 3 will leave $\mathbf{b}_2$ unchanged. In line 4, the LLL algorithm finds the condition $\|\mathbf{b}_1\| > t^2\|\mathbf{b}_2\|$ (remember $l = 2$) satisfied since $\|\mathbf{w}\|^2 > 4\|\mathbf{u}\|^2$ (cf. (16)) and $t^2 < 4$. Hence, the basis vectors are swapped to form $[\mathbf{b}_1\mathbf{b}_2] = [\mathbf{u}\,\mathbf{w}]$. In the next iteration $\mathbf{b}_2$ is replaced by

$$\mathbf{b}_2 - \lceil\mu_{21}\rfloor\mathbf{b}_1 = \mathbf{w} - \lceil\mu_{21}\rfloor\mathbf{u}$$

where

$$\mu_{21} = \frac{\mathbf{b}_2^{\mathrm{T}}\hat{\mathbf{b}}_1}{\|\hat{\mathbf{b}}_1\|^2} = \frac{\mathbf{b}_2^{\mathrm{T}}\mathbf{b}_1}{\|\mathbf{b}_1\|^2} = \frac{\mathbf{w}^{\mathrm{T}}\mathbf{u}}{\|\mathbf{u}\|^2} = r + \frac{\mathbf{v}^{\mathrm{T}}\mathbf{u}}{\|\mathbf{u}\|^2}\,.$$

By (14) it follows that $\lceil\mu_{21}\rfloor = r$. Hence, the algorithm replaces $\mathbf{b}_2$ with $\mathbf{w} - \lceil\mu_{21}\rfloor\mathbf{u} = \mathbf{w} - r\mathbf{u} = \mathbf{v}$ and reaches line 4 in the second iteration with the basis $[\mathbf{b}_1\mathbf{b}_2] = [\mathbf{u}\,\mathbf{v}]$ and $l = 2$. This, however, is exactly the same state as in the first iteration of the LLL reduction of $[\mathbf{u}\,\mathbf{v}]$. Hence, it follows that the LLL reduction of $[\mathbf{w}\,\mathbf{u}]$ will require exactly one iteration more than the LLL reduction of $[\mathbf{u}\,\mathbf{v}]$. Repeating the same argument reveals that the reduction of $[\mathbf{w}\,\mathbf{u}]\mathbf{M} = [\mathbf{u}\,\mathbf{v}]\mathbf{M}^2$ requires one iteration more than that of $[\mathbf{w}\,\mathbf{u}]$ and hence two iterations more than the reduction of $[\mathbf{u}\,\mathbf{v}]$. By induction, it follows that the LLL reduction of

$$[\mathbf{b}_1\mathbf{b}_2] = [\mathbf{u}\,\mathbf{v}]\mathbf{M}^{k-1}\,, \tag{18}$$

where $\mathbf{M}$ is given in (15), requires $k - 1$ iterations more than the reduction of $[\mathbf{u}\,\mathbf{v}]$ and hence at least $K \ge k$ LLL iterations in total.

Discussion. Proposition 1 implies that there is no upper bound on the number of LLL iterations for the set of lattices with generator matrices taken from $\mathbb{R}^{m\times n}$. This result is immediately applicable to the primal and dual Rayleigh model with $N \ge 2$, since the distributions of $\mathbf{B}_{\mathcal{P}}$ and $\mathbf{B}_{\mathcal{D}}$ do not prevent that their respective first two columns occasionally conform with (18).

Note also that the lengths of the basis vectors are completely irrelevant for this result. In fact, the number of LLL iterations is invariant to scaling of $\mathbf{B}$ [8] and the basis vectors could thus be assumed to satisfy any given length constraint. Proposition 1 rather relies on generator matrices with arbitrarily large condition number, which exist both under the primal and dual Rayleigh model. Indeed, the construction in (18) yields poorly conditioned generator matrices since the condition number of $\mathbf{M}^k$ is $\kappa(\mathbf{M}^k) = \kappa(\mathbf{M})^k \approx r^{2k}$.

3.3. Average-Case Analysis and Tail Probabilities

Based on (12), the statistics of K can be characterized via the statistical properties of $\kappa(\mathbf{H})$ previously investigated in [12]. Specifically, it has been shown that ($\mathrm{E}\{\cdot\}$ denotes expectation) [12]

$$\mathrm{E}\{\log_e \kappa(\mathbf{H})\} \leq \log_e \frac{N}{M-N+1} + 2.240 \tag{19}$$

for any $M \geq N$. Combining (12) for $n = 2N$ and (19) immediately yields the bound

$$\mathrm{E}\{K\} \leq 4N^2\left(\log_t \frac{N}{M-N+1} + \frac{2.240}{\log_e t}\right) + 2N\,,$$

which implies polynomial average complexity

$$\mathrm{E}\{K\} = O(N^2 \log N).$$

It was furthermore shown in [12] that for $x \geq M-N+1$

$$\mathrm{P}\left(\kappa(\mathbf{H}) > \frac{xN}{M-N+1}\right) \leq \frac{1}{2\pi}\left(\frac{C}{x}\right)^{2(M-N+1)} \tag{20}$$

with a universal constant C, $5.013 \leq C \leq 6.298$. By (12) it follows that the tail probability of K, i.e., the probability that K exceeds a given value k, is upper bounded according to

$$\mathrm{P}(K \geq k) \leq \mathrm{P}\left(\kappa(\mathbf{H}) \geq t^{\frac{k-n}{n^2}}\right).$$

Invoking (20) then implies that for $k \geq 4N^2 \log_t N + 2N$ we have

$$\mathrm{P}(K \geq k) \leq \beta\alpha^k$$

where

$$\alpha \triangleq t^{-\frac{M-N+1}{2N^2}} < 1, \qquad \beta \triangleq \frac{1}{2\pi}\left(\frac{CNt^{\frac{1}{2N}}}{M-N+1}\right)^{2(M-N+1)}. \tag{21}$$

The above results are summarized in the following proposition.

Proposition 2 *The average number of LLL iterations required to reduce a random basis generated according to either the primal or dual Rayleigh model is polynomial and satisfies*

$$\mathrm{E}\{K\} \leq 4N^2\left(\log_t \frac{N}{M-N+1} + \frac{2.240}{\log_e t}\right) + 2N\,. \tag{22}$$

Furthermore, the tail probability of K decays exponentially, i.e., for $k \geq 4N^2 \log_t N + 2N$ it holds that

$$\mathrm{P}(K \geq k) \leq \beta\alpha^k, \tag{23}$$

where $\alpha < 1$ and β are given by (21).

3.4. The Complex Case

We have so far only considered the real valued version of the LLL algorithm. However, our analysis straightforwardly carries over to the complex LLL algorithm presented in [7]. In particular, the average number of iterations, $K_{\mathbb{C}}$, required by the complex LLL algorithm when applied to a complex channel matrix $\mathbf{H}$ with i.i.d. complex Gaussian elements satisfies

$$\mathrm{E}\{K_{\mathbb{C}}\} \leq N^2\left(\log_t \frac{N}{M-N+1} + \frac{2.240}{\log_e t}\right) + N.$$

Furthermore, the worst-case number of iterations can also be shown to be unbounded. We note that [7], with reference to [6], incorrectly states $O(n^2 \log B)$ as an upper bound on the number of LLL iterations.

4. CONCLUSIONS

We have shown that it is a misconception that the LLL algorithm will run in polynomial time when applied in wireless MIMO systems. In particular, for i.i.d. Rayleigh fading there exists no upper bound on the number of LLL iterations required, let alone one which grows polynomially with the dimensions of channel matrix. This conclusion relies heavily on the fact that real-valued bases may have arbitrarily large condition number. While this result, strictly speaking, is restricted to real-valued computation models, state-of-the-art floating- and fixed-point implementations require high arithmetic precision to guarantee algorithm stability. Hence, the problem of very large worst-case execution time persists in that realm.

Further investigations are required if the algorithm is to be seriously considered for implementation in real-time MIMO systems. It is particularly important to understand how early termination of the LLL algorithm will affect the performance of LR-aided detection and precoding and *when* (i.e., after how many iterations) to forcefully terminate the LLL algorithm. The results in Section 3.3 represent a step towards answering these questions.

5. REFERENCES

[1] H. Yao and G. W. Wornell, "Lattice reduction aided detectors for MIMO communication systems," in *Proc. IEEE Global Telecommunications Conference, GLOBECOM*, Taipei (Taiwan), Nov. 2002, pp. 424–428.

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

[3] M. O. Damen, H. El Gamal, and G. Caire, "On maximum-likelihood detection and the search for the closest lattice point," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2389–2401, Oct. 2003.

[4] C. Windpassinger, R. F. H. Fischer, and J. B. Huber, "Lattice-reduction-aided broadcast precoding," *IEEE Transactions on Communications*, vol. 52, no. 12, pp. 2057–2060, Dec. 2004.

[5] M. Taherzadeh, A. Mobasher, and A. K. Khandani, "LLL reduction achieves the receive diversity in MIMO decoding," *IEEE Transactions on Information Theory*, 2006, submitted.

[6] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, pp. 515–534, 1982.

[7] Y. H. Gan and W. H. Mow, "Complex lattice reduction algorithms for low-complexity MIMO detection," in *Proc. IEEE Global Telecommunications Conference, GLOBECOM*, St. Louis (MO), Nov. 2005, pp. 2953–2957.

[8] 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, pp. 95–115, Jan. 1994.

[9] C. Ling and N. Howgrave-Graham, "Effective LLL reduction for lattice decoding," in *Proc. IEEE International Symposium on Information Theory, ISIT*, June 2007.

[10] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, 1985.

[11] B. Vallée, "The Gauss' algorithm revisited," *Journal of Algorithms*, vol. 12, no. 4, pp. 556–572, Dec. 1991.

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