HKZ and Minkowski Reduction Algorithms for Lattice-Reduction-Aided MIMO Detection

Wen Zhang, Sanzheng Qiao, and Yimin Wei

***Abstract*—Recently, lattice reduction has been widely used for signal detection in multiinput multioutput (MIMO) communications. In this paper, we present three novel lattice reduction algorithms. First, using a unimodular transformation, a significant improvement on an existing Hermite-Korkine-Zolotareff-reduction algorithm is proposed. Then, we present two practical algorithms for constructing Minkowski-reduced bases. To assess the output quality, we compare the orthogonality defect of the reduced bases produced by LLL algorithm and our new algorithms, and find that in practice Minkowski-reduced basis vectors are the closest to being orthogonal. An error-rate analysis of suboptimal decoding algorithms aided by different reduction notions is also presented. To this aim, the proximity factor is employed as a measurement. We improve some existing results and derive upper bounds for the proximity factors of Minkowski-reduction-aided decoding (MRAD) to show that MRAD can achieve the same diversity order with infinite lattice decoding (ILD).**

***Index Terms*—HKZ, lattice reduction, LLL, MIMO detection, Minkowski, proximity factors.**

I. Introduction

LATTICE reduction plays an important role in numerous fields of mathematics, computer science [1]–[4], and cryptology [5], [6]. Recently, lattice reduction turned out to be extremely useful for detection and precoding in wireless multiple-input multiple-output (MIMO) systems. For lattice type modulation, the optimal maximum-likelihood (ML) decoding can be modeled as the closest vector problem (CVP), which can be solved by the sphere decoding algorithms [7]–[11]. However, the complexity of the sphere decoding algorithms increases exponentially with the number of transmit antennas [7], [8], [12]. It has been found that lattice reduction, used as an efficient preprocessor, has the potential to achieve high performance for low-complexity sub-optimal decoding algorithms such as zero-forcing (ZF) decoding and successive interference cancellation (SIC) decoding [13]–[17]. The basic idea is to view the channel matrix as a lattice basis (generator) matrix, and lattice reduction can improve the orthogonality defect of the basis matrix. Then the detection/precoding problem is solved based on the reduced basis to improve performance and complexity of a low-complexity decoding algorithm. See [18] for an introduction to lattice reduction and a survey of its applications in wireless communications.

There are several definitions of reduction. In 1850, Hermite introduced the first notion of reduction [19], In 1873, Korkine and Zolotareff [20] strengthened the definition of Hermite-reduction. Their proposed notion is referred to as *HKZ-reduction* [2]. In 1983, using induction, Kannan [21] presented the first algorithm for constructing HKZ-reduced bases. Helfrich [22], Kannan [23], and Banihashemi and Khandani [24] further refined Kannan's algorithm and improved the complexity analysis. In 1891, Minkowski [25] defined a very strong reduction notion, which is now known as *Minkowski-reduction*. In 1982, Lenstra, Lenstra and Lovász relaxed the definition of Hermite-reduction [19] to obtain a new reduction criterion known as *LLL-reduction* [26]. The corresponding algorithm is the first polynomial-time lattice reduction algorithm and has been widely used in public-key cryptanalysis [2], [27] and MIMO detection/precoding [14], [18]. Further improvements of LLL algorithm have been developed. While some improve the output quality [28]–[30], others improve the efficiency [16], [31]–[33]. It has been shown that the LLL-reduction-aided decoding can achieve the full diversity of a MIMO fading channel [14], [34]–[37].

Due to the high computational complexity of their algorithms, the HKZ and Minkowski reductions have not been seriously considered in MIMO detection/precoding. In this paper, we propose three practical algorithms, one for HKZ-reduction and two for Minkowski-reduction. Our complexity analysis shows that our algorithms significantly reduce the computational costs of their existing counterparts. Moreover, we prove that the Minkowski-reduction-aided decoding (MRAD), such as ZF decoding and SIC decoding, can achieve the same receive diversity with infinite lattice decoding (ILD), where ILD is the lattice decoding ignoring boundary [8], [17]. This makes our reduction algorithms potentially viable for MIMO detection. In addition, we improve the upper bounds for the proximity factors of LLL-reduction-aided ZF decoding and SIC decoding given in [15], [17].

Our HKZ-reduction algorithm differs from the one in [7] in that a novel unimodular transformation technique [38], instead

Manuscript received September 05, 2011; revised March 26, 2012 and July 03, 2012; accepted July 17, 2012. Date of publication August 01, 2012; date of current version nulldate. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. David Love. The work of S. Qiao was supported in part by the Shanghai Key Laboratory of Contemporary Applied Mathematics. The work of Y. Wei was supported by the National Natural Science Foundation of China by Grant 11271084, the Doctoral Program of the Ministry of Education by Grant 20090071110003, the 973 Program Project by Grant 2010CB327900, and by the Shanghai Education Committee (Dawn Project).

W. Zhang is with the School of Mathematical Sciences, Fudan University, Shanghai, 200433 China (e-mail: zhangwen9801@gmail.com).

S. Qiao is with the Department of Computing and Software, McMaster University, Hamilton, ON, L8S 4K1, Canada (e-mail: qiao@cas.mcmaster.ca).

Y. Wei is with the School of Mathematical Sciences and Shanghai and Key Laboratory of Mathematics for Nonlinear Sciences, Fudan University, Shanghai, 200433 China (e-mail: ymwei@fudan.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSP.2012.2210708

of the Kannan's strategy [21], is used for the expansion of a shortest vector into a new lattice basis. Also note that Kannan's basis expansion method only works for rational lattices, while our unimodular transformation technique works for any real lattice and is much more efficient than Kannan's method.

In the other two algorithms, we model the Minkowski-reduction problem as a constrained integer least squares problem, modify the Schnorr-Euchner (SE) search strategy [9], and use the unimodular transformation technique [38] for basis expansion. Our second Minkowski-reduction algorithm improves upon the first one by dynamically monitoring the basis expansion condition during the search process. Simulation results show that the second algorithm is much faster than the first one, and both of them can significantly outperform the existing algorithms [22], [39].

Note that in many communication applications, the lattice needed for decoding changes slowly, while the observed received vectors change frequently. That is, the preprocessing of the lattice generator matrix needs to be performed only infrequently, while the reduced basis is typically used many times. So it is worthy to invoke a good preprocessing procedure, even it requires a relatively high complexity. Since the vectors of HKZ and Minkowski-reduced bases are shorter and have smaller orthogonality defect than those of LLL-reduced bases, the bit-error-rate (BER) performance of sub-optimal MIMO detectors is expected to be further improved by applying our new algorithms.

The rest of the paper is organized as follows. In Section II, we introduce the MIMO system model and review several concepts in lattice theory. The new algorithm for constructing HKZ-reduced bases is given in Section III. Section IV presents the first algorithm for constructing Minkowski-reduced bases. The second Minkowski-reduction algorithm and the partial lattice reduction preprocessor are presented in Section V. In Section VI, we discuss the performance of ZF decoding and SIC decoding aided by different reduction techniques. In Section VII, we present our experimental results.

Notations: Matrices and column vectors are denoted by upper and lowercase boldface letters, the determinant and transpose of a square matrix $\mathbf{B}$ by $\det(\mathbf{B})$ and $\mathbf{B}^{\mathrm{T}}$, respectively, and the Euclidean norm of a vector $\mathbf{v}$ by $\|\mathbf{v}\|_2$. $\mathbf{I}_n$ denotes the $n \times n$ identity matrix, $\mathbf{0}^n$ the n-dim all-zeros vector, $\boldsymbol{\phi}$ an empty set, $\mathbf{B}(a:b, c:d)$ a submatrix of $\mathbf{B}$ with elements from rows a to b and from columns c to d, where $:$ denotes a complete row or column.

II. Preliminaries

In this section, we briefly introduce the model of MIMO detection and some basic concepts of lattice theory. Details can be found in [18].

A. System Model and Detection Methods

Consider a MIMO system consisting of n transmit antennas and m receive antennas. The relationship between the $n \times 1$ transmitted signal vector $\mathbf{x}$ and the $m \times 1$ received signal vector $\mathbf{y}$ is given by

$$\mathbf{y} = \mathbf{B}\mathbf{x} + \mathbf{n}, \tag{1}$$

where $\mathbf{B}$, $\mathbf{y}$, $\mathbf{n}$ represent the channel matrix, the received and additive noise signals, respectively. The channel matrix $\mathbf{B}$ is assumed randomly drawn from some distribution. The noise $\mathbf{n}$ is assumed to be white Gaussian noise. The signal-to-noise ratio (SNR) at the receiver is defined as

$$\mathrm{SNR} = \frac{\mathrm{E}_{\mathbf{x}\in\mathcal{A}}(\|\mathbf{B}\mathbf{x}\|_2^2)}{\mathrm{E}(\|\mathbf{n}\|_2^2)}, \tag{2}$$

where the transmitted signals $\mathbf{x}$ are assumed to be uniformly distributed in the finite set of modulation alphabet $\mathcal{A}$. For simplicity, we assume that the entries of both $\mathbf{B}$ and $\mathbf{n}$ are real. Our discussion of real case can be readily generalized to the complex case.

Given a MIMO system modeled as (1), the optimum ML decoding selects $\mathbf{x}_{ML}$ that is a solution for the following minimization problem as the transmit signal:

$$\mathbf{x}_{ML} = \arg\min_{\mathbf{x}\in\mathcal{A}} \|\mathbf{y} - \mathbf{B}\mathbf{x}\|_2. \tag{3}$$

Assume that the constellation $\mathcal{A}$ is of lattice type, such as PAM or QAM, then upon scaling and shifting the problem (3) can be transformed into an integer least squares problem. For solving such problem exactly, several algorithms such as Kannan's method [21] as well as the sphere decoding algorithms [7], [9], [10] are proposed. However, the complexity of these algorithms increase exponentially with the number of transmit antennas [7], [8], [12]. So ML decoding is not feasible for large number of transmit antennas or real-time systems where the received signal changes rapidly.

To reduce the detection cost, many sub-optimal algorithms with low-complexity have been proposed, such as ZF decoding and SIC decoding [13], [14], [40]. The performance of sub-optimal detectors is highly related to the structure of $\mathbf{B}$. It is well known that the closer to being orthogonal the column vectors of $\mathbf{B}$ are, the lower BER the sub-optimal detectors have [14], [17], [34]. Especially, ZF decoding and SIC decoding are identical to ML decoding when the columns of $\mathbf{B}$ are orthogonal. Lattice reduction can improve the orthogonality defect of $\mathbf{B}$, resulting in large performance gains.

B. Some Basic Concepts of Lattice Theory

1) Lattices and Bases: Suppose that $\mathbf{B}$ is an m-by-n, $m \geq n$, real matrix of full column rank, then the *lattice* generated by $\mathbf{B}$ is defined by the set:

$$L(\mathbf{B}) = \{\mathbf{B}\mathbf{z} \quad | \quad \mathbf{z} \in \mathbb{Z}^n\},$$

where $\mathbb{Z}^n$ denotes the set of integer n-vectors. The columns of $\mathbf{B}$ form a *basis* for the lattice $L(\mathbf{B})$, and the value of n is called the *dimension* of $L(\mathbf{B})$. When $n \geq 2$, the lattice $L(\mathbf{B})$ can have infinitely many different bases other than $\mathbf{B}$.

An integer matrix $\mathbf{Z} \in \mathbb{Z}^{n\times n}$ is called *unimodular* if $|\det(\mathbf{Z})| = 1$. In general, the columns of any matrix $\mathbf{B}'$ can form a basis for $L(\mathbf{B})$ if and only if $\mathbf{B}'$ can be factorized as $\mathbf{B}' = \mathbf{B}\mathbf{Z}$, where $\mathbf{Z}$ is a unimodular matrix. Given $\mathbf{B}$, a lattice reduction algorithm finds a unimodular matrix $\mathbf{Z}$ such that $\mathbf{B}\mathbf{Z}$ is reduced.

2) Lattice Volume and Orthogonality Defect: Let $\mathbf{B} \triangleq [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n] \in \mathbb{R}^{m\times n}$, then the *volume* of $L(\mathbf{B})$ is defined as $vol(L(\mathbf{B})) = \sqrt{\det(\mathbf{B}^{\mathrm{T}}\mathbf{B})}$. From the definition of unimodular matrix, we have $\det(\mathbf{B}^{\mathrm{T}}\mathbf{B}) = \det((\mathbf{BZ})^{\mathrm{T}}\mathbf{BZ})$ for any unimodular $\mathbf{Z} \in \mathbb{Z}^{n\times n}$. Hence the volume of a lattice is independent of the choice of basis. The *orthogonality defect* of a basis $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n\}$ for $L(\mathbf{B})$ is defined as $\delta(\mathbf{B}) = \frac{(\prod_{i=1}^{n}\|\mathbf{b}_i\|_2)}{vol(L(\mathbf{B}))}$. The concept of orthogonality defect is used to measure the degree of orthogonality for a given matrix. From Hardamard's Inequality, $\delta(\mathbf{B})$ is always larger than or equal to 1, with equality if and only if the columns of $\mathbf{B}$ are orthogonal to each other.

3) Gram-Schmidt Orthogonalization and QR Decomposition: Let $\mathbf{B} \triangleq [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ be of full column rank. Then *Gram-Schmidt orthogonalization* (GSO) $\mathbf{q}_1^*, \ldots, \mathbf{q}_n^*$ are defined as follows: for any $1 \leq j \leq n$, $\mathbf{q}_j^*$ is the component of $\mathbf{b}_j$ that is orthogonal to the subspace spanned by the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_{j-1}$. Initializing $\mathbf{q}_1^* = \mathbf{b}_1$, the vectors $\mathbf{q}_2^*, \ldots, \mathbf{q}_n^*$ can be calculated successively by

$$\mathbf{q}_j^* = \mathbf{b}_j - \sum_{i<j} u_{i,j}\mathbf{q}_i^*, \quad 1 < j \leq n, \tag{4}$$

where $u_{i,j} = \frac{\mathbf{b}_j^{\mathrm{T}}\cdot\mathbf{q}_i^*}{\|\mathbf{q}_i^*\|_2^2}$. Another orthogonalization approach is the QR decomposition, obtained by applying a sequence of orthogonal transformations such as Householder transformations [41]:

$$\mathbf{B} = \mathbf{QR}, \tag{5}$$

where $\mathbf{Q}$ consists of orthonormal columns, and $\mathbf{R}$ is an upper triangular matrix with positive diagonal. Instead of GSO, many recent lattice reduction algorithms [18], [29], [34], [35], [42], [43] adopt the QR decomposition approach, since the QR decomposition can be performed efficiently and numerically more stable than GSO.

4) Minkowski's Successive Minima and Hermite's Constant: Let L be an n-dim lattice in $\mathbb{R}^m$. For $1 \leq i \leq n$, the i-th *Minkowski's successive minima* $\lambda_i(L)$ is the radius of the smallest closed ball centered at the origin containing at least i linearly independent lattice vectors. In particular, $\lambda_1(L)$ is the Euclidean length of a shortest nonzero lattice vector of L. There always exist independent lattice vectors $\mathbf{v}_i$'s such that $\|\mathbf{v}_i\|_2 = \lambda_i(L)$ for all i. Note that for $n > 4$, such vectors do not necessarily form a basis for L. It is a classical result that $\frac{\lambda_1(L)}{vol(L)^{1/n}}$ can be upper bounded over all n-dim lattices L, and Hermite's constant γ_n is defined as the supremum of $\frac{\lambda_1(L)^2}{vol(L)^{2/n}}$ over all n-dim lattices. Finding the exact value of γ_n is a very difficult problem, which plays a central role in the theory of geometry of numbers. The exact value of γ_n is only known for $1 \leq n \leq 8$ and $n = 24$ [2, Page33]. An upper bound of Hermite's constant is given in [2, Page35]:

$$\gamma_n \leq 1 + \frac{n}{4}, \quad \text{for all } n \geq 1. \tag{6}$$

```
Input: $\mathbf{R} \in \mathbb{R}^{n\times n}$, $\mathbf{Z} \in \mathbb{Z}^{n\times n}$, and indices $i, j$
Output: $\mathbf{R}$ with $|r_{i,j}| \leq |r_{i,i}|/2$, and updated $\mathbf{Z}$.
if $|r_{i,j}| > |r_{i,i}|/2$ then
    $t \leftarrow \lfloor r_{i,j}/r_{i,i}\rceil$
    $\mathbf{R}(1:i,j) \leftarrow \mathbf{R}(1:i,j) - t\cdot\mathbf{R}(1:i,i)$
    $\mathbf{Z}(:,j) \leftarrow \mathbf{Z}(:,j) - t\cdot\mathbf{Z}(:,i)$
end if
```

Fig. 1. Procedure SIZE-REDUCE.

5) Size-Reduction and HKZ-Reduction: A lattice generator matrix $\mathbf{B} \in \mathbb{R}^{m\times n}$ is called *size-reduced* if the upper triangular factor $\mathbf{R} \triangleq [r_{i,j}]$ of its QR decomposition satisfies:

$$|r_{i,j}| \leq \frac{1}{2}|r_{i,i}|, \quad \text{for } 1 \leq i < j \leq n. \tag{7}$$

By calling the procedure in Fig. 1, the condition (7) can be enforced. A generator matrix $\mathbf{B}$ is called HKZ-reduced if it is size-reduced and its R-factor $\mathbf{R}$ satisfies: for all $1 \leq i \leq n$, $r_{i,i} = \lambda_1(L(\mathbf{R}(i:n, i:n)))$, where $L(\mathbf{R}(i:n, i:n))$ is the lattice generated by $\mathbf{R}(i:n, i:n)$. It is proved in [44] that the length of each HKZ-reduced basis vector can approximate Minkowski's successive minima within a polynomial factor:

$$\frac{4}{i+3} \leq \frac{\|\mathbf{b}_i\|_2^2}{\lambda_i^2(L)} \leq \frac{i+3}{4}, \quad 1 \leq i \leq n; \tag{8}$$

$$\prod_{i=1}^{n}\|\mathbf{b}_i\|_2 \leq \left(\gamma_n^n \prod_{i=1}^{n}\frac{i+3}{4}\right)^{\frac{1}{2}} \cdot \mathrm{vol}(L). \tag{9}$$

6) Minkowski-Reduction: A lattice generator matrix $\mathbf{B} \triangleq [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ is called Minkowski-reduced if for all $1 \leq i \leq n$, the vector $\mathbf{b}_i$ has the minimum norm among all lattice vectors $\mathbf{b}_i$ such that $\{\mathbf{b}_1, \ldots, \mathbf{b}_i\}$ can be extended to a basis for $L(\mathbf{B})$ [25]. Intuitively, Minkowski-reduction requires each basis vector as short as possible. From [45], the length of each Minkowski-reduced basis vector can be bounded by

$$\lambda_i^2(L) \leq \|\mathbf{b}_i\|_2^2 \leq \max\left\{1, \left(\frac{5}{4}\right)^{(n-4)}\right\}\lambda_i^2(L), \quad 1 \leq i \leq n; \tag{10}$$

$$\prod_{i=1}^{n}\|\mathbf{b}_i\|_2 \leq \gamma_n^{\frac{n}{2}} \cdot \mathrm{vol}(L), \text{ for } \quad n \leq 4; \tag{11}$$

$$\prod_{i=1}^{n}\|\mathbf{b}_i\|_2 \leq \gamma_n^{\frac{n}{2}} \cdot \left(\frac{5}{4}\right)^{\frac{(n-3)(n-4)}{4}} \cdot \mathrm{vol}(L), \text{ for } n > 4. \tag{12}$$

From (10), for lattices of dimension $n \leq 4$, the norms of Minkowski-reduced basis vectors simultaneously achieve Minkowski's successive minima. In high dimensions, however, there need not exist a Minkowski-reduced basis whose vector norms simultaneously reach Minkowski's successive minima.

7) LLL-Reduction: A lattice generator matrix $\mathbf{B} \in \mathbb{R}^{m\times n}$ is called LLL-reduced if it is size-reduced and its R-factor $\mathbf{R} \triangleq [r_{i,j}]$ satisfies:

$$r_{i,i}^2 + r_{i-1,i}^2 \geq \omega\, r_{i-1,i-1}^2, \quad 1 < i \leq n \tag{13}$$

where $\omega \in \left(\frac{1}{4}, 1\right)$ is a parameter which influences the quality of the reduced basis. Obviously, an HKZ-reduced basis is LLL-reduced for any $\frac{1}{4} < \omega < 1$. To justify that an LLL-reduced basis consists of vectors reasonably short, it is shown in [26] that

$$\beta^{1-i}\lambda_i^2 \le \|\mathbf{b}_i\|_2^2 \le \beta^{n-1}\lambda_i^2, \tag{14}$$

$$\prod_{i=1}^{n} \|\mathbf{b}_i\|_2 \le \beta^{\frac{n(n-1)}{4}} \cdot \mathrm{vol}(L). \tag{15}$$

where $\beta = \left(\omega - \frac{1}{4}\right)^{-1}$. Like Minkowski-reduction, the upper bound in the right hand side of (14) grows exponentially with the dimension of lattice. However, Minkowski-reduction is stronger than LLL-reduction, since the exponential factor in (10) is smaller than that of LLL-reduction for any $\frac{1}{4} < \omega < 1$.

III. A New Algorithm for Constructing HKZ-Reduced Bases

From the definition of HKZ-reduction, the key to the construction of an HKZ-reduced basis is to recursively find a shortest nonzero lattice vector in a projected lattice and then extend this vector to a basis for the lattice. In this section, we shall present a new efficient algorithm for constructing HKZ-reduced bases for general lattices.

A. Algorithms for Solving SVP

The construction of HKZ-reduced bases consists of a sequence of *shortest vector problems* (SVP) in projected lattices. As a fundamental problem in lattice theory, SVP has attracted much attention. Although this problem has been proved to be NP-hard for randomized reductions [46], there are many practical algorithms for solving it exactly, and the choice of methods depends on the structure of the lattice generator matrix. For many classical lattices, efficient search algorithms exploiting the special structure of the lattice generator matrix are known [47], [48]. For general SVP, that is, the lattice generator matrix has no exploitable structure, related algorithms can be classified in three categories: algorithms based on Kannan's strategy [21]–[24], the sphere decoding algorithms [7], [9], [10], [49], [50] and the randomized sieve algorithms [51]–[53]. The efficiencies of the three strategies were compared in [52], [54], and simulation results in [52], [53] suggest that for lattices of dimension less than 40, the sphere decoding algorithm using the SE enumeration is the most efficient algorithm.

B. A New Basis Expansion Method

As pointed out previously, the sphere decoding algorithm using the SE enumeration is currently the most efficient method for solving general SVP with small dimensions. Therefore, to calculate an HKZ-reduced basis efficiently, it is natural to combine SE enumeration and Kannan's basis expansion method [21]. Indeed, this is the method presented in [7]. Like the algorithm in [7], we also adopt the SE enumeration to solve SVP. However, instead of Kannan's basis expansion method, we use a novel unimodular transformation basis expansion method.

Firstly, we briefly analyze the complexity of Kannan's basis expansion method [23]. The algorithm recursively selects basis vectors. In the kth, $1 \le k \le n$, recursion, it first solves two $(n-k+1)$-dim systems of linear equations to determine linear dependency (require $O\left((n-k)^3\right)$ operations), and performs a Gram-Schmidt like procedure involving $n-k+1$ vectors to obtain a projected lattice of dimension $n-k$, then selects a basis for the resulted lattice followed by lifting the $n-k$ basis vectors (require $O\left((n-k)^2\right)$ operations). Thus, the complexity of Kannan's basis expansion method is at least $O(n^4)(O(\sum_{k=1}^{n}(n-k)^3))$. On the other hand, numerical results in [52] show that for lattice of relative small dimensions, the SE enumeration can be very practical. Hence, from a practical point of view, the computational cost required by Kannan's basis expansion method is not negligible. Moreover, note that Kannan's basis expansion method only works for rational lattices, not general real-valued lattices.

Secondly, based on the unimodular transformation presented in [38], we propose a new basis expansion method, which is applicable to lattices of any type, provided that the coordinates of a shortest nonzero lattice point is available. Specifically, let $\mathbf{B} \in \mathbb{R}^{m\times n}$ be a generator matrix for an n-dim lattice L. Suppose that $\mathbf{Bz}$ is a shortest nonzero point in L, where $\mathbf{z} = [z_i] \in \mathbb{Z}^n$. Then the problem of expanding $\mathbf{Bz}$ to a basis for L is equivalent to the problem of constructing an n-by-n unimodular matrix $\mathbf{Z}$ whose first column is $\mathbf{z}$. In other words, $\mathbf{Z}^{-1}\mathbf{z} = \mathbf{e}_1$, which says that $\mathbf{Z}^{-1}$, also unimodular, transforms $\mathbf{z}$ into the first unit vector $\mathbf{e}_1$.

For the special case when $n = 2$, such a unimodular matrix is easy to construct. Suppose that $\mathbf{z} = [p, q]^{\mathrm{T}} \in \mathbb{Z}^2$, and let $\gcd(p, q) = d$. Using the extended Euclidean algorithm, one can find integers a and b such that $ap + bq = d$. Construct

$$\mathbf{U} = \begin{bmatrix} \frac{p}{d} & -b \\ \frac{q}{d} & a \end{bmatrix}. \tag{16}$$

It is obvious that $\mathbf{U}$ is a unimodular matrix with

$$\mathbf{U}^{-1} = \begin{bmatrix} a & b \\ \frac{-q}{d} & \frac{p}{d} \end{bmatrix}, \quad \mathbf{U}^{-1}\begin{bmatrix} p \\ q \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}. \tag{17}$$

Thus, $\mathbf{U}^{-1}$ can be applied to $\mathbf{z}$ to annihilate its second entry. In particular, if $\gcd(p, q) = \pm 1$, then $\mathbf{z}$ can be transformed into the first unit vector.

Now we consider the general case when $n > 2$. Since $\mathbf{Bz}$ is a shortest nonzero lattice point, we have $\gcd(z_i) = \pm 1$. Thus, $\mathbf{z}$ can be transformed into the first unit vector by applying a sequence of the plane unimodular transformations $\mathbf{U}$ of the form (16) to annihilate the last $n-1$ entries of $\mathbf{z}$, for example, bottom up. Putting all things together, we present our new algorithm for constructing an HKZ reduced basis in Fig. 2, where basis expansion is performed by Procedure Transform in Fig. 3.

Now we analyze the complexity of Procedure Transform. For each iteration of the for-loop, the computations from line 5 to line 8 require $O(n)$ fp operations. Then we consider the cost of line 2. Given two integers p and q, it is shown in [55] that the complexity of Euclidean algorithm is $O(\log g)$, where $g = \min\{|p|, |q|\}$. Thus, the cost of the gcd computation called in the first iteration of the for-loop can be obtained if an upper bound of $|z_{n-k+1}|$ is found. Suppose now that $\mathbf{R}(k:n, k:n)$ is LLL-reduced with a parameter $\omega = \frac{3}{4}$. It follows from [26] that $r_{k,k}^2 \le 2^{n-k} r_{n,n}^2$, which implies that in the k-th iteration of Algorithm HKZ-Red, the initial radius of the SE enumeration called in line

```
Input: $\mathbf{B} \in \mathbb{R}^{m\times n}$, and the LLL parameter $\omega$, $1/4 < \omega < 1$
Output: a unimodular matrix $\mathbf{Z} \in \mathbb{Z}^{n\times n}$ such that the columns of
    $\mathbf{BZ}$ form an HKZ-reduced basis
1: QR decomposition: $\mathbf{B} = \mathbf{QR}$
2: $\mathbf{Z} \leftarrow \mathbf{I}_n$
3: for $k = 1$ to $n-1$ do
4:     use LLL-aided SE enumeration to find a vector $\mathbf{z} \in \mathbb{Z}^{n-k+1}$
       such that $\mathbf{R}(k:n, k:n)\mathbf{z}$ is a shortest nonzero point in the
       lattice generated by $\mathbf{R}(k:n, k:n)$
5:     $[\mathbf{R}, \mathbf{Z}] \leftarrow$ TRANSFORM($\mathbf{R}$, $\mathbf{Z}$, $\mathbf{z}$, $k$)
6: end for
7: size reduce $\mathbf{R}$
```

Fig. 2. Algorithm HKZ-RED.

```
Input: an upper triangular $\mathbf{R} \in \mathbb{R}^{n\times n}$, a unimodular $\mathbf{Z} \in \mathbb{Z}^{n\times n}$,
    $\mathbf{z} \in \mathbb{Z}^{n-k+1}$, and the index $k$
Output: the updated $\mathbf{R} = [r_{i,j}]$ with $r_{k,k} = \|\mathbf{R}(k:n, k:n)\mathbf{z}\|_2$,
    and the updated $\mathbf{Z} \in \mathbb{Z}^{n\times n}$
1: for $j = n-k+1$ down to 2 do
2:     $d \leftarrow \gcd(z_{j-1}, z_j)$, and find integers $a$ and $b$ such that
       $az_{j-1} + bz_j = d$
3:     $\mathbf{U} \leftarrow \begin{bmatrix} z_{j-1}/d & -b \\ z_j/d & a \end{bmatrix}$
4:     $z_{j-1} \leftarrow d$
5:     $\mathbf{R}(1:j+k-1, j+k-2:j+k-1) \leftarrow \mathbf{R}(1:j+k-$
       $1, j+k-2:j+k-1) \cdot \mathbf{U}$
6:     $\mathbf{Z}(:, j+k-2:j+k-1) \leftarrow \mathbf{Z}(:, j+k-2:j+k-1) \cdot \mathbf{U}$
7:     find a Givens rotation $\mathbf{G}$ such that
           $\mathbf{G} \cdot \begin{bmatrix} r_{j+k-2,j+k-2} \\ r_{j+k-1,j+k-2} \end{bmatrix} = \begin{bmatrix} \times \\ 0 \end{bmatrix}$
8:     $\mathbf{R}(j+k-2:j+k-1, j+k-2:n) \leftarrow \mathbf{G} \cdot \mathbf{R}(j+k-2:$
       $j+k-1, j+k-2:n)$
9: end for
```

Fig. 3. Procedure TRANSFORM.

4 of Algorithm HKZ-RED is bounded by $2^{\frac{(n-k)}{2}} r_{n,n}$. Consequently, we have $|z_{n-k+1}| \leq 2^{\frac{(n-k)}{2}}$. Thus, the gcd computation called in the first iteration of Procedure TRANSFORM requires a complexity of $O(n-k)$ operations. After the first iteration, z_{n-k} is updated as $d = \gcd(z_{n-k}, z_{n-k+1})$. It is easy to verify that the complexity of the gcd computation called in the second iteration is also upper bounded by $O(n-k)$, since the updated $z_{n-k} = d \leq 2^{\frac{(n-k)}{2}}$. By induction, the complexity of each gcd computation called in the following iterations is $O(n-k)$. Therefore, the total cost of Procedure TRANSFORM is of $O(n(n-k))$ operations. In particular, when the size of $\mathbf{z}$ is n, the complexity is $O(n^2)$. Hence, Procedure TRANSFORM is much more efficient than Kannan's basis expansion method, whose complexity is at least $O(n^4)$.

C. Complexity Analysis

In this subsection, we derive an upper bound for the expected asymptotic complexity of Algorithm HKZ-RED, where the expectation is taken over matrices with its elements being i.i.d. Gaussian random variables $N(0,1)$. From the analysis in Section III-B, the overall complexity of the algorithm shall be dominated by the SE enumeration as the dimension n increases, since the complexity of other parts of the algorithm are polynomial. In the following, we analyze the complexity of the SE enumeration. In [8], the search process of sphere decoding is modeled as a tree with depth n. Specifically, suppose that the initial radius is d, then it can be seen from [8] that the expected number of lattice points visited by the sphere decoding in the kth $(1 \leq k \leq n)$ level of the tree is proportional to the volume of the k-dimensional sphere of radius d, which is given by

$$V(k,d) = \frac{\pi^{\frac{k}{2}}}{\Gamma(\frac{k}{2}+1)} d^k, \tag{18}$$

where

$$\Gamma\left(\frac{k}{2}+1\right) = \begin{cases} \left(\frac{k}{2}\right)!, & \text{if } k \text{ is an even number;} \\ \frac{(k+1)! \cdot \sqrt{\pi}}{\left(\frac{k+1}{2}\right)! \cdot 2^{k+1}}, & \text{if } k \text{ is an odd number.} \end{cases} \tag{19}$$

Thus, the expected complexity of the SE enumeration is given by

$$\sum_{k=1}^{n} V(k,d) \cdot (2k+7), \tag{20}$$

where the coefficient $2k+7$ is the number of elementary operations (additions/subtractions/multiplications) that the SE enumeration performs per each visited points in dimension k. Therefore, the complexity of Algorithm HKZ-RED can be estimated if the upper bound for the initial radius of the SE enumeration, which is called in each for-loop of Fig. 2, can be found.

Suppose that $\mathbf{B} \triangleq [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{R}^{m\times n}$ is a Gaussian matrix, then it is obvious that the expectation of the Euclidean length of $\mathbf{b}_k,\ 1 \leq k \leq n$, satisfies

$$E(\|\mathbf{b}_k\|_2^2) = m.$$

It then follows that $E(\lambda_n^2(L(\mathbf{B}))) \leq m$. On the other hand, let $\mathbf{H}$ be an HKZ-reduced basis of $L(\mathbf{B})$, and let $\mathbf{R} \triangleq [r_{i,j}]$ be the upper triangular factor of $\mathbf{H}$, then it can be seen from [44] that $r_{k,k}^2 \leq \lambda_k^2(L(\mathbf{B}))$ for $1 \leq k \leq n$, thus

$$E(r_{k,k}^2) \leq E(\lambda_k^2(L(\mathbf{B}))) \leq m, \quad 1 \leq k \leq n,$$

which implies that the initial radius of the SE enumeration called in each iteration of Algorithm HKZ-RED can be upper bounded by $\sqrt{m}$. Thus, the expected asymptotic complexity of this algorithm is given by

$$C(m,n) = \sum_{j=1}^{n} \sum_{k=1}^{j} V(k, \sqrt{m}) \cdot (2k+7). \tag{21}$$

To obtain a more explicit expression of $C(m,n)$, we recall Stirling's formula [56]:

$$\lim_{n \longrightarrow \infty} \frac{n!}{\sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n} = 1. \tag{22}$$

Combining (18), (19), (21), and (22), it is not difficult to derive that

$$C(m,n) = \left(\frac{2\pi e m}{n}\right)^{\frac{n}{2} + O(\log n)}. \tag{23}$$

Thus, the expected complexity of Algorithm HKZ-RED is exponential with the lattice dimension n, provided that m is of the same order of magnitude as n.

From (23), Algorithm HKZ-RED is expected to be much more time-consuming than the LLL algorithm, whose average complexity is $O(mn^3 \log n)$[16]. Therefore, the proposed new algorithm is not feasible for fast fading case where the channel matrix changes rapidly. However, this algorithm is still promising for the general case where the channel matrix keeps constant during a frame of data, since the cost of lattice reduction can be shared by the decoding algorithms [7], [17].

IV. CONSTRUCTIONS OF MINKOWSKI-REDUCED BASES: I

Among all reduction notions, Minkowski-reduction is perhaps the most intuitive and strongest one, and up to dimension four, Minkowski-reduction is better than any other known reduction, because it can exactly reach Minkowski's successive minima.

A. Existing Algorithms

In 1773, Lagrange [57] presented the first algorithm for constructing Minkowski-reduced bases for lattices of dimension two. Recently, this algorithm was extended to dimensions three and four by Semaev [58] and Nguyen and Stehlé [59], respectively. More generally, Helfrich [22] and Afflerbach and Grothe [39] presented algorithms for constructing Minkowski-reduced bases for lattices of arbitrary dimension.

Given an n-dim lattice L, suppose that $\mathbf{B}^{(p)}$ is a generator matrix of L such that the first $p-1$ columns of $\mathbf{B}^{(p)}$ can be extended to a Minkowski-reduced basis for L. Then it follows from [22], [39] that the p-th Minkowski-reduced basis vector $\mathbf{m}_p$, which can be extended to a Minkowski-reduced basis with the first $p-1$ columns of $\mathbf{B}^{(p)}$, must satisfy

$$\|\mathbf{m}_p\|_2 = \min\{\|\mathbf{B}^{(p)}\mathbf{z}\|_2 : \mathbf{z} \in \mathbb{Z}^n,\ \gcd(z_p, \ldots, z_n) = 1\}. \quad (24)$$

Obviously, the minimization problem (24) can be viewed as an SVP with the constraint $\gcd(z_p, \ldots, z_n) = 1$. Therefore, (24) can be solved by incorporating such gcd constraint into the SVP solvers introduced in Section III-A. Effort in this direction was firstly taken by Helfrich [22]. Briefly speaking, a variant of Kannan's strategy [21] was proposed in [22] to solve (24). Unfortunately, this variant is more complicated and time-consuming than the original Kannan's strategy, since it associates with solving roughly $\left(\frac{5}{4}\right)^{\frac{n^3}{(4-o(1))}}$ $(p-1)$-dim CVPs. Hence, like Kannan's algorithm [21], [23], Helfrich's algorithm is also intended as a theoretical result rather than a practical tool.

The algorithm presented in [39] constructs a Minkowski-reduced basis in a quite different way. Starting from $p = 1$, this algorithm first performs Phost enumeration [10], [49], and during the search process, whenever an intermediate lattice point $\mathbf{B}^{(p)}\mathbf{z}$ inside the search region satisfying $\gcd(z_p, \ldots, z_n) = 1 (n > 7)$ or $z_p = 1 (n \leq 7)$ is found, the p-th column of $\mathbf{B}^{(p)}$ is then replaced by $\mathbf{B}^{(p)}\mathbf{z}$ and the algorithm is restarted from $p = 1$. On the other hand, if the p-th column of $\mathbf{B}^{(p)}$ is already the shortest lattice point satisfying the corresponding gcd constraint, we set $p = p + 1$ and repeat the above process. The algorithm terminates when $p = n + 1$. Note that the number of lattice points enumerated by Phost's strategy grows exponentially with the dimension n. Therefore, in practice the algorithm in [39] is restarted many times, and the complexity quickly becomes prohibitive as the dimension increases.

```
Input: $\mathbf{R} \in \mathbb{R}^{n \times n}$, the LLL parameter $\omega$, and an index $p$, $1 \leq p \leq n$
Output: a vector $\mathbf{z} \in \mathbb{Z}^n$ such that $\mathbf{Rz}$ is a shortest lattice point
    with $\gcd(z_p, \cdots, z_n) = 1$
1: if $n = 1$ then
2:     return $\mathbf{z} = 1$
3: else
4:     set the initial size $r \leftarrow \|\mathbf{R}(:, p)\|_2^2$
5:     apply LLL reduction to $\mathbf{R}$ to obtain an LLL-reduced matrix
       $\mathbf{R}_{new}$ and the corresponding unimodular $\mathbf{Z}$
6:     $[\mathbf{z}, l] \leftarrow$M-SEARCH-1($\mathbf{R}_{new}$, $\mathbf{Z}$, $\mathbf{0}^n$, $\phi$, $r$, 0, $p$)
7: end if
```

Fig. 4. Procedure M-DECODE-1.

B. A New Algorithm

In this subsection, we shall present a practical algorithm for constructing Minkowski-reduced bases for general lattices. Differing from the algorithm in [39], the proposed new algorithm is based on the SE enumeration.

Apparently, the first Minkowski-reduced basis vector $\mathbf{m}_1$ is a shortest nonzero lattice vector in L, which can be obtained by applying SE enumeration [7], [9]. We can extend $\mathbf{m}_1$ to a basis for L by calling Procedure TRANSFORM. Now, suppose that a basis $\{\mathbf{m}_1, \ldots, \mathbf{m}_{p-1}, \mathbf{b}_p, \ldots, \mathbf{b}_n\}$, $1 < p \leq n$, has been obtained, to extend $\{\mathbf{m}_1, \ldots, \mathbf{m}_{p-1}\}$ to an Minkowski-reduced basis for L, we have to solve the following two problems:

- Constructing the p-th Minkowski-reduced basis vector $\mathbf{m}_p$.
- Extending $\{\mathbf{m}_1, \ldots, \mathbf{m}_p\}$ to a basis for L.

From (24), $\mathbf{m}_p$ can be obtained by incorporating the constraint $\gcd(z_p, \ldots, z_n) = 1$ into SE enumeration. Instead of the Euclidean norm of the first column of the basis matrix, we use the Euclidean length of the p-th column as the initial size of search region, so that at least one lattice point satisfying such gcd constraint lies inside the search region. To further accelerate the search process, LLL algorithm can be applied as a preprocessor. Putting all things together, we present the algorithm for calculating $\mathbf{m}_p$ in Fig. 4.

As shown in Fig. 4, Procedure M-DECODE-1 is a wrapper function. It calls procedure M-SEARCH-1, which finds a solution for a more general problem: an SVP with the constraint $\gcd(z_p, \ldots, z_n) = 1$. Thus M-SEARCH-1 is a modified SE enumeration. Specifically, M-SEARCH-1 applies the SE enumeration on the LLL-reduced matrix $\mathbf{R}_{new}$ obtained in line 5. During the search process, whenever a shorter lattice point with coordinate $\mathbf{z}'$ is found, it then tests the constraint $\gcd(z_p, \ldots, z_n) = 1$ on $\mathbf{z} = \mathbf{Zz}'$. If the gcd constraint is satisfied, it then adjusts the search radius as $\|\mathbf{R}_{new}\mathbf{z}'\|_2$ and save $\mathbf{z}$ as a candidate, or it will drop $\mathbf{z}'$ and continue the SE enumeration without adjusting the search radius. Due to the additional gcd constraint, the search space of Procedure M-SEARCH-1 is expected to be larger than that of the original SE enumeration. A MATLAB implementation of M-SEARCH-1 can be found in [54].

Once the p-th Minkowski-reduced basis vector $\mathbf{m}_p = \mathbf{B}^{(p)}\mathbf{z}$ is found, the second problem is to extend $\{\mathbf{m}_1, \ldots, \mathbf{m}_p\}$ to a basis for L. In terms of matrices, it is to find a unimodular matrix $\mathbf{Z}$ such that

$$\mathbf{B}^{(p+1)} = \mathbf{B}^{(p)}\mathbf{Z}, \quad (25)$$

```
Input: $\mathbf{B} \in \mathbb{R}^{m\times n}$, and the LLL parameter $\omega$, $1/4 < \omega < 1$
Output: a unimodular $\mathbf{Z} \in \mathbb{Z}^{n\times n}$ such that the columns of $\mathbf{BZ}$ form
    a Minkowski-reduced basis
QR decomposition: $\mathbf{B} = \mathbf{QR}$
$\mathbf{Z} \leftarrow \mathbf{I}_n$
for $k = 1$ to $n$ do
    $\mathbf{z} \leftarrow$M-DECODE-1($\mathbf{R}$, $\omega$, $k$)
    $[\mathbf{R}, \mathbf{Z}] \leftarrow$ TRANSFORM($\mathbf{R}$, $\mathbf{Z}$, $\mathbf{z}$, $k$)
    $\mathbf{R}(1:k-1,k) \leftarrow \mathbf{R}(1:k-1,k) + \mathbf{R}(1:k-1,1:k-1)\cdot[z_1,\cdots,z_{k-1}]^{\mathrm{T}}$
    $\mathbf{Z}(:,k) \leftarrow \mathbf{Z}(:,k) + \mathbf{Z}(:,1:k-1)\cdot[z_1,\cdots,z_{k-1}]^{\mathrm{T}}$
end for
```

Fig. 5. Algorithm M-RED-1.

which implies that the first $p-1$ columns of $\mathbf{Z}$ are the first $p-1$ unit vectors $\mathbf{e}_i, i = 1,\ldots,p-1$, and the p-th column of $\mathbf{Z}$ is the integer vector $\mathbf{z}$ found by Procedure M-DECODE-1, so that the first $p-1$ columns of $\mathbf{B}^{(p+1)}$ equal the first $p-1$ columns $\mathbf{m}_1,\ldots,\mathbf{m}_{p-1}$ of $\mathbf{B}^{(p)}$ and the p-th column of $\mathbf{B}^{(p+1)}$ is $\mathbf{m}_p = \mathbf{B}^{(p)}\mathbf{z}$ as desired. Since $\gcd(z_p,\ldots,z_n) = 1$, from the discussion in Section III, one can construct an $(n-p+1)\times(n-p+1)$ unimodular matrix $\mathbf{U}$ whose first column is $[z_p,\ldots,z_n]^{\mathrm{T}}$. Now consider the two $n\times n$ unimodular matrices

$$\mathbf{Z}_1 = \begin{bmatrix} \mathbf{I}_{p-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{U} \end{bmatrix},\ \mathbf{Z}_2 = \begin{bmatrix} & z_1 & & \\ \mathbf{I}_{p-1} & \vdots & & \mathbf{0} \\ & z_{p-1} & & \\ & 1 & & \\ & & \ddots & \\ \mathbf{0} & & & 1 \end{bmatrix}. \tag{26}$$

We claim that the product $\mathbf{Z}_1\mathbf{Z}_2$ is a unimodular matrix satisfying (25). Indeed, $\mathbf{Z}_1\mathbf{Z}_2$ is unimodular since both $\mathbf{Z}_1$ and $\mathbf{Z}_2$ are unimodular. From (26), the first $p-1$ columns of $\mathbf{Z}_1\mathbf{Z}_2$ are the first $p-1$ unit vectors and the p-th column of $\mathbf{Z}_1\mathbf{Z}_2$ is $\mathbf{z} = [z_1,\ldots,z_n]^{\mathrm{T}}$.

The application of $\mathbf{Z}_1$ can be performed by Procedure TRANSFORM and the application of $\mathbf{Z}_2$ is the calculation of a linear combination of the first p columns. Putting all things together, the new algorithm for constructing Minkowski-reduced bases for general lattices is presented in Fig. 5.

C. Complexity Analysis

In this subsection, we shall analyze the expected asymptotic complexity of Algorithm M-RED-1. Also, the expectation is taken over matrices with its elements being i.i.d. Gaussian random variables $N(0,1)$. Like Algorithm HKZ-RED, the overall complexity of M-RED-1 shall be dominated by Procedure M-DECODE-1 as the dimension n increases, since the complexity of other parts of the algorithm are polynomial. From the analysis in Section IV-B, the computation of M-DECODE-1 mainly includes two parts: the modified SE enumeration and the gcd conditions checking. Following [8] and the analysis presented in Section III-C, it is not difficult to see that the complexity of the modified SE enumeration is bounded above by (20). Therefore, an upper bound for the initial radius of the modified SE enumeration, which is called in each for-loop of M-RED-1, is required.

Suppose that $\mathbf{B} \in \mathbb{R}^{m\times n}$ is a Gaussian matrix, and let $\mathbf{M} \triangleq [\mathbf{m}_1,\ldots,\mathbf{m}_n]$ be a Minkowski-reduced basis for $L(\mathbf{B})$. Then from (10),

$$\|\mathbf{m}_k\|_2^2 \le \max\left\{1, \left(\frac{5}{4}\right)^{(n-4)}\right\}\lambda_k^2(L(\mathbf{B})), \quad 1 \le k \le n. \tag{27}$$

Thus, for $1 \le k \le n$, we have

$$\begin{aligned} \mathrm{E}(\|\mathbf{m}_k\|^2) &\le \max\left\{1 \left(\frac{5}{4}\right)^{(n-4)}\right\}\mathrm{E}(\lambda_k^2(L(\mathbf{B}))) \\ &\le \max\left\{m, \left(\frac{5}{4}\right)^{(n-4)} m\right\}, \end{aligned} \tag{28}$$

which implies that the initial radius of the modified SE enumeration called in each iteration of Algorithm M-RED-1 is bounded above by

$$\max\left\{\sqrt{m}, \left(\frac{5}{4}\right)^{\frac{(n-4)}{2}}\sqrt{m}\right\}. \tag{29}$$

Combining (20) and (29), the overall complexity of the enumeration part of M-RED-1 is given by

$$n \times \sum_{k=1}^{n} V\left(k, \max\left\{\sqrt{m}, \left(\frac{5}{4}\right)^{\frac{(n-4)}{2}}\sqrt{m}\right\}\right)\cdot(2k+7). \tag{30}$$

Now, we consider the complexity of the gcd conditions checking part. It is easy to verify that during the process of each SE enumeration, the number of lattice points for which the gcd conditions are checked is proportional to the volume of the n-dim sphere of radius (29). On the other hand, from the analysis in Section III-B, the elementary operations performed by the gcd condition checking per lattice point is $O(n^2)$. Thus, the overall complexity of the gcd conditions checking part is

$$n \times V\left(n, \max\left\{\sqrt{m}, \left(\frac{5}{4}\right)^{\frac{(n-4)}{2}}\sqrt{m}\right\}\right) \times O(n^2) \tag{31}$$

Combining (30) and (31), the expected asymptotic complexity of Algorithm M-RED-1 is given by

$$\begin{aligned} C(m,n) &= V\left(n, \max\left\{\sqrt{m}, \left(\frac{5}{4}\right)^{\frac{(n-4)}{2}}\sqrt{m}\right\}\right) \times O(n^3) \\ &= \left(\frac{5}{4}\right)^{\frac{n^2}{2}+O\left(n\log\frac{m}{n}\right)}. \end{aligned} \tag{32}$$

Comparing (23) and (32), Algorithm M-RED-1 is expected to be much more time-consuming than Algorithm HKZ-RED, and this shall be confirmed by the simulation results presented in Section VII.

V. CONSTRUCTIONS OF MINKOWSKI-REDUCED BASES: II

From the discussion in Section IV, the search space of procedure M-SEARCH-1 is larger than that of the original SE enumeration. This motivates us to design a more efficient way to calculate each Minkowski-reduced basis vector. Our idea is to impose the constraint as early as possible to reduce the number of points to be searched. Clearly, $\gcd(z_p, \ldots, z_n)$ can be calculated as soon as $z_p, \ldots, z_n$ are available. Note that during the process of SE enumeration, a solution is built bottom-up, from z_n to z_1, thus the gcd condition can be checked at level p, instead of level 1 as in M-SEARCH-1. We call this procedure M-SEARCH-2. A MATLAB implementation can be found in [54]. Since in M-SEARCH-2, the $(p-1)$-dim subproblems indexed by those $\mathbf{z}$ not satisfying $\gcd(z_p, \ldots, z_n) = 1$ are excluded from the search process, the search space of M-SEARCH-2 is expected to be drastically reduced from the original SE enumeration.

However, one drawback of procedure M-SEARCH-2 is: LLL algorithm cannot be used as its preprocessor to accelerate the search process. Specifically, if LLL algorithm were applied, the unimodular matrix obtained from LLL algorithm would have to be applied to the solution vector before checking the gcd condition. Unfortunately, the application of the unimodular matrix requires a complete n-vector, whereas at level p, where $\gcd(z_p, \ldots, z_n)$ is calculated in procedure M-SEARCH-2, only a subvector $\mathbf{z}(p:n)$ is available. To alleviate the problem, we propose a new lattice reduction technique to accelerate M-SEARCH-2.

Consider an $n \times n$ unimodular matrix $\mathbf{Z}$ with the following structure:

$$\mathbf{Z} = \begin{bmatrix} \mathbf{D} & \mathbf{E} \\ \mathbf{0}^{(n-p+1)\times(p-1)} & \mathbf{F} \end{bmatrix}, \tag{33}$$

where $\mathbf{D}$, $\mathbf{E}$, and $\mathbf{F}$ have proper dimensions. Then both $\mathbf{D}$ and $\mathbf{F}$ are unimodular. If an integer vector $\hat{\mathbf{z}}$ satisfies $\gcd(\hat{\mathbf{z}}(p), \ldots, \hat{\mathbf{z}}(n)) = 1$, then the integer vector $\mathbf{z} = \mathbf{Z}\hat{\mathbf{z}}$ also satisfies the condition $\gcd(\mathbf{z}(p), \ldots, \mathbf{z}(n)) = 1$, since $\mathbf{z}(p:n) = \mathbf{F}\hat{\mathbf{z}}(p:n)$ and $\mathbf{F}$ is unimodular. Thus, if an appropriate unimodular matrix $\mathbf{Z}$ with the form (33) is chosen as a preprocessor for M-SEARCH-2, the information of the subvector $\hat{\mathbf{z}}(p:n)$ obtained at level p is sufficient to check the gcd condition of the solution $\mathbf{z} = \mathbf{Z}\hat{\mathbf{z}}$.

Suppose now that the first $p-1$ columns $\mathbf{m}_1, \ldots, \mathbf{m}_{p-1}$ of the current basis matrix $\mathbf{B}^{(p)}$ can be extended to a Minkowski-reduced basis. Let $\mathbf{R}$ be the R-factor of $\mathbf{B}^{(p)}$. Then it is obvious that the first $p-1$ columns of $\mathbf{R}$ is Minkowski-reduced. Thus the submatrix $\mathbf{D}$ in (33) can be chosen as $\mathbf{I}_{p-1}$. In other words, we only need to reduce the submatrix of $\mathbf{R}$ consisting of its last $n-p+1$ columns. A natural approach is to use the partial reduction technique [60]. That is, we select the submatrices $\mathbf{E}$ and $\mathbf{F}$ appropriately such that after preprocessing, $\mathbf{R}(p:n, p:n)$ is LLL-reduced and all off-diagonal entries of $\mathbf{R}$ belonging to the last $n-p+1$ columns are size-reduced. Fig. 6 shows an implementation of this idea.

Combining Procedure PARTIAL-LR and Procedure M-SEARCH-2, we present the algorithm for calculating $\mathbf{m}_p$ in Fig. 7. Finally, the second algorithm M-RED-2 for constructing a Minkowski-reduced basis can be obtained by simply replacing Procedure M-DECODE-1 in Algorithm M-RED-1 with Procedure M-DECODE-2.

For the complexity of Algorithm M-RED-2, we shall not go to detailed discussions. Following the analysis presented in Section IV-C, it is not difficult to prove that the complexity of M-RED-2 is also upper bounded by (32).

```
Input: $\mathbf{R} \in \mathbb{R}^{n\times n}$, the LLL parameter $\omega$, and an index $p$, $1 \le p \le n$
Output: the updated $\mathbf{R}$ and a unimodular matrix $\mathbf{Z}$ such that the
    last $n-p+1$ columns of $\mathbf{R}$ are reduced
$\mathbf{Z} \leftarrow \mathbf{I}_n$
$k \leftarrow p+1$
while $k \le n$ do
    $[\mathbf{R}, \mathbf{Z}] \leftarrow$ SIZE-REDUCE ($\mathbf{R}$, $\mathbf{Z}$, $k-1$, $k$)
    if $r_{k-1,k}^2 + r_{k,k}^2 \le \omega \cdot r_{k-1,k-1}^2$ then
        swap columns $k-1$ and $k$ in $\mathbf{R}$ and $\mathbf{Z}$
        find a Givens rotation to restore the upper triangular structure of $\mathbf{R}$
        $k \leftarrow \max\{k-1, p+1\}$
    else
        $k \leftarrow k+1$
    end if
end while
for $j = p$ to $n$ do
    for $i = j-1$ down to $1$ do
        $[\mathbf{R}, \mathbf{Z}] \leftarrow$ SIZE-REDUCE ($\mathbf{R}$, $\mathbf{Z}$, $i$, $j$)
    end for
end for
```

Fig. 6. Procedure PARTIAL-LR[60].

```
Input: $\mathbf{R} \in \mathbb{R}^{n\times n}$, the LLL parameter $\omega$, and an index $p$, $1 \le p \le n$
Output: a vector $\mathbf{z} \in \mathbb{Z}^n$ such that $\mathbf{Rz}$ is a shortest lattice point
    with $\gcd(z_p, \cdots, z_n) = 1$
if $n = 1$ then
    return $\mathbf{z} = 1$
else
    $[\mathbf{R}_{new}, \mathbf{Z}] \leftarrow$PARTIAL-LR($\mathbf{R}$, $\omega$, $p$)
    set the initial size $r \leftarrow \|\mathbf{R}_{new}(:,p)\|_2^2$
    $[\mathbf{z}', l] \leftarrow$M-SEARCH-2($\mathbf{R}_{new}$, $\mathbf{0}^n$, $\phi$, $r$, $0$, $p$)
    $\mathbf{z} \leftarrow \mathbf{Zz}'$
end if
```

Fig. 7. Procedure M-DECODE-2.

VI. PERFORMANCE ANALYSIS

In this section, we firstly compare the theoretical upper bounds on the orthogonality defect of LLL, HKZ, and Minkowski-reduced bases. Then after presenting existing results on the proximity factors of sub-optimal lattice decoding [15]–[17], we give new improved upper bounds for the proximity factors of LLL-reduction-aided SIC decoding and LLL-reduction-aided ZF decoding. Also, we derive upper bounds for the proximity factors of both Minkowski-reduction-aided SIC decoding and Minkowski-reduction-aided ZF decoding. Thus, like LLL-reduction and HKZ-reduction, sub-optimal decoding algorithms aided by Minkowski-reduction can also achieve the same diversity order with ILD.

A. Orthogonality Defect

As pointed out previously, the orthogonality defect is a commonly used indicator to reveal the degree of orthogonality for a given lattice basis. Denote $\delta_{H,n}$, $\delta_{L,n}$, and $\delta_{M,n}$ the upper bounds of the orthogonality defect over all $n \times n$ HKZ, LLL (with $w = \frac{3}{4}$) and Minkowski-reduced bases, respectively. Then from (9), (15), (12) and (6), one can immediately obtain

$$\delta_{H,n} \le \gamma_n^{\frac{n}{2}} \left(\prod_{i=1}^{n} \frac{i+3}{4} \right)^{\frac{1}{2}} = 2^{O(n \log n)}; \tag{34}$$

$$\delta_{L,n} \le 2^{\frac{n(n-1)}{4}}; \tag{35}$$

$$\delta_{M,n} \le \gamma_n^{\frac{n}{2}} \left(\frac{5}{4} \right)^{\frac{(n-3)(n-4)}{4}} = \left(\frac{5}{4} \right)^{\frac{n^2}{4} + O(n \log n)}. \tag{36}$$

TABLE I
UPPER BOUNDS OF ORTHOGONALITY DEFECT OF HKZ, LLL $\left(\omega = \frac{3}{4}\right)$, AND MINKOWSKI-REDUCED BASES.

n	2	3	4	5	6	7	8	24
γ_n	$2/\sqrt{3}$	$2^{1/3}$	$\sqrt{2}$	$8^{1/5}$	$(64/3)^{1/6}$	$64^{1/7}$	2	4
$\delta_{H,n}$	1.291	1.937	3.623	7.246	17.75	48.61	161.2	4.26×10^{13}
$\delta_{L,n}$	1.414	2.828	8	32	181.0	1.45×10^{3}	1.64×10^{4}	3.48×10^{41}
$\delta_{M,n}$	1.155	1.414	2	3.162	6.455	15.63	48.83	2.51×10^{17}

Thus, in the worst case, the HKZ-reduced basis is expected to be more orthogonal than LLL or Minkowski-reduced basis for lattices of high dimension. Note that the values of γ_n are known for $1 \leq n \leq 8$ and $n = 24$[2, Page33]. Thus for lattices of these dimensions, relatively tight upper bounds on the orthogonality defect can be calculated. From Table I, one can see that for lattices of dimension $n \leq 8$, the upper bound of the orthogonality defect of Minkowski-reduced bases is slightly smaller than that of HKZ-reduced bases, and the LLL-reduction has the worst performance, especially for $n = 7$ and $n = 8$. However, for lattices of a little higher dimensions such as $n = 24$, the upper bound associated with the HKZ-reduced performs better than the Minkowski-reduction, and the gap between HKZ-reduction and LLL-reduction gets larger quickly as dimension increases. Note that the upper bounds given in this subsection only represent the theoretical results in the worst case. The average orthogonality defect of these reduction notions in simulations shall be shown in Section VII.

B. Proximity Factors and Error Probability

The commonly used SIC decoding and ZF decoding were proposed by Babai [13] in 1986. Both theoretical results [36], [37] and computer simulation [14], [34], [35] show that LLL-reduction-aided decoding can always achieve the full receive diversity of a MIMO fading channel. To characterize the performance gap between sub-optimal decoding and ILD in a more precise way, a novel proximity factor was defined in [15] and further discussed in [16], [17].

Given a lattice generator matrix $\mathbf{B} \triangleq [\mathbf{b}_1, \ldots, \mathbf{b}_n]$, denote ϕ_i the acute angle between $\mathbf{b}_i$ and the linear space spanned by the previous $i-1$ basis vectors, and denote θ_i the acute angle between $\mathbf{b}_i$ and the linear space spanned by the rest $n-1$ basis vectors, then the proximity factors [15] of SIC and ZF decoding are defined as:

$$\begin{aligned} \rho_{i,SIC} &\triangleq \sup_{\mathbf{B} \in \mathcal{B}_{Red}} \frac{\lambda_1^2(L(\mathbf{B}))}{\|\mathbf{b}_i\|_2^2 \sin \phi_i^2}, \\ \rho_{i,ZF} &\triangleq \sup_{\mathbf{B} \in \mathcal{B}_{Red}} \frac{\lambda_1^2(L(\mathbf{B}))}{\|\mathbf{b}_i\|_2^2 \sin \theta_i^2}, \end{aligned} \tag{37}$$

respectively, where the supremum is taken over the set $\mathcal{B}_{Red}$ of bases satisfying a certain reduction notion for any n-dim lattice L. We further define $\rho_{SIC} \triangleq \max_i\{\rho_{i,SIC}\}$ and $\rho_{ZF} \triangleq \max_i\{\rho_{i,ZF}\}$. From [17], the average error probability of ZF decoding can be bounded as

$$\begin{aligned} P_{e,ZF}(\mathrm{SNR}) &\leq \sum_{i=1}^{n} P_{e,ILD}\left(\frac{\mathrm{SNR}}{\rho_{i,ZF}}\right) \\ &\leq n P_{e,ILD}\left(\frac{\mathrm{SNR}}{\rho_{ZF}}\right) \end{aligned}$$

for arbitrary SNR. A similar bound exists for SIC decoding.

C. Proximity Factors of SIC Decoding

1) LLL-Reduction: Let $\mathbf{B} \in \mathbb{R}^{m \times n}$, $m \geq n$, be an LLL-reduced matrix and let $\mathbf{R}$ be the R-factor of $\mathbf{B}$. From [26], we have

$$r_{j,j}^2 \leq \beta^{i-j} r_{i,i}^2, \quad \text{for} \quad 1 \leq j < i \leq n, \tag{38}$$

where $\beta = \frac{1}{\left(\omega - \frac{1}{4}\right)} \geq \frac{4}{3}$. Based on (38), an upper bound of $\rho_{i,SIC}$ was presented in [17]:

$$\rho_{i,SIC} \leq 1 + \frac{\beta}{4(\beta - 1)}(\beta^{i-1} - 1). \tag{39}$$

Now we present an improvement of the above bound. Suppose that $\mathbf{B}_i$, $1 \leq i \leq n$, is the submatrix of $\mathbf{B}$ consisting of the first i columns of $\mathbf{B}$. Then it is obvious that $\lambda_1^2(L(\mathbf{B})) \leq \lambda_1^2(L(\mathbf{B}_i))$, $1 \leq i \leq n$. From the definition of Hermite's constant, we have

$$\begin{aligned} \lambda_1^2(L(\mathbf{B})) &\leq \lambda_1^2(L(\mathbf{B}_i)) \\ &\leq \gamma_i \cdot (r_{1,1} r_{2,2} \cdots r_{i,i})^{\frac{2}{i}}, \ 1 < i \leq n. \end{aligned} \tag{40}$$

Substituting (6) and (38) into (40), we obtain

$$\rho_{i,SIC} = \sup \frac{\lambda_1^2(L(\mathbf{B}))}{r_{i,i}^2} \leq \gamma_i \cdot \beta^{\frac{i-1}{2}} \leq \left(1 + \frac{i}{4}\right) \beta^{\frac{i-1}{2}}. \tag{41}$$

It follows from (41) that

$$\rho_{SIC} = \rho_{n,SIC} \leq \gamma_n \cdot \beta^{\frac{n-1}{2}} \leq \left(1 + \frac{n}{4}\right) \beta^{\frac{n-1}{2}}. \tag{42}$$

Although the new upper bound (41) is still exponential with respect to the dimension n, it significantly improves the currently best known estimation (39).

The proximity factor for HKZ-reduction was given in [17]:

$$\rho_{SIC} = \rho_{n,SIC} \leq \gamma_n \prod_{t=2}^{n} \gamma_t^{\frac{1}{(t-1)}}. \tag{43}$$

Comparing (42) and (43), the HKZ-reduction is expected to perform better than the LLL-reduction, since (43) grows sub-exponentially with the dimension n.

2) Minkowski-Reduction: We first present a result which will be used later.

Proposition 1: If the columns of $\mathbf{M} = [\mathbf{m}_1, \ldots, \mathbf{m}_n]$ form a Minkowski-reduced basis for $L(\mathbf{M})$, then for each submatrix $\mathbf{M}_i = [\mathbf{m}_1, \ldots, \mathbf{m}_i]$, $1 \leq i \leq n$, the columns of $\mathbf{M}_i$ form a Minkowski-reduced basis for $L(\mathbf{M}_i)$.

Proof: For $i = 1$, $\mathbf{m}_1$ is a shortest nonzero vector in both $L(\mathbf{M})$ and $L(\mathbf{M}_1)$. For $i = 2$, let $\mathbf{b}_2 \in L(\mathbf{M}_2)$ and suppose that $\mathbf{m}_1, \mathbf{b}_2$ form a basis for $L(\mathbf{M}_2)$, then it is easy to verify that $\mathbf{m}_1, \mathbf{b}_2, \mathbf{m}_3, \ldots, \mathbf{m}_n$ can form a basis for $L(\mathbf{M})$, which implies that $\|\mathbf{m}_2\|_2 \leq \|\mathbf{b}_2\|_2$. Thus $\mathbf{m}_1, \mathbf{m}_2$ form a Minkowski-reduced basis for $L(\mathbf{M}_2)$. Similarly, we can prove that for $i = 3, 4, \ldots, n$. Thus, the proof is completed.

Let $\mathbf{B} \in \mathbb{R}^{m\times n}$ be a Minkowski-reduced matrix and let $\mathbf{R}$ be the R-factor of $\mathbf{B}$. Denote $\mathbf{B}_i$, $1 \leq i \leq n$, the submatrix which consists of the first i columns of $\mathbf{B}$. Then it follows from Proposition 1, (11), and (12) that for $n \leq 4$,

$$\rho_{i,SIC} = \sup \frac{\lambda_1^2(L(\mathbf{B}_i))}{r_{i,i}^2} \leq \frac{\|\mathbf{b}_i\|_2^2}{r_{i,i}^2} \leq \gamma_i^i, \quad 1 \leq i \leq n, \tag{44}$$

while for $n > 4$,

$$\rho_{i,SIC} \leq \frac{\|\mathbf{b}_i\|_2^2}{r_{i,i}^2} \leq \gamma_i^i \cdot \left(\frac{5}{4}\right)^{\frac{(i-3)(i-4)}{2}}, \quad 1 \leq i \leq n. \tag{45}$$

Hence, we have

$$\rho_{SIC} = \rho_{n,SIC} \leq \max\left\{\gamma_n^n, \gamma_n^n \left(\frac{5}{4}\right)^{\frac{(n-3)(n-4)}{2}}\right\}. \tag{46}$$

In particular, when $n = 2$, we have $\rho_{SIC} = \gamma_2^2 = \frac{4}{3}$, which agrees with Gaussian reduction. Certainly, the proximity factor (46) may not be tight since it grows super-exponentially with the dimension n. However, this upper bound is sufficient to prove that Minkowski-reduction-aided SIC decoding can achieve the same diversity order with ILD.

D. Proximity Factors of ZF Decoding

The upper bounds of ρ_{ZF} for LLL and HKZ-reduction were given in [15], [17]. In this subsection, we shall improve existing result on ρ_{ZF} for LLL-reduction, and derive an upper bound of ρ_{ZF} for Minkowski-reduction.

The derivation for ρ_{ZF} needs a lower bound of $\sin\theta_i^2$. Let $\mathbf{R}$ be the R-factor of $\mathbf{B}$, and set $\mathbf{A}_i = \mathbf{R}(i:n, i:n)^{\mathrm{T}}\mathbf{R}(i:n, i:n)$, $1 \leq i \leq n$. Then it is proved in [17] that

$$\rho_{i,ZF} = \sup_{\mathbf{B}\in\mathcal{B}_{Red}} \lambda_1^2(L(\mathbf{B})) \cdot (\mathbf{A}_i^{-1})_{1,1}. \tag{47}$$

So an upper bound of $\rho_{i,ZF}$ can be immediately determined if the upper bound of $(\mathbf{A}_i^{-1})_{1,1}$ is found.

1) LLL-Reduction: In [17], using an estimation for $(\mathbf{A}_i^{-1})_{1,1}$, an upper bound of ρ_{ZF} for the LLL-reduction was given as

$$\rho_{ZF} \leq \frac{\beta}{9\beta - 4}\left(\frac{9\beta}{4}\right)^{n-1} + \frac{8\beta - 4}{9\beta - 4}. \tag{48}$$

Now we present an improvement of the above bound. To this aim, we first recall the following result.

Lemma 2 ([17]): Let $\mathbf{R} \triangleq [r_{i,j}]$ be the R-factor of a size-reduced lattice generator matrix $\mathbf{B} \in \mathbb{R}^{m\times n}$. Then

$$(\mathbf{A}_i^{-1})_{1,1} \leq r_{i,i}^{-2} + \frac{1}{9}\sum_{j=1}^{n-i}\left(\frac{9}{4}\right)^j r_{i+j,i+j}^{-2}. \tag{49}$$

From (47) and (49),

$$\rho_{i,ZF} \leq \frac{\lambda_1^2(L)}{r_{i,i}^2} + \frac{1}{9}\sum_{j=1}^{n-i}\left(\frac{9}{4}\right)^j \frac{\lambda_1^2(L)}{r_{i+j,i+j}^2}. \tag{50}$$

Substituting (41) into (50), we obtain

$$\rho_{i,ZF} \leq \gamma_i \beta^{\frac{i-1}{2}} + \frac{1}{9}\sum_{j=1}^{n-i}\left(\frac{9}{4}\right)^j \gamma_{i+j}\beta^{\frac{i+j-1}{2}}. \tag{51}$$

Thus,

$$\rho_{ZF} = \rho_{1,ZF} \leq 1 + \frac{1}{9}\sum_{j=1}^{n-1}\left(\frac{9}{4}\right)^j \gamma_{j+1}\beta^{\frac{j}{2}}. \tag{52}$$

It is easy to verify that the new bound (52) is better than the previous bound (48).

In [17], an upper bound of ρ_{ZF} for HKZ-reduction is also given:

$$\rho_{ZF} \leq 1 + \frac{1}{9}\sum_{j=1}^{n-1}\left(\frac{9}{4}\right)^j \xi_{j+1} \leq \left(\frac{9}{4}\right)^{n-1} n^{1+\ln n}. \tag{53}$$

Comparing (52) and (53), the proximity factor of HKZ-reduction is smaller than that of LLL-reduction. This is in accordance with the fact that HKZ-reduction is a stronger notion than LLL-reduction.

2) Minkowski-Reduction: To derive the upper bound of $\rho_{i,ZF}$ for Minkowski-reduction, we give a technical lemma. The proof is given in Appendix A.

Lemma 3: Given a Minkowski-reduced basis $\mathbf{B} \in \mathbb{R}^{m\times n}$ and its R-factor $\mathbf{R} \in \mathbb{R}^{n\times n}$. If $n \leq 4$, then

$$(\mathbf{A}_i^{-1})_{1,1} \leq r_{i,i}^{-2} \cdot \prod_{k=i+1}^{n} \gamma_k^k, \tag{54}$$

else

$$(\mathbf{A}_i^{-1})_{1,1} \leq r_{i,i}^{-2} \cdot \prod_{k=i+1}^{n} \gamma_k^k \cdot \prod_{k=\max\{5,i+1\}}^{n} \left(\frac{5}{4}\right)^{\frac{(k-3)(k-4)}{2}}. \tag{55}$$

It follows from (47), (54) and (11) that if $n \leq 4$,

$$\rho_{i,ZF} \leq \frac{\lambda_1^2(L)}{r_{i,i}^2} \prod_{k=i+1}^{n} \gamma_k^k \leq \prod_{k=i}^{n} \gamma_k^k. \tag{56}$$

Similarly, for the case $n > 4$, we can deduce

$$\rho_{i,ZF} \leq \prod_{k=i}^{n} \gamma_k^k \cdot \prod_{k=\max\{5,i\}}^{n} \left(\frac{5}{4}\right)^{\frac{(k-3)(k-4)}{2}}. \tag{57}$$

Thus, we have

$$\rho_{ZF} = \rho_{1,ZF} \leq \prod_{k=1}^{n} \max\left\{\gamma_k^k, \gamma_k^k\left(\frac{5}{4}\right)^{\frac{(k-3)(k-4)}{2}}\right\}. \tag{58}$$

In particular, when $n = 2$, we have $\rho_{ZF} = \gamma_2^2 = \frac{4}{3}$, which agrees with Gaussian reduction. Comparing (46) with (58), the proximity factor of SIC decoding is much smaller than ZF decoding for Minkowski-reduction.

VII. Simulation Results

In this section, we compare the efficiency of the proposed new algorithms by means of computer simulation. The proximity factors as well as the BER performance of sub-optimal decoding algorithms aided by LLL, HKZ and Minkowski-reduced bases are also compared. All experiments were performed on complex matrices with random entries, drawn from i.i.d. zero-mean, unit variance Gaussian distributions.[1] Firstly, we compare the running times of Algorithm HKZ-Red, Algorithm M-Red-1 and Algorithm M-Red-2 with the HKZ-reduction algorithm presented in [7], the Minkowski-reduction algorithm presented in [39], and the LLL algorithm [26]. To assess the efficiency of these algorithms, the median of the average running times for 1000 random matrices are computed. Occasionally, a random matrix with very long running time is drawn. Using the median rather than the mean guarantees that these rare matrices do not dominate the average running times. Fig. 8 depicts our results, where each point is given in average time (in seconds) of dimension n, using a DELL computer with a 2.0-GHz Pentium Dual processor, with MATLAB running under Windows XP. Note that for each dimension, the running times for all the algorithms are averaged using the same matrices. Fig. 8 shows that Algorithm HKZ-Red is more efficient, about one magnitude order, than the HKZ-reduction algorithm presented in [7] (with the legend HKZ02). This illustrates that the new basis expansion strategy Procedure Transform is more efficient than Kannan's basis expansion method. Also, our second improved Minkowski-reduction algorithm M-Red-2 is more efficient than the first algorithm M-Red-1, and the gap between them becomes larger quickly as the dimension increases. Both M-Red-1 and M-Red-2 are much more efficient than the algorithm presented in [39] (with the legend M85). Apparently, the LLL algorithm is always the fastest, due to its polynomial complexity.

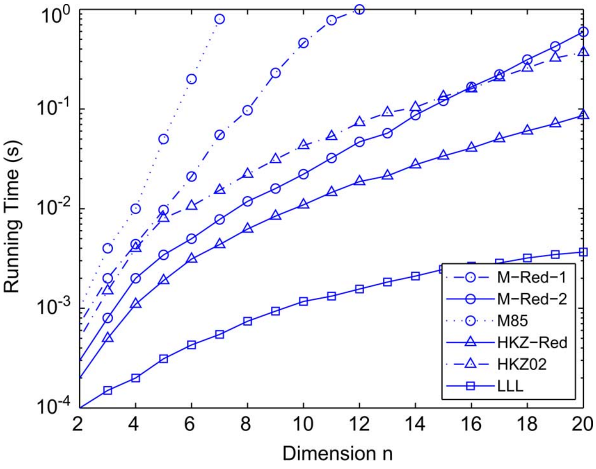

Fig. 8. Comparison of the average running times among algorithms HKZ-Red, M-Red-1, M-Red-2, the HKZ-reduction algorithm in [7] (HKZ02), the minkowski-reduction algorithm in [39] (M85), and the LLL algorithm $(\omega = \frac{3}{4})$ for gaussian random matrices.

Secondly, during the process of algorithms HKZ-Red, M-Red-1, M-Red-2, the computational cost in each iteration is dominated by SE enumeration, Procedure M-Decode-1 and Procedure M-Decode-2, respectively. Then, to further investigate the efficiency of the three reduction algorithms, we compare the average complexity of the three procedures called in each iteration, by using the cardinality of the search space and the number of gcd computations as a measurement. We show our results in Table II. Again, each entry in the table is the average of 1000 random matrices of order 20, and the index of iterations is denoted by k. Table II shows that as the iteration continues, more basis vectors are produced, the search space of SE enumeration (called in HKZ-Red) decreases, the search space of Procedure M-Decode-1 (called in M-Red-1) increases, while the search space of Procedure M-Decode-2 (called in M-Red-2) stays about the same. This can be explained as follows. In HKZ-reduction, after each iteration, the dimension of the sublattice to be searched is reduced by one, thus the search space of SE enumeration decreases rapidly as k increases. However, for Minkowski-reduction, the dimension of the sublattice to be searched stays the same as the iteration continues. Note that in Procedure M-Decode-2, the constraint $\gcd(z_k, \ldots, z_n) = 1$ is imposed as soon as $z_k, \ldots, z_n$ are available. Thus the complexity of Procedure M-Decode-2 do not vary much for different k. But for Procedure M-Decode-1, the gcd constraint can not be checked until the whole integer vector $\mathbf{z}$ is available. Therefore Procedure M-Decode-1 always costs more than Procedure M-Decode-2. Moreover, as the iteration continues, the search space of Procedure M-Decode-1 increases rapidly, since the constraint $\gcd(z_k, \ldots, z_n) = 1$ gets more severe as k increases. We can also obtain from Table II that for each iteration, the average numbers of gcd operations performed in both of the two procedures are roughly 1/10 of the cardinality of the search space. Thus, checking the gcd constraint does not costs much when compared with the total complexity.

Thirdly, we compare the average orthogonality defect of LLL, HKZ and Minkowski-reduced bases produced by our new algorithms in Fig. 9. As shown in the figure, the orthogonality defect of Minkowski-reduction is always the best, and the LLL-reduction has the worst performance. This suggests that sub-optimal decoding algorithms aided by Minkowski and HKZ-reductions are expected to perform better than those aided by LLL-reduction.

Fourthly, we compare the proximity factors of ZF decoding and SIC decoding with LLL, HKZ, and Minkowski-reduced bases. Fig. 10 shows the theoretical upper bounds. For all the bounds, we have applied the bounds (6) on Hermite's constants when the exact values are unknown. As described in Section VI, for each reduction, the proximity factor of SIC decoding is much smaller than that of ZF decoding. For both SIC decoding and ZF decoding, the proximity factor of LLL-reduction is larger than

[1] The proposed algorithms were not applied to the complex matrices directly. Following [18], a complex system can be easily transformed into an equivalent real system with doubled size by separating the real part apart from the imaginary part.

TABLE II
THE AVERAGE CARDINALITY OF THE SEARCH SPACE AND THE NUMBER OF GCD OPERATIONS COSTED IN EACH ITERATION OF ALGORITHMS HKZ-RED, M-RED-1 AND M-RED-2, OVER RANDOM MATRICES OF ORDER 20

k	search space			# of gcd operations	
	SE	M-DECODE-1	M-DECODE-2	M-DECODE-1	M-DECODE-2
1	7.16×10^2	4.10×10^3	7.16×10^2	3.66×10^2	1.97×10^1
5	4.01×10^2	1.15×10^4	2.68×10^3	1.69×10^3	1.53×10^2
10	1.76×10^2	1.64×10^4	3.14×10^3	2.62×10^3	2.72×10^2
15	3.60×10^1	4.74×10^4	2.86×10^3	8.10×10^3	6.34×10^1
19	6.48×10^0	1.03×10^5	2.98×10^3	8.91×10^3	5.26×10^0

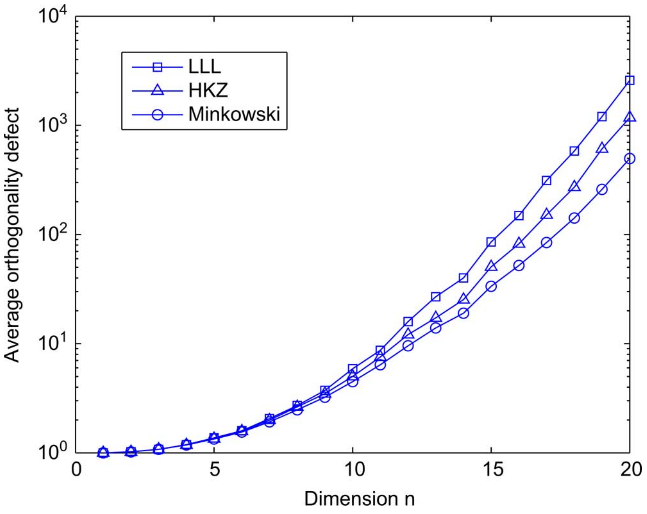

Fig. 9. Comparison of the average orthogonality defect among the LLL, HKZ, and minkowski-reduced bases for Gaussian random matrices.

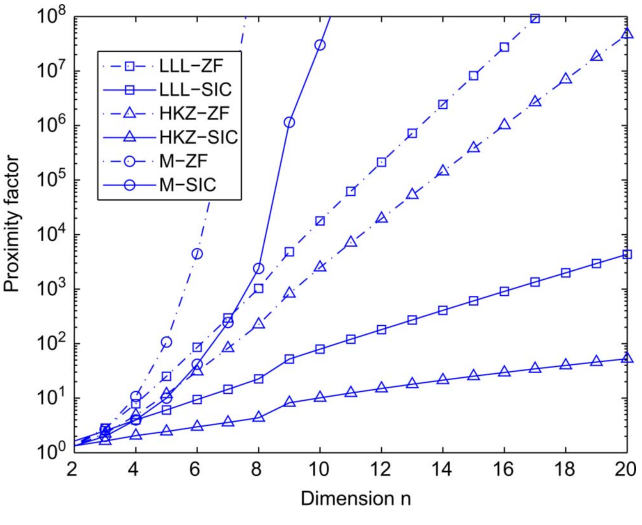

Fig. 10. Comparison of the theoretical upper bounds on the proximity factors for ZF decoding and SIC decoding with LLL, HKZ, and minkowski-reduced bases.

that of HKZ-reduction, and Minkowski-reduction is the largest.

To obtain a practical view of the proximity factors, we simulated them by means of numerical experimentation. For each value of n, we generate 1000 random matrices and apply LLL algorithm and our new algorithms to obtain LLL, HKZ, and Minkowski-reduced bases. Then the proximity factors can be taken as the maximum over these reduced bases. Although the maximum may not reach the bounds in the worst case, they can serve as an experimental lower bound on the theoretical proximity factors [17]. Fig. 11 shows the numerical results. We can learn from this figure that for ZF decoding, the proximity factor of Minkowski-reduction is the smallest, while for SIC decoding, the proximity factor of HKZ-reduction is the smallest. For both ZF decoding and SIC decoding, the proximity factor of LLL-reduction is the largest. Comparing Fig. 10 with Fig. 11, we can find that the theoretical upper bounds for Minkowski-reduction are not tight. Especially, the bound (46) is unlikely to be tight, because we have applied the trivial bound $\lambda_1^2(L) \leq \|\mathbf{b}_i\|_2^2$ in (44). Since we know from (10) that $\left(\frac{5}{4}\right)^{-(n-4)} \leq \frac{\lambda_i^2(L)}{\|\mathbf{b}_i\|_2^2} \leq 1$, this is likely to loosen the bound by a factor of $\left(\frac{5}{4}\right)^{(n-4)}$ at the worst.

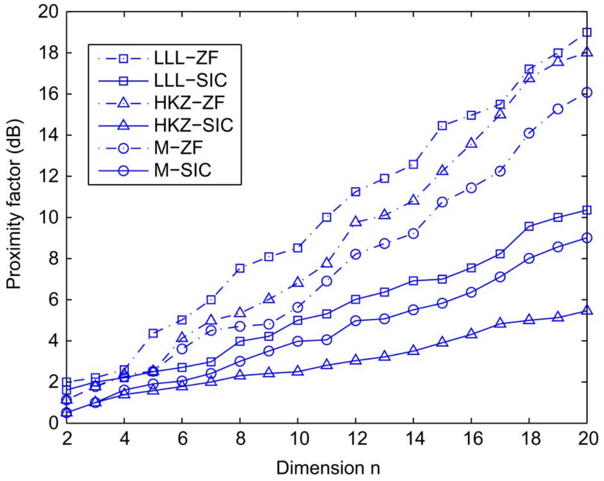

Fig. 11. Comparison of the simulated results on the proximity factors for ZF decoding and SIC decoding with LLL, HKZ, and minkowski-reduced bases.

Finally, we investigate the BER performance of both ZF and SIC decoding with different reduction notions. In Fig. 12, we simulated the BER of different decoding algorithms for an 8×8 MIMO system with a 64-QAM constellation. Also, the entries of the channel matrix are i.i.d. complex Gaussian random variables with zero mean, unit variance. Both the ILD and ML decoding are based on the SE enumeration. This figure shows that for ZF decoding, Minkowski-reduction has the lowest BER, while for SIC decoding, HKZ-reduction has the lowest BER, which is consistent with the simulation results on the proximity factors depicted in Fig. 11.

VIII. CONCLUSIONS

In this paper, we present three new lattice reduction algorithms: one for the HKZ-reduction, and two for the Minkowski-reduction. The expected complexity of the three algorithms are

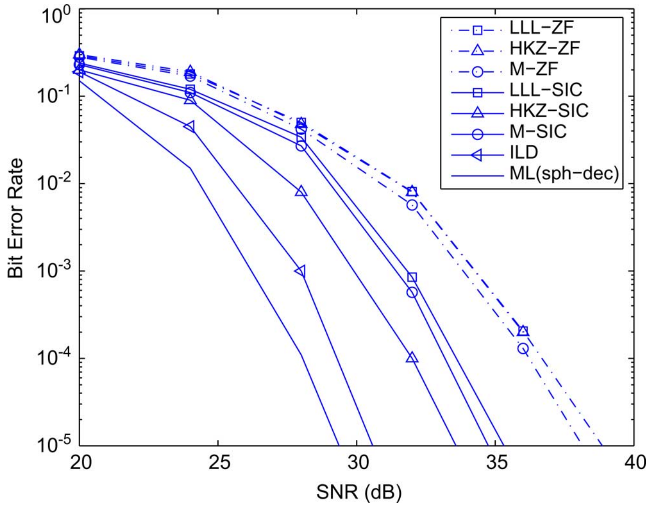

Fig. 12. The BER performance of ILD, ML (sphere) decoding, ZF and SIC decoding with LLL, HKZ, and minkowski-reduced bases in an uncoded 8×8 complex-valued MIMO system with a 64-QAM constellation.

also discussed. Numerical results in Fig. 8 show that they are much more efficient than their existing counterparts. To measure the effects of the LLL, HKZ, and Minkowski-reduced bases on the performance of sub-optimal MIMO detectors, the orthogonality defect as well as the proximity factors are concerned. We further improve some existing results on the proximity factors associated with the LLL-reduction [17]. Moreover, the upper bounds (46) and (58) for Minkowski-reduction are also given. Although the two bounds are not tight, they are sufficient to prove that MRAD can achieve the same diversity order with ILD. Note that MRAD is seldomly considered in the previous references, especially for lattices of dimension $n > 4$. In this paper, we take the first step in this direction.

The proposed algorithms provide better BER performance at the cost of higher complexity than the LLL algorithm. Thus, they are applicable to slow varying channels. For future research, we will improve the efficiency of our algorithms and the theoretical proximity factors for various reduction notions, especially for the Minkowski-reduction.

Appendix
Proof of Lemma 3

From the definition of $\mathbf{A}_i$, $(\mathbf{A}_i^{-1})_{1,1}$ is the squared Euclidean length of the first row of $\mathbf{R}(i:n, i:n)^{-1}$. For $i \le k < n$, we denote $\mathbf{S}_k = \mathbf{R}(i:k, i:k)^{-1}$. Then it is easy to verify that $\mathbf{S}_i = \frac{1}{r_{i,i}}$ and

$$\mathbf{S}_k = \begin{bmatrix} \mathbf{S}_{k-1} & \frac{1}{r_{k,k}} \cdot \mathbf{S}_{k-1} \cdot \mathbf{R}(i:k-1,k) \\ 0 & \frac{1}{r_{k,k}} \end{bmatrix} \tag{59}$$

for $i < k \le n$.

From (11) and (12), one can derive that if $n \le 4$,

$$\|\mathbf{R}(i:k-1,k)\|_2^2 \le \|\mathbf{R}(1:k-1,k)\|_2^2 \le (\gamma_k^k - 1) r_{k,k}^2; \tag{60}$$

else,

$$\|\mathbf{R}(i:k-1,k)\|_2^2 \le \left(\gamma_k^k \cdot \left(\frac{5}{4}\right)^{\frac{(n-3)(n-4)}{2}} - 1\right) r_{k,k}^2. \tag{61}$$

It follows from (59), (60) that if $n \le 4$

$$\begin{aligned} \|\mathbf{S}_k(1,:)\|_2^2 \le \|\mathbf{S}_{k-1}(1,:)\|_2^2 & \\ + \frac{\|\mathbf{S}_{k-1}(1,:)\|_2^2 \cdot \|\mathbf{R}(i:k-1,k)\|_2^2}{r_{k,k}^2} & \\ \le \gamma_k^k \|\mathbf{S}_{k-1}(1,:)\|_2^2. & \end{aligned} \tag{62}$$

From (62), we can derive by induction that

$$\begin{aligned} (\mathbf{A}_i^{-1})_{1,1} &= \|\mathbf{S}_n(1,:)\|_2^2 \\ &\le \mathbf{S}_i^2 \cdot \prod_{k=i+1}^{n} \gamma_k^k \le r_{i,i}^{-2} \cdot \prod_{k=i+1}^{n} \gamma_k^k. \end{aligned} \tag{63}$$

Based on (59) and (61), the inequality (55) for the case $n > 4$ can be easily obtained by using an induction approach similar to (62). Thus the proof is complete.

Acknowledgment

The authors are deeply grateful to the anonymous reviewers for their detailed and constructive comments, which made the paper more updated and presentable. Also, the authors would like to thank Prof. Tim Davidson for his valuable suggestions.

References

[1] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, 2nd ed. Berlin, Germany: Springer-Verlag, 1997.
[2] *The LLL Algorithm: Survey and Applications*, P. Q. Nguyen and B. Vallée, Eds. Berlin, Germany: Springer-Verlag, 2009.
[3] D. E. Knuth, *The Art of Computer Programming, Reading*, 2nd ed. Reading, MA: Addison-Wesley, 1981.
[4] M. Grötschel, L. Lovász, and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*. Berlin, Germany: Springer-Verlag, 1993.
[5] A. Joux and J. Stern, "Lattice reduction: A toolbox for the cryptanalyst," *J. Cryptol.*, vol. 11, no. 3, pp. 161–185, 1998.
[6] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*. Boston, MA: Kluwer Academic, 2002.
[7] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2201–2214, Aug. 2002.
[8] B. Hassibi and H. Vikalo, "On the sphere-decoding algorithm I: Expected complexity," *IEEE Trans. Signal Process.*, vol. 53, no. 8, pp. 2806–2818, Jul. 2005.
[9] C. P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," *Math. Program.*, vol. 66, pp. 181–199, 1994.
[10] M. Phost, "On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications," *ACM SIGSAM Bull.*, vol. 15, pp. 37–44, Feb. 1981.
[11] M. O. Damen, H. E. Gamal, and G. Caire, "On maximum-likelihood detection and the search for the closest lattice point," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2389–2402, Oct. 2003.
[12] J. Jaldén and B. Ottersen, "On the complexity of sphere decoding in digital communications," *IEEE Trans. Signal Process.*, vol. 53, no. 4, pp. 1474–1484, Mar. 2005.
[13] L. Babai, "On lovász's lattice reduction and the nearest lattice point problem," *Combinatorica*, vol. 6, pp. 1–13, 1986.
[14] W. H. Mow, "Universal lattice decoding: Principle and recent advances," *Wireless Commun. Mobile Comput., Special Issue on Coding and Its Appl. Wireless CDMA Syst.*, vol. 3, pp. 553–569, Aug. 2003.
[15] C. Ling, "Towards characterizing the performance of approximate lattice decoding," in *Proc. Int. Symp. Turbo Codes/Int. Conf. Source Channel Coding '06*, Munich, Germany, Apr. 2006.
[16] Y. H. Gan, C. Ling, and H. M. Mow, "Complex lattice reduction algorithm for low-complexity full-diversity MIMO detection," *IEEE Trans. Signal Process.*, vol. 57, no. 7, pp. 2701–2710, Jul. 2009.
[17] C. Ling, "On the proximity factors of lattice reduction-aided decoding," *IEEE Trans. Signal Process.*, vol. 59, no. 6, pp. 2795–2808, Jun. 2011.
[18] D. Wübben, D. Seethaler, J. Jaldén, and G. Marz, "Lattice reduction: A survey with applications in wireless communications," *IEEE Signal Process. Mag.*, vol. 28, no. 3, pp. 70–91, May 2011.

[19] C. Hermite, "Extraits de lettres de M. Hermiteà M. Jacobi sur différents objets de la théorie des nombres," *J. Reine Angew. Math.*, vol. 40, pp. 279–290.

[20] A. Korkine and G. Zolotareff, "Sur les formes quadratiques," *Math. Ann.*, vol. 6, pp. 366–389.

[21] R. Kannan, "Improved algorithms for integer programming and related lattice problems," in *Proc. ACM Symp. Theory Comput.*, Boston, MA, Apr. 1983, pp. 193–206.

[22] B. Helfrich, "Algorithms to construct Minkowski reduced and Hermite reduced lattice bases," *Theory Comput. Sci.*, vol. 41, no. 2–3, pp. 125–139, 1985.

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

[24] A. H. Banihashemi and A. K. Khandani, "On the complexity of decoding lattices using the Korking-Zolotarev reduced basis," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 162–171, Jan. 1998.

[25] H. Minkowski, "Über die positiven quadratischen formen undüber kettenbruchähnliche algorithmen," *J. Reine und Angewandte Math.*, vol. 107, pp. 278–297.

[26] A. K. Lenstra, H. Lenstra Jr, and L. Lovász, "Factorizing polynomials with rational coefficients," *Math. Ann.*, vol. 261, pp. 515–534, Dec. 1982.

[27] D. Boneh, "Twenty years of attacks on the RSA cryptosystem," *Notices Amer. Math. Soc.*, vol. 46, pp. 203–213, 1999.

[28] C. P. Schnorr, "A hierarchy of polynomial lattice basis reduction algorithms," *Theor. Comput. Sci.*, vol. 53, no. 2–3, pp. 201–224, 1987.

[29] F. T. Luk and D. M. Tracy, "An improved LLL algorithm," *Linear Algebra Appl.*, vol. 428, no. 2–3, pp. 441–452, Jan. 2008.

[30] F. T. Luk and S. Qiao, "A pivoted LLL algorithm," *Linear Algebra Appl.*, vol. 434, no. 11, pp. 2296–2307, Jun. 2011.

[31] P. Q. Nguyen and D. Stehlé, "An LLL algorithm with quadratic complexity," *SIAM J. Comput.*, vol. 39, no. 3, pp. 874–903, 2009.

[32] Y. H. Gan and W. H. Mow, "Novel joint sorting and reduction technique for delay-constrained LLL-aided MIMO detection," *IEEE Signal Process. Lett.*, vol. 15, pp. 194–197, 2008.

[33] C. Ling and N. Howgrave-Graham, "Effective LLL reduction for lattice decoding," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Nice, France, Jun. 2007.

[34] D. Wübben, R. Böhnke, V. Kühn, and K. D. Kammeyer, "Near-maximum-likelihood detection of MIMO systems using MMSE-based lattice reduction," in *Proc. Int. Commun. Conf. (ICC' 04)*, Jun. 2004, pp. 798–802.

[35] D. Wübben, R. Böhnke, V. Kühn, and K. D. Kammeyer, "MMSE-based lattice-reduction for near-ML detection of MIMO systems," in *Proc. Int. ITG Workshop on Smart Antennas*, Munich, Germany, Mar. 2004, pp. 106–113.

[36] 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, Dec. 2007.

[37] J. Jaldén and P. Elia, "DMT optimality of LR-aided linear decoders for a general class of channels, lattice designs, and system models," *IEEE Trans. Inf. Theory*, vol. 56, no. 10, pp. 4765–4780, Oct. 2010.

[38] F. T. Luk, S. Qiao, and W. Zhang, "Lattice basis reduction algorithm," Inst. Computat. Math., Hong Kong Baptist Univ., 2010, Tech. Rep. 10-04.

[39] L. Afflerbach and H. Grothe, "Calculation of Minkowski-reduced lattice bases," *Computing*, vol. 35, no. 3–4, pp. 269–276, 1985.

[40] P. W. Wolniansky, G. J. Foschini, G. D. Golden, and R. A. Valenzuela, "V-blast: An architecture for realizing very high data rates over the rich-scattering wireless channel," in *Proc. IEEE Int. Symp. Signals. Syst. Electron. Conf. (ISSSE'98)*, Pisa, Italy, Sep. 1998, pp. 295–300.

[41] G. H. Golub and C. F. Van Loan, *Matrix Computations*, 3rd ed. Baltimore, MD: The Johns Hopkins Univ. Press, 1996.

[42] I. Morel, D. Stehlé, and G. Villard, "H-LLL: Using housholder inside LLL," in *Proc. Int. Symp. on Symb. and Alg. Comput. (ISSAC' 09)*, Seoul, Korea, Jul. 2009, pp. 271–278.

[43] X. W. Chang and G. H. Golub, "Solving ellipsoid-constrained integer least squares problems," *SIAM J. Matrix Anal. Appl.*, vol. 31, no. 3, pp. 1071–1089, 2009.

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

[45] B. L. Van Der Waerden and H. Gross, *Studien zur Theorie der Quadratischen Formen*. Basel: Birkhäuser, 1968.

[46] M. Ajtai, "The shortest vector problem in L_2 is NP-hard for randomized reductions," in *Proc. 30th Annu. ACM Symp. Theory of Comput.*, Dallas, TX, May 1998.

[47] A. Vardy and Y. Be'ery, "Maximum-likelihood decoding of the leech lattice," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1435–1444, Jul. 1993.

[48] A. H. Banihashemi and I. F. Blake, "Trellis complexity and minimal trellis diagrams of lattices," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 1829–1847, Sep. 1998.

[49] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Math. Comput.*, vol. 44, no. 170, pp. 463–471, Apr. 1985.

[50] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1639–1642, Jul. 1999.

[51] M. Ajtai, R. Kumar, and D. Sivakumar, "A sieve algorithm for the shortest lattice vector problem," in *Proc. ACM STOC '01*, Crete, Greece, Jul. 2001, pp. 601–610.

[52] P. Q. Nguyen and T. Vidick, "Sieve algorithms for the shortest vector problem are practical," *J. Math. Crypt.*, vol. 2, no. 2, pp. 181–207, 2008.

[53] D. Micciancio and P. Voulgaris, "Faster exponential time algorithms for the shortest vector problem," in *Proc. ACM/SIAM SODA '10*, Austin, TX, Jan. 2010, pp. 1468–1480.

[54] W. Zhang, S. Qiao, and Y. Wei, "Practical HKZ and Minkowski Lattice Reduction Algorithms," Dept. Comput. Software, McMaster Univ., Hamilton, ON, Canada, 2011, Tech. Rep. CAS-11-04-SQ.

[55] H. Grossman, "On the number of divisions in finding a G.C.D," *Amer. Math. Month.* , vol. 31, pp. 443–443, 1924.

[56] D. Romik, "Stirling's approximation for n!: The ultimate short proof?," *Amer. Math. Month.*, vol. 107, pp. 556–557, 2000.

[57] J. L. Lagrange, "Recherches d'arithmétique," in *Proc. Nouv. Mém. Acad.*, Berlin, 1773.

[58] I. Semaev, "A 3-dimensional lattice reduction algorithm," in *Proc. Cryptogr. Lattices Conf. (CALC'01)*, RI, Mar. 2001, pp. 181–193.

[59] P. Q. Nguyen and D. Stehlé, "Low-dimensional lattice basis reduction revisited," *ACM Trans. Algor.*, vol. 5, no. 4, Oct. 2009.

[60] C. Ling, W. H. Mow, and L. Gan, "Dual-lattice ordering and partial lattice reduction for SIC-based MIMO detection," *IEEE J. Sel. Topics Signal Process.*, vol. 3, pp. 975–985, Dec. 2009.

Wen Zhang received the B.S. degree in information and computation science and the M.S. degree in computational mathematics from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2006 and 2009 respectively.

Currently, he is working toward the Ph.D. degree in computational mathematics at the School of Mathematical Sciences, Fudan University. His research interests include signal processing for wireless communications, lattice theory, and numerical linear algebra.

Sanzheng Qiao received the B.S. degree in mathematics and the M.S. degree in computational mathematics from Shanghai Normal University, Shanghai, China, in 1966 and 1981, respectively. He received the M.S. degree in computer science and the Ph.D. degree in applied mathematics from Cornell University, Ithaca, NY, in 1986 and 1987, respectively.

He then became an Assistant Professor of Computer Science at Ithaca College. In 1989, he joined the Department of Computer Science and Communications Research Laboratory, McMaster University, Hamilton, Ontario, Canada, as an Assistant Professor. Since 1999, he has been a Professor of computer science at McMaster University. His research interests include numerical linear algebra and its applications in signal processing and scientific computing.

Yimin Wei received the B.S. and Ph.D. degrees in computational mathematics from Shanghai Normal University and Fudan University in 1991 and 1997, respectively.

He was a Lecturer with the Department of Mathematics, Fudan University, from 1997 to 2000. He was a Visiting Scholar with the Division of Engineering and Applied Science, Harvard University, Boston, MA, from 2000 to 2001. From 2001 to 2005, he was an Associate Professor in the School of Mathematical Sciences, Fudan University. He is currently a Professor with the School of Mathematical Sciences of Fudan University. His research interests include numerical linear algebra and its applications, sensitivity in computational linear control, and perturbation analysis.