On Low-complexity Lattice Reduction Algorithms for Large-scale MIMO Detection: the Blessing of Sequential Reduction

Shanxiang Lyu, Jinming Wen, Jian Weng and Cong Ling

Abstract—Lattice reduction is a popular preprocessing strategy in multiple-input multiple-output (MIMO) detection. In a quest for developing a low-complexity reduction algorithm for largescale problems, this paper investigates a new framework called sequential reduction (SR), which aims to reduce the lengths of all basis vectors. The performance upper bounds of the strongest reduction in SR are given when the lattice dimension is no larger than 4. The proposed new framework enables the implementation of a hash-based low-complexity lattice reduction algorithm, which becomes especially tempting when applied to large-scale MIMO detection. Simulation results show that, compared to other reduction algorithms, the hash-based SR algorithm exhibits the lowest complexity while maintaining comparable error performance.

Index Terms—lattice reduction, MIMO, large-scale, hash-based.

I. INTRODUCTION

The number of antennas has been scaled up to tens or hundreds in multiple-input multiple-output (MIMO) systems to fulfill the performance requirements needed by the next generation communication systems [1]. A critical challenge that comes with very large arrays is to design reliable and computationally efficient detectors. Though the well-known maximum likelihood detector (MLD) provides optimal error performance, it suffers from exponential complexity that grows with the number of transmit antennas [2]. In the past two decades, lattice-reduction-aided suboptimal detection techniques have been well investigated [3]-[5], whose instantaneous complexity does not depend on constellation size and noise realizations, but collect the same diversity as the MLD for MIMO systems [6]-[8]. Although conventional lattice reduction algorithms suffice for small-scale MIMO systems, there is still an avenue to pursue a more practical low-complexity reduction algorithm for large-scale systems. Moreover, an efficient reduction algorithm for large-scale problems may also find its applications to cryptanalysis [9] and image processing [10].

1

The principle of designing a reduction algorithm varies depending on the desired basis properties: to make all the basis vectors short, or to make the condition number of the reduced basis small. There are several popular types of lattice reduction strategies, such as Minkowski reduction, Korkine-Zolotareff reduction (KZ) [11], Gauss reduction [12], Lenstra– Lenstra–Lovász (LLL) reduction [13], Seysen reduction [14], etc. They yield reduced bases with shorter or more orthogonal basis vectors, and provide a trade-off between the quality of the reduced basis and the computational effort required for finding it. In essence, a reduction algorithm aims to find a unimodular matrix to transform an input basis into another one with better property. The process involves a series of elementary operations noted as reflection, swapping, and translation. These operations vary for distinct algorithms.

Much work has been done to advance conventional reduction algorithms. Regarding KZ, refs. [15]–[17] give some practical implementations and improve the performance bounds. As for blockwise KZ, its faster implementations and the expected basis properties are given in [18]. Researchers have also been constructing and analyzing the variants of LLL with great effort. For instance, the size reduction step is optimized in [16], [19], [20], the implementation order of swaps is simplified in [21]–[23], and the fixed complexity versions of LLL are given in [19], [22], [24]. In contrast, the direction on Seysen reduction has few follow-up studies [25], [26], partly because of the fact that Seysen reduction has unsatisfactory performance in high dimensions.

While LLL and blockwise KZ are still the default choices in cryptography to reduce a basis in hundreds of dimensions, the element-based lattice reduction (ELR) proposed in [27] has become more attracting in large MIMO, which preprocesses a large basis with even lower complexity than LLL. Later ref. [27] has been generalized to ELR^+ [28] for small-scale problems, but the theoretical characterization of ELR and ELR^+ has not been given a rigorous treatment, even for small dimensions. It is noteworthy that ELR and ELR^+ have totally different structures with LLL variants, and one might be lured into the belief that ELR and ELR^+ can be tuned to arrive at more sophisticated methods. Nevertheless, no analytical skills can be inherited from LLL/KZ literature [12], [13], which makes the performance analysis of the new algorithms

This work was supported in part by the National Natural Science Foundation of China under Grants 61902149, 61932010 and 11871248, in part by the Major Program of Guangdong Basic and Applied Research under Grant 2019B030302008, in part by the Natural Science Foundation of Guangdong Province under Grants 2019B010136003 and 2019B010137005, in part by the Fundamental Research Funds for the Central Universities under Grant 2017YFB0802203 and 2018YFB1003701. This paper was presented in part at the 8th International Conference on Wireless Communications and Signal Processing (WCSP), Yangzhou, China, Oct. 2016.

S. Lyu, J. Wen and J. Weng are with the College of Cyber Security, Jinan University, Guangzhou 510632, China (e-mail: shanxianglyu@gmail.com, jinmingwen1@163.com, cryptjweng@gmail.com). S. Lyu is also with the State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China.

C. Ling is with the Department of Electrical and Electronic Engineering, Imperial College London, London SW7 2AZ, United Kingdom (e-mail: cling@ieee.org).

complicated.

In this work, we investigate a general form of ELR and ELR⁺ which we refer to as sequential reduction (SR). We derive the objective function from a MIMO detection task, and present the general form of an SR algorithm which can solve/approximate the smallest basis problem. Unlike KZ or Minkowski reduction, SR reduces the basis vectors by using sub-lattices so as to avoid a basis expansion process. The strongest algorithm in SR tries to minimize the length of basis vectors with the aid of a closest vector problem (CVP) oracle. We show bounds on the basis lengths and orthogonal defects for small dimensions. After that, the feasibility of applying SR to reduce a large dimensional basis is analyzed, and we actually construct a hash-based algorithm for this task. Our simulation results then show the plausibility of using SR in large-scale MIMO systems.

Preliminary results of this work have been partly presented in a conference paper [29]. Compared with [29], this work contains the following new contributions:

- The performance bounds on small dimensional bases are rigorously analyzed (Theorems 2 and 3). Unlike the results in [29] that rely on an assumption about covering radius, these bounds hold for all input bases.
- Comparisons with other types of strong&weak reduction are made (Section III-B, Section IV-D), including η-Greedy reduction, KZ and its variants, Minkowski reduction, LLL and its variants, and Seysen reduction.
- A Hash-based SR algorithm is constructed (Section IV). More specifically, the nearest neighbor search problem is approximately solved with the aid of hashing, and not through a brute-force search.
- The theoretical studies are supported with more simulation results (Section V), these include the comparisons with major lattice-reduction-aided MIMO detection algorithms, and the BER performance tested for various channels.
- The types of bases feasible for using SR-Hash is discussed (Appendix A). We numerically show that the dual of large-scale Gaussian random bases have dense pairwise angles.

It is worth mentioning that SR is emerging as a new building block in lattice-reduction-aided MIMO detection. Thus, the proposed SR variants may also benefit list sphere decoding [30] and Klein's sampling algorithm [31].

The rest of this paper is organized as follows. Backgrounds about lattices and lattice reduction in MIMO are reviewed in Section II. The SR framework is subsequently introduced in Section III. The low-complexity version of SR based on hashing is given in Section IV. After that, Section V presents the simulation results. Conclusions and possible future research are presented in the last section.

Notation: Matrices and column vectors are denoted by uppercase and lowercase boldface letters. The *i*th column and (j, i)th entry of **B** are respectively denoted as \mathbf{b}_i and $b_{i,j}$. \mathbf{I}_n and $\mathbf{0}_n$ respectively denote the $n \times n$ identity matrix and $n \times 1$ zero vector, and the operation $(\cdot)^{\top}$ denotes matrix transposition. [n] denotes the set $\{1, \ldots, n\}$. For a set Γ , \mathbf{B}_{Γ} denotes the columns of **B** indexed by Γ . span (\mathbf{B}_{Γ}) denotes the vector space spanned by vectors in \mathbf{B}_{Γ} . $\pi_{\mathbf{B}_{\Gamma}}(\mathbf{x})$ and $\pi_{\mathbf{B}_{\Gamma}}^{\perp}(\mathbf{x})$ denote the projection of \mathbf{x} onto $\operatorname{span}(\mathbf{B}_{\Gamma})$ and the orthogonal complement of $\operatorname{span}(\mathbf{B}_{\Gamma})$, respectively. $\lfloor x \rceil$ denotes rounding x to the nearest integer, |x| denotes getting the absolute value of x, and $\|\mathbf{x}\|$ denote the Euclidean norm of vector \mathbf{x} . \mathbb{N} and \mathbb{Z} respectively denotes the set of natural numbers and integers. The set of $n \times n$ integer matrices with determinants ± 1 is denoted by $\operatorname{GL}_n(\mathbb{Z})$.

II. PRELIMINARIES

A. Lattices

An *n*-dimensional lattice Λ is a discrete additive subgroup in the real field \mathbb{R}^n . Similarly to the fact that any finitedimensional vector space has a basis, a lattice has a basis. To consider a square matrix for simplicity, a lattice generated by basis $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{R}^{n \times n}$ is defined as

$$\Lambda(\mathbf{B}) = \left\{ \mathbf{v} \mid \mathbf{v} = \sum_{i \in [n]} c_i \mathbf{b}_i \, ; \, c_i \in \mathbb{Z} \right\}.$$

The dual lattice of Λ is defined as $\Lambda^{\dagger} = \{\mathbf{u} \in \mathbb{R}^n \mid \langle \mathbf{u}, \mathbf{v} \rangle \in \mathbb{Z}, \forall \mathbf{v} \in \Lambda\}$. One basis of Λ^{\dagger} is given by $\mathbf{B}^{-\top}$.

The Gram-Schmidt (GS) basis of **B**, referred to as **B**^{*}, is found by using $\mathbf{b}_i^* = \pi_{\{\mathbf{b}_1^*,...,\mathbf{b}_{i-1}^*\}}(\mathbf{b}_i) = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{b}_j^*$, where $\mu_{i,j} = \langle \mathbf{b}_i, \mathbf{b}_j^* \rangle / ||\mathbf{b}_j^*||^2$.

The *i*th successive minimum of an *n* dimensional lattice $\Lambda(\mathbf{B})$ is the smallest real positive number *r* such that Λ contains *i* linearly independent vectors of length at most *r*:

$$\lambda_i(\mathbf{B}) = \inf \{r \mid \dim(\operatorname{span}((\Lambda \cap \mathcal{B}(\mathbf{0}, r))) \geq i\},\$$

in which $\mathcal{B}(\mathbf{t}, r)$ denotes a ball centered at \mathbf{t} with radius r.

The orthogonality defect (OD) can alternatively quantify the goodness of a basis

$$\eta(\mathbf{B}) = \frac{\prod_{i=1}^{n} ||\mathbf{b}_i||}{\sqrt{|\det(\mathbf{B}^T \mathbf{B})|}}.$$
(1)

From Hadamard's inequality, we know that $\eta(\mathbf{B}) \geq 1$. As the determinant of a given basis is fixed, the parameter is proportional to the product of the lengths of the basis vectors. A necessary condition for reaching the smallest orthogonality defect is to have a short basis length defined as $l(\mathbf{B}) = \max_i ||\mathbf{b}_i||$.

The ε CVP problem is, given a vector $\mathbf{y} \in \mathbb{R}^n$ and a lattice $\Lambda(\mathbf{B})$, find a vector $\mathbf{v} \in \Lambda(\mathbf{B})$ such that:

$$\|\mathbf{y} - \mathbf{v}\|^2 \le \varepsilon \|\mathbf{y} - \mathbf{w}\|^2, \ \forall \, \mathbf{w} \in \Lambda(\mathbf{B}).$$

An algorithm that solves an ε CVP problem is referred to as an ε CVP oracle. We write $\mathbf{v} = \varepsilon$ CVP(\mathbf{y}, \mathbf{B}) or $\mathbf{v} =$ CVP(\mathbf{y}, \mathbf{B}) if $\varepsilon = 1$.

B. Lattice-reduction-aided MIMO detection

We considered an uplink multiuser large MIMO system, in which n_T single-antenna users send data to a base station with n_R antennas, and both n_T , n_R are in the order of tens or hundreds. A received complex-valued signal vector at the base station is written as:

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

where $\mathbf{B}_c \in \mathbb{C}^{n_R \times n_T}$ denotes a channel matrix perfectly known at the base station, $\mathbf{x}_c \in \mathbb{C}^{n_T}$ refers to a signal vector with entries drawn from a QAM constellation, and $\mathbf{w}_c \in \mathbb{C}^{n_R}$ denotes a zero-mean additive noise vector with entries independently and identically following the complex normal distribution $\mathcal{CN}(0, \sigma_w^2)$.

To simplify the analysis we will focus on representations in the real field, so (2) is transformed to an equivalent real value system with

$$\mathbf{y} = \bar{\mathbf{B}}\mathbf{x} + \mathbf{w},\tag{3}$$

where

$$\bar{\mathbf{B}} = \begin{bmatrix} \Re(\mathbf{B}_c) & -\Im(\mathbf{B}_c) \\ \Im(\mathbf{B}_c) & \Re(\mathbf{B}_c) \end{bmatrix},$$
(4)

and $\mathbf{y} = [\Re(\mathbf{y})^{\top}, \Im(\mathbf{y})^{\top}]^{\top}$, $\mathbf{x} = [\Re(\mathbf{x})^{\top}, \Im(\mathbf{x})^{\top}]^{\top}$, $\mathbf{w} = [\Re(\mathbf{w})^{\top}, \Im(\mathbf{w})^{\top}]^{\top}$ are all real and imaginary compositions. Here the noise variance of \mathbf{w} becomes $\sigma^2 = \sigma_w^2/2$.

Lattice reduction is essentially multiplying a given basis with a unimodular matrix $\mathbf{U} \in \operatorname{GL}_n(\mathbb{Z})$ to get a reduced basis $\tilde{\mathbf{B}} \triangleq \bar{\mathbf{B}}\mathbf{U}$. For a lattice-reduction-aided detector, we first rewrite Eq. (3) as:

$$\mathbf{y} = \tilde{\mathbf{B}}(\mathbf{U}^{-1}\mathbf{x}) + \mathbf{w}.$$

To make the unimodular transform compact for the QAM constellation, we need to scale and shift signal vector \mathbf{x} to get $\mathbf{x} \leftarrow (\mathbf{x} + \mathbf{1}_{n \times 1})/2$, so that the constraint on \mathbf{x} become a consecutive integer set Ξ^n . Let $\mathbf{y} \leftarrow (\mathbf{y} + \tilde{\mathbf{B}}\mathbf{U}^{-1}\mathbf{1}_{n \times 1})/2$, then the inferred signal vector is given by:

$$\hat{\mathbf{x}} = 2\mathcal{Q}_{\Xi^n}(\mathbf{U}\mathcal{Q}_{\mathbb{Z}^n}(\mathcal{E}(\mathbf{y}, \tilde{\mathbf{B}}))) - \mathbf{1}_{n \times 1},$$
(5)

where $\mathcal{E}(\mathbf{y}, \mathbf{B})$ denotes a low-complexity detector that could be zero-forcing (ZF) or successive-interference-cancellation (SIC), and $Q(\cdot)$ denotes a quantization function with respect to its subscript. Given certain information about the signal vector, the detectors can be implemented under an minimum-meansquare-error (MMSE) principle. The MMSE-based ZF/SIC detectors are similarly given by extending the size of the system: $\mathbf{y} \leftarrow [\mathbf{y}^{\top}, \mathbf{0}_{1\times n}]^{\top}, \ \mathbf{\bar{B}} \leftarrow [\mathbf{\bar{B}}^{\top}, \sigma/\sigma_s \mathbf{I}_n]^{\top}, \ \text{with } \sigma_s^2$ referring to the variance of a signal symbol.

C. The objective in lattice reduction

Hereby we explain the design criteria of lattice reduction used in MIMO detection. For a set of linearly independent vectors $\bar{\mathbf{B}} = [\bar{\mathbf{b}}_1, \dots, \bar{\mathbf{b}}_n]$, we define its fundamental parallelepiped as

$$\mathcal{P}(\bar{\mathbf{B}}) = \left\{ \sum_{i=1}^{n} c_i \bar{\mathbf{b}}_i \mid -1/2 \le c_i \le 1/2 \right\}.$$

Choosing $\mathcal{E}(\mathbf{y}, \mathbf{B})$ as the SIC [32] detector, then the pairwise error probability P_e based on (5) becomes

$$P_{e} = 1 - \Pr(\mathbf{w} \in \mathcal{P}(\bar{\mathbf{B}}^{*}))$$

$$= 1 - \prod_{i=1}^{n} \Pr(|\mathbf{w}^{\top} \bar{\mathbf{b}}_{i}^{*}| < ||\bar{\mathbf{b}}_{i}^{*}||^{2}/2)$$

$$= 1 - \prod_{i=1}^{n} \operatorname{erf}\left(\frac{||\bar{\mathbf{b}}_{i}^{*}||}{2\sqrt{2}\sigma}\right)$$

$$\leq 1 - \prod_{i=1}^{n} \operatorname{erf}\left(\frac{1}{2\sqrt{2}\sigma} ||\mathbf{d}_{i}||\right)$$
(6)

where the last inequality comes from $\|\bar{\mathbf{b}}_i^*\| = \|\pi_{\bar{\mathbf{b}}_1,\ldots,\bar{\mathbf{b}}_{i-1}}(\bar{\mathbf{b}}_i)\| \geq \|\pi_{\bar{\mathbf{b}}_1,\ldots,\bar{\mathbf{b}}_{i-1},\bar{\mathbf{b}}_i,\ldots,\bar{\mathbf{b}}_n}(\bar{\mathbf{b}}_i)\| = 1/\|\mathbf{d}_i\|,$ and \mathbf{d}_i is the *i*th vector in the dual basis of Λ^{\dagger} .

From (6), it becomes clear that the upper bound on P_e is mainly controlled by the lengths of vectors in the dual basis, i.e., $\|\mathbf{d}_1\|, \ldots, \|\mathbf{d}_n\|$. Based on this observation, we can solve/approximate the following problem in the dual lattice to attain better error rate performance for the above lattice-reduction-aided SIC detector.

Definition 1 (SBP). The smallest basis problem (SBP) is, given a lattice Λ , find the basis with the smallest orthogonality defect.

To address SBP, a designed reduction algorithm should make all basis vectors as short as possible. Moreover, since the basis dimension is in the order of tens or hundreds in large MIMO, we need a low-complexity lattice reduction algorithm that reduces the basis with satisfactory performance.

III. SEQUENTIAL REDUCTION FRAMEWORK

The fundamental principle of sequential reduction is to reduce a basis vector by using all other vectors that span a sublattice. In the new method, given an input basis \mathbf{B}^1 , we sequentially solve $\mathbf{s}_i = \varepsilon \text{CVP}(\mathbf{b}_i, \mathbf{B}_{[n]\setminus i})$ with $[n] \setminus i =$ $\{1, ..., n\} \setminus i$. For each \mathbf{s}_i , we test whether the residue distance is shorter: $||\mathbf{b}_i - \mathbf{s}_i||^2 < \tau ||\mathbf{b}_i||^2$, where $\tau \in (0, 1]^2$ is a parameter to control the complexity. If this holds, we update \mathbf{b}_i by $\mathbf{b}_i \leftarrow \mathbf{b}_i - \mathbf{s}_i$. Here both $\mathbf{s}_i = \mathbf{0}$ and the \mathbf{s}_i that makes $||\mathbf{b}_i - \mathbf{s}_i|| = ||\mathbf{b}_i||$ are declared as ineffective attempts. A threshold parameter m is set to count these useless trials. The algorithm terminates if m > n, which means no more vectors can be further reduced. The general form of sequential reduction is summarized in Algorithm 1.

An SR algorithm maintains a lattice basis due to the following reason. In round m, suppose $\sum_{k \in [n] \setminus i} c_k \mathbf{b}_k$ is a valid reduction on \mathbf{b}_i , then the lattice basis updating process becomes $\mathbf{B} \leftarrow \mathbf{BT}^m$, with $T_{k,k}^m = 1 \forall k \in [n], T_{k,i}^m = -c_k \forall k \in [n] \setminus i$ and all other entries are zeros. Since \mathbf{T}^m is an integer matrix with determinant 1, \mathbf{T}^m is unimodular, and the composition of the transform matrices from different rounds maintains a unimodular matrix.

If an exact CVP oracle is chosen in line 4 of Algorithm 1, we call the algorithm SR-CVP. By choosing other approximate

¹Unless otherwise specified, **B** is chosen from the dual of a channel matrix.

 $^{^2}$ Choosing $\tau>1$ may make the algorithm diverge.

Algorithm 1: The general form of an SR algorithm.

Input: lattice basis $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n]$, complexity threshold τ ; Output: reduced lattice basis B. i = 0, m = 1;2 while $m \leq n$ do $i \leftarrow (i \mod n) + 1;$ \triangleright The column index; 3 $\mathbf{s}_i = \varepsilon \mathrm{CVP}(\mathbf{b}_i, \mathbf{B}_{[n]\setminus i});$ ▷ Exact/approximated CVP 4 solvers; if $||{\bf b}_i - {\bf s}_i||^2 < \tau ||{\bf b}_i||^2$ then 5 $\mathbf{b}_i \leftarrow \mathbf{b}_i - \mathbf{s}_i;$ 6 7 m = 1;else 8 9 $m \leftarrow m+1;$

CVP solvers, we can obtain other variants that have lower complexity. As shown in Fig. 1, SR encompasses SR-CVP, SR-Pair and SR-Hash. The red box in the figure denotes SR, whose SR-CVP, SR-Pair and SR-Hash algorithms feature decreasing complexity. Their analogies in the conventional KZ framework are shown in the black box.



Fig. 1: SR contains algorithms with different performance-complexity trade-offs.

A. Basis properties of SR-CVP

We need to understand the performance limits of SR by first analyzing SR-CVP. Hereby we set $\tau = 1$ in the analysis for brevity. When no more attempts using $\mathbf{s}_i = \text{CVP}(\mathbf{b}_i, \mathbf{B}_{[n]\setminus i})$ can further reduce the basis in the algorithm, for all $\mathbf{s}_i \in \Lambda(\mathbf{B}_{[n]\setminus i})$ we have

$$\underbrace{\|\mathbf{b}_{i}\|^{2}}_{\text{term 1}} \leq \|\mathbf{b}_{i} - \mathbf{s}_{i}\|^{2}$$

$$= \|\pi_{\mathbf{B}_{[n]\setminus i}}^{\perp}(\mathbf{b}_{i}) + \pi_{\mathbf{B}_{[n]\setminus i}}(\mathbf{b}_{i}) - \mathbf{s}_{i}\|^{2}$$

$$= \underbrace{\left\|\pi_{\mathbf{B}_{[n]\setminus i}}^{\perp}(\mathbf{b}_{i})\right\|^{2}}_{\text{term 2}} + \underbrace{\left\|\pi_{\mathbf{B}_{[n]\setminus i}}(\mathbf{b}_{i}) - \mathbf{s}_{i}\right\|^{2}}_{\text{term 3}}, \quad (7)$$

where the second equality is due to Pythagoras' theorem. Note that SR-CVP provides the tightest constraint on term 3, and approximations of CVP oracles also distinguish themselves on the same term. Based on (7), we can prove the following theorem that consists of upper bounds for the basis length and the orthogonality defect.

Theorem 2. For any dimension $n \le 4$, an SR-CVP reduced basis satisfies:

$$\mathcal{L}(\mathbf{B}) \leq \sqrt{\frac{4n}{5-n}}\lambda_n(\mathbf{B}),$$
 (8)

$$\eta(\mathbf{B}) \leq \left(\frac{4}{5-n}\right)^{n/2} \frac{\lambda_n^n(\mathbf{B})}{\lambda_1^n(\mathbf{B})}.$$
(9)

Proof. We first show upper bounds for terms 2 and 3 in (7), respectively. By constructing a sublattice $\Lambda(\mathbf{B}')$ from vectors with lengths $\lambda_1(\mathbf{B}), ..., \lambda_n(\mathbf{B})$ in $\Lambda(\mathbf{B})$, the covering radius satisfies

$$\rho(\mathbf{B}) = \max_{\mathbf{x}} \operatorname{dist}(\mathbf{x}, \Lambda(\mathbf{B}))$$

$$\leq \max_{\mathbf{x}} \operatorname{dist}(\mathbf{x}, \Lambda(\mathbf{B}'))$$

$$\leq 1/2 \sqrt{\sum_{i=1}^{n} \lambda_i^2(\mathbf{B})},$$

where the last inequality is obtained after applying Babai's nearest plane algorithm [33]. Since the residue distance of CVP is upper bounded by the covering radius of the sublattice $\Lambda(\mathbf{B}_{[n]\setminus i})$, we have for term 3 that

$$\begin{aligned} \left\| \pi_{\mathbf{B}_{[n]\setminus i}}(\mathbf{b}_{i}) - \mathbf{s}_{i} \right\|^{2} &\leq \rho^{2}(\mathbf{B}_{[n]\setminus i}) \\ &\leq \frac{1}{4} \sum_{j \neq i} \lambda_{j}^{2}(\mathbf{B}_{[n]\setminus i}) \\ &\leq \frac{1}{4} \sum_{j \neq i} \|\mathbf{b}_{j}\|^{2} \,. \end{aligned}$$
(10)

Regarding term 2, we use QR decomposition to get $[\mathbf{B}_{[n]\setminus i}, \mathbf{b}_i] = \mathbf{QR}$, from which we obtain $\left\| \pi_{\mathbf{B}_{[n]\setminus i}}^{\perp}(\mathbf{b}_i) \right\| = |r_{n,n}|$. Now w.l.o.g. assume that the successive minima $\lambda_1(\mathbf{B}), ..., \lambda_n(\mathbf{B})$ come from vectors $\mathbf{v}_1 \triangleq [\mathbf{B}_{[n]\setminus i}, \mathbf{b}_i] \mathbf{c}_1, ..., \mathbf{v}_n \triangleq [\mathbf{B}_{[n]\setminus i}, \mathbf{b}_i] \mathbf{c}_n$. To produce n linearly independent vectors, there exists at least one vector denoted as \mathbf{c}_k whose nth entry $c_{k,n}$ is nonzero. Then we have $\|\mathbf{Rc}_k\|^2 = \lambda_k^2(\mathbf{B}) \leq \lambda_n^2(\mathbf{B})$. Together with $\|\mathbf{Rc}_k\|^2 = c_{k,n}^2 r_{n,n}^2 + \sum_{j=1}^{n-1} v_{n,j}^2 \geq \|\pi_{\mathbf{B}_{[n]\setminus i}}^{\perp}(\mathbf{b}_i)\|^2$, it arrives at

$$\left\|\pi_{\mathbf{B}_{[n]\setminus i}}^{\perp}(\mathbf{b}_{i})\right\|^{2} \leq \lambda_{n}^{2}(\mathbf{B}).$$
(11)

By substituting (10) and (11) to (7) for all basis vectors, we have

$$\begin{cases} \|\mathbf{b}_{1}\|^{2} \leq \lambda_{n}^{2}(\mathbf{B}) + \frac{1}{4} \sum_{j \neq 1} \|\mathbf{b}_{j}\|^{2}, \\ \vdots \\ \|\mathbf{b}_{n}\|^{2} \leq \lambda_{n}^{2}(\mathbf{B}) + \frac{1}{4} \sum_{j \neq n} \|\mathbf{b}_{j}\|^{2}. \end{cases}$$

The sum of these n inequalities yields

$$\sum_{i=1}^{n} \|\mathbf{b}_{i}\|^{2} \le n\lambda_{n}^{2}(\mathbf{B}) + \frac{n-1}{4}\sum_{i=1}^{n} \|\mathbf{b}_{i}\|^{2}$$

If $n \leq 4$, we have

$$\sum_{i=1}^{n} \|\mathbf{b}_{i}\|^{2} \le \frac{4n}{5-n} \lambda_{n}^{2}(\mathbf{B}).$$
(12)

Based on Eq. (12), the longest vector in the basis can be trivially bounded as

$$l(\mathbf{B}) \le \sqrt{\frac{4n}{5-n}} \lambda_n(\mathbf{B})$$

To analyze the orthogonal defect, we apply the arithmetic mean-geometric mean inequality on (12) to get

$$\prod_{i=1}^{n} ||\mathbf{b}_{i}|| \leq \left(\frac{1}{n} \sum_{i=1}^{n} ||\mathbf{b}_{i}||^{2}\right)^{n/2} \leq \left(\frac{4}{5-n}\right)^{n/2} \lambda_{n}^{n}(\mathbf{B}).$$
(13)

Clearly the volume of the lattice is lower bounded by λ_1^n (**B**) for $n \leq 4$, so along with (13) we obtain (9).

If we alternatively set $\tau < 1$, then upon termination of SR we have $||\mathbf{b}_i||^2 \le 1/\tau ||\mathbf{b}_i - \mathbf{s}_i||^2$. Along with the techniques used in Theorem 2, we obtain

$$l(\mathbf{B}) \le \sqrt{\frac{4n}{4\tau - n + 1}} \lambda_n(\mathbf{B}).$$
(14)

Since we have to ensure that the denominator $4\tau - n + 1$ is larger than 0, we claim that inequality (14) holds if $n < 4\tau + 1$. If the CVP oracle is replaced by another suboptimal solver referred to as ε CVP, then when bounding term 3 we have

$$\left\|\pi_{\mathbf{B}_{[n]\setminus i}}(\mathbf{b}_{i})-\mathbf{s}_{i}\right\|^{2}\leq \varepsilon\rho^{2}(\mathbf{B}_{[n]\setminus i}).$$

Similarly to the above, it yields

$$l(\mathbf{B}) \le \sqrt{\frac{4n}{4 - \varepsilon n + \varepsilon}} \lambda_n(\mathbf{B}), \tag{15}$$

in which $n < 4/\varepsilon + 1$.

Let θ_i be the angle between \mathbf{b}_i and the subspace $\operatorname{span}(\mathbf{B}_{[n]\setminus i})$, and define $\theta_{\max} \triangleq \max_i \theta_i$. Such a maximum angle between basis vectors and subspaces can also be bounded, as shown in the following theorem.

Theorem 3. An SR-CVP reduced basis satisfies $\cos^2 \theta_{\max} \leq \frac{n-1}{4}$.

Proof: Based on (7) and (10) we have

$$\|\mathbf{b}_{i}\|^{2} - \left\|\pi_{\mathbf{B}_{[n]\setminus i}}^{\perp}(\mathbf{b}_{i})\right\|^{2} \leq \left\|\pi_{\mathbf{B}_{[n]\setminus i}}(\mathbf{b}_{i}) - \mathbf{s}_{i}\right\|^{2} \leq \frac{1}{4} \sum_{j \neq i} \|\mathbf{b}_{j}\|^{2}$$
(16)

It then follows from $\|\mathbf{b}_i\|^2 \cos^2 \theta_i = \|\mathbf{b}_i\|^2 - \left\|\pi_{\mathbf{B}_{[n]\setminus i}}^{\perp}(\mathbf{b}_i)\right\|^2$ that

$$\|\mathbf{b}_i\|^2 \cos^2 \theta_{\max} \le \|\mathbf{b}_i\|^2 \cos^2 \theta_i \le \frac{1}{4} \sum_{j \ne i} \|\mathbf{b}_j\|^2$$

Similarly to the techniques used in proving Theorem 2, we sum (16) for i = 1, ..., n to get

$$\cos^2\theta_{\max} \le \frac{n-1}{4}$$

Clearly the above theorem is non-trivial when $n \leq 4$, and this will come in handy when attacking a counter example in subsection IV-D.

B. Discussions

 Comparison with η-Greedy reduction [34, Fig.5] (also noted as ELR⁺-SLV in [28]). Rather than applying CVP for all vectors, η-Greedy reduction only performs CVP for the longest basis vector . According to its definition [34], it is only a special case of SR-CVP and all SR-CVP reduced basis must be greedy-reduced. For example, consider the following basis

2	0	0	0	1
0	2	0	0	1
0	0	2	0	1
0	0	0	2	1
0	0	0	0	ε

with parameter $\varepsilon \in (0, 1)$. The shortest vector $\begin{bmatrix} 0 & 0 & 0 & \pm 2\varepsilon \end{bmatrix}^{\top}$ cannot be reached by greedy reduction. Specifically, by using $1 \times \mathbf{b}_5$ as the query point, η -Greedy cannot find $2\mathbf{b}_5 - \mathbf{b}_1 - \mathbf{b}_2 - \mathbf{b}_3 - \mathbf{b}_4$ and $-2\mathbf{b}_5 + \mathbf{b}_1 + \mathbf{b}_2 + \mathbf{b}_3 + \mathbf{b}_4$. In contrast, SR-CVP additionally considers the cases of using $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$, and \mathbf{b}_4 as query points. A shortest vector $\mathbf{v} = \sum_{i=1}^{n} c_i \mathbf{b}_i$ with at least one coefficient $c_k = \pm 1$ must be contained in the SR-CVP reduced basis.

- Comparison with KZ and its variants [16], [35]. Recall that a basis B is called KZ reduced if it satisfies the size reduction conditions, and π[⊥]_{B[i-1]}(b_i) is the shortest vector of the projected lattice π[⊥]_{B[i-1]}([b_i,...,b_n]) for 1 ≤ i ≤ n [35]. For a KZ reduced basis, it satisfies [35] ||b_i|| ≤ ^{√i+3}/₂ λ_i(B), 1 ≤ i ≤ n. Though boosted KZ [16] can solve the length increasing issue caused by size reduction, tuning π[⊥]_{B[i-1]}(b_i) to be the shortest vector in the projected lattice can still make the basis longer. On the contrary, this issue is totally avoided in SR-CVP.
- 3) Comparison with Minkowski reduction. Recall that a lattice basis **B** is called Minkowski reduced if for any integers $c_1, ..., c_n$ such that $c_i, ..., c_n$ are altogether coprime, it has $\|\mathbf{b}_1 c_1 + \cdots + \mathbf{b}_n c_n\| \ge \|\mathbf{b}_i\|$ for $1 \le |\mathbf{b}_n|$ $i \leq n$ [15]. For a Minkowski reduced basis, it satisfies [15] $\|\mathbf{b}_i\| \le \max\{1, (5/4)^{(i-4)/2}\} \lambda_i(\mathbf{B}), 1 \le i \le n.$ Whereas Minkowski reduction is optimal as it reaches all the successive minima when n < 4, our results in Theorem 2 only show the SR-CVP reduced basis is not far from the optimal one. Here we argue that SR-CVP has simpler structure. While Minkowski reduction requires solving integer least squares problems with GCD constraints and delicate basis expansion, SR-CVP only involves unconditional CVP solvers and its basis expansion process is trivial. Moreover, the SR-CVP algorithm can be approximately implemented by its many low-complexity siblings in the SR family.

C. Complexity of SR and SR-CVP

We argue that even when the threshold parameter $\tau = 1$, the decrease from $||\mathbf{b}_i||$ to $||\mathbf{b}_i - \mathbf{s}_i||$ can be finitely counted because a lattice is discrete. Therefore we define $\epsilon = \sup_{\mathbf{b}_i, \mathbf{s}_i} \frac{||\mathbf{b}_i - \mathbf{s}_i||}{||\mathbf{b}_i||}$ which satisfies $\epsilon < 1$. As $\sum_{i=1}^n ||\mathbf{b}_i||^2$ is no smaller than $\sum_{i=1}^n \lambda_i^2(\mathbf{B})$ while this metric keeps decreasing for every *n* iterations, the number of calls to the CVP oracle is not larger than $n \log(\frac{||\mathbf{B}||_F^2}{\sum_{i=1}^n \lambda_i(\mathbf{B})})$ with $\tau \le 1$, where $||\mathbf{B}||_F^2$ denotes the Frobenius norm of the input basis, and the log function is over min $\{1/\tau, 1/\epsilon\}$. Therefore we conclude that the number of iterations in SR is polynomial.

Regarding SR-CVP, since the reduction in each round is quite strong, we can use the following heuristic implementation to minimize the number of iterations: first reduce the longest vector (similarly to η -Greedy), then reduce other basis vectors in descending order with n - 1 rounds of CVP. Our simulation results show that this version of SR-CVP is competitive with Minkowski reduction and boosted KZ reduction.

While we can employ a state-of-the-art implementation for CVP, its complexity for a random basis is exponential [36]–[38]. In the next section, we will focus on approximate versions of CVP.

IV. HASH-BASED APPROXIMATION: SR-HASH

A. The nearest neighbor problem in SR-Pair

When the ε CVP subroutine is not implemented with an exact CVP algorithm but rather a pairwise cancellation with the following form:

$$\mathbf{b}_{i} = \arg\min ||\mathbf{b}_{i}^{(j)}||, j = \{1, \dots, N\} \setminus i, \qquad (17)$$
$$\mathbf{b}_{i}^{(j)} = \mathbf{b}_{i} - \lfloor \langle \mathbf{b}_{i}, \mathbf{b}_{j} \rangle / \langle \mathbf{b}_{j}, \mathbf{b}_{j} \rangle] \mathbf{b}_{j},$$

we refer to the whole algorithm as SR-Pair. This algorithm coincides with the element-based reduction in [27]. Although this sub-routine only has a complexity in the order of O(nN), reaching another variant with lower complexity is possible.

Recall the nearest neighbor problem in the field of large dimensional data processing is: given a list of *n*-dimensional vectors $L = {\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_N} \in \mathbb{R}^n$, preprocess *L* in such a way that, when later given a target vector $\mathbf{q} \notin L$, one can efficiently find an element $\mathbf{v} \in L$ which is almost the closest to \mathbf{q} . Since Eq. (17) exactly defines a search for the nearest neighbor of \mathbf{b}_i among the vectors in \mathbf{B} , then it motivates us to reduce this complexity to $O(n \log N)$ based on localitysensitive-hashing (LSH) [39], [40].

Remark 4. If we choose SIC as the ε CVP subroutine, then along with LLL preprocessing we have [33]

$$\left\|\mathbf{b}_{i} - \pi_{\mathbf{B}_{[n]\setminus i}}(\mathbf{b}_{i}) - \mathbf{s}_{i}\right\| \le 2(2/\sqrt{3})^{n-1}\rho(\mathbf{B})$$
(18)

for such an SR-SIC algorithm. However, the computation complexity of this algorithm is still too high as it requires the pre-processing by LLL.

B. Angular LSH

LSH roughly works as follows: first all N candidates are dispatched to different buckets with labels, then when searching the nearest neighbor of a query point \mathbf{q} , we can alternatively do this only for N' candidates that have the same label with \mathbf{q} , where $N' \ll N$. There are label functions fwhich map an *n*-dimensional vector \mathbf{v} to a low-dimensional sketch of \mathbf{v} . For certain distance function D, vectors which are nearby in the sense of D have a high probability of having the same sketch, while vectors which are far away have a low probability of having the same image under f.

To reach this property, we introduce the definition of an LSH family \mathcal{F} .

Definition 5. A family $\mathcal{F} = \{f : \mathbb{R}^n \to \mathbb{N}\}$ of hash functions is said to be (r_1, r_2, p_1, p_2) -sensitive for a similarity measure D if for any $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$, we have i) If $D(\mathbf{u}, \mathbf{v}) \leq r_1$, then $\Pr_{f \in \mathcal{F}}(f(\mathbf{u}) = f(\mathbf{v})) \geq p_1$; ii)If $D(\mathbf{u}, \mathbf{v}) \geq r_2$, then $\Pr_{f \in \mathcal{F}}(f(\mathbf{u}) = f(\mathbf{v})) \leq p_2$.

For the sake of constructing a hash family with $p_1 \approx 1$ and $p_2 \approx 0$, normally one first constructs $p_1 \approx p_2$ and then uses the so called AND- and OR-compositions to turn it into an (r_1, r_2, p'_1, p'_2) -sensitive hash family \mathcal{F}' with $p'_1 > p_1$ and $p'_2 < p_2$, thereby amplifying the gap between p_1 and p_2 . Specifically, by combining k AND-compositions and t OR-compositions, we can turn an (r_1, r_2, p_1, p_2) -sensitive hash family \mathcal{F} into an $(r_1, r_2, 1 - (1 - p_1^k)^t, 1 - (1 - p_2^k)^t)$ sensitive hash family \mathcal{F}' . As long as $p_1 > p_2$, we can always find values of k and t such that $1 - (1 - p_1^k)^t \to 1$ and $1 - (1 - p_2^k)^t \to 0$.

Note that if given a hash family \mathcal{H} which is (r_1, r_2, p_1, p_2) sensitive with $p_1 \gg p_2$, then we can use \mathcal{F} to distinguish between vectors which are at most r_1 away from \mathbf{v} , and vectors which are at least r_2 away from \mathbf{v} with non-negligible probability, by only looking at their hash values. Although large values of k and t can amplify the gap between p_1 and p_2 , large parameters come at the cost of having to compute many hashes and having to store many hash tables in memory. To minimize the overall time complexity, we need the following lemma that shows how to balance k and t. In practice, we can further tune k and t to have the best performance.

Lemma 6 ([41], [42]). Suppose there exists an (r_1, r_2, p_1, p_2) -sensitive family \mathcal{F} . For a list L of size N, let

$$\rho = \frac{\log p_1^{-1}}{\log p_2^{-1}}, \, k = \frac{\log N}{\log p_2^{-1}}, \, t = O(N^{\rho}).$$

Then given a query point \mathbf{q} , with high probability we can either find an element $\mathbf{v} \in L$ such that $D(\mathbf{q}, \mathbf{v}) \leq r_2$, or conclude that with high probability, no element $\mathbf{v} \in L$ with $D(\mathbf{q}, \mathbf{v}) >$ r_1 exist, with the following costs: i) Time for preprocessing the list: $O(kN^{1+\rho})$; ii) Space complexity of the preprocessed data: $O(N^{1+\rho})$; iii) Time for answering a query: $O(N^{\rho})$.

In the sequel, we examine the implementation of LSH based on angular hashing. Angular hashing means generating random hyperplanes $\mathbf{h}_1, \ldots, \mathbf{h}_k$, such that the whole space is sliced into 2^k regions. After that, to find the nearest neighbor of \mathbf{q} , one only compares q to points in the same region \mathcal{R} . Here we introduce the angular distance similarity function

$$D(\mathbf{u}, \mathbf{v}) = \arccos\left(\frac{\mathbf{u}^{\top} \mathbf{v}}{\|\mathbf{u}\| \|\mathbf{v}\|}\right).$$

With this measure two vectors are nearby if their common angle is small. Its corresponding hash family is defined by

$$\mathcal{F} = \left\{ f_{\mathbf{a}} : \, \mathbf{a} \in \mathbb{R}^{n}, \|\mathbf{a}\| = 1 \right\}, f_{\mathbf{a}}(\mathbf{v}) = \begin{cases} 1 & \text{if } \mathbf{a}^{\top} \mathbf{v} \ge 0; \\ 0 & \text{if } \mathbf{a}^{\top} \mathbf{v} < 0. \end{cases}$$

Intuitively, the space that is orthogonal to a defines a hyperplane, and f_{a} maps the two regions separated by this hyperplane to different bits. In particular, for any two angles $\theta_{1} < \theta_{2}$, the family \mathcal{F} is $(\theta_{1}, \theta_{2}, 1 - \frac{\theta_{1}}{\pi}, 1 - \frac{\theta_{2}}{\pi})$ -sensitive. Further with k AND- and t OR- compositions, we have $(\theta_{1}, \theta_{2}, 1 - (1 - (1 - \frac{\theta_{1}}{\pi})^{k})^{t}, 1 - (1 - (1 - \frac{\theta_{2}}{\pi})^{k})^{t})$ -sensitive hash family.

To illustrate LSH and in particular the angular LSH method described above, Fig. 2 shows how hyperplane hashing might work in a 2-D setting. In the figure, we have a list of 8 candidates: $L = {\mathbf{b}_1, \ldots, \mathbf{b}_8}$, and we use k = 2 hyperplanes for t = 2 hash tables. Each table stores the hash keys (labels) along with elements being placed in buckets, where elements having the same keys will be placed in the same buckets. In the two tables, the AND-compositions of 11 respectively correspond to $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ and \mathbf{b}_1 . Based on OR-composition, the nearest neighbor of \mathbf{b}_1 is found inside ${\mathbf{b}_2, \mathbf{b}_3}$.



Fig. 2: Demonstration of LSH.

C. LSH-Based Reduction

Now we show how to incorporate LSH into the sequential reduction algorithm. The pseudo-codes of SR-Hash are presented in Algorithm 2. It first hashes all vectors in lines 2-3. Then inside the loop of the element-based reduction, the search for finding the nearest neighbor of \mathbf{b}_i is within $\mathbf{C} = \bigcup_{l=1}^t T_l(f_l(\pm \mathbf{b}_i))$. Every time when a shorter \mathbf{b}_i is found, its hash labels and positions in buckets are updated in lines 11 and 13.

In summary, SR-Hash can be seen as a generalization of the naive brute-force search inside SR-Pair for finding nearest neighbors, as k = 0, t = 1 corresponds to checking all other basis vectors for nearby vectors, while increasing both k and t leads to fewer comparisons but a higher cost of computing hash keys and checking buckets.

Algorithm 2: The SR-Hash algorithm. **Input:** original lattice basis $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n]$, complexity threshold τ , LSH parameters t, k. **Output:** Reduced basis $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of Λ . 1 Initialize t empty hash tables $(T_l)_{l=1}^{\iota}$, each has k random hash functions $f_{l,1}, \ldots f_{l,k} \in \mathcal{F}$; 2 for $i = 1 \cdots n$ do 3 Add \mathbf{b}_i to all hash tables $(T_l)_{l=1}^t$, with hash values $(f_l(\mathbf{b}_i))_{l=1}^t$ and vectors in the same bucket noted as $T_l(f_l(\mathbf{b}_i));$ 4 i = 0, m = 1;5 while m < n do 6 $i \leftarrow (i \mod n) + 1;$ \triangleright The column index; Obtain the set of candidates $\mathbf{C} = \bigcup_{l=1}^{t} T_l \left(f_l \left(\pm \mathbf{b}_i \right) \right);$ 7 $\mathbf{c}_{l} = \arg\min_{\mathbf{c}_{l} \in \mathbf{C}} \|\mathbf{b}_{i} - \lfloor \langle \mathbf{b}_{i}, \mathbf{c}_{l} \rangle / \langle \mathbf{c}_{l}, \mathbf{c}_{l} \rangle \|^{2};$ 8 $\mathbf{s}_i = |\langle \mathbf{b}_i, \mathbf{c}_l \rangle / \langle \mathbf{c}_l, \mathbf{c}_l \rangle] \mathbf{c}_l;$ 9 if $||{\bf b}_i - {\bf s}_i||^2 < \tau ||{\bf b}_i||^2$ then 10 Remove \mathbf{b}_i from all hash tables; 11 $\mathbf{b}_i \leftarrow \mathbf{b}_i - \mathbf{s}_i;$ 12 Add \mathbf{b}_i to all hash tables; 13 14 m = 1;else 15 $m \leftarrow m + 1;$ 16

D. Discussions

 Comparison with SR-CVP. Here we emphasize that SR-Pair/SR-Hash is only a weak approximation for SR-CVP, and these low complexity algorithms may have quite inferior performance. Consider the counter example given for ELR [27] (the same as SR-Pair). Clearly SR-Pair/SR-Hash is unable to reduce a basis whose Gram matrix is

$$\mathbf{G} = \begin{bmatrix} 1 & 0.5 - \nu & 0.5 - \nu \\ 0.5 - \nu & 1 & -0.5 + \nu \\ 0.5 - \nu & -0.5 + \nu & 1 \end{bmatrix}$$

with $\nu \rightarrow 0$. Under spherical coordinate system of (r, ϱ, φ) with r = 1, $\varrho = \pi/3$, and $\varphi = \pi/2 - \nu$, the lattice basis **A** corresponded to **G** (up to a unitary transform) is given by

$$\mathbf{A} = \begin{bmatrix} \sin\varphi\cos(\pi/3) & -\sin\varphi\cos(\pi/3) & 1\\ \sin\varphi\sin(\pi/3) & \sin\varphi\sin(\pi/3) & 0\\ \cos\varphi & -\cos\varphi & 0 \end{bmatrix}.$$
(10)

This basis has an angle $\theta_i < \nu \to 0$ between any \mathbf{a}_i and span $(\mathbf{A}_{[3]\setminus i})$, and $\eta(\mathbf{A}) = \infty$ if $\nu \to 0$. If \boldsymbol{A} is reduced by using SR-CVP, we have $\theta_{\max} \ge \pi/4$ according to Theorem 3, so \mathbf{A} is not a stable basis for SR-CVP. Moreover, the actual reduced basis has the following form:

$$\tilde{\mathbf{A}} = \begin{bmatrix} 2\sin\varphi\cos(\pi/3) - 1 & -\sin\varphi\cos(\pi/3) & 1\\ 0 & \sin\varphi\sin(\pi/3) & 0\\ 2\cos\varphi & -\cos\varphi & 0 \end{bmatrix}.$$

Its OD is

$$\eta(\tilde{\mathbf{A}}) = \frac{\sqrt{4\cos^2\varphi + \sin^2\varphi - 2\sin\varphi + 1}}{\sqrt{3}\sin\varphi\cos\varphi}$$

when given $\varphi = \pi/2 - 10^{-4}$, we have $\eta(\tilde{\mathbf{A}})|_{\varphi=\pi/2-10^{-4}} = 1.1547$. Therefore, the proposed low-complexity SR algorithms are only feasible for bases whose input vectors are dense in some directions. Our simulation results and Appendix A will show that the dual lattice basis in MIMO detection is one example of this.

- 2) Comparison with LLL and its variants [19], [22], [24]. Note that the worst case complexity of LLL for bases in the real field is unbounded [43], and the variants that control the order of swaps or a selective implementation of size reduction cannot remove this curse. On the contrary, SR variants with a polynomial time ε CVP routine can enjoy the overall polynomial-time complexity. Regarding performance bounds, LLL and its variants (the maintains the Siegel condition and size reduction condition) often have bounds of the form $l(\mathbf{B}) \leq 2^{n-1}\lambda_n(\mathbf{B})$, while SR-Pair and SR-Hash are heuristic.
- 3) Comparison with Seysen reduction [14]. Rather than minimizing the orthogonality defect of a basis, a metric called Seysen's measure can reflect whether both the primal and dual bases are short: ∑_{i=1}ⁿ ||**b**_i||² ||**d**_i||². Seeking for the global minimum of this metric is extremely hard; when referring to Seysen's algorithm [25], it is the one that finds a local minimum of ∑_{i=1}ⁿ ||**b**_i||² ||**d**_i||² without any theoretical performance guarantee. Similarly to SR-Pair, Seysen's algorithm performs basis updates in a pair-wise manner:

$$\mathbf{b}_j = \mathbf{b}_j + c_{i,j} \mathbf{b}_i, i \neq j,$$

with $c_{i,j} = \lfloor \frac{1}{2} \left(\frac{\langle \mathbf{d}_i, \mathbf{d}_j \rangle}{\|\mathbf{d}_i\|^2} - \frac{\langle \mathbf{b}_i, \mathbf{b}_j \rangle}{\|\mathbf{b}_i\|^2} \right) \rceil$. Due to the additional inner product calculation in the dual basis, Seysen's algorithm is more complicated than SR-Pair, and it does not support the hash-based implementation. Moreover, in large (≥ 35) dimensions Seysen's algorithm often halts at a local minimum [14, P.375]. Since the error rate performance is only controlled by the length of the dual basis, our empirical results also show that Seysen's algorithm is not competitive for large dimensions.

V. SIMULATION RESULTS

A. Performance of SR-CVP

Hereby we employ the OD's to compare SR-CVP with other strong lattice reduction algorithms, including the boosted Korkin-Zolotarev reduction noted as "bKZ", the Minkowski reduction noted as "Minkowski", and the η -Greedy reduction [34, Fig.5] noted as " η -Greedy". Results are averaged over 1×10^4 Monte-Carlo runs, and SR-CVP is implemented by the heuristic version in subsection III-C.

Fig. 3 plots dimension versus OD for distinct algorithms for the primal and dual of a Gaussian random matrix with





Fig. 3: The orthogonal defects of different types of strong reduction.

entries from $\mathcal{N}(0,1)$, respectively. The figure shows that ODs of SR-CVP, bKZ and Minkowski reduced bases are almost indistinguishable. η -Greedy has the worst performance as expected, because it is not designed to minimized all basis vectors. Since Minkowski reduction is the state-of-the-art algorithm for generating the shortest basis in practice, our results show that SR-CVP practically reaches optimality as well.

Fig. 4 plots the averaged number of CVP runs in Fig. 3 when using η -Greedy and SR-CVP. It is known that both Minkowski and bKZ cost around *n* oracles for the shortest vector problem (SVP) or CVP. Fig. 4 reflects that SR-CVP actually needs fewer than *n* rounds of CVP, and is only slightly more complicated than η -Greedy.

B. SR-Hash vs. SR-Pair and LLL variants

In this subsection, we study the complexity/performance tradeoffs of different types of weak lattice reduction. The modulation is set as 16 QAM, and the results are obtained from 1×10^4 Monte Carlo runs. We denote the zero-forcing detector by "ZF", the successive interference cancellation detector by "SIC", and lattice-reduction-aided detectors with prefixes: "LLL-SIC/ZF" [32], "bLLL-SIC/ZF" [16], "SR-Pair-SIC/ZF" (this paper), "SR-Hash-SIC/ZF" (this paper), and "Seysen-SIC/ZF" [26]. Here comparisons are made for major lattice-reduction-aided methods in large-scale MIMO systems, because they represent pre-processing based methods that may attain the diversity order of ML detection [6], [44].

1) i.i.d. channels: Assume that each entry of the channel matrix is chosen from a standard normal distribution $\mathcal{CN}(0,1)$. Fig. 5 plots the bit error rate (BER) performance of different uncoded MIMO detectors in a real domain $2n_T \times 2n_R = 60 \times 60$ MIMO system. Here the linear detectors are



Fig. 4: The number of effective CVP runs in η -Greedy and SR-CVP.

implemented with the MMSE criterion. Parameters in LSH are chosen as $t = \lfloor n^{0.585} \rfloor = 11$, $k = \lfloor \log n \rfloor = 6$.

In the high SNR region of Fig. 5-(a), we observe that, in addition to the well-known fact that ZF, SIC and Seysen-SIC fail to achieve the full diversity order, b-LLL-SIC, SR-Pair-SIC and SR-Hash-SIC all attain approximately 1dB gain over LLL-SIC. As for Fig. 5-(b), the variants of SR both outperform conventional and boosted LLL algorithms. Both sub-figures indicate that SR-Hash gets very close to SR-Pair.

The complexity of implementing the lattice reduction algorithms is plotted in Fig. 6, where sub-figure (a) is for the effective channel matrix under the MMSE criterion, and subfigure (b) under the ZF criterion. Considering the difficulty in analyzing the number of floating-point operations for hash operations, here we measure the complexity by the number of vector comparisons. This equals to the number of iterations times: the size of the basis for SR-Pair, the number of vectors in the same buckets for SR-Hash, and to the size of vectors for doing size-reductions for both LLL and bLLL. From Fig. 6-(a), we observe that the LLL variants are not affected by SNR in the MMSE matrix, and Seysen, SR-Pair and SR-Hash gradually increase with the rise of SNR. This shows the complexity of Seysen, SR-Pair and SR-Hash are dependent on the quality of the input bases. Regarding the stationary lines in Fig. 6-(b), the numbers of comparisons of Seysen, SR-Pair and SR-Hash reflect the asymptotic values of their counterparts in Fig. 6-(a). Both subfigures reveal that the hash method helps to reduce the complexity of SR-Pair significantly. A natural question that arises here is whether the complexity dependency of SR-Pair&SR-Hash on input bases may lead to inferior performance at low SNR. To address this question, we plot the SNR versus OD relations of different reduction algorithms in Fig. 7. We observe from the figure that even at low SNR, SR-Pair&SR-Hash featuring low complexity still



Fig. 5: The BER performance of different detectors in large MIMO.

outperform Seysen and LLL in terms of OD.

2) Correlated Channels: Results in the last example were obtained for i.i.d. frequency-flat Rayleigh fading channels. The performance of MIMO systems in realistic radio environments however sometimes depends on spatial correlation. Therefore, we investigated the effect of channel correlation on the performance of the new reduction algorithms. Based on [45], the spatially correlated channel is modeled as

$$\mathbf{B}_{c}=\Psi\mathbf{B}_{c},$$

where $\Psi \in \mathbb{R}^{n_R \times n_R}$ is the correlation matrix defined by

$$\Psi = \begin{bmatrix} 1 & \rho & \dots & \rho^{n_R-1} \\ \rho & 1 & \dots & \rho^{n_R-2} \\ \vdots & \vdots & \ddots & \vdots \\ \rho^{n_R-1} & \rho^{n_R-2} & \dots & 1 \end{bmatrix},$$

and ρ refers to the spatial correlation coefficient.

With the same chosen parameters in the algorithm as those for i.i.d. channels, Fig. 8 demonstrates the BER performances against SNR in correlated channels respectively with $\rho = 0.1$ and $\rho = 0.3$. It reveals that, as ρ increases, the SR aided detectors suffer from more severe performance degradation



Fig. 6: The complexity of different lattice reduction algorithms in i.i.d. channels.



Fig. 7: The ODs of MMSE matrices reduced by different algorithms.

than the LLL aided methods, although the BER gaps between SR variants and LLL variants are very small. This is not unexpected because we do have examples showing SR-Pair/SR-Hash cannot reduce certain matrices (e.g., the matrix in (19)). Lastly, as plotted in Fig. 9, the complexity of SR-Pair/SR-Hash is still much lower than those of LLL variants and Seysen, and the proposed SR-Hash has much lower complexity than SR-Pair.

VI. CONCLUSIONS AND FUTURE WORK

To summarize, we have unveiled a new lattice reduction family called sequential reduction, which enjoys a polynomial number of iterations. Theoretical bounds on basis lengths and orthogonality defects are derived under the premise that an exact CVP subroutine has been invoked. Though we only manage to prove these results for small dimensions, they still provide insights on understanding the performance of such a class of



Fig. 8: The BER performance of lattice-reduction-aided SIC detectors in correlated channels with $\rho = 0.1$ and $\rho = 0.3$.

algorithms. Within the SR framework, the SR-Hash method can serve as an effective subprogram, and simulation results show that the complexity-performance trade-off outperforms those of SR-Pair and LLL variants in large MIMO detection.

We believe that the studies we initiated here, only scratch the tip of the iceberg about the new lattice reduction family. Many important questions remain to be answered. Research on the interactions and combinations of SR with other techniques such as floating-point arithmetic [46], [47], randomized detection algorithms [31], [48], success probability analysis [49], [50], and numerous other topics is now being pursued.

APPENDIX A On the type of bases feasible for SR-Pair&SR-Hash

We first argue that a large dimensional Gaussian random basis is always SR-CVP reduced, and thus being SR-Pair and SR-Hash reduced. The inability to change such bases is however not a problem because these bases are close to being orthogonal.



Fig. 9: The complexity of lattice reduction algorithms in correlated channels with $\rho = 0.1$ and $\rho = 0.3$.

Proposition 7. For a Gaussian random basis whose entries follow the distribution $\mathcal{N}(0,1)$, the probability that it is not SR-CVP reduced goes to zero as $n \to \infty$.

Proof: We need to show that for all choices of coefficients $a'_i s$ in \mathbb{Z} with at least one nonzero a_i , the probability

$$\Pr\left(\left\|\mathbf{b}_{1}+\sum_{i=2}^{n}\mathbf{b}_{i}a_{i}\right\|^{2}\leq\left\|\mathbf{b}_{1}\right\|^{2}\right)$$

vanishes as the problem size n increases. Since $\sum_{i=2}^{n} \mathbf{b}_{i}a_{i}$ is an isotropic Gaussian random vector with covariance $\mathbb{E}\left(\left(\sum_{i=2}^{n} \mathbf{b}_{i}a_{i}\right)\left(\sum_{i=2}^{n} \mathbf{b}_{i}a_{i}\right)^{\top}\right) = \left(\sum_{i=2}^{n} a_{i}^{2}\right)\mathbf{I}_{n}$, then for any $\beta > 0$,

$$\Pr\left(\left\|\mathbf{b}_{1}+\sum_{i=2}^{n}\mathbf{b}_{i}a_{i}\right\|^{2} \leq \|\mathbf{b}_{1}\|^{2}\right)$$

$$\leq \mathbb{E}\left(e^{-\beta\left(\left\|\mathbf{b}_{1}+\sum_{i=2}^{n}\mathbf{b}_{i}a_{i}\right\|^{2}-\|\mathbf{b}_{1}\|^{2}\right)}\right),$$

$$=\int \frac{d\mathbf{x}d\mathbf{v}}{(2\pi)^{n}}$$

$$e^{-\frac{1}{2}\left[\mathbf{v}^{\top},\mathbf{x}^{\top}\right]\left[\begin{array}{c}\mathbf{I}_{n} & 2\sqrt{\sum_{i=2}^{n}a_{i}^{2}}\beta\mathbf{I}_{n}\\ 2\sqrt{\sum_{i=2}^{n}a_{i}^{2}}\beta\mathbf{I}_{n} & \left(1+2\beta\sum_{i=2}^{n}a_{i}^{2}\right)\mathbf{I}_{n}\end{array}\right]\left[\begin{array}{c}\mathbf{v}\\\mathbf{x}\end{array}\right]$$

$$=\det\left(\left[\begin{array}{c}\mathbf{I}_{n} & 2\sqrt{\sum_{i=2}^{n}a_{i}^{2}}\beta\mathbf{I}_{n}\\ 2\sqrt{\sum_{i=2}^{n}a_{i}^{2}}\beta\mathbf{I}_{n} & \left(1+2\beta\sum_{i=2}^{n}a_{i}^{2}\right)\mathbf{I}_{n}\end{array}\right]\right)^{-1/2}$$

$$=\left(\frac{1}{1+2\beta\left(1-2\beta\right)\sum_{i=2}^{n}a_{i}^{2}}\right)^{n/2}.$$
(20)

By optimizing over β in the denominator, we have $1 + 2\beta (1-2\beta) \sum_{i=2}^{n} a_i^2 \leq 1 + \frac{1}{4} \sum_{i=2}^{n} a_i^2$. This means we can use $\beta = \frac{1}{4}$ to reach the tightest bound for inequality (20). Therefore, for any $\varepsilon > 0$, we have

$$\lim_{n \to \infty} \Pr\left(\left\| \mathbf{b}_1 + \sum_{i=2}^n \mathbf{b}_i a_i \right\|^2 \le \|\mathbf{b}_1\|^2\right)$$
$$\le \lim_{n \to \infty} \left(\frac{1}{1 + 2\beta (1 - 2\beta) \sum_{i=2}^n a_i^2}\right)^{n/2}$$
$$< \varepsilon.$$

Next, we investigate the reduction on the dual of a Gaussian random basis, which arises in our detection problem. For an input basis \mathbf{B} we define

$$\theta_{i,j} = \arccos\left(\frac{|\langle \mathbf{b}_i, \mathbf{b}_j \rangle|}{\|\mathbf{b}_i\| \|\mathbf{b}_j\|}\right), 1 \le i \ne j \le n.$$

The following lemma says that the SR-Pair method can provide a Gauss-reduced basis for all pairs of vectors with pairwise angles $\theta_{i,j} > \pi/3$.

Lemma 8. For an SR-Pair reduced basis, we have $\theta_{i,j} > \pi/3$ for all $i \neq j$.

Proof. If a lattice basis **B** is non-reducible by SR-Pair, we have $\lfloor \langle \mathbf{b}_i, \mathbf{b}_j \rangle / \langle \mathbf{b}_j, \mathbf{b}_j \rangle \rceil = 0 \quad \forall i \neq j$. Therefore the lemma follows from

$$\cos \theta_{i,j} < \frac{1}{2} \frac{\|\mathbf{b}_i\|}{\|\mathbf{b}_j\|} < \frac{1}{2} \frac{\min(\|\mathbf{b}_i\|, \|\mathbf{b}_j\|)}{\max(\|\mathbf{b}_i\|, \|\mathbf{b}_j\|)} \le 1/2.$$

Here we argue that the pairwise angles are dense in the dual of a Gaussian random basis. Fig. 10-(a) plots the histogram of such random matrices. It shows that so a large number of vectors satisfy $\theta_{i,j} < \pi/3$, and these vectors will trigger the reduction in SR-Pair/SR-Hash. On the contrary, as predicted by Proposition 7, Fig. 10-(b) shows that the primal basis will not be reduced by SR-Pair/SR-Hash. Bases with dense angles also feature large orthogonality defects. In Fig. 11, we plot the OD versus dimension *n* relations respectively for the dual and primal Gaussian random matrices. The figure shows the dual bases approximately have a growth rate of $O(20^{n^{1.5}})$, while that of the primal basis is extremely small. The above confirms that the objective lattice bases in MIMO detection are easily reducible by tuning the pairwise angles.

REFERENCES

- [1] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up MIMO: opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 40–60, 2013.
- [2] 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, 2002.
- [3] H. Yao and G. W. Wornell, "Lattice-reduction-aided detectors for MIMO communication systems," in *Proc. Global Telecommunications Conference (GLOBECOM), Taipei, Taiwan*, pp. 424–428, 2002.
- [4] C. Windpassinger, R. F. H. Fischer, and J. B. Huber, "Lattice-reductionaided broadcast precoding," *IEEE Trans. Commun.*, vol. 52, no. 12, pp. 2057–2060, 2004.
- [5] Z. Wang, Y. Huang, and S. Lyu, "Lattice-reduction-aided gibbs algorithm for lattice gaussian sampling: Convergence enhancement and decoding optimization," *IEEE Trans. Signal Processing*, vol. 67, no. 16, pp. 4342–4356, 2019.



Fig. 10: The histogram of the pairwise angles for the dual and primal of 60×60 Gaussian random bases.



Fig. 11: The ODs of square Gaussian random bases.

- [6] M. Taherzadeh, A. Mobasher, and A. K. Khandani, "LLL reduction achieves the receive diversity in MIMO decoding," *IEEE Trans. Information Theory*, vol. 53, no. 12, pp. 4801–4805, 2007.
- [7] —, "Communication over MIMO broadcast channels using latticebasis reduction," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4567– 4582, 2007.
- [8] X. Ma and W. Zhang, "Performance analysis for MIMO systems with lattice-reduction aided linear equalization," *IEEE Trans. Commun.*, vol. 56, no. 2, pp. 309–318, 2008.
- [9] P. Q. Nguyen and B. Vallée, Eds., *The LLL Algorithm*. Springer Berlin Heidelberg, 2010.
- [10] R. Neelamani, R. L. de Queiroz, and R. G. Baraniuk, "Compression color space estimation of JPEG images using lattice basis reduction," in *Proc. IEEE Int. Conf. Image Process. (ICIP), Thessaloniki, Greece*, pp. 890–893, 2001.
- [11] A. Korkinge and G. Zolotareff, "Sur les formes quadratiques positives," *Math. Ann.*, vol. 11, no. 2, pp. 242–292, 1877.
- [12] D. Micciancio and S. Goldwasser, Complexity of Lattice Problems. Boston, MA: Springer, 2002.
- [13] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, no. 4, pp. 515–534, 1982.
- [14] M. Seysen, "Simultaneous reduction of a lattice basis and its reciprocal

basis," Combinatorica, vol. 13, no. 3, pp. 363-376, sep 1993.

- [15] W. Zhang, S. Qiao, and Y. Wei, "HKZ and minkowski reduction algorithms for lattice-reduction-aided MIMO detection," *IEEE Trans. Signal Process.*, vol. 60, no. 11, pp. 5963–5976, 2012.
- [16] S. Lyu and C. Ling, "Boosted KZ and LLL algorithms," *IEEE Trans. Signal Process.*, vol. 65, no. 18, pp. 4784–4796, Sep. 2017.
- [17] J. Wen and X. Chang, "On the KZ reduction," *IEEE Trans. Information Theory*, pp. 1–1, 2018.
- [18] Y. Chen and P. Q. Nguyen, "BKZ 2.0: Better lattice security estimates," in Proc. ASIACRYPT, Seoul, South Korea, 2011, pp. 1–20, 2011.
- [19] C. Ling, W. H. Mow, and N. Howgrave-Graham, "Reduced and fixedcomplexity variants of the LLL algorithm for communications," *IEEE Trans. Commun.*, vol. 61, no. 3, pp. 1040–1050, 2013.
- [20] W. Zhang, S. Qiao, and Y. Wei, "A diagonal lattice reduction algorithm for MIMO detection," *IEEE Signal Process. Lett.*, vol. 19, no. 5, pp. 311–314, 2012.
- [21] H. Vetter, V. Ponnampalam, M. Sandell, and P. A. Hoeher, "Fixed complexity LLL algorithm," *IEEE Trans. Signal Process.*, vol. 57, no. 4, pp. 1634–1637, 2009.
- [22] Q. Wen, Q. Zhou, and X. Ma, "An enhanced fixed-complexity LLL algorithm for MIMO detection," in *Proc. Global Telecommunications Conference (GLOBECOM), Austin, TX, USA*, pp. 3231–3236, 2014.
- [23] Q. Wen and X. Ma, "Efficient greedy LLL algorithms for lattice decoding," *IEEE Trans. Wirel. Commun.*, vol. 15, no. 5, pp. 3560–3572, 2016.
- [24] J. Wen and X. Chang, "Gfclll: A greedy selection-based approach for fixed-complexity LLL reduction," *IEEE Commun. Lett.*, vol. 21, no. 9, pp. 1965–1968, 2017.
- [25] D. Seethaler, G. Matz, and F. Hlawatsch, "Low-complexity MIMO data detection using seysen's lattice reduction algorithm," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), Honolulu, Hawaii,* USA, pp. 53–56, 2007.
- [26] W. Zhang, X. Ma, and A. Swami, "Designing low-complexity detectors based on seysen's algorithm," *IEEE Trans. Wireless Communications*, vol. 9, no. 10, pp. 3301–3311, 2010.
- [27] Q. Zhou and X. Ma, "Element-based lattice reduction algorithms for large MIMO detection," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 274–286, 2013.
- [28] —, "Improved element-based lattice reduction algorithms for wireless communications," *IEEE Trans. Wirel. Commun.*, vol. 12, no. 9, pp. 4414–4421, 2013.
- [29] S. Lyu and C. Ling, "Sequential lattice reduction," in Proc. 8th Int. Conf. Wirel. Comm. & Signal Process. (WCSP), Yangzhou, China, pp. 1–5, 2016.
- [30] B. M. Hochwald and S. Ten Brink, "Achieving near-capacity on a multiple-antenna channel," *IEEE Trans. Commun.*, vol. 51, no. 3, pp. 389–399, 2003.
- [31] S. Liu, C. Ling, and D. Stehlé, "Decoding by sampling: A randomized lattice algorithm for bounded distance decoding," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5933–5945, 2011.
- [32] C. Ling, "On the proximity factors of lattice reduction-aided decoding," *IEEE Trans. Signal Process.*, vol. 59, no. 6, pp. 2795–2808, 2011.
- [33] L. Babai, "On lovász' lattice reduction and the nearest lattice point problem," *Combinatorica*, vol. 6, no. 1, pp. 1–13, 1986.
- [34] P. Q. Nguyen and D. Stehlé, "Low-dimensional lattice basis reduction revisited," ACM Trans. Algorithms, vol. 5, no. 4, pp. 46:1–46:48, 2009.
- [35] J. C. Lagarias, H. W. Lenstra, and C.-P. Schnorr, "Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice," *Combinatorica*, vol. 10, no. 4, pp. 333–348, 1990.
- [36] Y. Aono and P. Q. Nguyen, "Random sampling revisited: Lattice enumeration with discrete pruning," in *Proc. Advances in Cryptology -EUROCRYPT, Paris, France, 2017*, pp. 65–102, 2017.
- [37] Z. Wang and C. Ling, "On the geometric ergodicity of metropolishastings algorithms for lattice gaussian sampling," *IEEE Trans. Information Theory*, vol. 64, no. 2, pp. 738–751, 2018.
- [38] J. Jaldén and B. Ottersten, "On the complexity of sphere decoding in digital communications," *IEEE Trans. Signal Process.*, vol. 53, no. 4, pp. 1474–1484, 2005.
- [39] A. Gionis, P. Indyk, and R. Motwani, "Similarity search in high dimensions via hashing," in Proc. 25th International Conference on Very Large Data Bases, VLDB'99, Edinburgh, Scotland, UK, pp. 518–529, 1999.
- [40] A. Andoni and P. Indyk, "Near-optimal hashing algorithms for approximate nearest neighbor in high dimensions," in *Proc. 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS), Berkeley, California, USA*, pp. 459–468, 2006.

- [41] P. Indyk and R. Motwani, "Approximate nearest neighbors: Towards removing the curse of dimensionality," in Proc. 30th ACM Symposium on the Theory of Computing (STOC), Dallas, Texas, USA, pp. 604-613, 1998
- [42] T. Laarhoven, "Sieving for shortest vectors in lattices using angular locality-sensitive hashing," in Proc. Advances in Cryptology - CRYPTO, Santa Barbara, CA, USA, 2015, pp. 3-22, 2015.
- [43] J. Jaldén, D. Seethaler, and G. Matz, "Worst- and average-case complexity of LLL lattice reduction in MIMO wireless systems," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), Caesars Palace, Las Vegas, Nevada, USA, pp. 2685-2688, 2008.
- [44] D. Wübben, D. Seethaler, J. Jaldén, and G. Matz, "Lattice reduction," IEEE Signal Process. Mag., vol. 28, no. 3, pp. 70-91, 2011.
- [45] J. Choi, S. R. Kim, and I. Choi, "Statistical eigen-beamforming with selection diversity for spatially correlated OFDM downlink," IEEE Trans. Vehicular Technology, vol. 56, no. 5, pp. 2931-2940, 2007.
- [46] P. Q. Nguyen and D. Stehlé, "Floating-point LLL revisited," in Proc. Advances in Cryptology - EUROCRYPT, Aarhus, Denmark, 2005, pp. 215-233, 2005.
- [47] X. Chang, D. Stehlé, and G. Villard, "Perturbation analysis of the QR factor R in the context of LLL lattice basis reduction," Math. Comput., vol. 81, no. 279, pp. 1487-1511, 2012.
- [48] P. Xie, H. Xiang, and Y. Wei, "Randomized algorithms for total least squares problems," Numerical Lin. Alg. with Applic., vol. 26, no. 1, 2019.
- [49] J. Wen and X. Chang, "Success probability of the babai estimators for box-constrained integer linear models," IEEE Trans. Information Theory, vol. 63, no. 1, pp. 631-648, 2017.
- [50] X. Chang, J. Wen, and X. Xie, "Effects of the LLL reduction on the success probability of the babai point and on the complexity of sphere decoding," IEEE Trans. Information Theory, vol. 59, no. 8, pp. 4915-4926, 2013.

13

South China University of Technology, Guangzhou, China, in 2001 and 2004, respectively, and the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2008. He is currently a Professor and the Executive Dean with the College of Information Science and Technology, Jinan University, Guangzhou, China. He has authored/coauthored 80 papers in international conferences and journals, such as CRYPTO, EUROCRYPT, ASIACRYPT, TCC, PKC, CT-RSA, IEEE TPAMI, IEEE TDSC, etc. His research areas include public key cryptography, cloud security, blockchain, etc. Prof. Weng was a recipient of the Young Scientists Fund of the National Natural Science Foundation of China in 2018, and the Cryptography Innovation Award from Chinese Association for Cryptologic Research (CACR) in 2015. He served as the General Co-Chair for SecureComm 2016, TPC Co-Chairs for RFIDsec13 Asia, and ISPEC 2011, and program committee members for more than 40 international cryptography and information security conferences. He also serves as an Associate Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.

Shanxiang Lyu received the B.S. and M.S. degrees in electronic and information engineering from South China University of Technology, Guangzhou, China, in 2011 and 2014, respectively, and the Ph.D. degree from the Electrical and Electronic Engineering Department, Imperial College London, in 2018. He is currently a lecturer with the College of Cyber Security, Jinan University. His research interests are in lattice theory, algebraic number theory, and their applications.

Cong Ling (S'99-A'01-M'04) received the B.S. and M.S. degrees in electrical engineering from the Nanjing Institute of Communications Engineering, Nanjing, China, in 1995 and 1997, respectively, and the Ph.D. degree in electrical engineering from the Nanyang Technological University, Singapore, in 2005. He had been on the faculties of the Nanjing Institute of Communications Engineering and King's College. He is currently a Reader (Associate Professor) with the Electrical and Electronic Engineering Department, Imperial College London. His research interests are coding, information theory, and security, with a focus on lattices. Dr. Ling has served as an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.

Jinming Wen received his Bachelor degree in Information and Computing Science from Jilin Institute of Chemical Technology, Jilin, China, in 2008, his M.Sc. degree in Pure Mathematics from the Mathematics Institute of Jilin University, Jilin, China, in 2010, and his Ph.D degree in Applied Mathematics from McGill University, Montreal, Canada, in 2015. He was a postdoctoral research fellow at Laboratoire LIP (from March 2015 to August 2016), University of Alberta (from September 2016 to August 2017) and University of Toronto (from September 2017 to August 2018). He has been a full professor in Jinan University, Guangzhou since September 2018. His research interests are in the areas of lattice reduction and sparse recovery. He has published around 50 papers in top journals (including Applied and Computational Harmonic Analysis, IEEE Transactions on Information Theory/Signal Processing/Wireless Communications) and conferences. He is an Associate Editor of IEEE Access.