GfcLLL: A Greedy Selection Based Approach for Fixed-Complexity LLL Reduction

Jinming Wen and Xiao-Wen Chang

Abstract—The LLL lattice reduction has been widely used to decrease the bit error rate (BER) of the Babai point, but its running time varies much from matrix to matrix. To address this problem, some fixed-complexity LLL reductions (FCLLL) have been proposed. In this paper, we propose two greedy selection based FCLLL algorithms: GfcLLL(1) and GfcLLL(2). Simulations show that both of them give Babai points with lower BER in similar or much shorter CPU time than existing ones.

Index Terms—Integer least squares problem, fixed-complexity LLL reduction, success probability, GfcLLL.

I. INTRODUCTION

In MIMO detection and some other applications, we need to estimate an unknown parameter vector $\hat{x} \in \mathbb{Z}^n$ from

$$\boldsymbol{y} = \boldsymbol{A}\hat{\boldsymbol{x}} + \boldsymbol{v}, \quad \boldsymbol{v} \sim \mathcal{N}(\boldsymbol{0}, \sigma^2 \boldsymbol{I}),$$
 (1)

where $y \in \mathbb{R}^m$ is an observation vector, $A \in \mathbb{R}^{m \times n}$ is a full column rank model matrix and $v \in \mathbb{R}^m$ is a noise vector.

A common method to estimate \hat{x} is to solve the following ordinary integer least squares (ILS) problem:

$$\min_{\boldsymbol{x}\in\mathbb{Z}^n}\|\boldsymbol{y}-\boldsymbol{A}\boldsymbol{x}\|_2^2,\tag{2}$$

whose solution is the maximum likelihood estimator of \hat{x} . Since (2) is NP-hard, for some real-time applications, a suboptimal solution, which can be produced quickly, is computed instead of solving (2). One often used suboptimal solution is the ordinary Babai point x^{B} , produced by the Babai's nearest plane algorithm [1]. It is shown in [2] that the LLL reduction algorithm [3] can always increase the success probability of x^{B} which is the probability of $x^{\text{B}} = \hat{x}$.

In communications, the parameter vector \hat{x} is often subject to a box constraint (after some transformations), i.e.,

$$\hat{\boldsymbol{x}} \in \mathcal{B} := \{ \boldsymbol{x} : \boldsymbol{l} \le \boldsymbol{x} \le \boldsymbol{u}, \ \boldsymbol{x} \in \mathbb{Z}^n \}.$$
(3)

In this situation, one can first use the LLL reduction to get the LLL-aided ordinary Babai point, then round it into the constraint box \mathcal{B} to get an estimate of \hat{x} .

The LLL reduction is useful to improve the accuracy of the Babai points for both unconstrained and box-constrained cases [2] [4]. However, its running time varies much from matrix to matrix even for a fixed dimension. Moreover, it

was shown in [5] that in the MIMO context, the worst-case computational cost of the LLL reduction for reducing A is not even bounded by a function of n. This may cause problems for real-time communications applications, where limited and known run-time is essential [6], from the implementation point of view. To address this issue, some so called fixedcomplexity LLL (FCLLL) reduction algorithms have been proposed [6]–[8]. For a given A, an FCLLL algorithm is to get a reduced matrix of A that is close to the LLL reduced matrix of A in a computational cost more or less fixed for matrices with the same dimensions. For the FCLLL algorithms in [6]-[8], the number of sweeps or the number of tests of the Lovász condition is fixed, while for the new FCLLL algorithms to be proposed in this paper, the number of column permutations is fixed. Note that an FCLLL algorithm may have different numbers of arithmetic operations for different matrices with the same dimensions. However, the difference is small. Moreover, there is an upper bound on the complexity in terms of number of arithmetic operations, which is truly fixed for the same dimensions.

In this paper, we will propose a new approach for FCLLL reduction. Unlike existing approaches, which use predefined traversal order for selecting two consecutive columns for size reductions and permutation, our new approach uses a traversal order based on a greedy selection strategy. It is motivated by increasing the success probability of the Babai point. Two greedy selection strategies are proposed for this purpose, leading to two FCLLL algorithms GfcLLL(1) and GfcLLL(2), respectively. The first strategy was originally proposed in [9] for computing the full LLL reduction and the other one is new and more effective. The greedy approach takes more data communication time to find the columns to do size reductions and column interchanges than approaches with fixed traversal order. However, simulations show that both GfcLLL(1) and GfcLLL(2) can produce Babai points with lower bit error rate (BER) than the FCLLL algorithms proposed in [6]-[8], with similar or much less CPU time.

The rest of this paper is organized as follows. In Section II, we introduce the LLL and FCLLL reductions. In Section III, we present our new algorithms. In Section IV, we do some simulations to show the effectiveness and efficiency of the new algorithms. Finally we summarize this paper in Section V.

II. BACKGROUND

In this section, we first introduce the LLL reduction and the success probability of the Babai point which is the motivation for our new algorithm, then we briefly review some recent FCLLL algorithms which will be used for comparisons later.

This work was supported by NSERC of Canada grant 217191-17 and postdoc research fellowship from Fonds de recherche Nature et technologies. Jinming Wen is with the Department of Electrical and Computer En-

jinming wen is with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton T6G 2V4, Canada (e-mail: jinming1@ualberta.ca).

X.-W. Chang is with the School of Computer Science, McGill University, Montreal, QC H3A 0E9, Canada (e-mail: chang@cs.mcgill.ca).

Let A in (1) have the following QR factorization

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{Q}_1, \boldsymbol{Q}_2 \\ n & m-n \end{bmatrix} \begin{bmatrix} \boldsymbol{R} \\ \boldsymbol{0} \end{bmatrix}, \qquad (4)$$

where $[\boldsymbol{Q}_1, \boldsymbol{Q}_2] \in \mathbb{R}^{m \times m}$ is orthogonal and $\boldsymbol{R} \in \mathbb{R}^{n \times n}$ is upper triangular. Define $\tilde{\boldsymbol{y}} = \boldsymbol{Q}_1^T \boldsymbol{y}$ and $\tilde{\boldsymbol{v}} = \boldsymbol{Q}_1^T \boldsymbol{v}$, then (1) can be transformed to

$$\tilde{\boldsymbol{y}} = \boldsymbol{R}\hat{\boldsymbol{x}} + \tilde{\boldsymbol{v}}, \quad \tilde{\boldsymbol{v}} \sim \mathcal{N}(\boldsymbol{0}, \sigma^2 \boldsymbol{I}).$$
 (5)

The ordinary Babai (integer) point $x^{B} \in \mathbb{Z}^{n}$ found by the Babai nearest plane algorithm [1] is defined as

$$c_n = \tilde{y}_n / r_{nn}, \quad x_n^{\mathsf{B}} = \lfloor c_n \rceil,$$

$$c_i = (\tilde{y}_i - \sum_{j=i+1}^n r_{ij} x_j^{\mathsf{B}}) / r_{ii}, x_i^{\mathsf{B}} = \lfloor c_i \rceil, i = n-1, \dots, 1.$$
(6)

The ordinary Babai point $x^{\scriptscriptstyle \mathrm{B}} \in \mathbb{Z}^n$ can be used as an estimator of \hat{x} , and its success probability is (see [2])

$$P(\boldsymbol{R}) := \Pr(\boldsymbol{x}^{\mathsf{B}} = \hat{\boldsymbol{x}}) = \prod_{i=1}^{n} \phi(r_{ii}), \tag{7}$$

$$\phi(r_{ii}) = \sqrt{\frac{2}{\pi}} \int_0^{|r_{ii}|/(2\sigma)} \exp(-\frac{1}{2}t^2) dt.$$
(8)

With the QR factorization (4), the LLL reduction algorithm [3] reduces \boldsymbol{R} to $\bar{\boldsymbol{R}}$ via $\bar{\boldsymbol{Q}}^T \boldsymbol{R} \boldsymbol{Z} = \bar{\boldsymbol{R}}$, where $\bar{\boldsymbol{Q}} \in \mathbb{R}^{n \times n}$ is orthogonal, $Z \in \mathbb{Z}^{n \times n}$ is unimodular (i.e., $det(Z) = \pm 1$) and $\bar{R} \in \mathbb{R}^{n \times n}$ is an upper triangular matrix satisfying

$$|\bar{r}_{ik}| \le \frac{1}{2} |\bar{r}_{ii}|, \quad i = 1, 2, \dots, k-1,$$
(9)

$$\delta \bar{r}_{k-1,k-1}^2 \le \bar{r}_{k-1,k}^2 + \bar{r}_{kk}^2, \quad k = 2, 3, \dots, n, \tag{10}$$

where δ is a constant satisfying $1/4 < \delta \le 1$. Define $\bar{\boldsymbol{y}} = \bar{\boldsymbol{Q}}^T \tilde{\boldsymbol{y}}, \quad \bar{\boldsymbol{v}} = \bar{\boldsymbol{Q}}^T \tilde{\boldsymbol{v}}, \quad \hat{\boldsymbol{z}} = \boldsymbol{Z}^{-1} \hat{\boldsymbol{x}}, \text{ then (5) can$ be transformed to $\bar{y} = \bar{R}\hat{z} + \bar{v}, \quad \bar{v} \sim \mathcal{N}(0, \sigma^2 I)$. Using (6), we can obtain its Babai point z^{B} . Then we get the LLLaided ordinary Babai point $x^{\text{\tiny LB}} = Z z^{\text{\tiny B}}$, which can be used to estimate \hat{x} . If $\hat{x} \in \mathcal{B}$ (see (3)), after obtaining x^{LB} , we round it to the nearest point in \mathcal{B} , leading to the box-constrained LLL-aided Babai point.

The LLL algorithm in [3] starts with column 2 of R and ends with column n of R. When the reduction processes at column k, it first performs size reductions on r_{ik} for i = k-1: -1:1, and then checks if (10) holds. If so, the column index increases by 1; otherwise it permutes columns k-1 and k of R and the column index decreases by 1. One does not know exactly how many iterations are required to finish the reduction process (here the number of iteration means the number of tests on (10) [7]). The FCLLL algorithm in [6], to be referred to as fcLLL, is a modification of the LLL algorithm. It always goes from column 2 to column n and never comes back in the process. But it repeats the process J times, where J is a fixed positive integer, resulting in L = J(n-1) iterations.

A modification of fcLLL, referred to as EfcLLL, was given in [7]. EfcLLL does only size reductions on the super-diagonal entries of R. Like the LLL algorithm [3], both fcLLL and EfcLLL start the iterations from the second column and finish at the last column of **R**. Different from this traversal strategy, the most recent FCLLL, referred to as EnfcLLL, was proposed in [8]. It uses a novel two-stage column traversal strategy.

III. NEW FCLLL REDUCTION ALGORITHMS

As explained in Section II, both fcLLL and EfcLLL start the iterations from the second column and finish at the last column which may not be effective in increasing the success probability of the Babai point in fixed time. EnfcLLL uses a different traversal strategy and can improve the performance significantly. But like the previous ones, its traversal order is still fixed in advance. Let us use an extreme case to explain why a fixed order, which ignores the particularity of a channel matrix, may not work well sometimes. Suppose we are allowed to do only one column permutation, then it is obvious that the order-fixed algorithms are unlikely to produce the best result.

The idea of our approach is that at each step, we choose two consecutive columns to do size reduction and permutation so that we get highest improvement of the success probability of the Babai point.

Given an upper triangular matrix R, suppose that for any specific k, (10) is not satisfied after $r_{k-1,k}$ is size reduced, i.e.

$$\delta r_{k-1,k-1}^2 > \left(r_{k-1,k} - \left\lfloor \frac{r_{k-1,k}}{r_{k-1,k-1}} \right\rceil r_{k-1,k-1} \right)^2 + r_{kk}^2.$$
(11)

After the size reduction on $r_{k-1,k}$ (i.e., applying a unimodular matrix to R from right so that (9) holds), permutation of the two columns and triangularization, we obtain \bar{R} which satisfies

$$\bar{r}_{k-1,k} = r_{k-1,k} - \lfloor r_{k-1,k}/r_{k-1,k-1} \rceil r_{k-1,k-1},$$

$$\bar{r}_{k-1,k-1} = \sqrt{\bar{r}_{k-1,k}^2 + r_{kk}^2},$$

$$|\bar{r}_{kk}| = |r_{k-1,k-1}r_{kk}/\bar{r}_{k-1,k-1}|.$$
(12)

Note that the above operations decrease $|r_{k-1,k-1}|$ and increase $|r_{kk}|$. Then by (7),

$$\frac{P(\mathbf{R})}{P(\mathbf{R})} = \frac{\phi(\bar{r}_{k-1,k-1})\phi(\bar{r}_{kk})}{\phi(r_{k-1,k-1})\phi(r_{kk})} := T_k.$$

In [2] it is proved that $T_k > 1$. Ideally we wish to find k such that T_k is the largest, then perform size reduction, column permutation and triangularization. However, computing $\phi(\zeta)$ (see (8)) involves numerical integrations and is expensive. Instead we will look at other more efficient greedy strategies.

In the following, we propose two different greedy selection strategies to choose two columns of R to do reduction at each step. The first greedy selection strategy is to find

$$j = \arg\max_{k} \{T_{k}^{(1)} : T_{k}^{(1)} = \frac{|r_{k-1,k-1}|}{|\bar{r}_{k-1,k-1}|}, (11) \text{ holds} \}.$$

If the above j does not exist, R is essentially LLL reduced as it can become LLL reduced after performing size reductions. Otherwise, we perform a size reduction on $r_{j-1,j}$, permute columns j-1 and j of \mathbf{R} , and triangularize \mathbf{R} by a Givens rotation. After that, we update $T_j^{(1)}$, $T_{j-1}^{(1)}$ (if j > 1) and $T_{j+1}^{(1)}$ (if j < n) (note that other $T_i^{(1)}$'s are not changed), and start the next iteration. This greedy selection strategy is to find a pair of columns which can reduce the larger one of the two diagonal elements most significantly and it was first proposed in [9] for computing the LLL reduction in solving an ILS problem for GPS applications. Later the same strategy was used in [10] and [11]. One problem with this strategy is $|r_{k-1,k-1}|/|\bar{r}_{k-1,k-1}|$

is invariant with respect to scaling of R(:, k - 1:k), but the success probability of the Babai point changes by scaling.

The second greedy selection strategy is to find

$$j = \arg\max_{k} \{T_{k}^{(2)} : T_{k}^{(2)} = \frac{1}{|r_{kk}|} - \frac{1}{|\bar{r}_{kk}|}, (11) \text{ holds}\}.$$

Note that in the LLL reduction, after columns k-1 and k are permutated, $|r_{kk}|$ will increase, and $1/|r_{kk}|$ will decrease. This strategy is to find columns j-1 and j such that $1/|r_{jj}|$ decreases most. We can rewrite $T_k^{(2)}$ as

$$T_k^{(2)} = \frac{|r_{k-1,k-1}| - |\bar{r}_{k-1,k-1}|}{|r_{k-1,k-1}r_{kk}|}$$

which is a relative gap between $|r_{k-1,k-1}|$ and $|\bar{r}_{k-1,k-1}|$ (note that the denominator is the determinant of the lattice $\{\mathbf{R}(k-1:k,k-1:k)\mathbf{x}|\mathbf{x} \in \mathbb{Z}^2\}$). Like T_k , $T_k^{(2)}$ is variant with respect to scaling of $\mathbf{R}(:,k-1:k)$. Our numerical tests indicate that the two columns found by maximizing $T_k^{(2)}$ are more likely to the same as those found by maximizing T_k than those found by maximizing $T_k^{(1)}$. For the sake of convenience, when (11) does not hold, we

For the sake of convenience, when (11) does not hold, we set $T_k^{(i)} = 0$ for i = 1, 2. In our algorithms, we suppose the maximum number of column permutations (denoted by N) is given. The description of our algorithms is as follows:

Algorithm 1 GfcLLL(*i*)

1: compute the QR factorization (4), set swap = 0, $Z = I_n$; 2: compute $T_k^{(i)}$ for k = 2:n; 2: compare \mathbb{I}_k 3: for j = 1 : N do 4: find j such that $T_j^{(i)} = \max_{2 \le k \le n} T_k^{(i)}$; ${\rm if} \; T_j^{(i)} > 0 \; {\rm then} \;$ 5: 6: perform size reduction on $r_{j-1,j}$ and update Z; permute columns j-1 and j of \boldsymbol{R} and triangularize 7: **R**, and update **Z** and **Q**; update $T_{j}^{(i)}$, $T_{j-1}^{(i)}$ if j > 1, and $T_{j+1}^{(i)}$ if j < n-1; 8: 9: else 10: break; end if 11: 12: end for

Like J in [6] and [7], and N_{max} in [8], N depends on applications. By using sone techniques similar to that for showing the LLL algorithm is a polynomial time algorithm in [3], we can derive a complexity result for GfcLLL(i), which depends on N. Then for any specific application which has a fixed complexity requirement, we can find N.

IV. SIMULATIONS

In this section, we compare the efficiency and effectiveness of GfcLLL(i) with existing FCLLL algorithms. As the boxconstrained Babai points found by applying fcLLL and EfcLL are the same and fcLLL is slower than EfcLLL, we do not compare GfcLLL(i) with fcLLL. Two greedy LLL algorithms were proposed in [12] and one is faster than the other one. For comparison, we modified the faster one by fixing the number of column permutations so that it became an FCLLL algorithm, and refer it to as GfcLLL-WM. In the tests, we took the parameter $\delta = 1$. All of the tests were performed with MATLAB 2016b on a desktop computer with Intel(R) Xeon(R) CPU E5-1603 v4 working at 2.80 GHz.

For a fixed dimension, a fixed type of QAM and a fixed E_b/N_0 , we randomly generated 10^3 complex channel matrices A whose entries independently and identically follow the standard complex normal distribution. For each generated matrix, we randomly generated 10^3 complex signal vectors \hat{x} and 10^3 complex Gaussian noise vectors v, resulting in 10^6 instances of complex linear models. Each complex instance was then transformed to an instance of the real model (1).

To compare GfcLLL(i) with other FCLLL algorithms, we control the number of column permutations each algorithm performs so that they have similar costs. We first fix the number of sweeps J for EfcLLL. For any channel matrix, we record the number of column permutations performed by EfcLLL, which is denoted by K. Then for the same channel matrix, we set the number of column permutations for EnfcLLL, GfcLLL-WM and GfcLLL(i) as $\lfloor 0.35K \rceil$, $\lfloor 0.7K \rceil$ and $\lfloor 0.7K \rceil$, respectively. Our simulations indicate that the above choices usually make the CPU time taken by our GfcLLL(i) less than those taken by other algorithms.

Figures 1 and 2 show the average BER (over 10^6 instances) versus $E_b/N_0 = 2:2:30$ for the 8×8 complex MIMO systems with 4-QAM for J = 1 and J = 2, respectively. Similarly, Figures 3 and 4 show the corresponding results for the 16×16 complex MIMO systems with 16-QAM for J = 1 and J = 2, respectively.



Fig. 1: BER versus $E_b/N_0 = 2:2:30$ for the 8×8 MIMO system with 4-QAM, J = 1

Tables I and II respectively display the total CPU time of computing reductions for the 1000 8×8 and 16×16 complex channel matrices with J = 1, 2.

TABLE I: Total CPU time for 1000 8×8 channel matrices

J	LLL	EfcLLL	EnfcLLL	GfcLLL-WM	GfcLLL1	GfcLLL2
1	2.5333	0.3124	0.2783	0.2473	0.2392	0.2380
2	2.7438	0.5735	0.4315	0.4214	0.4061	0.4175

From Figures 1–4 and Tables I and II, we can see that the box-constrained Babai points aided by GfcLLL(i) (i = 1, 2) have lower BER than those aided by existing FCLLL reductions, while the former cost less than the latter. Thus our



Fig. 2: BER versus $E_b/N_0 = 2:2:30$ for the 8×8 MIMO system with 4-QAM, J = 2



Fig. 3: BER versus $E_b/N_0 = 2:2:30$ for the 16×16 MIMO system with 16-QAM, J = 1



Fig. 4: BER versus $E_b/N_0 = 2:2:30$ for the 16×16 MIMO system with 16-QAM, J = 2

TABLE II: Total CPU time for $1000 \ 16 \times 16$ channel matrices

J	LLL	EfcLLL	EnfcLLL	GfcLLL-WM	GfcLLL1	GfcLLL2
1	9.4890	0.6705	0.6488	0.5325	0.5058	0.5257
2	9.1026	1.1286	1.0107	0.8390	0.8135	0.8204

proposed GfcLLL(i) (i = 1, 2) are more efficient and effective. We also observe that GfcLLL(2) gives better performance than GfcLLL(1) with similar cost. The simulation results also show that GfcLLL(i) can decrease the BER of the box-constrained Babai points significantly by performing a small number of permutations after the QR factorization.

In the above tests, EnfcLLL performed about a half number of permutations performed by GfcLLL(i). In our simulations we found that if we set the same number of permutations for both EnfcLLL and GfcLLL(i), the former is still worse than the latter in decreasing the BER of the box-constrained Babai points (note that in this case, the CPU time used by EnfcLLL is much higher than those by GfcLLL(i)).

V. SUMMARY

We have proposed two greedy selection based FCLLL algorithms: GfcLLL(1) and GfcLLL(2). Simulations showed that both result in the box-constrained Babai points with lower BER in shorter CPU time than existing FCLLL algorithms and GfcLLL(2) is more effective than GfcLLL(1).

REFERENCES

- L. Babai, "On lovasz lattice reduction and the nearest lattice point problem," *Combinatorica*, vol. 6, no. 1, pp. 1–13, 1986.
- [2] X.-W. 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. Inf. Theory*, vol. 59, no. 8, pp. 4915–4926, 2013.
- [3] A. Lenstra, H. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Math. Ann.*, vol. 261, no. 4, pp. 515–534, 1982.
- [4] J. Wen and X.-W. Chang, "The success probability of the Babai point estimator and the integer least squares estimator in box-constrained integer linear models," *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 631– 648, 2017.
- [5] J. Jaldén, D. Seethaler, and G. Matz, "Worst-and average-case complexity of LLL lattice reduction in MIMO wireless systems," in *Proceedings* of the 2008 IEEE ICASSP, 2008, pp. 2685–2688.
- [6] 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.
- [7] C. Ling, W. 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.
- [8] Q. Wen, Q. Zhou, and X. Ma, "An enhanced fixed-complexity LLL algorithm for MIMO detection," in 2014 IEEE Global Communications Conference. IEEE, 2014, pp. 3231–3236.
- [9] X.-W. Chang, X. Yang, and T. Zhou, "MLAMBDA: A modified LAMBDA method for integer least-squares estimation," *Journal of Geodesy*, vol. 79, no. 9, pp. 552–565, 2005.
- [10] K. Zhao, Y. Li, H. Jiang, and S. Du, "A low complexity fast lattice reduction algorithm for mimo detection," in 23rd PIMRC, Sept 2012, pp. 1612–1616.
- [11] 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.
- [12] Q. Wen and X. Ma, "Efficient greedy LLL algorithms for lattice decoding," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 3560– 3572, Nov. 2016.