Proceedings of the 2nd World Congress on Electrical Engineering and Computer Systems and Science (EECSS'16)
Budapest, Hungary - August 16 - 17, 2016
Paper No. EEE 108
DOI: 10.11159/eee16.108

A Hybrid Method for Lattice-Reduction-Aided MIMO Detection

Zhaofei Tian, Sanzheng Qiao
Department of Computing and Software, McMaster University
1280 Main Street West, Hamilton, Ontario, Canada
tianz3@mcmaster.ca; qiao@cas.mcmaster.ca

Abstract - Lattice reduction has been successfully applied to data detection in multiple-input multiple-output (MIMO) systems. In this paper, we introduce a polynomial time algorithm for lattice-reduction-aided (LR-aided) MIMO detection. The hybrid method we present integrates the length-based size reduction technique into an angle-measured method. To assess the performance of the algorithm, we compare it with the LLL algorithm, a widely used algorithm in MIMO and wireless communications. Our experimental results show that despite that the two algorithms have the same complexity, the hybrid method is empirically more efficient than the LLL algorithm, and the communication channels improved by our hybrid method have smaller bit error rate (BER) than those improved by the LLL algorithm in data detection.

Keywords: Signal processing, MIMO detection, Lattice reduction, LLL, Jacobi method

1. Introduction

Lattice reduction plays an important role in numerous fields of mathematics, computer science, cryptography and signal processing. Recently, lattice reduction has shown its advantages on data detection in MIMO systems [1-5]. For example, the LLL algorithm is widely adopted in MIMO systems because of its relatively low complexity in computation. It has been shown that the sub-optimal LLL algorithm can improve the performance of MIMO systems with respect to high spectral efficiency in signal transmission, high accuracy for data detection and the maximum receive diversity over fading channels [15, 6, 7]. See [8] for more details about the applications of lattice basis reduction in wireless communications.

Consider an $m \times n$ MIMO system of n transmit antennas and m receive antennas. The relation between an $n \times 1$ transmitted signal $\mathbf{x}$ and an $m \times 1$ received signal $\mathbf{y}$ is modelled by $\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{n}$, where $\mathbf{A}$ and $\mathbf{n}$ represent the channel matrix and the additive noise, respectively. The channel matrix $\mathbf{A}$ is complex in a full-rank flat-fading MIMO system, but it can be transformed into a real matrix of double size straightforwardly [8]. Hence, in this paper, we assume $\mathbf{A}$ is real. The optimum maximum likelihood (ML) decoding selects $\mathbf{x}_{ML}$ that is a solution for the following minimization integer least squares problem:

$$\mathbf{x}_{ML} = \arg\min_{\mathbf{x}\in\mathscr{A}} ||\mathbf{y} - \mathbf{A}\mathbf{x}||_2, \tag{1}$$

where $\mathscr{A}$ denotes the finite set of real-valued modulation alphabet being used. The complexity of solving (1) grows exponentially corresponding to the number of antennas [3, 9]. Hence ML decoding is not feasible for large number of transmit antennas. To reduce the decoding cost, many approximate algorithms have been introduced to achieve high performance with low complexity, such as zero-forcing (ZF) decoding and minimum mean-square-error (MMSE) decoding [5]. The performance of those decoding strategies heavily depends on the quality of $\mathbf{A}$. Lattice reduction algorithms can improve the quality of the channel matrix $\mathbf{A}$ w.r.t. the orthogonality of columns and condition number of the matrix.

Suppose $\mathbf{A}$ is an $m \times n$ $(m \geq n)$ real matrix of full column rank, a *lattice* generated by $\mathbf{A}$ is defined as $L(\mathbf{A}) = \{\mathbf{A}\mathbf{z} \mid \mathbf{z} \in \mathbb{Z}^n\}$, where $\mathbb{Z}^n$ is the set of all integer n-vectors. The columns of $\mathbf{A}$ and n are respectively called the *basis* and the *dimension* of the lattice. A lattice of dimension at least 2 has infinitely many bases [4]. Any two bases $\mathbf{A}$ and $\mathbf{A}'$ for the same lattice are related by a unimodular matrix $\mathbf{Z}$, i.e., $\mathbf{Z}$ is an integer matrix and $|\det(\mathbf{Z})| = 1$, such that $\mathbf{A} = \mathbf{A}'\mathbf{Z}$. For a given basis, the lattice reduction algorithms are aimed to find a reduced basis with relatively shorter and more orthogonal vectors. There are several notions of reduced basis, such as the Minkowski reduced basis [10, 11] and the HKZ reduced basis [12], both need exponential time to be computed. Another category of reduced basis can be found in polynomial time, such as the Schnorr reduced basis [13] and the widely used LLL reduced basis [14]. It has been proven that the LLL-reduction-aided decoding can achieve the full diversity of a MIMO fading channel [15, 6].

In this paper, we present a hybrid method for LR-aided MIMO detection. We first show that the hybrid method has the same time complexity as the LLL algorithm, which is widely used in many signal processing applications. Then we compare our algorithm with the LLL algorithm by experiments, To our best knowledge, the LLL algorithm (including its variants) is considered to be the only sub-optimal method that practically produces reasonably good results in polynomial time. Our experimental results show that the hybrid method computes lattice bases of better quality in less time than the LLL algorithm

for MIMO systems. In our MIMO simulations, the communication channels improved by the hybrid method has smaller BER than the channels improved by the LLL algorithm.

Notations: We choose column-version representation for matrices and vectors in this paper. The length of a vector $\mathbf{v}$ is measured by the Euclidean norm $\|\mathbf{v}\|_2$, denoted by $\|\mathbf{v}\|$ for simplicity, and $\mathbf{I}_n$ denotes the identity matrix of order n.

2. A Generic Jacobi Method

We call a two dimensional basis matrix $\mathbf{A} = [\mathbf{a}_1, \mathbf{a}_2]$ Lagrange reduced, if $||\mathbf{a}_1||_2 \leq ||\mathbf{a}_2||_2$ and $|\mathbf{a}_1^T \mathbf{a}_2| \leq ||\mathbf{a}_1||_2^2/2$. Denote θ the angle between $\mathbf{a}_1$ and $\mathbf{a}_2$, then $|\cos(\theta)| = |\mathbf{a}_1^T \mathbf{a}_2|/(||\mathbf{a}_1||_2 \cdot ||\mathbf{a}_2||_2) \leq |\mathbf{a}_1^T \mathbf{a}_2|/||\mathbf{a}_1||_2^2 \leq 1/2$. Thus, we have $\pi/3 \leq \theta \leq 2\pi/3$ [16]. We generalize the definition of the Lagrange reduction to n-dimensional lattices. We say that a basis matrix $\mathbf{A} = [\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n]$ is Jacobi reduced, if $|\mathbf{a}_i^T \mathbf{a}_j| \leq \|\mathbf{a}_i\|_2^2/2$ and $\|\mathbf{a}_i\|_2 \leq \|\mathbf{a}_j\|_2$, for all $1 \leq i < j \leq n$. Let $\mathbf{G} = [g_{ij}] = \mathbf{A}^T\mathbf{A}$ be the Gram matrix and $\mathbf{R}$ be the upper triangular matrix in the QR decomposition of $\mathbf{A}$, respectively. We have $g_{ij} = \mathbf{a}_i^T \mathbf{a}_j$ and $g_{jj} = ||\mathbf{a}_j||_2^2$. Hence the above conditions of the Jacobi reduction are equivalent to $|g_{ij}| \leq g_{ii}/2$ and $g_{ii} \leq g_{jj}$.

In 2012, S. Qiao presented a generic Jacobi method for lattice basis reduction [16]. It computes a Jacobi reduced basis by repeatedly applying the Lagrange reduction, shown as Procedure 1, to every pair of vectors in an n-dimensional basis, until every pair is Lagrange reduced. Algorithm 1 shows the row-cyclic version of a slightly improved generic Jacobi method.

Procedure 1: `Lagrange`$(\mathbf{G}, \mathbf{Z}, \mathbf{R}, i, j)$

Input : $\mathbf{G}$, $\mathbf{Z}$, indices i, j $(1 \leq i < j \leq n)$, and optional $\mathbf{R}$
Output: Updated $\mathbf{G}$, $\mathbf{Z}$ and optional $\mathbf{R}$

1 Set integer $\mathtt{s} \in \{i, j\}$ such that $g_{ss} = \min(g_{ii}, g_{jj})$, and Set integer `l` the other index in $\{i, j\}$;
2 $q = \lfloor g_{ij}/g_{ss} \rceil$; `// Nearest integer rounding`
3 Set $\mathbf{Z}_{ij} = \mathbf{I}_n$ except $z_{sl} = -q$;
4 $\mathbf{G} \leftarrow \mathbf{Z}_{ij}^T \mathbf{G} \mathbf{Z}_{ij}$;
5 $\mathbf{Z} \leftarrow \mathbf{Z}\mathbf{Z}_{ij}$;
6 **if** $\mathbf{R}$ *is present* **then**
7 $\quad \mathbf{R} \leftarrow \mathbf{R}\mathbf{Z}_{ij}$;

Algorithm 1: The Generic Jacobi Method

Input : A basis matrix $\mathbf{A}$
Output: A Jacobi reduced basis matrix $\mathbf{A}$

1 $\mathbf{G} = \mathbf{A}^T\mathbf{A}$, $\mathbf{Z} = \mathbf{I}_n$;
2 **while** $\mathbf{AZ}$ *is not Jacobi reduced* **do**
3 $\quad$ **for** $i = 1$ **to** $n-1$ **do**
4 $\quad\quad$ **for** $j = i+1$ **to** n **do**
5 $\quad\quad\quad$ **if** $|g_{ij}| \leq g_{ii}/2$ *and* $g_{ii} \leq g_{jj}$ *are not satisfied* **then**
6 $\quad\quad\quad\quad$ $[\mathbf{G}, \mathbf{Z}] \leftarrow$ `Lagrange`$(\mathbf{G}, \mathbf{Z}, i, j)$;
7 $\quad\quad\quad\quad$ Swap the ith and jth columns of $\mathbf{Z}$;
8 $\quad\quad\quad\quad$ Swap the ith and jth columns, ith and jth rows of $\mathbf{G}$
9 $\mathbf{A} = \mathbf{AZ}$;

Let $\mathbf{G}$ and $\mathbf{G}'$ be the input and the output Gram matrix in procedure `Lagrange`$(\mathbf{G}, \mathbf{Z}, \mathbf{R}, i, j)$, respectively. We call $\tau = \sqrt{\Pi_{k=1}^n g'_{kk}/\Pi_{k=1}^n g_{kk}}$ the reduction factor of the procedure. In line 2, we compute g_{ij}/g_{ss} and round the value to the nearest integer q. Then we reduce g_{ll} using g_{ss} and g_{ls}, i.e., $g'_{ll} = g_{ll} + q^2 g_{ss} - 2q g_{ls}$. If $|q| > 1$, the reduction factor τ of `Lagrange` is less than or equal to $1/\sqrt{3}$; if $|q| = 1$, then τ may arbitrarily close to 1 [17, 18]. Procedure `Lagrange` costs $O(n)$ (additions and multiplications) by vector operations, since it only operates a maximum of two columns and two rows of each input matrix. However, the time complexity of Algorithm 1, the generic Jacobi method, remains unknown.

3. A Hybrid Method for Lattice Basis Reduction

To further improve the quality of the basis matrices computed by the Jacobi method, especially measured by condition number, we integrate the size reduction into Algorithm 1. We first introduce a notion of partial size reduction, which is a generalization of the size reduction [14] used in many lattice reduction algorithms. A basis matrix $\mathbf{A}$ is *partially size reduced* with respect to an index pair (i, j), $1 \leq i < j \leq n$, if the upper triangular matrix $\mathbf{R}$ in the QR decomposition of $\mathbf{A}$ satisfies $|r_{k,j}| \leq |r_{k,k}|/2$, for all $1 \leq k \leq i$. Thus, if $\mathbf{A}$ is partially size reduced with respect to $(i, i+1)$ for all i, $1 \leq i < n$, then $\mathbf{A}$ is size reduced. Secondly, to ensure that the reduction factor of procedure `Lagrange()` is strictly smaller than 1, that is, the basis vector length is strictly reduced, we introduce a condition parameter ω to the definition of the Jacobi reduction.

Definition (ω-reduced) We say that an n-dimensional basis matrix $\mathbf{A} = [\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n]$ is *ω-reduced*, if every pair of basis vectors $(\mathbf{a}_i, \mathbf{a}_j)$ satisfies

$$|\lfloor \mathbf{a}_i^T \mathbf{a}_j / \|\mathbf{a}_s\|_2^2 \rceil| \leq 1 \tag{2}$$

$$\omega \|\mathbf{a}_l\|_2 \ < \ \|\mathbf{a}_l - \zeta \cdot \mathbf{a}_s\|_2 \tag{3}$$

for all $1 \leq i < j \leq n$, where $1/\sqrt{3} \leq \omega < 1$, notation $\zeta = \pm 1$ denotes the sign of $\mathbf{a}_i^T \mathbf{a}_j$, $\mathbf{a}_s$ and $\mathbf{a}_l$ are the shorter and the longer of $\|\mathbf{a}_i\|_2$ and $\|\mathbf{a}_j\|_2$, respectively. In terms of the gram matrix $\mathbf{G}$, we have $|\zeta \cdot \mathbf{a}_l^T \mathbf{a}_s| = |g_{ij}|$. Then, (2) and (3) are equivalent to

$$|\lfloor g_{ij}/g_{ss} \rceil| \leq 1, \tag{4}$$

$$\omega^2 g_{ll} < g_{ii} + g_{jj} - 2|g_{ij}|. \tag{5}$$

Algorithm 2 shows our hybrid Jacobi method. The `for` loop between Line 4 to 6 reduces the ith basis vector and creates non-zero entries $r_{k,i}$, $k = i+1, ..., j$. The first part of the process `Triangulate` $\mathbf{R}$ eliminates the non-zero entries from $r_{j,i}$ to $r_{i+1,i}$ by the plane rotations [19, 20]. The elimination process will create another sequence of non-zero elements $r_{k+1,k}$, $k = i+1, ..., j-1$ on the subdiagonal. Likewise, the second part of `Triangulate` $\mathbf{R}$ eliminates the newly created non-zero elements from $r_{k+2,k+1}$ to $r_{j,j-1}$ by the plane rotations. Similarly, in line 13, we triangulate $\mathbf{R}$ after swapping the ith and the kth column of $\mathbf{R}$ in line 11. To make the length reduction of basis vectors to be more effective, after each inner `j`-loop, we push the shorter basis vector to the front. In line 14, we introduce a condition for partial size reduction to prevent the lengths of basis vectors from increasing. Specifically, we will not apply the partial size reduction process if it cannot decrease g_{ii}. Notice that the partial size reduction process also changes matrices $\mathbf{G}$ and $\mathbf{Z}$ accordingly. We refer [14, 21] for the detailed procedure of the size reduction.

Input : A basis matrix $\mathbf{A}$ and a reduction factor ω $(1/\sqrt{3} \leq \omega < 1)$
Output: Reduced $\mathbf{A}$

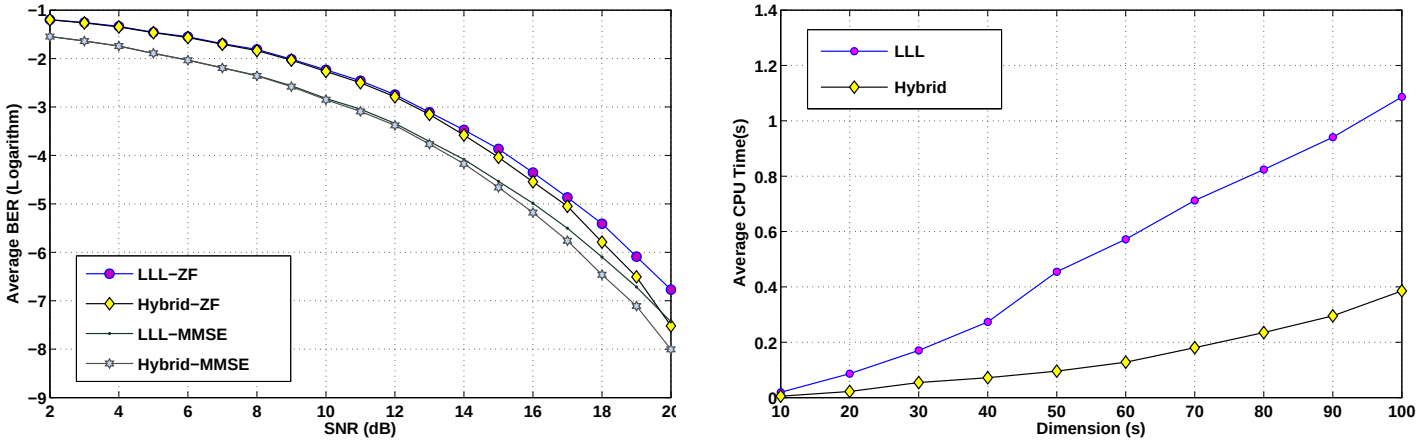
1 $\mathbf{G} = \mathbf{A}^T\mathbf{A}$, $\mathbf{Z} = \mathbf{I}_n$, get $\mathbf{R}$ from the QR decomposition of $\mathbf{A}$;
2 **while** *not all elements* g_{ij} *satisfy (4) and (5)* **do**
3 **for** $i = 1$ **to** n **do**
4 **for** $j = i+1$ **to** n **do**
5 **if** g_{ij} *doesn't satisfy (4) and (5)* **then**
6 $[\mathbf{G}, \mathbf{Z}, \mathbf{R}] \leftarrow$ `Lagrange`$(\mathbf{G}, \mathbf{Z}, \mathbf{R}, i, j)$;
7 Triangulate $\mathbf{R}$ using the plane rotations ;
8 Find an index k $(i \leq k \leq n)$, s.t. $g_{kk} = \min_{l=i}^{n} g_{ll}$;
9 **if** $k \neq i$ **then**
10 Swap the ith and kth columns in $\mathbf{Z}$;
11 Swap the ith and kth columns in $\mathbf{R}$;
12 Swap the ith and kth columns, and the ith and kth rows in $\mathbf{G}$;
13 Triangulate $\mathbf{R}$ using the plane rotations ;
14 Apply partial size reduction on $\mathbf{R}$ w.r.t. $(i-1, i)$ only if g_{ii} is reduced after the application ;
15 $\mathbf{A} = \mathbf{A}\mathbf{Z}$;

Algorithm 2: Hybrid Jacobi method

Let $B = \max_{1 \leq i \leq n} \|\mathbf{a}_i\|_2$. `Lagrange`() reduces the length of a basis vector with a factor of at least ω. Thus, Algorithm 2 calls `Lagrange`() maximum $O(n \log B)$ times [18]. Using vector operations, the time complexities of `Lagrange`() and partial size reduction process are $O(n)$ and $O(n^2)$, respectively. Hence, the number of arithmetic operations needed by Algorithm 2, the hybrid Jacobi method for lattice basis reduction, is $O(n^4 \log B)$, the same as the widely-used LLL algorithm [14].

4. Experimental Results

In signal processing, the performance of radio communications depends on an antenna system. Hence, MIMO has become an essential element of wireless communication standards for wireless LANs, 3G and 4G mobile-phone networks. The lattice reduction technique has been successfully introduced to numerous applications in signal processing for decades. In this section, we simulate data detection process in MIMO systems. In our simulation, we compare the BER performance of the two LR-aided data detection algorithms, the hybrid method and the well-known LLL algorithm, as shown in Fig. 1. Our MIMO systems use 8×8 antennas. The signal noise ratio `SNR` varies from 2 dB to 20 dB. We generate $1,000$ channel matrices for each SNR. The entries of the channel matrices are random Gaussian distributed complex numbers of zero-mean and unit variance. For each channel matrix, we transmit $1,000,000$ random binary bits to the receiver with 4-QAM modulation scheme. Fig. 1 (a) shows that the hybrid method performs better than the LLL algorithm with respect to BER in both ZF and MMSE detection. Fig. 1 (b) indicates that the hybrid method requires about one third of time as the LLL algorithm.



(a) Bit Error Rates (b) Time Performances

Fig. 1: Comparison of the hybrid method and the LLL algorithm in MIMO simulations

5. Conclusion

In this paper, we present a novel hybrid method for lattice reduction aided decoding in MOMO systems. Our experimental results showed that the presented algorithm is empirically much faster than the LLL algorithm. The simulations also showed that the communication channels improved by the hybrid method have smaller BER than the widely used LLL algorithm for 8×8 MIMO systems. Thus the proposed algorithm can be potentially used in large MIMO systems.

References

[1] A. Goldsmith, *Wireless Communications*. New York: Cambridge University Press, 2005.

[2] J. R. Hampton, *Introduction to MIMO Communications*. Cambridge University Press, 2013.

[3] B. Hassibi and H. Vikalo, "On the sphere-decoding algorithm I. Expected complexity," in *IEEE Trans. Sig. Proc*, pp. 2806-2818, 2005.

[4] J. Hoffstein, J. C. Pipher, and J. H. Silverman, *An introduction to mathematical cryptography*. Springer, 2008.

[5] W. H. Mow, "Universal Lattice Decoding: Principle and Recent Advances," *Wireless Communications and Mobile Computing*, vol. 3, pp. 553-569, 2003.

[6] Y. H. Gan and W. H. Mow, "Complex lattice reduction algorithms for low-complexity MIMO detection," in *Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE*, vol. 5, pp. - 2957, 2005.

[7] M. Taherzadeh, A. Mobasher, and A. K. Khandani, "LLL Reduction Achieves the Receive Diversity in MIMO Decoding," *Information Theory, IEEE Transactions on*, vol. 53, no. 12, pp. 4801-4805, 2007.

[8] D. Wübben, D. Seethaler, J. Jalden, and G. Matz, "Lattice Reduction: A Survey with Applications in Wireless Communications," *IEEE Signal Processing Magazine*, vol. 28, no. 3, pp. 70-91, 2011.

[9] J. Jalden and B. Ottersten, "On the complexity of sphere decoding in digital communications," *Signal Processing, IEEE Transactions on*, vol. 53, no. 4, pp. 1474 - 1484, 2005.

[10] H. Minkowski, "Discontinuity region for arithmetical equivalence," *J. reine Angew*, no. 129, pp. 220-274, 1905.

[11] J. L. Donaldson, "Minkowski reduction of integral matrices," *j-MATH-COMPUT*, vol. 33, no. 145, pp. 201-216, 1979.

[12] A. Korkine and G. Zolotareff, "Sur les formes quadratiques," *Mathematische Annalen*, vol. 6, no. 3, pp. 366-389, 1873.

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

[14] A. K. Lenstra and L. Lovász, "Factoring polynomials with rational coefficients," *Math. Ann.*, vol. 261, pp. 515–534, 1982.

[15] L. Bai and J. Choi, *Low Complexity MIMO Detection*. New York: Springer, 2012.

[16] S. Qiao, "A Jacobi Method for Lattice Basis Reduction," in *Proceedings of 2012 Spring World Congress on Engineering and Technology (SCET2012)*, 2012, vol. 2, pp. 649-652.

[17] 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.

[18] Z. Tian and S. Qiao, "A complexity analysis of a Jacobi method for lattice basis reduction," in *Proceedings of the Fifth International C* Conference on Computer Science and Software Engineering*, 2012, pp. 53–60.

[19] G. H. Golub and C. F. Van Loan, *Matrix Computations*, 3rd Ed. The Johns Hopkins University Press, 1996.

[20] F. T. Luk and S. Qiao, ”Conditioning properties of the LLL algorithm,” in *Mathematics for Signal and Information Processing*, vol. 7444, pp. 7444-17. Proc. of SPIE, 2009.
[21] P. Nguyen, ”Lattice Reduction Algorithms: Theory and Practice,” in *Advances in Cryptology - EUROCRYPT 2011*, K. Paterson Ed. vol. 6632, pp. 2-6. Springer Berlin / Heidelberg, 2011.