Analysis of Lattice based Algorithms in Wireless Communication

[1]Maheshwari M
PG Student, ECE Department
SSN College of Engineering
Chennai, India

[2]Joseph Gladwin S
Assistant Professor, ECE Department
SSN College of Engineering
Chennai, India

***Abstract*—Lattice reduction (LR) techniques are developed to improve the performance of multiple-input multiple-output (MIMO) digital communication system. In cryptographic methods the lattice problems are high that is the problem of finding short basis is more. This type of reduction problem have a great impact on many areas of technology mainly in modern cryptanalysis.**

In this paper analysis of various LR technique were carried out based on its speed on the basis of number of operations during the reduction process and also we analyze the path detection of information to be transmitted based on reduced lattice points.

***Keywords*— Lattice reduction; size reduction; gram schmidt orthogonalization; babai point; lenstra lenstra lovasz; schnoor-euchner.**

I. INTRODUCTION

Lattice reduction (LR) has been proposed in the context of multiple input multiple output (MIMO) systems as a means of improving the performance of sub-optimal detectors [9]. This is achieved by pre-processing followed in MIMO channel by an LR algorithm [3], which transforms the channel into a more orthogonal form. The lattice reduction [14] has been successfully used in signal processing applications for global positioning system (GPS), frequency estimation, particularly data detection and pre-coding in wireless communication systems. Beyond mathematics , lattice have various diverse applications such as cryptography, coding theory and so on. It is also used to develop highly realistic source and channel codes for various communication applications, specifically in multiple terminals.

This paper is on the basis of analyzing various lattice reduction algorithms Lenstra [15] and Schnoor-Euchner with its speed and path detection of the information to be transmitted with-respect to the number of operations and the reduced lattice points respectively [16].

II. ALGORITHMS BASED ON LATTICE REDUCTION

A. Lenstra Lenstra Lovasz (LLL) algorithm

In a basis-reduction algorithm, the so called LLL basis reduction [2] is introduced which results in relatively short basis vectors with a polynomial-time computational complexity. A multiple-antenna system with M transmit antennas and N receive antennas $M \le N$ were considered, where different transmit antennas is denoted as different users.

Considering the vectors,

$$Y = [Y_1, Y_2, \ldots., Y_N]^T \qquad (1)$$

$$X = [X_1, X_2, \ldots., X_M]^T \qquad (2)$$

$$W = [W_1, W_2, \ldots, W_N]^T \qquad (3)$$

to be the transmitted, the noise vector and the channel matrix respectively. The channel model is described by the following equation

$$Y = HX + W \qquad (4)$$

The channel is considered to be Rayleigh and the noise is Gaussian that is the elements of H are independent and identically distributed with the zero-mean unit-variance complex Gaussian distribution [4]. The following were the steps involved in LLL algorithm

- Gram Schmidt Orthogonalization (GSO)
- Size-reduction
- Swapping & updating GSO

Gram Schmidt Orthogonalization (GSO) :

The orthogonalization is done by using the following equation

$$V_i^* = V_i - \Sigma_{j=1}^{i-1} \left\{ \left. \langle V_i, V_j^* \rangle \middle/ \left\| V_j^* \right\|^2 \right. \right\} \bullet V_j^* \qquad (5)$$

$i = 1,2,\ldots..,m,$ m is number of column vectors.

Where , $$\mu_{ij} = \left\{ \left\langle V_i, V_j^* \right\rangle \Big/ \left\| V_j^* \right\|^2 \right\} \qquad (6)$$

Size- reduction :

The size-reduction that is in order to reduce the elements of the channel matrix the following equation were taken into account

$$V_i = V_i - \text{round}\left(\mu_{ij}\right) \bullet V_j \qquad (7)$$

Swapping & updating GSO:

Swapping the current size reduced vectors and updating GSO using orthogonalization process.

B. Complex Lenstra Lenstra Lovasz (CLLL) algorithm

The average overall complexity of the complex LLL (CLLL) algorithm is almost half of the real LLL (RLLL) algorithm. In lattice-reduction decoding the CLLL achieve full diversity as that of RLLL. Whereas the bit-error-rate (BER) performance of both the reduced basis with the help of CLLL and RLLL in MIMO detection schemes contribute to be in similar manner. Compare to RLLL, the CLLL compute less complexity because of the avoidance of doubling the channel matrix dimension. Thus, it can reduce the complexity of other parts of the MIMO detector also. By considering the received Symbol vector Y, complex baseband equivalent model can be expressed as

$$Y = HS + V \qquad (8)$$

H is a flat fading channel matrix, S is a complex transmit signal vector of N_T dimensional, V is a Complex Gaussian noise vector of N_R dimensional.

$$H = QR \qquad (9)$$

H, Q is $N_R \times N_T$ dimensional

R is $N_T \times N_T$ dimensional.

The following were the steps involved in CLLL algorithm

- GSO: A modified orthogonalization is followed compare to LLL.
- Size reduction: Similar to the reduction method used in LLL .
- Basis vector swapping: Initially as in LLL , here also the basis vectors were swapped. The idea is that, after swapping, size reduction can be repeated to make basis vectors shorter.

The performance of CLLL is improved from that of LLL because of the use of following conditions.

1) The condition of size reduction is stronger if $\left|\mu_{ij}\right|^2 \le 0.5$ resulting in fewer size reduction computations.

2) The algorithm checks if $\left|\text{Re}\left(\mu_{k,k-1}\right)\right| > 0.5$ or $\left|\text{Im}\left(\mu_{k,k-1}\right)\right| > 0.5$ before doing size-reduction.

The check will avoid unnecessary operations, thus the computational complexity is reduced with increase in speed of the algorithmic computations.

C. Schnoor-Euchner (SE) algorithm

The Schnorr-Euchner algorithm [10] was used in cryptography applications and also mainly in sphere decoding [11]. This algorithm has the same principle as the Viterbo-Boutrous (VB), which is used for the closest point search [13]. It is based on the following two stages.

- The first stage consists of finding the “Babai point” (BP), which is not similar to that of closest point. This point derive bounding error.
- In the second stage, modification of the BP is repeated until the closest point [12] is found. If the BP is very far from the closest point, then the signal to noise ratio (SNR) is low which makes the algorithm to take more time to converge. However, if the BP is close to the closest point, then the SNR is high which makes the algorithm to converge in less time.

D. Schnoor-Euchner Adaptive Search Radius Algorithm

It is similar to that of SEA, where node without children were also applicable and the next siblings is analysed by boundary control. By stacking complex to real conversion is done before Schnoor-Euchner Adaptive LAST (SEAL) sphere algorithm.

III. ANALYSIS OF ALGORITHM IN MATLAB

Analysis of LLL and SE algorithm were carried out using matlab simulation tool. The following simulation results were done .

A. Realization of Lenstra algorithm based on lattice reduction

Considering a two dimensional square matrix,

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

Fig. 1. shows the elements of the channel matrix row wise indicating,

$A(:,1) = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$ the first column vector of A matrix and

$A(:,2) = \begin{bmatrix} 2 \\ 4 \end{bmatrix}$ the second column vector of A matrix.

The number of vectors will vary according to the matrix dimension.

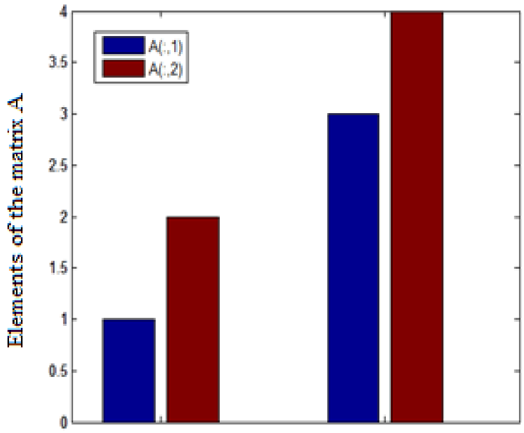

Fig. 1. Elements of the channel matrix before lattice reduction.

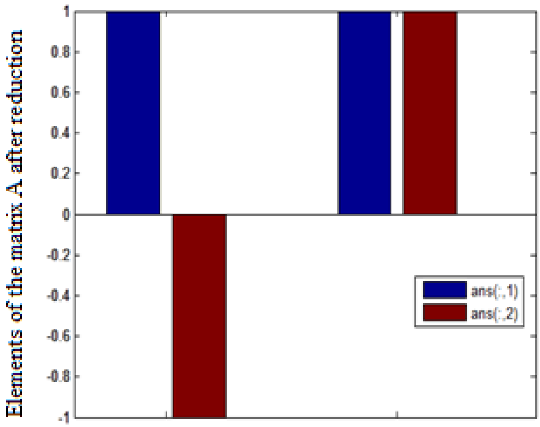

Fig. 2. Elements of the channel matrix after lattice reduction.

Fig. 2. shows representation of less complexity based reduced form of channel matrix due to lattice reduction in Euclidian space. Thus as the elements value reduction will be directly proportional to the orthogonality too.

B. Realization of Schnoor-Euchner algorithm for path detection of the information based on lattice points

In Fig.3.

- The closest lattice point is identified based on the weight of each point which is denoted as node.
- If the weight of the node is less than the distance between the current and the nearest lattice point. This distance threshold is initially set to infinity.
- If the weight of the node under is larger than the distance threshold, the current search path is terminated since it cannot lead to a closest lattice point.

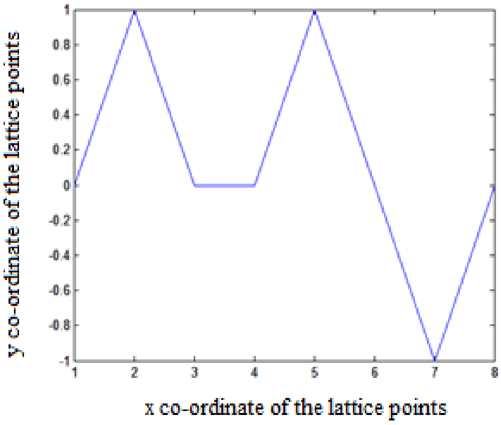

Fig. 3.Path with-respect to lattice points

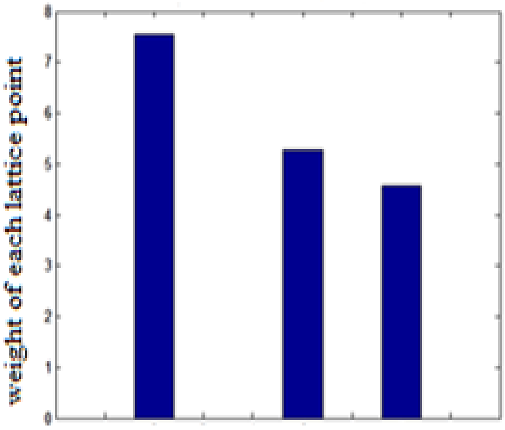

Fig. 4.Weight with-respect to each lattice points

In Fig. 4.the weight of the lattice points is represented in such a way that the previous lattice point weight must be lesser the current lattice point weight.

IV. CONCLUSION

In this paper analysis of various algorithm based on lattice-reduction were carried out. LLL algorithm makes more number of operations in complex channel rather than real channel because of the absence of complexity due to imaginary part. Whereas the number of operations is reduced for both complex and real channel in CLLL algorithm due to the conditions followed in size reduction based on the mean square value.

For path detection with respect to lattice points analysis of schnoor-euchner algorithm was carried out, where real channel can be applicable in SEAL and complex channel for SEA. Using Schnoor the path of the information where the effect of external disturbance is maintained to be less in impact is analysed with the help of the lattice points and the lattice points were considered to be identified such that their weight must be in descending order from its initial lattice point.

REFERENCES

[1] Mahmoud Taherzadeh, Amin Mobasher and Amir K.Khandani, “Communication Over MIMO Broadcast Channels Using Lattice-Basis Reduction,” IEEE Trans. on Information theory, vol. 53, no. 12, Dec. 2007.

[2] Taherzadeh, A.Mobasher and A.K.Khandani, “LLL reduction achieves the receive diversity in MIMO decoding,” IEEE Trans. on Information Theory, vol. 53, no. 12, Dec. 2007, pp. 4801–4805.

[3] Wubben and D.Seethaler, “On the performance of lattice reduction schemes for MIMO data detection,” in Proc. IEEE Asilomar, Pacific Grove, CA, Nov. 2007, pp. 1534–1538.

[4] Bruderer, C.Studer, D.Seethaler, M.Wenk, and A.Burg, “VLSI implementation of a low-complexity LLL lattice reduction algorithm for MIMO detection,” in Proc. IEEE ISCAS, Paris, France,May 2010,pp. 3745–3748.

[5] P.Nguyen, J. Stern, “The two faces of lattices in cryptology,” in Proc CALC, Springer, LNCS, vol. 2146, 2001, pp.146–180.

[6] YAP. “Fundamental problems in algorithmic algebra,” Princeton University Press 1996.

[7] H. W. Lenstra, “Integer programming with a fixed number of variables,” Mathematics of Operations Research, vol. 8, 4, 1983, pp.538–548.

[8] H. COHEN. A course in Computational Algebraic Number Theory, GTM 138, Springer Verlag, 4th Edition 2000.

[9] Yao and G. W. Wornell, “Lattice-reduction-aided detectors for MIMO communication systems,” in Proc. IEEE GLOBECOM, vol. 1, Taipei, Taiwan, Nov. 2002, pp.424–428.

[10] Zhan Guo and Peter Nilsson. ”Reduced Complexity Schnorr–Euchner Decoding Algorithms for MIMO systems,” in Proc. IEEE Communications Letters, vol. 8, no. 5, May 2004.

[11] J. Jald´en and B. Ottersten, “On the complexity of sphere decoding in digital communications,”IEEE Trans. on Signal Process-ing,vol. 53, no. 4, pp. 1474–1484, 2005.

[12] M. O. Damen, H. E. Gamal, and G. Caire, “On maximum likeli-hood detection and the search for the closest lattice point,”IEEE Trans. on Information Theory, vol. 49, no. 10, pp. 2389–2402, 2003.

[13] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, “Closest point search in lattices,”IEEE Trans. on Information Theory, vol. 48, no. 8, pp. 2201–2214, 2002.

[14] C. Schnorr and M. Euchner, “Lattice basis reduction: improved practical algorithms and solving subset sum problems,”Mathemat-ical Programming, vol. 66, pp. 181–191, 1994.

[15] L. Babai, “On Lovasz lattice reduction and the nearest lattice point problem,”Combinatorica, vol. 6, no. 1, pp. 1–13, 1986

[16] B. A. LaMacchia, “Basis reduction algorithms and subset sum problems,” Master’s thesis, Massachusetts Inst. Technol., May 1991