A Multiple Lattice Reduction Based Detector for Space Time Block Codes based on Cyclotomic Extensions

Aditya Gopalan and Srikrishna Bhashyam

***Abstract*— Full diversity high-rate Space Time Block Codes (STBCs) based on cyclotomic field extensions $\mathbb{Q}(\omega_l)$, where ω_l is the complex lth root of unity, can be decoded by Lenstra-Lenstra-Lovász (LLL) lattice reduction-aided linear equalization followed by appropriate zero forcing. LLL lattice reduction-aided linear equalization enables lower complexity decoding compared to sphere decoding, while resulting in a performance loss. In this paper, we propose a new suboptimal detection algorithm which exploits the algebraic structure of this class of STBCs and applies LLL lattice reduction-based detection multiple times on the received space-time symbol to arrive at an estimate of the transmitted codeword matrix. The decoding complexity is still significantly lower than sphere decoding complexity. Using simulations, the proposed scheme is shown to perform better than the conventional LLL reduction-based scheme in terms of bit error rate. We also point out that the computational effort for the multiple lattice reduction-based scheme can be significantly reduced for codes over certain numbers of transmit antennas.**

I. Introduction

Full-rank and minimal-delay space time block codes constructed using field extensions [1] offer flexibility in design with respect to number of transmit antennas, while providing advantages like information losslessness. However, due to their non-orthogonal nature, they cannot be decoded using simple receiver-side linear processing. We have to resort to generic approaches like sphere decoding [2] for maximum likelihood (ML) detection. Though sphere decoding for such STBCs yields optimal error performance, it is costly in terms of complexity [3]. It is interesting to consider suboptimal alternatives such as linear equalization aided by Lenstra-Lenstra-Lovász (LLL) lattice reduction [4], which is computationally cheap and is proved to achieve full receive diversity in multiple-input-multiple-output (MIMO) systems [5]. The complexity of LLL reduction, unlike that of sphere decoding, stays constant and is unaffected by parameters like signal-to-noise ratio and constellation size.

LLL reduction-based decoding is a generic detection approach for the case of MIMO systems employing lattice signal constellations like QAM. We desire a decoding scheme specific to the structure of STBCs derived from cyclotomic field extensions, which can provide better error performance than conventional LLL reduction based decoding while being lower in complexity than sphere decoding. In the following sections, we first describe the process of LLL lattice reduction-aided detection for a MIMO system which uses STBCs based on cyclotomic extensions. We then propose a detection scheme that employs LLL lattice reduction-aided detection multiple times to extract more information out of the received symbol. Simulations for systems with 2, 3 and 4 transmit antennas show that this scheme provides an advantage in terms of bit-error performance over single LLL lattice reduction-aided decoding.

II. System Model

We consider a MIMO-STBC system with n transmit and m receive antennas, communicating over a Rayleigh flat fading channel with additive white Gaussian noise (AWGN). Data to be sent over the wireless link is divided into fixed-length blocks. Each block is mapped to a corresponding $n \times n$ complex space time codeword matrix $\mathbf{X}$, whose entries represent symbols derived from a QAM signal set used by the transmitter. The codeword matrix $\mathbf{X}$ is transmitted column-wise from the n transmit antennas, over n symbol periods. We let an $m \times n$ matrix $\mathbf{H}$ denote the fading wireless channel, with its entries as independent zero-mean complex Gaussian random variables having variance 0.5 for the real and imaginary parts. An array of m receive antennas captures the received $m \times n$ signal $\mathbf{Y}$ over n symbol periods. The AWGN is represented by an $m \times n$ matrix $\mathbf{W}$ with independent, circularly symmetric, zero-mean complex Gaussian-distributed entries. The system equation is thus

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{W} \tag{1}$$

We restrict the matrix $\mathbf{X}$ to be associated with a space-time block code derived from the nth cyclotomic field extension. Such a code is obtained by the technique of embedding a cyclotomic extension in a complex matrix ring, as described in [1]. The form of such an $n \times n$ STBC $\mathcal{C}$ is given by

$$\begin{aligned}\mathcal{C} = \{f_0\mathbf{I}_n + f_1\mathbf{M} + f_2\mathbf{M}^2 + \cdots + f_{n-1}\mathbf{M}^{n-1} \mid \\ f_i \in \text{QAM},\ \ i = 0, \ldots, n-1\}\end{aligned} \tag{2}$$

The matrix $\mathbf{M}$ in this equation has the structure

$$\mathbf{M} = \begin{bmatrix} 0 & 0 & \cdots & 0 & \omega_n \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & 0 & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \tag{3}$$

where $\omega_n = e^{j\frac{2\pi}{n}}$ and $f_0, \ldots, f_{n-1}$ denote independent complex QAM symbols which are essentially functions of

The authors are with the Department of Electrical Engineering, Indian Institute of Technology Madras, Chennai 600036, India. {gadit,skrishna}@ee.iitm.ac.in

the input data block. Note that $\mathbf{M}^n = \omega_n \mathbf{I}_n$, where $\mathbf{I}_n$ is the identity matrix of size n.

For the setup described above, the maximum likelihood detection rule takes the form

$$\hat{\mathbf{X}} = \arg\max_{\mathbf{X}\in\mathcal{C}} ||\mathbf{Y} - \mathbf{H}\mathbf{X}||_F \tag{4}$$

where $\hat{\mathbf{X}}$ is the maximum likelihood estimate for the transmitted codeword matrix $\mathbf{X}$.

III. Lattice Reduction-aided Zero Forcing Detection

To effectively apply LLL Lattice Reduction-aided Zero Forcing (LRZF) to our STBC, we first transform the STBC transmission equation (1) to a real, vector form, as suggested by [6]. The procedure consists of first vectorizing $\mathbf{Y}$, $\mathbf{X}$ and $\mathbf{W}$ and then appropriately separating the real and imaginary matrix parts from the resulting equation. We arrive at the equation

$$\mathbf{s} = \mathbf{G}\mathbf{r} + \mathbf{n} \tag{5}$$

where $\mathbf{s}$ and $\mathbf{n}$ are real $2mn \times 1$ vectors, $\mathbf{G}$ is a $2mn \times 2n$ real matrix and $\mathbf{r}$ is a $2n \times 1$ integer vector (lowercase quantities denote vectors). The integer property of $\mathbf{r}$ is due to the fact that the transmitters use a rectangular lattice constellation (QAM in this case) which, after suitable scaling, takes integer coordinates.

Conventional LLL lattice reduction-aided linear equalization, as detailed in [7], first finds an equivalent lattice generator matrix $\tilde{\mathbf{G}} = \mathbf{G}\mathbf{T}$ (with $\mathbf{T}$ a unimodular integer matrix) such that the columns of $\tilde{\mathbf{G}}$ are 'roughly orthogonal'. The Lenstra-Lenstra-Lovász criteria for near-orthogonality were first specified in [4]. By introducing the integer vector $\mathbf{z} = \mathbf{T}^{-1}\mathbf{r}$, we can write (5) as

$$\mathbf{s} = \mathbf{G}\mathbf{r} + \mathbf{n} = \mathbf{G}\mathbf{T}\mathbf{T}^{-1}\mathbf{r} + \mathbf{n} = \tilde{\mathbf{G}}\mathbf{z} + \mathbf{n} \tag{6}$$

The LLL-reduced matrix $\tilde{\mathbf{G}}$ is usually much better conditioned than the original matrix $\mathbf{G}$; we premultiply the above equation by $\tilde{\mathbf{G}}^+$ - the pseudoinverse of $\tilde{\mathbf{G}}$ - and round the result $\mathbf{s}_{LRZF}$ to the nearest integer vector:

$$\mathbf{s}_{LRZF} = \tilde{\mathbf{G}}^+\mathbf{s} = \mathbf{z} + \tilde{\mathbf{G}}^+\mathbf{n} \tag{7}$$

Multiplying the rounded result by $\mathbf{T}$ yields the LLL reduction-aided estimate for $\mathbf{r}$ and hence an estimate for $\mathbf{X}$. This decoding procedure can be applied to any STBC which uses transmit symbols from a lattice-based constellation. In the next section, we utilize the algebraic structure of STBCs based on cyclotomic extensions to devise a multiple LLL reduction-based decoding scheme for such codes.

IV. Proposed Decoding Scheme

For deriving our detection scheme based on multiple LLL reduction, we rewrite the transmission-reception model (1) for the case of STBCs derived from cyclotomic extensions as

$$\mathbf{Y} = \mathbf{H}(f_0\mathbf{I}_n + f_1\mathbf{M} + f_2\mathbf{M}^2 + \cdots + f_{n-1}\mathbf{M}^{n-1}) + \mathbf{W} \tag{8}$$

where $f_0, \ldots, f_{n-1}$ belong to QAM. Post-multiplying the above equation throughout by $\mathbf{M}$ yields

$$\begin{aligned}\mathbf{Y}\mathbf{M} &= \mathbf{H}(f_0\mathbf{M} + f_1\mathbf{M}^2 + f_2\mathbf{M}^3 + \cdots + f_{n-1}\mathbf{M}^n) + \mathbf{W}\mathbf{M}\\ &= \mathbf{H}(\omega_n f_{n-1}\mathbf{I}_n + f_0\mathbf{M} + f_1\mathbf{M}^2 + f_2\mathbf{M}^3 + \cdots\\ &\qquad + f_{n-2}\mathbf{M}^{n-1}) + \mathbf{W}\mathbf{M}\end{aligned} \tag{9}$$

which is functionally similar to (8), with $f_0, f_1, \ldots, f_{n-1}$ replaced by $\omega_n f_{n-1}, f_0, \ldots, f_{n-2}$. We successively multiply (8) by $\mathbf{M}^2, \ldots, \mathbf{M}^{n-1}$ and appropriately rearrange in ascending powers of $\mathbf{M}$ to get

$$\begin{aligned}\mathbf{Y}\mathbf{M}^2 &= \mathbf{H}(\omega_n f_{n-2}\mathbf{I}_n + \omega_n f_{n-1}\mathbf{M} + f_0\mathbf{M}^2 + f_1\mathbf{M}^3 +\\ &\qquad \cdots + f_{n-3}\mathbf{M}^{n-1}) + \mathbf{W}\mathbf{M}^2\\ \mathbf{Y}\mathbf{M}^3 &= \mathbf{H}(\omega_n f_{n-3}\mathbf{I}_n + \omega_n f_{n-2}\mathbf{M} + \omega_n f_{n-1}\mathbf{M}^2 +\\ &\qquad f_0\mathbf{M}^3 + \cdots + f_{n-4}\mathbf{M}^{n-1}) + \mathbf{W}\mathbf{M}^3\\ \vdots \quad & \quad \vdots\\ \mathbf{Y}\mathbf{M}^{n-1} &= \mathbf{H}(\omega_n f_1\mathbf{I}_n + \omega_n f_2\mathbf{M} + \omega_n f_3\mathbf{M}^2 + \omega_n f_4\mathbf{M}^3 +\\ &\qquad \cdots + f_0\mathbf{M}^{n-1}) + \mathbf{W}\mathbf{M}^{n-1}\end{aligned} \tag{10}$$

We note that $\mathbf{M}\mathbf{M}^H = \mathbf{M}^H\mathbf{M} = \mathbf{I}_n$, hence $\mathbf{M}$ is a unitary matrix and the products $\mathbf{W}\mathbf{M}^i, i = 1, \ldots, n-1$ still retain AWGN properties. The scheme we propose is to apply lattice reduction zero forcing detection independently on each of the above n equations and derive n estimates $\hat{\mathbf{X}}_i, i = 0, \ldots, n-1$ for the transmitted codeword. If all the obtained estimates agree ($\hat{\mathbf{X}}_0 = \cdots = \hat{\mathbf{X}}_{n-1}$), we are through and our final estimate is this common codeword. Since each of the estimates $\mathbf{X}_i$ obtained by LLL reduction-aided zero forcing is suboptimal, there is a possibility of the estimates being different. If there is a discrepancy in the n estimates, i.e. two of more estimates differ, then we pick the most likely of the two estimates (simple resolution):

$$\hat{\mathbf{X}} = \arg\min_{i\in\{0,\ldots,n-1\}} ||\mathbf{Y} - \mathbf{H}\hat{\mathbf{X}}_i||_F^2 \tag{11}$$

where $||\cdot||_F$ denotes the Frobenius matrix norm operation.

In effect, we perform n lattice reduction zero forcing procedures and make a simple norm-based decision on the results returned by these procedures, hoping to get a more likely estimate of the transmitted codeword. To see in detail how multiple estimates are obtained using LLL-based lattice reduction zero forcing, note that lattice reduction involves transforming (8) to the form of (5) as follows:

$$\begin{aligned}\mathbf{Y} &= \mathbf{H}\mathbf{X} + \mathbf{W}\\ \Rightarrow \text{vec}(\mathbf{Y}) &= \tilde{\mathbf{H}}\text{vec}(\mathbf{X}) + \text{vec}(\mathbf{W})\\ \text{i.e. } \tilde{\mathbf{y}} &= \tilde{\mathbf{H}}\mathbf{K}\mathbf{f} + \tilde{\mathbf{w}}\\ &= \tilde{\mathbf{G}}\mathbf{f} + \tilde{\mathbf{w}} \qquad (12)\\ \therefore \tilde{\mathbf{y}}' &= \tilde{\mathbf{G}}'\mathbf{f}' + \tilde{\mathbf{w}}' \qquad (13)\end{aligned}$$

where $\mathbf{f} = \begin{bmatrix} f_0 & f_1 & \ldots & f_{n-1} \end{bmatrix}^T$, for the base case of (8). The operation $\text{vec}(\cdot)$ stacks up the columns of a matrix into a vector. $\mathbf{K}$ is a transform from the vector of independent symbols $\mathbf{f}$ to the vector form of the space-time codeword matrix $\mathbf{X}$. For (9), according to the above procedure, $\mathbf{f} = \left[\begin{array}{cccc} \omega_n f_{n-1} & f_0 & \dots & f_{n-2} \end{array}\right]^T$. In this case, the vector $\mathbf{f}$ is modified to $\left[\begin{array}{cccc} f_{n-1} & f_0 & \dots & f_{n-2} \end{array}\right]^T$ - a cyclic shift of the original $\mathbf{f}$ vector - while suitably modifying the matrix $\tilde{\mathbf{G}}$ in (12) by multiplying its first column by ω_n. This ensures that the product $\tilde{\mathbf{G}}\mathbf{f}$ remains the same. The next step separates the real and imaginary parts of (12), as described in [6], to yield (13) which is of the form shown in (5). LLL-reduction and zero forcing proceed subsequently to yield estimates for $f_0, f_1, \dots, f_{n-1}$. A similar method is followed for (10) corresponding to multiplication by higher powers of $\mathbf{M}$.

We make the important observation that in the case of STBCs constructed using the cyclotomic field extension $\mathbb{Q}(\omega_4) = \mathbb{Q}(j)$, the codeword matrices are of the form described in (3) with $\gamma = \omega_4 = j$. With the symbols $f_0, f_1, \dots, f_{n-1}$ all coming from a rectangular QAM constellation (which is a subset of $\mathbb{Q}(j)$), all the entries of all codeword matrices are completely over QAM (instead of rotated QAM symbols), whence we *need to perform LLL reduction only once*. Hence, the matrix $\tilde{\mathbf{G}}$ and the vector $\mathbf{f}$ in (12) need no modification since $\mathbf{f}$ is completely over the QAM signal set. A single LLL reduction for the matrix $\tilde{\mathbf{G}}$ in (13) is enough to zero-force the set of equations (8), (9) and (10). This strategy can be applied to codes derived from the extension $\mathbb{Q}(j)$ for any 2^k transmit antennas, using the irreducibility of $x^{2^k} - j$ over $\mathbb{Q}(j)$ as shown in [1].

As an alternative to choosing the estimate yielding minimum distance as suggested by (11), we can perform sphere decoding in the case of a discrepancy in the n LRZF estimates (ML resolution). This produces an increase in overall detection complexity compared to simple resolution described above; however we can speed up the sphere decoder significantly by giving it a search radius equal to the minimum distance found in (11), a method known as using the *Babai estimate* [8]. In this manner, we ensure that at least one valid codeword is tested inside the sphere, at the same time reducing the number of possible candidates being tested. The error performance of the ML resolution strategy helps to lower-bound the performance of the scheme based on simple minimum-distance resolution.

A block diagram of the proposed decoder based on multiple LLL lattice reduction is shown in Figure 1.

V. Results and Discussion

The bit-error performance of plain zero forcing (ZF), lattice reduction-aided zero forcing (LRZF), multiple LRZF with simple resolution, multiple LRZF with ML resolution and ML (sphere) decoding methods applied to STBCs based on cyclotomic extensions over a 16-QAM signal set, for 2, 3 and 4 antennas, are shown in Figures 2, 3 and 4 respectively. It follows from the plots that as the number of transmit (and receive) antennas increases, the scheme based on simple resolution (11) performs much better than conventional lattice reduction-aided zero forcing and closely approaches the ML resolution strategy in terms of error performance.

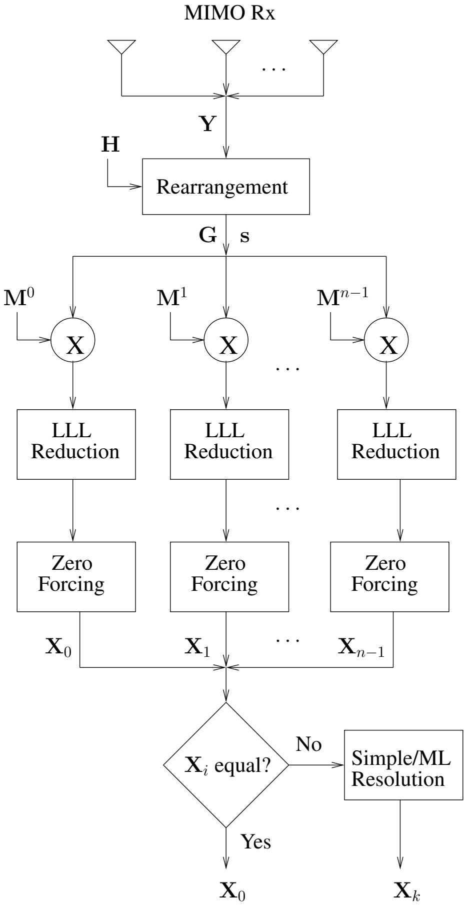

Fig. 1. Block diagram of proposed STBC decoder using multiple LLL reduction

For the case of the 2 × 2 code, the curves for multiple LRZF detection (simple resolution and ML resolution) are lower than that of LRZF by a fraction of a dB. The difference in performance between the multiple decoding and single decoding LRZF methods increases to about 0.5 dB for the 3 × 3 code at high SNR ($\geq$ 20 dB), and 1 dB for the 4 × 4 code, at moderate SNR (15 to 20 dB). The intuitive understanding behind the increase in performance of multiple lattice reduction is that there is more information extracted from the received signal, thereby producing a more likely estimate of the transmitted codeword. Also, deviations from the optimal estimate for a single lattice reduction decoder are better 'averaged out' if multiple reduction is followed.

It is instructive to note, from the presented simulation results, that the slope of the LLL-based detection curves tends to the slope of the ML detection curve with increasing SNR. This helps verify the fact that LLL reduction based

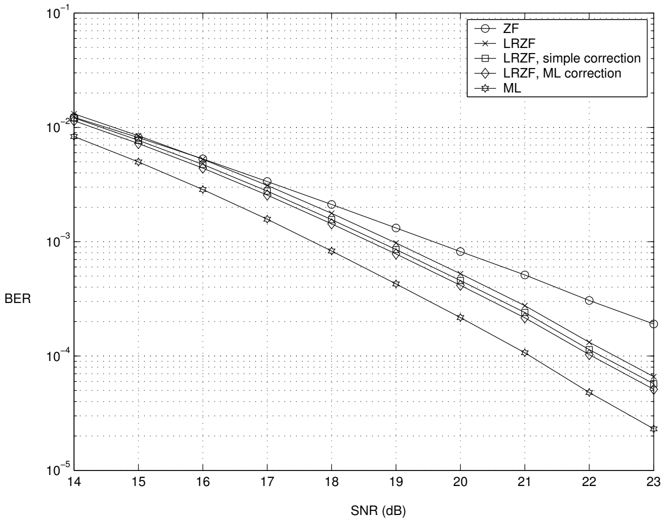

Fig. 2. Bit error performance comparison of decoding methods for 2×2 STBC based on the cyclotomic field extension $\mathbb{Q}(\omega_4)$

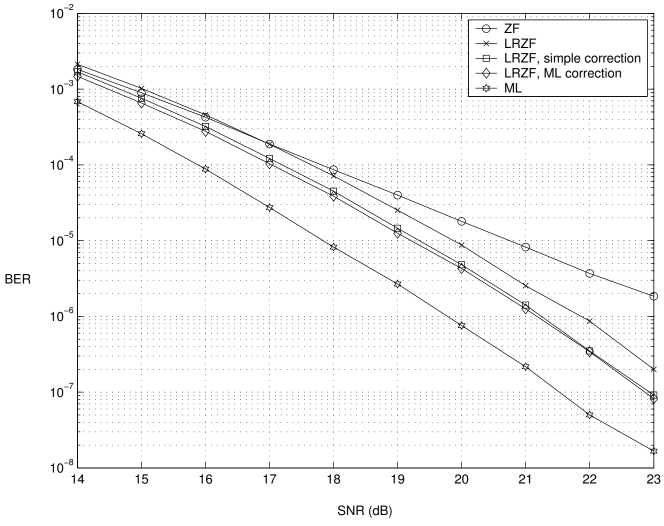

Fig. 3. Bit error performance comparison of decoding methods for 3×3 STBC based on the cyclotomic field extension $\mathbb{Q}(\omega_3)$

detection achieves the full receive diversity in MIMO systems [5].

In the performance graphs, we note that LLL reduction-aided zero forcing performs worse than plain zero forcing in the low SNR regime. The effect is also noted in the LRZF detection performance graphs in [7]. This phenomenon is due to the fact that lattice reduction-aided zero forcing, as stated by (6) and (7), involves rounding to the integer vector $\mathbf{z} = \mathbf{T}^{-1}\mathbf{r}$. Since integer rounding to the closest element of $\mathbf{T}^{-1}\mathbf{r}$ is computationally nontrivial, we choose to first round $\mathbf{s}_{LRZF}$ to the nearest integer vector, apply $\mathbf{T}$ to it and then round the result again to within the limits of the QAM signal set being used, introducing a degradation in performance at lower SNRs.

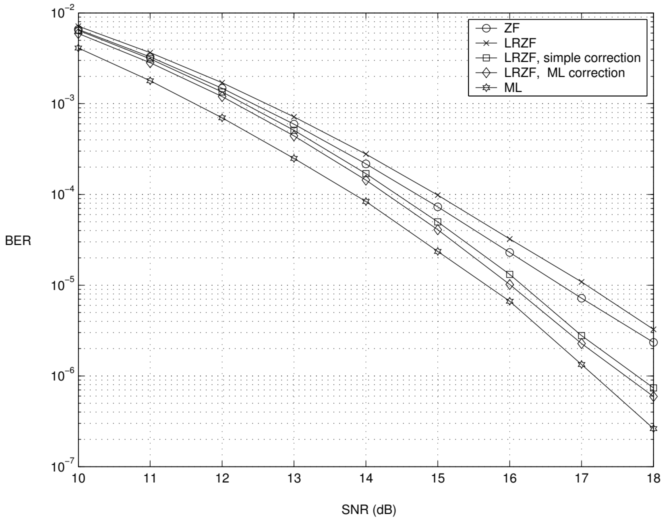

Fig. 4. Bit error performance comparison of decoding methods for 4×4 STBC based on the cyclotomic field extension $\mathbb{Q}(\omega_4)$

From an architectural point of view, the proposed multiple LLL lattice reduction strategy naturally lends itself to parallel implementation; each lattice reduction based decoder operates independent of the others. The observation that using simple norm-based resolution (11) in conjunction with multiple lattice reduction provides performance nearly equal to using ML resolution suggests that one need not use specialized hardware for sphere decoding in the presence of already available lattice reduction-aided detectors. Furthermore, complexity improvements to the basic LLL reduction detector are possible, as suggested in [9].

VI. Summary

We conclude that the detection scheme based on multiple LLL reduction-aided zero forcing followed by simple norm-based resolution, for STBCs based on cyclotomic extensions, yields a performance gain over single LRZF detection. Detection based on the simple resolution strategy yields error performance very close to that of the ML resolution strategy. The additional complexity of multiple LLL reduction can be overcome by parallel implementation of LRZF decoders. For 2^k transmit antennas, the nature of the cyclotomic STBCs allows for a significant reduction in decoding complexity - in such cases, LLL reduction needs to be applied only once, followed by multiple zero-forcing operations and simple resolution of the multiple estimates.

References

[1] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. on Info. Theory*, vol. 49, no. 10, pp. 2596–2616, October 2003.

[2] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. on Info. Theory*, vol. 44, no. 5, pp. 1639–1642, 1999.

[3] J. Jaldén and B. Ottersten, "On the limits of sphere decoding," in *International Symposium on Info. Theory*. IEEE, 2005.

[4] A. K. Lenstra, H. W. Lenstra, and L. Lovász, “Factoring polynomials with rational coefficients,” *Math. Ann.*, vol. 261, pp. 515–534, 1982.

[5] M. Taherzadeh, A. Mobasher, and A. K. Khandani, “LLL lattice-basis reduction achieves the maximum diversity in MIMO systems,” in *International Symposium on Info. Theory*. IEEE, 2005.

[6] M. O. Damen, A. Chkeif, and J. C. Belfiore, “Lattice code decoder for space-time codes,” *IEEE Communications Letters*, vol. 4, no. 5, pp. 161–163, May 2000.

[7] D. Wübben, R. Böhnke, V. Kühn, and K.-D. Kammeyer, “Near-maximum-likelihood detection of MIMO systems using MMSE-based lattice reduction,” in *IEEE International Conf. on Communications*. IEEE, June 2004, pp. 798–802.

[8] B. Hassibi and H. Vikalo, “On the sphere-decoding algorithm I: Expected complexity,” *IEEE Trans. on Signal Processing*, vol. 53, no. 8, pp. 2806–2818, August 2002.

[9] C.-P. Schnorr, “Fast LLL-type lattice reduction.” *Inf. Comput.*, vol. 204, no. 1, pp. 1–25, 2006.