Communication Over MIMO Broadcast Channels Using Lattice-Basis Reduction[1]

Mahmoud Taherzadeh, Amin Mobasher, and Amir K. Khandani

Coding & Signal Transmission Laboratory
Department of Electrical & Computer Engineering
University of Waterloo
Waterloo, Ontario, Canada, N2L 3G1

Abstract

A new viewpoint for adopting the lattice reduction in communication over MIMO broadcast channels is introduced. Lattice basis reduction helps us to reduce the average transmitted energy by modifying the region which includes the constellation points. The new viewpoint helps us to generalize the idea of lattice-reduction-aided precoding for the case of unequal-rate transmission, and obtain analytic results for the asymptotic behavior (SNR$\longrightarrow \infty$) of the symbol-error-rate for the lattice-reduction-aided precoding and the perturbation technique. Also, the outage probability for both cases of fixed-rate users and fixed sum-rate is analyzed. It is shown that the lattice-reduction-aided method, using LLL algorithm, achieves the optimum asymptotic slope of symbol-error-rate (called the precoding diversity).

I. Introduction

In the recent years, communications over multiple-antenna fading channels has attracted the attention of many researchers. Initially, the main interest has been on the point-to-point Multiple-Input Multiple-Output (MIMO) communications [1]–[5]. In [1] and [2], the authors have shown that the capacity of a MIMO point-to-point channel increases linearly with the minimum number of the transmit and the receive antennas.

More recently, new information theoretic results [6], [7], [8], [9] have shown that in multiuser MIMO systems, one can exploit most of the advantages of multiple-antenna systems. It has been shown that in a MIMO broadcast system, the sum-capacity grows

[1]This work was supported in part by funding from Communications and Information Technology Ontario (CITO), Nortel Networks, and Natural Sciences and Engineering Research Council of Canada (NSERC). The material of this paper was presented at the IEEE International Symposium on Information Theory, Adelaide, Australia, September 2005.

linearly with the minimum number of the transmit and receive antennas [7], [8], [9]. To achieve the sum capacity, some information theoretic schemes, based on dirty-paper coding, are introduced. Dirty-paper coding was originally proposed for the Gaussian interference channel when the interfering signal is known at the transmitter [10]. Some methods, such as using nested lattices, are introduced as practical techniques to achieve the sum-capacity promised by the dirty-paper coding [11]. However, these methods are not easy to implement.

As a simple precoding scheme for MIMO broadcast systems, the channel inversion technique (or zero-forcing beamforming [6]) can be used at the transmitter to separate the data for different users. To improve the performance of the channel inversion technique, a zero-forcing approximation of the dirty paper coding (based on QR decomposition) is introduced in [6] (which can be seen as a scalar approximation of [11]). However, both of these methods are vulnerable to the poor channel conditions, due to the occasional near-singularity of the channel matrix (when the channel matrix has at least one small eigenvalue). This drawback results in a poor performance in terms of the symbol-error-rate for the mentioned methods [12].

In [12], the authors have introduced a *vector perturbation technique* which has a good performance in terms of symbol error rate. Nonetheless, this technique requires a lattice decoder which is an NP-hard problem. To reduce the complexity of the lattice decoder, in [13]–[16], the authors have used lattice-basis reduction to approximate the closest lattice point (using Babai approximation).

In this paper, we present a new viewpoint for the MIMO broadcast channel based on the lattice-basis reduction. Instead of approximating the closest lattice point in the perturbation problem, we use the lattice-basis reduction to reduce the average transmitted energy by reducing the second moment of the fundamental region generated by the lattice basis. As we will see later, this viewpoint helps us to: (i) achieve a better performance as compared to [14], for the case that the data consists of odd integers (e.g. regular QAM constellations), (ii) extend the idea for the case of unequal-rate transmission, and (iii) obtain some analytic results for the asymptotic behavior (SNR$\longrightarrow \infty$) of the symbol-error-rate for both the proposed technique and the perturbation technique of [12].

The rest of the paper is organized as the following: Sections II and III briefly describe the system model and introduce the concept of lattice basis reduction. In section IV, the proposed method is described and in section V, the proposed approach is extended for the case of unequal-rate transmission. In section VI, we consider the asymptotic performance of the proposed method for high SNR values, in terms of the probability of error. We define the precoding diversity and the outage probability for the case of fixed-rate users. It is shown that by using lattice basis reduction, we can achieve the maximum precoding diversity. For the proof, we use a bound on the orthogonal deficiency of an LLL-reduced basis. Also, an upper bound is given for the probability that the length of the shortest vector of a lattice (generated by complex Gaussian vectors) is smaller than a given value. Using this result, we also show that the perturbation technique achieves the maximum precoding diversity. In section VII, some simulation results are presented. These results show that the proposed method offers almost the same performance as [12] with a much smaller complexity. As compared to [14], the proposed method offers almost the same performance. However, by sending a very small amount of side information (a few bits for one fading block), the modified proposed method offers a better performance with a similar complexity (detailed discussion about the relevance with [14] is presented in section IV). Finally, in section VIII, some concluding remarks are presented.

II. System Model and Problem Formulation

We consider a multiple-antenna broadcast system with N transmit antennas and M single-antenna users ($N \geq M$). Consider $\mathbf{y} = [y_1, ..., y_M]^T$, $\mathbf{x} = [x_1, ..., x_N]^T$, $\mathbf{w} = [w_1, ..., w_M]^T$, and the $M \times N$ matrix $\mathbf{H}$, respectively, as the received signal, the transmitted signal, the noise vector, and the channel matrix. The transmission over the channel can be formulated as,

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{w}. \tag{1}$$

The channel is assumed to be Raleigh, i.e. the elements of $\mathbf{H}$ are i.i.d. with the zero-mean unit-variance complex Gaussian distribution and the noise is i.i.d. additive Gaussian. Moreover, we have the energy constraint on the transmitted signal, $\mathrm{E}(\|\mathbf{x}\|^2) = 1$. The energy

of the additive noise is σ^2 per antenna, i.e. $\mathrm{E}(\|\mathbf{w}\|^2) = M\sigma^2$. The Signal-to-Noise Ratio (SNR) is defined as $\rho = \frac{1}{\sigma^2}$.

In a broadcast system, the receivers do not cooperate with each other (they should decode their respective data, independently). The main strategy in dealing with this restriction is to apply an appropriate precoding scheme at the transmitter. The simplest method in this category is using the channel inversion technique at the transmitter to separate the data for different users:

$$\mathbf{s} = \mathbf{H}^{+}\mathbf{u}, \tag{2}$$

where $\mathbf{H}^{+} = \mathbf{H}^{\mathtt{H}}(\mathbf{H}\mathbf{H}^{\mathtt{H}})^{-1}$, and $\mathbf{H}^{\mathtt{H}}$ is the Hermitian of $\mathbf{H}$. Moreover, $\mathbf{s}$ is the transmitted signal before the normalization ($\mathbf{x} = \dfrac{\mathbf{s}}{\sqrt{\mathrm{E}(\|\mathbf{s}\|^2)}}$ is the normalized transmitted signal), and $\mathbf{u}$ is the data vector, i.e. u_i is the data for the i'th user. For $N = M$ (the number of transmit antennas and the number of users are equal), the transmitted signal is

$$\mathbf{s} = \mathbf{H}^{-1}\mathbf{u}. \tag{3}$$

The problem arises when $\mathbf{H}$ is poorly conditioned and $\|\mathbf{s}\|$ becomes very large, resulting in a high power consumption. This situation occurs when at least one of the singular values of $\mathbf{H}$ is very small which results in vectors with large norms as the columns of $\mathbf{H}^{+}$. Fortunately, most of the time (especially for high SNRs), we can combat the effect of a small singular value by changing the supporting region of the constellation which is the main motivation behind the current article.

When the data of different users are selected from $\mathbb{Z}[i]$, the overall constellation can be seen as a set of lattice points. In this case, lattice algorithms can be used to modify the constellation. Especially, lattice-basis reduction is a natural solution for modifying the supporting region of the constellation.

III. Lattice-Basis Reduction

Lattice structures have been frequently used in different communication applications such as quantization or decoding of MIMO systems. A real (or complex) lattice Λ is a discrete set of N-D vectors in the real Euclidean space $\mathbb{R}^N$ (or the complex Euclidean space

$\mathbb{C}^N$) that forms a group under ordinary vector addition. Every lattice Λ is generated by the integer linear combinations of some set of linearly independent vectors $\mathbf{b}_1, \cdots, \mathbf{b}_M \in \Lambda$, where the integer M, $M \leq N$, is called the dimension of the lattice Λ. The set of vectors $\{\mathbf{b}_1, \cdots, \mathbf{b}_M\}$ is called a basis of Λ, and the matrix $\mathbf{B} = [\mathbf{b}_1, \cdots, \mathbf{b}_M]$, which has the basis vectors as its columns, is called the basis matrix (or generator matrix) of Λ.

The basis for representing a lattice is not unique. Usually a basis consisting of relatively short and nearly orthogonal vectors is desirable. The procedure of finding such a basis for a lattice is called *Lattice Basis Reduction*. A popular criterion for lattice-basis reduction is to find a basis such that $\|\mathbf{b}_1\| \cdot ... \cdot \|\mathbf{b}_M\|$ is minimized. Because the volume of the lattice[2] does not change with the change of basis, this problem is equivalent to minimizing the orthogonality defect which is defined as

$$\delta \triangleq \frac{(\|\mathbf{b}_1\|^2 \|\mathbf{b}_2\|^2 ... \|\mathbf{b}_M\|^2)}{\det \mathbf{B}^{\text{H}}\mathbf{B}}. \tag{4}$$

The problem of finding such a basis is NP-hard [17]. Several distinct sub-optimal reductions have been studied in the literature, including those associated to the names Minkowski, Korkin-Zolotarev, and more recently Lenstra-Lenstra and Lovasz (LLL) [18].

An ordered basis $(\mathbf{b}_1, \cdots, \mathbf{b}_M)$ is a *Minkowski-Reduced Basis* [19] if

- $\mathbf{b}_1$ is the shortest nonzero vector in the lattice Λ, and
- For each $k = 2, ..., M$, $\mathbf{b}_k$ is the shortest nonzero vector in Λ such that $(\mathbf{b}_1, \cdots, \mathbf{b}_k)$ may be extended to a basis of Λ.

Minkowski reduction can be seen as a greedy solution for the lattice-basis reduction problem. However, finding Minkowski reduced basis is equivalent to finding the shortest vector in the lattice and this problem by itself is NP-hard. Thus, there is no polynomial time algorithm for this reduction method.

In [20], a reduction algorithm (called *LLL algorithm*) is introduced which uses the Gram-Schmidt orthogonalization and has a polynomial complexity and guarantees a bounded orthogonality defect. For any ordered basis of Λ, say $(\mathbf{b}_1, \cdots, \mathbf{b}_M)$, one can compute an ordered set of Gram-Schmidt vectors, $\left(\hat{\mathbf{b}}_1, \cdots, \hat{\mathbf{b}}_M\right)$, which are mutually orthogonal, using the following recursion:

[2]Volume of the lattice generated by $\mathbf{B}$ is $\left(\det \mathbf{B}^{\text{H}}\mathbf{B}\right)^{\frac{1}{2}}$.

$$\begin{aligned} \hat{\mathbf{b}}_i &= \mathbf{b}_i - \textstyle\sum_{j=1}^{i-1} \mu_{ij} \hat{\mathbf{b}}_j, \text{ with} \\ \mu_{ij} &= \frac{< \mathbf{b}_i, \hat{\mathbf{b}}_j >}{< \mathbf{b}_j, \hat{\mathbf{b}}_j >}. \end{aligned} \tag{5}$$

where $< \cdot, \cdot >$ is the inner product. An ordered basis $(\mathbf{b}_1, \cdots, \mathbf{b}_M)$ is an *LLL Reduced Basis* [20] if,

- $\|\mu_{ij}\| \leq \frac{1}{2}$ for $1 \leq i < j \leq M$, and
- $p \cdot \|\hat{\mathbf{b}}_i\|^2 \leq \|\hat{\mathbf{b}}_{i+1} + \mu_{i+1,i}\hat{\mathbf{b}}_i\|^2$

where $\frac{1}{4} < p < 1$, and $\left(\hat{\mathbf{b}}_1, \cdots, \hat{\mathbf{b}}_M\right)$ is the Gram-Schmidt orthogonalization of the ordered basis and $\mathbf{b}_i = \sum_{j=1}^{i} \mu_{ij}\hat{\mathbf{b}}_j$ for $i = 1, ..., M$.

It is shown that LLL basis-reduction algorithm produces relatively short basis vectors with a polynomial-time computational complexity [20]. The LLL basis reduction has found extended applications in several contexts due to its polynomial-time complexity. In [21], LLL algorithm is generalized for Euclidean rings (including the ring of complex integers). In this paper, we will use the following important property of the complex LLL reduction (for $p = \frac{3}{4}$):

Theorem 1 (see [21]): Let Λ be an M-dimensional complex lattice and $\mathbf{B} = [\mathbf{b}_1 ... \mathbf{b}_M]$ be the LLL reduced basis of Λ. If δ is the orthogonality defect of $\mathbf{B}$, then,

$$\sqrt{\delta} \leq 2^{M(M-1)}. \tag{6}$$

In the rest of this paper, all matrix computations are in complex domain and also for the lattice-basis reduction, the complex LLL algorithm is used.

IV. Proposed Approach

Assume that the data for different users, u_i, is selected from the points of the integer lattice (or from the half-integer grid [22]). The data vector $\mathbf{u}$ is a point in the Cartesian product of these sub-constellations. As a result, the overall receive constellation consists of the points from $\mathbb{Z}^{2M}$, bounded within a $2M$-dimensional hypercube. At the transmitter side, when we use the channel inversion technique, the transmitted signal is a point inside a parallelotope whose edges are parallel to vectors, defined by the columns of $\mathbf{H}^{+}$. If the data is a point from the integer lattice $\mathbb{Z}^{2M}$, the transmitted signal is a point in the lattice

generated by $\mathbf{H}^+$. When the squared norm of at least one of the columns of $\mathbf{H}^+$ is too large, some of the constellation points require high energy for the transmission. We try to reduce the average transmitted energy, by replacing these points with some other points with smaller square norms. However, the lack of cooperation among the users imposes the restriction that the received signals should belong to the integer lattice $\mathbb{Z}^{2M}$ (to avoid the interference among the users). The core of the idea in this paper is based on using an appropriate supporting region for the transmitted signal set to minimize the average energy, without changing the underlying lattice. This is achieved through the lattice-basis reduction.

When we use the continuous approximation (which is appropriate for large constellations), the average energy of the transmitted signal is approximated by the second moment of the transmitted region [22]. When we assume equal rates for the users, e.g. R bits per user ($\frac{R}{2}$ bits per dimension), the signal points (at the receiver) are inside a hypercube with an edge of length a where

$$a = 2^{R/2}. \tag{7}$$

Therefore, the supporting region of the transmitted signal is the scaled version of the fundamental region of the lattice generated by $\mathbf{H}^+$ (corresponding to its basis) with the scaling factor a. Note that by changing the basis for this lattice, we can change the corresponding fundamental region (a parallelotope generated by the basis of the lattice and centered at the origin). The second moment of the resulting region is proportional to the sum of the squared norms of the basis vectors (see Appendix A). Therefore, we should try to find a basis reduction method which minimizes the sum of the squared norms of the basis vectors. Figure 1 shows the application of the lattice basis reduction in reducing the average energy by replacing the old basis with a new basis which has shorter vectors. In this figure, by changing the basis $\mathbf{a}_1, \mathbf{a}_2$ (columns of $\mathbf{H}^+$) to $\mathbf{b}_1, \mathbf{b}_2$ (the reduced basis), the fundamental region $\mathcal{F}$, generated by the original basis, is replaced by $\mathcal{F}'$, generated by the reduced basis.

Among the known reduction algorithms, the Minkowski reduction can be considered as an appropriate greedy algorithm for our problem. Indeed, the Minkowski algorithm is the successively optimum solution because in each step, it finds the shortest vector. However, the complexity of the Minkowski reduction is equal to the complexity of the shortest-lattice-

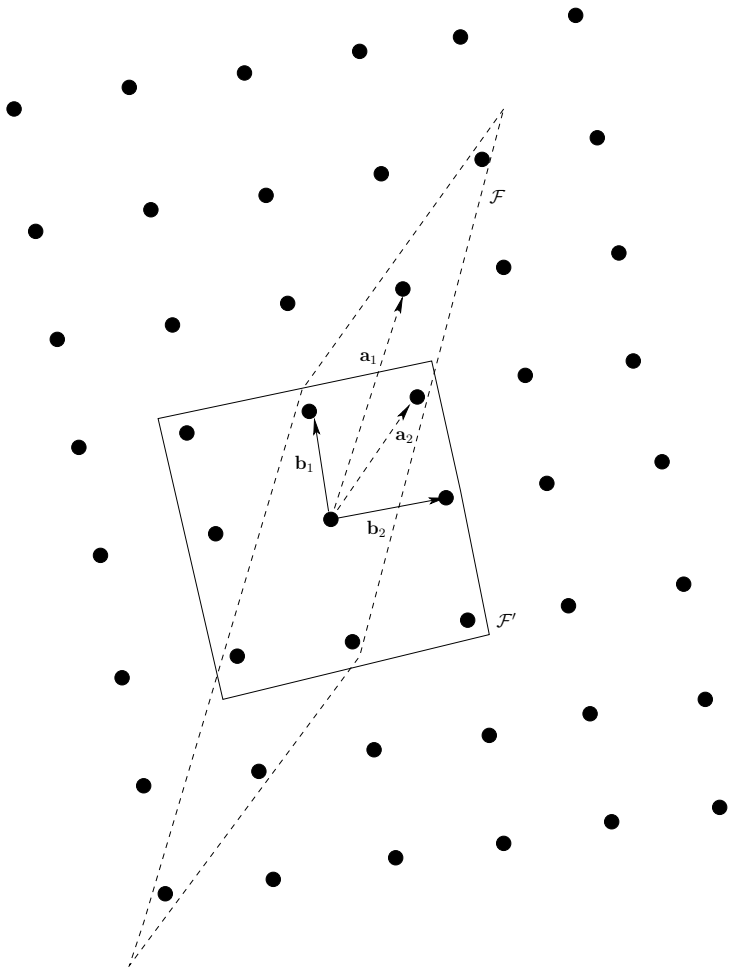

Fig. 1. Using lattice-basis reduction for reducing the average energy

vector problem which is known to be NP-hard [23]. Therefore, we use the LLL reduction algorithm which is a suboptimum solution with a polynomial complexity.

Assume that $\mathbf{B} = \mathbf{H}^{+}\mathbf{U}$ is the LLL-reduced basis for the lattice obtained by $\mathbf{H}^{+}$, where $\mathbf{U}$ is an $M \times M$ unimodular matrix (both $\mathbf{U}$ and $\mathbf{U}^{-1}$ have integer entries). We use $\mathbf{x} = \mathbf{B}\mathbf{u}' = \mathbf{H}^{+}\mathbf{U}\mathbf{u}'$ as the transmitted signal where

$$\mathbf{u}' = \mathbf{U}^{-1}\mathbf{u} \mod a \tag{8}$$

is the precoded data vector, $\mathbf{u}$ is the original data vector, and a is the length of the edges of the hypercube, defined by (7). At the receiver side, we use modulo operation to find the

original data:

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n} = \mathbf{H}\mathbf{H}^{+}\mathbf{U}(\mathbf{U}^{-1}\mathbf{u} \mod a) + \mathbf{n} = \mathbf{U}(\mathbf{U}^{-1}\mathbf{u} \mod a) + \mathbf{n} \tag{9}$$

$$= \mathbf{U}\mathbf{U}^{-1}\mathbf{u} \mod a + \mathbf{n} = \mathbf{u} \mod a + \mathbf{n}. \tag{10}$$

In obtaining (10) from (9), we use the fact that $\mathbf{U}$ and $\mathbf{U}^{-1}$ have integer entries.

In this method, at the beginning of each fading block, we reduce the lattice obtained by $\mathbf{H}^{+}$ and during this block the transmitted signal is computed using (8). Neglecting the preprocessing at the beginning of the block (for lattice reduction), the complexity of the precoding is in the order of a matrix multiplication and a modulo operation. Therefore, the complexity of the proposed precoding method is comparable to the complexity of the channel inversion method. However, as we will show by the simulation results, the performance of this method is significantly better, and indeed, is near the performance of the perturbation method, presented in [12].

In the perturbation technique [12], the idea of changing the support region of the constellation has been implemented using a different approach. In [12], $\mathbf{u}' = \mathbf{u} + a\mathbf{l}$ is used as the precoded data, where the integer vector $\mathbf{l}$ is chosen to minimize $\|\mathbf{H}^{+}(\mathbf{u} + a\mathbf{l})\|$. This problem is equivalent to the closest-lattice-point problem for the lattice generated by $a\mathbf{H}^{+}$ (i.e. finding the lattice point which is closer to $-\mathbf{H}^{+}\mathbf{u}$). Therefore, in the perturbation technique, the support region of the constellation is a scaled version of the Voronoi region [24] of the lattice. In the proposed method, we use a parallelotope (generated by the reduced basis of the lattice), instead of the Voronoi region. Although this approximation results in a larger second moment (i.e. higher energy consumption), it enables us to use a simple precoding technique, instead of solving the closest-lattice-point problem.

For the lattice constellations, using a parallelotope instead of the Voronoi region (presented in this paper) is equivalent with using the Babai approximation instead of the exact lattice decoding (previously introduced in [14]). In the case of using all lattice points inside a region, the only practical difference between our lattice-reduction-aided scheme and the scheme presented in [14] is that we reduce $\mathbf{H}^{+}$, while in [14], $\mathbf{H}^{\mathrm{H}}$ is reduced. This difference

has no significant effect on the performance. However, the new viewpoint helps us in extending the proposed method for the case of variable-rate transmission and obtaining some analytical results for the asymptotic performance.

The performance of the proposed lattice-reduction aided scheme can be improved by combining it with other schemes, such as regularization [25] or the V-BLAST precoding [26], or by sending a very small amount of side information. In the rest of this section, we present two of these modifications.

A. Regularized lattice-reduction-aided precoding

In [25], the authors have proposed a regularization scheme to reduce the transmitted power, by avoiding the near-singularity of $\mathbf{H}$. In this method, instead of using $\mathbf{H}^{+} = \mathbf{H}^{\mathtt{H}}\left(\mathbf{H}\mathbf{H}^{\mathtt{H}}\right)^{-1}$, the transmitted vector is constructed as

$$\mathbf{x} = \mathbf{H}^{\mathtt{H}}\left(\mathbf{H}\mathbf{H}^{\mathtt{H}} + \alpha\mathbf{I}\right)^{-1}\mathbf{u} \tag{11}$$

where α is a positive number. To combine the regularized scheme with our lattice-reduction-aided scheme, we consider $\mathbf{B}_r$ as the matrix corresponding to the reduced basis of the lattice generated by $\mathbf{H}^{\mathtt{H}}\left(\mathbf{H}\mathbf{H}^{\mathtt{H}} + \alpha\mathbf{I}\right)^{-1}$. When we use the regularization, the received signals of different users are not orthogonal anymore and the interference acts like extra noise. Parameter α should be optimized such that the ratio between the power of received signal and the power of the effective noise is minimized [25].

B. Modified lattice-reduction-aided precoding with small side information

In practical systems, we are interested in using a subset of points with odd coordinates from the integer lattice. In these cases, we can improve the performance of the proposed method by sending a very small amount of side information. When the data vector $\mathbf{u}$ consists of odd integers, using the lattice-basis reduction may result in points with some even coordinates (i.e. $\mathbf{U}^{-1}\mathbf{u}$ has some even elements), instead of points with all-odd coordinates in the new basis. For this case, in (8), the set of precoded data $\mathbf{u}'$ is not centered at the origin, hence the transmitted constellation (which includes all the valid points $\mathbf{B}\mathbf{u}'$) is not centered at the origin. Therefore, we can reduce the transmitted energy and improve the performance by

shifting the center of the constellation to the origin. This situation is depicted in figure 2 for a small constellation. For the sake of simplicity, this example is shown for a 2-dimensional real space, but all the discussion in the paper are for complex vectors and matrices (In this example, $\mathbf{U}^{-1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.). In comparison to the scheme presented in [14], which is the lattice-reduction-aided approximation of the precoding scheme, our approach helps us to utilize the fact that only a subset of lattice points (i.e. odd lattice points) are used in the transmission.

It can be shown that the translation vector is equal to $(\mathbf{U}^{-1}[1+i, 1+i, \cdots, 1+i]^{\mathtt{T}} + [1+i, 1+i, \cdots, 1+i]^{\mathtt{T}}) \mod 2$ where $i = \sqrt{-1}$. When we use this shifted version of the constellation, we must send the translation vector to the users (by sending 2 bits per user) at the beginning of the block. However, compared to the size of the block of data, the overhead of these two bits is negligible. Also, it should be noted that in all MIMO broadcast schemes, at the beginning of the fading block we need to send the information about power normalization.

The above idea of using a shift vector can be also used to improve the perturbation technique (if we only use the odd points of the lattice). After reducing the inverse of the channel matrix and obtaining the bits (corresponding to the shift vector) at the beginning of each fading block, the closest point to the signal computed in equation (8) can be found by using the sphere decoder. Then, the transmitted signal is obtained by

$$\mathbf{x} = \mathbf{B}\left(\mathbf{u}' + a\mathbf{l} + \mathbf{u}_{par}\right), \tag{12}$$

where $\mathbf{u}_{par}$ is the zero-one shift vector, which is computed for users at the beginning of the fading block, and the perturbation vector $\mathbf{l}$ is an even integer vector such that the vector $\mathbf{x}$ has the minimum energy. This method which can be considered as *modified perturbation method* outperforms the perturbation method in [12]. When we are not restricted to the odd lattice points, using (12) instead of $\mathbf{H}^{+}\left(\mathbf{u}' + a\mathbf{l}\right)$ does not change the performance of the perturbation method. It only reduces the complexity of the lattice decoder [27].

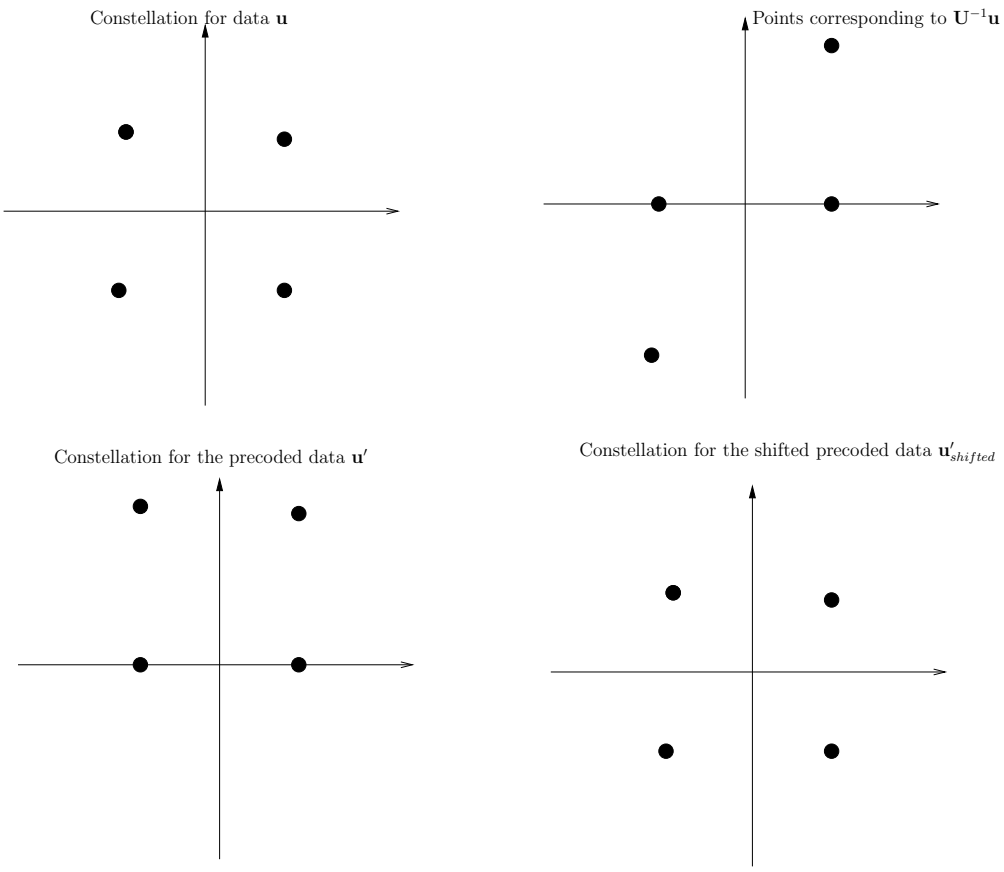

Fig. 2. In the case of using odd lattice points, when $\mathbf{U}^{-1}\mathbf{u}$ has some even entries, we can shift the precoded data to reduce the average energy. For the sake of simplicity, this example is shown for a 2-dimensional real space, but all the discussions in the paper are for complex vectors and matrices.

V. Unequal-Rate Transmission

In the previous section, we had considered the case that the transmission rates for different users are equal. In some applications, we are interested in assigning different rates to different users. Consider $R_1, ..., R_M$ as the transmission rates[3] for the users (we consider them as even integer numbers). Equation (8) should be modified as

$$\mathbf{u}' = \mathbf{U}^{-1}\mathbf{u} \mod \mathbf{a}, \tag{13}$$

[3] $R_1, ..., R_M$ are rates per complex dimension (rate per real dimension for different users are $\frac{R_1}{2}, ..., \frac{R_M}{2}$)

where the entries of $\mathbf{a} = [a_1, ..., a_M]^T$ are equal to[4]

$$a_i = 2^{R_i/2}. \tag{14}$$

Also, at the receiver side, instead of (9) and (10), we have

$$\mathbf{y} = \mathbf{Hx} + \mathbf{n} = \mathbf{HH}^{+}\mathbf{U}(\mathbf{U}^{-1}\mathbf{u} \mod \mathbf{a}) + \mathbf{n} = \mathbf{U}(\mathbf{U}^{-1}\mathbf{u} \mod \mathbf{a}) + \mathbf{n} \tag{15}$$

$$= \mathbf{U}\mathbf{U}^{-1}\mathbf{u} \mod \mathbf{a} + \mathbf{n} = \mathbf{u} \mod \mathbf{a} + \mathbf{n}. \tag{16}$$

If we are interested in sum-rate, instead of individual rates, we can improve the performance of the proposed method by assigning variable rates to different users. We assume that the sum-rate (rather than the individual rates) is fixed and we want to reduce the average transmitted energy. To simplify the analysis, we use the continuous approximation which has a good accuracy for high rates.

Considering continuous approximation, the sum-rate is proportional to the logarithm of the volume of the lattice with basis $\mathbf{B}$ and the average energy is proportional to the second moment of the corresponding parallelotope, which is proportional to $\sum_{i=1}^{M} \|\mathbf{b}_i\|^2 = \mathrm{tr}\mathbf{B}\mathbf{B}^{\mathtt{H}}$ (see Appendix A). The goal is to minimize the average energy while the sum-rate is fixed. We can use another lattice generated by $\mathbf{B}'$ with the same volume, where its basis vectors are scaled versions of the vectors of the basis $\mathbf{B}$, according to different rates for different users. Therefore, we can use $\mathbf{B}' = \mathbf{BD}$ instead of $\mathbf{B}$ (where $\mathbf{D}$ is a unit determinant $M \times M$ diagonal matrix which does not change the volume of the lattice). For a given reduced basis $\mathbf{B}$, the product of the squared norms of the new basis vectors is constant:

$$\begin{aligned} \|\mathbf{b}'_1\|^2\|\mathbf{b}'_2\|^2...\|\mathbf{b}'_M\|^2 &= (\|\mathbf{b}_1\|^2\|\mathbf{b}_2\|^2...\|\mathbf{b}_M\|^2)\det\mathbf{D} \\ &= \|\mathbf{b}_1\|^2\|\mathbf{b}_2\|^2...\|\mathbf{b}_M\|^2 = \mathrm{const}. \end{aligned} \tag{17}$$

The average energy corresponding to the new lattice basis should be minimized. When we use the modified basis $\mathbf{B}'$ instead of $\mathbf{B}$, the average energy is proportional to $\sum_{i=1}^{M} \|\mathbf{b}'_i\|^2 = \mathrm{tr}\mathbf{B}'\mathbf{B}'^{\mathtt{H}}$ (see Appendix A). According to the arithmetic-geometric mean inequality, $\sum_{i=1}^{M} \|\mathbf{b}'_i\|^2 = \mathrm{tr}\mathbf{B}'\mathbf{B}'^{\mathtt{H}}$ is minimized iff

$$\|\mathbf{b}'_1\| = \|\mathbf{b}'_2\| = ... = \|\mathbf{b}'_M\|. \tag{18}$$

[4]The data is assumed to be from $\mathbb{Z}[i]$. With this assumption, to have rate $\frac{R_i}{2}$ per real dimension, $a_i = 2^{\frac{R_i}{2}}$.

Therefore,

$$\min \mathrm{tr}\mathbf{B}'\mathbf{B}'^{\mathtt{H}} = M\left(\|\mathbf{b}'_1\|^2\|\mathbf{b}'_2\|^2...\|\mathbf{b}'_M\|^2\right)^{\frac{1}{M}} = M\left(\|\mathbf{b}_1\|^2\|\mathbf{b}_2\|^2...\|\mathbf{b}_M\|^2\right)^{\frac{1}{M}} \qquad (19)$$

Having the matrix $\mathbf{B}$, the columns of matrix $\mathbf{B}'$ can be found using the equation (18) and $\mathrm{tr}\mathbf{B}'\mathbf{B}'^{\mathtt{H}}$ can be obtained by (19). Now, for the selection of the reduced basis $\mathbf{B}$, we should find $\mathbf{B}$ such that $\|\mathbf{b}_1\|^2\|\mathbf{b}_2\|^2...\|\mathbf{b}_M\|^2$ is minimized. Because $\det \mathbf{B}^{\mathtt{H}}\mathbf{B} = \det\left(\mathbf{H}^{+}\right)^{\mathtt{H}}\mathbf{H}^{+}$ is given, the best basis reduction is the reduction which maximizes $\frac{\|\mathbf{b}_1\|^2\|\mathbf{b}_2\|^2.....\|\mathbf{b}_M\|^2}{|\det \mathbf{B}^{\mathtt{H}}\mathbf{B}|}$, or in other words, minimizes the orthogonality defect.

In practice, we use discrete values for the rate, and sometimes, we should assign the rate zero to some users (when their channel is very bad). In this case, for the rate assignment for other users, we use the lattice reduction on the corresponding sublattice. It should be noted that the average transmit power is fixed per channel realization and no long-run averaging is considered, and no long-run power allocation is used. Also, the design criteria is guided by continuous approximation, which is not appropriate for low rates and low SNR values. However, as it is shown in the simulation results, the scheme works well.

VI. Diversity and Outage Probability

In this section, we consider the asymptotic behavior ($\rho \longrightarrow \infty$) of the symbol error rate (SER) for the proposed method and the perturbation technique. We show that for both of these methods, the asymptotic slope of the SER curve is equal to the number of transmit antennas. By considering the outage probability of a fixed-rate MIMO broadcast system, we will show that for the SER curve in high SNR, the slope obtained by the proposed method has the largest achievable value. Also, we analyze the asymptotic behavior of the outage probability for the case of fixed sum-rate. We show that in this case, the slope of the corresponding curve is equal to the product of the number of transmit antennas and the number of single-antenna users.

A. Fixed-rate users

When we have the Channel-State Information (CSI) at the transmitter, without any assumption on the transmission rates, the outage probability is not meaningful. However,

when we consider given rates $R_1, ..., R_M$ for different users, we can define the outage probability P_{out} as the probability that the point $(R_1, ..., R_M)$ is outside the capacity region.

Theorem 2: For a MIMO broadcast system with N transmit antennas, M single-antenna receivers ($N \geq M$), and given rates $R_1, ..., R_M$,

$$\lim_{\rho \to \infty} \frac{-\log P_{out}}{\log \rho} \leq N. \tag{20}$$

Proof: Define P_{out1} as the probability that the capacity of the point-to-point system corresponding to the first user (consisting of N transmit antennas and one receive antenna with independent channel coefficients and CSI at the transmitter) is less than R_1:

$$P_{out1} = \Pr\{\log\left(1 + \rho\|\mathbf{h}_1\|^2\right) \leq R_1\} \tag{21}$$

where $\mathbf{h}_1$ is the vector defined by the first row of $\mathbf{H}$. Note that the entries of $\mathbf{h}_1$ have iid complex Gaussian distribution with unit variance. Thus, its square norm has a chi square distribution. We have,

$$\Pr\left\{\log\left(2\rho\|\mathbf{h}_1\|^2\right) \leq R_1\right\} \tag{22}$$

$$= \Pr\left\{\|\mathbf{h}_1\|^2 \leq \frac{2^{R_1}}{2\rho}\right\} \tag{23}$$

$$= \int_0^{\frac{2^{R_1}}{2\rho}} f_{\|\mathbf{h}_1\|^2}(x)\, dx \tag{24}$$

$$= \int_0^{\frac{2^{R_1}}{2\rho}} \frac{1}{(N-1)!} x^{N-1} e^{-x}\, dx \tag{25}$$

We are interested in the large values of ρ. For $\rho > 2^{R_1 - 1}$,

$$\int_0^{\frac{2^{R_1}}{2\rho}} \frac{1}{(N-1)!} x^{N-1} e^{-x}\, dx \geq \int_0^{\frac{2^{R_1}}{2\rho}} \frac{1}{(N-1)!} x^{N-1} e^{-1}\, dx \tag{26}$$

$$= \frac{e^{-1}}{(N-1)!} \int_0^{\frac{2^{R_1}}{2\rho}} x^{N-1}\, dx \tag{27}$$

$$= \frac{2^{NR_1} c}{\rho^N} \tag{28}$$

where $c = \frac{e^{-1}}{2^N N!}$ is a constant number. Now,

$$\log\left(1+\rho\|\mathbf{h}_1\|^2\right) \leq \log\left(2\rho\|\mathbf{h}_1\|^2\right) \quad \text{for} \;\; \rho > \frac{1}{\|\mathbf{h}_1\|^2} \tag{29}$$

$$\Longrightarrow \lim_{\rho\to\infty} \frac{-\log \Pr\{\log\left(1+\rho\|\mathbf{h}_1\|^2\right) \leq R_1\}}{\log\rho} \tag{30}$$

$$\leq \lim_{\rho\to\infty} \frac{-\log \Pr\{\log\left(2\rho\|\mathbf{h}_1\|^2\right) \leq R_1\}}{\log\rho} \tag{31}$$

$$\leq \lim_{\rho\to\infty} \frac{-\log \frac{2^{NR_1}c}{\rho^N}}{\log\rho} = N \tag{32}$$

$$\Longrightarrow \lim_{\rho\to\infty} \frac{-\log P_{out1}}{\log\rho} \leq N. \tag{33}$$

According to the definition of P_{out1}, $P_{out} \geq P_{out1}$. Therefore,

$$\lim_{\rho\to\infty} \frac{-\log P_{out}}{\log\rho} \leq \lim_{\rho\to\infty} \frac{-\log P_{out1}}{\log\rho} \leq N. \tag{34}$$

■

We can define the diversity gain of a MIMO broadcast constellation or its *precoding diversity* as $\lim_{\rho\to\infty} \frac{-\log P_e}{\log\rho}$ where P_e is the probability of error. Similar to [28, lemma 5], we can bound the precoding diversity by $\lim_{\rho\to\infty} \frac{-\log P_{out}}{\log\rho}$. Thus, based on theorem 2, the maximum achievable diversity is N.

We show that the proposed method (based on lattice-basis reduction) achieves the maximum precoding diversity. To prove this, in lemma 1 and lemma 2, we relate the length of the largest vector of the reduced basis $\mathbf{B}$ to $d_{\mathbf{H}^{\mathrm{H}}}$ (the minimum distance of the lattice generated by $\mathbf{H}^{\mathrm{H}}$). In lemma 3, we bound the probability that $d_{\mathbf{H}^{\mathrm{H}}}$ is too small. Finally, in theorem 3, we prove the main result by relating the minimum distance of the receive constellation to the length of the largest vector of the reduced basis $\mathbf{B}$, and combining the bounds on the probability that $d_{\mathbf{H}^{\mathrm{H}}}$ is too small, and the probability that the noise vector is too large.

Lemma 1: Consider $\mathbf{B} = [\mathbf{b}_1 ... \mathbf{b}_M]$ as an $N \times M$ matrix, with the orthogonality defect δ, and $\mathbf{B}^{-\mathtt{H}} = [\mathbf{a}_1 ... \mathbf{a}_M]$ as the inverse of its Hermitian (or its pseudo-inverse if $M < N$). Then,

$$\max\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\} \leq \frac{\sqrt{\delta}}{\min\{\|\mathbf{a}_1\|, ..., \|\mathbf{a}_M\|\}} \tag{35}$$

and

$$\max\{\|\mathbf{a}_1\|, ..., \|\mathbf{a}_M\|\} \leq \frac{\sqrt{\delta}}{\min\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\}}. \tag{36}$$

Proof: Consider $\mathbf{b}_i$ as an arbitrary column of $\mathbf{B}$. The vector $\mathbf{b}_i$ can be written as $\mathbf{b}'_i + \sum_{i \neq j} c_{i,j}\mathbf{b}_j$, where $\mathbf{b}'_i$ is orthogonal to $\mathbf{b}_j$ for $i \neq j$. Now, $[\mathbf{b}_1 ... \mathbf{b}_{i-1}\mathbf{b}'_i\mathbf{b}_{i+1} ... \mathbf{b}_M]$ can be written as $\mathbf{BP}$ where $\mathbf{P}$ is a unit-determinant $M \times M$ matrix (a column operation matrix):

$$\|\mathbf{b}_1\|^2 ... \|\mathbf{b}_{i-1}\|^2 . \|\mathbf{b}_i\|^2 . \|\mathbf{b}_{i+1}\|^2 ... \|\mathbf{b}_M\|^2 \tag{37}$$

$$= \delta \det \mathbf{B}^{\mathtt{H}}\mathbf{B} = \delta \det \mathbf{P}^{\mathtt{H}}\mathbf{B}^{\mathtt{H}}\mathbf{B}\mathbf{P} \tag{38}$$

$$= \delta \det \left([\mathbf{b}_1 ... \mathbf{b}_{i-1}\mathbf{b}'_i\mathbf{b}_{i+1} ... \mathbf{b}_M]^{\mathtt{H}} [\mathbf{b}_1 ... \mathbf{b}_{i-1}\mathbf{b}'_i\mathbf{b}_{i+1} ... \mathbf{b}_M] \right). \tag{39}$$

According to the Hadamard theorem:

$$\det \left([\mathbf{b}_1 ... \mathbf{b}_{i-1}\mathbf{b}'_i\mathbf{b}_{i+1} ... \mathbf{b}_M]^{\mathtt{H}} [\mathbf{b}_1 ... \mathbf{b}_{i-1}\mathbf{b}'_i\mathbf{b}_{i+1} ... \mathbf{b}_M] \right) \leq \tag{40}$$

$$\|\mathbf{b}_1\|^2 ... \|\mathbf{b}_{i-1}\|^2 . \|\mathbf{b}'_i\|^2 . \|\mathbf{b}_{i+1}\|^2 ... \|\mathbf{b}_M\|^2. \tag{41}$$

Therefore,

$$\|\mathbf{b}_1\|^2 ... \|\mathbf{b}_{i-1}\|^2 . \|\mathbf{b}_i\|^2 . \|\mathbf{b}_{i+1}\|^2 ... \|\mathbf{b}_M\|^2 \leq \delta \|\mathbf{b}_1\|^2 ... \|\mathbf{b}_{i-1}\|^2 . \|\mathbf{b}'_i\|^2 . \|\mathbf{b}_{i+1}\|^2 ... \|\mathbf{b}_M\|^2 \tag{42}$$

$$\Longrightarrow \|\mathbf{b}_i\| \leq \sqrt{\delta} \|\mathbf{b}'_i\|. \tag{43}$$

Also, $\mathbf{B}^{+}\mathbf{B} = \mathbf{I}$ results in $<\mathbf{a}_i, \mathbf{b}_i> = 1$ and $<\mathbf{a}_i, \mathbf{b}_j> = 0$ for $i \neq j$. Therefore,

$$1 \ = \ <\mathbf{a}_i, \mathbf{b}_i> \ = \ <\mathbf{a}_i, (\mathbf{b}'_i + \sum_{i \neq j} c_{i,j}\mathbf{b}_j)> \ = \ <\mathbf{a}_i, \mathbf{b}'_i> \tag{44}$$

Now, $\mathbf{a}_i$ and $\mathbf{b}'_i$, both are orthogonal to the $(M-1)$-dimensional subspace generated by the vectors $\mathbf{b}_j$ $(j \neq i)$. Thus,

$$1 = \ <\mathbf{a}_i, \mathbf{b}'_i> \ = \ \|\mathbf{a}_i\| . \|\mathbf{b}'_i\| \geq \|\mathbf{a}_i\| . \frac{\|\mathbf{b}_i\|}{\sqrt{\delta}} \tag{45}$$

$$\Longrightarrow 1 \geq \|\mathbf{b}_i\|.\frac{\|\mathbf{a}_i\|}{\sqrt{\delta}} \tag{46}$$

$$\Longrightarrow \|\mathbf{b}_i\| \leq \frac{\sqrt{\delta}}{\|\mathbf{a}_i\|} \tag{47}$$

The above relation is valid for every i, $1 \leq i \leq M$. Without loss of generality, we can assume that $\max\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\} = \|\mathbf{b}_k\|$:

$$\max\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\} = \|\mathbf{b}_k\| \leq \frac{\sqrt{\delta}}{\|\mathbf{a}_k\|} \tag{48}$$

$$\leq \frac{\sqrt{\delta}}{\min\{\|\mathbf{a}_1\|, ..., \|\mathbf{a}_M\|\}}. \tag{49}$$

Similarly, by using (47), we can also obtain the following inequality:

$$\max\{\|\mathbf{a}_1\|, ..., \|\mathbf{a}_M\|\} \leq \frac{\sqrt{\delta}}{\min\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\}}. \tag{50}$$

■

Lemma 2: Consider $\mathbf{B} = [\mathbf{b}_1 ... \mathbf{b}_M]$ as an LLL-reduced basis for the lattice generated by $\mathbf{H}^+$ and $d_{\mathbf{H}^{\mathtt{H}}}$ as the minimum distance of the lattice generated by $\mathbf{H}^{\mathtt{H}}$. Then, there is a constant α_M (independent of $\mathbf{H}$) such that

$$\max\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\} \leq \frac{\alpha_M}{d_{\mathbf{H}^{\mathtt{H}}}}. \tag{51}$$

Proof: According to the theorem 1,

$$\sqrt{\delta} \leq 2^{M(M-1)}. \tag{52}$$

Consider $\mathbf{B}^{-\mathtt{H}} = [\mathbf{a}_1, ..., \mathbf{a}_M]$. By using lemma 1 and (52),

$$\max\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\} \leq \frac{\sqrt{\delta}}{\min\{\|\mathbf{a}_1\|, ..., \|\mathbf{a}_M\|\}} \leq \frac{2^{M(M-1)}}{\min\{\|\mathbf{a}_1\|, ..., \|\mathbf{a}_M\|\}} \tag{53}$$

The basis $\mathbf{B}$ can be written as $\mathbf{B} = \mathbf{H}^+\mathbf{U}$ for some unimodular matrix $\mathbf{U}$:

$$\mathbf{B}^{-\mathtt{H}} = ((\mathbf{H}^+\mathbf{U})^{\mathtt{H}})^+ = (\mathbf{U}^{\mathtt{H}}\mathbf{H}^{-\mathtt{H}})^+ = \mathbf{H}^{\mathtt{H}}\mathbf{U}^{-\mathtt{H}}. \tag{54}$$

Noting that $\mathbf{U}^{-\mathtt{H}}$ is unimodular, $\mathbf{B}^{-\mathtt{H}} = [\mathbf{a}_1, ..., \mathbf{a}_M]$ is another basis for the lattice generated by $\mathbf{H}^{\mathtt{H}}$. Therefore, the vectors $\mathbf{a}_1, ..., \mathbf{a}_M$ are vectors from the lattice generated by $\mathbf{H}^{\mathtt{H}}$, and therefore, the length of each of them is at least $d_{\mathbf{H}^{\mathtt{H}}}$:

$$\|\mathbf{a}_i\| \geq d_{\mathbf{H}^{\mathtt{H}}} \quad \text{for} \;\; 1 \leq i \leq M \tag{55}$$

$$\Longrightarrow \min\{\|\mathbf{a}_1\|, ..., \|\mathbf{a}_M\|\} \geq d_{\mathbf{H}^{\mathrm{H}}} \tag{56}$$

$$(53) \text{ and } (56) \Longrightarrow \max\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\} \leq \frac{2^{M(M-1)}}{d_{\mathbf{H}^{\mathrm{H}}}}. \tag{57}$$

■

Lemma 3: Assume that the entries of the $N \times M$ matrix $\mathbf{H}$ has independent complex Gaussian distribution with zero mean and unit variance and consider $d_{\mathbf{H}}$ as the minimum distance of the lattice generated by $\mathbf{H}$. Then, there is a constant $\beta_{N,M}$ such that

$$\Pr\{d_{\mathbf{H}} \leq \varepsilon\} \leq \begin{cases} \beta_{N,M}\varepsilon^{2N} & \text{for } M < N \\ \beta_{N,N}\varepsilon^{2N}.\max\left\{-(\ln\varepsilon)^{N+1}, 1\right\} & \text{for } M = N \end{cases}. \tag{58}$$

Proof: See Appendix B.

Theorem 3: For a MIMO broadcast system with N transmit antennas and M single-antenna receivers ($N \geq M$) and fixed rates $R_1, ..., R_M$, using the lattice-basis-reduction method,

$$\lim_{\rho\to\infty} \frac{-\log P_e}{\log \rho} = N. \tag{59}$$

Proof: Consider $\mathbf{B} = [\mathbf{b}_1 ... \mathbf{b}_M]$ as the LLL-reduced basis for the lattice generated by $\mathbf{H}^+$. Each transmitted vector $\mathbf{s}$ is inside the parallelotope, generated by $r_1\mathbf{b}_1, ..., r_M\mathbf{b}_M$ (where $r_1, ..., r_M$ are constant values determined by the rates of the users). Thus, every transmitted vector $\mathbf{s}$ can be written as

$$\mathbf{s} = t_1\mathbf{b}_1 + ... + t_M\mathbf{b}_M, \quad \frac{-r_i}{2} \leq t_i \leq \frac{r_i}{2}. \tag{60}$$

For each of the transmitted vectors, the energy is

$$P = \|\mathbf{s}\|^2 = \|t_1\mathbf{b}_1 + ... + t_M\mathbf{b}_M\|^2 \tag{61}$$

$$\Longrightarrow P \leq (\|t_1\mathbf{b}_1\| + ... + \|t_M\mathbf{b}_M\|)^2 \tag{62}$$

$$\Longrightarrow P \leq \left(\frac{r_1}{2}\|\mathbf{b}_1\| + ... + \frac{r_M}{2}\|\mathbf{b}_M\|\right)^2. \tag{63}$$

Thus, the average transmitted energy is

$$P_{av} = \mathrm{E}(P) \leq M^2\left(\max\left\{\frac{r_1}{2}\|\mathbf{b}_1\|, ..., \frac{r_M}{2}\|\mathbf{b}_M\|\right\}\right)^2 \leq c_1.(\max\{\|\mathbf{b}_1\|^2, ..., \|\mathbf{b}_M\|^2\}) \tag{64}$$

where $c_1 = \frac{M^2}{4} \max\{r_1^2, ..., r_M^2\}$. The received signals (without the effect of noise) are points from the $\mathbb{Z}^{2M}$ lattice. If we consider the normalized system (by scaling the signals such that the average transmitted energy becomes equal to one),

$$d^2 = \frac{1}{P_{av}} \geq \frac{1}{c_1.(\max\{\|\mathbf{b}_1\|^2, ..., \|\mathbf{b}_M\|^2\})} \tag{65}$$

is the squared distance between the received signal points.

For the normalized system, $\frac{1}{\rho}$ is the energy of the noise at each receiver and $\frac{1}{2\rho}$ is the energy of the noise per each real dimension. Using (65), for any positive number γ,

$$\begin{aligned} &\Pr\left\{d^2 \leq \frac{\gamma}{\rho}\right\} \\ &\leq \Pr\left\{\frac{1}{c_1 \max\{\|\mathbf{b}_1\|^2, ..., \|\mathbf{b}_M\|^2\}} \leq \frac{\gamma}{\rho}\right\} \end{aligned} \tag{66}$$

Using lemma 2,

$$\max\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\} \leq \frac{\alpha_M}{d_{\mathbf{H}^{\mathtt{H}}}} \tag{67}$$

$$(66), (67) \Longrightarrow \Pr\left\{d^2 \leq \frac{\gamma}{\rho}\right\} \leq \Pr\left\{\frac{d^2_{\mathbf{H}^{\mathtt{H}}}}{c_1 \alpha_M^2} \leq \frac{\gamma}{\rho}\right\} = \Pr\left\{d^2_{\mathbf{H}^{\mathtt{H}}} \leq \frac{\gamma c_1 \alpha_M^2}{\rho}\right\} \tag{68}$$

The $N \times M$ matrix $\mathbf{H}^{\mathtt{H}}$ has independent complex Gaussian distribution with zero mean and unit variance. Therefore, by using lemma 3, we can bound the probability that $d_{\mathbf{H}^{\mathtt{H}}}$ is too small.

Case 1, $M = N$:

$$\Pr\left\{d^2 \leq \frac{\gamma}{\rho}\right\} \leq \Pr\left\{d^2_{\mathbf{H}^{\mathtt{H}}} \leq \frac{\gamma c_1 \alpha_N^2}{\rho}\right\} \tag{69}$$

$$\leq \beta_{N,N} \left(\frac{\gamma c_1 \alpha_N^2}{\rho}\right)^N \max\left\{\left(-\frac{1}{2} \ln \frac{\gamma c_1 \alpha_N^2}{\rho}\right)^{N+1}, 1\right\} \tag{70}$$

$$\leq \beta_{N,N} \left(\frac{\gamma c_1 \alpha_N^2}{\rho} \right)^N \max \left\{ (\ln \rho)^{N+1}, 1 \right\} \quad \text{for } \gamma > 1 \text{ and } \rho > \frac{1}{c_1 \alpha_N^2} \tag{71}$$

$$\leq \frac{c_2 \gamma^N}{\rho^N} (\ln \rho)^{N+1} \quad \text{for } \gamma > 1 \text{ and } \rho > \max \left\{ \frac{1}{c_1 \alpha_N^2}, e \right\} \tag{72}$$

where c_2 is a constant number and e is the Euler number.

If the magnitude of the noise component in each real dimension is less than $\frac{1}{2}d$, the transmitted data will be decoded correctly. Thus, we can bound the probability of error by the probability that $|w_i|^2$ is greater than $\frac{1}{4}d^2$ for at least one i, $1 \leq i \leq 2N$. Therefore, using the union bound,

$$P_e \leq 2N \left(\Pr \left\{ |w_1|^2 \geq \frac{1}{4} d^2 \right\} \right) \tag{73}$$

$$\begin{aligned} &= 2N \left(\Pr \left\{ d^2 \leq \frac{4}{\rho} \right\} . \Pr \left\{ |w_1|^2 \geq \frac{1}{4} d^2 \middle| d^2 \leq \frac{4}{\rho} \right\} \right. \\ &+ \Pr \left\{ \frac{4}{\rho} \leq d^2 \leq \frac{8}{\rho} \right\} . \Pr \left\{ |w_1|^2 \geq \frac{1}{4} d^2 \middle| \frac{4}{\rho} \leq d^2 \leq \frac{8}{\rho} \right\} \\ &\left. + \Pr \left\{ \frac{8}{\rho} \leq d^2 \leq \frac{16}{\rho} \right\} . \Pr \left\{ |w_1|^2 \geq \frac{1}{4} d^2 \middle| \frac{8}{\rho} \leq d^2 \leq \frac{16}{\rho} \right\} + ... \right) \end{aligned} \tag{74}$$

$$\begin{aligned} &\leq 2N \left(\Pr \left\{ d^2 \leq \frac{4}{\rho} \right\} + \Pr \left\{ \frac{4}{\rho} \leq d^2 \leq \frac{8}{\rho} \right\} . \Pr \left\{ |w_1|^2 \geq \frac{1}{4} . \frac{4}{\rho} \right\} \right. \\ &\left. + \Pr \left\{ \frac{8}{\rho} \leq d^2 \leq \frac{16}{\rho} \right\} . \Pr \left\{ |w_1|^2 \geq \frac{1}{4} . \frac{8}{\rho} \right\} + ... \right) \end{aligned} \tag{75}$$

$$\begin{aligned} &\leq 2N \left(\Pr \left\{ d^2 \leq \frac{4}{\rho} \right\} + \Pr \left\{ d^2 \leq \frac{8}{\rho} \right\} . \Pr \left\{ |w_1|^2 \geq \frac{1}{\rho} \right\} \right. \\ &\left. + \Pr \left\{ d^2 \leq \frac{16}{\rho} \right\} . \Pr \left\{ |w_1|^2 \geq \frac{2}{\rho} \right\} + ... \right) \end{aligned} \tag{76}$$

For the product terms in (76), we can bound the first part by (72). To bound the second part, we note that w_1 has real Gaussian distribution with variance $\frac{1}{2\rho}$. Therefore,

$$\Pr \left\{ |w_1|^2 \geq \frac{\theta}{\rho} \right\} = Q(\sqrt{2\theta}) \leq e^{-\theta} \tag{77}$$

Now, for $\rho > \max\left\{\frac{1}{c_1\alpha_N^2}, e\right\}$,

$$(72),\ (76) \text{ and } (77) \Longrightarrow P_e \leq 2N\left(\Pr\left\{|w_1|^2 \geq \frac{1}{4}d^2\right\}\right) \tag{78}$$

$$\leq 2N\left(\frac{4^N c_2}{\rho^N}\left(\ln\rho\right)^{N+1} + \sum_{i=0}^{\infty}\frac{2^{N(i+3)}c_2}{\rho^N}\left(\ln\rho\right)^{N+1}e^{-2^i}\right) \tag{79}$$

$$\leq \frac{(\ln\rho)^{N+1}}{\rho^N}.c_2.2N\left(4^N + \sum_{i=0}^{\infty}2^{N(i+3)}e^{-2^i}\right) \tag{80}$$

$$\leq \frac{c_3(\ln\rho)^{N+1}}{\rho^N} \tag{81}$$

where c_3 is a constant number which only depends on N. Thus,

$$\lim_{\rho\to\infty}\frac{-\log P_e}{\log\rho} \geq \lim_{\rho\to\infty}\frac{N\log\rho - \log(\ln\rho)^{N+1} - \log c_3}{\log\rho} = N. \tag{82}$$

According to Theorem 2, this limit can not be greater than N. Therefore,

$$\lim_{\rho\to\infty}\frac{-\log P_e}{\log\rho} = N. \tag{83}$$

Case 2, $M < N$:

For the $N\times M$ matrix $\mathbf{H}^{\mathrm{H}}$, we use the first inequality in lemma 3 to bound the probability that $d_{\mathbf{H}^{\mathrm{H}}}$ is too small:

$$\Pr\left\{d^2 \leq \frac{\gamma}{\rho}\right\} \leq \Pr\left\{d_{\mathbf{H}^{\mathrm{H}}}^2 \leq \frac{\gamma c_1\alpha_M^2}{\rho}\right\} \tag{84}$$

$$\leq \beta_{N,M}\left(\frac{\gamma c_1\alpha_M^2}{\rho}\right)^N \tag{85}$$

$$\leq \beta_{N,M}\left(\frac{\gamma c_1\alpha_M^2}{\rho}\right)^N \quad \text{for } \gamma > 1 \text{ and } \rho > \frac{1}{c_1\alpha_M^2} \tag{86}$$

$$\leq \frac{c_2\gamma^N}{\rho^N} \quad \text{for } \gamma > 1 \text{ and } \rho > \frac{1}{c_1\alpha_M^2} \tag{87}$$

.

The rest of proof is similar to the case 1.

■

Corollary 1: Perturbation technique achieves the maximum precoding diversity in fixed-rate MIMO broadcast systems.

Proof: In the perturbation technique, for the transmission of each data vector $\mathbf{u}$, among the set $\left\{\mathbf{H}^{+}(\mathbf{u}+a\mathbf{l})\|\mathbf{l}\in\mathbb{Z}^{2M}\right\}$, the nearest point to the origin is chosen. The transmitted vector in the lattice-reduction-based method belongs to that set. Therefore, the energy of the transmitted signal in the lattice-reduction-based method can not be less than the transmitted energy in the perturbation technique. Thus, the average transmitted energy for the perturbation method is at most equal to the average transmitted energy of the lattice-reduction-based method. The rest of the proof is the same as the proof of theorem 3. ■

B. Fixed sum-rate

When the sum-rate R_{sum} is given, similar to the previous part, we can define the outage probability as the probability that the sum-capacity of the broadcast system is less than R_{sum}.

Theorem 4: For a MIMO broadcast system with N transmit antennas, M single-antenna receivers, and a given sum-rate R_{sum},

$$\lim_{\rho\to\infty}\frac{-\log P_{out}}{\log\rho}\leq NM. \tag{88}$$

Proof:

For any channel matrix $\mathbf{H}$, we have [9]

$$C_{sum}=\sup_{\mathbf{D}}\log\left|\mathbf{I}_M+\rho\mathbf{H}^{\mathrm{H}}\mathbf{D}\mathbf{H}\right| \tag{89}$$

where $\mathbf{D}$ is a diagonal matrix with non-negative elements and unit trace. Also, [29]

$$\left|2\rho\mathbf{H}^{\mathrm{H}}\mathbf{D}\mathbf{H}\right|\leq\frac{\left(2\rho\mathrm{tr}\mathbf{H}^{\mathrm{H}}\mathbf{D}\mathbf{H}\right)^{M}}{M^{M}}=\frac{\left(2\rho\mathrm{tr}\mathbf{H}^{\mathrm{H}}\mathbf{H}\right)^{M}}{M^{M}}. \tag{90}$$

The entries of $\mathbf{H}$ have iid complex Gaussian distribution with unit variance. Thus $\mathrm{tr}\rho\mathbf{H}^{\mathrm{H}}\mathbf{H}$ is equal to the square norm of an NM-dimensional complex Gaussian vector and

has a chi square distribution with $2NM$ degrees of freedom. Thus, we have (similar to the equations 22-28, in the proof of theorem 2),

$$\Pr\left\{\log\frac{(2\rho\mathrm{tr}\mathbf{H}^{\mathtt{H}}\mathbf{H})^{M}}{M^{M}}\leq R_{sum}\right\} \tag{91}$$

$$=\Pr\left\{\mathrm{tr}\mathbf{H}^{\mathtt{H}}\mathbf{H}\leq\frac{2^{\frac{R_{sum}}{M}}M}{2\rho}\right\} \tag{92}$$

$$\geq\frac{2^{NR_{sum}}M^{NM}c}{\rho^{NM}}\qquad(\text{for }\rho>\frac{2^{\frac{R_{sum}}{M}}M}{2}) \tag{93}$$

where c is a constant number. Now,

$$\lim_{\rho\to\infty}\frac{-\log P_{out}}{\log\rho}= \tag{94}$$

$$\lim_{\rho\to\infty}\frac{-\log\Pr\left\{\sup_{\mathbf{D}}\log|\mathbf{I}_{M}+\rho\mathbf{H}^{\mathtt{H}}\mathbf{D}\mathbf{H}|\leq R_{sum}\right\}}{\log\rho} \tag{95}$$

$$\leq\lim_{\rho\to\infty}\frac{-\log\Pr\{\sup_{\mathbf{D}}\log|2\rho\mathbf{H}^{\mathtt{H}}\mathbf{D}\mathbf{H}|\leq R_{sum}\}}{\log\rho}. \tag{96}$$

By using (90), (93), and (96):

$$\lim_{\rho\to\infty}\frac{-\log P_{out}}{\log\rho}\leq\lim_{\rho\to\infty}\frac{-\log\frac{2^{NR_{sum}}M^{NM}c}{\rho^{NM}}}{\log\rho}=NM. \tag{97}$$

■

The slope NM for the SER curve can be easily achieved by sending to only the best user. Similar to the proof of theorem 3, the slope of the symbol-error rate curve is asymptoticly determined by the slope of the probability that $|h_{max}|$ is smaller than a constant number, where h_{max} is the entry of $\mathbf{H}$ with maximum norm. Due to the iid complex Gaussian distribution of the entries of $\mathbf{H}$, this probability decays with the same rate as ρ^{-NM}, for large ρ. However, although sending to only the best user achieves the optimum slope for the SER curve, it is not an efficient transmission technique because it reduces the capacity to the order of $\log\rho$ (instead of $M\log\rho$).

VII. Simulation Results

Figure 3 presents the simulation results for the performance of the proposed schemes, the perturbation scheme [12], and the naive channel inversion approach. The number of the transmit antennas is $N = 4$ and there are $M = 4$ single-antenna users in the system. The overall transmission rate is 8 bits per channel use, where 2 bits are assigned to each user, i.e. a QPSK constellation is assigned to each user (i.e. the rate is 2 bits per complex dimension or 1 bit per real dimension).

By considering the slope of the curves in figure 3, we see that by using the proposed reduction-based schemes, we can achieve the maximum precoding diversity, with a low complexity. Also, as compared to the perturbation scheme, we have a negligible loss in the performance (about 0.2 dB). Moreover, compared to the approximated perturbation method [14], we have about 1.5 dB improvement by sending the bits, corresponding to the shift vector, at the beginning of the transmission. Without sending the shift vector, the performance of the proposed method is the same as that of the approximated perturbation method [14]. The modified perturbation method (with sending two shift bits for each user) has around 0.3 dB improvement compared to the perturbation method.

Figure 4 compares the regularized proposed scheme with V-BLAST modifications of Zero-Forcing and Babai approximation for the same setting. As shown in the simulation results (and also in the simulation results in [12] and [14]), the modulo-MMSE-VBLAST scheme does not achieve a precoding diversity better than zero forcing (though it has a good performance in the low SNR region). However, combining the lattice-reduction-aided (LRA) scheme with MMSE-VBLAST precoding or other schemes such as regularization improves its performance by a finite coding gain (without changing the slope of the curve of symbol-error-rate). Combining both the regularization and the shift vector can result in better performance compared to other alternatives.

Figure 5 compares the performances of the fixed-rate and the variable-rate transmission using lattice-basis reduction for $N = 2$ transmit antennas and $M = 2$ users. In both cases, the sum-rate is 8 bits per channel use (in the case of fixed individual rates, a 16QAM constellation is assigned to each user). We see that by eliminating the equal-rate constraint,

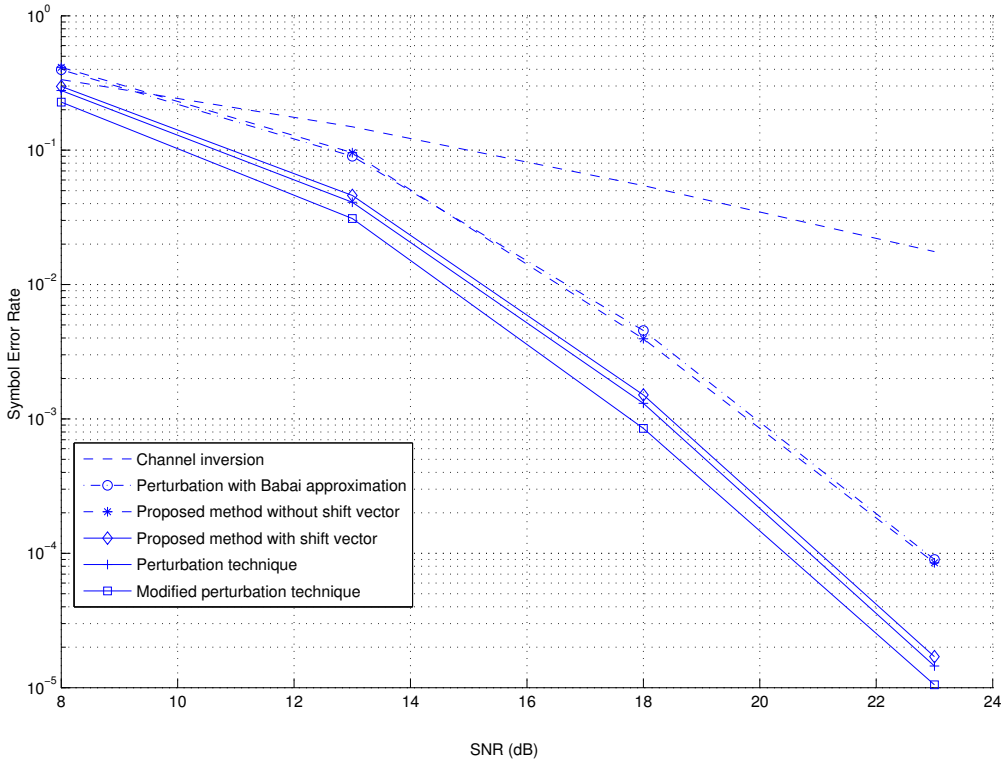

Fig. 3. Symbol Error Rate of the proposed schemes, the perturbation scheme [12], and the naive channel inversion approach for $N = 4$ transmit antennas and $M = 4$ single-antenna receivers with the rate $R = 2$ bits per channel use per user.

we can considerably improve the performance (especially, for high rates). In fact, the diversity gains for the equal-rate and the unequal-rate methods are, respectively, M and NM. It should be noted that the average transmit power and also the sum-rate are fixed for different channel realizations and no long-run power allocation is used. The gain of the variable-rate originates from allocating higher rates to users who have better channels.

VIII. Conclusion

A new viewpoint for designing and analysing lattice-reduction-aided communications over MIMO broadcast channels is introduced. Lattice basis reduction helps us to reduce the average transmitted energy by modifying the region which includes the constellation points. It is shown by a mathematical proof that the lattice-reduction-aided precoding (which has

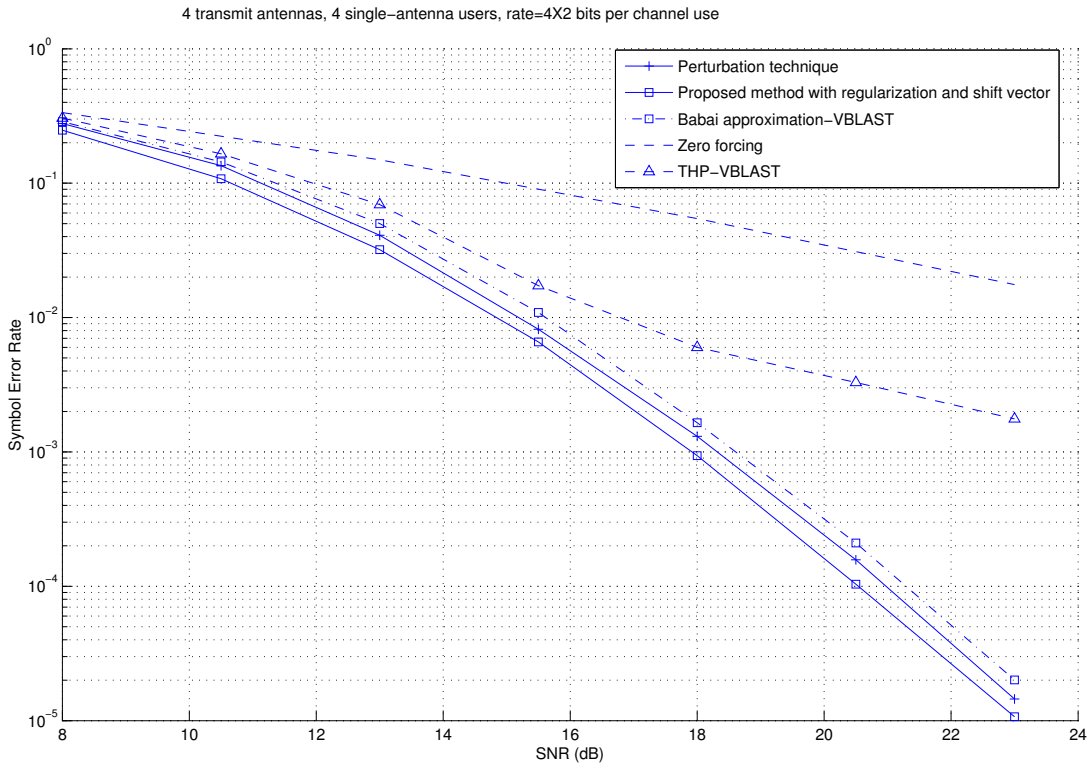

Fig. 4. Comparison of the regularized proposed scheme with V-BLAST modifications of Zero-Forcing and Babai approximation (for $N = 4$ transmit antennas and $M = 4$ single-antenna receivers with the rate $R = 2$ bits per channel use per user.).

a polynomial-time complexity) achieves the maximum precoding diversity. Also, simulation results show that the performance of the proposed modified scheme is very close to the performance of the perturbation method. Also,

APPENDIX A

In this Appendix, we compute the second moment of a parallelotope whose centroid is the origin and its edges are equal to the basis vectors of the lattice.

Assume that $\mathcal{A}$ is an M-dimensional parallelotope and X is its second moment. The second moment of $\frac{1}{2}\mathcal{A}$ is $\left(\frac{1}{2}\right)^{M+2} X$. The parallelotope $\mathcal{A}$ can be considered as the union of 2^M smaller parallelotopes which are constructed by $\pm\frac{1}{2}\mathbf{b}_1, \pm\frac{1}{2}\mathbf{b}_2, ..., \pm\frac{1}{2}\mathbf{b}_M$, where $\mathbf{b}_i$, $1 \leq i \leq M$, is a basis vector. These parallelotopes are translated versions of $\frac{1}{2}\mathcal{A}$ with the

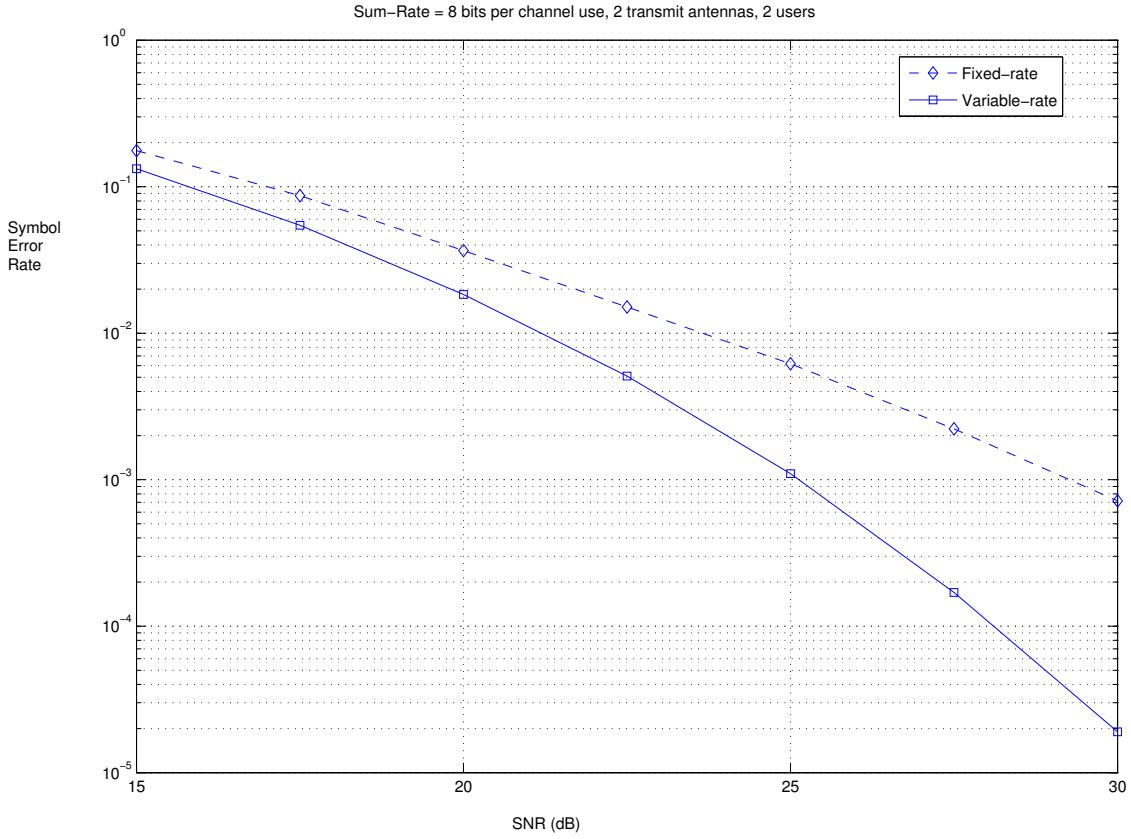

Fig. 5. Performance comparison between the fixed-rate and the variable-rate transmission for $N = 2$ transmit antennas and $M = 2$ single-antenna receivers with sum-rate 8 bits per channel use.

translation vectors $T_i = \pm\frac{1}{2}\mathbf{b}_1 \pm \frac{1}{2}\mathbf{b}_2 \pm .... \pm \frac{1}{2}\mathbf{b}_M$, $1 \leq i \leq 2^M$. The second moments of these parallelotopes are equal to $\left(\frac{1}{2}\right)^{M+2} X + \|T_i\|^2 \text{Vol}(\frac{1}{2}\mathcal{A})$, $1 \leq i \leq 2^M$. By the summation over all these second moments, we can find the second moment of $\mathcal{A}$.

$$X = \sum_{i=1}^{2^M} \left[\left(\frac{1}{2}\right)^{M+2} X + \|T_i\|^2 . \text{Vol}(\frac{1}{2}\mathcal{A}) \right] \tag{98}$$

$$= \left(\frac{1}{2}\right)^2 X + 2^{M-2}(\|\mathbf{b}_1\|^2 + ... + \|\mathbf{b}_M\|^2) . \text{Vol}(\frac{1}{2}\mathcal{A}) \tag{99}$$

$$= \frac{1}{4}X + \frac{1}{4}(\|\mathbf{b}_1\|^2 + ... + \|\mathbf{b}_M\|^2) . \text{Vol}(\mathcal{A}) \tag{100}$$

$$\Longrightarrow X = \frac{1}{3}(\|\mathbf{b}_1\|^2 + ... + \|\mathbf{b}_M\|^2) . \text{Vol}(\mathcal{A}). \tag{101}$$

APPENDIX B
PROOF OF LEMMA 3

Lemma 3 states that the probability that a lattice, generated by M independent N-dimensional complex Gaussian vectors, $N \geq M$, with a unit variance per each dimension, has a nonzero point inside a sphere (centered at origin and with the radius ε) is bounded by $\beta_{N,M}\varepsilon^{2N}$ for $N > M$, and $\beta_{N,M}\varepsilon^{2N}\max\left\{(-\ln\varepsilon)^{N+1}, 1\right\}$ for $N = M \geq 2$. We can assume that $\varepsilon < 1$ (for $\varepsilon \geq 1$, lemma 3 is trivial because the probability is bounded).

A. *Case 1:* $M = 1$

When $M = 1$, the lattice consists of the integer multiples of the basis vector $\mathbf{v}$. If the norm of one of these vectors is less than ε, then the norm of $\mathbf{v}$ is less than ε. Consider the variance of the components of $\mathbf{v}$ as ϱ^2. The vector $\mathbf{v}$ has an N-dimensional complex Gaussian distribution, $f_{\mathbf{v}}(\mathbf{v})$. Therefore, the probability of this event is,

$$\Pr\{\|\mathbf{v}\| \leq \varepsilon\} = \int_{\|\mathbf{v}\|\leq\varepsilon} f_{\mathbf{v}}(\mathbf{v})\, d\mathbf{v} \leq \int_{\|\mathbf{v}\|\leq\varepsilon} \frac{1}{\pi^N \varrho^{2N}}\, d\mathbf{v} \leq \beta_{N,1}\frac{\varepsilon^{2N}}{\varrho^{2N}}. \tag{102}$$

When the variance of the components of $\mathbf{v}$ is equal to one, we have,

$$\Pr\{\|\mathbf{v}\| \leq \varepsilon\} \leq \beta_{N,1}\varepsilon^{2N}. \tag{103}$$

B. *Case 2:* $N > M > 1$

Consider $L_{(\mathbf{v}_1,...,\mathbf{v}_M)}$ as the lattice generated by $\mathbf{v}_1$,$\mathbf{v}_2$,...,$\mathbf{v}_M$. Each point of $L_{(\mathbf{v}_1,...,\mathbf{v}_M)}$ can be represented by $\mathbf{v}_{(z_1,...,z_M)} = z_1\mathbf{v}_1 + z_2\mathbf{v}_2 + ... + z_M\mathbf{v}_M$, where $z_1, ..., z_M$ are complex integer numbers. The vectors $\mathbf{v}_1$,$\mathbf{v}_2$,...,$\mathbf{v}_M$ are independent and jointly Gaussian. Therefore, for every integer vector $\mathbf{z} = (z_1, ..., z_M)$, the entries of the vector $\mathbf{v}_{(z_1,...,z_M)}$ have complex Gaussian distributions with the variance

$$\varrho_{\mathbf{z}}^2 = \|\mathbf{z}\|^2\varrho^2 = \left(|z_1|^2 + ... + |z_M|^2\right)\varrho^2. \tag{104}$$

Therefore, according to the lemma for $M = 1$,

$$\Pr\left\{\|\mathbf{v}_{(z_1,...,z_M)}\| \leq \varepsilon\right\} \leq \beta_{N,1}\frac{\varepsilon^{2N}}{\left(|z_1|^2 + ... + |z_M|^2\right)^N}. \tag{105}$$

Now, by using the union bound,

$$\Pr\left\{d_{\mathbf{H}} \leq \varepsilon\right\} \leq \sum_{\mathbf{z}\neq 0} \Pr\left\{\|\mathbf{v}_{(z_1,...,z_M)}\| \leq \varepsilon\right\} \tag{106}$$

$$\leq \sum_{\mathbf{z}\neq 0} \beta_{N,1} \frac{\varepsilon^{2N}}{\left(|z_1|^2 + ... + |z_M|^2\right)^N} \tag{107}$$

$$= \beta_{N,1} \left(\sum_{1\leq\|\mathbf{z}\|<2} \frac{\varepsilon^{2N}}{\|\mathbf{z}\|^{2N}} + \sum_{2\leq\|\mathbf{z}\|<3} \frac{\varepsilon^{2N}}{\|\mathbf{z}\|^{2N}} + \sum_{3\leq\|\mathbf{z}\|<4} \frac{\varepsilon^{2N}}{\|\mathbf{z}\|^{2N}} + ... \right). \tag{108}$$

The M-dimensional complex integer points $\mathbf{z} = (z_1, ..., z_M)$, such that $k \leq \|\mathbf{z}\| < k+1$, can be considered as the centers of disjoint unit-volume cubes. All these cubes are inside the region between the $2M$-dimensional spheres, with radii $k-1$ and $k+2$. Therefore, the number of M-dimensional complex integer points $\mathbf{z} = (z_1, ..., z_M)$, such that $k \leq \|\mathbf{z}\| < k+1$, can be bounded by the volume of the region between these two $2M$-dimensional spheres. Thus, this number is bounded by $c_1 k^{2M-1}$ for some constant[5] c_1. Therefore,

$$\sum_{k\leq\|\mathbf{z}\|<k+1} \frac{\varepsilon^{2N}}{\|\mathbf{z}\|^{2N}} \leq c_1 k^{2M-1} \frac{\varepsilon^{2N}}{k^{2N}} \tag{109}$$

$$(108), (109) \Longrightarrow \Pr\left\{d_{\mathbf{H}} \leq \varepsilon\right\} \leq c_1\beta_{N,1}\varepsilon^{2N} + 2^{2M-1}c_1\beta_{N,1}\frac{\varepsilon^{2N}}{2^{2N}} +$$

$$+3^{2M-1}c_1\beta_{N,1}\frac{\varepsilon^{2N}}{3^{2N}} + ... \tag{110}$$

$$\leq c_1\beta_{N,1}\varepsilon^{2N} \sum_{k=1}^{\infty} \frac{1}{k^{2N-2M+1}}. \tag{111}$$

According to the assumption of this case, $N > M$; hence, $2N-2M+1 \geq 2$. Therefore, the above summation is convergent:

$$\Pr\left\{\|\mathbf{v}\| \leq \varepsilon\right\} \leq \beta_{N,M}\varepsilon^{2N}. \tag{112}$$

[5]Throughout this proof, $c_1, c_2, ...$ are some constant numbers.

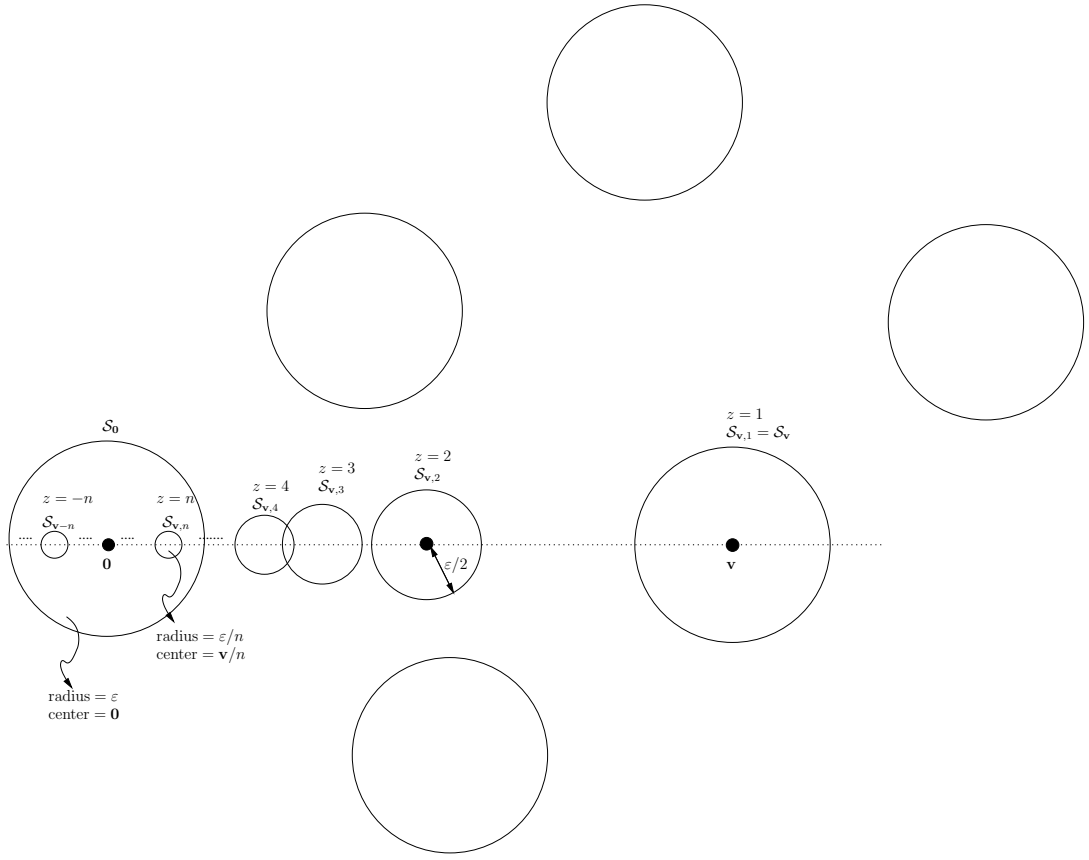

Fig. 6. The family of spheres $\mathcal{S}_{\mathbf{v},z}$

C. Case 3: $N = M > 1$

Each point of $L_{(\mathbf{v}_1,\ldots,\mathbf{v}_N)}$ can be represented by $z\mathbf{v}_N - \mathbf{v}$, where $\mathbf{v}$ belongs to the lattice $L_{(\mathbf{v}_1,\ldots,\mathbf{v}_{N-1})}$ and z is a complex integer. Consider $\mathcal{S}_{\mathbf{v}}$ as the sphere with radius ε and centered at $\mathbf{v}$. Now, $z\mathbf{v}_N - \mathbf{v}$ belongs to $\mathcal{S}_{\mathbf{0}}$ iff the $z\mathbf{v}_N$ belongs to $\mathcal{S}_{\mathbf{v}}$. Also, the sphere $\mathcal{S}_{\mathbf{v}}$ includes a point $z\mathbf{v}_N$ iff $\mathcal{S}_{\mathbf{v},z}$ includes $\mathbf{v}$, where $\mathcal{S}_{\mathbf{v},z} = \frac{\mathcal{S}_{\mathbf{v}}}{z}$ is the sphere centered at $\mathbf{v}/z$ with radius $\dfrac{\varepsilon}{|z|}$ (see figure 6). Therefore, the probability that a lattice point exists in $\mathcal{S}_{\mathbf{v}}$ is equal to the probability that $\mathbf{v}_N$ is in at least one of the spheres $\{\mathcal{S}_{\mathbf{v},z}\}$, $z \neq 0$.

If we consider $d_{\mathbf{H}}$ as the minimum distance of $L_{(\mathbf{v}_1,\ldots,\mathbf{v}_N)}$ and R as an arbitrary number greater than 1:

$$\Pr\{d_{\mathbf{H}} \leq \varepsilon\} = \Pr\left\{\left(L_{(\mathbf{v}_1,\ldots,\mathbf{v}_N)} - 0\right) \cap \mathcal{S}_{\mathbf{0}} \neq \varnothing\right\} = \Pr\left\{\mathbf{v}_N \in \bigcup_{\mathbf{v}} \bigcup_{z \neq 0} \mathcal{S}_{\mathbf{v},z}\right\} \tag{113}$$

$$\leq \Pr\left\{\mathbf{v}_N \in \bigcup_{\|\frac{\mathbf{v}}{z}\| \leq R} \mathcal{S}_{\mathbf{v},z}\right\} + \Pr\left\{\mathbf{v}_N \in \bigcup_{\|\frac{\mathbf{v}}{z}\| > R} \mathcal{S}_{\mathbf{v},z}\right\} \tag{114}$$

In the second term of (114), all the spheres have centers with norms greater than R and radii less than 1 (because $|z| \geq 1$). Therefore,

$$\bigcup_{\|\frac{\mathbf{v}}{z}\| > R} \mathcal{S}_{\mathbf{v},z} \subset \{\mathbf{x} \,|\, \|\mathbf{x}\| > R - 1\} \tag{115}$$

$$(115) \Longrightarrow (114) \leq \Pr\left\{\mathbf{v}_N \in \bigcup_{\|\frac{\mathbf{v}}{z}\| \leq R} \mathcal{S}_{\mathbf{v},z}\right\} + \Pr\{\|\mathbf{v}_N\| > R - 1\} \tag{116}$$

$$\leq \Pr\left\{\mathbf{v}_N \in \bigcup_{\|\frac{\mathbf{v}}{z}\| \leq R, |z| \leq \varepsilon^{1-N}} \mathcal{S}_{\mathbf{v},z}\right\} + \Pr\left\{\mathbf{v}_N \in \bigcup_{\|\frac{\mathbf{v}}{z}\| \leq R, |z| > \varepsilon^{1-N}} \mathcal{S}_{\mathbf{v},z}\right\} + \Pr\{\|\mathbf{v}_N\| > R - 1\}. \tag{117}$$

We bound the first term of (117) as the following:

$$\Pr\{\mathbf{v}_N \in \bigcup_{\|\frac{\mathbf{v}}{z}\| \leq R, |z| \leq \varepsilon^{1-N}} \mathcal{S}_{\mathbf{v},z}\} \tag{118}$$

$$\leq \left(\sum_{\|\mathbf{v}\| \leq 2R} \sum_{|z| \geq 1} \Pr\{\mathbf{v}_N \in \mathcal{S}_{\mathbf{v},z}\} + \sum_{2R < \|\mathbf{v}\| \leq 3R} \sum_{|z| \geq 2} \Pr\{\mathbf{v}_N \in \mathcal{S}_{\mathbf{v},z}\} + \right.$$

$$\left. \ldots + \sum_{\lfloor \varepsilon^{1-N} \rfloor R < \|\mathbf{v}\| \leq (\lfloor \varepsilon^{1-N} \rfloor + 1)R} \sum_{|z| \geq \lfloor \varepsilon^{1-N} \rfloor} \Pr\{\mathbf{v}_N \in \mathcal{S}_{\mathbf{v},z}\} \right). \tag{119}$$

Noting that the pdf of $\mathbf{v}_N$ is less than or equal to $\frac{1}{\pi^N}$,

$$(118) \leq \frac{1}{\pi^N} \left(\sum_{\|\mathbf{v}\| \leq 2R} \sum_{|z| \geq 1} \mathrm{Vol}(\mathcal{S}_{\mathbf{v},z}) + \sum_{2R < \|\mathbf{v}\| \leq 3R} \sum_{|z| \geq 2} \mathrm{Vol}(\mathcal{S}_{\mathbf{v},z}) + \right.$$

$$\left. \ldots + \sum_{\lfloor \varepsilon^{1-N} \rfloor R < \|\mathbf{v}\| \leq (\lfloor \varepsilon^{1-N} \rfloor + 1)R} \sum_{|z| \geq \lfloor \varepsilon^{1-N} \rfloor} \mathrm{Vol}(\mathcal{S}_{\mathbf{v},z}) \right) \tag{120}$$

$$\leq \frac{1}{\pi^N}\left(\sum_{\|\mathbf{v}\|\leq 2R}\sum_{|z|\geq 1}\frac{c_2\varepsilon^{2N}}{|z|^{2N}}+\sum_{2R<\|\mathbf{v}\|\leq 3R}\sum_{|z|\geq 2}\frac{c_2\varepsilon^{2N}}{|z|^{2N}}+\right.$$

$$\left.\ldots+\sum_{\lfloor\varepsilon^{1-N}\rfloor R<\|\mathbf{v}\|\leq(\lfloor\varepsilon^{1-N}\rfloor+1)R}\quad\sum_{|z|\geq\lfloor\varepsilon^{1-N}\rfloor}\frac{c_2\varepsilon^{2N}}{|z|^{2N}}\right). \tag{121}$$

By using (109), for one-dimensional complex vector $\mathbf{z}=z$,

$$\sum_{|z|\geq i}\frac{c_2\varepsilon^{2N}}{|z|^{2N}}=\sum_{k=i}^{\infty}c_2.\sum_{k\leq|z|\leq k+1}\frac{\varepsilon^{2N}}{|z|^{2N}}\leq\sum_{k=i}^{\infty}\frac{c_1c_2\varepsilon^{2N}}{k^{2N-1}}\leq\frac{c_3\varepsilon^{2N}}{i^{2N-2}} \tag{122}$$

Now,

$$(122)\Longrightarrow(118)\leq\frac{1}{\pi^N}\left(\sum_{\|\mathbf{v}\|\leq 2R}c_3\varepsilon^{2N}+\sum_{2R<\|\mathbf{v}\|\leq 3R}\frac{c_3\varepsilon^{2N}}{2^{2N-2}}+\right.$$

$$\left.\ldots+\sum_{\lfloor\varepsilon^{1-N}\rfloor R<\|\mathbf{v}\|\leq(\lfloor\varepsilon^{1-N}\rfloor+1)R}\frac{c_3\varepsilon^{2N}}{\lfloor\varepsilon^{1-N}\rfloor^{2N-2}}\right). \tag{123}$$

Assume that the minimum distance of $L_{(\mathbf{v}_1,\ldots,\mathbf{v}_{N-1})}$ is d_{N-1}. The spheres with the radius $d_{N-1}/2$ and centered by the points of $L_{(\mathbf{v}_1,\ldots,\mathbf{v}_{N-1})}$ are disjoint. Therefore, the number of points from the $(N-1)$-dimensional complex lattice $L_{(\mathbf{v}_1,\ldots,\mathbf{v}_{N-1})}$, such that $\|\mathbf{v}\|\leq 2R$, is bounded by $\frac{c_4(2R+d_{N-1}/2)^{2N-2}}{d_{N-1}^{2N-2}}$ (it is bounded by the ratio between the volumes of $(2N-2)$-dimensional spheres with radii $2R+d_{N-1}/2$ and $d_{N-1}/2$). Also, the number of points from $L_{(\mathbf{v}_1,\ldots,\mathbf{v}_{N-1})}$, such that $(k-1)R<\|\mathbf{v}\|\leq kR$, is bounded by $\frac{c_4(kR)^{2N-3}(R+d_{N-1})}{d_{N-1}^{2N-2}}$ (it is bounded by the ratio between the volumes of the region defined by $(k-1)R-d_{N-1}/2<\|\mathbf{x}\|\leq kR+d_{N-1}/2$ and the sphere with radius $d_{N-1}/2$):

$$(123)\leq\frac{c_5(2R+d_{N-1}/2)^{2N-2}}{d_{N-1}^{2N-2}}.\varepsilon^{2N}+\frac{c_5R^{2N-3}(R+d_{N-1})}{d_{N-1}^{2N-2}}.\varepsilon^{2N}\sum_{k=2}^{\lfloor\varepsilon^{1-N}\rfloor}\frac{1}{k} \tag{124}$$

$$(123)\leq\frac{c_5(2R+d_{N-1}/2)^{2N-2}}{d_{N-1}^{2N-2}}.\varepsilon^{2N}+\frac{c_5R^{2N-3}(R+d_{N-1})}{d_{N-1}^{2N-2}}.\varepsilon^{2N}.\ln(\varepsilon^{1-N}) \tag{125}$$

$$\leq c_6\varepsilon^{2N}.\max\left(\frac{R^{2N-2}}{d_{N-1}^{2N-2}},1\right).\max\left\{-\ln\varepsilon,1\right\}. \tag{126}$$

According to the proof of the case 2, we have $\Pr\{d_{N-1} \leq \eta\} \leq \beta_{N,N-1}\eta^{2N}$. Therefore,

$$\mathrm{E}_{d_{N-1}}\left\{\max\left(\frac{R^{2N-2}}{d_{N-1}^{2N-2}}, 1\right)\right\} \tag{127}$$

$$\leq 1.\Pr\{d_{N-1} > R\} + 2^{2N-2}.\Pr\left\{\frac{1}{2}R < d_{N-1} \leq R\right\} + 3^{2N-2}.\Pr\left\{\frac{1}{3}R < d_{N-1} \leq \frac{1}{2}R\right\} + ... \tag{128}$$

$$\leq 1 + 2^{2N-2}.\Pr\{d_{N-1} \leq R\} + 3^{2N-2}.\Pr\left\{d_{N-1} \leq \frac{1}{2}R\right\} + ... \tag{129}$$

$$\leq 1 + \sum_{k=1}^{\infty}\frac{(k+1)^{2N-2}}{k^{2N}}.R^{2N}\beta_{N,N-1} \leq c_7 R^{2N} \tag{130}$$

$$\Longrightarrow \mathrm{E}_{d_{N-1}}\left\{c_6\varepsilon^{2N}.\max\left(\frac{R^{2N-2}}{d_{N-1}^{2N-2}}, 1\right).\max\{-\ln\varepsilon, 1\}\right\} \leq c_8\varepsilon^{2N}.R^{2N}.\max\{-\ln\varepsilon, 1\}. \tag{131}$$

To bound the second term of (117), we note that for $|z| \geq \varepsilon^{1-N}$, the radii of the spheres $\mathcal{S}_{\mathbf{v},z}$ are less or equal to ε^N, and the centers of these spheres lie on the $(N-1)$-dimensional complex subspace containing $L_{\mathbf{v}_1,...,\mathbf{v}_{N-1}}$. Also, the norm of these centers are less than R. Therefore, all of these spheres are inside the region $\mathcal{A}$ which is an orthotope centered at the origin, with $2N$ real dimensions (see figure 7):

$$\bigcup_{\|\frac{\mathbf{v}}{z}\| \leq R, |z| > \varepsilon^{1-N}} \mathcal{S}_{\mathbf{v},z} \subset \mathcal{A} \tag{132}$$

$$\Longrightarrow \Pr\{\mathbf{v}_N \in \bigcup_{\|\frac{\mathbf{v}}{z}\| \leq R, |z| > \varepsilon^{1-N}} \mathcal{S}_{\mathbf{v},z}\} \leq \frac{1}{\pi^N}\mathrm{Vol}\left(\bigcup_{\|\frac{\mathbf{v}}{z}\| \leq R, |z| > \varepsilon^{1-N}} \mathcal{S}_{\mathbf{v},z}\right) \leq \frac{1}{\pi^N}\mathrm{Vol}(\mathcal{A}) \tag{133}$$

$$\leq \frac{1}{\pi^N}(2\varepsilon^N)^2(2R + \varepsilon^N)^{2N-2} \tag{134}$$

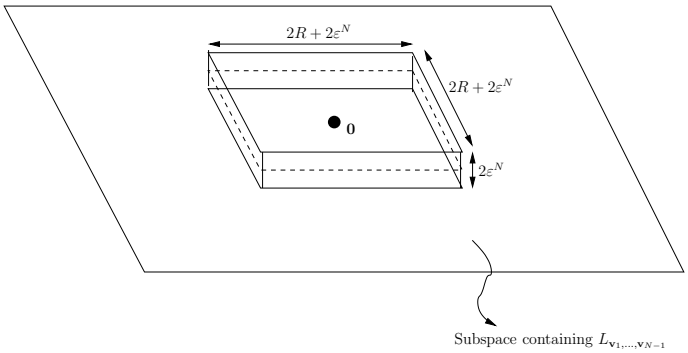

Fig. 7. The orthotope $\mathcal{A}$

Also, according to the Gaussian distribution of the entries of $\mathbf{v}_N$ (which have Variance $\frac{1}{2}$ on each real dimension), we can bound the third term of (117) as,

$$\Pr\{\|\mathbf{v}_N\| > R-1\} \leq 2NQ\left(\sqrt{\frac{R-1}{N}}\right) \leq c_9 e^{-\left(\frac{R-1}{\sqrt{2N}}\right)^2}. \tag{135}$$

By using (131), (134), and (135),

$$\Pr\left\{d_{\mathbf{H}} \leq \varepsilon\right\} \leq c_8 \varepsilon^{2N}.R^{2N}.\max\left\{-\ln\varepsilon, 1\right\} + \frac{1}{\pi^N}(2\varepsilon^N)^2(2R+\varepsilon^N)^{2N-2} + c_9 e^{-\left(\frac{R-1}{\sqrt{2N}}\right)^2}. \tag{136}$$

The above equation is true for every $R > 1$. Therefore, using $R = \sqrt{2}N\sqrt{-\ln(\varepsilon^{2N})} + 1$,

$$\Pr\left\{d_{\mathbf{H}} \leq \varepsilon\right\} \leq \beta_{N,N}\varepsilon^{2N}.\max\left\{(-\ln\varepsilon)^{N+1}, 1\right\}. \tag{137}$$

REFERENCES

[1] I. E. Telatar, "Capacity of multi-antenna gaussian channels," *Europ. Trans. Telecommun.*, pp. 585–595, Nov. 1999.

[2] G. J. Foschini, "Layered space-time architechture for wireless communication in a fading environment when using multi-element antennas," *Bell labs. Tech. J.*, vol. 1, no. 2, pp. 41–59, 1996.

[3] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Info. Theory*, vol. 44, pp. 744–765, Mar. 1998.

[4] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Info. Theory*, vol. 45, pp. 1456–1467, July 1999.

[5] S. M. Alamouti, "A simple transmitter diversity scheme for wireless communications," *IEEE J. Selec. Areas Commun.*, vol. 16, pp. 1451–1458, Oct. 1998.

[6] G. Caire and S. Shamai, "On the acheivable throughput of a multiple-antenna Gaussian broadcast channel," *IEEE Trans. Info. Theory*, pp. 1691–1706, July 2003.

[7] W. Yu and J. Cioffi, "Sum capacity of a Gaussian vector broadcast channel," in *Proceedings IEEE International Symposium on Information Theory*, p. 498, 2002.

[8] P. Viswanath and D. Tse, "Sum capacity of the vector Gaussian broadcast channel and uplink-downlink duality," *IEEE Trans. Info Theory*, pp. 1912–1921, August 2003.

[9] S. Vishwanath, N. Jindal, and A. Goldsmith, "Duality, acheivable rates and sum capacity of Gaussian MIMO broadcast channels," *IEEE Trans. Info. Theory*, pp. 2658–2658, August 2003.

[10] M. Costa, "Writing on dirty paper," *IEEE Trans. Info. Theory*, vol. 29, pp. 439–441, May 1983.

[11] U. Erez, S. Shamai, and R. Zamir, "Capacity and lattice strategies for canceling known interference," *IEEE Trans. Info. Theory*, pp. 3820 – 3833, Nov. 2005.

[12] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst, "A vector-perturbation technique for near-capacity multiple-antenna multi-user communications-Part II: Perturbation," *IEEE Trans. Comm.*, pp. 537 – 544, March 2005.

[13] C. Windpassinger and R. Fischer, "Low-complexity near-maximum-likelihood detection and precoding for MIMO systems using lattice reduction," in *Proceedings of Information Theory Workshop*, 2003.

[14] C. Windpassinger, R. F. H. Fischer, and J. B. Huber, "Lattice-reduction-aided broadcast precoding," in *5th International ITG Conference on Source and Channel Coding (SCC)*, (Erlangen, Germany), pp. 403–408, January 2004.

[15] C. Windpassinger, R. Fischer, and J. B. Huber, "Lattice-reduction-aided broadcast precoding," *IEEE Trans. Communications*, pp. 2057–2060, Dec. 2004.

[16] R. Fischer, "Lattice-reduction-aided equalization and generalized partial response signaling for point-to-point transmission over flat-fading MIMO channels," in *6th International ITG-Conference on Source and Channel Coding*, (Munich, Germany), April 2006.

[17] M. Grotschel, L. Lovasz, and A. Schrijver, *Geometrical algorithms and combinatorial optimization*, ch. 5. Springer-Verlag, 1993.

[18] P. M. Gruber and C. G. Lekkerkerker, *Geometry of numbers*. North-Holland, 1987.

[19] B. Helfrich, "Algorithms to construct minkowski reduced and hermit reduced lattice bases," *Theoretical Computer Sci. 41*, pp. 125–139, 1985.

[20] A. K. Lenstra, H. W. Lenstra, and L. Lovasz, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, pp. 515–534, 1982.

[21] H. Napias, "A generalization of the LLL algorithm over euclidean rings or orders," *Journal de thorie des nombres de Bordeaux*, vol. 8, pp. 387–396, 1996.

[22] G. D. Forney and L. F. Wei, "Multidimensional constellations-Part I: Introduction, figures of merit, and generalized cross constellations," *IEEE J. Select Areas Commun.*, vol. 7, pp. 877–892, August 1989.

[23] M. Ajtai, "The shortest vector problem in L2 is NP-hard for randomized reductions," in *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pp. 10–19, 1998.

[24] J. H. Conway and N. J. A. Sloane, *Sphere packing, lattices and groups*. Springer-Verlag, 1999.

[25] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst, "A vector-perturbation technique for near-capacity multiple-antenna multi-user communications-Part I: channel inversion and regularization," *IEEE Trans. Comm.*, pp. 195 – 202, Jan. 2005.

[26] D. A. Schmidt, M. Joham, and W. Utschick, "Minimum mean square error vector precoding," in *PIMRC 2005*, pp. 107–111, 2005.

[27] E. Agrell, T. Eriksson, A. Vardy, , and K. Zeger, "Closest point search in lattices," *IEEE Trans. Info. Theory*, vol. 48, pp. 2201–2214, August 2002.

[28] L. Zheng and D. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," *IEEE Trans. Info. Theory*, pp. 1073–1096, May 2003.

[29] M. Markus and H. Minc, *A survey of matrix theory and matrix inequalities*. Dover, 1964.