LLL Lattice-Basis Reduction Achieves the Maximum Diversity in MIMO Systems

Mahmoud Taherzadeh, Amin Mobasher and Amir. K. Khandani
Coding & Signal Transmission Laboratory (www.cst.uwaterloo.ca)
Dept. of Elec. and Comp. Eng., University of Waterloo, Waterloo, ON, Canada, N2L 3G1
e-mail: {taherzad, amin, khandani}@cst.uwaterloo.ca, Tel: 519-8848552, Fax: 519-8884338

***Abstract*— Diversity order is an important measure for the performance of different communication systems over MIMO fading channels. In this paper, we define the precoding diversity for the fixed-rate MIMO broadcast systems and we prove that in these systems, lattice-reduction-aided precoding achieves the precoding diversity. Also, we prove that lattice-reduction-aided decoding achieves the receive diversity in MIMO point-to-point and multiple-access systems[1].**

I. Introduction

In the recent years, MIMO communications over multiple-antenna channels has attracted many researchers. In [1], a transmission technique called V-BLAST is introduced for high-rate communications over point-to point MIMO fading channels. V-BLAST sends independent symbols over different transmit antennas. Therefore, it can also be used for MIMO multi-access systems. The basic proposed sub-optimum decoding methods for BLAST (such as nulling and cancelling, zero forcing and GDFE-type methods) can not achieve the maximum receive diversity which is equal to the number of receive antennas. In [2], a lattice decoder is proposed for the decoding of BLAST which achieves the maximum diversity. However, its complexity is exponential with the number of antennas. In [3], an approximation of lattice decoding, using lattice-basis reduction, is introduced which has a polynomial complexity and the simulation results show that it achieves the receive diversity.

Recently, new information theoretic results [4], [5], [6], [7], have shown that also in multiuser MIMO systems we can exploit many of the advantages of multiple-antenna systems. In [8], the authors have introduced a *vector perturbation technique* which has a good performance in terms of symbol error rate and they have shown by simulation that it achieves a diversity order equal to the number of transmit antennas. Nonetheless, this technique requires a lattice-decoder which is an NP-hard problem. In [9], the authors have used lattice-basis reduction to approximate the closest lattice point (using Babai approximation). Also, in [10], a similar lattice-reduction-aided precoding is used to reduce the average transmitted power by reducing the second moment of the fundamental region of the lattice. In this paper, we define the precoding diversity for fixed-rate MIMO broadcast systems and prove that by using the method based on lattice-basis reduction, we achieve the maximum precoding diversity in fixed-rate MIMO broadcast systems. Also, we explain its relation with MIMO multiple-access and point-to-point systems and give a mathematical proof for achieving the receive diversity by the lattice-reduction-aided decoding.

[1]This work is financially supported by Communications and Information Technology Ontario (CITO), Nortel Networks, and Natural Sciences and Engineering Research Council of Canada (NSERC).

II. System Model

We consider a multiple-antenna system with M transmit antennas and M receive antennas. In the broadcast system, we consider different receive antennas as different users and in the multi-access system, we consider separate transmit antennas. If we consider $\mathbf{y} = [y_1, ..., y_M]^T$, $\mathbf{x} = [x_1, ..., x_M]^T$, $\mathbf{w} = [w_1, ..., w_M]^T$ and the $M \times M$ matrix $\mathbf{H}$, respectively, as the received signal, the transmitted signal, the noise vector and the channel matrix, we have the following matrix equation:

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

The channel is assumed to be Raleigh and the noise is Gaussian, i.e. the elements of $\mathbf{H}$ are i.i.d with the zero-mean unit-variance complex Gaussian distribution. Also, we have the power constraint on the transmitted signal, $\mathrm{E}\|\mathbf{x}\|^2 = 1$. The power of the additive noise is σ^2 per antenna, i.e. $\mathrm{E}\|\mathbf{w}\|^2 = M\sigma^2$. Therefore, the signal to noise ratio (SNR) is defined as $\rho = \frac{1}{\sigma^2}$.

For the broadcast system, in the decoding of the received signal, the users can not cooperate with each other. To resolve this problem, we can construct the transmitted signals such that the interference is cancelled in the receiver, i.e. different users see independent signals (only their data which is added by the additive noise). Consider $\mathbf{B}$ as the reduced version of $\mathbf{H}^{-1}$ and $\mathbf{u}$ as the data vector which consists of integer elements. At the transmitter we send $\mathbf{x} = \mathbf{B}\mathbf{u}'$ where $\mathbf{u} = \mathbf{u}' \bmod a$, and a is a constant number, related to the size of constellation.

For the multiple-access system, we send the transmitted vector $\mathbf{x}$ with independent entries from $\mathbb{Z}^2$ and at the receiver, we find $\tilde{\mathbf{x}}$ as the closest integer point to $\mathbf{B}\mathbf{y}$ where $\mathbf{B}$ is the reduced version of $\mathbf{H}^{*-1}$ ($\mathbf{B} = \mathbf{H}^{*-1}\mathbf{U}$ where $\mathbf{U}$ is a unimodular matrix). When the data is restricted in a hypercube with size a, the transmitted vector can be decoded by modulo operation:

$$\widehat{\mathbf{x}} = \mathbf{U}\tilde{\mathbf{x}} \bmod a$$

III. Diversity and Outage Probability for Fixed-Rate MIMO Broadcast Systems

When we have the channel-state information at the transmitter, if there is no assumption on the transmission rates, the outage probability is not meaningful. However, when we consider fixed 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 of the capacity region.

Theorem 1: For a MIMO broadcast system with M transmit antennas and M single-antenna receivers and fixed rates $R_1, ..., R_M$,

$$\lim_{\rho\to\infty} \frac{-\log P_{out}}{\log \rho} \leq M.$$

Proof: If we consider P_{out1} as the probability that the capacity of the point-to-point system consisting of M transmit antennas and one receive antenna (with independent channel coefficient and CSI at the transmitter) is less than R_1,

$$P_{out} \geq P_{out1}$$

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

By using the Chernoff bound, we have,

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

$$\Longrightarrow \lim_{\rho\to\infty} \frac{-\log P_{out}}{\log \rho} \leq \lim_{\rho\to\infty} \frac{-\log P_{out1}}{\log \rho} \leq M.$$

We can also 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. Based on theorem 1, the maximum achievable diversity is M. We show that the proposed method (based on lattice-basis reduction) achieves the maximum diversity.

Lemma 1: Consider $\mathbf{B} = [\mathbf{b}_1...\mathbf{b}_M]$ as an $M \times M$ matrix, with the orthogonality defect[2] δ, and $(\mathbf{B}^{-1})^* = [\mathbf{a}_1...\mathbf{a}_M]$ as the Hermitian of its inverse. Then,

$$\max\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\} \leq \frac{\sqrt{\delta}}{\min\{\|\mathbf{a}_1\|, ..., \|\mathbf{a}_M\|\}}. \quad (2)$$

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,

$$\|\mathbf{b}_1\|...\|\mathbf{b}_{i-1}\|.\|\mathbf{b}_i\|.\|\mathbf{b}_{i+1}\|...\|\mathbf{b}_M\| = \det\mathbf{B}\sqrt{\delta}$$
$$= \det[\mathbf{b}_1...\mathbf{b}_{i-1}\mathbf{b}'_i\mathbf{b}_{i+1}...\mathbf{b}_M]\sqrt{\delta} \quad (3)$$

Acoording to the Hadamard theorem:

$$\det[\mathbf{b}_1...\mathbf{b}_{i-1}\mathbf{b}'_i\mathbf{b}_{i+1}...\mathbf{b}_M] \leq$$
$$\|\mathbf{b}_1\|...\|\mathbf{b}_{i-1}\|.\|\mathbf{b}'_i\|.\|\mathbf{b}_{i+1}\|...\|\mathbf{b}_M\| \quad (4)$$

Therefore,

$$\|\mathbf{b}_1\|...\|\mathbf{b}_{i-1}\|.\|\mathbf{b}_i\|.\|\mathbf{b}_{i+1}\|...\|\mathbf{b}_M\| \leq$$
$$\|\mathbf{b}_1\|...\|\mathbf{b}_{i-1}\|.\|\mathbf{b}'_i\|.\|\mathbf{b}_{i+1}\|...\|\mathbf{b}_M\|\sqrt{\delta}$$
$$\Longrightarrow \|\mathbf{b}_i\| \leq \|\mathbf{b}'_i\|\sqrt{\delta}. \quad (5)$$

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

$$1 = <\mathbf{a}_i, (\mathbf{b}'_i + \sum_{i\neq j} c_{i,j}\mathbf{b}_j)> = <\mathbf{a}_i, \mathbf{b}'_i> = \|\mathbf{a}_i\|.\|\mathbf{b}'_i\| \quad (6)$$

$$\Longrightarrow \|\mathbf{a}_i\|.\|\mathbf{b}_i\| \leq \sqrt{\delta} \quad (7)$$

$$\Longrightarrow \|\mathbf{b}_i\| \leq \frac{\sqrt{\delta}}{\|\mathbf{a}_i\|} \quad (8)$$

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

$$\max\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\} = \mathbf{b}_i \leq \frac{\sqrt{\delta}}{\|\mathbf{a}_i\|} \quad (9)$$

$$\leq \frac{\sqrt{\delta}}{\min\{\|\mathbf{a}_1\|, ..., \|\mathbf{a}_M\|\}}. \quad (10)$$

■

Lemma 2: Consider $\mathbf{B} = [\mathbf{b}_1...\mathbf{b}_M]$ as an LLL-reduced basis for the lattice generated by $\mathbf{H}^{-1}$ and $d_{\mathbf{H}^*}$ as the minimum distance of the lattice generated by $\mathbf{H}^*$. Then, there is a constant α_M (independent of $\mathbf{H}$) such that

$$\max\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\} \leq \frac{\alpha_M}{d_{\mathbf{H}^*}}. \quad (11)$$

Proof: For a lattice basis obtained by LLL reduction [11],

$$\sqrt{\delta} \leq 2^{M(M-1)/4}. \quad (12)$$

Consider $(\mathbf{B}^{-1})^* = [\mathbf{a}_1, ..., \mathbf{a}_M]$. By using (2) and (12),

$$\max\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\} \leq \frac{\sqrt{\delta}}{\min\{\|\mathbf{a}_1\|, ..., \|\mathbf{a}_M\|\}} \leq$$
$$\frac{2^{M(M-1)/4}}{\min\{\|\mathbf{a}_1\|, ..., \|\mathbf{a}_M\|\}} \quad (13)$$

The basis $\mathbf{B}$ can be written as $\mathbf{B} = \mathbf{H}^{-1}\mathbf{U}$ for some unimodular matrix $\mathbf{U}$:

$$(\mathbf{B}^{-1})^* = ((\mathbf{H}^{-1}\mathbf{U})^{-1})^* = (\mathbf{U}^{-1}\mathbf{H})^* = \mathbf{H}^*(\mathbf{U}^{-1})^* \quad (14)$$

Thus, $(\mathbf{B}^{-1})^* = [\mathbf{a}_1, ..., \mathbf{a}_M]$ is another basis for the lattice generated by $\mathbf{H}^*$. Therefore, the vectors $\mathbf{a}_1, ..., \mathbf{a}_M$ are vectors from the lattice generated by $\mathbf{H}^*$, and therefore, the length of each of them is at least $d_{\mathbf{H}^*}$:

$$\|\mathbf{a}_i\| \geq d_{\mathbf{H}^*} \text{ for } 1 \leq i \leq M \quad (15)$$

[2] orthogonality defect is defined as $\delta = \frac{(\|\mathbf{b}_1\|^2\|\mathbf{b}_2\|^2...\|\mathbf{b}_M\|^2)}{\det\mathbf{B}\mathbf{B}^*}$

$$\Longrightarrow \min\{\|\mathbf{a}_1\|, ..., \|\mathbf{a}_M\|\} \geq d_{\mathbf{H}^*} \tag{16}$$

$$(13) \text{ and } (16) \Longrightarrow \max\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\} \leq \frac{2^{M(M-1)/4}}{d_{\mathbf{H}^*}}. \tag{17}$$

■

Lemma 3: Assume that the entries of the $M \times M$ matrix $\mathbf{H}$ has independent complex Gaussian distributions 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 β_M such that [12],

$$\Pr\{d_{\mathbf{H}} \leq \epsilon\} \leq \beta_M \epsilon^{2M}. \tag{18}$$

Sketch of the proof: We prove this lemma by induction on M, the number of vectors. We should show that the probability that a lattice, generated by M independent Gaussian N-dimensional vectors, has a point inside the sphere, centered at origin and with radius ε, is bounded by $C^{(N,M)}\varepsilon^{2M}$ where $C^{(N,M)}$ is a constant value. Indeed, we prove a stronger statement. We show that When we have M vectors $\mathbf{v}_1, ..., \mathbf{v}_M$ with independent complex Gaussian elements (with zero mean and unit variance) in an N dimensional complex space ($N \geq M$), for any sphere $\mathcal{S}$ (with radius ε and centered at $\mathbf{r}$ where $|\mathbf{r}| = R$):

$$\Pr\{L_{(\mathbf{v}_1,...,\mathbf{v}_M)} \cap \mathcal{S} \neq \varnothing\}$$

$$\leq \begin{cases} C^{(N,M)}\varepsilon^{2N} \text{ for } R \leq 1 \\ \dfrac{C^{(N,M)}\varepsilon^{2N}}{R^{2N-2M+2}} \text{ for } R > 1 \end{cases}. \tag{19}$$

When $M = 1$, the lattice generated by $\mathbf{v}_1$ consists of the integer multiples of $\mathbf{v}_1$. Therefore, the probability of existing a lattice point in $\mathcal{S}$ is equal to the probability that $\mathbf{v}_1$ is in at least one of the spheres $\{\mathcal{S}_z\}$ ($z = n + im$ can be every nonzero Gaussian integer) where $\mathcal{S}_z$ is the sphere which is centered at $\mathbf{r}/z$ and its radius is equal to $\dfrac{\varepsilon}{|z|}$.

$$\Pr\{v_1 \in \mathcal{S}_z\} \leq \begin{cases} 2^{2N}\dfrac{\varepsilon^{2N}}{|z|^{2N}} & for\ R \leq 1 \\ 2^{2N}\dfrac{\varepsilon^{2N}}{|z|^{2N}}e^{-R^2} & for\ R > 1 \end{cases} \tag{20}$$

$$\Longrightarrow \Pr\{L_{(v_1)} \cap \mathcal{S} \neq \varnothing\} \leq \sum_z \Pr\{v_1 \in \mathcal{S}_z\}$$

$$\leq \begin{cases} C^{(N,1)}\varepsilon^{2N} & \text{for } R \leq 1 \\ \dfrac{C^{(N,1)}\varepsilon^{2N}}{R^{2N}} & \text{for } R > 1 \end{cases}. \tag{21}$$

Now, we prove the induction step from M to $M + 1$. Consider $L_{(\mathbf{v}_1,...,\mathbf{v}_{M+1})}$ as the lattice generated by the vectors $\mathbf{v}_1, ..., \mathbf{v}_M, \mathbf{v}_{M+1}$. Each point of $L_{(\mathbf{v}_1,...,\mathbf{v}_{M+1})}$ can be represented by $i\mathbf{v}_{M+1} + \mathbf{v}$ where $\mathbf{v}$ is point in the lattice, generated by $\mathbf{v}_1, ..., \mathbf{v}_M$ and i is a Gaussian integer. Therefore, the probability of existing a lattice point in $\mathcal{S}$ is equal to the probability that there is least one point of $L_{(\mathbf{v}_1,...,v_M)}$ in one of the spheres $\{\mathcal{S}_z^{(M)}\}$, where $\mathcal{S}_z^{(M)}$ is the sphere with center $\mathbf{r} - z\mathbf{v}_{M+1}$ and radius ε and z is a nonzero Gaussian integer. If $|\mathbf{v}_{M+1}| = x$,

$$\Pr\{L_{(\mathbf{v}_1,...,\mathbf{v}_M)} \cap \mathcal{S}_i^{(M)} \neq \varnothing\}$$

$$\leq \begin{cases} C^{(N,M)}\dfrac{\varepsilon^{2N}}{|i|^{2N}} & \text{for } R_z \leq 1 \\ C^{(N,M)}\dfrac{\varepsilon^{2N}}{R_z^{2N-2M+2}} & \text{for } R_z > 1 \end{cases} \tag{22}$$

$$\Longrightarrow \Pr\{L_{(\mathbf{v}_1,...,\mathbf{v}_M,\mathbf{v}_{M+1})} \cap \mathcal{S} \neq \varnothing\}$$

$$\leq \sum_z \Pr\{L_{(\mathbf{v}_1,...,\mathbf{v}_M)} \cap \mathcal{S}_z^{(M)} \neq \varnothing\}$$

$$\leq \begin{cases} \dfrac{1}{x^2}c'\varepsilon^{2N} & \text{for } R \leq 1 \\ \dfrac{1}{x^2}\dfrac{c'\varepsilon^{2N}}{R^{2N-2(M+1)+2}} & \text{for } R > 1 \end{cases} \tag{23}$$

where c' is a constant. Now, by obtaining the average over x:

$$\Longrightarrow \Pr\{L_{(\mathbf{v}_1,...,\mathbf{v}_M,\mathbf{v}_{M+1})} \cap \mathcal{S} \neq \varnothing\}$$

$$\leq \begin{cases} C^(N, M+1)\varepsilon^{2N} & \text{for } R \leq 1 \\ \dfrac{C^{(N,M+1)}\varepsilon^{2N}}{R^{2N-2(M+1)+2}} & \text{for } R > 1 \end{cases}. \tag{24}$$

Theorem 2: For a MIMO broadcast system with M transmit antennas and M single-antenna receivers and fixed rates $R_1, ..., R_M$, using the lattice-basis-reduction method,

$$\lim_{\rho \to \infty} \frac{-\log P_e}{\log \rho} = M. \tag{25}$$

Proof: Consider $\mathbf{B} = [\mathbf{b}_1 ... \mathbf{b}_M]$ as the LLL-reduced basis for the lattice, generated by $\mathbf{H}^{-1}$. Each transmitted vector $\mathbf{s}$ is inside the paralletope, 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 wtitten as

$$\mathbf{s} = t_1\mathbf{b}_1 + ... + t_M\mathbf{b}_M, \quad \frac{-r_i}{2} \leq t_i \leq \frac{r_i}{2} \tag{26}$$

For each of the transmitted vectors, the energy is

$$P = \|\mathbf{s}\|^2 = \|t_1\mathbf{b}_1 + ... + t_M\mathbf{b}_M\|^2 \tag{27}$$

$$\Longrightarrow P \leq \frac{1}{4}r_1^2\|\mathbf{b}_1\|^2 + ... + \frac{1}{4}r_M^2\|\mathbf{b}_M\|^2 \tag{28}$$

Thus, the average transmitted energy is

$$P_{av} \leq c_1(\|\mathbf{b}_1\|^2 + ... + \|\mathbf{b}_M\|^2) \leq$$
$$c_1 M.(\max\{\|\mathbf{b}_1\|^2, ..., \|\mathbf{b}_M\|^2\}) \tag{29}$$

where $c_1 = \frac{1}{4}\max\{r_1^2, ..., r_M^2\}$. The received signals (without the effect of noise) are points from the $\mathbb{Z}^{2M}$ lattice. If we consider the normalized system, $d^2 = \frac{1}{P_{av}} \geq \frac{1}{c_1(\|\mathbf{b}_1\|^2 + ... + \|\mathbf{b}_M\|^2)}$ is the squared distance between the received signal points and $\frac{M}{\rho}$ is the energy of the noise at the receiver.

Now, for any positive number γ,

$$\Pr\{d^2 \leq \frac{\gamma M}{\rho}\} \tag{30}$$

$$\leq \Pr\{\frac{1}{c_1 M \max\{\|\mathbf{b}_1\|^2, ..., \|\mathbf{b}_M\|^2\}} \leq \frac{\gamma M}{\rho}\} \tag{31}$$

Using lemma 2,

$$\max\{\|\mathbf{b}_1\|, ..., \|\mathbf{b}_M\|\} \leq \frac{\alpha_M}{d_{\mathbf{H}^*}} \tag{32}$$

$$\Longrightarrow \Pr\{d^2 \leq \frac{aM}{\rho}\} \leq \Pr\{\frac{d_{\mathbf{H}^*}^2}{c_1 \alpha_M M} \leq \frac{\gamma M}{\rho}\} \tag{33}$$

Therefore, according to lemma 3,

$$\Pr\{d^2 \leq \frac{aM}{\rho}\} = \Pr\{d_{\mathbf{H}^*}^2 \leq \frac{\gamma c_1 \alpha_M M^2}{\rho}\} \tag{34}$$

$$\leq \frac{c_2 \gamma^M}{\rho^M} \tag{35}$$

where c_1, c_2 are constant numbers and $d_{\mathbf{H}^*}$ is the minimum distance of the lattice generated by $\mathbf{H}^*$. If the magnitude of the noise component in each 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, $1 \leq i \leq M$. Therefore,

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

$$\leq M\Bigg(\Pr\{d^2 \leq \frac{2^2 M}{\rho}\} +$$

$$\Pr\{\frac{2^2 M}{\rho} \leq d^2 \leq \frac{4^2 M}{\rho}\}.\Pr\left\{|w_1|^2 \geq \frac{2^2 M}{\rho}\right\}$$

$$+\Pr\{\frac{4^2 M}{\rho} \leq d^2 \leq \frac{8^2 M}{\rho}\}.\Pr\left\{|w_1|^2 \geq \frac{4^2 M}{\rho}\right\} + ...\Bigg) \tag{36}$$

The components of the noise vector have complex Gaussian distribution with unit variance. Therefore,

$$\Pr\left\{|w_1|^2 \geq \frac{\gamma M}{\rho}\right\} \leq e^{-\gamma} \text{ for } \gamma \geq 1 \tag{37}$$

$$\Longrightarrow P_e \leq M\left(\Pr\left\{|w_1|^2 \geq \frac{1}{4}d^2\right\}\right) \tag{38}$$

$$\leq M\left(\frac{c_2}{\rho^M} + \frac{4^M c_2}{\rho^M}e^{-4} + \frac{16^M c_2}{\rho^M}e^{-16} + ...\right) \tag{39}$$

$$= M\left(\frac{c_2}{\rho^M}(1 + 4^M e^{-4} + 16^M e^{-16} + ...)\right) \tag{40}$$

$$\leq \frac{c_M}{\rho^M} \tag{41}$$

where c_M is a constant number which only depends on *M*. Thus,

$$\lim_{\rho\to\infty} \frac{-\log P_e}{\log \rho} \geq M. \tag{42}$$

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

$$\lim_{\rho\to\infty} \frac{-\log P_e}{\log \rho} = M. \tag{43}$$

■

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

IV. Relation with Lattice Decoding for MIMO systems

Similar to the previous section, by considering the outage probability, we can show that the maximum achievable diversity for a MIMO multiaccess system with fixed rates is equal to the number of receive antennas. When we have a finite constellation, for each pair of constellation points, the pair-wise error probability can be bounded by Chernoff bound (similar to [13]) and by using the union bound, we can show that the exact ML decoding achieve the diversity order of M, the number of antennas. However, when we use lattice decoding for a finite constellation and consider the out-of-region decoded lattice points as errors, achieving the maximum diversity by lattice decoding is not trivial anymore. However, by using Theorem 2, we can show that the imperfect lattice decoding still achieve the maximum diversity.

Lemma 4: Consider $\mathbf{B} = [\mathbf{b}_1 ... \mathbf{b}_M]$ as a reduced basis (LLL) [11] for the lattice generated by $\mathbf{H}^{*-1}$, $\mathbf{B}^{*-1} = [\mathbf{a}_1 ... \mathbf{a}_M]$, and δ as the orthogonality defect of the reduction. Then, if the magnitude of the noise vector is less than $\frac{\|\mathbf{a}_{min}\|}{2\sqrt{M\delta}}$, the LLL-aided decoding method correctly decodes the transmitted signal.

Proof: When we use the LLL-aided decoding method, we find the nearest integer point to $\mathbf{By}$. We should show that this point is the same as the transmitted vector; or in the other words, all the elements of $\mathbf{Bw}$ are in the interval $(-\frac{1}{2}, \frac{1}{2})$. To prove this, we show that $\|\mathbf{Bw}\| \leq \frac{1}{2}$:

$$\|\mathbf{Bw}\| \leq \sqrt{M}\|\mathbf{b}_{max}\|.\|\mathbf{w}\|$$

Now, according to lemma 1,

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

Therefore,

$$\|\mathbf{Bw}\| \leq \frac{\sqrt{M\delta}.\|\mathbf{w}\|}{\|\mathbf{a}_{min}\|}$$

$$\leq \frac{\sqrt{M}.\frac{1}{2\sqrt{M}}\sqrt{\delta}\|\mathbf{a}_{min}\|}{\sqrt{\delta}.\|\mathbf{a}_{min}\|}$$

$$\Longrightarrow \|\mathbf{Bw}\| \leq \frac{1}{2}.$$

Lemma 5: Consider $\mathbf{B} = [\mathbf{b}_1 ... \mathbf{b}_M]$ as a reduced basis (LLL) [11] for the lattice generated by $\mathbf{H}$ and $d_{\mathbf{H}}$ as the minimum distance of the lattice generated by $\mathbf{H}$. Then, there is a constant number c_M (independent of $\mathbf{H}$) such that the LLL-aided decoding method correctly decodes the transmitted signal, if the magnitude of the noise vector is less than $c_M d_{\mathbf{H}}$.

Proof: For an LLL reduction,

$$\sqrt{\delta} \leq 2^{M(M-1)/4}.$$

Therefore, if we consider $c_M = \frac{2^{-1-M(M-1)/4}}{\sqrt{M}}$,

$$\|\mathbf{w}\| \leq c_M d_{\mathbf{H}}$$

$$\Longrightarrow \|\mathbf{w}\| \leq \frac{1}{2\sqrt{M\delta}} d_{\mathbf{H}}$$

The basis $\mathbf{B}$ can be written as $\mathbf{B} = (\mathbf{H})^{*^{-1}}\mathbf{U}$ for some unimodular matrix $\mathbf{U}$:

$$(\mathbf{B}^{-1})^* = ((\mathbf{H}^{-1^*}\mathbf{U})^{-1})^* = (\mathbf{U}^{-1}\mathbf{H}^*)^* = \mathbf{H}(\mathbf{U}^{-1})^* \quad (44)$$

Thus, $(\mathbf{B}^{-1})^* = [\mathbf{a}_1, ..., \mathbf{a}_M]$ is another basis for the lattice generated by $\mathbf{H}$. Therefore, the vectors $\mathbf{a}_1, ..., \mathbf{a}_M$ are vectors from the lattice generated by $\mathbf{H}$, and therefore, the length of each of them is at least $d_{\mathbf{H}}$. Therefore,

$$\|\mathbf{w}\| \leq \frac{1}{2\sqrt{M\delta}}\|\mathbf{a}_{min}\|.$$

Thus, according to lemma 4, LLL-aided decoding method correctly decodes the transmitted signal.

Theorem 3: For a MIMO multi-access system (or a point-to-point MIMO system with the V-BLAST transmission method) with M transmit antennas and M single-antenna receivers and fixed rates $R_1, ..., R_M$, when we use the LLL lattice-basis-reduction method [14],

$$\lim_{\rho\to\infty} \frac{-\log P_e}{\log \rho} = M.$$

Proof: When $\|\mathbf{w}\| \leq c_M d_{\mathbf{H}}$, we have no decoding error. Thus, similar to the proof of theorem 2,

$$P_e \leq \Pr\{c_M^2 d_{\mathbf{H}}^2 \leq \frac{M}{\rho}\}$$

$$+ \Pr\{c_M^2 d_{\mathbf{H}}^2 \leq \frac{2^2 M}{\rho}\}.\Pr\left\{\|\mathbf{w}\|^2 \geq \frac{M}{\rho}\right\}$$

$$+ \Pr\{c_M^2 d_{\mathbf{H}}^2 \leq \frac{4^2 M}{\rho}\}.\Pr\left\{\|\mathbf{w}\|^2 \geq \frac{2^2 M}{\rho}\right\} + ...$$

$$\Longrightarrow P_e \leq \frac{c'}{\rho^M}$$

where c' is a constant. Therefore,

$$\lim_{\rho\to\infty} \frac{-\log P_e}{\log \rho} \geq M.$$

V. Conclusions

We have shown that LLL reduction, which is a polynomial-time algorithm, achieves the maximum precoding diversity in fixed-rate MIMO broadcast systems. Also, we have shown that by using LLL reduction we can achieve the maximum receive diversity in MIMO decoding. By using LLL reduction and the Babai approximation, the complexity of the MIMO decoding is equal to the complexity of the zero-forcing method with an additional polynomial time preprocessing.

References

[1] 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.

[2] O. Damen, A. Chkeif, and J.-C. Belfiore, "Lattice code decoder for space-time codes," *IEEE Communications Letters*, pp. 161–163, May 2000.

[3] 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.

[4] 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.

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

[6] 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.

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

[8] 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," *Submitted to IEEE Trans. Comm.*, 2003.

[9] 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.

[10] M. Taherzadeh, A. Mobasher, and A. K. Khandani, "Communication over mimo broadcast channels using lattice-basis reduction," in *Proceedings of 42nd Allerton Conference*, Sep. 2004.

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

[12] M. Taherzadeh, A. Mobasher, and A. K. Khandani, "Communication over MIMO broadcast channels using lattice-basis reduction." Technical Report UW-E&CE#2004-8.

[13] 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.

[14] M. Taherzadeh, A. Mobasher, and A. K. Khandani, "LLL reduction achieves receive diversity in MIMO decoding." Technical Report UW-E&CE#2005-3.