On The Limitations of The Naive Lattice Decoding

Mahmoud Taherzadeh 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, khandani}@cst.uwaterloo.ca, Tel: 519-8848552, Fax: 519-8884338

[1] ***Abstract*— In this paper, the inherent drawbacks of the naive lattice decoding for MIMO fading systems is investigated. We show that using the naive lattice decoding for MIMO systems has considerable deficiencies in terms of the rate-diversity trade-off. Unlike the case of maximum-likelihood decoding, in this case, even the perfect lattice space-time codes which have the non-vanishing determinant property can not achieve the optimal rate-diversity trade-off. Indeed, we show that in the case of naive lattice decoding, all the codes based on full-rate lattices have the same rate-diversity trade-off as V-BLAST. Also, we drive a lower bound on the symbol error probability of the naive lattice decoding for the fixed-rate MIMO systems (with equal numbers of receive and transmit antennas). This bound shows that asymptotically, the naive lattice decoding has an unbounded loss in terms of the required SNR, compared to the maximum likelihood decoding.**

I. Introduction

In recent years, there has been extensive research on designing practical encoding/decoding schemes to approach theoretical limits of MIMO fading systems. The optimal rate-diversity trade-off [1] is considered as an important theoretical benchmark for practical systems. For the encoding part, recently, several lattice codes are introduced which have the non-vanishing determinant property and achieve the optimal trade-off, conditioned on using the exact maximum-likelihood decoding [2] [3] [4]. The lattice structure of these codes facilitates the encoding. For the decoding part, various lattice decoders, including the sphere decoder and the lattice-reduction-aided decoding are presented in the literature [5] [6]. To achieve the exact maximum likelihood performance, we need to find the closest point of the lattice inside the constellation region, which can be much more complex than finding the closest point in an infinite lattice. To avoid this complexity, one can perform the traditional lattice decoding (for the infinite lattice) and then, discard the out-of-region points. This approach is called Naive Lattice Decoding (NLD).

In [7], the authors have shown that this sub-optimum decoding (and even its lattice-reduction-aided approximation) still achieve the maximum receive diversity in the fixed-rate MIMO systems. Achieving the optimal receive diversity by a low decoding complexity makes lattice-reduction-aided decoding (using the LLL reduction) an attractive choice for different applications. Nonetheless, this work shows that for the case of rate-diversity trade-off, the optimality can not be provided by the naive-lattice decoding or its approximations.

[1]Financial support provided by Nortel and the corresponding matching funds by the Natural Sciences and Engineering Research Council of Canada (NSERC), and Ontario Centres of Excellence (OCE) are gratefully acknowledged.

In [8], using a probabilistic method, a lower bound on the best achievable trade-off, using the naive lattice decoding, is presented. In this paper, we present an upper bound for the performance of the naive lattice decoding for codes based on full-rate lattices. We show that NLD can not achieve the optimum rate-diversity trade-off. Also, for the special case of equal number of transmit and receive antennas, we show that even the best full-rate lattice codes (including perfect space-time codes such as the golden code [3]) can not perform better than the simple V-BLAST (if we use the naive lattice decoding at the receiver).

In section IV, we complement the result of [7] by showing that for the special case of equal number of transmit and receive antennas, although the naive lattice decoding (and its LLL-aided approximation) still achieve the maximum receive diversity, their gap with the optimal ML decoding grows unboundedly with SNR.

II. System Model

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

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{w}. \quad (1)$$

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 Gaussian. 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. $\mathrm{E}\|\mathbf{w}\|^2 = N\sigma^2$. The signal to noise ratio (SNR) is defined as $\rho = \frac{M}{\sigma^2}$.

We send the transmitted vector $\mathbf{x}$ with independent entries from $\mathbb{Z}[i]$ and at the receiver, we find $\tilde{\mathbf{x}}$ as $\mathbf{H}^{-1}\tilde{\mathbf{y}}$ where $\tilde{\mathbf{y}}$ is the closest lattice point to $\mathbf{y}$.

III. Rate-diversity trade-off for the naive lattice decoding

To drive the upper bound on the rate-diversity trade-off of naive lattice decoding (NLD), we first present a lower bound on the probability that the received lattice (the lattice code, after passing through the fading channel) has a short vector.

Lemma 1 *Assume that the entries of the $N \times M$ 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 $\mathbf{H}_T\mathbf{L}$, where $\mathbf{L}$ is the full-rank $MT \times MT$ generator of a complex lattice and $\mathbf{H}_T$ is the $NT \times MT$ block diagonal matrix constructed from $\mathbf{H}$. Then, there is a constant C such that,*

$$Prob\{d_{\mathbf{H}} \leq \varepsilon\} \geq$$

$$C(\det\Lambda)^{-\frac{(N-M+1)}{T}}\varepsilon^{2M(N-M+1)}$$

where $\det\Lambda \triangleq \det(\mathbf{L}^*\mathbf{L})^{\frac{1}{2}}$ *is the volume of the fundamental region of* $\mathbf{L}$.

Sketch of the proof: The probability that $\mathbf{H}$ has a singular value less than $\frac{\varepsilon^M.(\det\Lambda)^{-\frac{1}{2T}}}{2^M(MN)^{(M-1)}}$ can be lower bounded by

$$\Pr\left\{\sigma_{min} < \frac{\varepsilon^M.(\det\Lambda)^{\frac{-1}{2T}}}{2^M\,(MN)^{(M-1)}}\right\}$$

$$\geq c_1\left(\frac{\varepsilon^M.(\det\Lambda)^{\frac{-1}{2T}}}{2^M\,(MN)^{(M-1)}}\right)^{2(N-M+1)}$$

where c_1 is a constant[2].

Consider $\mathbf{v}_{min}$ as the singular vector of $\mathbf{H}$, corresponding to σ_{min}. For each MT-dimensional complex vector $\mathbf{v} = [a_1\mathbf{v}_{min}^{\mathsf{T}}\ \ a_2\mathbf{v}_{min}^{\mathsf{T}}...\ a_T\mathbf{v}_{min}^{\mathsf{T}}]^{\mathsf{T}}$,

$$\|\mathbf{H}_T\mathbf{v}\| \leq \frac{\varepsilon^M.(\det\Lambda)^{\frac{-1}{2T}}}{2^M\,(MN)^{(M-1)}}\|\mathbf{v}\|$$

Consider $\mathcal{A}$ as a $2MT$-dimensional orthotope whose $2T$ edges are parallel to the subspace spanned by these vectors (with length $\frac{2(MN)^{(M-1)}(\det\Lambda)^{\frac{1}{2T}}}{\varepsilon^M}$) and the other $2T(M-1)$ edges are orthogonal to that subspace and have length 2. There are more than $\varepsilon^{-2MT}\,(MN)^{2T(M-1)}$ points of lattice $\mathbf{L}$ inside this orthotope.

Now, if σ_{max} (the largest singular value of $\mathbf{H}$) is less than MN, then $\mathbf{H}_T\mathcal{A}$ is inside an $2MT$-dimensional orthotope (in the subspace spanned by $\mathbf{H}_T$) whose $2T$ edges have length 2^{1-M} and the length of the other $2T(M-1)$ edges are at most $2MN$. This orthotope can be covered by $\varepsilon^{-2MT}\,(MN)^{2T(M-1)}$ hypercubes of size ε. By using Dirichlet's box principle, in one of these hypercubes there are at least 2 points of the new lattice, hence $d_{\mathbf{H}} \leq \varepsilon$.

It is easy to show that $\Pr\{\sigma_{max} < MN\} \geq \frac{1}{2}$. Therefore,

$$\Pr\{d_{\mathbf{H}} \leq \varepsilon\} \geq$$

$$\Pr\left\{\sigma_{min} < \frac{\varepsilon^M.(\det\Lambda)^{\frac{-1}{2T}}}{2^M\,(MN)^{(M-1)}}\right\}\cdot\Pr\{\sigma_{max} < MN\}$$

$$\geq c_2\left(\frac{\varepsilon^M.(\det\Lambda)^{\frac{-1}{2T}}}{2^M\,(MN)^{(M-1)}}\right)^{2(N-M+1)}$$

$$\geq C(\det\Lambda)^{\frac{-(N-M+1)}{T}}\varepsilon^{2M(N-M+1)}.$$

[2]Throughout this paper, c_1, c_2, ... are constants.

■

Theorem 2 *Consider a MIMO fading channel with M transmit and N receive antennas ($M \leq N$) with codebooks from a MT-dimensional lattice $\mathbf{L}$, which are sent over T channel uses. For the naive lattice decoding, the rate-diversity trade-off of the system is*

$$d_{NLD}(r) \leq M(N-M+1) - r\,(N-M+1)\,,$$

$$\text{for } 0 \leq r \leq M.$$

Sketch of the proof: Consider the code of rate r, constructed from the lattice. According to lemma 1,

$$\Pr\{d_{\mathbf{H}} \leq \varepsilon\} \geq$$

$$C(\det\Lambda)^{\frac{-(N-M+1)}{T}}\varepsilon^{2M(N-M+1)}$$

$$\geq C(SNR)^{rT\cdot\frac{(N-M+1)}{T}}\varepsilon^{2M(N-M+1)}.$$

Now, having $SNR = \frac{M}{\sigma^2}$, we bound the symbol error probability P_e,

$$P_e \geq \Pr\left\{d_{\mathbf{H}} \leq \frac{1}{\sqrt{SNR}}\right\}.Q\left(\frac{1}{\sqrt{M}}\right)$$

$$\geq c_3\frac{(SNR)^{r(N-M+1)}}{SNR^{M(N-M+1)}}$$

$$\Longrightarrow d_{NLD}(r) = \lim_{SNR\to\infty}\frac{-\log P_e}{\log SNR}$$

$$\leq M(N-M+1) - r\,(N-M+1)$$

■

Corollary 1 *In a MIMO fading channel with $M = N$ transmit and receive antennas, if we use the naive lattice decoding, the rate-diversity trade-off for full-rate lattice code can not be better than that of V-BLAST.*

Proof: When $M = N$, according to Theorem 1,

$$d_{NLD}(r) \leq M - r$$

On the other hand, for the V-BLAST system [1] with lattice decoding,

$$d(r) = M - r$$

■

It is interesting to compare this result with the results on lattice space-time codes which have non-vanishing determinants. Although by ML decoding, these codes (such as the 2×2 golden code) achieve the optimal rate-diversity trade-off, when we replace ML decoding with the naive lattice decoding (and its approximations), their performance is not much better than the simple V-BLAST scheme (specially when the number of transmit and receive antennas are the same)

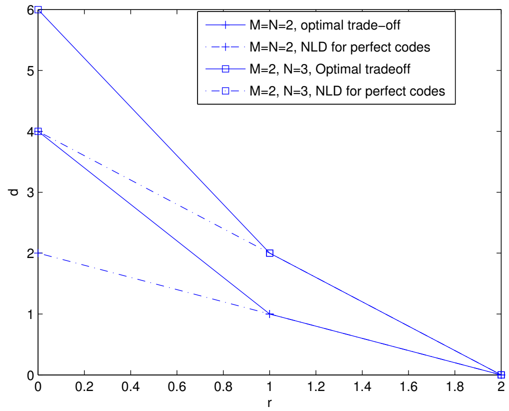

Fig. 1. Comparison between the optimal rate-diversity tradeoff and the upper bound on the rate-diversity trade-off of full-rate lattice codes (including perfect space-time codes such as the golden code)

To better understand the difference between the naive lattice decoding and the ML decoding, we note that for small constellations, when the generator of the received lattice has a small singular value, the minimum distance of the lattice can be much smaller than the minimum distance of the constellation. Figure 2 shows this situation for a small 4-point constellation from a 2-dimensional lattice.

We should note that this upper bound is for full-rate lattices. Lattices which lower rates, can provide higher diversity, but their rate is limited by the dimension of the lattice. For example, The Alamouti code, based on QAM constellations, can achieve the full diversity for fixed rates ($r = 0$), but its rate is limited by one. For the general case (including non-full-rate lattices), we have these conjectures:

Conjecture 1 *Consider a MIMO fading channel with M transmit and N receive antennas ($M \leq N$) with codebooks from a KT-dimensional lattice L ($1 \leq K \leq M$), sent over T channel uses. For the naive lattice decoding, the rate-diversity trade-off of the system is upper bounded by*

$$d_{NLD-K}(r) \leq M(N-K+1) - \left(\frac{K(N-K+1)}{M}r\right), \quad \text{for } 0 \leq r \leq K.$$

Conjecture 2 *For a MIMO fading channel with M transmit and N receive antennas ($M \leq N$), if we restrict ourself to lattice coding and the naive lattice decoding, the best achievable rate-multiplexing trade-off is*

$$d^*_{NLD}(r) = \max_K \left\{ M(N-K+1) - \left(\frac{K(N-K+1)}{M}r\right)\right\}, \quad \text{for } 0 \leq r \leq M.$$

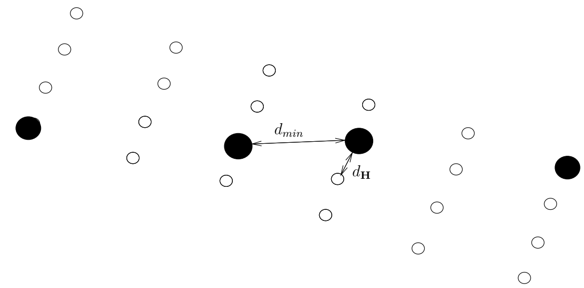

Fig. 2. Minimum distance of the lattice, compared to the minimum distance of the code

IV. Asymptotic performance of the naive lattice decoding for $M = N$

In [7], it is shown that for $N \geq M$, the naive lattice decoding achieves the receive diversity in V-BLAST systems (indeed, even its simple latice-reduction-aided approximation still achieves the optimum receive diversity of order N). However, there is a difference between two cases of $M < N$ and $M = N$. While for $M < N$, compared to ML decoding, the performance loss of the naive lattice decoding is bounded in terms of SNR, this is not valid for the case of $M = N$. This dichotomy is related to the bounds on the probability of having a short lattice vector in a lattice generated by a random Gaussian $N \times M$ matrix.

In [9], the following upper bound on the probability of having a short lattice vector is given

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_H as the minimum distance of the lattice generated by $\mathbf{H}$. Then, there is a constant C such that [9],*

$$Prob\{d_{\mathbf{H}} \leq \varepsilon\} \geq C\varepsilon^{2M} \ln\left(\frac{1}{\varepsilon}\right)^{N-1}.$$

The term $\ln\left(\frac{1}{\varepsilon}\right)$ suggests an unboundedly increasing gap between the performance of ML decoding and the naive lattice decoding (though both of them have the same slope N).

In this section, we present a lower bound for the error probability of the naive lattice decoding and show that this unboundedly increasing gap does exist.

Lemma 4 *For the lattice generated by a $M \times M$ random complex Gaussian matrix $\mathbf{H}$,*

$$Prob\{d_{\mathbf{H}} \geq \varepsilon\} \geq C'\varepsilon^{2M} \ln\left(\frac{1}{\varepsilon}\right).$$

Sketch of the proof: 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

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

Therefore, we have this bound:

$$c_4 \frac{\varepsilon^{2M}}{\left(|z_1|^2 + ... + |z_M|^2\right)^M} \geq \Pr\left\{\|\mathbf{v}_{(z_1,...,z_M)}\| \leq \varepsilon\right\}$$

$$\geq c_5 \frac{\varepsilon^{2M}}{\left(|z_1|^2 + ... + |z_M|^2\right)^M}.$$

Now, we find an upper bound on the probability of this event for two different complex integer vectors $\mathbf{z}'$ and $\mathbf{z}''$ (which are not multiplier of eachother), at the same time. We can write $\mathbf{z}'$ as $a\mathbf{z}'' + \mathbf{z}'''$ where a is a complex number and $\mathbf{z}'''$ is orthogonal to $\mathbf{z}''$. Assuming $\|\mathbf{z}'\| < \varepsilon^{-\frac{1}{2M}}$ and $\|\mathbf{z}''\| < \varepsilon^{-\frac{1}{2M}}$, we can show that $\|\mathbf{z}'''\| > \varepsilon^{\frac{1}{2M}}$ and $a < \varepsilon^{-\frac{1}{2M}}$. Therefore, after straightforward steps,

$$\Pr\left\{\|\mathbf{v}_{\mathbf{z}'}\| \leq \varepsilon, \|\mathbf{v}_{\mathbf{z}''}\| \leq \varepsilon\right\}$$

$$\leq \Pr\left\{\|\mathbf{v}_{\mathbf{z}''}\| \leq \varepsilon\right\} \cdot \Pr\left\{\|\mathbf{v}_{\mathbf{z}'''}\| \leq \varepsilon^{1-\frac{1}{2M}}\right\}$$

$$\leq c_6 \varepsilon^{4M-2}$$

Now, we use the Bonferroni inequality [10],

$$\Pr\left\{d_{\mathbf{H}} \leq \varepsilon\right\} \geq \Pr\left\{\|\mathbf{v}_{\mathbf{z}}\| \leq \varepsilon, \|\mathbf{z}\| < \varepsilon^{-\frac{1}{2M}}\right\}$$

$$\geq \sum_{\mathbf{z} \neq 0, \|\mathbf{z}\| < \varepsilon^{-\frac{1}{2M}}} \Pr\left\{\|\mathbf{v}_{\mathbf{z}}\| \leq \varepsilon\right\}$$

$$- \sum_{0 < \|\mathbf{z}'\|, \|\mathbf{z}''\| < \varepsilon^{-\frac{1}{2M}}} \Pr\left\{\|\mathbf{v}_{\mathbf{z}'}\| \leq \varepsilon, \|\mathbf{v}_{\mathbf{z}''}\| \leq \varepsilon\right\}$$

$$\geq c_7 \varepsilon^{2M} \ln\left(\frac{1}{\varepsilon}\right) - c_8 \varepsilon^{-2M \times \frac{1}{2M}} . \varepsilon^{4M-2}$$

$$\geq c_7 \varepsilon^{2M} \ln\left(\frac{1}{\varepsilon}\right) - c_8 \varepsilon^{4M-3}$$

$$\geq C' \varepsilon^{2M} \ln\left(\frac{1}{\varepsilon}\right)$$

■

Theorem 5 *Consider a MIMO fading channel with M transmit and M receive antennas and a V-BLAST transmission system. The naive lattice-decoding has an asymptotically unbounded loss, campared to the exact ML decoding.*

Proof: For ML decoding, by using the Chernoff bound for the pairwise error probability and then applying the union bound for the finite constellation, we have

$$P_{error-ML} \leq c_9 (SNR)^{-M}$$

For naive lattice decoding,

$$P_{error-NLD} \geq \Pr\left\{d_{\mathbf{H}} \leq \frac{1}{\sqrt{SNR}}\right\} . Q\left(\frac{1}{\sqrt{M}}\right)$$

$$\geq c_{10} (SNR)^{-M} \ln(SNR)$$

Therefore, although both of them asymptotically have the same slope and achieve the optimal receive diversity of order M, for large SNRs, the gap between their performances is unbounded (with a logarithmic growth, or in other words, $\log \log SNR$ in dB scale). ■

V. Conclusions

In this paper, the inherent limitations of the performance of the naive lattice decoding is investigated. The naive lattice decoding and various implementions of it (such as the sphere decoding) and its simple approximated versions (such as the LLL-aided decoding) are very attractive for the practical MIMO systems. Nontheless, to achieve theoretical benchmarks (such as the rate-diversity trade-off), these techniques can not be always sufficient. For the rate-diversity trade-off, although different elegant lattice codes have been introduced which achieve the optimal trade-off, the problem of achieving it by a practical decoding scheme is still open.

References

[1] L. Zheng and D. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," *IEEE Trans. Info. Theory*, vol. 49, pp. 1073–1096, May 2003.

[2] P. Elia, K. R. Kumar, S. A. Pawar, and P. V. K. H.-F. Lu, "Explicit spacetime codes achieving the diversitymultiplexing gain tradeoff," *IEEE Trans. Info. Theory*, vol. 52, pp. 3869–3884, Sep. 2006.

[3] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect spacetime block codes," *IEEE Trans. Info. Theory*, vol. 52, pp. 3885–3902, Sep. 2006.

[4] L. Hsiao-Feng and P. V. Kumar, "A unified construction of space-time codes with optimal rate-diversity tradeoff," *IEEE Trans. Info. Theory*, vol. 51, pp. 1709–1730, May 2005.

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

[6] 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.

[7] M. Taherzadeh, A. Mobasher, and A. K. Khandani, "LLL reduction achieves receive diversity in MIMO decoding," *Submitted to IEEE Trans. Info. Theory*, 2006.

[8] H. E. Gamal, G. Caire, and M. O. Damen, "Lattice coding and decoding achieve the optimal diversity-multiplexing tradeoff of mimo channels," *IEEE Trans. Info. Theory*, vol. 50, pp. 968 – 985, June 2004.

[9] M. Taherzadeh, A. Mobasher, and A. K. Khandani, "Communication over mimo broadcast channels using lattice-basis reduction," *Submitted to IEEE Trans. Info. Theory*, 2006.

[10] J. Galambos and I. Simonelli, *Bonferroni-type inequalities with applications*. Springer-Verlag, 1996.