

An error event sensitive trade-off between rate and coding gain in MIMO MAC

Toni Ernvall, Jyrki Lahtonen *Member, IEEE*, Hsiao-feng (Francis) Lu, *Member, IEEE* and Roope Vehkalahti, *Member, IEEE*

Abstract

This work considers space-time block coding for the Rayleigh fading multiple-input multiple-output (MIMO) multiple access channel (MAC). If we suppose that the receiver is performing joint maximum-likelihood (ML) decoding, optimizing a MIMO MAC code against a fixed error event leads to a situation where the joint codewords of the users in error can be seen as a single user MIMO code. In such a case pair-wise error probability (PEP) based determinant criterion of Tarokh et al. can be used to upper bound the error probability.

It was already proven by Lahtonen et al. that irrespective of the used codes the determinants of the differences of codewords of the overall codematrixes will decay as a function of the rates of the users.

This work will study this decay phenomenon further and derive upper bounds for the decay of determinants corresponding any error event. Lower bounds for the optimal decay are studied by constructions based on algebraic number theory and Diophantine approximation. For some error profiles the constructed codes will be proven to be optimal.

While the perspective of the paper is that of PEP, the final part of the paper proves how the achieved decay results can be turned into statements about the diversity-multiplexing gain trade-off (DMT).

I. INTRODUCTION

Assume that we are to design a system for U simultaneously transmitting synchronized users, each transmitting with n_t transmit antennas and, for simplicity so that we end up with square matrices, over Un_t channel uses. We can describe each user's signals as $n_t \times Un_t$ complex matrices. A multiuser MIMO signal is then viewed as a

The research of T. Ernvall is supported in part by the Academy of Finland grant #131745.

The research of R. Vehkalahti is funded by the Academy of Finland grant #252457.

The research of H.-f. Lu was funded in part by Taiwan National Science Council under Grants NSC 100-2221-E-009-046 -MY3 and NSC 101-2923-E-009-001-MY3.

Part of this work appeared at ITW 2010 [5] and ISIT 2012 [1]

T. Ernvall is with the Turku Center of Computer Science, Turku, Finland and with with the Department of Mathematics and Statistics, FI-20014, University of Turku, Finland (e-mail:tmernv@utu.fi).

J. Lahtonen and R. Vehkalahti are with the Department of Mathematics and Statistics, FI-20014, University of Turku, Finland (e-mails: {lahtonen, roiiive}@utu.fi).

H.-f. Lu is with the Department of Electrical Engineering, National Chiao Tung University, Hsinchu, Taiwan (e-mail:francis@mail.nctu.edu.tw).

$Un_t \times Un_t$ matrix obtained by using the signals of the individual users as blocks. So each user is occupying n_t rows in this overall transmission matrix.

We are not interested on the scenario, where single users have fixed finite codes, but of coding schemes, where each user has a family of growing codes. A natural source for such schemes is to assume that each user has a lattice and that the finite codes of individual users are carved out of these user specific lattices. We are then interested on the asymptotic behavior of error probabilities when we let the rates of each user grow.

In the Rayleigh fading multiple-input multiple-output (MIMO) multiple access channel (MAC) it is a natural idea to develop a code design criteria by splitting the whole error probability space to separate error events based on which users are in error. If we suppose that the receiver is performing joint maximum-likelihood (ML) decoding, optimizing a MIMO MAC code against a fixed error event leads to a situation where the joint codewords of the users in error can be seen as a single user MIMO code. In such a case pair-wise error probability based determinant criterion from [16] can be applied to upper bound the error probability. This approach was first taken in [17] and was developed further in [3] and [14].

The approach was also suggested for reaching the MAC DMT [2] in [3]. Unfortunately in [7] it was proved that the criteria given in [3] is too tight, at least in the case where the codes of the single users are lattice space-time codes. The *pigeon hole bound* in [7] proves that, irrespective of the code design, the determinants of the overall code matrices will decay with a polynomial speed with respect to the code-size and methods, similar to those used in [21], to prove the DMT optimality for single user MIMO codes do not work.

In this paper we will study this decay phenomenon further and will give general upper and lower bounds for the decay of determinants corresponding any error event. The achieved results are then used to draw conclusions of the DMT of the analyzed codes.

The upper bounds we derive will be functions of rates of each users and are independent of the used codes. These results will reveal a trade-off between the rate and protection against error. It is possible to design a MAC code in such a way that the codewords corresponding each error event will have maximal possible rank. If we have such a code, then in each error event the code is protected by maximal possible diversity. However, in the spirit of DMT, our bounds will reveal that when the rates of users of the corresponding error events are growing the determinants of the matrices offering the maximal diversity will decay. This interplay creates a trade-off between the coding gain and rate, which is close relative to DMT, but not the same concept.

The proofs of the upper bounds are based on using pigeon hole principle, projection mappings and properties of the determinant function. The results are purely algebraic corresponding all lattice codes with certain properties. Only in the statement of the problem we are using Rayleigh fading MIMO MAC as a motivation.

While the first part of the paper provides upper bounds for the decay of the determinants in MIMO MAC, the second part of the paper concentrates on giving code constructions where we have tried to optimize the codes from the decay point of view. In [5] it was proved that the two user single antenna code (BB-code) given in [14] has in some sense the best possible decay. In this paper we are now giving a vast generalization of this code to general MIMO MAC. The codes we will build fulfill the so called *generalized rank criterion* and do reach the pigeon hole

bound. Our method will share the basic structure with the original generalization of BB-code given in [13].

The single user codes we are using are based on the *multi-block* codes from division algebras [8] and [9]. This approach has been taken in several recent papers on MIMO MAC. However, in these papers the full rank criterion has been achieved by using either transcendental elements [13] (with exception of $n_t = 2$ case, which is dealt with algebraic elements having low degree) or algebraic elements with high degree [6]. Both of these methods make it extremely difficult to measure the decay of the codes and can lead to bad decay. For a survey of these recent results, we refer the reader to thesis of Maya Badr [15].

Instead of the usual algebraic independence strategy we will use *valuation theory* to achieve the full rank condition. This technical tool allows us to use algebraic elements with low degree. By applying Galois theoretic method of Lu et al. [7] and methods from Diophantine approximation, originally introduced by Lahtonen et al. in [5], we will prove that our codes achieve good decay and in particular reach the pigeon hole bound.

In Section IV we will show how the lower bounds for the decay of our codes can be translated to lower bounds for the DMT. This analysis will reveal that in many cases the constructed codes do achieve the optimal diversity-multiplexing gain trade-off for low multiplexing gains.

A. Multi-user codes, error events and corresponding decay functions

In this section we will show how the decay functions appear as a natural generalization of the minimum determinant criterion used in the design of single user MIMO space-time block codes.

Let us suppose that we have U users, each having n_t antennas and that the receiver has n_r antennas and complete channels state information. We also suppose that the fading for each user stays stable for k time units, where $k \geq Un_t$. Let us refer to the channel matrix of the i th user with $H_i \in M_{n_r \times n_t}(\mathbb{C})$ and let us suppose that each of these have i.i.d complex Gaussian random variables with zero mean and unit variance as coefficients. In this scenario the base station receives

$$Y = \sum_{i=1}^U H_i X_i + W,$$

where, $X_i \in M_{n_t \times k}(\mathbb{C})$, is the transmitted codeword from the i th user, and $W \in M_{n_r \times k}(\mathbb{C})$ presents the noise having i.i.d complex Gaussian random variables as coefficients. In this scenario multiuser MIMO signal is a $Un_t \times k$ matrix where the rows $(j-1)n_t + 1, (j-1)n_t + 2, \dots, (j-1)n_t + n_t$ represent j th user's signal ($j = 1, \dots, U$).

In order to keep the analysis in the paper streamlined and clean, we will assume that the single user space-time codes are always of the following type.

Definition 1.1: A matrix lattice $\mathbf{L} \subseteq M_{n_t \times k}(\mathbb{C})$ has the form

$$\mathbf{L} = \mathbb{Z}B_1 \oplus \mathbb{Z}B_2 \oplus \dots \oplus \mathbb{Z}B_r,$$

where the matrices B_1, \dots, B_r are linearly independent over \mathbb{R} , *i.e.*, form a lattice basis, and r is called the *rank* or the *dimension* of the lattice.

Let us suppose that x_i are matrices in $M_{n_t \times k}(\mathbb{C})$. Throughout the paper we will use the notation

$$\mathbb{R}(x_1, \dots, x_j) = \mathbb{R}x_1 + \dots + \mathbb{R}x_j.$$

If \mathbf{L} is a lattice we also write

$$\mathbb{R}(\mathbf{L}) = \mathbb{R}B_1 \oplus \mathbb{R}B_2 \oplus \cdots \oplus \mathbb{R}B_r.$$

The finite single user codes used in the actual transmission are of form

$$\mathbf{L}(M) = \left\{ \sum_{i=1}^r b_i B_i \mid b_i \in \mathbb{Z}, -M \leq b_i \leq M \right\},$$

where M is a given positive number.

In the single user MIMO transmission the usual pairwise error probability based design criteria [16], leads to maximizing

$$\min_{X, Y \in \mathbf{L}(M), X \neq Y} \det((X - Y)(X - Y)^\dagger).$$

As $X - Y \in \mathbf{L}(2M)$, we can just as well try to maximize

$$\min_{X \in \mathbf{L}(M), X \neq 0} \det(XX^\dagger). \quad (1)$$

The first step is of course that this value should always be non-zero. This is the *rank criterion*. Maximizing the value is called the *minimum determinant criterion*. Let us now show how this criterion can be generalized to MIMO MAC context.

In the rest of the paper we suppose that each user applies a lattice space-time code $\mathbf{L}_j \subseteq M_{n_t \times k}(\mathbb{C})$, $j = 1, \dots, U$. We also assume that each user's lattice is of full rank $r = 2n_t k$, and denote the basis of the lattice \mathbf{L}_j by $B_{j,1}, \dots, B_{j,r}$. Now the code associated with the j th user is a restriction of lattice \mathbf{L}_j

$$\mathbf{L}_j(N_j) = \left\{ \sum_{i=1}^r b_i B_{j,i} \mid b_i \in \mathbb{Z}, -N_j \leq b_i \leq N_j \right\},$$

where N_j is a given positive number.

Using these definitions the U -user MIMO MAC code is $(\mathbf{L}_1(N_1), \mathbf{L}_2(N_2), \dots, \mathbf{L}_U(N_U))$. Let $\mathcal{I}_u = \{i_1, \dots, i_u\} \subseteq \{1, \dots, U\}$ be of size $u > 0$. We will then use the notation $M(X_{i_1}, \dots, X_{i_u}) \in M_{u n_t \times k}(\mathbb{C})$, where we have stacked the codewords X_{i_j} from the users $\{i_1, \dots, i_u\}$ on top of each other.

The following example shows how the different error events leads to different code design criteria.

Example 1.1: Let us suppose that we have three user MIMO MAC channel. The channel equation can now be written as

$$[H_1, H_2, H_3] \begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix} + W = H_1 X_1 + H_2 X_2 + H_3 X_3 + W.$$

Let us suppose that the receiver manages to decode the message X_1 of the first user. As we supposed that the receiver has perfect channel state information we can simply subtract the matrix $H_1 X_1$ from the channel equation. Therefore, if we like to design the code against an error event where exactly the second and the third user are in error, we can consider simply the code $(\mathbf{L}_2, \mathbf{L}_3)$ and try to maximize

$$\min_{0 \neq X_i \in \mathbf{L}_i(M)} \det(M(X_2, X_3)M(X_2, X_3)^\dagger), \quad (2)$$

with the assumption $X_i \neq 0$. Here we again took a benefit of the fact that \mathbf{L}_2 and \mathbf{L}_3 are lattices and therefore additively closed. Similar analysis obviously provides us with a minimum determinant criterion for any error event.

The previous example reveal that we should aim at maximizing the minimum determinants of subcodes corresponding to any error events. The design criterion for each error event is then the usual minimum determinant criterion, but with an extra assumption that the code matrices of the users in error are non-zero.

Definition 1.2: Let $C_{U,n_t} = (\mathbf{L}_1, \mathbf{L}_2, \dots, \mathbf{L}_U)$ and $\mathcal{I}_u = \{i_1, \dots, i_u\}$ and write $C_{U,n_t}^{\mathcal{I}_u} = (\mathbf{L}_{i_1}, \mathbf{L}_{i_2}, \dots, \mathbf{L}_{i_u})$. Define the decay function for $C_{U,n_t}^{\mathcal{I}_u}$ by setting

$$D_{\mathcal{I}_u}(N_{i_1}, \dots, N_{i_u}) = \min_{X_{i_j} \in \mathbf{L}_{i_j}(N_{i_j}) \setminus \{0\}} \sqrt{\det(MM^\dagger)},$$

where $M = M(X_{i_1}, \dots, X_{i_u})$.

For a special case $N_1 = \dots = N_U = N$ we write

$$D_{\mathcal{I}_u}(N) = D_{\mathcal{I}_u}(N_{i_1} = N, \dots, N_{i_u} = N).$$

We also use notion

$$D(N_1, \dots, N_U) = D_{\{1, \dots, U\}}(N_1, \dots, N_U)$$

and similarly as above

$$D(N) = D_{\{1, \dots, U\}}(N_1 = N, \dots, N_U = N).$$

If we have a U -user code with decay function $D(N_1, \dots, N_U)$, such that $D(N_1, \dots, N_U) \neq 0$ for all $N_1, \dots, N_U \in \mathbb{Z}_+$, we say that the code satisfies (*generalized*) *rank criterion*.

II. UPPER BOUNDS FOR THE DECAY OF DETERMINANTS

There are several single user MIMO codes $\mathbf{L} \subseteq M_{n \times k}(\mathbb{C})$ that satisfy

$$\inf_{0 \neq X \in \mathbf{L}} \det(XX^\dagger) > 0.$$

Such a lattice code is said to have the *non-vanishing determinant* (NVD) property. This is obviously a guarantee that the minimum determinants of all the finite codes $\mathbf{L}(M)$ are lower bounded and from the PEP point of view such a property is very desirable.

It is tempting to try to build such MIMO MAC code C_{U,n_t} that for any subset of user $\mathcal{I}_u = \{i_1, \dots, i_u\} \subset I$ the decay function would satisfy

$$D_{\mathcal{I}_u}(N_{i_1}, \dots, N_{i_u}) \geq \epsilon,$$

for some fixed $\epsilon > 0$, irrespective of the code sizes of the users i_j . Unfortunately this is not possible. Already in [7] it was proved that no matter how we build the codes, the function $D(N)$ will decay as a function of N . In this section we will give upper bounds for $D_{\mathcal{I}_u}(N_{i_1}, \dots, N_{i_u})$ for any subset \mathcal{I}_u of user. The bounds will depend on the size of the code of each user and will reveal a trade-off between rate and diversity.

In order to keep the paper easy to understand we delay the proof of Theorem 2.5 to the end of the paper. However, in order to give some idea of the proof, we introduce some concepts and results that are most crucial and demonstrate the basic ideas in Example 2.1.

A. The pigeon hole principle in a subspace

Let us consider the space $M_{n \times k}(\mathbb{C})$, where $k \geq n$ over the real numbers. It is $2nk$ -dimensional real vector space with a real inner product

$$\langle X, Y \rangle = \Re(\text{Tr}(XY^\dagger)),$$

where Tr is the matrix trace. This inner product also naturally defines a metric on the space $M_{n \times k}(\mathbb{C})$, when setting $\|X\| = \sqrt{\langle X, X \rangle}$.

Definition 2.1: Let us suppose that A is a subspace of $M_{n \times k}(\mathbb{C})$. We then have that

$$A^\perp := \{x \mid x \in M_{n \times k}(\mathbb{C}), \langle x, a \rangle = 0 \forall a \in A\},$$

is an \mathbb{R} -linear subspace of $M_{n \times k}(\mathbb{C})$.

The following lemma is a collection of well known results from basic linear algebra.

Lemma 2.1: Let us suppose that A is a k -dimensional subspace of $M_{n \times k}(\mathbb{C})$. Then

$$M_{n \times k}(\mathbb{C}) = A \oplus A^\perp,$$

$\dim_{\mathbb{R}}(A^\perp) = 2nk - \dim_{\mathbb{R}}(A) = v$ and A^\perp has a v -dimensional orthonormal basis $\{e_1, \dots, e_v\}$ with respect to the real inner product of $M_{n \times k}(\mathbb{C})$.

Let us suppose that x is an element of $M_{n \times k}(\mathbb{C})$ and A a subspace. According to Lemma 2.1 we can now write x uniquely in the form

$$x = a_1 + a_2, \tag{3}$$

where $a_1 \in A$ and $a_2 \in A^\perp$. This decomposition gives us a well defined \mathbb{R} -linear mapping $\pi_{A^\perp} : M_{n \times k}(\mathbb{C}) \mapsto A^\perp$, where

$$\pi_{A^\perp}(x) = a_2. \tag{4}$$

Lemma 2.2 (Pigeon hole principle in a subspace): Let us suppose that we have a set of matrices $S = \{x_1, \dots, x_s\} \subset M_{n \times k}(\mathbb{C})$, where $\|x_l\| \leq M, \forall l$ and a subspace $A \subset M_{n \times k}(\mathbb{C})$. Then the set S includes matrices x_i and x_j , where $x_i \neq x_j$ such that

$$\|\pi_{A^\perp}(x_i) - \pi_{A^\perp}(x_j)\| \leq 4h \frac{M}{s^{1/h}},$$

where h is the real dimension of the subspace A^\perp .

Proof: If the set S includes such elements x_i and x_j that $\pi_{A^\perp}(x_i) = \pi_{A^\perp}(x_j)$, we are done. We can now suppose that $\pi_{A^\perp}(S)$ has s different elements. The space A^\perp has an orthonormal basis $E = \{e_1, \dots, e_h\} \subseteq M_{n \times k}(\mathbb{C})$. We can now define a cube

$$C(M) = \left\{ \sum_{l=1}^h b_l e_l \mid b_l \in \mathbb{R}, -M \leq b_l \leq M \right\},$$

which has volume $(2M)^k$. The projection is a shrinking map and therefore $\pi_{A^\perp}(S) \subset C(M)$.

The cube $C(M)$ can be divided into smaller cubes of side length $4M/s^{1/h}$. The $C(M)$ gets now partitioned to $(2M)^h/(4M/s^{1/h})^h = s/2^h$ small cubes. As $\pi_{A^\perp}(S)$ has s elements, there must be at least two that are in the same cube of side length $4M/s^{1/h}$. ■

Corollary 2.3: Let us suppose that we have an l -dimensional lattice $\mathbf{L} \subset M_{n \times k}(\mathbb{C})$, where each of the basis elements y_i has norm less than a constant K , and a subspace $A \subset M_{n \times k}(\mathbb{C})$. The subset $\mathbf{L}(M)$ has such a non zero matrix z that

$$\|\pi_{A^\perp}(z)\| \leq 2^{l/h+2} h K M^{\frac{h-l}{h}},$$

where h is the real dimension of the space A^\perp and $M \geq 4$.

Proof: Let us suppose that y_1, \dots, y_l is the basis of the lattice \mathbf{L} . Every element of \mathbf{L} is a \mathbb{Z} -linear combination of the basis elements and we have the inequality

$$\|n_1 y_1 + \dots + n_l y_l\| \leq \sum_{i=1}^l |n_i| \|y_i\|.$$

Therefore, for any element $x \in \mathbf{L}(M)$, we have

$$\|x\| \leq KM.$$

The set $\mathbf{L}(M/2)$ has now at least $(M/2)^l$ elements. According to Lemma 2.2 there is then a pair of elements x_i and x_j such that

$$\|\pi_{A^\perp}(x_i) - \pi_{A^\perp}(x_j)\| \leq 4hK2^{l/h} \frac{M}{M^{l/h}}.$$

As π_{A^\perp} is linear we have that $\|\pi_{A^\perp}(x_i - x_j)\| \leq 2^{l/h+2} h K \frac{M}{M^{l/h}}$. Both x_i and x_j belong to $\mathbf{L}(M/2)$ and therefore $x_i - x_j \in \mathbf{L}(M)$ and we are done. ■

B. Upper bounds for the decay

Let us give one more tool before stating the main result of the section.

Let us suppose that X is a matrix in $M_{n \times k}(\mathbb{C})$. Let the set of row indices $J = \{1, \dots, n\}$ be partitioned to subset J_1, \dots, J_r . If we stack the rows in J_i , we will get a matrix in $M_{|J_i| \times k}(\mathbb{C})$. Let us denote it with X_i . We then have the following.

Lemma 2.4: Let us suppose that $X \in M_{n \times k}(\mathbb{C})$ and write $|J_i| = j_i$. We then have

$$\det(XX^\dagger) \leq \det(X_1 X_1^\dagger) \cdots \det(X_r X_r^\dagger) \leq \prod_{i=1}^r \frac{\|X_i\|_F^{2j_i}}{j_i^{j_i}}.$$

Proof: The first inequality is the generalized Hadamard inequality [4] page 254. The second inequality is then an application of Hadamard inequality to the rows of X_i 's and AM-GM inequality. ■

The following theorem states that if the single user codes are large the overall code corresponding to each error event will automatically include matrices with small determinants. This can be seen as a trade-off between rate and coding gain.

Theorem 2.5 (Generalized pigeon hole bound): Let us suppose we have a MIMO MAC code $(\mathbf{L}_1(N_1), \mathbf{L}_2(N_2), \dots, \mathbf{L}_U(N_U))$ of U users. Let us also suppose that each user has n_t transmission antennas and that the individual codes \mathbf{L}_i are $2kn_t$ -dimensional lattice codes in $M_{n_t \times k}(\mathbb{C})$, where $k \geq Un_t$. We then have that

$$D_{\mathcal{I}_u}(N_{i_1}, \dots, N_{i_u}) \leq K \prod_{l=1}^{u-1} N_{i_l}^{-\frac{n_t^2(u-l)}{k-n_t(u-l)}}$$

and in particular

$$D_{\mathcal{I}_u}(N) \leq \frac{K}{N^\alpha},$$

where $\alpha = \sum_{l=1}^{u-1} \frac{n_t^2(u-l)}{k-n_t(u-l)}$ and K is a fixed constant.

The proof of the previous theorem is given only in the Appendix, but let us describe the proof in a simple case of three users in the following example.

Example 2.1: Let us suppose we have $U = 3$ users, each transmitting with $n_t = 1$ antenna, and that the code length is $k = Un_t = 3$. For simplicity, let us also assume that $N_1 = N_2 = N_3 = N$. Let us now study the behavior of the decay function $D(N)$ in this scenario.

Let us first fix some small $C_3 \in \mathbf{L}_3(N)$. Hence $\|C_3\| = \mathcal{O}(1)$. Let $W_3 = \mathbb{R}(C_3)$ and let $V_3 = W_3^\perp$ be its orthogonal complement. The corresponding orthogonal projection is $\pi_3 : M_{1 \times 3}(\mathbb{C}) \rightarrow V_3$.

A subspace V_3 has $\dim_{\mathbb{R}}(V_3) = 2n_t k - \dim_{\mathbb{R}}(W_3) = 6 - 2 = 4$ so the image $\pi_3(\mathbf{L}_2(N))$ falls into a 4-dimensional hypercube with side length of size $\mathcal{O}(N)$. We also have $|\mathbf{L}_2(N)| = \theta(N^6)$ and therefore by pigeon hole principle, we have such $C_2 \in \mathbf{L}_2(N)$ that

$$\pi_3(C_2) = \mathcal{O}\left(\sqrt[4]{\frac{N^4}{N^6}}\right) = \mathcal{O}(N^{-\frac{1}{2}}).$$

Now similarly build $V_2 = W_2^\perp$ by setting $W_2 = \mathbb{R}(C_2, C_3)$. This gives $\dim_{\mathbb{R}}(V_2) = 2$. And again we find such C_1 that

$$\pi_2(C_1) = \mathcal{O}\left(\sqrt{\frac{N^2}{N^6}}\right) = \mathcal{O}(N^{-2})$$

with $\pi_2 : M_{1 \times 3}(\mathbb{C}) \rightarrow V_2$ being an orthogonal projection.

Hence we have a matrix A in our code such that the determinant $\det(AA^\dagger)$ is by Lemmas 7.1 and 2.4 of size

$$\mathcal{O}(N^{2 \cdot (-\frac{1}{2})} \cdot N^{2 \cdot (-2)}) = \mathcal{O}(N^{-5})$$

and hence $D(N) = \mathcal{O}(N^{-\frac{5}{2}})$.

Note that in the special case of this example A is a square matrix and hence it is not necessary to use Lemma 7.1. It is enough to notice that $\det(AA^\dagger) = |\det(A)|^2$ and

$$\det(A) = \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} \pi_2(C_1) \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} \pi_2(C_1) \\ \pi_3(C_2) \\ C_3 \end{pmatrix}$$

and then use Lemma 2.4 to estimate the size of the determinant $\det(AA^\dagger)$.

III. LOWER BOUNDS FOR THE DECAY BY EXPLICIT CONSTRUCTIONS

Due to the strongly algebraic nature of our constructions in Section V-B, we will only preview the results of that section here and give a simple example of our approach.

The main result in V-B is a completely general construction for MIMO MAC codes where each of the U single users with n_t antennas, will have a lattice code \mathbf{L}_i in $M_{n_t \times U n_t}(\mathbb{C})$ and where the overall MAC code $C_{U, n_t} = (\mathbf{L}_1, \mathbf{L}_2, \dots, \mathbf{L}_U)$ has the generalized full rank property and promising decay properties. The goal of these constructions is to give a general construction of MIMO MAC codes that would have as good as possible decay in every error event.

The natural comparison for the following result is the upper bound of Theorem 2.5. Let C_{U, n_t} be a MAC code build in Section V-B. We then have the following two results.

Result 1 (Theorem 6.5): For a code C_{U, n_t} there exists a constant $K > 0$ such that

$$D_{\mathcal{I}_u}(N_{i_1}, \dots, N_{i_u}) \geq \begin{cases} \frac{K}{(N_{i_1} \dots N_{i_u})^{(U-1)n_t}} & \text{if } u > 1 \\ K & \text{if } u = 1. \end{cases}$$

In particular we have

$$D_{\mathcal{I}_u}(N) \geq \begin{cases} \frac{K}{N^{u(U-1)n_t}} & \text{if } u > 1 \\ K & \text{if } u = 1. \end{cases}$$

The following result proves that in the case where we let only the rate of a fixed single user grow we achieve the optimal decay.

Result 2 (Corollary 6.6): For a code C_{U, n_t} there exists constants $k > 0$ and $K > 0$ such that

$$\frac{k}{N^{(U-1)n_t}} \leq D(N_1 = N, N_2 = \dots = N_U = 1) \leq \frac{K}{N^{(U-1)n_t}}.$$

Let us now give an example of our constructions.

Example 3.1: Let us suppose that we have U users, each having a single antenna.

We can now find a degree U cyclic extension $L/\mathbb{Q}(i)$ and have the Minkowski embedding $\psi : L \mapsto \mathbb{C}^U$, where

$$\psi(x) = (x, \sigma(x), \dots, \sigma^{n-1}(x)),$$

for $x \in L$. If we concentrate on the ring of algebraic integers \mathcal{O}_L , we have that $\psi(\mathcal{O}_L)$ is a $2n$ -dimensional lattice in \mathcal{O}_L .

Let us now suppose that p is a prime number which is totally inert in the extension L/\mathbb{Q} . We can then modify the embedding ψ to get U single user lattice codes $\psi_{i, p^{-1}}(\mathcal{O}_L)$, where

$$\psi_{i, p^{-1}}(x) = (x, \sigma(x), \dots, p^{-1}\sigma^{i-1}(x), \dots, \sigma^{U-1}(x)).$$

A U user MAC code $C_{U, 1}$ can now be defined by

$$(\psi_{1, p^{-1}}(\mathcal{O}_L), \psi_{2, p^{-1}}(\mathcal{O}_L), \dots, \psi_{U, p^{-1}}(\mathcal{O}_L)),$$

where each of the single user codes are previously defined $2U$ -dimensional lattices in \mathbb{C}^U .

The overall code matrices in this MAC code then have the form

$$\begin{pmatrix} p^{-1}x_1 & \sigma(x_1) & \sigma^2(x_1) & \dots & \sigma^{U-1}(x_1) \\ x_2 & p^{-1}\sigma(x_2) & \sigma^2(x_2) & \dots & \sigma^{U-1}(x_2) \\ x_3 & \sigma(x_3) & p^{-1}\sigma^2(x_3) & \dots & \sigma^{U-1}(x_3) \\ \vdots & \vdots & \vdots & & \vdots \\ x_U & \sigma(x_U) & \sigma^2(x_U) & \dots & p^{-1}\sigma^{U-1}(x_U) \end{pmatrix}. \quad (5)$$

The key to the generalized rank criteria is the choice of the element p . By analyzing the p -adic valuation of the determinant of the overall code matrix (5), we find that when all the rows are non-zero, the valuation of the determinant can not be ∞ and therefore the determinant can not be zero.

We could have also used for example transcendental element on place of p^{-1} , but as we will later see, from the decay point of view it is crucial that the element p^{-1} is from the field L . By such choice of the diagonal element, all the elements in codematrices are from a low degree number field L and we can effectively use results from Diophantine approximation to prove results about the decay.

If we suppose that $U = 3$ Theorem 6.5 gives us that

$$D_{\{1,2,3\}}(N, N, N) \geq \frac{K}{N^6},$$

for some constant K .

IV. LOWER BOUNDS FOR THE DMT OF OUR CONSTRUCTIONS

It was proved in [21] and [12] that if a $2n_t k$ dimensional lattice code $L \subset M_{n_t \times k}(\mathbb{C})$ has the NVD property, then it is DMT optimal in the single user $n_t \times n_r$ MIMO channel. It is a natural idea to see what can be said about the DMT of the codes constructed in this paper based on the lower bounds for the decay of determinants.

Having obtained in Theorem 8.3 a lower bound on the minimum determinant among all the nonzero code matrices in code C_{U, n_t} , in this section we will apply this bound to investigate the diversity-multiplexing gain tradeoff (DMT) achieved by C_{U, n_t} . We note that in this section the analyzed codes C_{U, n_t} are the MAC codes we constructed in Section V-B.

A. Some Preliminaries

We first introduce a power constraint on the transmitted signal matrices and reformulate the MIMO multiple-access channel as

$$Y = \sum_{i=1}^U \kappa_i H_i X_i + W,$$

where $H_i \in M_{n_r \times n_t}(\mathbb{C})$ is the channel matrix of the i th user, and $W \in M_{n_r \times k}(\mathbb{C})$ is the white noise matrix; both are defined as before. Realizations of H_i are known perfectly to the receiver but are unknown to the users. $X_i \in \mathbf{L}_i(N_i) \subset M_{n_t \times k}(\mathbb{C})$ is the signal matrix transmitted by the i th user. $\kappa_i \in \mathbb{R}^+$ is an amplification factor such

that the average signal-to-noise power ratio (SNR) of the i th user equals SNR, *i.e.*,

$$\kappa_i^2 \frac{1}{|\mathbf{L}_i(N_i)|} \sum_{X_i \in \mathbf{L}_i(N_i)} \|X_i\|^2 = \text{SNR}.$$

Having specified N_i , the transmission rate, in bits per channel use, of the i th user is

$$R_i = \frac{1}{k} \log_2 |\mathbf{L}_i(N_i)|.$$

By increasing the rate R_i as a linear function of $\log_2 \text{SNR}$ as $\text{SNR} \rightarrow \infty$, following [18], we say the i th user transmits at multiplexing gain r_i if

$$\lim_{\text{SNR} \rightarrow \infty} \frac{R_i}{\log_2 \text{SNR}} = r_i.$$

Equivalently, we shall adopt the dotted-equality notation ¹ introduced in [18] to rewrite the above as

$$|\mathbf{L}_i(N_i)| \doteq \text{SNR}^{kr_i}.$$

As $\mathbf{L}_i(N_i) = \left\{ \sum_{j=1}^{2n_t k} b_j B_{i,j} | b_j \in \mathbb{Z}, |b_j| \leq N_i \right\}$ and $|\mathbf{L}_i(N_i)| = (2N_i + 1)^{2n_t k}$, transmitting at multiplexing gain r_i implies that

$$N_i \doteq \text{SNR}^{\frac{r_i}{2n_t}}. \quad (6)$$

On the other hand, note that the basis matrices $B_{i,1}, \dots, B_{i,2n_t k}$ are constant matrices and are independent of SNR. It can be shown that for $N_i \gtrsim \text{SNR}^0$

$$\frac{1}{|\mathbf{L}_i(N_i)|} \sum_{X_i \in \mathbf{L}_i(N_i)} \|X_i\|^2 \doteq N_i^2.$$

Hence, the amplification factor associated with a fixed multiplexing gain r_i is

$$\kappa_i^2 \doteq \text{SNR}^{1 - \frac{r_i}{n_t}}. \quad (7)$$

Finally, we say the code C_{U,n_t} achieves diversity gain $d(r_1, \dots, r_U)$ if the codeword error probability $P_{\text{cwe}}(r_1, \dots, r_U)$ subject to the joint maximal-likelihood decoding of (X_1, \dots, X_U) at the receiver satisfies

$$P_{\text{cwe}}(r_1, \dots, r_U) \doteq \text{SNR}^{-d(r_1, \dots, r_U)}.$$

The function $d(r_1, \dots, r_U)$ is also termed the MIMO MAC DMT for code C_{U,n_t} . It is known [2], [7] that $d(r_1, \dots, r_U)$ is upper bounded by

$$d(r_1, \dots, r_U) \leq \min \left\{ d_{un_t, n_r}^* \left(\sum_{i \in \mathcal{I}} r_i \right) \mid \begin{array}{l} \mathcal{I} \subseteq \{1, 2, \dots, U\}, \\ |\mathcal{I}| = u, u = 1, \dots, U \end{array} \right\} \quad (8)$$

where the RHS represents the best possible diversity gain that can be achieved by any MIMO MAC codes when transmitted at multiplexing gains r_1, \dots, r_U , respectively. The function $d_{m,n}^*(r)$ is the optimal DMT for a point-to-point MIMO channel with m transmitting and n receiving antennas and transmitting at multiplexing gain r . In particular, $d_{m,n}^*(r)$ is a piecewise linear function obtained by joining the points $(r, (m-r)(n-r))$ for $r = 0, 1, \dots, \min\{m, n\}$.

¹Let $f(\text{SNR})$ and $g(\text{SNR})$ be two functions of SNR. We say $f(\text{SNR}) \doteq g(\text{SNR})$ if $\lim_{\text{SNR} \rightarrow \infty} \frac{f(\text{SNR})}{\log_2 \text{SNR}} = \lim_{\text{SNR} \rightarrow \infty} \frac{g(\text{SNR})}{\log_2 \text{SNR}}$. The dotted inequalities such as \gtrsim , \lesssim , \gtrdot , and \lesssimdot are defined similarly.

B. Lower Bounds on $d(r_1, \dots, r_U)$

To analyze $d(r_1, \dots, r_U)$ for code C_{U, n_t} , let $\mathcal{E}_{\mathcal{I}}$ denote the event that only the signals of users in set \mathcal{I} , $\mathcal{I} \subseteq \mathcal{U} = \{1, 2, \dots, U\}$, are erroneously decoded. Clearly, the overall error event is $\mathcal{E} = \bigcup_{\mathcal{I} \subseteq \mathcal{U}} \mathcal{E}_{\mathcal{I}}$, and the codeword error probability is upper bounded by

$$P_{\text{cwe}}(r_1, \dots, r_U) = \Pr\{\mathcal{E}\} \leq \sum_{\mathcal{I} \subseteq \mathcal{U}} \Pr\{\mathcal{E}_{\mathcal{I}}\}. \quad (9)$$

To further upper-bound the probability of error event $\mathcal{E}_{\mathcal{I}}$ we employ the bounded-distance decoder introduced in [21]. Specifically, given the channel matrices H_i , $i = 1, \dots, U$, the bounded-distance decoder searches for code matrices (X_1, \dots, X_U) such that $\left\| Y - \sum_{i=1}^U \kappa_i H_i X_i \right\| < \frac{1}{2} d_{\min}(H_1, \dots, H_U)$, where $d_{\min}(H_1, \dots, H_U)$ is the minimum distance among matrices $\sum_{i=1}^U \kappa_i H_i X_i$ for all $X_i \in \mathbf{L}_i(N_i)$, that is,

$$d_{\min}(H_1, \dots, H_U) = \min \left\{ \left\| \sum_{i=1}^U \kappa_i H_i \Delta X_i \right\| \mid \begin{array}{l} \Delta X_i \in \mathbf{L}_i(2N_i) \text{ and} \\ \text{not all } \Delta X_i = \mathbf{0} \end{array} \right\}.$$

It should be noted that as the matrices H_1, \dots, H_U are random, the minimum distance $d_{\min}(H_1, \dots, H_U)$ is indeed a nonnegative random variable. Furthermore, it is clear that

$$\Pr\{\mathcal{E}\} \leq \Pr \left\{ \|W\| \geq \frac{1}{2} d_{\min}(H_1, \dots, H_U) \right\}$$

where W is the noise matrix, and the RHS represents an upper bound on the probability of decoding error/failure of such bounded distance decoder. Now focusing on the error event $\mathcal{E}_{\mathcal{I}}$, where only the signals of users in set $\mathcal{I} = \{i_1, \dots, i_u\}$ and $|\mathcal{I}| = u$ are decoded in error. We define the corresponding minimum distance in this case by

$$d_{\min}(H_{i_1}, \dots, H_{i_u}) = \min \left\{ \left\| \sum_{i \in \mathcal{I}} \kappa_i H_i \Delta X_i \right\| \mid \begin{array}{l} \Delta X_i \in \mathbf{L}_i(2N_i) \text{ and} \\ \text{not all } \Delta X_i = \mathbf{0} \end{array} \right\}.$$

Similarly, it can be shown that

$$\Pr\{\mathcal{E}_{\mathcal{I}}\} \leq \Pr \left\{ \|W\| \geq \frac{1}{2} d_{\min}(H_{i_1}, \dots, H_{i_u}) \right\}. \quad (10)$$

The lower bound on the minimal determinant given in Theorem 8.3 then allows us to obtain a lower bound on $d_{\min}(H_{i_1}, \dots, H_{i_u})$ and therefore leads to a further upper bound on the error probability $\Pr\{\mathcal{E}_{\mathcal{I}}\}$. The proof of the following Theorem will be given in Appendix.

Theorem 4.1: For a MIMO MAC code $C_{U, n_t} \subset M_{U n_t \times k}(\mathbb{C})$ of U users defined as before, assume the users transmit at multiplexing gains r_1, \dots, r_U , respectively. The probability of event $\mathcal{E}_{\mathcal{I}}$ that only the signals of users in set \mathcal{I} , $\mathcal{I} \subseteq \mathcal{U}$, are erroneously decoded is upper bounded by

$$\Pr\{\mathcal{E}_{\mathcal{I}}\} \leq \begin{cases} \text{SNR}^{-d_{U, n_t, n_r}^*(U \sum_{i \in \mathcal{I}} r_i)}, & \text{if } |\mathcal{I}| = u > 1, \\ \text{SNR}^{-d_{n_t, n_r}^*(r_i)}, & \text{if } \mathcal{I} = \{i\}. \end{cases} \quad (11)$$

Applying Theorem 4.1 to the union bound of $\Pr\{\mathcal{E}\}$ in (9) we immediately arrive at the following corollary. This gives a lower bound on the MAC DMT for code C_{U, n_t} .

Corollary 4.2 (Lower bound on $d(r_1, \dots, r_U)$): For a MIMO MAC code $C_{U, n_t} \subset M_{U n_t \times k}(\mathbb{C})$ of U users defined as before, the corresponding MAC DMT is lower bounded by

$$d(r_1, \dots, r_U) \geq \min \left\{ \begin{array}{l} d_{u n_t, n_r}^* (U \sum_{i \in \mathcal{I}} r_i), d_{n_t, n_r}^*(r_j) \\ \mathcal{I} \subseteq \mathcal{U}, |\mathcal{I}| = u > 1, j \in \mathcal{U} \end{array} \right\}. \quad (12)$$

In particular, for the symmetric MIMO MAC where $r_1 = r_2 = \dots = r_U = r$, we have

$$d(r, \dots, r) \geq \min \{ d_{u n_t, n_r}^* (U u r), d_{n_t, n_r}^*(r) | u = 2, \dots, U \} \\ = \begin{cases} \min \{ d_{2 n_t, n_r}^* (2 U r), d_{n_t, n_r}^*(r) \}, & \text{if } r \in [0, \theta] \\ \min \{ d_{U n_t, n_r}^* (U^2 r), d_{n_t, n_r}^*(r) \} & \text{if } r \in [\theta, \frac{n_t}{U}] \end{cases}, \quad (13)$$

where $\theta = \min \{ \frac{n_t}{U}, \frac{n_r}{U(U+2)} \}$.

Proof: It simply follows from (9), after noting that when $\text{SNR} \rightarrow \infty$ we have

$$P_{\text{cwe}}(r_1, \dots, r_U) \leq \sum_{\mathcal{I} \subseteq \mathcal{U}} \Pr \{ \mathcal{E}_{\mathcal{I}} \} \doteq \max_{\mathcal{I} \subseteq \mathcal{U}} \Pr \{ \mathcal{E}_{\mathcal{I}} \}.$$

The second equality in (13) can be shown by arguing similarly as in [2, Sec. VIII] that

$$\min \{ d_{u n_t, n_r}^* (u \gamma) | u = 2, \dots, U \} = \begin{cases} d_{2 n_t, n_r}^* (2 \gamma) & \text{if } \gamma \in [0, \theta'] \\ d_{U n_t, n_r}^* (U \gamma) & \text{if } \gamma \in [\theta', n_t] \end{cases}$$

where $\theta' = \min \{ n_t, \frac{n_r}{U+2} \}$ and by setting $\gamma = U r$. ■

To summarize, in this section we have presented a general lower bound (12) on the DMT performance of code C_{U, n_t} . The lower bound for the symmetric case is given in (13). While the optimal MAC DMT [2] for all possible MIMO MAC codes is given by

$$d_{U, n_t, n_r}^*(r_1, \dots, r_U) = \min \left\{ \begin{array}{l} d_{u n_t, n_r}^* (\sum_{i \in \mathcal{I}} r_i), d_{n_t, n_r}^*(r_j) \\ \mathcal{I} \subseteq \mathcal{U}, |\mathcal{I}| = u > 1, j \in \mathcal{U} \end{array} \right\}. \quad (14)$$

Below we apply the bounds to study the DMT performance of code C_{U, n_t} over some MIMO MACs. For simplicity, we will focus only on the symmetric case. In Fig. 1 we present the bounds on the DMT performance of C_{U, n_t} for $n_t = 2$, $n_r = 4$ and $U = 3$. The ‘‘optimal’’ DMT curve represents the optimal MIMO MAC DMT $d_{U, n_t, n_r}^*(r_1, \dots, r_U)$ given in (14). It is known [2] that the maximal possible multiplexing gain for this channel is $\frac{\min \{ U n_t, n_r \}}{U} = \frac{4}{3}$. This means that whenever $r > \frac{4}{3}$ the corresponding diversity gain must be zero, and communications over this channel cannot be reliable. Furthermore, Tse *et al.* [2] show that for $r \leq \frac{\min \{ U n_t, n_r \}}{U+1} = 1$ the optimal DMT is dominated by the single-user performance. The remaining region where $1 \leq r \leq \frac{4}{3}$ is termed the ‘‘antenna pooling’’ region [2] and the DMT performance is dominated by the case when all user’s signals are erroneously decoded. From Fig. 1 we see that the code C_{u, n_t} is in fact MAC-DMT optimal for $r \leq 0.24$.

In Fig. 2 we present the bounds on the DMT performance of code C_{U, n_t} for $n_t = 2$, $n_r = 8$ and $U = 3$, corresponding to the case without antenna pooling region. The optimal MAC-DMT is completely dominated by the single-user performance. It is seen from Fig. 2 that the code C_{U, n_t} remains to be DMT optimal whenever $r \leq \frac{23}{45} \approx 0.311$. Fig. 3 shows the bounds on the DMT performance of code C_{U, n_t} for $n_t = 3$, $n_r = 6$ and $U = 2$. We see that the code C_{U, n_t} is DMT optimal whenever $r \leq 0.6$.

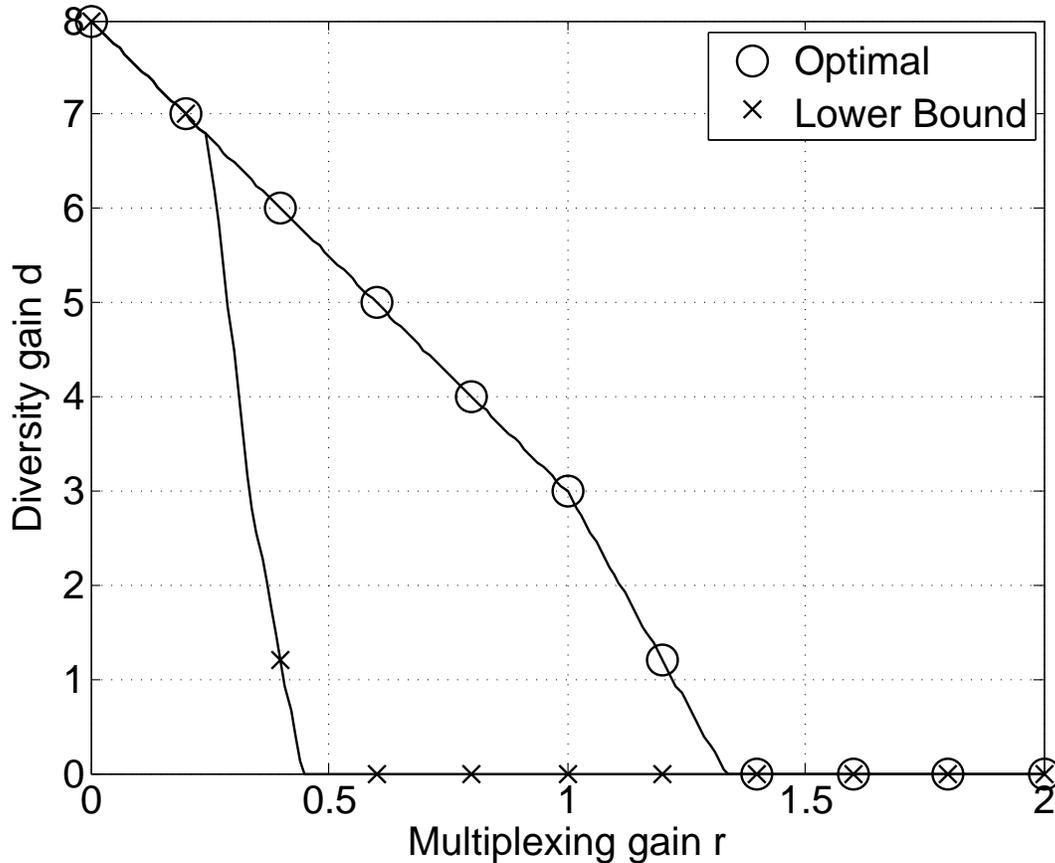


Fig. 1. Bounds on the DMT performance of code C_{U,n_t} for $n_t = 2$, $n_r = 4$ and $U = 3$

V. CONSTRUCTIONS

In this section we are giving our general constructions, having properties discussed in Section III. As explained there the main idea is to build codes having as good as possible decay. Unfortunately we are forced to use several techniques from different parts of number theory and will assume that the reader has working knowledge on the topic. We will also skip some of the proofs as they are purely number theoretical and rather standard.

First in Subsection V-A we analyze the single antenna two user case thoroughly. Then in Subsection V-B we will generalize this construction for U users with n_t transmit antennas.

A. A 2-user code

In [14] Badr and Belfiore introduced a 2-user single antenna MAC code where the matrix coefficients were from the field $\mathbb{Q}(i, \sqrt{5})$ and had the generalized full rank property. It was proved in [5] that their construction had particularly good decay behavior and that the key to this behavior was that the algebraic elements in the code matrices were from a numberfield of low degree (4 to be exact). We will now study a general version of their

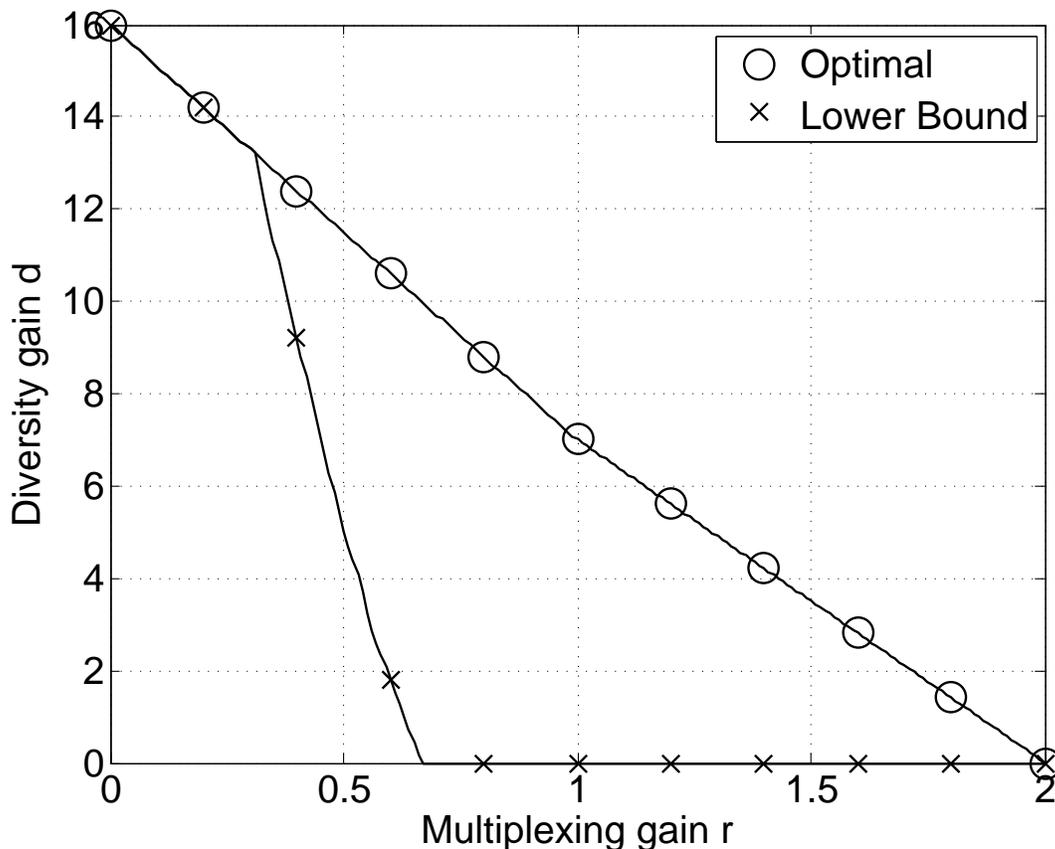


Fig. 2. Bounds on the DMT performance of code C_{U,n_t} for $n_t = 2$, $n_r = 8$ and $U = 3$

construction and study under which conditions it is possible to achieve the full rank condition under the extra condition that the coefficients of the codematrices are from a degree 4 number field.

Let us now suppose we have a complex quadratic field K and a degree two extension L/K and denote the Galois group $G(L/K)$ with $\langle \sigma \rangle$.

If a and b are non zero elements from L , we can define an embedding $\psi_{a,b} : \mathcal{O}_K \mapsto \mathbb{C}^2$ where

$$\psi_{a,b}(x) = (ax, b\sigma(x)),$$

for $x \in \mathcal{O}_L$. The following is then a standard result.

Proposition 5.1: We have that $\psi_{a,b}(\mathcal{O}_L)$ is a 4-dimensional lattice in \mathbb{C}^2 , has NVD property and is therefore DMT optimal in 1×1 MIMO channel.

Let us now suppose we have chosen elements a, b, c and d from the field L and that the first user has code $\psi_{a,b}(\mathcal{O}_L)$ and the second user has code $\psi_{c,d}(\mathcal{O}_L)$. The joint codewords in the MAC code $(\psi_{a,b}(\mathcal{O}_L), \psi_{c,d}(\mathcal{O}_L))$

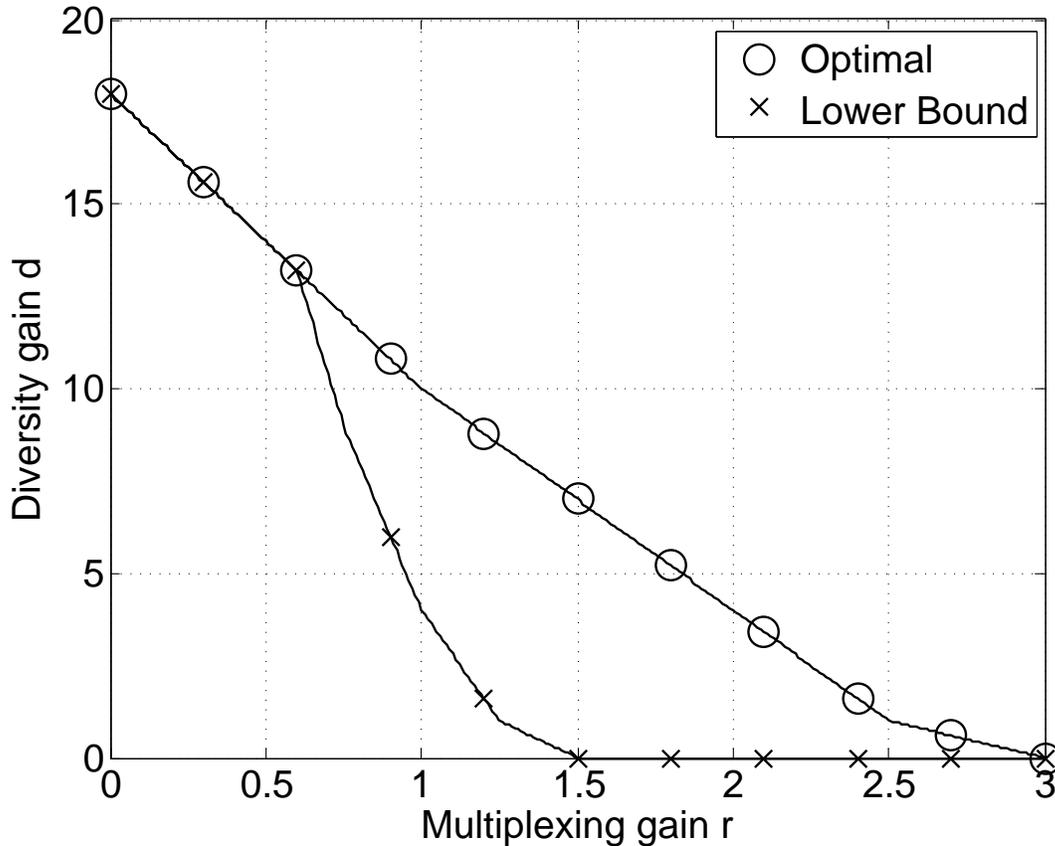


Fig. 3. Bounds on the DMT performance of code C_{U,n_t} for $n_t = 3$, $n_r = 6$ and $U = 2$

now have form

$$\begin{pmatrix} ax & b\sigma(x) \\ cy & d\sigma(y) \end{pmatrix}.$$

We are now interested in when this construction will yield codes with generalized full rank property.

We will denote with \mathcal{O}_L^* the ring of integers of L without zero element.

Theorem 5.2: Let K/\mathbb{Q} and L/K be two field extensions of degree 2 and $a, b, c, d \in L$. Let also σ be the non-trivial element in the Galois group $Gal(L/K)$. Define

$$C = \left\{ \begin{pmatrix} ax & b\sigma(x) \\ cy & d\sigma(y) \end{pmatrix} \mid x, y \in \mathcal{O}_L^* \right\}.$$

There exists a matrix in C with zero determinant if and only if

$$\begin{vmatrix} N(a) & N(b) \\ N(c) & N(d) \end{vmatrix} = 0, \quad (15)$$

where the function $N = N_{L/K}$ denotes the norm of extension L/K .

Proof: Assume first that we have a matrix

$$\begin{pmatrix} ax & b\sigma(x) \\ cy & d\sigma(y) \end{pmatrix}$$

with zero determinant. This means that $adx\sigma(y) = bc\sigma(x)y$, which gives $N(a)N(d)N(x)N(\sigma(y)) = N(b)N(c)N(\sigma(x))N(y)$.

Continuing we get $N(a)N(d) = N(b)N(c)$ i.e. $N(a)N(d) - N(b)N(c) = 0$.

Assume then that $N(a)N(d) - N(b)N(c) = 0$. If b or c is zero then $N(a)N(d) = 0$ i.e. a or d is zero and then for all $x, y \in \mathcal{O}_L$ we have

$$\begin{vmatrix} ax & b\sigma(x) \\ cy & d\sigma(y) \end{vmatrix} = 0.$$

Otherwise $N(\frac{ad}{bc}) = 1$. Then by Hilbert 90 we have some $z \in L$ such that $\frac{ad}{bc} = \frac{\sigma(z)}{z}$. Then write $z = \frac{w}{n}$ with $w \in \mathcal{O}_L^*$ and $n \in \mathbb{Z}$. This gives $\frac{ad}{bc} = \frac{\sigma(w)}{w}$ i.e. $adw - bc\sigma(w) = 0$. This means that the determinant of

$$\begin{pmatrix} aw & b\sigma(w) \\ c1 & d\sigma(1) \end{pmatrix}$$

is zero. ■

Let us now summarize the properties of the codes of previous type.

- The single user codes are DMT optimal lattice codes.
- The MAC code has generalized full rank property.
- The overall MAC code matrices have coefficients from a number field of low degree.

In the next section we will generalize these properties for the MAC codes. The reader can check Equation (18) to see that when restricting to a single antenna case our general construction has indeed the form described in this section.

B. Construction of multi access codes with several transmission antennas

From now on we concentrate on the scenario where we have $U \in \mathbb{Z}_+$ users and each user has $n_t \in \mathbb{Z}_+$ transmission antennas. Throughout this section we assume K to be an imaginary quadratic extension of \mathbb{Q} with class number 1. The field L is a cyclic Galois extension of K of degree Un_t , such that $L = K(\alpha)$ with $\alpha \in \mathbb{R}$, σ a generating element in $Gal(L/K)$ and $p \in \mathcal{O}_K$ an inert prime in L/K . We also define $\tau = \sigma^U$ and F to be the fixed field of τ . So we have $[L : F] = n_t$, $[F : K] = U$, $Gal(L/F) = \langle \tau \rangle$, and $Gal(F/K) = \langle \sigma_F \rangle$ where σ_F is a restriction of σ in F . Let $v = v_p$ be the p -adic valuation of the field L . In this section, when we say that L/K , p , and σ are suitable we mean that they are as above.

We skip the proof of the following proposition.

Proposition 5.3: For every complex quadratic field K , having class number 1, and for any U and for any n_t we have a suitable degree $n_t U$ extension L/K , prime $p \in \mathcal{O}_K$ and automorphism $\sigma \in Gal(L/K)$.

We are now ready to begin to build our MAC codes.

We can define an associative F -algebra

$$\mathcal{D} = (L/F, \tau, p) = L \oplus uL \oplus u^2L \oplus \cdots \oplus u^{n_t-1}L,$$

where $u \in \mathcal{A}$ is an auxiliary generating element subject to the relations $xu = u\tau(x)$ for all $x \in L$ and $u^{n_t} = p$.

The choice of p and fields L and F guarantees that \mathcal{D} is a division algebra.

The \mathcal{O}_L -module

$$\Lambda = \mathcal{O}_L \oplus u\mathcal{O}_L \oplus \cdots \oplus u^{n_t-1}\mathcal{O}_L,$$

where \mathcal{O}_L is the ring of integers, is a subring in the algebra $(L/F, \tau, p)$. We refer to this ring as the *natural order*.

Let us now suppose that we have an element $x \in \Lambda$. It can be written as $\sum_{i=0}^{n_t-1} x_i u^i$, where $x_j \in \mathcal{O}_L$ for all $j = 1, \dots, n_t$. We now have the left regular representation $\psi : \Lambda \mapsto M_{n_t}(\mathcal{O}_L)$, where $\psi(x) =$

$$\begin{pmatrix} x_1 & p\tau(x_{n_t}) & p\tau^2(x_{n_t-1}) & \cdots & p\tau^{n_t-1}(x_2) \\ x_2 & \tau(x_1) & p\tau^2(x_{n_t}) & \cdots & p\tau^{n_t-1}(x_3) \\ x_3 & \tau(x_2) & \tau^2(x_1) & \cdots & p\tau^{n-1}(x_4) \\ \vdots & \vdots & \vdots & & \vdots \\ x_{n_t-1} & \tau(x_{n_t-2}) & \tau^2(x_{n_t-3}) & \cdots & p\tau^{n_t-1}(x_{n_t}) \\ x_{n_t} & \tau(x_{n_t-1}) & \tau^2(x_{n_t-2}) & \cdots & \tau^{n_t-1}(x_1) \end{pmatrix}. \quad (16)$$

If the context is clear we can also use the notation $M(x_1, \dots, x_{n_t}) = \psi(x)$.

Let us suppose we consider U user MAC scenario, where each of the single users has n_t transmit antennas. Note that in this definition we are using the notation $M(x_1, \dots, x_{n_t}) = \psi(x_1 + x_2u + \cdots + x_{n_t}u^{n_t-1})$.

Definition 5.1 (MAC code): Define $M_j = M(x_{j,1}, x_{j,2}, \dots, x_{j,n_t})$ for all $j = 1, \dots, U$. In our multi access system the code \mathcal{C}_j of j th user consists of $n_t \times U n_t$ matrices $B_j =$

$$(M_j, \sigma(M_j), \sigma^2(M_j), \dots, p^{-m}\sigma^{j-1}(M_j), \dots, \sigma^{U-1}(M_j))$$

where m is any rational integer strictly greater than $\frac{U(n_t-1)}{2}$ and $x_{j,l} \neq 0$ for some l . Here m is same for all the users. Then the whole code C_{U, n_t} consists of matrices

$$A = \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_U \end{pmatrix},$$

where $B_j \in \mathcal{C}_j$ for all $j = 1, \dots, U$. This means that the matrices $A \in C_{U, n_t}$ have form

$$\begin{pmatrix} p^{-m}M_1 & \sigma(M_1) & \cdots & \sigma^{U-1}(M_1) \\ M_2 & p^{-m}\sigma(M_2) & \cdots & \sigma^{U-1}(M_2) \\ \vdots & \vdots & & \vdots \\ M_U & \sigma(M_U) & \cdots & p^{-m}\sigma^{U-1}(M_U) \end{pmatrix}. \quad (17)$$

The code depends on how we did choose L/K , p , σ , and m , so to be precise, we can also refer to C_{U,n_t} with $C_{U,n_t}(L/K, p, \sigma, m)$. Let us call the family of all such codes $C_{U,n_t}(L/K, p, \sigma, m)$ (i.e. codes constructed with any suitable L/K , p , σ , and m) by \mathfrak{C}_{U,n_t} . That is

$$\mathfrak{C}_{U,n_t} = \bigcup_{L/K, p, \sigma, m} \{C_{U,n_t}(L/K, p, \sigma, m)\}$$

where L/K , p , σ , and m are any suitable ones.

According to Proposition 5.3 we can always find suitable L/K , p , σ , and m for any $U \in \mathbb{Z}_+$ and $n_t \in \mathbb{Z}_+$. We therefore have the following theorem.

Theorem 5.4: For any choice of $U \in \mathbb{Z}_+$ and $n_t \in \mathbb{Z}_+$ we have $\mathfrak{C}_{U,n_t} \neq \emptyset$.

We will skip the proof of the following proposition, stating that each of the single user codes satisfies the NVD condition and are therefore DMT optimal as a single user MIMO code.

Proposition 5.5: Let $C_{U,n_t} \in \mathfrak{C}_{U,n_t}$ and C_j be the j th users code in the system C_{U,n_t} for some $j \in 1, \dots, U$. Then the code C_j is a $2Un_t^2$ -dimensional lattice code with the NVD property.

Note that the code $C_{U,1} = C_{U,1}(L/K, p, \sigma, 1) \in \mathfrak{C}_{U,1}$, a code for U users each having one transmission antenna, consists of matrices of form

$$\begin{pmatrix} p^{-1}x_1 & \sigma(x_1) & \sigma^2(x_1) & \dots & \sigma^{U-1}(x_1) \\ x_2 & p^{-1}\sigma(x_2) & \sigma^2(x_2) & \dots & \sigma^{U-1}(x_2) \\ x_3 & \sigma(x_3) & p^{-1}\sigma^2(x_3) & \dots & \sigma^{U-1}(x_3) \\ \vdots & \vdots & \vdots & & \vdots \\ x_U & \sigma(x_U) & \sigma^2(x_U) & \dots & p^{-1}\sigma^{U-1}(x_U) \end{pmatrix}. \quad (18)$$

Note also that the code $C_{1,n_t} = C_{1,n_t}(L/K, p, \sigma, m) \in \mathfrak{C}_{1,n_t}$ is a usual single user code multiplied by p^{-m} .

Let us now prove that the defined MAC code satisfies the generalized rank criterion. We need first the following Lemma.

Lemma 5.6: Let $x_j \in \mathcal{O}_L$ for all $j = 1, \dots, n_t$ such that $x_l \neq 0$ for some l and $\min(v(x_1), \dots, v(x_{n_t})) = 0$.

We then have

$$\det(M(x_1, x_2, \dots, x_{n_t})) \neq 0$$

and

$$v(\det(M(x_1, x_2, \dots, x_{n_t}))) \leq n_t - 1.$$

Proof: The first inequality follows as according to equation (16) $M(x_1, x_2, \dots, x_{n_t})$ is a matrix representation of a nonzero element in a division algebra \mathcal{D} and determinant of $M(x_1, x_2, \dots, x_{n_t})$ is the reduced norm. Write $M = M(x_1, x_2, \dots, x_{n_t})$ and $N = N_{L/F}$. Assume first that $v(x_1) = 0$. Then the determinant is $N(x_1) + py$ for some $y \in \mathcal{O}_L$ and hence we have $v(\det(M)) = \min(v(N(x_1)), v(py)) = 0$. Assume then that $v(x_1), v(x_2), \dots, v(x_{l-1}) > 0$ and $v(x_l) = 0$ with $1 < l \leq n_t$. Notice that in this case all the other elements a of matrix M , than those in the left lower corner block of side length $n_t - l + 1$, have $v(a) > 0$. Either they have coefficient p or they are automorphic

images of elements x_1, x_2, \dots, x_{l-1} . Now $\det(M) = \pm p^{l-1}N(x_l) + p^l z$ for some $z \in \mathcal{O}_L$ since all the other terms except $\pm p^{l-1}N(x_l)$ have at most $n_t - l$ factors from this left lower corner and hence at least $n_t - (n_t - l) = l$ terms have factor p . This gives that $v(\det(M)) = \min(v(p^{l-1}N(x_l)), v(p^l z)) = l - 1 \leq n_t - 1$. ■

Theorem 5.7: Let $C_{U, n_t} \in \mathfrak{C}_{U, n_t}$. The code C_{U, n_t} is a full rate code and satisfies the generalized rank criterion.

Proof: Let $A \in C_{U, n_t} = C_{U, n_t}(L/K, p, \sigma, m)$. We may assume that $\min(v(x_{j,1}), \dots, v(x_{j, n_t})) = 0$, for all $j = 1, \dots, U$, because otherwise we can divide extra p 's off. That does not have any impact on whether $\det(A) = 0$ or not. The determinant of A is

$$p^{-mU n_t} \prod_{l=1}^U \det(\sigma^{l-1}(M_l)) + y$$

where $v(y) \geq -m(U n_t - 2)$. We know that $v(\sigma^{l-1}(\det(M_l))) = v(\det(M_l))$ because p is from K , i.e. from the fixed field of σ , and $\det(M_l) \neq 0$ for all l . Therefore

$$v(p^{-mU n_t} \prod_{l=1}^U \det(\sigma^{l-1}(M_l))) = -kU n + \sum_{l=1}^U v(\det(M_l))$$

that is less or equal to $-mU n_t + U(n_t - 1) = U(n_t - 1 - mn_t)$ by 5.6. But if we would have $\det(A) = 0$ then

$$v(y) = v(p^{-mU n_t} \prod_{l=1}^U \det(\sigma^{l-1}(M_l)))$$

and hence $v(y) \leq U(n_t - 1 - mn_t)$ implying $-m(U n_t - 2) \leq U(n_t - 1 - mn_t)$. This gives $2m \leq U(n_t - 1)$ i.e. $m \leq \frac{U(n_t - 1)}{2}$ a contradiction. ■

Remark 5.1: Using multiblock codes from division algebras as single user codes in the MIMO MAC scenario has been done before for example in [14], [6] and [7]. In [14] the full rank condition for codes with $n_t > 1$ is achieved by using transcendental elements. In [6] the same effect is achieved with algebraic elements of high degree.

C. Examples

Let us now give a few examples of our general code constructions. In Table 1 we have collected some examples of suitable fields K and L and inert primes p , fulfilling the conditions of Proposition 5.3. If $K = \mathbb{Q}(i)$ then $p_i \mathcal{O}_K$ refers to the inert prime and if $K = \mathbb{Q}(\sqrt{-3})$ then $p_{\sqrt{-3}} \mathcal{O}_K$ is inert. The inert primes and fields L are found by looking at totally real subfields of $\mathbb{Q}(\zeta_h)/\mathbb{Q}$ and then composing them with the field K .

TABLE I

$[L : K]$	L	p_i	$p_{\sqrt{-3}}$
3	$K(\zeta_7 + \zeta_7^{-1})$	$2 + i$	$\sqrt{-3}$
4	$K(\zeta_{17} + \zeta_{17}^4 + \zeta_{17}^{-4} + \zeta_{17}^{-1})$	$2 + i$	$\sqrt{-3}$
5	$K(\zeta_{11} + \zeta_{11}^{-1})$	$1 + i$	$2 + \sqrt{-3}$
6	$K(\zeta_{13} + \zeta_{13}^{-1})$	$1 + i$	$2 + \sqrt{-3}$
7	$K(\zeta_{29} + \zeta_{29}^{12} + \zeta_{29}^{-12} + \zeta_{29}^{-1})$	$1 + i$	$\sqrt{-3}$

We get a code $C_{3,1} = C_{3,1}(\mathbb{Q}(i, \zeta_7 + \zeta_7^{-1}), 2 + i, \sigma, 1)$ i.e. 3-user code with each user having 1 antenna by setting $L = K(\zeta_7 + \zeta_7^{-1})$, $K = \mathbb{Q}(i)$, $p = 2 + i$, and $\text{Gal}(L/K) = \langle \sigma \rangle$. Now the actual code consists of matrices

$$\begin{pmatrix} p^{-1}x & \sigma(x) & \sigma^2(x) \\ y & p^{-1}\sigma(y) & \sigma^2(y) \\ z & \sigma(z) & p^{-1}\sigma^2(z) \end{pmatrix}$$

where $x, y, z \in \mathcal{O}_L^*$.

We get a code $C_{2,2} = C_{2,2}(\mathbb{Q}(\sqrt{-3}, \zeta_{17} + \zeta_{17}^4 + \zeta_{17}^{-4} + \zeta_{17}^{-1}), \sqrt{-3}, \sigma, 2)$ i.e. 2-user code with each user having 2 antennas by setting $L = K(\zeta_{17} + \zeta_{17}^4 + \zeta_{17}^{-4} + \zeta_{17}^{-1})$, $K = \mathbb{Q}(\sqrt{-3})$, $p = \sqrt{-3}$, $m = 2 > \frac{U(n_t-1)}{2}$, and $\text{Gal}(L/K) = \langle \sigma \rangle$. Now the actual code consists of matrices

$$\begin{pmatrix} p^{-2}x_1 & p^{-1}\sigma^2(x_2) & \sigma(x_1) & p\sigma^3(x_2) \\ p^{-2}x_2 & p^{-2}\sigma^2(x_1) & \sigma(x_2) & \sigma^3(x_1) \\ y_1 & p\sigma^2(y_2) & p^{-2}\sigma(y_1) & p^{-1}\sigma^3(y_2) \\ y_2 & \sigma^2(y_1) & p^{-2}\sigma(y_2) & p^{-2}\sigma^3(y_1) \end{pmatrix}$$

where $x_1, x_2, y_1, y_2 \in \mathcal{O}_L$ and $x_1 \neq 0$ or $x_2 \neq 0$ and $y_1 \neq 0$ or $y_2 \neq 0$.

VI. ON THE DECAY FUNCTION OF CODES IN \mathfrak{C}_{U,n_t}

In this section we will prove an asymptotic lower bound for the decay function of codes from \mathfrak{C}_{U,n_t} . In [5] the authors give a general asymptotic upper bound for a decay function in the case that only one user is properly using the code i.e. N_1 can be anything but $N_2 = \dots = N_U = 1$ are restricted. We will see that in this special case our codes have asymptotically the best possible decay.

Lemma 6.1: [22, Theorem 7.8.8] If $A, B \in M_n(\mathbb{C})$ are positive definite, we have

$$(\det(A + B))^{1/n} \geq \det(A)^{1/n} + \det(B)^{1/n},$$

where n is an integer.

Lemma 6.2: Let us suppose that F is an algebraic number field, $\mathcal{D} = (L/F, \tau, \gamma)$ an index n F -central division algebra and that ψ is a left regular representation of \mathcal{D} . If A is block matrix

$$A = \begin{pmatrix} A_{1,1} & \cdots & A_{1,k} \\ \vdots & & \vdots \\ A_{n,1} & \cdots & A_{k,k} \end{pmatrix}$$

where $A_{i,j} = \psi(x_{i,j})$ for some elements $x_{i,j} \in D$, we then have that

$$\det(A) \in F.$$

Proof: The matrix A can be considered as an element in the central simple algebra $M_k(\mathcal{D})$ and the determinant is then simply the reduced norm of this element. The theory of central simple algebras gives that reduced norm of any element of $M_k(\mathcal{D})$ belongs to the center. ■

In the following we use the notation of (17).

Lemma 6.3: Let $C_{U,n_t} = C_{U,n_t}(L/K, p, \sigma, m) \in \mathfrak{C}_{U,n_t}$, $A \in C_{U,n_t}$, and let F be the center of the used division algebra $\mathcal{D} = (L/F, \tau, p)$. Then for any square matrix A that consists of blocks of form $\sigma_j(M_i)$ or $p^{-m}\sigma_j(M_i)$ we have that $\det(A) \in F$.

Proof: Each of the matrices M_i in (17) are left regular representation ψ of elements x in \mathcal{D} . If $\psi(x) = M_i$, then $\psi(p^{-m}x) = p^{-m}M_i$. The isomorphisms σ^j are elements in $Gal(L/\mathbb{Q})$ and we can therefore see that for any pair i, j we have $p^{-m}\sigma_j(M_i) = \psi(y_1)$ and $\sigma_j(M_i) = \psi(y_2)$, for some $y_1, y_2 \in D$. The final result is then a direct consequence of Lemma 6.2. ■

For the next theorem we need few definitions. Let $p(x) = p_0 + p_1x + \dots + p_lx^l \in \mathbb{Z}[x]$ be a polynomial. Then we say that $H(p(x)) = \max\{|p_j|\}$ is the height of the polynomial $p(x)$ and for an algebraic number α we define $H(\alpha) = H(\phi_\alpha)$ where ϕ_α is the minimal polynomial of α . The next generalization of Liouville's theorem can be found from [11, p. 31].

Theorem 6.4: Let $\alpha \in \mathbb{R}$ be an algebraic number of degree κ , $H(\alpha) \leq h$, $H(P) \leq H$ and $\deg(P(x)) = l \in \mathbb{Z}^+$. Then either $P(\alpha) = 0$ or

$$|P(\alpha)| \geq \frac{c^l}{H^{\kappa-1}}$$

with $c = \frac{1}{3^{\kappa-1}h^\kappa}$.

Now we are ready to give a lower bound for the decay function of our codes. The proof can be seen as an extension to the analysis given for BB-code in [5].

Theorem 6.5: For a code $C_{U,n_t} \in \mathfrak{C}_{U,n_t}$ there exists constant $K > 0$ such that

$$D_{\mathcal{I}_u}(N_{i_1}, \dots, N_{i_u}) \geq \begin{cases} \frac{K}{(N_{i_1} \dots N_{i_u})^{(U-1)n_t}} & \text{if } u > 1 \\ K & \text{if } u = 1 \end{cases}$$

Especially

$$D_{\mathcal{I}_u}(N) \geq \begin{cases} \frac{K}{N^{u(U-1)n_t}} & \text{if } u > 1 \\ K & \text{if } u = 1 \end{cases}$$

Proof: If $u = 1$ then the claim is true by Proposition 5.5. Next we will prove the claim in detail in the case that $u = U$ and at the end of the proof it is explained how the proof is extended for the case $1 < u < U$.

Let $C_{U,n_t} = C_{U,n_t}(L/K, p, \sigma, m)$. Field extension L/\mathbb{Q} has a basis $S_1 \cup S_2$ where $S_1 = \{1, \delta, \delta^2, \dots, \delta^{U-1}, \beta, \beta\delta, \beta\delta^2, \dots, \beta\delta^{U-1}\}$ is a basis of F/\mathbb{Q} with $\delta \in \mathbb{R}$, $K = \mathbb{Q}(\beta)$ and $\beta = \sqrt{-w}$ for some positive integer w . Notice that if $L = F$ then $S_2 = \emptyset$.

The ring \mathcal{O}_L has a \mathbb{Z} -basis $\{\gamma_1, \dots, \gamma_{2Un_t}\}$. Each of these basis elements can be presented as

$$\gamma_l = \sum_{a \in S_1 \cup S_2} s_{l,a} a,$$

where $s_{l,a} \in \mathbb{Q}$ for all $l = 1, \dots, 2Un_t$ and $a \in S_1 \cup S_2$.

Let $A \in C_{U,n}$ be

$$\begin{pmatrix} p^{-m}M_1 & \sigma(M_1) & \dots & \sigma^{U-1}(M_1) \\ M_2 & p^{-m}\sigma(M_2) & \dots & \sigma^{U-1}(M_2) \\ \vdots & \vdots & & \vdots \\ M_U & \sigma(M_U) & \dots & p^{-m}\sigma^{U-1}(M_U) \end{pmatrix}$$

and $M_j = M(x_{j,1}, x_{j,2}, \dots, x_{j,n_t})$ be

$$\begin{pmatrix} x_{j,1} & p\tau(x_{j,n_t}) & p\tau^2(x_{j,n_t-1}) & \dots & p\tau^{n_t-1}(x_{j,2}) \\ x_{j,2} & \tau(x_{j,1}) & p\tau^2(x_{j,n_t}) & \dots & p\tau^{n_t-1}(x_{j,3}) \\ x_{j,3} & \tau(x_{j,2}) & \tau^2(x_{j,1}) & \dots & p\tau^{n_t-1}(x_{j,4}) \\ \vdots & \vdots & \vdots & & \vdots \\ x_{j,n_t} & \tau(x_{j,n_t-1}) & \tau^2(x_{j,n_t-2}) & \dots & \tau^{n_t-1}(x_{j,1}) \end{pmatrix}$$

as usual.

Now for any $j = 0, \dots, Un_t - 1$ we have

$$\sigma^j(x_{i,h}) = \sum_{l=1}^{2Un_t} u_{i,h,l} \sigma^j(\gamma_l)$$

where $u_{i,h,l} \in \mathbb{Z}$ and $|u_{i,h,l}| \leq N_i$ for all i, h and l .

Then the determinant $\det(A)$ is a sum consisting of $Un_t!$ elements of form

$$p^{-f} \prod_{j=0}^{Un_t} \sigma^j(x_{i_j, h_j}) = p^{-f} \prod_{j=0}^{Un_t} \left(\sum_{l=1}^{2Un_t} u_{i_j, h_j, l} \sigma^j(\gamma_l) \right)$$

where $f \leq kUn_t$ and i_j gets exactly n_t times all the values $1, \dots, U$ and h_j gets values from $\{1, \dots, n_t\}$.

Now substituting $\gamma_l = \sum_{a \in S_1 \cup S_2} s_{l,a} a$ gives that the determinant is a sum consisting of elements of form

$$p^{-f} \prod_{j=0}^{Un_t} \left(\sum_{l=1}^{2Un_t} u_{i_j, h_j, l} \sum_{a \in S_1 \cup S_2} s_{l,a} \sigma^j(a) \right).$$

We also write

$$\sigma^j(a) = \sum_{a \in S_1 \cup S_2} t_{j,a} a$$

where $t_{j,a} \in \mathbb{Q}$ for all j, a and find that $p^{-f} \prod_{j=0}^{Un_t} \left(\sum_{l=1}^{2Un_t} u_{i_j, h_j, l} \sum_{a \in S_1 \cup S_2} s_{l,a} \sigma^j(a) \right)$ can be written as a sum of elements of form

$$K_1 p^{-f} \sum_{a \in S_1 \cup S_2} u_a a$$

where $K_1 \in \mathbb{Q}$ is some constant, $u_a \in \mathbb{Z}$, and $u_a = \mathcal{O}((N_1 \dots N_U)^{n_t})$.

Writing also p using basis $S_1 \cup S_2$ we see that the whole determinant $\det(A)$ can be written as a sum of elements of form

$$\sum_{a \in S_1 \cup S_2} u'_a a$$

multiplied by some constant K_2 and here we have $u'_a \in \mathbb{Z}$, and $u'_a = \mathcal{O}((N_1 \dots N_U)^{n_t})$.

On the other hand we know that $\det(A) \in F$ so by uniqueness of basis representation we know that $\det(A)$ is a sum consisting of elements of form

$$\sum_{a \in S_1} u'_a a = \sum_{i=0}^{U-1} u'_{\delta^i} \delta^i + \beta \sum_{i=0}^{U-1} u'_{\delta^i \beta} \delta^i$$

and hence

$$|\det(A)| = |K_2| \left| \sum_{l=0}^{U-1} H_l \delta^l + \beta \sum_{l=0}^{U-1} J_l \delta^l \right|,$$

where $H_l, J_l \in \mathbb{Z}$ and $|H_l|, |J_l|$ are of size $\mathcal{O}((N_1 \cdots N_U)^{n_t})$ for all $l = 0, \dots, U-1$.

Using the fact that δ is real we get

$$|\det(A)| \geq \frac{K_2}{2} \left(\left| \sum_{l=0}^{U-1} H_l \delta^l \right| + \left| \sum_{l=0}^{U-1} J_l \delta^l \right| \right).$$

Now using 6.4 and noticing that $\deg(\delta) = U$ we have

$$|\det(A)| \geq \frac{K}{(N_1 \cdots N_U)^{(U-1)n_t}},$$

where K is some positive constant.

Assume now that $1 < u < U$. Write $M = M(X_{i_1}, \dots, X_{i_u})$. It is well known that

$$\text{rank}(MM^\dagger) = \text{rank}(M) = un_t$$

and hence the determinant of MM^\dagger is nonzero.

By Lemma 6.3 we see that $\det(MM^\dagger) \in F$. MM^\dagger is a matrix where the element in the place (\hat{i}, \hat{j}) where $(i-1)n_t < \hat{i} \leq in_t$ and $(j-1)n_t < \hat{j} \leq jn_t$, is of size $\mathcal{O}(N_i N_j)$. Using these facts we get the wanted result. ■

Corollary 6.6: For a code $C_{U, n_t} \in \mathcal{C}_{U, n_t}$ there exists constants $k > 0$ and $K > 0$ such that

$$\frac{k}{N^{(U-1)n_t}} \leq D(N_1 = N, N_2 = \dots = N_U = 1) \leq \frac{K}{N^{(U-1)n_t}}.$$

VII. APPENDIX

In this section we will give proofs of some results that were earlier postponed.

Lemma 7.1: Let $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_k, \mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_{k-1} \in \mathbb{C}^n$, and $\mathbf{c}_i - \mathbf{e}_i \in \mathbb{R}(\mathbf{c}_{i+1}, \mathbf{c}_{i+2}, \dots, \mathbf{c}_k)$ for $i = 1, \dots, k-1$.

Write also

$$A = \begin{pmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 \\ \vdots \\ \mathbf{c}_{k-1} \\ \mathbf{c}_k \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \\ \vdots \\ \mathbf{e}_{k-1} \\ \mathbf{c}_k \end{pmatrix}.$$

Then we have $\det(AA^\dagger) = \det(BB^\dagger)$.

Proof: If $k > n$ then $\det(AA^\dagger) = 0 = \det(BB^\dagger)$. If $k = n$ then $\det(A)$ is

$$\begin{vmatrix} \mathbf{c}_1 & & \mathbf{e}_1 & & \mathbf{e}_1 & & \mathbf{e}_1 \\ \mathbf{c}_2 & & \mathbf{c}_2 & & \mathbf{e}_2 & & \mathbf{e}_2 \\ \vdots & & \vdots & & \vdots & & \vdots \\ \mathbf{c}_{k-1} & & \mathbf{c}_{k-1} & & \mathbf{c}_{k-1} & & \mathbf{e}_{k-1} \\ \mathbf{c}_k & & \mathbf{c}_k & & \mathbf{c}_k & & \mathbf{c}_k \end{vmatrix} = \begin{vmatrix} \mathbf{e}_1 & & \mathbf{e}_1 & & \mathbf{e}_1 & & \mathbf{e}_1 \\ \mathbf{c}_2 & & \mathbf{c}_2 & & \mathbf{c}_2 & & \mathbf{c}_2 \\ \vdots & & \vdots & & \vdots & & \vdots \\ \mathbf{c}_{k-1} & & \mathbf{c}_{k-1} & & \mathbf{c}_{k-1} & & \mathbf{c}_{k-1} \\ \mathbf{c}_k & & \mathbf{c}_k & & \mathbf{c}_k & & \mathbf{c}_k \end{vmatrix} = \dots = \begin{vmatrix} \mathbf{e}_1 & & \mathbf{e}_1 & & \mathbf{e}_1 & & \mathbf{e}_1 \\ \mathbf{c}_2 & & \mathbf{c}_2 & & \mathbf{c}_2 & & \mathbf{c}_2 \\ \vdots & & \vdots & & \vdots & & \vdots \\ \mathbf{c}_{k-1} & & \mathbf{c}_{k-1} & & \mathbf{c}_{k-1} & & \mathbf{c}_{k-1} \\ \mathbf{c}_k & & \mathbf{c}_k & & \mathbf{c}_k & & \mathbf{c}_k \end{vmatrix}$$

i.e. $\det(B)$ and hence $\det(AA^\dagger) = \det(BB^\dagger)$.

Assume $k < n$. Let $\mathbf{v}_1, \dots, \mathbf{v}_{n-k} \in \mathbb{C}^n$ be such that $\mathbf{v}_1 \in \mathbb{R}(\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_k)^\perp \setminus \{\mathbf{0}\}$, $\mathbf{v}_2 \in \mathbb{R}(\mathbf{v}_1, \mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_k)^\perp \setminus \{\mathbf{0}\}$, ..., $\mathbf{v}_{n-k} \in \mathbb{R}(\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{n-k-1}, \mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_k)^\perp \setminus \{\mathbf{0}\}$. Now (as in the case $n = k$) we have

$$\det \begin{pmatrix} \mathbf{c}_1 \\ \vdots \\ \mathbf{c}_{k-1} \\ \mathbf{c}_k \\ \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_{n-k} \end{pmatrix} = \det \begin{pmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_{k-1} \\ \mathbf{c}_k \\ \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_{n-k} \end{pmatrix}$$

and hence

$$\begin{vmatrix} \mathbf{c}_1 \mathbf{c}_1^* & \dots & \mathbf{c}_1 \mathbf{c}_k^* & \mathbf{c}_1 \mathbf{v}_1^* & \dots & \mathbf{c}_1 \mathbf{v}_{n-k}^* \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{c}_k \mathbf{c}_1^* & \dots & \mathbf{c}_k \mathbf{c}_k^* & \mathbf{c}_k \mathbf{v}_1^* & \dots & \mathbf{c}_k \mathbf{v}_{n-k}^* \\ \mathbf{v}_1 \mathbf{c}_1^* & \dots & \mathbf{v}_1 \mathbf{c}_k^* & \mathbf{v}_1 \mathbf{v}_1^* & \dots & \mathbf{v}_1 \mathbf{v}_{n-k}^* \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{v}_{n-k} \mathbf{c}_1^* & \dots & \mathbf{v}_{n-k} \mathbf{c}_k^* & \mathbf{v}_{n-k} \mathbf{v}_1^* & \dots & \mathbf{v}_{n-k} \mathbf{v}_{n-k}^* \end{vmatrix}$$

is equal to

$$\begin{vmatrix} \mathbf{e}_1 \mathbf{e}_1^* & \dots & \mathbf{e}_1 \mathbf{c}_k^* & \mathbf{e}_1 \mathbf{v}_1^* & \dots & \mathbf{e}_1 \mathbf{v}_{n-k}^* \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{c}_k \mathbf{e}_1^* & \dots & \mathbf{c}_k \mathbf{c}_k^* & \mathbf{c}_k \mathbf{v}_1^* & \dots & \mathbf{c}_k \mathbf{v}_{n-k}^* \\ \mathbf{v}_1 \mathbf{e}_1^* & \dots & \mathbf{v}_1 \mathbf{c}_k^* & \mathbf{v}_1 \mathbf{v}_1^* & \dots & \mathbf{v}_1 \mathbf{v}_{n-k}^* \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{v}_{n-k} \mathbf{e}_1^* & \dots & \mathbf{v}_{n-k} \mathbf{c}_k^* & \mathbf{v}_{n-k} \mathbf{v}_1^* & \dots & \mathbf{v}_{n-k} \mathbf{v}_{n-k}^* \end{vmatrix}.$$

And since the way we chose $\mathbf{v}_1, \dots, \mathbf{v}_{n-k}$ this means that

$$\begin{vmatrix} \mathbf{c}_1 \mathbf{c}_1^* & \dots & \mathbf{c}_1 \mathbf{c}_k^* & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{c}_k \mathbf{c}_1^* & \dots & \mathbf{c}_k \mathbf{c}_k^* & 0 & \dots & 0 \\ 0 & \dots & 0 & \mathbf{v}_1 \mathbf{v}_1^* & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & \dots & \mathbf{v}_{n-k} \mathbf{v}_{n-k}^* \end{vmatrix}$$

is equal to

$$\begin{vmatrix} \mathbf{e}_1 \mathbf{e}_1^* & \dots & \mathbf{e}_1 \mathbf{c}_k^* & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{c}_k \mathbf{e}_1^* & \dots & \mathbf{c}_k \mathbf{c}_k^* & 0 & \dots & 0 \\ 0 & \dots & 0 & \mathbf{v}_1 \mathbf{v}_1^* & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & \dots & \mathbf{v}_{n-k} \mathbf{v}_{n-k}^* \end{vmatrix}$$

because if we write $\mathbf{e}_i = \mathbf{c}_i - \mathbf{x}_i$ where $\mathbf{x}_i \in L(\mathbf{c}_{i+1}, \dots, \mathbf{c}_k)$ then $\mathbf{v}_j \mathbf{e}_i^* = \mathbf{v}_j (\mathbf{c}_i - \mathbf{x}_i)^* = \mathbf{v}_j \mathbf{c}_i^* - \mathbf{v}_j \mathbf{x}_i^* = 0 - 0 = 0$ for all $i = 1, \dots, n-1$ and $j = 1, \dots, n-k$. This gives that

$$|\mathbf{v}_1|^2 \dots |\mathbf{v}_{n-k}|^2 \det(AA^\dagger) = |\mathbf{v}_1|^2 \dots |\mathbf{v}_{n-k}|^2 \det(BB^\dagger)$$

and hence $\det(AA^\dagger) = \det(BB^\dagger)$. ■

The proof of Theorem 2.5: Let us use the notation $C_l = (\mathbf{c}_{l,1}^\top, \dots, \mathbf{c}_{l,n_t}^\top)^\top$ for $l = i_1, \dots, i_u$.

Let us first fix some small $C_{i_u} \in \mathbf{L}_{i_u}(N_{i_u})$. Now $|C_{i_u}| = \mathcal{O}(1)$. Then write

$$W_{i_u} = \{(\mathbf{x}_1^\top, \dots, \mathbf{x}_{n_t}^\top)^\top \mid \mathbf{x}_i \in \mathbb{R}(\mathbf{c}_{i_u,1}, \dots, \mathbf{c}_{i_u,n_t})\}.$$

Then let $\pi_{W_{i_u}^\perp} : M_{n_t \times k}(\mathbb{C}) \rightarrow W_{i_u}^\perp$ be an orthogonal projection as before.

A subspace $W_{i_u}^\perp$ has $\dim_{\mathbb{R}}(W_{i_u}^\perp) = 2n_t k - \dim_{\mathbb{R}}(W_{i_u}) = 2n_t k - 2n_t^2 = 2n_t(k - n_t)$. By corollary 2.3 we have some $C_{i_{u-1}} \in \mathbf{L}_{i_{u-1}}(N_{i_{u-1}})$ such that

$$\|\pi_{W_{i_u}^\perp}(C_{i_{u-1}})\| = \mathcal{O}\left(N_{i_{u-1}}^{\frac{\dim_{\mathbb{R}}(W_{i_u}^\perp) - \dim_{\mathbb{R}}(\mathbf{L}_{i_{u-1}})}{\dim_{\mathbb{R}}(W_{i_u}^\perp)}}\right) = \mathcal{O}\left(N_{i_{u-1}}^{-\frac{n_t}{k-n_t}}\right).$$

Now similarly build $W_{i_{u-l}}$ for $l = 0, \dots, u-2$ by setting

$$\begin{aligned} W_{i_{u-l}} = \{(\mathbf{x}_1^\top, \dots, \mathbf{x}_{n_t}^\top)^\top \mid \mathbf{x}_i \in \mathbb{R}(\mathbf{c}_{i_u,1}, \dots, \mathbf{c}_{i_u,n_t}, \mathbf{c}_{i_{u-1},1}, \\ \dots, \mathbf{c}_{i_{u-1},n_t}, \dots, \mathbf{c}_{i_{u-l},1}, \dots, \mathbf{c}_{i_{u-l},n_t})\} \end{aligned} \quad (19)$$

This gives $\dim_{\mathbb{R}}(W_{i_u-l}^\perp) = 2n_t k - \dim_{\mathbb{R}}(W_{i_u-l}) = 2n_t k - 2n_t^2(l+1) = 2n_t(k - n_t l - n_t)$. And again, by corollary 2.3 we find $C_{i_u-l-1} \in \mathbf{L}_{i_u-l-1}(N_{i_u-l-1})$ such that

$$\begin{aligned} \|\pi_{W_{i_u-l}^\perp}(C_{i_u-l-1})\| &= \mathcal{O}\left(N_{i_u-l-1}^{\frac{\dim_{\mathbb{R}}(W_{i_u-l}^\perp) - \dim_{\mathbb{R}}(\mathbf{L}_{i_u-l-1})}{\dim_{\mathbb{R}}(W_{i_u-l}^\perp)}}\right) \\ &= \mathcal{O}\left(N_{i_u-l-1}^{-\frac{n_t l + n_t}{k - n_t l - n_t}}\right) \end{aligned}$$

where $\pi_{W_{i_u-l}^\perp} : M_{n_t \times k}(\mathbb{C}) \rightarrow W_{i_u-l}^\perp$ is an orthogonal projection as before.

Lemma 7.1 gives that if $A = (C_{i_1}^\top, \dots, C_{i_u}^\top)^\top$ and $B = (\pi_{i_2}(C_{i_1})^\top, \dots, \pi_{i_u}(C_{i_{u-1}})^\top, C_{i_u}^\top)^\top$ then $\det(AA^\dagger) = \det(BB^\dagger)$ that is of size

$$\mathcal{O}\left(\prod_{l=0}^{u-2} N_{i_u-l-1}^{-\frac{n_t l + n_t}{k - n_t l - n_t}}\right)^{2n_t} = \mathcal{O}\left(\prod_{l=1}^{u-1} N_{i_l}^{-\frac{2n_t^2(u-l)}{k - n_t(u-l)}}\right).$$

■

The proof of Theorem 4.1: Given $\mathcal{I} = \{i_1, \dots, i_u\}$, we first derive a lower bound on $d_{\min}(H_{i_1}, \dots, H_{i_u})$. Let $H_{\mathcal{I}} = [H_{i_1} \ \cdots \ H_{i_u}]$, $A_{\mathcal{I}} = \text{diag}(\kappa_{i_1} I_{n_t}, \dots, \kappa_{i_u} I_{n_t})$, $\Delta X_{\mathcal{I}} = [\Delta X_{i_1}^\top \ \cdots \ \Delta X_{i_u}^\top]^\top$, and $\Delta \tilde{X}_{\mathcal{I}} = A_{\mathcal{I}} \Delta X_{\mathcal{I}}$. Note that

$$\left\| \sum_{i \in \mathcal{I}} \kappa_i H_i \Delta X_i \right\|^2 = \text{Tr} \left(H_{\mathcal{I}}^\dagger H_{\mathcal{I}} \Delta \tilde{X}_{\mathcal{I}} \Delta \tilde{X}_{\mathcal{I}}^\dagger \right).$$

Let λ_i and ℓ_j be respectively the eigenvalues of $H_{\mathcal{I}}^\dagger H_{\mathcal{I}}$ and $\Delta \tilde{X}_{\mathcal{I}} \Delta \tilde{X}_{\mathcal{I}}^\dagger$ that are ordered as

$$\begin{aligned} 0 &= \lambda_1 = \cdots = \lambda_{un_t - K_u} < \lambda_{un_t - K_u + 1} \leq \cdots \leq \lambda_{un_t} \\ \ell_1 &\geq \ell_2 \cdots \geq \ell_{un_t} \end{aligned}$$

where $K_u = \min\{un_t, n_r\}$. For each $t \in \mathbb{Z}$, $1 \leq t \leq K_u$, we have

$$\begin{aligned} d_{\min}(H_{i_1}, \dots, H_{i_u}) &= \min_{\Delta X_{\mathcal{I}} \neq \mathbf{0}} \text{Tr} \left(H_{\mathcal{I}}^\dagger H_{\mathcal{I}} \Delta \tilde{X}_{\mathcal{I}} \Delta \tilde{X}_{\mathcal{I}}^\dagger \right) \\ &\stackrel{(a)}{\geq} \min_{\Delta X_{\mathcal{I}} \neq \mathbf{0}} \sum_{i=un_t - K_u + 1}^{un_t} \lambda_i \ell_i \geq \min_{\Delta X_{\mathcal{I}} \neq \mathbf{0}} \sum_{i=un_t - t + 1}^{un_t} \lambda_i \ell_i \\ &\stackrel{(b)}{\geq} \min_{\Delta X_{\mathcal{I}} \neq \mathbf{0}} \left[\prod_{i=un_t - t + 1}^{un_t} \lambda_i \ell_i \right]^{\frac{1}{t}} \stackrel{(c)}{\geq} \min_{\Delta X_{\mathcal{I}} \neq \mathbf{0}} \left[\prod_{i=un_t - t + 1}^{un_t} \lambda_i \right]^{\frac{1}{t}} \left[\frac{(\det(A_{\mathcal{I}}) D_{\mathcal{I}}(N_{i_1}, \dots, N_{i_u}))^2}{\prod_{i=1}^{un_t - t} \ell_i} \right]^{\frac{1}{t}} \\ &\stackrel{(d)}{\geq} \left[\prod_{i=un_t - t + 1}^{un_t} \lambda_i \right]^{\frac{1}{t}} \left[\frac{(\det(A_{\mathcal{I}}) D_{\mathcal{I}}(N_{i_1}, \dots, N_{i_u}))^2}{\text{SNR}^{un_t - t}} \right]^{\frac{1}{t}} \end{aligned}$$

where (a) follows from the mis-match inequality [23], (b) is due to the AM-GM inequality, (c) follows from the definition of $D_{\mathcal{I}}(N_{i_1}, \dots, N_{i_u})$ and that $\prod_{i=1}^{un_t} \ell_i = \det \left(A_{\mathcal{I}} \Delta X_{\mathcal{I}} \Delta X_{\mathcal{I}}^\dagger A_{\mathcal{I}} \right) \geq (\det(A_{\mathcal{I}}) D_{\mathcal{I}}(N_{i_1}, \dots, N_{i_u}))^2$, and (d) is again from the AM-GM inequality and

$$\prod_{i=1}^{un_t - t} \ell_i \leq \left(\sum_{i=1}^{un_t - t} \ell_i \right)^{un_t - t} \leq \|\Delta \tilde{X}_{\mathcal{I}}\|^{2(un_t - t)} \leq \text{SNR}^{un_t - t}.$$

Set $\lambda_{i+un_t - K_u} = \text{SNR}^{-\alpha_i}$ for $i = 1, \dots, K_u$. Below we distinguish two cases.

1) If $u > 1$, then setting $N_{i_j} = \text{SNR}^{\frac{r_{i_j}}{2n_t}}$, $\kappa_{i_j}^2 = \text{SNR}^{1 - \frac{r_{i_j}}{n_t}}$, and replacing $D_{\mathcal{I}}(N_{i_1}, \dots, N_{i_u})$ by the lower bound in Theorem 8.3 gives

$$d_{\min}(H_{i_1}, \dots, H_{i_u}) \stackrel{\cdot}{\geq} \max_{1 \leq t \leq K_u} \text{SNR}^{-\frac{1}{t} \sum_{i=K_u-t+1}^{K_u} \alpha_i} \text{SNR}^{\frac{1}{t} \sum_{j=1}^u (n_t - r_{i_j})} \times \text{SNR}^{-\frac{(U-1)}{t} \sum_{j=1}^u r_{i_j}} \text{SNR}^{-\frac{un_t-t}{t}}. \quad (20)$$

2) If $u = 1$ and $\mathcal{I} = \{i_1\}$, then similarly we have

$$d_{\min}(H_{i_1}) \stackrel{\cdot}{\geq} \max_{1 \leq t \leq K_u} \text{SNR}^{-\frac{1}{t} \sum_{i=K_u-t+1}^{K_u} \alpha_i} \times \text{SNR}^{\frac{1}{t} (n_t - r_{i_1})} \text{SNR}^{-\frac{n_t-t}{t}},$$

as $D_{\mathcal{I}}(N_{i_1}) \stackrel{\cdot}{\geq} 1$ from Theorem 8.3.

For simplicity, below we focus only on the case $u > 1$ as the analysis of the other case follows the same approach. Note that the norm $\|W\|^2$ of the noise matrix is a χ^2 random variable with $2n_r k$ degrees of freedom. Continuing from (10), we have

$$\begin{aligned} & \Pr \{ \mathcal{E}_{\mathcal{I}} \} \\ & \leq \Pr \left\{ \|W\| \geq \frac{1}{2} d_{\min}(H_{i_1}, \dots, H_{i_u}) \right\} \\ & \doteq \Pr \left\{ d_{\min}(H_{i_1}, \dots, H_{i_u}) \leq 1 \right\} \\ & \stackrel{(a)}{\doteq} \Pr \left\{ \max_{1 \leq t \leq K_u} \left\{ \sum_{i=K_u-t+1}^{K_u} (1 - \alpha_i) - U \sum_{j=1}^u r_{i_j} \right\} \leq 0 \right\} \\ & = \Pr \left\{ \sum_{i=K_u-t+1}^{K_u} (1 - \alpha_i) \leq U \sum_{j=1}^u r_{i_j}, t = 1, 2, \dots, K_u \right\} \\ & \stackrel{(b)}{\doteq} \text{SNR}^{-d_{u n_t, n_r}^* (U \sum_{i \in \mathcal{I}} r_i)}, \end{aligned}$$

where (a) follows from the lower bound on $d_{\min}(H_{i_1}, \dots, H_{i_u})$ in (20), and to establish (b) a similar derivation can be found for example in [19, p.3313]. \blacksquare

VIII. CONCLUSION

While this paper concentrated on building and analyzing codes for MIMO-MAC the mathematical methods we used and developed can hopefully be applied to varied problems related to wireless communication.

Here we have collected some of the main tools we used in this work to the following list.

- Pigeon hole principle in subspace (Section II-A).
- Use of valuation theory to achieve linear independence (Lemma 5.6).
- Use of Diophantine approximation to achieve Euclidean separation beyond linear independence (Theorem 6.5).

Besides MIMO-MAC these methods might be useful in the study of single user MIMO and interference channels.

ACKNOWLEDGEMENT

The authors would like to thank Tapani Matala-aho for his help with the Diophantine approximation.

REFERENCES

- [1] T. Ernvall and R. Vehkalahti, "Construction of MIMO MAC Codes Achieving the Pigeon Hole Bound, *Proc. 2012 IEEE Int. Symp. Inform. Theory*, Boston, USA, 2012.
- [2] D. Tse, P. Viswanath, and L. Zheng, "Diversity and multiplexing tradeoff in multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 1859–1874, 2004.
- [3] P. Coronel, M. Gärtner, and H. Bölcskei, "Selective-fading multiple-access MIMO channels, Diversity-multiplexing tradeoff and dominant outage event regions", preprint available at <http://www.nari.ee.ethz.ch/commth/pubs/p/CGB09> .
- [4] F.R. Gantmacher, *The theory of matrices*, Chelsea publishing company, New York, N.Y. 1959.
- [5] J. Lahtonen, R. Vehkalahti, H.-F. Lu, C. Hollanti, and E. Viterbo, "On the Decay of the Determinants of Multiuser MIMO Lattice Codes", *Proc. 2010 IEEE Inf. Theory Workshop*, Cairo, Egypt, Jan. 2010.
- [6] H.-F. Lu, R. Vehkalahti, C. Hollanti, J. Lahtonen, Y. Hong, and E. Viterbo, "New Space-Time Code Constructions for Two-User Multiple Access Channels", *IEEE J. Selected Topics in Signal Processing: Managing Complexity in Multiuser MIMO System*, vol. 3, no. 6, pp. 939-957, Dec. 2009.
- [7] H. F. Lu, C. Hollanti, R. Vehkalahti, J. Lahtonen, "DMT Optimal Code Constructions for Multiple-Access MIMO Channel", *IEEE Trans. Inform. Theory*, vol. 57, no. 6, pp. 3594–3617, Jun. 2011.
- [8] H. F. Lu, "Constructions of multi-block space-time coding schemes that achieve the diversity-multiplexing tradeoff", *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3790–3796, Aug. 2008.
- [9] S. Yang and J.-C. Belfiore, "Optimal space-time codes for the MIMO amplify-and-forward cooperative channel", *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 647–663, Feb. 2007.
- [10] H.-F. Lu, J. Lahtonen, R. Vehkalahti, and C. Hollanti, "Remarks on the criteria of constructing MAC-DMT optimal codes", *Proc. 2010 IEEE Inf. Theory Workshop*, Cairo, Egypt, Jan. 2010.
- [11] Andrei B. Shidlovskii, *Transcendental numbers*, Studies in mathematics, vol. 12, Walter de Gruyter, Berlin, New York, 1989.
- [12] S. Tavildar and P. Viswanath, "Approximately Universal Codes Over Slow-Fading Channels", *IEEE Trans. Inf. Theory*, vol. 52, pp. 3233–3258, July 2006.
- [13] M. Badr and J.-C. Belfiore, "Distributed Space-Time Block Codes for the MIMO Multiple Access Channel", *2008 IEEE Int. Symp. Inform. Theory*, pp. 2553–2557, July, 2008.
- [14] M. Badr and J.-C. Belfiore, "Distributed space-time block codes for the non-cooperative multiple-access channel", *Proc. 2008 International Zurich Seminar on Communication*, Zurich, Germany, pp. 132-135, Mar 2008.
- [15] M. Badr, "Codage Espace-Temps pour les Canaux MIMO à Accès Multiple", PhD thesis, 2010, available at http://pastel.archives-ouvertes.fr/docs/00/55/93/24/PDF/main_thesis.pdf
- [16] V. Tarokh, N. Seshadri, and A.R. Calderbank, "Space-Time Codes for High Data Rate Wireless Communications: Performance Criterion and Code Construction", *IEEE Trans. Inf. Theory*, vol. 44, pp. 744–765, March 1998.
- [17] M. E. Gärtner and H. Bölcskei, "Multiuser Space-Time/Frequency code design", *2006 IEEE Int. Symp. Inform. Theory*, pp. 2819–2823, July 2006.
- [18] L. Zheng and D. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple antenna channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.
- [19] S. A. Pawar, K. R. Kumar, P. Elia, P. V. Kumar, and B. A. Sethuraman, "Space-time codes achieving the DMD tradeoff of the MIMO-ARQ channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3101–3114, Jul. 2009.
- [20] H. F. Lu, Y. Wang, P. V. Kumar, and K. M. Chugg, "Remarks on space-time codes including a new lower bound and an improved code," *IEEE Trans. Inf. Theory*, pp. 2752–2757, Oct. 2003.
- [21] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H.-F. Lu, "Explicit construction of space-time block codes achieving the diversity-multiplexing gain tradeoff," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3869–3884, Sep. 2006.
- [22] R. Horn and C. Johnson, *Matrix analysis*, Cambridge university press, Cambridge, 1990.
- [23] C. Köse and R. D. Wesel, "Universal space-time trellis codes", *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp. 2717–2727, Oct. 2003.