On the Decay of the Determinants of Multiuser MIMO Lattice Codes

Jyrki Lahtonen, Roope Vehkalahti, Hsiao-feng (Francis) Lu, Camilla Hollanti, and Emanuele Viterbo

***Abstract*— In a recent work, Coronel *et al.* initiated the study of the relation between the diversity-multiplexing tradeoff (DMT) performance of a multiuser multiple-input multiple-output (MU-MIMO) lattice code and the rate of the decay of the determinants of the code matrix as a function of the size of the signal constellation. In this note, we state a simple but general upper bound on the decay function and study the promising code proposed by Badr & Belfiore in close detail. We derive a lower bound to its decay function based on a classical theorem due to Liouville. The resulting bound is applicable also to other codes with constructions based on algebraic number theory. Further, we study an example sequence of small determinants within the Badr–Belfiore code and derive a tighter upper bound to its decay function. The upper bound has certain conjectural asymptotic uncertainties, whence we also list the exact bound for several finite data rates.**

I. Background and the decay function

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

Any study of DMT questions calls for a scalable set of finite signal constellations. For the sake of convenience most authors assume that the signal sets of individual users are carved out from a user specific lattice $\mathbf{L}_j \subset \mathcal{M}_{n_t \times Un_t}, j = 1, \ldots, U$.

When studying DMT questions it is natural to assume that each user is maximally using the degrees of freedom available to him/her. Therefore, the lattices of the individual users should be of full rank $n = 2Un_t^2$, so that each user's signals consist of integral linear combinations of n user specific basis matrices. A natural scaling parameter is the range of the integer coefficients. We assume that the range is parameterized by a natural number N. Specifically, for the jth user, let $\mathbf{B}_{j,1}, \cdots, \mathbf{B}_{j,n}$ be a basis for the lattice $\mathbf{L}_j$ of the jth user. Then the code associated with the jth user is given by

$$\mathcal{X}_j \;=\; \left\{ X_j \;=\; \sum_{i=1}^{n} b_i \mathbf{B}_{n,i} \;:\; b_i \in \mathbb{Z}, -N \le b_i \le N \right\} \quad (1)$$

where each coefficient $b_i, i = 1, \ldots, n$, can be freely chosen from the interval $[-N, N]$. Alternatively, an N-PAM coordinate set could be used. What is essential for our study is that the set of available signals for a certain user is of the order $\mathcal{O}(N^n)$. Our bounds are blind to constant multipliers, so for example using a spherically shaped signal set instead will not matter. A QAM-oriented reader may then view encoding as linear dispersion of $\frac{n}{2} = Un_t^2$ independently chosen N^2-QAM symbols. On the other hand, each user may transmit at a different rate or, equivalently, have his/her own rate parameter. We denote these by $N_1, N_2, \ldots, N_U$, and by $\mathbf{L}_j(N_j)$ the finite signal constellation obtained by restricting the coefficients of the basis matrices of lattice $\mathbf{L}_j$ to have absolute value at most N_j.

Typical values of N_j are set in terms of the DMT. Assume that the jth user transmits at the multiplexing gain r_j. It in turn means that the size of $\mathcal{X}_j$ equals

$$|\mathcal{X}_j| \;=\; \mathrm{SNR}^{r_j U n_t}.$$

Note that by definition $|\mathcal{X}_j| \;=\; (N_j)^n$ and $n = 2Un_t^2$. Hence to achieve multiplexing gain r_j for the jth user we have to set

$$N_j \;=\; \mathrm{SNR}^{\frac{r_j}{2n_t}}. \quad (2)$$

We will discuss the code $\mathcal{X}_j$ in greater detail when we examine the DMT performance of the Badr-Belfiore code in Section IV.

An important class of error events is formed by those, where the receiver is about to make an error in estimating every user's signal. This is dominating the system performance in some cases, because with even a relatively well designed code the channel state may make the received linear combination of individual error vectors cancel each other out to a significant extent. Such a cancellation is easier to arrange when all the users are using a large codebook at the same time corresponding to the cases, where all the users are transmitting at a relatively high rate. The standard PEP-driven space-time analysis shows that the probability of such an error event can be related to the determinant of the matrix $X := M(X_1, X_2, \ldots, X_U) = \begin{pmatrix} X_1^T & X_2^T & \cdots & X_U^T \end{pmatrix}^T$, where the $n_t \times Un_t$ block X_j from user $\#j$ is a non-zero matrix $\in \mathbf{L}_j$. The following quantity is then of interest:

$$D(N_1, N_2, \ldots, N_U) = \min_{X_j \in \mathbf{L}_j(N_j) \setminus \{0\}} |\det M(X_1, \ldots, X_U)|.$$

As a natural special case, when all the users are transmitting at exactly the same rate, we give special attention to the function

$$D(N) = D(N_1 = N, ..., N_U = N).$$

We call both these functions the *decay function* of the MU-MIMO code $(\mathbf{L}_j),\ j = 1, \ldots, U$. We have tacitly made the assumption that the code designer has provided us with a form of a generalized *rank criterion* stating that the matrix $M(X_1, X_2, \ldots, X_U)$ has full rank, whenever all the blocks $X_j, j = 1, 2, \ldots, U$, are non-zero. Under the (generalized)

rank criterion the decay function will then only take non-zero values.

Is this a misnomer? After all, in the single user MIMO code, lattices within cyclic division algebras such as the Golden code and the Golden+ code enjoy the so called non-vanishing determinant (NVD) property stating that there is an absolute constant $\omega > 0$ with the property that $D(N) > \omega$ for all values of N. In [1] it was shown that the NVD-property guarantees the DMT-optimality of a single user code. As we shall see shortly, this is not possible in the multiuser case, and the determinants will necessarily tend toward zero (under the assumption of the generalized rank criterion[1]).

A natural goal for the research in MU-MIMO channels would be to have at hand both an explicit criterion guaranteeing the DMT-optimality of the family of lattices $(\mathbf{L}_j), j = 1, 2, \ldots, U$, **and** a class of constructions meeting this criterion.

Progress in these questions has been made in [4], [3], [2], and it is easy to believe that a condition expressed in terms of the decay function is also out there [4]. In this note we state some interesting results from [5] about the available decay functions of all MU-MIMO lattice codes in general. Based on them, and as the main contribution of this paper, we study in particular the decay function of the code proposed by Badr & Belfiore (BB-code, in short).

What kind of decay functions should one expect? We have shown in [5] that inverse polynomial decay is forced upon us. All our upper and lower bounds for $D(N)$ are of the form $CN^{-\delta}$, where $\delta > 0$ is a real constant.

Definition 1.1: If the decay function of a MU-MIMO code has an upper bound of the form $D(N) \leq C_u N^{-\delta_1}$, we say that the determinants of this code decay with exponent at least δ_1. Similarly, if the decay function has a lower bound of the form $D(N) \geq C_\ell N^{-\delta_2}$, then we say that the decay exponent is at most δ_2. Finally, if for a particular code we find lower and upper bounds of the form $C_\ell N^{-\delta} \leq D(N) \leq C_u N^{-\delta}$, we say that the determinants of this code *decay with exponent* δ.

Of course, asymptotically we prefer a code with a smaller decay exponent. Equivalently, we say that the code decays with exponent δ whenever $\lim_{N\to\infty} -\frac{\log D(N)}{\log N} = \delta$.

As a word of caution, it is not at all clear that any code has a well defined decay exponent. For example, it may be that one only gets results for limes superior or limes inferior here.

One of our main results is to show that in the case of the BB-code we can find positive constants C_ℓ and C_u such that for this promising code we have the bounds

$$\frac{C_\ell}{N^2} \leq D(N) \leq \frac{C_u}{N^{5/3}}.$$

We also give reasoning for our conjecture that, asymptotically, for very large N we expect $\delta = 2$. In other words the determinants decay by the inverse square law. We view this as good news for the BB-code. Its decay function is under control in this sense. It would not surprise us if further work on this topic would show that the inverse square decay is essentially the best possible when $U = 2$ and $n_t = 1$.

Let us now state two theorems from [5] that will be used for studying the BB-code. Both theorems are based on the pigeon hole principle.

Theorem 1.1: (Pigeon hole bound, multiantenna case) For any full-rate U-user code, each user transmitting with n_t antennas, there exists a constant $K > 0$ such that

$$D(N_1 = N, N_2 = N_3 = \cdots = N_U = 1) \leq \frac{K}{N^{(U-1)n_t}}.$$

In other words, the determinants of any full-rate U-user n_t-antenna code decay with exponent at least $(U-1)n_t$.

Theorem 1.2: (Pigeon hole bound, single antenna case) For any full-rate U-user code $(\mathbf{L}_1, \mathbf{L}_2, \ldots, \mathbf{L}_U)$ with $n_t = 1$ there exists a constant $K > 0$ such that

$$D(N_1 = N, N_2 = N_3 = \cdots = N_U = 1) \leq \frac{K}{N^{U-1}}.$$

In other words the determinants of any single transmit antenna full-rate U-user code decay with exponent $\delta \geq U - 1$.

II. A lower bound to the decay of the Badr–Belfiore code

Let us recall the code construction from [6]. See also equation (49) in [4]. This promising code is expressed in terms of certain algebraic number fields. Everything happens inside the field $E = \mathbf{Q}(i, \sqrt{5})$. We shall also encounter its subfields $F_1 = \mathbf{Q}(i)$, $F_2 = \mathbf{Q}(\sqrt{5})$ and $F_3 = \mathbf{Q}(i\sqrt{5})$. The respective rings of algebraic integers of these quadratic fields are $\mathcal{O}_1 = \mathbf{Z}[i]$, $\mathcal{O}_2 = \mathbf{Z}[\tau]$ and $\mathcal{O}_3 = \mathbf{Z}[i\sqrt{5}]$, where $\tau = (1+\sqrt{5})/2$ is the golden ratio. The ring of integers $\mathcal{O}_E = \mathbf{Z}[i, \tau]$ of E then consists of numbers of the form $(a+bi)+(c+di)\tau$, where a, b, c, d are any rational integers.

The Galois group $G = \mathrm{Gal}(E/\mathbf{Q})$ has four elements: $1_G; \rho : i \mapsto -i,\ \sqrt{5} \mapsto \sqrt{5}$; $\sigma : i \mapsto i,\ \sqrt{5} \mapsto -\sqrt{5}$, and $\mu = \sigma\rho = \rho\sigma :\ i \mapsto -i,\ \sqrt{5} \mapsto -\sqrt{5}$. The respective fixed fields of σ, ρ and μ are F_1, F_2, and F_3.

We are now ready to describe the BB-code. It fits into our general framework with parameters $U = 2$ and $n_t = 1$ so it is a single-antenna two-user code. Both users linearly disperse two Gaussian integers. User $\#j$ first combines the Gaussian integers $z_{1j}, z_{2j} \in \mathcal{O}_1$ into an element $x_j = z_{1j} + z_{2j}\tau$ of the ring $\mathcal{O}_E$. Then the users' encoding methods differ a little bit, and user $\#1$ transmits the vector $(x_1, \sigma(x_1))$, whereas the user $\#2$ transmits the vector $(\gamma x_2, \sigma(x_2))$. In [6] and [4] it is explained that the choice $\gamma = i$ results in a code that satisfies the generalized rank criterion. In other words, the composite matrix

$$X = \begin{pmatrix} x_1 & \sigma(x_1) \\ \gamma x_2 & \sigma(x_2) \end{pmatrix} \tag{3}$$

is invertible, whenever both x_1 and x_2 are non-zero.

Following [4], the determinant under study here is

$$\det(X) = x - \gamma\sigma(x) = x - i\sigma(x),$$

where $x = x_1\sigma(x_2)$. Next we describe our finite constellations more precisely. Let $(a_j, b_j, c_j, d_j) \in \mathbf{Z}^4$ correspond to the signal transmitted by user $\#j$, $j = 1$ or $j = 2$. In other words,

[1] It has been shown that in order to design DMT-optimal MAC codes, one does not necessarily need to keep up with the generalized rank criterion. It is enough to satisfy the so-called conditional NVD property, see [2], [3] for details. Naturally for such codes $D(N) = 0$, so they are not of interest here.

$z_{1j} = a_j + ib_j$ and $z_{2j} = c_j + id_j$. Then the constellations $\mathbf{L}_1(N)$ and $\mathbf{L}_2(N)$ are obtained from the above constructions by restricting the integer coefficients a_j, b_j, c_j, d_j ($j = 1$ or 2) into the range $[-N, N]$.

The determinant will now be of the form

$$\det(X) = (R + S\tau) + (T + V\tau)i,$$

where R, S, T, V are quadratic homogeneous polynomials with integer coefficients in the 8 integer unknowns $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2$. The result stating that $\det(X) \neq 0$ can be rewritten in the form that these four polynomials cannot vanish simultaneously, unless the input from one of the users is all zeros. As we shall see, our estimate on the decay rate will depend on the size of the integer coefficients R, S, T, V. We note the following obvious lemma without proof.

Lemma 2.1: There exists a constant $K_1 > 0$ such that for all $x_1 \in \mathbf{L}_1(N_1)$, $x_2 \in \mathbf{L}_2(N_2)$ we have the upper bounds $|S| < K_1 N_1 N_2$ and $|V| < K_1 N_1 N_2$.

We remark here that further limiting the choices of the inputs of individual users (for example to the ideal of the ring of integers of E used in the construction of the Golden code) amounts to placing a family of congruences that the input vector (a, b, c, d) must satisfy. This will not change anything in what follows. After all, then the desired single user constellation will be a subset of a set of the form $\mathbf{L}(\alpha N)$, where $\alpha >$ is a constant that does not depend on N. Thus our estimates will also be valid for such constellations, because the contribution from α can be absorbed into the coefficient K_1 (by replacing it with another positive constant). Neither will replacing i with another non-norm element γ affect our conclusions — albeit naturally all the calculations have to be carried out separately for each γ.

We already know from the pigeon hole bound that for some constant C the decay function of the BB-code has an upper bound of the form $D(N_1, N_2) \leq K/\max\{N_1, N_2\}$ for some constant $K > 0$, i.e., the determinant decays with exponent at least $\delta \geq 1$.

For a badly chosen code the decay could be very fast indeed. We shall next show that the number theoretic structure of the BB-code can be used to derive an inverse polynomial lower bound. Thus this code is promising in the sense that it belongs to a class of MU-MIMO codes with inverse polynomial decay.

A. Approximating τ by rational numbers

It is known that it is impossible to approximate algebraic integers too well by rational numbers in the sense made precise by the following result by Liouville[2]. Similar methods have been used in e.g. [7], [8].

Theorem 2.2: ([9, p.146], Liouville's approximation theorem) Let θ be a real algebraic number of degree $n \geq 2$. Then there is a positive constant $C(\theta)$, depending only on θ, such that for all integers h and k with $k > 0$ we have

$$\left|\theta - \frac{h}{k}\right| > \frac{C(\theta)}{k^n}.$$

As an immediate corollary we get the following.

Corollary 2.3: There exists a constant C such that for all integers h and k with $k > 0$ we have $|k\tau - h| > \frac{C}{k}$.

As a corollary of Lemma 2.1 and Corollary 2.3 we get our main result:

Theorem 2.4: There exists a constant $K > 0$ such that for all sufficiently large N_1, N_2 we have $D(N_1, N_2) \geq \frac{K}{N_1 N_2}$. In particular as $N \to \infty$, we get a decay estimate $D(N) \geq \frac{K}{N^2}$. In other words the decay of the BB-code has a lower bound corresponding to an estimate of the decay exponent $\delta \leq 2$.

We want to remark that the result of Corollary 2.3 is essentially the best possible. For example, it is impossible to replace the exponent 1 of the parameter k in the denominator with a larger number. This is because a simple application of the pigeon hole principle tells us that there are infinitely many integer pairs (h, k) such that $|k\theta - h| < \frac{1}{k}$ for *any* irrational real number θ.

III. More on the decay exponent of the Badr–Belfiore code

We already know that the decay exponent of the BB-code is in the interval $[1, 2]$. As the pigeon hole bound has the air of suboptimality, we seek to replace it with something tighter for this specific code.

A. An example sequence of small determinants in Badr–Belfiore code

In this section we study a sequence of determinants appearing in the BB-code that converges towards zero. The example utilizes the fact that, within the ring $\mathcal{O}_2$, there are arbitrary small numbers. For example, because $|2 - \sqrt{5}| \approx 0.2369 < 1/4$, its powers $(2-\sqrt{5})^n = a_n - b_n\sqrt{5}$ can be made as small as required.

Let us consider the case $x_2 = 1$ and $x_1 = a + b\sqrt{5}i$, where $a, b \in \mathbf{Z}$. Then $x = x_1, \sigma(x) = a - b\sqrt{5}i$, so $\det(X) = x - i\sigma(x) = (a - b\sqrt{5})(1 - i)$.

In order to make this as specific as possible, let us study the sequence of such matrices X_n with $a = a_n$, $b = b_n$, where for all $n > 0$ the integers a_n and b_n are determined by the equation $a_n - b_n\sqrt{5} = (2 - \sqrt{5})^n$. We remark that this is by no means the only sequence we could consider to achieve our goal. We can form other such sequences by multiplying this with constants and also use other small algebraic integers: any pair $(a, b) \in \mathbf{Z}^2$ such that $(a - b\sqrt{5})$ is small will yield small determinants by this construction.

The number $\alpha = 2 + \sqrt{5} = \tau^3$ is a unit in the ring $\mathbf{Z}[\tau]$. Its norm is $N_{\mathbf{Q}}^{F_2}(\alpha) = \alpha\sigma(\alpha) = (2 - \sqrt{5})(2 + \sqrt{5}) = -1$, and hence $\sigma(\alpha) = 2 - \sqrt{5} = -1/\alpha$. This norm equation gives us the identity $a_n^2 - 5b_n^2 = (-1)^n$ that is valid for all integers $n > 0$. At this time we infer from this formula that $|b_n| < |a_n|$ for all $n > 0$.

We also have use for the trace function $tr_{\mathbf{Q}}^{F_2} : F_2 \to \mathbf{Q}, x \mapsto x + \sigma(x)$. For example, as $\sigma(a_n - b_n\sqrt{5}) = a_n + b_n\sqrt{5}$, we

[2]For more general real algebraic numbers one should asymptotically use a deep result due to K. F. Roth stating that the exponent n can be replaced with an exponent of the form $2 + \epsilon$ for any $\epsilon > 0$. The price one pays when doing this is that one no longer has any means of estimating the constant in the numerator. For asymptotic work Roth's result is obviously superior.

get the formula $2a_n = tr_{\mathbf{Q}}^{F_2}(\alpha^n) = \alpha^n + (-1/\alpha)^n$. In this formula the second term always has absolute value < 1, so the first term dominates for large values of n, and we get the asymptotic formula $a_n \approx \frac{1}{2}(2+\sqrt{5})^n$. We shall also need an explicit expression of b_n in terms of α, and the following formula is immediate from the definitions $2\sqrt{5}b_n = \alpha^n - (-1/\alpha)^n$.

Now if we set in the BB-code $x_2 = 1$ and $x_1 = z_n = a_n + i\sqrt{5}b_n$, then the logarithm of the resulting determinant looks like $\log|\det(X)| = \log|(1+i)(2-\sqrt{5})^n| = \log\sqrt{2} + n\log|2-\sqrt{5}| = \frac{\log 2}{2} - n\log\alpha$.

At the same time the range parameter N grows as $\log N = n\log\alpha - \log 2$. Therefore with this example sequence we get the limit $\lim_{n\to\infty}\frac{\log|\det(X)|}{\log N} = -1$.

Thus this example sequence of matrices simply makes the single antenna pigeon hole bound explicit for the BB-code. The obvious route to a better upper bound for the decay function $D(N)$ of the BB-code is to use this sequence of determinants, but to split the energy more evenly between the two users. After all, here (as in our proof of the pigeon hole bound) one user was stuck with a low rate signal, while the other user's data rate was unbounded. To do this we want to write the numbers $z_n = a_n + i\sqrt{5}b_n$ in the form $z_n = x_1\sigma(x_2)$, where x_1 and x_2 would both use, if not equal then at least comparable, amounts of transmission power. While we cannot do this for all the numbers z_n, a useful factorization exists, when $5|n$. This is the topic of the following subsection.

B. Certain factorizations in $\mathcal{O}_E$

Let $\zeta = e^{2\pi i/5}$ be a fifth root of unity. Our field of interest E is a subfield of the twentieth cyclotomic field $L = \mathbf{Q}(i,\zeta)$, and $[L:E] = 2$. This follows from the fact that $-\zeta - \zeta^{-1} = -2\cos(2\pi/5) < 0$ is a zero of the polynomial $x^2 - x - 1 = (x-\tau)(x-1+\tau)$, and hence $\tau = \zeta + 1 + \zeta^{-1}$.

The degree $[L:\mathbf{Q}] = 8$ follows from the fact that the minimal polynomial of any primitive twentieth root of unity, such as $i\zeta$, is $\phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1$. This is, perhaps, easiest to see starting with the factorization $p(x) := x^{10} + 1 = (x^2+1)\phi_{20}(x)$.

There is an automorphism ν of L that is determined by $i \mapsto i, \zeta \mapsto \zeta^{-1}$. We immediately see that ν is of order two, and that E is the fixed field of ν. So if w is any root of unity of order 20, then the polynomial $(x-w)(x-\nu(w))$ has coefficients in the field E. Using this we arrive at the following factorization of $\phi_{20}(x)$ into irreducible factors in the ring $E[x]$: $\phi_{20}(x) = p_1(x)p_2(x)p_3(x)p_4(x)$, where

$$\begin{aligned}
p_1(x) &= (x-i\zeta)(x-i\zeta^{-1}) = x^2 + i(1-\tau)x - 1,\\
p_2(x) &= (x+i\zeta)(x+i\zeta^{-1}) = x^2 - i(1-\tau)x - 1,\\
p_3(x) &= (x-i\zeta^2)(x-i\zeta^{-2}) = x^2 + i\tau x - 1,\\
p_4(x) &= (x+i\zeta^2)(x+i\zeta^{-2}) = x^2 - i\tau x - 1.
\end{aligned}$$

The task at hand is to factorize the number $z_n = a_n + i\sqrt{5}b_n$. The symmetries of these numbers become more apparent, if we take a detour via $\mathbf{Q}$: we start by considering the $F_3 \to \mathbf{Q}$ norm $z_n\rho(z_n) = a_n^2 + 5b_n^2 = a_{2n} = \frac{1}{2}\left(\alpha^{2n} + \alpha^{-2n}\right)$.

As before, here $\alpha = 2+\sqrt{5}$, so $\mu(\alpha) = \sigma(\alpha) = 2-\sqrt{5} = -1/\alpha$. The number $u = \alpha^{2n}$ will appear frequently in our calculations. We start our work on z_{5n} with

$$\begin{aligned}
\frac{a_{10n}}{a_{2n}} &= \frac{\alpha^{10n}+\alpha^{-10n}}{\alpha^{2n}+\alpha^{-2n}} = \frac{u^5+u^{-5}}{u+u^{-1}} = \frac{u^{-4}(u^{10}+1)}{u^2+1}\\
&= u^{-4}\phi_{20}(u) = m_1(n)m_2(n)m_3(n)m_4(n),
\end{aligned}$$

where for $j = 1,2,3,4$ we denote $m_j(n) = u^{-1}p_j(u) = \alpha^{-2n}p_j(\alpha^{2n}) \in \mathcal{O}_E$.

As $\mu(u) = 1/u$, we have for example

$$\mu(m_1(n)) = \mu(u + i(1-\tau) - u^{-1}) = u^{-1} - i\tau - u = -m_3(n).$$

Similarly $\mu(m_2(n)) = -m_4(n)$. As $\mu^2 = 1$ in the Galois group, we get that $m_1(n)m_3(n)$ and $m_2(n)m_4(n)$ are invariant under μ, and hence are integers in the field F_3. Thus we may expect that one of these pairs is a factor of z_{5n}.

We need one more pair of polynomial factorizations, this time in the ring $\mathcal{O}_1 = \mathbf{Z}[i]$:

$$x^5 \pm i = (x \pm i)(x^4 \mp ix^3 - x^2 \pm ix + 1). \tag{4}$$

These arise similarly from factoring $x^{20} - 1$, or rather its factors $x^5 + i$ and $x^5 - i$ respectively, in $F_1[x]$. They are needed in the following lemma that is the main result of this subsection.

Lemma 3.1: The number z_{5n} is always divisible by z_n and can be factored in the ring $\mathcal{O}_E$ as $z_{5n} = z_n m_2(n)m_4(n)$, when n is odd, and as $z_{5n} = z_n m_1(n)m_3(n)$, when n is even.

Proof: Both of these identities follow from the earlier expressions for a_n and b_n in terms of powers of α. These may be compressed into formula $z_n = \frac{1}{2}(1+i)(\alpha^n - i(-1/\alpha)^n)$. Using our earlier abbreviation $u = \alpha^{2n}$, we see that

$$\begin{aligned}
m_2(n)m_4(n) &= u^2 - iu - 1 + iu^{-1} + u^{-2},\\
m_1(n)m_3(n) &= u^2 + iu - 1 - iu^{-1} + u^{-2}.
\end{aligned}$$

Let us consider the case n odd. We can write $z_n = \alpha^{-n}(1+i)(u+i)/2$. We also see that $m_2(n)m_4(n) = \alpha^{-4n}(u^4 - iu^3 - u^2 + iu + 1)$. Therefore the claim follows from the first of the above polynomial factorizations by substituting $x = u$. The even case follows similarly from the second polynomial factorization. ∎

C. Sharper upper bounds to the decay function of the Badr–Belfiore code and numerical data

Let us take a closer look at the factorization in Lemma 3.1. We want to say something about the sizes of the coordinates of these algebraic integers with respect to the integral basis $\{1, i, \tau, i\tau\}$. From all the previous identities it immediately follows that the coordinates of the factors $m_j(n), j = 1,2,3,4$, have absolute values bounded from above by a constant multiple of α^{2n}. Therefore the coordinates of $x_1 = z_n m_j(n)$ ($j = 1$ or $j = 2$) can be approximated by a constant multiple of α^{3n}, and the coordinates of $x_2 = \sigma(m_{j+2}(n))$ by a constant multiple of α^{2n}. Recall that these choices yield a determinant of absolute value $\sqrt{2}\alpha^{-5n}$.

As any size parameter N can be approximated up to a constant ($< \alpha^5$) multiplier with a power of α^5, we have the following result.

Corollary 3.2: There exists such a constant $K > 0$ that for all N the decay of the BB-code has an upper bound

$$D(N^{3/5}, N^{2/5}) \leq \frac{K}{N}.$$

In particular, the decay exponent δ has the estimates

$$5/3 \leq \delta(\text{BB-code}) \leq 2.$$

One way of getting better upper bounds for the decay exponent is to apply Lemma 3.1 repeatedly. After all, we get an even better balance between the factors x_1 and x_2, when n is a multiple of 25, because in the factorization $z_{25n} = z_{5n} m_j(5n) m_{j+2}(5n)$ we can factor z_{5n} further.

Observe that when doing this, we effectively restrict our scale to the sizes $a_1, a_5, a_{25}, a_{125}, \ldots$. Thus we lose the ability to estimate (up to a constant multiplier) an arbitrary scale parameter N by a member of this sequence. Therefore the following result is stated in terms of limes superior.

Corollary 3.3: For the BB-code we get the result

$$\limsup_{N\to\infty} -\frac{\log D(N,N)}{\log N} = 2.$$

We conclude this section by a table of numerical results based on the above factorization. Two things are obvious. The multiples of 25 stand out. Note also that the coordinates of these factors are quite large (but the determinant is then correspondingly very small), and surely beyond the range of all ongoing simulations.

TABLE I
SOME SMALL DETERMINANTS IN BB-CODE AND ESTIMATES OF δ

n	$m =$ max size of x_i a factor of z_n	$\delta = -\log\det(X)/\log m$
5	38	1.889
10	2880	1.769
15	219640	1.732
20	16692480	1.715
25	66563198	1.984

IV. DMT PERFORMANCE OF THE BADR-BELFIORE CODE

Recall that in Section II, the rows of the BB code are formed by the lattices associated with each user with coordinates a_j, b_j, c_j, d_j, $j = 1, 2$, lying within the range $[-N, N]$. Thus, following from (2), assuming the users are to achieve multiplexing gain $r_1 = r_2 = r$, the corresponding value for N is

$$N \doteq \text{SNR}^{\frac{r}{2}},$$

since $n_t = 1$. Furthermore, as the elements τ and γ are fixed and do not vary with SNR, it is straightforward to see that the overall BB-code matrix X in (3) has average power $\mathbb{E}\|X\|^2 \doteq N^2 = \text{SNR}^r$.

In [4] Coronel *et al.* had provided some initial DMT analysis of the BB code. They showed that the BB code will be MAC-DMT optimal if the following inequality is satisfied

$$2r + \delta \leq r_{\mathcal{S}}\left(d_{\mathcal{S}^*}\left(r\left(\mathcal{S}^*\right)\right),\right) \tag{5}$$

where $r_{\mathcal{S}}\left(d_{\mathcal{S}^*}\left(r\left(\mathcal{S}^*\right)\right)\right)$ is the maximum of the sum of multiplexing gains of users in set $\mathcal{S}$ such that the dominant diversity gain $d^*(r) = d_{\mathcal{S}^*}\left(r\left(\mathcal{S}^*\right)\right) = \max\left\{d^*_{1,2}(r), d^*_{2,2}(2r)\right\}$ can be achieved. $\mathcal{S}^*$ is the set of the users that is dominant in the DMT error performance. Specifically, $\mathcal{S}^* = \{1\}$ for $r \in [0, \frac{2}{3}]$ and is called single-user performance region in [10]. For $r \in \left[\frac{2}{3}, 1\right]$ we have $\mathcal{S}^* = \{1, 2\}$ and this is termed the antenna-pooling region. $d^*_{p,q}(x)$ is the point-to-point DMT with p transmit and q receive antennas given multiplexing gain x given in [11]. Note that $d^*_{1,2}(x) = 2 - 2x$ for $x \in [0, 1]$, $d^*_{2,2}(x) = 4 - 3x$ for $x \in [0, 1]$, and $d^*_{2,2}(x) = 2 - x$ for $x \in [1, 2]$. To achieve diversity gain $d^*(r) = 2 - 2r$, it is easy to show that for $\mathcal{S} = \{1, 2\}$ we have

$$r_{\mathcal{S}}\left(d_{\mathcal{S}^*}\left(r\left(\mathcal{S}^*\right)\right)\right) = \begin{cases} \frac{2+2r}{3}, & r \in \left[0, \frac{1}{2}\right] \\ 2r, & r \in \left[\frac{1}{2}, 1\right] \end{cases}.$$

The other parameter δ shown in (5) is defined as

$$\delta := -\limsup_{\text{SNR}\to\infty} \log_{\text{SNR}} \min_{X \neq X'} \left|\det\left(X - X'\right)\right|^2$$

where X and X' are distinct overall matrices of the BB-code. In terms of $D(N, N)$, we asymptotically have (SNR $\to \infty$)

$$\delta = -\log_{\text{SNR}} |D(N,N)|^2 = \log_{\text{SNR}} N^4 = 2r,$$

where the second equality follows from Corollary 3.3, and where we have set $N = \text{SNR}^{\frac{r}{2}}$ such that both users achieve multiplexing gain r. Putting all of the above together into (5) shows that the BB code is MAC-DMT optimal when the multiplexing gain falls in the interval $\left[0, \frac{1}{5}\right]$, but fails to achieve the condition (5) by Coronel *et al.* for $r \geq \frac{1}{5}$. We summarize the above in the following result.

Theorem 4.1: The BB-code is MAC-DMT optimal (at least) when the multiplexing gain $r \leq \frac{1}{5}$.

REFERENCES

[1] 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.

[2] H.-F. Lu and C. Hollanti, "Diversity-multiplexing tradeoff-optimal code constructions for symmetric MIMO multiple access channels," in *Proc. 2009 IEEE Int. Symp. Inform. Theory*, Seoul, South Korea, Jul. 2009.

[3] C. Hollanti, H.-F. Lu, and R. Vehkalahti, "An algebraic tool for obtaining conditional non-vanishing determinants," in *Proc. 2009 IEEE Int. Symp. Inform. Theory*, Seoul, South Korea, Jul. 2009.

[4] Coronel, Gärner, and Bölcskei, "Selective-fading multiple-access MIMO channels: Diversity multiplexing tradeoff and dominant outage event regions," submitted 2009, available from ArXiv.

[5] H.-F. Lu, J. Lahtonen, R. Vehkalahti, and C. Hollanti, "Remarks on the criteria of constructing MAC-DMT optimal codes," to appear in *Proc. 2010 IEEE Inf. Theory Workshop*, Cairo, Egypt, Jan. 2010. Available from ArXiv.

[6] M. Badr and J.-C. Belfiore, "Distributed space-time block codes for the non-cooperative multiple-access channel," in *Proc. 2008 International Zurich Seminar on Communication*, Zurich, Germany, Mar. 2008, pp. 132–135.

[7] M. O. Damen and N. C. Beaulieu, "On two high-rate algebraic space-time codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 1059– 1063, Apr. 2003.

[8] M. O. Damen, A. Tewfik, and J.-C. Belfiore, "A construction of a space-time code based on number theory," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 753–760, Mar. 2002.

[9] T. A. Apostol, *Modular Functions and Dirichlet Series in Number Theory*. Springer GTM series #41, 1990.

[10] D. N. C. Tse, P. Viswanath, and L. Zheng, "Diversity-multiplexing tradeoff in multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 1859–1874, Sep. 2004.

[11] 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.