Bounding Rate and Performance of Differential Unitary Space-Time Codes Using Integral Geometry Measures

Zhengdao Wang and Georgios B. Giannakis[1]
Dept. of ECE
Univ. of Minnesota
Minneapolis, MN 55455
e-mail: {zhengdao,georgios}@ece.umn.edu

Abstract — **We consider lower bounding the maximum achievable rate of a differential unitary space-time transmission subject to a prescribed performance. We characterize the performance using a suitably defined distance between two unitary matrices, which was previously obtained through pairwise error probability analysis. Considering the set of all unitary or orthogonal matrices as a compact manifold with some invariant volume form or kinematic density, we derive a Varshamov-Gilbert type lower bound on the transmission rate, which asserts the existence of a differential unitary space-time code with the given minimum diversity product for certain rates. On the way to obtaining this bound, the probability density function and the cumulative distribution function for the distance between a random unitary matrix and a fixed unitary matrix are also obtained in closed form in terms of Meijer G-functions.**

I. Introduction

Future wireless communication systems are likely to employ some form of multiple antenna arrays at the transmitter and/or receiver to boost data rate and cope with channel fading effects. Documented studies on capacity and performance have motivated exciting research on *coherent* multi-antenna systems. Various space-time codes have been designed aiming at either high rate or good performance or both. Many of these codes assume that channel state information (CSI) is available at receiver, so that coherent detection can be performed. When the channel varies fast, however, the acquisition of CSI can become costly and inefficient.

Differential space-time schemes are particularly useful for *"blind"* multi-antenna transmissions, as they bypass multichannel estimation that is needed for decoding [5, 6, 12]. Among differential space-time coding schemes, the *differential unitary space-time codes* have attracted most attention for a few reasons: i) They generalize the single-antenna differential phase-shift keying (DPSK) modulation to multiple antennas; ii) When the code matrices form a discrete group, some powerful group-theoretic tools can be used [6, 11]; ii) When the code matrices form a discrete group, they are relatively easy to store and operate — in most cases only a simple table lookup is needed; iv) Relative to non-unitary codes [8], they have better performance in terms of minimum product distance.

A large amount of differential unitary space-time codes have been designed. Noticeable ones include the cyclic and dicyclic codes in [6], and fix-point-free group codes based on representation theory in [11]. However, the fundamental limits of non-coherent and semi-coherent multi-antenna systems remain largely unexplored. In [13], the capacity of non-coherent space-time communication is evaluated based on geometric approaches by packing spheres on the Grassmann manifold. The results there only apply to the limiting case of infinite delay.

The design problem for unitary space-time codes with M transmit antennas can be described as follows [6, 11]. Find a set $\mathcal{G}$ of $L = 2^{RM}$ unitary $M \times M$ matrices such that for any two distinct ones $\mathbf{A}$ and $\mathbf{B}$, the $|\det(\mathbf{A} - \mathbf{B})|$ is as large as possible. The rate of the design is $R = (1/M)\log_2(L)$. If $|\det(\mathbf{A} - \mathbf{B})|$ is non zero for any $\mathbf{A} \neq \mathbf{B}$ from the set $\mathcal{G}$, then the system has full diversity. There is obviously a trade-off between R, and the *diversity product* that is defined as:

$$\zeta = \frac{1}{2} \min_{\mathbf{A},\mathbf{B}\in\mathcal{G}} |\det(\mathbf{A} - \mathbf{B})|^{1/M}. \tag{1}$$

Rather than designing specific constellations [3, 5, 6, 11], in this paper we seek the maximum achievable transmission rate for a given performance. That is, we ask the following question: "What is the maximum R for a given M and ζ ?" The exact answer is difficult except for very simple cases, e.g., when $M = 1$. However, it is possible to obtain a useful bound on the transmission rate. Specifically, we derive the Varshamov-Gilbert type lower bound for differential unitary space-time code that guarantees the existence of a certain rate code for a given ζ. We were not able to obtain the Hamming type upper bound on the achievable rate due to the non-metric behavior of the determinant of pairwise matrix difference.

II. System Description

We outline first the system model for differential space-time modulation.

With M transmit- and N receiver-antennas, a flat-fading multi-antenna system can be described by the following multiple-input multiple-output (MIMO) model:

$$\mathbf{x}_t = \sqrt{\rho}\,\mathbf{s}_t\mathbf{H} + \mathbf{w}_t \tag{2}$$

where $\mathbf{x}_t \in \mathbb{C}^{1\times N}$ is the received signal vector at time slot t, $\mathbf{s}_t \in \mathbb{C}^{1\times M}$ is the corresponding transmitted signal vector, $\mathbf{H} \in \mathbb{C}^{M\times N}$ denotes the multiple-input multiple-output channel, $\mathbf{w}_t$ denotes the additive noise, and ρ denotes the SNR per

[1]This work was supported by the NSF Wireless Initiative Grant No. 99-79443, the NSF Grant No. 01-0516, and by the ARL/CTA Grant No. DAAD19-01-2-011.

receive antenna. Entries of $\mathbf{H}_t$ and $\mathbf{w}_t$ are assumed to be independent complex Gaussian random variables of zero-mean and unit variance.

Stacking M transmit vectors $\mathbf{s}_t$ to form the $M \times M$ matrix $\mathbf{S}_i := [\mathbf{s}_{iM}^T, \mathbf{s}_{iM+1}^T, \ldots, \mathbf{s}_{iM+M-1}^T]^T$, where $(\cdot)^T$ denotes transpose and i is the block index, and defining $\mathbf{X}_i$ and $\mathbf{W}_i$ similar to $\mathbf{S}_i$, we can write the received matrix $\mathbf{X}_i$ as

$$\mathbf{X}_i = \sqrt{\rho}\, \mathbf{S}_i \mathbf{H} + \mathbf{W}_i, \tag{3}$$

where it is assumed that the channel $\mathbf{H}$ remains invariant for a duration of $2M$ time intervals.

In differential unitary space-time modulation [5,6], two consecutive transmitted blocks $\mathbf{S}_{i-1}$ and $\mathbf{S}_i$ are related by the matrix recursion

$$\mathbf{S}_i = \mathbf{U}_l \mathbf{S}_{i-1}, \qquad \mathbf{S}_0 = \mathbf{I}_M \tag{4}$$

where the size M identity matrix $\mathbf{I}_M$ is used for initialization, and $\{\mathbf{U}_l\}_{l=0}^{L-1}$ are different unitary matrix codewords corresponding to L possible symbols. The transmission rate is therefore $R = (1/M)\log_2 L$ bits per channel use, while the encoding delay of the system is M.

The average pairwise error probability (PEP) between two signals $\mathbf{U}_l$ and $\mathbf{U}_{l'}$ when maximum-likelihood (ML) decoding is used, has been tightly upper bounded at high signal-to-noise ratio (SNR) via the union bound [5,6]

$$\mathrm{P_e} \le \frac{1}{2}\left(\frac{8}{\rho}\right)^{MN} |\det(\mathbf{U}_l - \mathbf{U}_{l'})|^{-2N}. \tag{5}$$

Therefore, at high SNR, the average PEP is determined by the diversity product $\zeta = \frac{1}{2}\min_{0\le l\le l'\le L-1} |\det(\mathbf{U}_l - \mathbf{U}_{l'})|^{1/M}$.

Before designing a specified code for a given M, ζ and R, one must answer the question whether a code with the given parameters exists. For a differential unitary space-time code $\mathcal{G}$ of $L = 2^{MR}$ unitary matrices of size $M \times M$, we are interested in finding the maximum achievable rate $R_{\max}(M,\zeta)$ for a specified M and ζ:

$$R_{\max}(M,\zeta) := \max_{\mathcal{G}}\ \zeta \tag{6}$$

The exact form of $R_{\max}(M,\zeta)$ seems difficult to obtain. Relying on geometric probability and integral geometry tools, we will derive a lower bound on $R_{\max}(M,\zeta)$.

Before we state and prove our main result, let us first discuss elaborate briefly on the diversity product function

$$\delta(\mathbf{A},\mathbf{B}) := \frac{1}{2}|\det(\mathbf{A}-\mathbf{B})|^{1/M} \tag{7}$$

between two unitary matrices $\mathbf{A}$ and $\mathbf{B}$ of size $M \times M$. The following can be observed:

i) $\delta(\mathbf{A},\mathbf{B})$ is both left and right invariant with respect to unitary matrix multiplications. Specifically, for any $M \times M$ unitary matrix $\mathbf{U}$, we have

$$\delta(\mathbf{UA},\mathbf{UB}) = \delta(\mathbf{AU},\mathbf{BU}) = \delta(\mathbf{A},\mathbf{B}) \tag{8}$$

ii) $\delta(\mathbf{A},\mathbf{B})$ depends only on the eigenvalues of the matrix $\mathbf{A}^{-1}\mathbf{B}$. If we denote the eigenvalues of $\mathbf{A}^{-1}\mathbf{B}$ as $\lambda_1, \lambda_2, \ldots, \lambda_M$, then $\delta(\mathbf{A},\mathbf{B}) = \frac{1}{2}\prod_{m=1}^{M} |\lambda_m - 1|^{1/M}$;

iii) $\delta(\mathbf{A},\mathbf{B})$ satisfies: $0 \le \delta(\mathbf{A},\mathbf{B}) \le 1$;

iv) $\delta(\mathbf{A},\mathbf{B})$ is not a metric. Specifically, $\delta(\mathbf{A},\mathbf{B}) = 0 \not\Rightarrow \mathbf{A} = \mathbf{B}$. More important, the triangular inequality is not always satisfied: there exist $\mathbf{A}$, $\mathbf{B}$, $\mathbf{U}$ unitary such that

$$\delta(\mathbf{A},\mathbf{B}) > \delta(\mathbf{A},\mathbf{U}) + \delta(\mathbf{B},\mathbf{U}). \tag{9}$$

For example, take $\mathbf{A} = -\mathbf{B} = \mathbf{I}$ and $\mathbf{U} = \mathrm{diag}(1,-1,-1,...,-1)$, where $\mathbf{I}$ is the $M \times M$ identity matrix.

III. Lower Bound on Maximum Rate

In this section, we derive a lower bound on the maximum achievable rate $R_{\max}(M,\zeta)$ for a given number of transmit antennas and diversity product ζ. We view the set $\mathcal{U}_M$ of all $M \times M$ unitary matrices as a compact measurable space, and study the measures of suitable subsets of $\mathcal{U}_M$ that are of interest to us. By comparing the the measures of such subsets to the total measure of the space $\mathcal{U}_M$, we can get a sense of how many such subsets we can pack in the whole space $\mathcal{U}_M$.

We will use the gamma function

$$\Gamma(z) := \int_0^\infty t^{z-1} e^{-t} \mathrm{d}t$$

and the Meijer G-function [9]

$$G_{p,q}^{m,n} := \left(x \,\middle|\, \begin{matrix} a_1, \ldots, a_p \\ b_1, \ldots, b_q \end{matrix}\right) \tag{10}$$

$$\frac{1}{2\pi i}\int_{\gamma_c} \frac{\prod_{j=1}^{m}\Gamma(b_j+s)\prod_{j=1}^{n}\Gamma(1-a_j-s)}{\prod_{j=n+1}^{p}\Gamma(a_j+s)\prod_{j=m+1}^{q}\Gamma(1-b_j+s)} x^{-s}\mathrm{d}s, \tag{11}$$

where γ_c lies between the poles of $\Gamma(1-a_j-s)$, and the poles of $\Gamma(b_j+s)$.

The main result of the paper is stated in the following proposition.

Proposition 1 *For a given M and $\zeta \in (0,1)$, there exists a differential unitary space-time code of rate $\frac{1}{M}\log_2\lceil\frac{1}{P_M(\zeta)}\rceil$, where $\lceil\cdot\rceil$ is the integer ceiling function, and*

$$P_M(\zeta) = 1 - \left[\prod_{k=1}^{M}\frac{\Gamma(k)2^{k-1}}{\sqrt{\pi}}\right]\cdot G_{2M+1,2M+1}^{2M+1,0}\left(\zeta^{2M}\,\middle|\, \begin{matrix} 1, & \{k,k\}_{k=1}^{M} \\ 0, & \{(k+1)/2, k/2\}_{k=1}^{M} \end{matrix}\right). \tag{12}$$

The rest of the paper will be the proof of this proposition.

Consider the set $\mathcal{U}_M$ of all $M \times M$ unitary matrices, which is a group under the matrix product. The kinematic density or the invariant volume form at some $\mathbf{U} \in \mathcal{U}_M$ is given, up to a constant factor, by (see e.g., [10])

$$dU = [\bigwedge(\omega_{jk} \wedge \bar{\omega}_{jk})] \wedge (\bigwedge \omega_{hh}), \qquad 1 \le j < k \le M,\ 1 \le h \le M,$$

where

$$\omega_{jk} := \sum_{h=1}^{M} \bar{u}_{hj} du_{hk}, \qquad \omega_{jk} + \bar{\omega}_{kj} = 0 \tag{13}$$

form a system of Maurer-Cartan forms; u_{hk} are entries of $\mathbf{U}$, $\bar{(\cdot)}$ denotes conjugation, and $\wedge$ denotes wedge product. Since

the manifold $\mathcal{U}_M$ is compact, it is unimodular. As a result, the volume form dU is both left and right invariant. Integration of the volume form yields the Haar measure $m(\cdot)$, which gives the entire volume of the set $\mathcal{U}_M$ as [10]:

$$m(\mathcal{U}_M) = \int_{\mathbf{U}\in\mathcal{U}_M} dU = i^{M(M+1)/2} \prod_{h=1}^{M} \frac{(2\pi i)^h}{(h-1)!}, \qquad i = \sqrt{-1}. \tag{14}$$

For $\mathbf{U} \in \mathcal{U}_M$, we define the set $B(\mathbf{U}, r) := \{\mathbf{U}' : \mathbf{U}' \in \mathcal{U}_M, |\det(\mathbf{U} - \mathbf{U}')|^{1/M} \leq 2r\}$ as the "ball" with center $\mathbf{U}$ and radius r, the measure (volume) of which is $m(B(\mathbf{U}, r)) = \int_{\mathbf{U}'\in B(\mathbf{U},r)} dU'$. Because of the invariance of the function $\delta(\cdot,\cdot)$ and also the invariance of the measure $m(\cdot)$ with respect to both left and right unitary matrix multiplication, $m(B(\mathbf{U}, r))$ is independent of $\mathbf{U}$. Hence, we can rewrite $m(B(\mathbf{U}, r))$ as a function $V(r)$ of r only; i.e., $V(r)$ is the volume of a "ball" of radius r under the Haar measure $m(\cdot)$. We quote the word "ball" because the set $B(\mathbf{U}, r)$ is defined by a function $\delta(\cdot,\cdot)$ that is not a metric on $\mathcal{U}_M$. But it is still conceptually simple to imagine them as balls in the space. We will continue to use the word without quote.

To derive the lower bound in Proposition 1, we follow the Varshamov-Gilbert Bound method used in coding theory. Suppose a differential unitary space-time code $\mathcal{G}$ of size $L-1$ and minimum diversity product ζ has been found. Then, each matrix $\mathbf{U}$ in $\mathcal{G}$ has a ball $B(\mathbf{U}, \zeta)$ defined for it that contains no other members of $\mathcal{G}$. Because all such balls have equal volume $V(\zeta)$, the union of them can have volume at most equal to the sum of the volume $V(\zeta)$ of each. Therefore, the union of all the balls $\cup_{\mathbf{U}\in\mathcal{G}} B(\mathbf{U}, \zeta)$ has its volume upper bounded by $(L-1)V(\zeta)$. If $(L-1)V(\zeta)$ is less than the total volume $m(\mathcal{U}_M)$ of the space, then there exists at least one unitary matrix in $\mathcal{U}_M$ that is not in any of the balls $B(\mathbf{U}, \zeta)$, $\mathbf{U} \in \mathcal{G}$ and hence, it is at least ζ away from any of the members of $\mathcal{G}$. This extra unitary matrix can therefore be added to the code $\mathcal{G}$ and the resulting code will have L members, while the minimum diversity product is kept at least equal to ζ. This process can be repeated as long as the sum volume of all the balls $B(\mathbf{U}, \zeta)$, $\mathbf{U} \in \mathcal{G}$ is smaller than $m(\mathcal{U}_M)$. Therefore, there exists a differential unitary space-time code $\mathcal{G}$ with L members, as long as L satisfies the following inequality

$$(L-1)V(\zeta) < m(\mathcal{U}_M). \tag{15}$$

The problem boils down to evaluating the volume $V(\zeta)$, or, since $m(\mathcal{U}_M)$ is known, to evaluating $V(\zeta)/m(\mathcal{U}_M)$. If we normalize the Haar measure by the total volume of the space $\mathcal{U}_M$, then $\mathcal{U}_M$ becomes a probability space with the measurable sets defined as those measurable under the Haar measure. The matrices in $\mathcal{U}_M$ then become random realizations (samples) in this probability space and can be thought of as *uniformly distributed* with respect to the Haar probability measure.

This view point converts the problem of finding $V(\zeta)/m(\mathcal{U}_M)$ to a geometric probability problem. In other words, $V(\zeta)/m(\mathcal{U}_M)$ is the probability that a uniformly distributed random matrix is within a "distance" ζ of any fixed unitary matrix. Without loss of generality, we can choose the fixed unitary matrix to be the identity matrix $\mathbf{I}$. If $\mathbf{U}$ denotes a uniformly distributed random matrix, then $\delta(\mathbf{U}, \mathbf{I})$ as a function of $\mathbf{U}$ becomes a random variable with the image on the real line (actually, between 0 and 1). We denote this random variable as Δ.

We let $p_M(r)$ and $P_M(r)$ denote the probability density function and the cumulative distribution function, respectively. That is,

$$P_M(r) := \mathrm{P}(\Delta \leq r), \tag{16}$$

and $p_M(r) := dP_M(r)/dr$, $r \in [0, 1]$. With these notation, we can write

$$P_M(\zeta) = V(\zeta)/m(\mathcal{U}_M). \tag{17}$$

It seems difficult to evaluate $P_M(\zeta)$ directly from the Haar measure. In the following, we will evaluate $P_M(\zeta)$ using a different route.

Let λ_m denote the ith eigenvalue of $\mathbf{U}$, $m = 1, 2, \ldots, M$. Then

$$\delta(\mathbf{U}, \mathbf{I}) = (1/2) \prod_{m=1}^{M} |\lambda_m - 1|^{1/M}.$$

The distribution of $\delta(\mathbf{U}, \mathbf{I})$ therefore depends only on the joint probability density of all the M eigenvalues of $\mathbf{U}$.

Since $\mathbf{U}$ is unitary, all its eigenvalues have norm one. We can therefore write $\lambda_m = e^{j\theta_m}$, where $\theta_m \in [0, 2\pi)$, $m = 1, \ldots, M$. The joint probability density of λ_m, $m = 1, 2, \ldots, M$ has been found to be in the following form [4, page 135].

Lemma 1 *The joint probability density of λ_m, $m = 1, 2, \ldots, M$ is*

$$\frac{1}{M!} \prod_{m<n} |\lambda_m - \lambda_n|^2 = \frac{1}{M!} \prod_{m<n} |e^{i\theta_m} - e^{i\theta_n}|^2 \tag{18}$$

with respect to $d\lambda_1 d\lambda_2 \ldots d\lambda_M$, where $d\lambda_m = d\theta_m/2\pi$.

With this lemma, we can write $P_M(r)$ as an M-fold integral

$$P_M(r) = \int_{T_c} \frac{1}{M!} \prod_{m<n} |e^{i\theta_m} - e^{i\theta_n}|^2 \mathrm{d}\theta_1 \mathrm{d}\theta_2 \ldots \mathrm{d}\theta_M / (2\pi)^M \tag{19}$$

where T_c is the set

$$T_c := \{(\theta_1, \theta_2, \ldots, \theta_M) : \frac{1}{2} \prod_{m=1}^{M} |e^{j\theta_m} - 1|^{1/M} \leq r\}. \tag{20}$$

This integral is difficult to evaluate, because of the highly irregular shape of T_c.

To find out $P_M(r)$, we will first find $p_M(r)$ by making the following observation. The support of $p_M(r)$ is $[0, 1]$, which is compact. Therefore, $p_M(r)$ can be uniquely determined from all the moments of the random variable Δ. If we can find out all these moments, then we can reconstruct $p_M(r)$. It turned out that this is a viable method. A generalization of this "moment method" is based on the Mellin transformation and its application to the problem of determinant density of random matrices is due to Cicuta and Mehta [1]. Our problem is not exactly the determinant of a random matrix: it is the determinant of the difference of a random matrix and the identity matrix. However, after some twists, the method turned out to work well.

The Mellin transformation of a function $f(x)$ is defined as [2]

$$\hat{f}(s) := \int_0^\infty x^{s-1} f(x) dx. \tag{21}$$

If $f(x)$ is a probability density function with non-negative support, and if s is positive integer, then $\hat{f}(s)$ defines the $(s-1)$st moment of $f(x)$. But in general s is a complex number.

The inverse Mellin transform is given by

$$f(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} x^{-s}\hat{f}(s)ds. \tag{22}$$

The transform $\hat{f}(s)$ exists if the integral

$$\int_0^\infty |f(x)|x^{k-1}dx \tag{23}$$

is bounded for some $k > 0$, in which case the inverse $f(x)$ exists with $c > k$.

The Mellin transform of $p_M(r)$ is therefore the expectation of Δ^{s-1}:

$$\hat{p}_M(s) = \int_0^\infty x^{s-1}p_M(x)dx = \mathrm{E}[\Delta^{s-1}] \tag{24}$$

The expectation, using Lemma 1 is again an M-fold integral

$$\mathrm{E}[\Delta^{s-1}] = \int \frac{1}{2^{s-1}\cdot M!}\prod_{m=1}^{M}|e^{j\theta_m}-1|^{(s-1)/M} \prod_{m<n}|e^{i\theta_m}-e^{i\theta_n}|^2 \mathrm{d}\theta_1\mathrm{d}\theta_2\ldots\mathrm{d}\theta_M/(2\pi)^M, \tag{25}$$

where the integration is over $[0, 2\pi]^M$. The integral is in a "nicer" form than that of (19) because of its more regular integration region.

Using an orthogonal polynomial based method developed by Mehta [7], this integral can be shown to be equal to the determinant of an $M \times M$ matrix $\mathbf{R}$ whose (m, n)th entry $[\mathbf{R}]_{mn}$ is given by

$$\begin{aligned}[\mathbf{R}]_{mn} &= \int_0^{2\pi} 2^{-(s-1)}(2\sin\frac{\theta}{2})^{(s-1)/M}e^{j(m-n)\theta}\mathrm{d}\theta/2\pi \\ &= \frac{2^{-(s-1)}(-1)^{m-n}\Gamma(\frac{s-1}{M}+1)}{\Gamma(\frac{s-1}{2M}+m-n+1)\Gamma(\frac{s-1}{2M}-m+n+1)}\end{aligned} \tag{26}$$

Then $\hat{p}_M(s) = \mathrm{E}[\Delta^{s-1}] = \det(\mathbf{R})$ can be evaluated to be

$$\begin{aligned}\hat{p}_M(s) &= 2^{-(s-1)}\prod_{m=1}^{M}\frac{\Gamma(\frac{s-1}{M}+m)\Gamma(m)}{\Gamma(\frac{s-1}{2M}+m)^2} \\ &= 2^{-(s-1)}\prod_{m=1}^{M}\frac{\Gamma(\frac{s-1}{2M}+\frac{m-1}{2})\Gamma(\frac{s-1}{2M}+\frac{m}{2})\Gamma(m)2^{\frac{s-1}{M}+m-1}}{\sqrt{\pi}\Gamma(\frac{s-1}{2M}+m)^2}\end{aligned}$$

Using the definition of the Meijer G-function and the inverse Mellin transform, we can write the probability density function $p_M(r)$ as in the following proposition.

Proposition 2 *For $M \times M$ unitary $\mathbf{U}$ uniformly distributed with respect to the Haar measure, the random variable $\Delta = \delta(\mathbf{U}, \mathbf{I})$ has the following probability density function*

$$p_M(r) = 2M\prod_{m=1}^{M}\frac{\Gamma(m)2^{m-1}}{\sqrt{\pi}} G^{2M,0}_{2M,2M}\left(r^{2M}\middle|\begin{matrix}\{k-\frac{1}{2M}, k-\frac{1}{2M}\}_{k=1}^{M} \\ \{(k+1)/2-\frac{1}{2M}, k/2-\frac{1}{2M}\}_{k=1}^{M}\end{matrix}\right).$$

When $M = 1$, $p_M(r)$ simplifies to the following simple form

$$p_1(r) = \frac{2}{\pi\sqrt{1-y^2}}. \tag{27}$$

Using the following property of Mellin transform:

$$\int_0^\infty x^{s-1}\int_x^\infty f(t)\,\mathrm{d}t\,\mathrm{d}x = \frac{1}{s}\int_0^\infty x^s f(x)\,\mathrm{d}x \tag{28}$$

and the fact that $s = \Gamma(s+1)/\Gamma(s)$ we can obtain the function $1 - P_M(r)$. We then find the cumulative distribution function as in the following proposition.

Proposition 3 *For $M \times M$ unitary $\mathbf{U}$ uniformly distributed with respect to the Haar measure, the random variable $\Delta = \delta(\mathbf{U}, \mathbf{I})$ has the following cumulative distribution function*

$$P_M(r) = 1 - \prod_{m=1}^{M}\frac{\Gamma(m)2^{m-1}}{\sqrt{\pi}} G^{2M+1,0}_{2M+1,2M+1}\left(r^{2M}\middle|\begin{matrix}1, \{k, k\}_{k=1}^{M} \\ 0, \{(k+1)/2, k/2\}_{k=1}^{M}\end{matrix}\right). \tag{29}$$

Proposition 1 then follows from (15), (17), and (29).

IV. Conclusion

The paper derived a Varshamov-Gilbert type lower bound on the transmission rate of a differential unitary space-time code. The closed form expression of the probability density function and the cumulative distribution function for the distance between a random unitary matrix and a fixed unitary matrix were also obtained in closed form.

References

[1] G. M. Cicuta and M. L. Mehta, "Probability density of determinants of random matrices," *preprint*, 2000; downloadable from `http://www.pr.infn.it/preprints/2000/`

[2] B. Davies, *Integral Transforms and Their Applications*, Springer-Verlag, New York, 2nd edition, 1985.

[3] B. Hassibi and M. Khorrami, "Fully-diverse multiple-antenna signal constellations and fixed-point-free lie groups," *IEEE Transactions on Information Theory*, 2000 (submitted).

[4] F. Hiai and D. Petz, *The semicircle law, free random variables, and entropy*, American Mathematical Society, 2000.

[5] B. Hochwald and W. Sweldens, "Differential unitary space time modulation," *IEEE Transactions on Communications*, vol. 48, pp. 2041–2052, Dec. 2000.

[6] B. Hughes, "Differential space-time modulation," *IEEE Transactions on Information Theory*, pp. 2567–2578, Nov. 2000.

[7] M. L. Mehta, *Random matrices*, Academic Press, San Diego, 2nd edition, 1991.

[8] P. Oswald, "On codes for multiple-antenna differential modulation," *manuscript*, Apr. 1999; downloadable from `http://cm.bell-labs.com/who/poswald/`

[9] A. P. Prudnikov, Yu. A. Brychkov, and O. I. Marichev, *Integrals and Series*, vol. 3, Gordon and Breach Science Publishers, 1986.

[10] L. A. Santalo, *Integral Geometry and Geometric Probability (Encyclopedia of Mathematics and Its Applications, Vol 1)*, Addison-Wesley Publishing Company, Inc, 1976.

[11] A. Shokrollahi, B. Hassibi, B. M. Hochwald, and W. Sweldens, "Representation theory for high-rate multiple-antenna code design," *IEEE Transactions on Information Theory*, vol. 47, no. 6, pp. 2335–2367, Sept. 2001.

[12] V. Tarokh and Jafarkhani, "A differential detection scheme for transmit diversity," *IEEE Journal on Selected Areas in Communications*, pp. 1169–1174, July 2000.

[13] L. Zheng and D. Tse, "Communicating on the Grassmann manifold: A geometric approach to the non-coherent multiple antenna channel," *IEEE Transactions on Information Theory*, vol. 48, no. 2, pp. 359–383, Feb. 2002.