The DMT of Real and Quaternionic Lattice Codes and DMT Classification of Division Algebra Codes

Roope Vehkalahti and Laura Luzzi, *Member, IEEE*

***Abstract*—In this paper we consider the diversity-multiplexing gain tradeoff (DMT) of so-called minimum delay asymmetric space-time codes for the $n \times m$ MIMO channel. Such codes correspond to lattices in $M_n(\mathbb{C})$ with dimension smaller than $2n^2$. Currently, very little is known about their DMT, except in the case $m = 1$, corresponding to the multiple input single output (MISO) channel.**

Further, apart from the MISO case, no DMT optimal asymmetric codes are known.

We first discuss previous criteria used to analyze the DMT of space-time codes and comment on why these methods fail when applied to asymmetric codes. We then consider two special classes of asymmetric codes where the code-words are restricted to either real or quaternion matrices. We prove two separate diversity-multiplexing gain trade-off (DMT) upper bounds for such codes and provide a criterion for a lattice code to achieve these upper bounds. We also show that lattice codes based on $\mathbb{Q}$-central division algebras satisfy this optimality criterion. As a corollary this result provides a DMT classification for all $\mathbb{Q}$-central division algebra codes that are based on standard embeddings. While the $\mathbb{Q}$-central division algebra based codes achieve the largest possible DMT of a code restricted to either real or quaternion space, they still fall short of the optimal DMT apart from the MISO case.

***Index Terms*—division algebra, space-time block codes (STBCs), multiple-input multiple-output (MIMO), diversity-multiplexing gain trade-off (DMT), algebra, number theory.**

The research of R. Vehkalahti was supported by the Academy of Finland grant #299916.

This work was presented in part at the IEEE International Symposium on Information Theory (ISIT 2018), Vail, CO [1].

R. Vehkalahti is with the Department of Mathematics and Statistics, FI-40014, University of Jyväskylä, Jyväskylä, Finland (e-mail: roope.i.vehkalahti@jyu.fi). While this work was in progress, he was with the Department of Communications and Networking, FI-02150, Aalto University, Espoo, Finland.

L. Luzzi is with ETIS, UMR 8051 (CY Cergy Paris Université, ENSEA, CNRS), 95014 Cergy-Pontoise, France (e-mail: laura.luzzi@ensea.fr).

I. Introduction

The DMT [2] is a powerful tool for analyzing the performance of a space-time block code in one shot MIMO communication. Analyzing the DMT curve of a given code gives us a good grasp of the expected performance of the code over the Rayleigh fading channel. It is therefore of great interest to develop methods to measure the DMT of a given code.

The previous research reveals that this task is non-trivial. When the diversity-multiplexing gain trade-off was introduced in 2003 in by Zheng and Tse [2], the only explicit example of a code achieving the optimal DMT was the Alamouti code [3] when it was received with a single antenna. Later in [4] Elia *et al.* proved that in a MIMO system with n transmit and m receive antennas and minimal delay $T = n$, the non-vanishing

determinant property (NVD) is a sufficient condition for a $2n^2$-dimensional lattice code in $M_n(\mathbb{C})$ to achieve the optimal diversity-multiplexing gain trade-off. They also pointed out that division algebra based codes, such as the perfect codes [5], are DMT optimal, and gave a general construction for DMT-achieving $2n^2$-dimensional lattice codes in $M_n(\mathbb{C})$. This criterion was generalized by Tavildar and Viswanath [6] who showed that if the product of the smallest m singular values of any non-zero matrix in a $2nm$-dimensional lattice $L \subset M_n(\mathbb{C})$ stays above some fixed constant, then L achieves the optimal DMT curve in the $n \times m$ MIMO channel. In the case where $n = m$, this criterion coincides with the NVD condition.

The work in [4] revealed that there exist $2n^2$-dimensional codes in $M_n(\mathbb{C})$ achieving the optimal DMT curve, when received with an arbitrary number of receiving antennas m. Maximum likelihood (ML) decoding of these codes can be performed using the sphere decoding algorithm [7], although its complexity is in general exponential in the lattice dimension [8, 9]. On the other hand, it has been shown that the decoding complexity can be considerably reduced using lattice reduction (LR) aided regularized lattice decoding, which preserves DMT-optimality [10]. Moreover, in [11] the authors prove that with LR-aided regularized sphere decoding it is possible to get a vanishing gap to ML performance with subexponential complexity.

However, when receiving a full $2n^2$-dimensional space-time lattice code with minimum delay ($T = n$) with $m < n$ antennas, the dimension of the receiver space is only $2mT = 2mn$ and so the image of the infinite lattice is no longer a lattice, but a dense set of points. Thus the standard sphere decoding algorithm cannot be employed, although special techniques such as generalized sphere decoding have been proposed [12, 13]. Therefore, it is in many cases desirable to use lattice space-time codes that are at maximum $2nm$-dimensional[1]. On the other hand, a less than $2nm$-dimensional lattice would be a waste of receiving signal space and energy and is believed to lead to a suboptimal DMT curve. Therefore a $2nm$-dimensional lattice code is the "best fit" for the $n \times m$ MIMO channel. We refer to such a code as a *well fitting asymmetric space-time code*. In this case currently the only available general criterion for DMT-optimality is the approximate universality criterion given in [6].

However, when $n > m$ no asymmetric codes satisfying the approximate universality condition in [6] are known except in the case $m = 1$. It is also known that there are space-time codes that are DMT optimal despite not satisfying the approximate universality criterion [14]. This motivates the search for a more general and easily applicable DMT criterion.

In [15] the authors claimed, when translated into lattice theoretic language, that any $2nm$-dimensional lattice code $L \subset M_n(\mathbb{C})$ with NVD would achieve the optimal DMT curve with m receive antennas when $n > m$. This would imply that large families of asymmetric space-time codes are DMT optimal.

In this paper we study the DMT of asymmetric space-time codes. We begin by reviewing some of the previous DMT criteria and discuss why they seem to fall short when applied to asymmetric codes. We then construct a code that satisfies the DMT optimality criterion in [15], but is not DMT optimal. This suggests that, unfortunately, Theorem 2 in [15] is incorrect. Indeed, there are no known DMT optimal asymmetric codes except in the case of MISO channels.

Next, we consider the special class of asymmetric codes based on division algebras whose center is $\mathbb{Q}$.

[1]For example [11] assumes that the lattice code is well-fitting [11, equation (6)], and in particular it should be $2nm$-dimensional when $n > m$.

This choice seems natural since on one hand, this class includes the Alamouti code [3], which is one of the few DMT-optimal asymmetric space-time codes, and on the other hand, in [4] the optimal codes were based on division algebras. However, the difference is that in [4] the center of the algebras was complex quadratic, which always leads to lattice codes with full rank $2n^2$ in $M_n(\mathbb{C})$.

All the $\mathbb{Q}$-central division algebra codes have the NVD property and several examples have appeared previously in the literature [16, 17, 18, 19]. However, their DMT was still unknown, apart from Alamouti type codes in the 2×1 channel [2].

Unlike the case of complex quadratic center, we show that $\mathbb{Q}$-central division algebras are divided into two categories with respect to their DMT performance. This distinction is based on the ramification of the infinite Hasse-invariant of the division algebra, which determines whether the corresponding lattice code can be embedded into real or quaternionic space.

Our DMT classification holds for any multiplexing gain, extending previous partial results in [20, 21] which were based on the theory of Lie algebras. We note that the approach used in this paper is quite different and more general. In the spirit of [4] we are not just considering division algebra codes, but all space-time codes where the codewords are restricted to the real and quaternionic matrices $M_n(\mathbb{R})$ or $M_{n/2}(\mathbb{H})$ respectively. We provide DMT upper bounds for both cases, and prove that n^2-dimensional NVD lattice codes inside $M_n(\mathbb{R})$ (resp. $M_{n/2}(\mathbb{H})$) achieve the respective upper bounds. As the $\mathbb{Q}$-central division algebra codes are of this type, we get their DMT as a corollary. We note that while these codes achieve the best possible DMT for their natural ambient spaces, they don't achieve the general optimal DMT, the only exception being quaternionic codes in the 2×1 channel.

Finally we consider the DMT in multi-block channels, where we are allowed to encode and decode over a number of independently faded blocks. Again we find the best possible DMT of asymmetric multi-block codes whose elements belong either to real or quaternionic space and prove that certain division algebra based codes achieve this upper bound. This analysis also provides the DMT classification of all division algebras whose center is totally real.

Organization of the paper

Section II reviews the definition of diversity-multiplexing gain trade-off and basic properties of matrix lattices. Section III summarizes previous criteria for DMT-optimality and provides a counterexample to show that the NVD property is not sufficient for DMT-optimality in the asymmetric case. Section IV establishes DMT upper bounds for real and quaternionic space-time codes, and shows that codes with the NVD property achieve these upper bounds. Section V shows how to obtain real and quaternionic lattices with the NVD property from the embeddings of $\mathbb{Q}$-central division algebras, and presents a conjecture about the DMT of space-time codes arising from the regular representations of these algebras. Finally, Section VI extends the results of Section IV to the multi-block case.

II. Notation and preliminaries

A. Single-block channel model and DMT

Throughout the paper we will consider a MIMO system with n transmit and m receive antennas, and minimal delay $T = n$. The received signal is[2]

$$Y_c = \sqrt{\frac{\rho}{n}} H_c \bar{X} + W_c, \tag{1}$$

[2]A more general multi-block MIMO channel model will be considered in Section VI.

where $\bar{X} \in M_n(\mathbb{C})$ is the transmitted codeword, $H_c \in M_{m,n}(\mathbb{C})$ and $W_c \in M_{m,n}(\mathbb{C})$ are the channel and noise matrices with i.i.d. circularly symmetric complex Gaussian entries $h_{ij}, w_{ij} \sim \mathcal{N}_{\mathbb{C}}(0,1)$, and ρ is the signal-to-noise ratio (SNR). We suppose that perfect channel state information is available at the receiver but not at the transmitter.

Given a matrix $X \in M_{m,n}(\mathbb{C})$, let $\|X\|_F = \sqrt{\mathrm{tr}(X^\dagger X)}$ denote its Frobenius norm.

Definition 1: A *space-time block code* (STBC) C for some designated SNR level ρ is a set of $n \times n$ complex matrices satisfying the average power constraint

$$\frac{1}{|C|} \sum_{X \in C} \|X\|_F^2 \leq n^2. \tag{2}$$

A coding scheme $\{C(\rho)\}$ is a family of STBCs, one for each SNR level. The rate for the code $C(\rho)$ is $R(\rho) = \frac{1}{T} \log |C(\rho)|$.

We say that the coding scheme $\{C(\rho)\}$ achieves the *diversity-multiplexing gain trade-off* (DMT) of *spatial multiplexing gain* r and *diversity gain* $d(r)$ if the rate satisfies

$$\lim_{\rho \to \infty} \frac{R(\rho)}{\log(\rho)} = r, \tag{3}$$

and the average error probability is such that

$$P_e(\rho) \doteq \rho^{-d(r)},$$

where by the dotted equality we mean $f(M) \doteq g(M)$ if

$$\lim_{M \to \infty} \frac{\log(f(M))}{\log(M)} = \lim_{M \to \infty} \frac{\log(g(M))}{\log(M)}. \tag{4}$$

Notations such as $\dot{\geq}$ and $\dot{\leq}$ are defined in a similar way.

With the above definitions, the main result in [2] is the following.

Theorem 1 (Optimal DMT): Let n, m, T, $\{C(\rho)\}$, and $d(r)$ be defined as before. Then any STBC coding scheme $\{C(\rho)\}$ has error probability lower bounded by

$$P_e(\rho) \dot{\geq} \rho^{-d^*(r)} \tag{5}$$

or equivalently, the diversity gain

$$d(r) \leq d^*(r), \tag{6}$$

when the coding is limited within a block of T channel uses. The optimal diversity gain $r \mapsto d^*(r)$, also termed the optimal DMT, is a piece-wise linear function connecting the points $(r, (n-r)(m-r))$ for $r = 0, 1, \ldots, \min\{n, m\}$.

B. Matrix Lattices and their coding schemes

In this section we describe how to obtain a coding scheme that satisfies the rate condition (3) and average energy condition (2) from a matrix lattice $\mathcal{L} \subseteq M_n(\mathbb{C})$.

Definition 2: A *matrix lattice* $\mathcal{L} \subset M_n(\mathbb{C})$ has the form

$$\mathcal{L} = \mathbb{Z}B_1 \oplus \mathbb{Z}B_2 \oplus \cdots \oplus \mathbb{Z}B_k,$$

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

Definition 3: If the minimum determinant of the lattice $\mathcal{L} \subset M_n(\mathbb{C})$ is non-zero, i.e. it satisfies

$$\inf_{\mathbf{0} \neq X \in \mathcal{L}} |\det(X)| > 0,$$

we say that the lattice satisfies the *non-vanishing determinant* (NVD) property.

Definition 4 (Spherical shaping): Given a positive real number M and a k-dimensional lattice $\mathcal{L} \subset M_n(\mathbb{C})$, we define

$$\mathcal{L}(M) = \{X \in \mathcal{L} \,:\, \|X\|_F \leq M,\ X \neq \mathbf{0}\}.$$

The following two results are well known [22].

Lemma 1: If $\mathcal{L}$ is a k-dimensional lattice in $M_n(\mathbb{C})$ and $\mathcal{L}(M)$ is defined as above, then there exist real constants $K_1, K_2 > 0$, that are independent of M, so that

$$K_1 M^k \leq |\mathcal{L}(M)| \leq K_2 M^k. \tag{7}$$

Lemma 2: Let $\mathcal{L}$ be a k-dimensional lattice in $M_n(\mathbb{C})$. Then

$$s_2 M^{k+2} \leq \sum_{X \in \mathcal{L}(M)} \|X\|_F^2 \leq s_1 M^{k+2},$$

where s_1 and s_2 are constants independent of M.

We can now give a formal definition of a family of space-time lattice codes of finite size.

Definition 5: Given the lattice $\mathcal{L} \subset M_n(\mathbb{C})$, a space-time lattice coding scheme associated with $\mathcal{L}$ is a collection of STBCs given by

$$C_{\mathcal{L}}(\rho) = \rho^{-\frac{rn}{k}} \mathcal{L}\left(\rho^{\frac{rn}{k}}\right) \tag{8}$$

for the desired multiplexing gain r and for each ρ level. One can see that according to Lemma 1 the coding scheme defined this way indeed has multiplexing gain r.

From Lemma 2 we have

$$\sum_{X \in \mathcal{L}\left(\rho^{\frac{rn}{k}}\right)} \rho^{-\frac{2rn}{k}} \|X\|_F^2 \doteq \rho^{-\frac{2rn}{k}} (\rho^{\frac{rn}{k}})^{k+2} = \rho^{rn}.$$

On the other hand we also have that $|\mathcal{L}(\rho^{\frac{rn}{k}})| \doteq \rho^{rn}$ from Lemma 1. Combining the above shows that the code $C_{\mathcal{L}}(\rho)$ has the correct average power (2) from the DMT perspective, i.e., in terms of the dotted equality.

Remark 1: We discussed the question of transforming a lattice code into a coding scheme in detail since in Section III-A we will prove that a certain lattice code is not DMT optimal. It is therefore crucial that our coding schemes are using the lattices in an asymptotically optimal way.

III. Previous criteria for DMT optimality and failing of the NVD condition

Several methods have been proposed to analyze the DMT of a space-time code, but most of them are not tight enough to prove DMT-optimality except for special cases. For example, in [2] the authors analysed the DMT of different versions of BLAST [23]. They also showed the DMT optimality of the Alamouti code over the 2×1 channel by transforming the MISO channel into two parallel channels. A similar approach was used to prove that different diagonal space-time codes are DMT-optimal [6]. However, this criterion can be only applied to special classes of codes.

Using the union bound for the error probability to evaluate the DMT [6] is a universal approach that can be used to analyze any kind of space-time codes. However, it consistently gets too loose when the multiplexing gain is high [24, 21].

So far the most effective criterion to prove DMT optimality is the NVD criterion [24, 4]. This criterion was generalized by Tavildar and Viswanath in [6]. We begin by shortly reviewing their approximate universality (AU) criterion and draw some implications of their work for the lattice based coding schemes introduced in the previous section. We do not define AU, but do note that it is a considerably stronger condition that implies DMT. In particular a space-time code can be DMT optimal despite not being approximately universal.

Theorem 2: A sequence of codes $C(\rho)$ of rate $R(\rho)$ is approximately universal over the $n \times m$ MIMO channel if and only if, for every pair of distinct codewords $X, \bar{X} \in C(\rho)$,

$$\lambda_1^2 \cdots \lambda_s^2 \geq \frac{1}{2^{R(\rho)+o(\log \rho)}}, \tag{9}$$

where $\lambda_1, \ldots, \lambda_s$ are the smallest s singular values of the codeword difference matrix $X - \bar{X}$ and $s = \min(m, n)$.

Here the notation $o(\log \rho)$ refers to a function that is asymptotically dominated by $\epsilon \log \rho$ for any $\epsilon > 0$.
In the case $m \geq n$, this condition is simply the NVD condition of Definition 3.

Definition 6: We refer to the i-th smallest singular value of the matrix X with $\lambda_i(X)$ and for $s \leq n$, we set

$$\Delta_s(X) = \prod_{i=1}^{s} \lambda_i^2(X).$$

We can now extend this definition to lattices.

Definition 7: Given a lattice $\mathcal{L} \subset M_n(\mathbb{C})$, we define

$$\Delta_s(\mathcal{L}) := \inf\{\Delta_s(X) \mid X \in \mathcal{L} \setminus \{0\}\}.$$

The result by Tavildar and Viswanath now implies the following.

Corollary 1: Suppose that $n \geq m$, $\mathcal{L}$ is a $2mn$-dimensional lattice in $M_n(\mathbb{C})$ and that

$$\Delta_m(\mathcal{L}) \neq 0.$$

Then $C_{\mathcal{L}}(\rho)$ is approximately universal (and therefore DMT optimal), when received with m antennas.

Proof: Assume without loss of generality that we have scaled our lattice so that $\Delta_m(\mathcal{L}) = 1$. The finite codes we consider are of the type $C_{\mathcal{L}}(\rho) = \rho^{-\frac{r}{2m}}\mathcal{L}(\rho^{\frac{r}{2m}})$. Given two codewords $\rho^{-\frac{r}{2m}}X$ and $\rho^{-\frac{r}{2m}}\bar{X}$ in $\rho^{-\frac{r}{2m}}\mathcal{L}(\rho^{\frac{r}{2m}})$, we have

$$\Delta_m\left(\rho^{-\frac{r}{2m}}\left(X-\bar{X}\right)\right) = \rho^{-r}\Delta_m(X-\bar{X}) \geq \rho^{-r}.$$

The last inequality here follows as $X - \bar{X} \in \mathcal{L}$ and we assumed that $\Delta_m(\mathcal{L}) = 1$. On the other hand according to equation (7) we have $K_1\rho^{rn} \leq |C_{\mathcal{L}}(\rho)| \leq K_2\rho^{rn}$ for fixed constants $K_1, K_2 > 0$ and

$$\frac{1}{2^{R(C_{\mathcal{L}}(\rho))}} \leq \frac{1}{2^{\frac{1}{n}\log(K_1\rho^{rn})}} = \frac{\rho^{-r}}{2^{\frac{1}{n}\log K_1}}.$$

Thus condition (9) is satisfied, and we conclude that approximate universality holds as a consequence of Theorem 2. □

Remark 2: The reader should note that the approximate universality criterion in Theorem 2 is actually more general than Corollary 1 and does allow $\Delta_m(\mathcal{L})$ to vanish as long as $\Delta_m(\mathcal{L}) \geq \frac{1}{2^{o(\log\rho)}}$.

Example 1: The Alamouti code together with QAM modulation can be seen as a 4-dimensional lattice code $\mathcal{L}_{\text{Alam}} \subset M_2(\mathbb{C})$. For this code $\Delta_1(\mathcal{L}) > 0$. Therefore the coding scheme $C_{\mathcal{L}_{\text{Alam}}}(\rho)$ is approximately universal when received with a single antenna.

Example 2: The division algebra based codes such as the Perfect codes [5] are $2n^2$-dimensional lattices in $M_n(\mathbb{C})$ and have the NVD property and are therefore DMT optimal.

However, the conditions of Corollary 1 seem difficult to satisfy in other cases. As a matter of fact we conjecture the following:

Conjecture 1: The conditions of Corollary 1 can be satisfied only when either $m = n$ or when $n = 2$ and $m = 1$.

A. Failing of the NVD criterion

Many codes are DMT optimal despite not satisfying the approximate universality criterion of the previous section. For example the diagonal number field codes [25] and many of the fully diverse quasi-orthogonal codes [26] are DMT optimal in the $n \times 1$ MIMO channel [14]. Seen as lattice codes, these are $2n$-dimensional lattices in $M_n(\mathbb{C})$ and have the NVD property. However, they are not approximately universal [27].

It is a tempting idea that the NVD condition for a $2nm$-dimensional lattice $\mathcal{L} \subseteq M_n(\mathbb{C})$ would be enough for the coding scheme $C_{\mathcal{L}}(\rho)$ to be DMT optimal when received with m receiving antennas. This was suggested in [15].

Using the normalization in [15] we can state the NVD condition for a $2nm$ dimensional lattice $\mathcal{L}$ and scheme $\rho^{\frac{1}{2}}C_{\mathcal{L}}(\rho) = \rho^{\frac{1}{2}-\frac{r}{2m}}\mathcal{L}\left(\rho^{\frac{r}{2m}}\right)$ in the form

$$\Delta_n(X) \geq c\rho^{n(1-\frac{r}{m})}, \tag{10}$$

for any non-zero codeword X in $\rho^{1/2}C_{\mathcal{L}}(\rho)$ and fixed positive constant c. According to Theorem 2 in [15] this should be a sufficient condition for achieving the optimal DMT.

However, this is not the case and we will now build a code for the 4×1 MISO channel that satisfies the criterion (10), but is not DMT optimal in this channel.

Remark 3: One should notice that condition (10) is considerably weaker than the condition in Corollary 1. Using the normalization of [15], the condition of Corollary 1 can be written as follows: if a coding scheme

$\rho^{1/2}C_{\mathcal{L}}(\rho)$, based on a $2mn$-dimensional lattice code $\mathcal{L}$, satisfies

$$\Delta_m(X) \geq c\rho^{m(1-\frac{r}{m})},$$

for any non-zero codeword $X \in \rho^{1/2}C_{\mathcal{L}}(\rho)$, any ρ and some fixed constant c, then it is approximately universal.

Let us begin with the Golden Code $\mathcal{L}_{\text{Gold}}$ [28]. One can see it as an 8-dimensional NVD lattice in $M_2(\mathbb{C})$. According to (8) we can use scheme $\rho^{\frac{1}{2}-\frac{r}{4}}\mathcal{L}_{\text{Gold}}(\rho^{\frac{r}{4}})$ to study the DMT of $\mathcal{L}_{\text{Gold}}$. It was already proven in [4] that this scheme achieves the optimal DMT curve in the 2×2 MIMO channel.

Let's now transform the Golden Code into an 8-dimensional code in $M_4(\mathbb{C})$ by setting

$$\text{diag}(X, X) = \begin{pmatrix} X & \mathbf{0} \\ \mathbf{0} & X \end{pmatrix},$$

where $X \in M_2(\mathbb{C})$ and $\mathbf{0}$ is the 2×2 zero matrix. The set $\text{diag}(\mathcal{L}_{\text{Gold}}) = \{\text{diag}(X, X) \,|\, X \in \mathcal{L}_{\text{Gold}}\}$ is an 8-dimensional NVD lattice code in $M_4(\mathbb{C})$. In order to satisfy the energy normalization demands we have to consider the scheme $\rho^{\frac{1}{2}-\frac{r}{2}}\text{diag}(\mathcal{L}_{\text{Gold}})(\rho^{\frac{r}{2}}) = C_{\text{diag}(\mathcal{L}_{\text{Gold}})}(\rho)$.

Proposition 1: The scheme $C_{\text{diag}(\mathcal{L}_{\text{Gold}})}(\rho)$ is not a DMT optimal code over the 4×1 MISO channel.

Proof: Suppose that we transmit a codeword $\text{diag}(X, X)$, where

$$X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}.$$

Given the channel vector $\mathbf{h} = [h_1, h_2, h_3, h_4]$ and the noise $\mathbf{w} = [w_1, w_2, w_3, w_4]$, the received signal is

$$\mathbf{y} = [y_1, y_2, y_3, y_4] = \mathbf{h} \cdot \text{diag}(X, X) + \mathbf{w}$$
$$= [h_1x_1 + h_2x_3, h_1x_2 + h_2x_4, h_3x_1 + h_4x_3, h_3x_2 + h_4x_4] + \mathbf{w}.$$

But this system is equivalent to

$$\begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix} = \begin{pmatrix} h_1 & h_2 \\ h_3 & h_4 \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} + \begin{pmatrix} w_1 & w_2 \\ w_3 & w_4 \end{pmatrix}.$$

We can see that the error performance of $\text{diag}(\mathcal{L}_{\text{Gold}})$ when received with a single antenna is exactly that of $\mathcal{L}_{\text{Gold}}$ when received with two antennas. The DMT for the coding scheme $\rho^{\frac{1}{2}-\frac{r}{4}}\mathcal{L}_{\text{Gold}}(\rho^{\frac{r}{4}})$ is is the piecewise linear function connecting the points $[r, (2-r)(2-r)^+]$ for integer values. However, this is not directly the DMT for $\rho^{\frac{1}{2}-\frac{r}{2}}\text{diag}(\mathcal{L}_{\text{Gold}})(\rho^{\frac{r}{2}})$. This is due to the fact that for the diagonal scheme we have $T = 4$ and therefore the diversity gain achieved with multiplexing gain r in the 4×1 channel corresponds to diversity gain $d(2r)$ in the 2×2 channel. We then see that the DMT of $\rho^{\frac{1}{2}-\frac{r}{2}}\text{diag}(\mathcal{L}_{\text{Gold}})(\rho^{\frac{r}{2}})$ is represented by a line connecting points $[r, (2-2r)(2-2r)^+]$, where $r = 0, \frac{1}{2}, 1$. On the other hand the DMT of the 4×1 MISO channel is simply a straight line between $[0, 4]$ and $[1, 0]$. □

This result shows that for a lattice $\mathcal{L} \subset M_n(\mathbb{C})$ of dimension smaller than $2n^2$ the NVD condition is not enough for the code to reach the optimal DMT.

Remark 4: We point out that while our counterexample involves coding schemes of the form (8), it generalizes to other schemes.

IV. The DMT of Real and Quaternion Space-Time Codes

In the previous sections we have seen that characterizing the DMT of asymmetric codes is a difficult task. In the rest of the paper we propose a new approach that applies to a large class of asymmetric codes. We will prove that if the codewords of the space-time scheme belong to a certain restricted set of matrices, its DMT is automatically upper bounded by a limit that is tighter than the general DMT bound. We then show that if the space-time code belongs to this class of codes, has suitable degree and satisfies the NVD condition, it achieves this restricted DMT. Later, in Section V, we show that codes satisfying these conditions can be

obtained from division algebras, and conclude that our DMT upper bounds are tight.

The asymmetric space-time codes we are considering live in the subspaces of the $2n^2$-dimensional real vector space $M_n(\mathbb{C})$. The first such subspace consists of all the real matrices inside $M_n(\mathbb{C})$ and we denote it with $M_n(\mathbb{R})$. The other subspace of interest consists of quaternionic matrices.

Let us assume that $2 \mid n$. We denote with $M_{n/2}(\mathbb{H})$ the set of quaternionic matrices

$$\begin{pmatrix} A & -B^* \\ B & A^* \end{pmatrix} \in M_n(\mathbb{C}),$$

where $*$ refers to complex conjugation and A and B are complex matrices in $M_{n/2}(\mathbb{C})$.

The spaces $M_{n/2}(\mathbb{H})$ and $M_n(\mathbb{R})$ are n^2-dimensional real subspaces of $M_n(\mathbb{C})$. It follows that if a lattice $\mathcal{L}$ is a subset of either of these subspaces, its dimension is at most n^2.

A. Equivalent channel model for real lattice codes

In this section, we focus on the special case where $\mathcal{C}(\rho) \subset M_n(\mathbb{R})$, i.e. the code is a set of real matrices.

First, we show that the channel model (1) is equivalent to a real channel with n transmit and $2m$ receive antennas.

We can write $H_c = H_r + iH_i$, $W_c = W_r + iW_i$, where H_r, H_i, W_r, W_i have i.i.d. real Gaussian entries with variance $1/2$. If $Y_c = Y_r + iY_i$, with $Y_r, Y_i \in M_{m\times n}(\mathbb{R})$, we can write an equivalent real system with $2m$ receive antennas:

$$Y = \begin{pmatrix} Y_r \\ Y_i \end{pmatrix} = \sqrt{\frac{\rho}{n}} \begin{pmatrix} H_r \\ H_i \end{pmatrix} \bar{X} + \begin{pmatrix} W_r \\ W_i \end{pmatrix} = \sqrt{\frac{\rho}{n}} H\bar{X} + W, \tag{11}$$

where $H \in M_{2m\times n}(\mathbb{R})$, $W \in M_{2m\times n}(\mathbb{R})$ have real i.i.d. Gaussian entries with variance $1/2$.

B. General DMT upper bound for real codes

Using the equivalent real channel, we can now establish a general upper bound for the DMT of real codes.

Theorem 3: Suppose that $\forall \rho$, $\mathcal{C}(\rho) \subset M_n(\mathbb{R})$. Then the DMT of the code $\mathcal{C}$ is upper bounded by the function $d_1(r)$ connecting the points $(r, [(m-r)(n-2r)]^+)$ where $2r \in \mathbb{Z}$.

Proof: The proof is an adaptation of the results of [2] to the real case, so we only provide the main steps[3].

Given a rate $R = r \log \rho$, the outage probability is lower bounded by

$$P_{\text{out}}(R) \geq \mathbb{P}\left\{ \frac{1}{2} \log\det(I + \rho H^T H) \leq R \right\}.$$

Let $L = \min(2m, n)$, and $\Delta = |n - 2m|$. Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_L > 0$ be the nonzero eigenvalues of $H^T H$. The joint probability distribution of $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_L)$ is given by [29][4]:

$$p(\boldsymbol{\lambda}) = K e^{-\sum_{i=1}^{L} \lambda_i} \prod_{i=1}^{L} \lambda_i^{\frac{\Delta-1}{2}} \prod_{i<j} (\lambda_i - \lambda_j) \tag{12}$$

for some constant K. Consider the change of variables $\lambda_i = \rho^{-\alpha_i}$ $\forall i$. The corresponding distribution for $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_L)$ in the set $\mathcal{A} = \{\boldsymbol{\alpha} : \alpha_1 \leq \cdots \leq \alpha_L\}$ is

$$p(\boldsymbol{\alpha}) = K (\log \rho)^L e^{-\sum_{i=1}^{L} \rho^{-\alpha_i}} \rho^{-\sum_{i=1}^{L} \alpha_i \left(\frac{\Delta+1}{2}\right)} \prod_{i<j} \left(\rho^{-\alpha_i} - \rho^{-\alpha_j}\right) \tag{13}$$

To simplify notation, we take $s = 2r$. Then we have

$$P_{\text{out}}(R) \dot{\geq} \mathbb{P}\left\{ \prod_{i=1}^{L} \rho^{(1-\alpha_i)^+} \leq \rho^s \right\} \geq \mathbb{P}(\mathcal{A}_0),$$

[3]A detailed proof can be found in the preprint version of this paper at https://arxiv.org/pdf/2102.09910.

[4]We have slightly modified the expression to be consistent with our notation. In [29], the author considers a matrix AA^T where each element of A is $\mathcal{N}(0, 1)$.

where

$$\mathcal{A}_0 = \left\{ \boldsymbol{\alpha} \in \mathcal{A} : \ \alpha_i \geq 0 \ \forall i = 1, \ldots, L, \ \sum_{i=1}^{L} (1-\alpha_i)^+ \leq s \right\}$$
$$= \left\{ \boldsymbol{\alpha} \in \mathcal{A} \colon \alpha_j \geq 0, \ \sum_{i=1}^{j} (1-\alpha_i) \leq s \ \forall j = 1, \ldots, L \right\}. \tag{14}$$

Consider $S_\delta = \{\boldsymbol{\alpha} \in \mathcal{A} : \ |\alpha_i - \alpha_j| > \delta \ \forall i \neq j\}$. Then one can show that

$$P_{\text{out}}(R) \dot{\geq} \int_{\mathcal{A}_0 \cap S_\delta} \rho^{-\sum_{i=1}^{L} \alpha_i N_i} d\boldsymbol{\alpha},$$

where $N_i = \frac{1}{2}(\Delta + 2L - 2i + 1)$.

Lemma 3: Let $f(\boldsymbol{\alpha}) = \sum_{i=1}^{L} (q + L + 1 - 2i)\alpha_i$. Then

$$\inf_{\boldsymbol{\alpha} \in \mathcal{A}_0} f(\boldsymbol{\alpha}) = (-q - L + 2\lfloor s \rfloor + 1)s + qL - \lfloor s \rfloor (\lfloor s \rfloor + 1) = f(\boldsymbol{\alpha}^*)$$

where $\alpha_1^* = \ldots = \alpha_{k-1}^* = 0$, $\alpha_k^* = k - s$, $\alpha_{k+1}^* = \ldots = \alpha_L^* = 1$ for $k = \lfloor s \rfloor + 1$.

The proof of Lemma 3 can be found in Appendix A. Using Lemma 3 with $q = \Delta + L$, $s = 2r$, we find that $\inf_{\boldsymbol{\alpha} \in \mathcal{A}_0} \sum_{i=1}^{L} N_i \alpha_i = \inf_{\boldsymbol{\alpha} \in \mathcal{A}_0} \frac{f(\boldsymbol{\alpha})}{2}$ is equal to

$$\frac{1}{2}\left[(-\Delta - 2L + 2\lfloor 2r \rfloor + 1)2r + (\Delta + L)L - \lfloor 2r \rfloor (\lfloor 2r \rfloor + 1)\right]$$
$$= (-2m - n + 2\lfloor 2r \rfloor + 1)r + mn - \frac{\lfloor 2r \rfloor (\lfloor 2r \rfloor + 1)}{2}.$$

This is the piecewise function $d_1(r)$ connecting the points $(r, [(m-r)(n-2r)]^+)$ where $2r \in \mathbb{Z}$.

Using the Laplace principle, $\forall \delta > 0$ we have

$$\lim_{\rho \to \infty} -\frac{\log P_{\text{out}}(R)}{\log \rho} \geq \inf_{\mathcal{A}_0 \cap S_\delta} \frac{f(\boldsymbol{\alpha})}{2}.$$

Note that $\forall \delta$, the point $\boldsymbol{\alpha}_\delta$ such that $\alpha_{\delta,i} = \alpha_i^* + \frac{\delta i}{L}$ is in $\mathcal{A}_0 \cap S_{\frac{\delta}{L}}$ and when $\delta \to 0$, $\boldsymbol{\alpha}_\delta \to \boldsymbol{\alpha}^*$. By continuity of f,

$$\lim_{\delta \to 0} \inf_{\mathcal{A}_0 \cap S_\delta} \frac{f(\boldsymbol{\alpha})}{2} = \frac{f(\boldsymbol{\alpha}^*)}{2} = d_1(r). \qquad \square$$

C. DMT of real lattice codes with NVD

In this section, we show that real spherically shaped lattice codes with the NVD property achieve the DMT upper bound of Theorem 3. This result extends Proposition 4.2 in [21].

Theorem 4: Let $\mathcal{L}$ be an n^2-dimensional lattice in $M_n(\mathbb{R})$, and consider the code $\mathcal{C}(\rho) = \rho^{-\frac{r}{n}} \mathcal{L}(\rho^{\frac{r}{n}})$. If $\mathcal{L}$ has the NVD property, then the DMT of the code $\mathcal{C}(\rho)$ under ML decoding is the function $d_1(r)$ connecting the points $(r, [(m-r)(n-2r)]^+)$ where $2r \in \mathbb{Z}$.

Proof: Since the upper bound has already been established in Theorem 3, we only need to prove that the DMT is lower bounded by $d_1(r)$. The following section follows very closely the proof in [4], and thus some details are omitted. To simplify notation, we assume that $\det_{min}(\mathcal{L}) = 1$.

We consider the sphere bound for the error probability for the equivalent real channel (11): for a fixed channel realization H,

$$P_e(H) \leq \mathbb{P}\left\{ \|W\|^2 > d_H^2/4 \right\}$$

where d_H^2 is the squared minimum distance in the received constellation:

$$d_H^2 = \frac{\rho}{n} \min_{\bar{X}, \bar{X}' \in \mathcal{C}(\rho), \ \bar{X} \neq \bar{X}'} \left\| H(\bar{X} - \bar{X}') \right\|^2$$
$$= \frac{1}{n} \rho^{1 - \frac{2r}{n}} \min_{X, X' \in \mathcal{L}(\rho^{\frac{r}{n}}), \ X \neq X'} \|H(X - X')\|^2.$$

We denote $\Delta X = X - X'$. Let $L = \min(2m, n)$, and $\Delta = |n - 2m|$. Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_L > 0$ be the nonzero eigenvalues of $H^T H$, and $0 \leq \mu_1 \leq \cdots \leq \mu_n$ the eigenvalues of $\Delta X \Delta X^T$. Using the mismatched eigenvalue bound and the arithmetic-geometric inequality as in [4], for all $k = 1, \ldots, L$

$$d_H^2 = \frac{1}{n} \rho^{1 - \frac{2r}{n}} \min_{X, X' \in \mathcal{L}(\rho^{\frac{r}{n}}), \ X \neq X'} \operatorname{tr}(H \Delta X \Delta X^T H^T)$$
$$\geq \frac{1}{n} \rho^{1 - \frac{2r}{n}} \sum_{i=1}^{L} \mu_i \lambda_i \geq \frac{k}{n} \rho^{1 - \frac{2r}{n}} \left(\prod_{i=1}^{k} \lambda_i \right)^{\frac{1}{k}} \left(\prod_{i=1}^{k} \mu_i \right)^{\frac{1}{k}}.$$

For all $i = 1, \ldots, n$, $\mu_i \leq \|\Delta X\|^2 \leq 4\rho^{\frac{2r}{n}}$, and $\prod_{i=1}^{n} \mu_i = \det(\Delta X \Delta X^T) \geq 1$ due to the NVD

property. Consequently, for all $k = 1, \dots, L$

$$\prod_{i=1}^{k} \mu_i = \frac{\det(\Delta X \Delta X^T)}{\prod_{i=k+1}^{n} \mu_i} \geq \frac{1}{4^{n-k} \rho^{\frac{2r(n-k)}{n}}}.$$

Consider the change of variables $\lambda_i = \rho^{-\alpha_i}$ $\forall i = 1, \dots, L$. For $k = 1, \dots, L$ we can write

$$d_H^2 \geq \frac{k}{n 4^{\frac{n-k}{k}}} \rho^{1-\frac{2r}{n}} \rho^{-\frac{1}{k}\sum_{i=1}^{k}\alpha_i} \frac{1}{\rho^{\frac{2r(n-k)}{nk}}} = c_k \rho^{\delta_k(\boldsymbol{\alpha}, s)}, \tag{15}$$

where $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_L)$, $s = 2r$, $c_k = \frac{k}{n 4^{\frac{n-k}{k}}}$ and

$$\delta_k(\boldsymbol{\alpha}, s) = -\frac{1}{k}\left(\sum_{i=1}^{k} \alpha_i + s - k\right). \tag{16}$$

Since $2\|W\|^2 \sim \chi^2(2mn)$, we have $\mathbb{P}\left\{2\|W\|^2 > d\right\} = \Phi_{2mn}(d)$, where

$$\Phi_t(d) = \sum_{i=0}^{t-1} e^{-d} \frac{d^i}{i!}. \tag{17}$$

The distribution $p(\boldsymbol{\alpha})$ in (13) is bounded by

$$p(\boldsymbol{\alpha}) \leq p'(\boldsymbol{\alpha}) = K e^{-\sum_{i=1}^{L} \rho^{-\alpha_i}} \rho^{-\sum_{i=1}^{L} \alpha_i N_i} (\log \rho)^L \tag{18}$$

where $N_i = \frac{1}{2}(\Delta + 2L - 2i + 1)$. By averaging over the channel, the error probability is upper bounded by

$$\begin{aligned} P_e &\leq \int_{\mathcal{A}} \mathbb{P}\left\{2\|W\|^2 > \frac{d_H^2}{2}\right\} p(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \\ &\leq \int_{\mathcal{A}} \Phi_{2mn}\left(\frac{d_H^2}{2}\right) p'(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \end{aligned} \tag{19}$$

where $\mathcal{A} = \{\boldsymbol{\alpha} \,:\, \alpha_1 \leq \dots \leq \alpha_L\}$.

The following Lemma closely follows [30], and it is proven in Appendix B:

Lemma 4: Assuming that $d \geq c_k \rho^{\delta_k(\boldsymbol{\alpha}, s)}$ for some constants c_k, $k = 1, \dots, L$, then for all $t \in \mathbb{N}^+$,

$$-\lim_{\rho \to \infty} \frac{1}{\log \rho} \log \int_{\mathcal{A}} p'(\boldsymbol{\alpha}) \Phi_t(d)\, d\boldsymbol{\alpha} \geq \inf_{\boldsymbol{\alpha} \in \mathcal{A}_0} \sum_{i=1}^{L} N_i \alpha_i,$$

where $\mathcal{A}_0$ is defined in (14).

The proof of the Theorem is concluded using Lemma 3 with $q = \Delta + L$, $s = 2r$. □

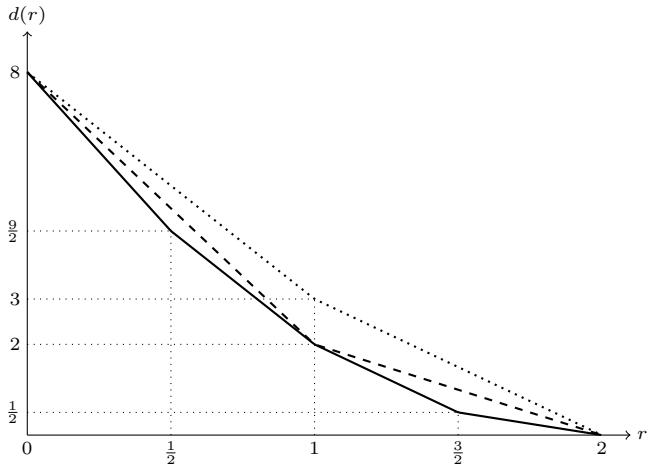

Fig. 1. DMT upper bounds for real (solid) and quaternion (dashed) codes for $n = 4$ and $m = 2$. The dotted lines correspond to the optimal DMT.

D. Equivalent channel model for quaternion lattice codes

Suppose that $n = 2p$ is even. We consider again the channel

$$Y_c = \sqrt{\frac{\rho}{n}} H_c \bar{X} + W_c, \tag{20}$$

and we suppose that the codewords $\bar{X}$ are of the form

$$\bar{X} = \begin{pmatrix} A & -B^* \\ B & A^* \end{pmatrix} \in M_{2p}(\mathbb{C}),$$

where $A, B \in M_p(\mathbb{C})$.

First, we derive an equivalent model where the channel has quaternionic form. We can write

$$Y_c = \begin{pmatrix} Y_1 & Y_2 \end{pmatrix}, \quad H_c = \begin{pmatrix} H_1 & H_2 \end{pmatrix}, \quad W_c = \begin{pmatrix} W_1 & W_2 \end{pmatrix},$$

where $Y_1, Y_2, H_1, H_2, W_1, W_2 \in M_{m \times p}(\mathbb{C})$. Then

$$\begin{aligned} Y_1 &= \sqrt{\frac{\rho}{n}}(H_1 A + H_2 B) + W_1, \\ Y_2 &= \sqrt{\frac{\rho}{n}}(-H_1 B^* + H_2 A^*) + W_2, \end{aligned}$$

and we have the equivalent "quaternionic channel":

$$\underbrace{\begin{pmatrix} Y_1 & Y_2 \\ -Y_2^* & Y_1^* \end{pmatrix}}_{Y} = \sqrt{\frac{\rho}{n}} \underbrace{\begin{pmatrix} H_1 & H_2 \\ -H_2^* & H_1^* \end{pmatrix}}_{H} \underbrace{\begin{pmatrix} A & -B^* \\ B & A^* \end{pmatrix}}_{\bar{X}} + \underbrace{\begin{pmatrix} W_1 & W_2 \\ -W_2^* & W_1^* \end{pmatrix}}_{W}.$$

E. General DMT upper bound for quaternion codes

Theorem 5: Suppose that $\forall \rho$, $\mathcal{C}(\rho) \subset M_{n/2}(\mathbb{H})$. Then the DMT of the code $\mathcal{C}$ is upper bounded by the function $d_2(r)$ connecting the points $(r, [(m-r)(n-2r)]^+)$ for $r \in \mathbb{Z}$.

Proof: The quaternionic channel can be written in the complex MIMO channel form

$$\begin{pmatrix} Y_1 \\ -Y_2^* \end{pmatrix} = \sqrt{\frac{\rho}{n}} \begin{pmatrix} H_1 & H_2 \\ -H_2^* & H_1^* \end{pmatrix} \begin{pmatrix} A \\ B \end{pmatrix} + \begin{pmatrix} W_1 \\ -W_2^* \end{pmatrix} \tag{21}$$

If r is the multiplexing gain of the original system (20), then the multiplexing gain of this channel is $2r$, since the same number of symbols is transmitted using half the frame length.

The proof follows once again the approach in [2]. Consider the eigenvalues $\lambda_1 = \lambda_1' \geq \lambda_2 = \lambda_2' \geq \cdots \geq \lambda_p = \lambda_p' \geq 0$ of $H^\dagger H$. Let $L = \min(m,p)$ the number of pairs of nonzero eigenvalues, and $\Delta = |p-m|$. For fixed H, the capacity of this channel is [31]

$$C(H) \doteq \log\det(I + \rho H^\dagger H) = 2\sum_{i=1}^{L} \log(1+\rho\lambda_i).$$

The joint eigenvalue density $p(\boldsymbol{\lambda}) = p(\lambda_1, \ldots, \lambda_L)$ of a quaternion Wishart matrix is [32][5]

$$p(\lambda_1, \ldots, \lambda_L) = K \prod_{i<j} (\lambda_i - \lambda_j)^4 \prod_{i=1}^{L} \lambda_i^{2\Delta+1} e^{-\sum_{i=1}^{L} \lambda_i}$$

for some constant K. With the change of variables $\lambda_i = \rho^{-\alpha_i}\ \forall i = 1, \ldots, L$, the distribution of $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_L)$ is

$$p(\boldsymbol{\alpha}) = K (\log\rho)^L e^{-\sum_{i=1}^{L} \rho^{-\alpha_i}} \rho^{-2\sum_{i=1}^{L} \alpha_i (\Delta+1)} \prod_{i<j} \left(\rho^{-\alpha_i} - \rho^{-\alpha_j}\right)^4$$

The outage probability for rate $R = r\log\rho$ is given by

$$P_{\text{out}}(R) \doteq \mathbb{P}\left\{ \prod_{i=1}^{L} \rho^{(1-\alpha_i)^+} < \rho^r \right\} \geq \mathbb{P}(\mathcal{A}_0)$$

where $\mathcal{A}_0 = \left\{ \boldsymbol{\alpha} : 0 \leq \alpha_1 \leq \ldots \leq \alpha_L,\ \sum_{i=1}^{L} (1-\alpha_i)^+ < r \right\}$. Given $\delta > 0$, define $S_\delta = \{\boldsymbol{\alpha} :\ |\alpha_i - \alpha_j| > \delta\ \forall i \neq j\}$. Then

$$P_{\text{out}}(R) \dot{\geq} \int_{\mathcal{A}_0 \cap S_\delta} \rho^{-\sum_{i=1}^{L} N_i \alpha_i} d\boldsymbol{\alpha}$$

where $N_i = 2(\Delta + 2L - 2i + 1)$. Let $f(\boldsymbol{\alpha}) = \sum_{i=1}^{L} (q + L - 2i + 1)$. Using the Laplace principle,

$$\lim_{\rho\to\infty} -\frac{\log P_{\text{out}}(R)}{\log\rho} \geq 2 \inf_{\mathcal{A}_0 \cap S_\delta} f(\alpha) \quad \forall \delta > 0.$$

Using Lemma 3 with $s = r$, $q = \Delta + L$, we find that $\inf_{\boldsymbol{\alpha} \in \mathcal{A}_0} N_i \alpha_i = 2f(\boldsymbol{\alpha}^*)$ is the piecewise linear function $d_2(r)$ connecting the points $(r, [2(p-r)(m-r)]^+) = (r, [(n-2r)(m-r)]^+)$ for $r \in \mathbb{Z}$. By continuity of f, $2\lim_{\delta\to 0} \inf_{\mathcal{A}_0 \cap S_\delta} f(\boldsymbol{\alpha}) = 2f(\boldsymbol{\alpha}^*) = d_2(r)$. □

F. DMT of quaternionic lattice codes with NVD

We now show that quaternionic lattice codes with NVD achieve the upper bound of Theorem 5. This result extends Proposition 4.3 in [21].

Theorem 6: Let $\mathcal{L}$ be an n^2-dimensional lattice in $M_{n/2}(\mathbb{H})$ with the NVD property. Then the DMT of the code $\mathcal{C}(\rho) = \rho^{-\frac{r}{n}} \mathcal{L}(\rho^{\frac{r}{n}})$ under ML decoding is the piecewise linear function $d_2(r)$ connecting the points $(r, [(m-r)(n-2r)]^+)$ for $r \in \mathbb{Z}$.

Proof: Assume $\det_{min}(\mathcal{L}) = 1$. For a fixed realization H, $P_e(H) \leq \mathbb{P}\left\{ \|W\|^2 > d_H^2/4 \right\}$, where

$$d_H^2 = \frac{1}{n} \rho^{1-\frac{2r}{n}} \min_{X, X' \in \mathcal{L}(\rho^{\frac{r}{n}}),\ X \neq X'} \|H(X - X')\|^2 .$$

Let $\Delta X = X - X'$. We denote by $\lambda_1 = \lambda_1' \geq \lambda_2 = \lambda_2' \geq \cdots \geq \lambda_p = \lambda_p' \geq 0$ the eigenvalues of $H^\dagger H$, and by $0 \leq \mu_1 = \mu_1' \leq \cdots \leq \mu_p = \mu_p'$ the eigenvalues of $\Delta X \Delta X^\dagger$. Both sets of eigenvalues have multiplicity 2 since H and X are quaternion matrices. Again we set $L = \min(m,p)$ and $\Delta = |p-m|$. Using the mismatched eigenvalue bound and the arithmetic-geometric mean inequality as in [4], for all $k = 1, \ldots, L$,

$$d_H^2 = \frac{1}{n} \rho^{1-\frac{2r}{n}} \min_{X, X' \in \mathcal{C}(\rho),\ X \neq X'} \operatorname{tr}(H \Delta X \Delta X^\dagger H^\dagger)$$

[5]The quaternion case corresponds to taking $\beta = 4$ in [32, equation (4.5)]. Note that we modify the distribution to take into account the fact that each entry of H has variance $1/2$ per real dimension.

$$\geq \frac{1}{n}\rho^{1-\frac{2r}{n}}\sum_{i=1}^{L}(2\mu_i\lambda_i) \geq \frac{k}{p}\rho^{1-\frac{2r}{n}}\left(\prod_{i=1}^{k}\lambda_i\right)^{\frac{1}{k}}\left(\prod_{i=1}^{k}\mu_i\right)^{\frac{1}{k}}$$

For all $i = 1,\ldots,p$, $\mu_i \leq \|\Delta X\|^2 \leq 4\rho^{\frac{2r}{n}}$, and $\prod_{i=1}^{p}\mu_i = \det(\Delta X\Delta X^\dagger)^{\frac{1}{2}} \geq 1$ using the NVD property. For all $k = 1,\ldots,L$

$$\prod_{i=1}^{k}\mu_i = \frac{\det(\Delta X\Delta X^\dagger)^{\frac{1}{2}}}{\prod_{i=k+1}^{p}\mu_i} \geq \frac{1}{4^{p-k}\rho^{\frac{r(p-k)}{p}}}.$$

Setting $\lambda_i = \rho^{-\alpha_i}\ \forall i = 1,\ldots,L$, we have

$$d_H^2 \geq c_k\rho^{1-\frac{r}{p}}\rho^{-\frac{1}{k}\sum_{i=1}^{k}\alpha_i}\rho^{-\frac{r(p-k)}{pk}} = c_k\rho^{\delta_k(\boldsymbol{\alpha})} \qquad (22)$$

for $k = 1,\ldots,L$, where $\boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_L)$, $\delta_k(\boldsymbol{\alpha}, r) = -\frac{1}{k}\left(\sum_{i=1}^{k}\alpha_i + r - k\right)$, and $c_k = \frac{k}{p4^{\frac{p-k}{k}}}$. Since $\|W\|^2 = 2\|W_1\|^2 + 2\|W_2\|^2 \sim \chi^2(4mp)$, we have

$$P_e(H) \leq \mathbb{P}\left\{\|W\|^2 > \frac{d_H^2}{4}\right\} = \Phi_{4mp}\left(\frac{d_H^2}{4}\right),$$

where Φ_t is defined in (17). By averaging with respect to $p(\boldsymbol{\alpha})$, we get

$$P_e \dot{\leq} \int_{\mathcal{A}} p'(\boldsymbol{\alpha})\Phi_{4mp}\left(\frac{d_H^2}{4}\right)d\boldsymbol{\alpha}$$

where $\mathcal{A} = \{\boldsymbol{\alpha} : \alpha_1 \leq \cdots \leq \alpha_L\}$, and

$$p'(\boldsymbol{\alpha}) = K(\log\rho)^L e^{-\sum_{i=1}^{L}\rho^{-\alpha_i}}\rho^{-\sum_{i=1}^{L}\alpha_i N_i},$$

where $N_i = 2(\Delta + 2L - 2i + 1)$. From Lemma 4 we find $d(r) \geq \inf_{\boldsymbol{\alpha}\in\mathcal{A}_0} 2\sum_{i=1}^{L}\alpha_i(\Delta+2L-2i+1)$, which by Lemma 3 is the piecewise linear function connecting the points $(r, [(n-2r)(m-r)]^+)$ for $r \in \mathbb{Z}$. □

V. Division Algebra Codes Achieve the Optimal Restricted DMT in $M_{n/2}(\mathbb{H})$ and $M_n(\mathbb{R})$

Theorems 4 and 6 state that n^2-dimensional NVD lattices in $M_n(\mathbb{R})$ and $M_{n/2}(\mathbb{H})$ do achieve the respective DMT upper bounds of Theorems 3 and 5. In order to show that these bounds are tight and indeed describe the optimal restricted DMTs, it is enough to prove the existence of n^2-dimensional NVD lattice codes in $M_n(\mathbb{R})$ and $M_{n/2}(\mathbb{H})$. For that we need some results from non-commutative algebra. For details and definitions we refer the reader to [33].

Let $\mathcal{D}$ be an index n $\mathbb{Q}$-central division algebra. We say that $\mathcal{D}$ is *ramified at the infinite place* if

$$\mathcal{D}\otimes_{\mathbb{Q}}\mathbb{R} \simeq M_{n/2}(\mathbb{H}).$$

If it is not, then

$$\mathcal{D}\otimes_{\mathbb{Q}}\mathbb{R} \simeq M_n(\mathbb{R}).$$

Let Λ be an *order* in an index n $\mathbb{Q}$-central division algebra $\mathcal{D}$. We then have the following.

Lemma 5: [16] If the infinite prime is ramified in the algebra $\mathcal{D}$, then there exists an embedding

$$\psi_{\text{abs}} : \mathcal{D} \to M_{n/2}(\mathbb{H})$$

such that $\psi_{\text{abs}}(\Lambda)$ is an n^2-dimensional NVD lattice. If $\mathcal{D}$ is not ramified at the infinite place, then there exists an embedding

$$\psi_{\text{abs}} : \mathcal{D} \to M_n(\mathbb{R})$$

such that $\psi_{\text{abs}}(\Lambda)$ is an n^2-dimensional NVD lattice. For every n there exists an index n $\mathbb{Q}$-central division algebra that is ramified at the infinite place and one which is not.

The following corollary follows from Theorems 4 and 6 and from Lemma 5. It proves that the upper bounds in Theorems 3 and 5 are tight.

Corollary 2: For every n there exists an n^2-dimensional NVD lattice $\mathcal{L} \subset M_n(\mathbb{R})$ that achieves the upper bound of Theorem 3. For every even n there exists an n^2-dimensional NVD lattice $\mathcal{L} \subset M_{n/2}(\mathbb{H})$ that achieves the upper bound of Theorem 5.

The following corollary gives us a complete DMT characterization of $\mathbb{Q}$-central division algebra codes. The DMT of such codes only depends on whether the corresponding algebra is ramified at the infinite place or not.

Corollary 3: Let Λ be an order in an index n $\mathbb{Q}$-central division algebra $\mathcal{D}$. If $\mathcal{D}$ is ramified at the infinite place, then the code $\psi_{\rm abs}(\Lambda) \subset M_{n/2}(\mathbb{H})$ achieves the upper bound of Theorem 5. If $\mathcal{D}$ is not ramified at the infinite place, then the DMT of the code $\psi_{\rm abs}(\Lambda) \subset M_n(\mathbb{R})$ achieves the upper bound of Theorem 3.

A. DMT of $\mathbb{Q}$ central division algebra codes based on the regular representation

In the previous sections we classified the DMT of all $\mathbb{Q}$-central division algebra codes. However, this result was proven in the case where the code lattices were constructed using the abstract embedding of Lemma 5. In contrast, explicit codes are typically built using *regular representations*. In this section we study the DMT of division algebra codes that are constructed by using such representations.

Let $E/\mathbb{Q}$ be a cyclic field extension of degree n with Galois group $G(E/\mathbb{Q}) = \langle \sigma \rangle$. Define a cyclic algebra

$$\mathcal{D} = (E/\mathbb{Q}, \sigma, \gamma) = E \oplus uE \oplus u^2E \oplus \cdots \oplus u^{n-1}E,$$

where $u \in \mathcal{D}$ is an auxiliary generating element subject to the relations $xu = u\sigma(x)$ for all $x \in E$ and $u^n = \gamma \in \mathbb{Q}^*$.

Considering $\mathcal{D}$ as a right vector space over E, every element $x = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathcal{D}$ has the following left regular representation as a matrix $\psi_{reg}(x)$:

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}.$$

The mapping ψ_{reg} is an injective $\mathbb{Q}$-algebra homomorphism that allows us to identify $\mathcal{D}$ with its image in $M_n(\mathbb{C})$.

Proposition 2: [33] If Λ is a $\mathbb{Z}$-order in an index n $\mathbb{Q}$-central division algebra $\mathcal{D}$, then $\psi_{reg}(\Lambda)$ is an n^2-dimensional NVD lattice in $M_n(\mathbb{C})$.

Example 3: Consider the following two algebras

$$\mathcal{A}_1 = (\mathbb{Q}(\sqrt{3})/\mathbb{Q}, \sigma, -1) \text{ and } \mathcal{A}_2 = (\mathbb{Q}(i)/\mathbb{Q}, \sigma, -1).$$

Let us use the notation $\mathbb{Z}[\sqrt{3}] = \mathbb{Z} + \mathbb{Z}\sqrt{3}$ and $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$. By using regular presentation ψ_{reg}, we can find the following 4-dimensional lattice codes

$$\mathcal{L}_1 = \left\{ \begin{pmatrix} x_1 & -x_2 \\ x_2 & x_1 \end{pmatrix} : \quad x_1, x_2 \in \mathbb{Z}[\sqrt{3}] \right\},$$

$$\mathcal{L}_2 = \left\{ \begin{pmatrix} x_1 & -x_2^* \\ x_2 & x_1^* \end{pmatrix} : \quad x_1, x_2 \in \mathbb{Z}[i] \right\}.$$

Here $\mathcal{L}_1$ corresponds to the algebra $\mathcal{A}_1$ [17], while $\mathcal{L}_2$ corresponds to the algebra $\mathcal{A}_2$ and is the lattice of the Alamouti code. As $\mathcal{L}_1$ is completely real and $\mathcal{L}_2$ is quaternionic, we can read their DMTs from Theorems 4 and 6. Here the DMT of Alamouti was already known, while the DMT of $\mathcal{L}_2$ is a new result.

However, in general, while the lattices of Proposition 2 have the correct dimension and the NVD property, there is no guarantee that they are always contained in $M_n(\mathbb{R})$ or in $M_{n/2}(\mathbb{H})$ and we can not directly apply Theorems 4 and 6. However, the following result shows that all the lattices produced by regular representations are conjugated versions of lattices whose DMT we know:

Lemma 6: [20, Lemma 9.10] Let $\mathcal{D}$ be an index n $\mathbb{Q}$-central division algebra and $\Lambda \subset \mathcal{D}$ an order. If the infinite prime is ramified in the algebra $\mathcal{D}$, then there exists an invertible matrix $A \in M_n(\mathbb{C})$ such that

$$A\psi_{reg}(\Lambda)A^{-1} = \psi_{abs}(\Lambda) \subset M_{n/2}(\mathbb{H}).$$

If $\mathcal{D}$ is not ramified at the infinite place, then there exists an invertible matrix $B \in M_n(\mathbb{C})$ such that

$$B\psi_{reg}(\Lambda)B^{-1} = \psi_{abs}(\Lambda) \subset M_n(\mathbb{R}).$$

The following conjecture then seems to be plausible, but its proof has eluded us.

Conjecture 2: Let $\mathcal{D}$ be an index n $\mathbb{Q}$-central division algebra and $\Lambda \subset \mathcal{D}$ an order. If $\mathcal{D}$ is ramified at the infinite prime, then the DMT of $\psi_{reg}(\Lambda)$ under ML decoding is equal to the DMT upper bound of Theorem 5. If $\mathcal{D}$ is not ramified at the infinite prime, then the DMT of $\psi_{reg}(\Lambda)$ under ML decoding is equal to the DMT upper bound of Theorem 3.

Example 4: Applying the regular representation to the algebra $\mathcal{D}_1 = (\mathbb{Q}(i)/\mathbb{Q}, \sigma, 3)$ yields the following lattice

$$\mathcal{L}_1 = \left\{ \begin{pmatrix} x_1 & 3x_2^* \\ x_2 & x_1^* \end{pmatrix} : \quad x_1, x_2 \in \mathbb{Z}[i] \right\}.$$

We can easily see that $\mathcal{D}_1$ is not ramified at the infinite place, but on the other hand $\mathcal{L}_1 \nsubseteq M_2(\mathbb{R})$. However, our conjecture claims that the DMT of $\mathcal{L}_1$ is described by Theorem 3.

VI. Multi-block codes

When introducing the concept of diversity-multiplexing trade-off in [2] the authors mostly focused on one shot quasi-static channels. However, they also considered a channel model where it is possible to decode and encode over a fixed number of independent faded blocks and found the corresponding optimal DMT curve.

In this section we consider such multi-block channels

$$Y_c^{(l)} = \sqrt{\frac{\rho}{n}} H_c^{(l)} \bar{X}^{(l)} + W_c^{(l)}, \quad l = 1, \ldots, k, \qquad (23)$$

where $H_c^{(l)}, W_c^{(l)} \in M_{m,n}(\mathbb{C})$ are the channel and noise matrices with i.i.d. circularly symmetric complex Gaussian entries in $\mathcal{N}_{\mathbb{C}}(0,1)$. The set of multi-block codewords $X = [X^{(1)}, \ldots, X^{(k)}]$ should satisfy the global power constraint

$$\frac{1}{kn^2} \frac{1}{|\mathcal{C}|} \sum_{X \in \mathcal{C}} \sum_{l=1}^{k} \left\| X^{(l)} \right\|_F^2 \leq 1. \qquad (24)$$

A *multi-block matrix lattice* $\mathcal{L} \subseteq M_{n \times nk}(\mathbb{C})$ has the form

$$\mathcal{L} = \mathbb{Z}B_1 \oplus \mathbb{Z}B_2 \oplus \cdots \oplus \mathbb{Z}B_d,$$

where the matrices $B_1, \ldots, B_d \in M_{n \times nk}(\mathbb{C})$ are linearly independent over $\mathbb{R}$, and $d \leq 2n^2k$ is the dimension of the lattice.

We then have a natural extension for the NVD condition. First we define

$$\mathrm{pdet}(X) = \prod_{i=1}^{k} \det(X^i).$$

Definition 8: Given a multi-block lattice $\mathcal{L} \subseteq M_{n \times nk}(\mathbb{C})$, we say that the lattice satisfies the *non-vanishing determinant* (NVD) property if

$$\inf_{X \in L \setminus \{\mathbf{0}\}} |\mathrm{pdet}(X)| > 0.$$

Given a multi-block lattice $\mathcal{L} \subseteq M_{n \times nk}(\mathbb{C})$ of dimension d, we consider spherically shaped multi-block codes of the form

$$\mathcal{C}(\rho) = \rho^{-\frac{rnk}{d}} \mathcal{L}(\rho^{\frac{rnk}{d}}). \qquad (25)$$

Note that such a code will satisfy the power constraint (24), and its multiplexing gain is r.

A general DMT upper bound for multi-block codes $\mathcal{C} \subset M_n(\mathbb{C})^k$ was given in [2, Section V]. In [34] it was proven that $2n^2k$-dimensional lattice multi-block codes with the NVD property achieve this DMT upper bound, extending the result of [4] to the multi-block case. However, as in the case of the single block channel, the DMT of asymmetric multi-block codes is mostly unknown.

We will now consider multi-block codes that are subsets of $M_{n \times n}(\mathbb{R})^k$ or $M_{n/2}(\mathbb{H})^k$, and show that if the codewords of a space-time code belong to either of these spaces, its DMT is limited by a bound that is tighter than the general DMT bound and depends on the ambient space. We then show that if a space-time lattice code belongs to $M_n(\mathbb{R})^k$ or $M_{n/2}(\mathbb{H})^k$, has degree n^2k and satisfies the NVD condition, it achieves the corresponding restricted DMT. Furthermore, we prove that division algebra based codes do achieve these restricted DMT limits for every k and n.

Let us now assume we have a degree k number field K with signature (r_1, r_2), and an index n K-central division algebra $\mathcal{D}$. We then have that

$$\mathcal{D}\otimes_{\mathbb{Q}}\mathbb{R} \cong M_{n/2}(\mathbb{H})^{\omega} \times M_n(\mathbb{R})^{r_1-\omega} \times M_n(\mathbb{C})^{2r_2}, \quad (26)$$

where $\omega \leq r_1$ is an integer depending on the structure of the algebra $\mathcal{D}$. We call the triplet $(\omega, r_1 - \omega, r_2)$ the *signature* of the algebra $\mathcal{D}$. We note that this result is an extension of Lemma 6. The signature of $\mathbb{Q}$ is $(1, 0)$. Hence any $\mathbb{Q}$-central division algebra has signature $(\omega, 1-\omega, 0)$. When $\omega = 1$ the algebra is ramified at the infinite prime and when $\omega = 0$ it is not.

Proposition 3: [16] Let $\mathcal{D}$ be a K-central division algebra with signature $(\omega, r_1 - \omega, r_2)$ of index n and Λ an order in $\mathcal{D}$. Then $\psi_{abs}(\Lambda)$ is a kn^2 dimensional lattice in $M_{n/2}(\mathbb{H})^{\omega} \times M_n(\mathbb{R})^{r_1-\omega} \times M_n(\mathbb{C})^{2r_2}$ and

$$\det_{min}\left(\psi_{abs}(\Lambda)\right) = 1.$$

Lemma 7: For any integer n and triplet $(\omega, r_1 - \omega, r_2)$ there exist a number field K and a K-central index n division algebra $\mathcal{D}$ with signature $(\omega, r_1 - \omega, r_2)$.

In particular, according to Proposition 3, for any n (respectively for any even n) and for any k, there exists a kn^2-dimensional multi-block code with NVD in $M_n(\mathbb{R})^k$ (respectively in $M_{n/2}(\mathbb{H})^k$).

A. Real multi-block codes

We have the following multi-block extensions of Theorems 3 and 4:

Theorem 7: Suppose that $\forall \rho$, $\mathcal{C}(\rho) \subset M_n(\mathbb{R})^k$. Then the DMT of the code $\mathcal{C}$ is upper bounded by $kd_1(r)$, where $d_1(r)$ is the function connecting the points $(r, [(m-r)(n-2r)]^+)$ for $2r \in \mathbb{Z}$.

Theorem 8: Let $\mathcal{L}$ be an n^2k-dimensional lattice in $M_n(\mathbb{R})^k$, and consider the spherically shaped code $\mathcal{C}(\rho) = \rho^{-\frac{r}{n}}\mathcal{L}(\rho^{\frac{r}{n}})$. If $\mathcal{L}$ has the NVD property, then the DMT of the code $\mathcal{C}(\rho)$ under ML decoding is the function $kd_1(r)$.

The proof of Theorems 7 and 8 can be found in Appendix C.

We then have the following corollary that follows directly from Theorem 8 and Lemma 7.

Corollary 4: For every n and k there exists a kn^2-dimensional NVD lattice $\mathcal{L} \subset M_n(\mathbb{R})^k$ that achieves the DMT of Theorem 7.

B. Quaternion multi-block codes

Similarly, we can extend Theorems 5 and 6 to the multi-block case:

Theorem 9: Suppose that $\forall \rho$, $\mathcal{C}(\rho) \subset M_{n/2}(\mathbb{H})^k$. Then the DMT of the code $\mathcal{C}$ is upper bounded by $kd_2(r)$, where $d_2(r)$ is the function connecting the points $(r, [(m-r)(n-2r)]^+)$ for $r \in \mathbb{Z}$.

Theorem 10: Let $\mathcal{L}$ be an n^2k-dimensional lattice in $M_{n/2}(\mathbb{H})^k$, and consider the spherically shaped code $\mathcal{C}(\rho) = \rho^{-\frac{r}{n}}\mathcal{L}(\rho^{\frac{r}{n}})$. If $\mathcal{L}$ has the NVD property, then the DMT of the code $\mathcal{C}(\rho)$ under ML decoding is the function $kd_2(r)$.

The proof of these Theorems can be found in Appendix D.

According to Lemma 7 we now have the following.

Corollary 5: For every even n and any k there exists a kn^2-dimensional NVD lattice $\mathcal{L} \subset M_{n/2}(\mathbb{H})^k$ that achieves the DMT of Theorem 9.

ACKNOWLEDGEMENTS

The authors acknowledge the support of ENSEA (AAP SRV 2018) for funding R. Vehkalahti's visit to ETIS in 2018.

The authors would like to thank the three anonymous reviewers for their detailed comments and suggestions which helped to improve the paper.

APPENDIX

A. Proof of Lemma 3

Let $\bar{d}(s) = (-q-L+2\lfloor s \rfloor +1)s+qL-\lfloor s \rfloor (\lfloor s \rfloor +1)$. Without loss of generality, we can suppose that $k-1 \leq s < k$ for some $k \in \mathbb{N}$, i.e. $k-1 = \lfloor s \rfloor$, $k = \lfloor s \rfloor + 1$. First, we show that $\forall \boldsymbol{\alpha} \in \mathcal{A}_0$, we have $f(\boldsymbol{\alpha}) \geq \bar{d}(s)$. In fact

$$
\begin{aligned}
f(\boldsymbol{\alpha}) &= (q-L-1)\sum_{i=1}^{L}\alpha_i + 2\sum_{i=1}^{L}(L-i+1)\alpha_i \\
&= (q-L-1)\sum_{i=1}^{L}\alpha_i + 2\sum_{i=1}^{L}\sum_{j=1}^{i}\alpha_j \\
&\geq (q-L-1)(L-s) + 2\sum_{i=k}^{L}\sum_{j=1}^{i}\alpha_j \\
&\geq (q-L-1)(L-s) + 2\sum_{i=k}^{L}(i-s) \\
&= (q-L-1)(L-s) + L(L+1) - (k-1)k - 2(L-k+1)s \\
&= \bar{d}(s).
\end{aligned}
$$

Next, we show that $\exists \boldsymbol{\alpha}^*$ such that $f(\boldsymbol{\alpha}^*) = \bar{d}(s)$. Let $\alpha_1^* = \ldots = \alpha_{k-1}^* = 0$, $\alpha_k^* = k-s$, $\alpha_{k+1}^* = \ldots = \alpha_L^* = 1$. Then

$$
\begin{aligned}
f(\boldsymbol{\alpha}^*) &= \sum_{i=1}^{L}(q+L+1)\alpha_i - 2\sum_{i=1}^{L} i\alpha_i \\
&= (q+L+1)(L-s) - 2k(k-s) - 2\sum_{i=k+1}^{L} i \\
&= (q+L+1)(L-s) - 2k(k-s) - L(L+1) + k(k+1) \\
&= \bar{d}(s) \qquad \square
\end{aligned}
$$

B. Proof of Lemma 4

The proof closely follows [30], which is a preliminary version of [4]. Note that $\Phi_t(d) \leq 1$ since it is a probability. Given $\varepsilon > 0$, we can bound the integral (19) as follows:

$$
\begin{aligned}
&\int_{\mathcal{A}} p'(\boldsymbol{\alpha})\Phi_t(d)\, d\boldsymbol{\alpha} \\
&\leq \int_{\bar{\mathcal{A}}} p'(\boldsymbol{\alpha})\Phi_t(d)\, d\boldsymbol{\alpha} + \sum_{j=1}^{L}\int_{\mathcal{A}_j} p'(\boldsymbol{\alpha})\Phi_t(d)\, d\boldsymbol{\alpha},
\end{aligned} \tag{27}
$$

where $\bar{\mathcal{A}} = \{\boldsymbol{\alpha} \in \mathcal{A} \ : \ \alpha_i \geq -\varepsilon \ \ \forall i = 1, \ldots, L\}$ and $\mathcal{A}_j = \{\boldsymbol{\alpha} \in \mathcal{A} \ : \ \alpha_j < -\varepsilon\}$. Note that

$$
\begin{aligned}
&\int_{\mathcal{A}_j} p'(\boldsymbol{\alpha})\Phi_t(d)\, d\boldsymbol{\alpha} \leq \int_{\mathcal{A}_j} p'(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \\
&\dot{\leq} \left(\prod_{i\neq j}\int_{-\infty}^{\infty} e^{-\rho^{-\alpha_i}}\rho^{-\alpha_i N_i} d\alpha_i\right)\int_{-\infty}^{-\varepsilon} e^{-\rho^{-\alpha_j}}\rho^{-\alpha_j N_j} d\alpha_j \\
&= \left(\prod_{i\neq j}\int_{0}^{\infty} \frac{e^{-\lambda_i}\lambda_i^{N_i-1}}{\log\rho} d\lambda_i\right)\int_{\rho^{\varepsilon}}^{\infty} \frac{\lambda_j^{N_j-1}e^{-\lambda_j}}{\log\rho} d\lambda_j \\
&\doteq \rho^0 \int_{\rho^{\varepsilon}}^{\infty} \frac{\lambda_j^{N_j-1}e^{-\lambda_j}}{\log\rho} d\lambda_j
\end{aligned}
$$

which vanishes exponentially fast as a function of ρ. For the first term in (27), we have

$$
\begin{aligned}
&\int_{\bar{\mathcal{A}}} p'(\boldsymbol{\alpha})\Phi_t(d)\, d\boldsymbol{\alpha} \\
&\quad \leq \int\limits_{\substack{\boldsymbol{\alpha}>-\varepsilon \\ \boldsymbol{\delta}(\alpha,s)<\varepsilon}} p'(\boldsymbol{\alpha})\Phi_t(d)\, d\boldsymbol{\alpha} + \sum_{j=1}^{L}\int\limits_{\substack{\boldsymbol{\alpha}>-\epsilon, \\ \delta_j(\boldsymbol{\alpha},s)\geq\varepsilon}} p'(\boldsymbol{\alpha})\Phi_t(d)\, d\boldsymbol{\alpha},
\end{aligned}
$$

where the notation $\boldsymbol{\alpha} > -\epsilon$ means $\alpha_i > -\epsilon \ \ \forall i = 1, \ldots, L$, and $\boldsymbol{\delta}(\boldsymbol{\alpha}, s) = (\delta_1(\boldsymbol{\alpha}, s), \ldots, \delta_L(\boldsymbol{\alpha}, s))$. Since $\Phi_t(d)$ is a decreasing function of d, using the assumption that $d \geq c_j\rho^{\delta_j(\boldsymbol{\alpha},s)} \ \forall j = 1, \ldots, L$, (15) we can write

$$
\begin{aligned}
&\int\limits_{\substack{\boldsymbol{\alpha}>-\epsilon, \\ \delta_j(\boldsymbol{\alpha},s)\geq\varepsilon}} p'(\boldsymbol{\alpha})\Phi_t(d)\, d\boldsymbol{\alpha} \dot{\leq} \int\limits_{\substack{\boldsymbol{\alpha}>-\epsilon, \\ \delta_j(\boldsymbol{\alpha},s)\geq\varepsilon}} p'(\boldsymbol{\alpha})\Phi_t\left(c_j\rho^{\delta_j(\boldsymbol{\alpha},s)}\right) d\boldsymbol{\alpha} \\
&\dot{\leq} \left(\prod_{i=j+1}^{L}\int\limits_{\alpha_i>-\varepsilon} \rho^{-\alpha_i N_i} d\alpha_i\right) \\
&\cdot \int\limits_{\substack{\alpha_1,\ldots,\alpha_j>-\varepsilon \\ \delta_j(\boldsymbol{\alpha},s)\geq\varepsilon}} e^{-c_j\rho^{\delta_j(\boldsymbol{\alpha},s)}} \sum_{\tau=0}^{t-1}\left(c_j\rho^{\delta_j(\boldsymbol{\alpha},s)}\right)^{\tau}\frac{1}{\tau!}\rho^{-\sum_{i=1}^{j}\alpha_i N_i}\prod_{i=1}^{j} d\alpha_i
\end{aligned}
$$

since $\delta_j(\boldsymbol{\alpha}, s)$ is independent of α_i for $i > j$. As $\delta_j(\boldsymbol{\alpha}, s) \geq \varepsilon$, $\alpha_i > -\varepsilon$, the second integral is over a

bounded region and tends to zero exponentially fast as a function of ρ, while the first integral has a finite SNR exponent. Thus, the previous expression tends to zero exponentially fast.

Finally, the SNR exponent of (19) is determined by the behavior of

$$\int\limits_{\substack{\boldsymbol{\alpha}>-\varepsilon \\ \boldsymbol{\delta}(\boldsymbol{\alpha},s)<\varepsilon}} p'(\boldsymbol{\alpha})\Phi_t\left(d\right)d\boldsymbol{\alpha} \leq \int\limits_{\substack{\boldsymbol{\alpha}>-\varepsilon \\ \boldsymbol{\delta}(\boldsymbol{\alpha},s)<\varepsilon}} p'(\boldsymbol{\alpha})d\boldsymbol{\alpha}$$

$$\dot{\leq} \int\limits_{\substack{\boldsymbol{\alpha}>-\varepsilon \\ \boldsymbol{\delta}(\boldsymbol{\alpha},s)<\varepsilon}} \rho^{-\sum\limits_{i=1}^{n} N_i\alpha_i} d\boldsymbol{\alpha}.$$

The conclusion follows by using the Laplace principle, and taking $\epsilon \to 0$. Note that

$$\mathcal{A}_0 = \left\{\boldsymbol{\alpha} \in \mathcal{A} :\ \alpha_j \geq 0,\ \sum_{i=1}^{j}(1-\alpha_i) \leq s\ \forall j = 1,\ldots,L\right\}$$

$$= \{\boldsymbol{\alpha} : \alpha_j \geq 0,\ \delta_j(\boldsymbol{\alpha},s) \leq 0\ \ \forall j = 1,\ldots,L\}. \qquad \square$$

C. Proof of Theorems 7 and 8 (DMT of real multi-block codes)

Consider a multi-block lattice $\mathcal{L} \subset M_n(\mathbb{R})^k$ of dimension $d = n^2k$, and a multi-block code $\mathcal{C}(\rho) = \rho^{-\frac{r}{n}}\mathcal{L}(\rho^{\frac{r}{n}})$. Every codeword is of the form $X = [X^{(1)},\ldots,X^{(k)}]$.

Similarly to the single-block case, for all $l = 1,\ldots,k$ we can write

$$Y_c^{(l)} = Y_r^{(l)} + iY_i^{(l)},\ H_c^{(l)} = H_r^{(l)} + iH_i^{(l)},\ W_c^{(l)} = W_r^{(l)} + iW_i^{(l)}$$

and obtain the equivalent real channel with $2m$ receive antennas:

$$Y_c^{(l)} = \begin{pmatrix} Y_r^{(l)} \\ Y_i^{(l)} \end{pmatrix} = \sqrt{\frac{\rho}{n}} \begin{pmatrix} H_r^{(l)} \\ H_i^{(l)} \end{pmatrix} X^{(l)} + \begin{pmatrix} W_r^{(l)} \\ W_i^{(l)} \end{pmatrix}$$

$$= H^{(l)}X^{(l)} + W^{(l)},$$

where $H^{(l)} \in M_{2m\times n}(\mathbb{R})$, $W^{(l)} \in M_{2m\times n}(\mathbb{R})$ have real i.i.d. Gaussian entries with variance $1/2$.

1) Proof of Theorem 7: We can write the outage probability as

$$P_{\text{out}}(R) = \mathbb{P}\left\{\frac{1}{k}\left(\frac{1}{2}\sum_{l=1}^{k}\log\det(I+\rho(H^{(l)})^TH^{(l)})\right) \leq R\right\}.$$

Define $L = \min(2m,n)$, $\Delta = |n-2m|$, and let

$$\lambda_1^{(l)} \geq \cdots \geq \lambda_L^{(l)}, \quad l = 1,\ldots,k$$

the ordered nonzero eigenvalues of $(H^{(l)})^TH^{(l)}$. Their distribution is

$$p(\lambda_1^{(l)},\ldots,\lambda_L^{(l)}) = K\prod_{i=1}^{L}(\lambda_i^{(l)})^{\frac{\Delta-1}{2}} e^{-\sum\limits_{i=1}^{L}\lambda_i^{(l)}} \prod_{i<j}\left|\lambda_i^{(l)} - \lambda_j^{(l)}\right|$$

for $l = 1,\ldots,k$. Thus, we can write the outage probability as

$$P_{\text{out}}(R) = \mathbb{P}\left\{\prod_{l=1}^{k}\prod_{i=1}^{L}(1+\rho\lambda_i^{(l)})^{1/2} \leq \rho^{rk}\right\}.$$

Consider the change of variables $\lambda_i^{(l)} = \rho^{-\alpha_i^{(l)}}\ \forall l = 1,\ldots,k$, and let

$$\mathcal{A} = \left\{\boldsymbol{\alpha} \in \mathbb{R}^{kL}\ :\ 0 \leq \alpha_1^{(l)} \leq \cdots \leq \alpha_L^{(l)}\ \ \forall l = 1,\ldots,k\right\}$$

Then

$$p(\boldsymbol{\alpha}) \doteq \rho^{-\sum\limits_{l=1}^{k}\sum\limits_{i=1}^{L}\frac{\Delta+1}{2}\alpha_i^{(l)}} e^{-\sum\limits_{l=1}^{k}\sum\limits_{i=1}^{L}\rho^{-\alpha_i^{(l)}}} \prod_{l=1}^{k}\prod_{i<j}\left|\rho^{-\alpha_i^{(l)}} - \rho^{-\alpha_j^{(l)}}\right|. \tag{28}$$

Recalling that $1+\rho^{1-x} \dot{\leq} \rho^{(1-x)^+}$, we have

$$P_{\text{out}}(R) = \mathbb{P}\left\{\prod_{l=1}^{k}\prod_{i=1}^{L}(1+\rho^{1-\alpha_i^{(l)}})^{1/2} \leq \rho^{rk}\right\} \geq \mathbb{P}(\mathcal{A}_0),$$

where

$$\mathcal{A}_0 = \left\{\boldsymbol{\alpha} \in \mathcal{A}\ :\ \frac{1}{2}\sum_{l=1}^{k}\sum_{i=1}^{L}(1-\alpha_i^{(l)})^+ \leq rk\right\}$$

$$= \left\{\boldsymbol{\alpha} \in \mathcal{A}\ :\ \forall \mathbf{j} \leq L,\ \frac{1}{2}\sum_{j=1}^{k}\sum_{i=1}^{j_l}(1-\alpha_i^{(l)}) \leq rk\right\}.$$

In the previous expression, given $\mathbf{j} = (j_1,\ldots,j_k)$, the notation $\mathbf{j} \leq L$ means $j_l \leq L$ for all $l = 1,\ldots,k$.

Given $\delta > 0$, let

$$\mathcal{S}_\delta = \left\{\boldsymbol{\alpha} \in \mathcal{A}\ :\ \forall i \neq j,\ \left|\alpha_i^{(l)} - \alpha_j^{(l)}\right| > \delta\ \ \forall l = 1,\ldots,k\right\}.$$

Then

$$\begin{aligned}
P_{\text{out}}(R) &\dot{\geq} \int_{\mathcal{A}_0 \cap S_\delta} p(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \\
&\doteq \int_{\mathcal{A}_0 \cap S_\delta} \rho^{-\sum_{l=1}^{k}\sum_{i=1}^{L} \alpha_i^{(l)} \frac{\Delta+1}{2}} e^{-\sum_{l=1}^{k}\sum_{i=1}^{L} \rho^{-\alpha_i^{(l)}}} \\
&\cdot \prod_{l=1}^{k} \prod_{1 \leq i < j \leq L} \left| \rho^{-\alpha_i^{(l)}} - \rho^{-\alpha_j^{(l)}} \right| d\boldsymbol{\alpha} \\
&\dot{\geq} \int_{\mathcal{A}_0 \cap S_\delta} \rho^{-\frac{1}{2}\sum_{l=1}^{k}\sum_{i=1}^{L} (\Delta+2L-2i+1)\alpha_i^{(l)}} d\boldsymbol{\alpha}.
\end{aligned}$$

To find the DMT upper bound, we need an extension of Lemma 3 to the multi-block case:

Lemma 8: Let $F(\boldsymbol{\alpha}) = \sum_{l=1}^{k}\sum_{i=1}^{L}(q+L-2i+1)\alpha_i^{(l)}$. Then

$$\begin{aligned}
&\inf_{\boldsymbol{\alpha} \in \mathcal{A}_0} F(\boldsymbol{\alpha}) \\
&= k\left[(-q-L+2\lfloor s \rfloor + 1)s + qL - \lfloor s \rfloor (\lfloor s \rfloor + 1)\right] = k\bar{d}(s).
\end{aligned}$$

Proof of Lemma 8: If $\forall l = 1, \ldots, k$ we have

$$\begin{aligned}
\bar{\alpha}_1^{(l)} &= \cdots = \bar{\alpha}_{\lfloor s \rfloor}^{(l)} = 0, \\
\bar{\alpha}_{\lfloor s \rfloor + 1}^{(l)} &= 1 + \lfloor s \rfloor - s, \\
\bar{\alpha}_{\lfloor s \rfloor + 2}^{(l)} &= \cdots = \bar{\alpha}_L^{(l)} = 1
\end{aligned}$$

then $\bar{\boldsymbol{\alpha}} \in \mathcal{A}_0$ and

$$F(\bar{\boldsymbol{\alpha}}) = k\left[(-q-L+2\lfloor s \rfloor + 1)s + qL - \lfloor s \rfloor (\lfloor s \rfloor + 1)\right].$$

We want to show that this value is the minimum of the function F over $\mathcal{A}_0$. For $\boldsymbol{\alpha} \in \mathcal{A}_0$ we have the following global constraints: $\forall j \leq L$,

$$\sum_{l=1}^{k}\sum_{i=1}^{j} \alpha_i^{(l)} \geq k(j-s). \tag{29}$$

Recalling that $\sum_{i=1}^{L}\sum_{j=1}^{i} \alpha_j = \sum_{i=1}^{L}(L-i+1)\alpha_i$, we can write

$$\begin{aligned}
F(\boldsymbol{\alpha}) &= (q-L-1)\sum_{l=1}^{k}\sum_{i=1}^{L} \alpha_i^{(l)} + 2\sum_{l=1}^{k}\sum_{i=1}^{L}(L-i+1)\alpha_i^{(l)} \\
&= (q-L-1)\sum_{l=1}^{k}\sum_{i=1}^{L} \alpha_i^{(l)} + 2\sum_{l=1}^{k}\sum_{i=1}^{L}\sum_{j=1}^{i} \alpha_j^{(l)} \\
&\geq k(q-L-1)(L-s) + 2\sum_{i=1}^{L} k(i-s) = k\bar{d}(s),
\end{aligned}$$

where the final step in the proof is the same as in Lemma 3. □

Using Lemma 8 with $q = \Delta + L$, $s = 2r$, we find that the DMT upper bound $\inf_{\boldsymbol{\alpha} \in \mathcal{A}_0} \frac{F(\boldsymbol{\alpha})}{2} = kd_1(r)$. This concludes the proof of Theorem 7. □

2) Proof of Theorem 8: The proof for the lower bound is similar to the proof of Theorem 2 in [34], but we include it for completeness[6]. Letting $H = \text{diag}(H^{(1)}, \ldots, H^{(k)})$ and $W = [W^{(1)}, \ldots, W^{(k)}]$ the multi-block channel matrix and noise for the equivalent real channel, we have the sphere bound $P_e(H) \leq \mathbb{P}\{\|W\|^2 > d_H^2/4\}$, where

$$\begin{aligned}
d_H^2 &= \frac{\rho}{n} \min_{\substack{X, X' \in \mathcal{C}(\rho) \\ X \neq X'}} \sum_{l=1}^{k} \left\| H^{(l)}(X^{(l)} - X'^{(l)}) \right\|^2 \\
&\geq \frac{1}{n}\rho^{1-\frac{2r}{n}} \sum_{l=1}^{k}\sum_{i=1}^{L} \lambda_i^{(l)}\mu_i^{(l)},
\end{aligned}$$

where $0 \leq \mu_1^{(l)} \leq \cdots \leq \mu_n^{(l)}$ are the ordered eigenvalues of $\Delta X^{(l)}(\Delta X^{(l)})^T$ with $\Delta X = X - X'$.

For any $\mathbf{j} = (j_1, \ldots, j_k)$ with $J = \sum_{l=1}^{k} j_l \geq 1$, we have

$$\begin{aligned}
d_H^2 &\geq \frac{1}{n}\rho^{1-\frac{2r}{n}} \sum_{l=1}^{k}\sum_{i=1}^{j_l} \lambda_i^{(l)}\mu_i^{(l)} \\
&\geq \frac{1}{n}\rho^{1-\frac{2r}{n}} \frac{J}{n} \left(\prod_{l=1}^{k}\prod_{i=1}^{j_l} \lambda_i^{(l)}\mu_i^{(l)} \right)^{\frac{1}{J}}.
\end{aligned}$$

Note that $\forall i = 1, \ldots, L$, $\forall l = 1, \ldots, k$, $\mu_i^{(l)} \leq 4\rho^{\frac{2r}{n}}$, and

$$\prod_{l=1}^{k}\prod_{i=1}^{j_l} \mu_i^{(l)} = \frac{\det(\Delta X \Delta X^T)}{\prod_{l=1}^{k}\prod_{i=j_l+1}^{n} \mu_i^{(l)}} \geq \frac{1}{4^{kn-J}\rho^{(kn-J)\frac{2r}{n}}}.$$

Therefore $\forall \mathbf{j} \neq 0$, $d_H^2 \geq c_j \rho^{\delta_{\mathbf{j}}(\boldsymbol{\alpha}, 2r)}$, where

$$\delta_{\mathbf{j}}(\boldsymbol{\alpha}, s) = -\frac{1}{\sum_{l=1}^{k} j_l} \sum_{l=1}^{k} \left(\sum_{i=1}^{j_l} \alpha_i^{(l)} + s - j_l \right),$$

[6]Note that compared to [34], we deal separately with the eigenvalues in each block instead of re-ordering them. The two approaches are equivalent.

and c_j is a suitable constant. The proof proceeds similarly to Section IV-C. The distribution $p(\boldsymbol{\alpha})$ in (28) is upper bounded as

$$p(\boldsymbol{\alpha}) \dot{\leq} p'(\boldsymbol{\alpha}) = e^{-\sum_{l=1}^{k}\sum_{i=1}^{L}\rho^{-\alpha_i^{(l)}}} \rho^{-\sum_{l=1}^{k}\sum_{i=1}^{L}\alpha_i^{(l)}N_i}$$

where $N_i = \frac{1}{2}(\Delta + 2L - 2i + 1)$. Since $2\|W\|^2 \sim \chi^2(2mnk)$, we have $\mathbb{P}\left\{\|W\|^2 > \frac{d_H^2}{4}\right\} = \Phi_{2mnk}\left(\frac{d_H^2}{2}\right)$, where Φ_t is defined in (17). So $\forall \mathbf{j} \neq \mathbf{0}$,

$$\begin{aligned} P_e &\leq \int \mathbb{P}\left\{\|W\|^2 > \frac{d_H^2}{4}\right\} p(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \\ &\leq \int_{\mathcal{A}} p'(\boldsymbol{\alpha}) \Phi_{2mnk}\left(\frac{d_H^2}{2}\right) d\boldsymbol{\alpha}. \end{aligned}$$

To conclude the proof, we need an extension of Lemma 4 to the multi-block case. As before, for a vector $\mathbf{j} = (j_1, \ldots, j_k)$, we use the notation $\mathbf{j} \leq L$ to mean that $j_l \leq L$ for all $l = 1, \ldots, k$.

Lemma 9: Assuming that $d \geq c_j \rho^{\delta_{\mathbf{j}}(\boldsymbol{\alpha}, s)}\ \forall \mathbf{j} \neq \mathbf{0}$, then $\forall t \in \mathbb{N}^+$,

$$-\lim_{\rho\to\infty} \frac{1}{\log \rho} \log \int_{\mathcal{A}} p'(\boldsymbol{\alpha}) \Phi\left(d\right) d\boldsymbol{\alpha} \geq \inf_{\boldsymbol{\alpha}\in\mathcal{A}_0} \sum_{l=1}^{k}\sum_{i=1}^{L} N_i \alpha_i^{(l)},$$

where $\mathcal{A}_0 = \left\{\boldsymbol{\alpha} \in \mathcal{A} \,:\, \forall \mathbf{j} \leq L,\ \sum_{l=1}^{k}\sum_{i=1}^{j_l}(1 - \alpha_i^{(l)}) \leq sk\right\}$.

Proof of Lemma 9: The proof is very similar to the proof of Lemma 4. We include a sketch for convenience. Note that $\Phi_t\left(\frac{d_H^2}{4}\right) \leq 1$ since it is a probability. If we define

$$\bar{\mathcal{A}} = \left\{\boldsymbol{\alpha} \in \mathcal{A} \,:\, \alpha_i^{(l)} \geq -\epsilon\ \forall i = 1, \ldots, L,\ \forall k = 1, \ldots, l\right\},$$
$$\mathcal{A}_i^{(l)} = \left\{\boldsymbol{\alpha} \in \mathcal{A} \,:\, \alpha_i^{(l)} < -\epsilon\right\},$$

then we have the bound

$$P_e \leq \int_{\bar{\mathcal{A}}} p'(\boldsymbol{\alpha}) \Phi_t\left(d\right) d\boldsymbol{\alpha} + \sum_{l=1}^{k}\sum_{i=1}^{L} \int_{\mathcal{A}_i^{(l)}} p'(\boldsymbol{\alpha}) \Phi_t\left(d\right) d\boldsymbol{\alpha} \tag{30}$$

With the change of variables $\lambda_i^{(l)} = \rho^{-\alpha_i^{(l)}} \quad \forall l = 1, \ldots, k,\ \forall i = 1, \ldots, L$, we have

$$\begin{aligned} &\int_{\mathcal{A}_i^{(l)}} p'(\boldsymbol{\alpha}) \Phi_t\left(d\right) d\boldsymbol{\alpha} \leq \int_{\mathcal{A}_i^{(l)}} p'(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \\ &\dot{\leq} \int_{-\infty}^{-\epsilon} e^{-\rho^{-\alpha_i^{(l)}}} \rho^{-\alpha_i^{(l)} N_i} d\alpha_i^{(l)} \prod_{(\bar{i},\bar{l})\neq(i,l)} \int_{-\infty}^{\infty} e^{-\rho^{-\alpha_{\bar{i}}^{(\bar{l})}}} \rho^{-\alpha_{\bar{i}}^{(\bar{l})} N_{\bar{i}}} d\alpha_{\bar{i}}^{(\bar{l})} \\ &= \int_{\rho^{\epsilon}}^{\infty} \frac{e^{-\lambda_i^{(l)}} (\lambda_i^{(l)})^{N_i - 1}}{\log \rho} d\lambda_i^{(l)} \prod_{(\bar{i},\bar{l})\neq(i,l)} \int_{0}^{\infty} \frac{e^{-\lambda_{\bar{i}}^{(\bar{l})}} (\lambda_{\bar{i}}^{(\bar{l})})^{N_{\bar{i}} - 1}}{\log \rho} d\lambda_{\bar{i}}^{(\bar{l})} \\ &\doteq \int_{\rho^{\epsilon}}^{\infty} \frac{e^{-\lambda_i^{(l)}} (\lambda_i^{(l)})^{N_i - 1}}{\log \rho} d\lambda_i^{(l)} \end{aligned}$$

which vanishes exponentially as a function of ρ. The first term in (30) is bounded by

$$\begin{aligned} &\int_{\bar{\mathcal{A}}} p'(\boldsymbol{\alpha}) \Phi_t\left(d\right) d\boldsymbol{\alpha} \\ &\leq \int_{\substack{\boldsymbol{\alpha}>-\epsilon, \\ \delta_{\mathbf{j}'}(\boldsymbol{\alpha},s)<\epsilon\ \forall \mathbf{j}'}} p'(\boldsymbol{\alpha}) \Phi_t\left(d\right) d\boldsymbol{\alpha} + \int_{\substack{\boldsymbol{\alpha}>-\epsilon, \\ \delta_{\mathbf{j}'}(\boldsymbol{\alpha},s)\geq\epsilon\ \forall \mathbf{j}'}} p'(\boldsymbol{\alpha}) \Phi_t\left(d\right) d\boldsymbol{\alpha}. \end{aligned} \tag{31}$$

Since Φ_t is decreasing, and using the assumption that $d \geq c_j \rho^{\delta_{\mathbf{j}}(\boldsymbol{\alpha}, s)}\ \forall \mathbf{j} \neq \mathbf{0}$, we have

$$\begin{aligned} &\int_{\substack{\boldsymbol{\alpha}>-\epsilon, \\ \delta_{\mathbf{j}'}(\boldsymbol{\alpha},s)\geq\epsilon\ \forall \mathbf{j}'}} p'(\boldsymbol{\alpha}) \Phi_t\left(d\right) d\boldsymbol{\alpha} \\ &\leq \int_{\substack{\boldsymbol{\alpha}>-\epsilon, \\ \delta_{\mathbf{j}'}(\boldsymbol{\alpha},s)\geq\epsilon\ \forall \mathbf{j}'}} p'(\boldsymbol{\alpha}) \Phi_t\left(c_j \rho^{\delta_{\mathbf{j}}(\boldsymbol{\alpha},s)}\right) d\boldsymbol{\alpha} \\ &\dot{\leq} \int_{\substack{\boldsymbol{\alpha}>-\epsilon, \\ \delta_{\mathbf{j}'}(\boldsymbol{\alpha},s)\geq\epsilon\ \forall \mathbf{j}'}} \Phi_t\left(c_j \rho^{\delta_{\mathbf{j}}(\boldsymbol{\alpha},s)}\right) \prod_{l=1}^{k}\prod_{i=1}^{L} \rho^{-\alpha_i^{(l)} N_i} d\boldsymbol{\alpha} \\ &\dot{\leq} \left(\prod_{l=1}^{k}\prod_{i>j_l} \int_{\alpha_i^{(l)}>-\epsilon} \rho^{-\alpha_i^{(l)} N_i} d\alpha_i^{(l)}\right) \\ &\cdot \int_{\substack{\alpha_i^{(l)}>-\epsilon\ \forall i<j_l \\ \delta_{\mathbf{j}'}(\boldsymbol{\alpha},s)\geq\epsilon}} \Phi_t\left(c_j \rho^{\delta_{\mathbf{j}}(\boldsymbol{\alpha},s)}\right) \rho^{-\sum_{l=1}^{k}\sum_{i=1}^{j_l} N_i} \prod_{l=1}^{k}\prod_{i=1}^{j_l} d\alpha_i^{(l)} \end{aligned}$$

since $\delta_{\mathbf{j}'}(\boldsymbol{\alpha}, s)$ is independent of $\alpha_i^{(l)}\ \forall i > j_l'$. The first integral has a finite SNR exponent, while the second is over a bounded region, and so it tends to 0 exponentially as a function of ρ. Thus, the product also tends to zero

exponentially.

To conclude, observe that the first term in (31) is upper bounded by

$$\int_{\substack{\boldsymbol{\alpha}>-\epsilon,\\ \delta_{\mathbf{j}'}(\boldsymbol{\alpha},s)<\epsilon\ \forall \mathbf{j}'}} p'(\boldsymbol{\alpha})d\boldsymbol{\alpha} \dot{\leq} \int_{\substack{\boldsymbol{\alpha}>-\epsilon,\\ \delta_{\mathbf{j}'}(\boldsymbol{\alpha},s)<\epsilon\ \forall \mathbf{j}'}} \rho^{-\sum_{l=1}^{k}\sum_{i=1}^{L}\alpha_i^{(l)}N_i} d\boldsymbol{\alpha}.$$

The statement follows by using the Laplace principle and taking $\epsilon \to 0$. □

To conclude the proof of Theorem 8, we use Lemma 8 with $q = \Delta + L$, $s = 2r$. □

D. Proof of Theorems 9 and 10 (DMT of quaternion multi-block codes)

Suppose $n = 2p$ is even. Consider a multi-block lattice $\mathcal{L} \subset M_{n/2}(\mathbb{H})^k$ of dimension $d = n^2k$, and a multi-block code $\mathcal{C}(\rho) = \rho^{-\frac{r}{n}}\mathcal{L}(\rho^{\frac{r}{n}})$. Every codeword is of the form $X = [X^{(1)}, \ldots, X^{(k)}] \in \mathcal{C}(\rho)$.

Referring back to the channel model (23), for all $l = 1, \ldots, k$ we can write

$$\begin{aligned} Y_c^{(l)} &= \begin{pmatrix} Y_1^{(l)} & Y_2^{(l)} \end{pmatrix}, \\ H_c^{(l)} &= \begin{pmatrix} H_1^{(l)} & H_2^{(l)} \end{pmatrix}, \\ W_c^{(l)} &= \begin{pmatrix} W_1^{(l)} & W_2^{(l)} \end{pmatrix}, \end{aligned}$$

where $Y_1^{(l)}, Y_2^{(l)}, H_1^{(l)}, H_2^{(l)}, W_1^{(l)}, W_2^{(l)} \in M_{m\times p}(\mathbb{C})$, and we have the equivalent quaternionic channel

$$Y^{(l)} = \sqrt{\frac{\rho}{n}} H^{(l)} X^{(l)} + W^{(l)},$$

where

$$\begin{aligned} Y^{(l)} &= \begin{pmatrix} Y_1^{(l)} & Y_2^{(l)} \\ -(Y_2^{(l)})^* & (Y_1^{(l)})^* \end{pmatrix}, \\ H^{(l)} &= \begin{pmatrix} H_1^{(l)} & H_2^{(l)} \\ -(H_2^{(l)})^* & (H_1^{(l)})^* \end{pmatrix}, \\ X^{(l)} &= \begin{pmatrix} A^{(l)} & -(B^{(l)})^* \\ B^{(l)} & (A^{(l)})^* \end{pmatrix}, \\ W^{(l)} &= \begin{pmatrix} W_1^{(l)} & W_2^{(l)} \\ -(W_2^{(l)})^* & (W_1^{(l)})^* \end{pmatrix}. \end{aligned}$$

1) Proof of Theorem 9: We can write the outage probability as

$$P_{\text{out}}(R) = \mathbb{P}\left\{ \frac{1}{k}\left(\sum_{l=1}^{k} \log\det(I + \rho(H^{(l)})^\dagger H^{(l)}) \right) \leq 2R \right\}.$$

Define $L = \min(m,p)$, $\Delta = |p-m|$, and let $\lambda_1^{(l)} \geq \cdots \geq \lambda_L^{(l)}$, $\quad l = 1, \ldots, k$ the ordered nonzero eigenvalues of $(H^{(l)})^\dagger H^{(l)}$ with distribution

$$\begin{aligned} &p(\lambda_1^{(l)}, \ldots, \lambda_L^{(l)}) \\ &= K \prod_{i=1}^{L} (\lambda_i^{(l)})^{2\Delta+1} e^{-\sum_{i=1}^{L}\lambda_i^{(l)}} \prod_{i<j}\left(\lambda_i^{(l)} - \lambda_j^{(l)}\right)^4. \end{aligned}$$

Let $\lambda_i^{(l)} = \rho^{-\alpha_i^{(l)}}$ $\forall l = 1, \ldots, k$, and

$$\mathcal{A} = \left\{ \boldsymbol{\alpha} \in \mathbb{R}^k \ : \ 0 \leq \alpha_1^{(l)} \leq \cdots \leq \alpha_L^{(l)} \ \ \forall l = 1, \ldots, k \right\}.$$

Then $p(\boldsymbol{\alpha})$ can be written as

$$\rho^{-2\sum_{l=1}^{k}\sum_{i=1}^{L}(\Delta+1)\alpha_i^{(l)}} e^{-\sum_{l=1}^{k}\sum_{i=1}^{L}\rho^{-\alpha_i^{(l)}}} \prod_{l=1}^{k}\prod_{i<j}\left(\rho^{-\alpha_i^{(l)}} - \rho^{-\alpha_j^{(l)}}\right)^4.$$

We have

$$P_{\text{out}}(R) = \mathbb{P}\left\{ \prod_{l=1}^{k}\prod_{i=1}^{L}(1+\rho^{1-\alpha_i^{(l)}}) \leq \rho^{rk} \right\} \geq \mathbb{P}(\mathcal{A}_0),$$

where

$$\begin{aligned} \mathcal{A}_0 &= \left\{ \boldsymbol{\alpha} \in \mathcal{A} \ : \ \sum_{l=1}^{k}\sum_{i=1}^{L}(1-\alpha_i^{(l)})^+ \leq rk \right\} \\ &= \left\{ \boldsymbol{\alpha} \in \mathcal{A} \ : \ \forall \mathbf{j} \leq L, \ \sum_{l=1}^{k}\sum_{i=1}^{j_l}(1-\alpha_i^{(l)}) \leq rk \right\}. \end{aligned}$$

Given $\delta > 0$, and letting

$$\mathcal{S}_\delta = \left\{ \boldsymbol{\alpha} \in \mathcal{A} \ : \ \forall i \neq j, \ \left|\alpha_i^{(l)} - \alpha_j^{(l)}\right| > \delta \ \ \forall l = 1, \ldots, k \right\},$$

we find that $P_{\text{out}}(R)$ is lower bounded by

$$\begin{aligned} &\int_{\mathcal{A}_0 \cap S_\delta} \rho^{-2\sum_{l=1}^{k}\sum_{i=1}^{L}\alpha_i^{(l)}(\Delta+1)} e^{-\sum_{l=1}^{k}\sum_{i=1}^{L}\rho^{-\alpha_i^{(l)}}} \prod_{l=1}^{k}\prod_{i<j}\left(\rho^{-\alpha_i^{(l)}} - \rho^{-\alpha_j^{(l)}}\right)^4 d\boldsymbol{\alpha} \\ &\dot{\geq} \int_{\mathcal{A}_0 \cap S_\delta} \rho^{-2\sum_{l=1}^{k}\sum_{i=1}^{L}(\Delta+2L-2i+1)\alpha_i^{(l)}} d\boldsymbol{\alpha}. \end{aligned}$$

Using Lemma 8 with $q = \Delta + L$, $s = r$, we find that the DMT upper bound is $2\inf_{\boldsymbol{\alpha}\in\mathcal{A}_0} F(\boldsymbol{\alpha}) = kd_2(r)$. □

2) Proof of Theorem 10: We only highlight the main steps of the proof. Let $H = \mathrm{diag}(H^{(1)}, \ldots, H^{(k)})$ and $W = [W^{(1)}, \ldots, W^{(k)}]$ the multi-block quaternion channel matrix and noise. We have

$$d_H^2 = \frac{\rho}{n} \min_{\substack{X, X' \in \mathcal{C}(\rho) \\ X \neq X'}} \sum_{l=1}^{k} \left\| H^{(l)} (X^{(l)} - X'^{(l)}) \right\|^2$$
$$\geq \frac{1}{p} \rho^{1-\frac{2r}{n}} \sum_{l=1}^{k} \sum_{i=1}^{L} \lambda_i^{(l)} \mu_i^{(l)},$$

where $0 \leq \mu_1^{(l)} = \mu_1^{(l)'} \leq \cdots \leq \mu_p^{(l)} = \mu_p^{(l)'}$ are the ordered eigenvalues of $\Delta X^{(l)} (\Delta X^{(l)})^\dagger$ with $\Delta X = X - X'$.

For any $\mathbf{j} = (j_1, \ldots, j_k)$ with $J = \sum_{l=1}^{k} j_l \geq 1$,

$$d_H^2 \geq \frac{J}{p} \rho^{1-\frac{2r}{n}} \left(\prod_{l=1}^{k} \prod_{i=1}^{j_l} \lambda_i^{(l)} \mu_i^{(l)} \right)^{\frac{1}{J}}.$$

Note that $\forall i = 1, \ldots, p$, $\forall l = 1, \ldots, k$, $\mu_i^{(l)} \dot{\leq} \rho^{\frac{2r}{n}}$, and

$$\prod_{l=1}^{k} \prod_{i=1}^{j_l} \mu_i^{(l)} = \frac{\det(\Delta X \Delta X^\dagger)^{\frac{1}{2}}}{\prod_{l=1}^{k} \prod_{i=j_l+1}^{p} \mu_i^{(l)}} \geq \frac{1}{4^{kp-J} \rho^{(kp-J)\frac{r}{p}}}.$$

Therefore $\forall \mathbf{j} \neq 0$, $d_H^2 \geq c_j \rho^{\delta_{\mathbf{j}}(\boldsymbol{\alpha}, r)}$, where

$$\delta_{\mathbf{j}}(\boldsymbol{\alpha}, r) = -\frac{1}{\sum_{l=1}^{k} j_l} \sum_{l=1}^{k} \left(\sum_{i=1}^{j_l} \alpha_i^{(l)} + r - j_l \right),$$

and c_j is a suitable constant. The distribution $p(\boldsymbol{\alpha})$ in (28) is upper bounded by

$$p(\boldsymbol{\alpha}) \dot{\leq} p'(\boldsymbol{\alpha}) = e^{-\sum_{l=1}^{k} \sum_{i=1}^{L} \rho^{-\alpha_i^{(l)}}} \rho^{-\sum_{l=1}^{k} \sum_{i=1}^{L} \alpha_i^{(l)} N_i}$$

where $N_i = 2(\Delta + 2L - 2i + 1)$. Since $\|W\|^2 \sim \chi^2(4mpk)$, we have

$$P_e \leq \int \mathbb{P} \left\{ \|W\|^2 > \frac{d_H^2}{4} \right\} p(\boldsymbol{\alpha}) d\boldsymbol{\alpha}$$
$$\leq \int_{\mathcal{A}} p'(\boldsymbol{\alpha}) \Phi_{4mpk} \left(\frac{d_H^2}{4} \right) d\boldsymbol{\alpha}.$$

To conclude the proof, we use Lemma 9 and Lemma 8 with $q = \Delta + L$, $s = r$. □

REFERENCES

[1] L. Luzzi and R. Vehkalahti, "The DMT classification of real and quaternionic lattice codes," in *Proc. IEEE Int. Symp. Inf. Theory*, June 2018, pp. 1026–1030.

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

[3] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1451–1458, Oct. 1998.

[4] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H.-F. Lu, "Explicit space-time codes achieving the diversity-multiplexing gain tradeoff," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3869–3884, Sept. 2006.

[5] F. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect space–time block codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3885–3902, Sept. 2006.

[6] S. Tavildar and P. Viswanath, "Approximately universal codes over slow-fading channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3233–3258, July 2006.

[7] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1639–1642, 1999.

[8] J. Jaldén and B. Ottersten, "On the complexity of sphere decoding in digital communications," *IEEE Transactions on Signal Processing*, vol. 53, no. 4, pp. 1474–1484, 2005.

[9] J. Jaldén and P. Elia, "Sphere decoding complexity exponent for decoding full-rate codes over the quasi-static MIMO channel," *IEEE Transactions on Information Theory*, vol. 58, no. 9, pp. 5785–5803, 2012.

[10] J. Jaldén and P. Elia, "DMT optimality of LR-aided linear decoders for a general class of channels, lattice designs, and system models," *IEEE Transactions on Information Theory*, vol. 56, no. 10, pp. 4765–4780, 2010.

[11] A. K. Singh, P. Elia, and J. Jaldén, "Achieving a vanishing SNR gap to exact lattice decoding at a subexponential complexity," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 3692–3707, 2012.

[12] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Generalised sphere decoder for asymmetrical space-time communication architecture," *Electronics Letters*, vol. 36, no. 2, pp. 166–167, 2000.

[13] P. Wang and T. Le-Ngoc, "A low-complexity generalized sphere decoding approach for underdetermined linear communication systems: performance and complexity evaluation," *IEEE Transactions on Communications*, vol. 57, no. 11, pp. 3376–3388, 2009.

[14] R. Vehkalahti, C. Hollanti, H.-F. Lu, and J. Lahtonen, "Some simple observations on MISO codes," in *Proc. 2010 IEEE Int. Symp. Inf. Theory and its Appl.*, Oct. 2010, pp. 537–541.

[15] K. P. Srinath and B. S. Rajan, "An enhanced DMT-optimality criterion for STBC schemes for asymmetric MIMO systems," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5944–5958, Sept. 2013.

[16] R. Vehkalahti, C. Hollanti, and F. Oggier, "Fast-decodable asym-

metric space-time codes from division algebras," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2362–2384, Apr. 2012.

[17] C. Abou-Rjeily, N. Daniele, and B. Belfiore, "Space-time coding for multiuser ultra-wideband communications," *IEEE Trans. Commun.*, vol. 54, no. 8, pp. 1514–1514, Aug. 2006.

[18] L. Luzzi and F. Oggier, "A family of fast-decodable MIDO codes from crossed-product algebras over $\mathbb{Q}$," in *Proc. IEEE Int. Symp. Inf. Theory*, July 2011, pp. 2030–2034.

[19] C. Hollanti, J. Lahtonen, and H.-F. Lu, "Maximal orders in the design of dense space-time lattice codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4493–4510, Aug. 2008.

[20] R. Vehkalahti, H.-F. Lu, and L. Luzzi, "Inverse determinant sums and connections between fading channel information theory and algebra," *IEEE Trans. Inf. Theory*, vol. 59, pp. 6060–6082, Sept. 2013.

[21] L. Luzzi, R. Vehkalahti, and A. Gorodnik, "Towards a complete DMT classification of division algebra codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, July 2016, pp. 2993–2997.

[22] E. Krätzel, *Lattice points*. Kluwer Academic Publishers, Berlin, 1988.

[23] G. J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs Tech. J.*, vol. 1, no. 2, pp. 41–59, 1996.

[24] H. Yao and G. Wornell, "Achieving the full MIMO diversity-multiplexing frontier with rotation based space-time codes," in *Proc. Allerton Conf. Comm., Control and Computing*, Oct 2003.

[25] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 628–636, Mar. 2002.

[26] W. Su and X.-G. Xia, "Signal constellations for quasi-orthogonal space-time block codes with full diversity," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2331–2347, Oct. 2004.

[27] P. Elia and J. Jaldén, "Construction criteria and existence results for approximately universal linear space-time codes with reduced decoding complexity," in *Allerton Conference on Communication, Control, and Computing*, September 2008.

[28] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "The Golden Code: a 2×2 full-rate space-time code with nonvanishing determinants," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1432–1436, April 2005.

[29] A. Edelman, "Eigenvalues and condition numbers of random matrices," Ph.D. dissertation, MIT, Cambridge, MA, USA, 1989.

[30] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H.-F. Lu, *Explicit, Minimum Delay Space-Time Codes Achieving the Diversity-Multiplexing Gain Tradeoff*. Technical report, Indian Institute of Science, Bangalore, 2005.

[31] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Europ. Trans. Telecomm.*, vol. 10, no. 6, pp. 585–595, Nov.-Dec. 1999.

[32] A. Edelman and N. R. Rao, "Random matrix theory," *Acta Numerica*, vol. 14, pp. 233–297, 2005.

[33] I. Reiner, *Maximal Orders*. Academic Press, New York, 1975.

[34] H.-F. Lu, "Constructions of multiblock space-time coding schemes that achieve the diversity-multiplexing tradeoff," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3790–3796, Aug. 2008.

Roope Vehkalahti received the M.Sc. and Ph.D. degrees from the University of Turku, Finland, in 2003 and 2008, respectively, both in pure mathematics. He was with the Department of Mathematics, University of Turku, Finland 2003-2016 and with Aalto University, Finland 2016-2021. In 2011-2012 he was visiting Swiss Federal Institute of Technology, Lausanne (EPFL). He is currently with the Department of Mathematics and Statistics, University of Jyväskylä, Jyväskylä, Finland. His research interests include applications of algebra and number theory to information theory.

Laura Luzzi received the degree in Mathematics from the University of Pisa, Italy, in 2003 and the Ph.D. degree in Mathematics for Technology and Industrial Applications from Scuola Normale Superiore, Pisa, Italy, in 2007. From 2007 to 2012 she held postdoctoral positions in Télécom-ParisTech and Supélec, France, and a Marie Curie IEF Fellowship at Imperial College London, United Kingdom. Since 2012, she is an Assistant Professor at ENSEA, Cergy-Pontoise, France, and a researcher at ETIS (UMR 8051, CY Cergy Paris Université, ENSEA, CNRS).

Her research interests include coding for wireless communications, physical layer security and lattice-based cryptography.