



The DMT classification of real and quaternionic lattice codes

Laura Luzzi, Roope Vehkalahti

► To cite this version:

Laura Luzzi, Roope Vehkalahti. The DMT classification of real and quaternionic lattice codes. IEEE International Symposium on Information Theory (ISIT), IEEE Information Theory Society, Jun 2018, Vail, Colorado, United States. hal-01740506

HAL Id: hal-01740506

<https://hal.science/hal-01740506>

Submitted on 31 Mar 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

The DMT classification of real and quaternionic lattice codes

Laura Luzzi

ETIS - Université Paris-Seine
(Université de Cergy-Pontoise, ENSEA, CNRS)
Cergy-Pontoise, France
laura.luzzi@ensea.fr

Roope Vehkalahti

Department of Communications and Networking
Aalto University
Helsinki, Finland
roope.vehkalahti@aalto.fi

Abstract—In this paper we consider space-time 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 point out 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.

I. INTRODUCTION

In [1] the authors proved that for every number of transmit antennas n there exist a DMT optimal code in the space $M_n(\mathbb{C})$. These codes are derived from division algebras where the center of the division algebra is a complex quadratic field. However, this result is actually more general, and their proof revealed that as long as a $2n^2$ -dimensional lattice code in $M_n(\mathbb{C})$ has the non-vanishing determinant property (NVD), it is DMT optimal. Yet, this result does not tell us anything about space-time lattice codes that are not full dimensional in $M_n(\mathbb{C})$. Such codes naturally appear in the scenario where we have less receive than transmit antennas and try to keep the decoding complexity limited.

One natural class of such space-time codes are the codes derived from \mathbb{Q} -central division algebras. In this paper we will measure their DMT. Unlike the case of complex quadratic center, \mathbb{Q} -central division algebras are divided into two categories with respect to their DMT performance. This division is based on the ramification of the infinite Hasse-invariant of the division algebra, which decides if the lattice code corresponding to the division algebra can be embedded into real or quaternionic space.

Our DMT classification holds for any multiplexing gain, extending previous partial results in [2, 3] 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 [1] we are not just considering division algebra codes, but all space-time codes where the code matrices are restricted to $M_n(\mathbb{R})$ (resp. $M_{n/2}(\mathbb{H})$), and provide two different upper bounds for the DMT of such codes. We then prove that if we have a degree n^2 -dimensional NVD lattice inside $M_n(\mathbb{R})$ (resp. $M_{n/2}(\mathbb{H})$) then this code achieves the respective upper

bound. As the \mathbb{Q} -central division algebra codes are of this type, we get their DMT as a corollary.

II. NOTATION AND PRELIMINARIES

Notation: Given a matrix X , we denote its complex conjugate by X^* , its transpose by X^T and its conjugate transpose by X^\dagger .

We use the dotted inequality $f(\rho) \dot{\leq} g(\rho)$ to mean $\lim_{\rho \rightarrow \infty} \frac{\log f(\rho)}{\log \rho} \leq \lim_{\rho \rightarrow \infty} \frac{\log g(\rho)}{\log \rho}$, and similarly for equality.

A. Subspaces and lattices

In this paper we will consider space-time codes that are subsets of certain 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 $M_{n/2}(\mathbb{C})$. Note that quaternionic matrices form a n^2 -dimensional subspace in $M_n(\mathbb{C})$.

The space-time codes we consider in this work are based on additive groups in $M_n(\mathbb{C})$.

Definition 1: A matrix lattice $L \subseteq M_n(\mathbb{C})$ has the form

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

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

We immediately see that if we have a lattice inside the space $M_n(\mathbb{R})$ or $M_{n/2}(\mathbb{H})$ the maximal dimension it can have is n^2 .

Definition 2: If the *minimum determinant* of the lattice $L \subseteq M_{n \times n}(\mathbb{C})$ is non-zero, i.e. satisfies

$$\det_{\min}(L) := \inf_{0 \neq X \in L} |\det(X)| > 0,$$

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

Building high dimensional NVD lattices is a highly non-trivial task. A natural source of such lattices are division

algebras. Let \mathcal{D} be a degree n \mathbb{Q} -central division algebra. We say that the algebra \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 \mathcal{D} .

Lemma 1: [2, Lemma 9.10] If the infinite prime is ramified in the algebra \mathcal{D} , then there exists an embedding

$$\psi : \mathcal{D} \rightarrow M_{n/2}(\mathbb{H})$$

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

$$\psi : \mathcal{D} \rightarrow M_n(\mathbb{R})$$

such that $\psi(\Lambda)$ is a n^2 dimensional NVD lattice.

B. Channel model

We consider a MIMO system with n transmit and m receive antennas, and minimal delay $T = n$. The received signal is

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

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). The set of transmitted codewords \mathcal{C} satisfies the average power constraint

$$\frac{1}{|\mathcal{C}|} \frac{1}{n^2} \sum_{X \in \mathcal{C}} \|X\|^2 \leq 1. \quad (2)$$

We suppose that perfect channel state information is available at the receiver but not at the transmitter, and that maximum likelihood decoding is performed.

In the DMT setting [4], we consider codes $\mathcal{C}(\rho)$ whose size grows with the SNR, and define the multiplexing gain as

$$r = \lim_{\rho \rightarrow \infty} \frac{1}{n} \frac{\log |\mathcal{C}|}{\log \rho},$$

and the diversity gain as

$$d(r) = - \lim_{\rho \rightarrow \infty} \frac{\log P_e}{\log \rho},$$

where P_e is the average error probability.

Spherically shaped lattice codes: Let now L be a lattice in $M_n(\mathbb{C})$. Given M , consider the subset of elements whose Frobenius norm is bounded by M :

$$L(M) = \{X \in L : \|X\| \leq M\}.$$

Let $k \leq 2n^2$ be the dimension of L as a \mathbb{Z} -module. As in [2], we choose $M = \rho^{\frac{rn}{k}}$ and consider codes of the form

$$\mathcal{C}(\rho) = M^{-1} L(M) = \rho^{-\frac{rn}{k}} L(\rho^{\frac{rn}{k}}),$$

which satisfy the power constraint (2). The multiplexing gain of this code is r .

III. 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.

A. Equivalent real channel

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:

$$Y = \begin{pmatrix} Y_r \\ Y_i \end{pmatrix} = \sqrt{\frac{\rho}{n}} \begin{pmatrix} H_r \\ H_i \end{pmatrix} \bar{X} + \begin{pmatrix} W_r \\ W_i \end{pmatrix} = \sqrt{\frac{\rho}{n}} H \bar{X} + W, \quad (3)$$

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 in the previous section, we can now establish a general upper bound for the DMT of real codes.

Theorem 1: 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: This part of the proof closely follows [4]. Given a rate $R = r \log \rho$, consider the outage probability [5]

$$P_{\text{out}}(R) = \inf_{Q \succ 0, \text{tr}(Q) \leq n} \mathbb{P}\{\Psi(Q, H) \leq R\}, \quad (4)$$

where $\Psi(Q, H)$ is the maximum mutual information per channel use of the real MIMO channel (3) with fixed H and real input with fixed covariance matrix Q .¹ Following a similar reasoning as in [5, Section 3.2], it is not hard to see that

$$\Psi(Q, H) = \frac{1}{2} \log \det(I + \frac{\rho}{n} H Q H^T).$$

As in [4, Section III.B], since $\log \det$ is increasing on the cone of positive definite symmetric matrices, for all Q such that $\text{tr}(Q) \leq n$ we have $\frac{Q}{n} \preceq I$ and

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

Note that $\det(I + \rho H H^T) = \det(I + \rho H^T H)$. Let $l = \min(2m, n)$, and $\Delta = |n - 2m|$. Let $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_l > 0$ be the nonzero eigenvalues of $H^T H$. The joint probability distribution of $\lambda = (\lambda_1, \dots, \lambda_l)$ is given by [6]²:

$$p(\lambda) = K e^{-\sum_{i=1}^l \lambda_i} \prod_{i=1}^l \lambda_i^{\frac{\Delta-1}{2}} \prod_{i < j} (\lambda_i - \lambda_j) \quad (5)$$

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

$$p(\alpha) = K (\log \rho)^l e^{-\sum_{i=1}^l \rho^{-\alpha_i}} \rho^{-\sum_{i=1}^l \alpha_i (\frac{\Delta+1}{2})} \prod_{i < j} (\rho^{-\alpha_i} - \rho^{-\alpha_j}) \quad (6)$$

¹Unlike [5] and [4], we don't use a strict inequality in the definition (4), but our definition is equivalent since the set of H such that $\Psi(Q, H) = R$ has measure zero.

²We have slightly modified the expression to be consistent with our notation. In [6], the author considers a matrix $A^T A$ where each element of A is $\mathcal{N}(0, 1)$.

Then we have

$$\begin{aligned} P_{\text{out}}(R) &\doteq \mathbb{P} \left\{ \prod_{i=1}^l (1 + \rho \lambda_i) \leq \rho^{2r} \right\} \\ &= \mathbb{P} \left\{ \prod_{i=1}^l (1 + \rho^{1-\alpha_i}) \leq \rho^{2r} \right\}. \end{aligned}$$

To simplify notation, we take $s = 2r$. Note that $1 + \rho^{1-\alpha_i} \leq 2\rho^{(1-\alpha_i)^+} \doteq \rho^{(1-\alpha_i)^+}$, therefore

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

where

$$\begin{aligned} \mathcal{A}_0 &= \left\{ \alpha \in \mathcal{A} : \alpha_i \geq 0 \ \forall i = 1, \dots, l, \sum_{i=1}^l (1 - \alpha_i)^+ \leq s \right\} \\ &= \left\{ \alpha \in \mathcal{A} : \alpha_j \geq 0, \sum_{i=1}^j (1 - \alpha_i) \leq s \ \forall j = 1, \dots, l \right\}. \quad (7) \end{aligned}$$

In fact, given $\alpha \in \mathcal{A}$, let $t = t(\alpha)$ be such that $\alpha_{t+1} \geq 1 \geq \alpha_t$. Then $\forall j = 1, \dots, l$, $\sum_{i=1}^j (1 - \alpha_i) \leq \sum_{i=1}^t (1 - \alpha_i) = \sum_{i=1}^l (1 - \alpha_i)^+$.

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

$$\begin{aligned} P_{\text{out}}(R) &\geq \int_{\mathcal{A}_0} e^{-\sum_{i=1}^l \rho^{-\alpha_i}} \rho^{-\sum_{i=1}^l \frac{(\Delta+1)\alpha_i}{2}} \prod_{i < j} (\rho^{-\alpha_i} - \rho^{-\alpha_j}) d\alpha \\ &\geq \int_{\mathcal{A}_0 \cap S_\delta} e^{-\sum_{i=1}^l \rho^{-\alpha_i}} \rho^{-\sum_{i=1}^l \frac{(\Delta+1)\alpha_i}{2}} \prod_{i < j} (\rho^{-\alpha_i} - \rho^{-\alpha_j}) d\alpha \\ &\geq \frac{(1 - \rho^{-\delta})^l}{e^l} \int_{\mathcal{A}_0 \cap S_\delta} \rho^{-\sum_{i=1}^l \alpha_i N_i} d\alpha \doteq \int_{\mathcal{A}_0 \cap S_\delta} \rho^{-\sum_{i=1}^l \alpha_i N_i} d\alpha, \end{aligned}$$

where $N_i = \frac{\Delta+2l-2i+1}{2}$. The previous inequality follows from the fact that $\rho^{-\alpha_i} - \rho^{-\alpha_j} > \rho^{-\alpha_i} (1 - \rho^{-\delta})$ for $\alpha \in S_\delta$, and $e^{-\sum_{i=1}^l \rho^{-\alpha_i}} \geq \frac{1}{e}$ if $\alpha_i \geq 0$. (Note that for a fixed i , there are $l-i$ possible values for j such that $i < j$.)

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

$\inf_{\alpha \in \mathcal{A}_0} f(\alpha) = (-q - l + 2 \lfloor s \rfloor + 1)s + ql - \lfloor s \rfloor (\lfloor s \rfloor + 1) = f(\alpha^*)$, where $\alpha_1^* = \dots = \alpha_{k-1}^* = 0$, $\alpha_k^* = k - s$, $\alpha_{k+1}^* = \dots = \alpha_l^* = 1$.

The proof of Lemma 2 can be found in Appendix A.

Using Lemma 2 with $q = \Delta + l$, $s = 2r$, we find that $\inf_{\alpha \in \mathcal{A}_0} \sum_{i=1}^l N_i \alpha_i = \inf_{\alpha \in \mathcal{A}_0} \frac{f(\alpha)}{2}$ is equal to

$$\begin{aligned} &\frac{1}{2} [(-\Delta - 2l + 2 \lfloor 2r \rfloor + 1)2r + (\Delta + l)l - \lfloor 2r \rfloor (\lfloor 2r \rfloor + 1)] \\ &= (-2m - n + 2 \lfloor 2r \rfloor + 1)r + mn - \frac{\lfloor 2r \rfloor (\lfloor 2r \rfloor + 1)}{2}. \end{aligned}$$

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

$$\lim_{\rho \rightarrow \infty} -\frac{\log P_{\text{out}}(R)}{\log \rho} \geq \inf_{\alpha \in S_\delta} \frac{f(\alpha)}{2}.$$

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

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

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 1. This result extends Proposition 4.2 in [3].

Theorem 2: Let L be an n^2 -dimensional lattice in $M_n(\mathbb{R})$, and consider the spherically shaped code $\mathcal{C}(\rho) = \rho^{-\frac{r}{n}} L(\rho^{\frac{r}{n}})$. If L has the NVD property, then the DMT of the code $\mathcal{C}(\rho)$ 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 1, we only need to prove that the DMT is lower bounded by $d_1(r)$. The following section follows very closely the proof in [1], and thus some details are omitted. To simplify notation, we assume that $\det_{\min}(L) = 1$.

We consider the sphere bound for the error probability for the equivalent real channel (3): 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:

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

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

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

For all $i = 1, \dots, n$, $\mu_i \leq \|\Delta X\|^2 \leq 4\rho^{\frac{2r}{n}}$, and

$$\prod_{i=1}^n \mu_i = \det(\Delta X \Delta X^T) \geq 1$$

due to the NVD property. Consequently, for all $k = 1, \dots, l$

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

With the change of variables $\lambda_i = \rho^{-\alpha_i} \ \forall i = 1, \dots, l$, we can write

$$d_H^2 \geq \rho^{1-\frac{2r}{n}} \rho^{-\frac{1}{k} \sum_{i=1}^k \alpha_i} \frac{1}{\rho^{\frac{2r(n-k)}{n}}} = \rho^{-\frac{1}{k} \left(\sum_{i=1}^k \alpha_i + 2r - k \right)}$$

$$= \rho^{\delta_k(\alpha, 2r)} \quad \forall k = 1, \dots, l,$$

where we have set $\alpha = (\alpha_1, \dots, \alpha_l)$ and

$$\delta_k(\alpha, s) = -\frac{1}{k} \left(\sum_{i=1}^k \alpha_i + s - k \right). \quad (8)$$

To simplify the notation, we will take $s = 2r$.

Since $2\|W\|^2$ is a $\chi^2(2mn)$ random variable, we have

$$\mathbb{P}\left\{\|W\|^2 > d\right\} = \sum_{j=0}^{mn-1} e^{-d} \frac{d^j}{j!}.$$

Let $p(\alpha)$ be the distribution of α in (6). Note that for $i < j$, $\rho^{-\alpha_i} \geq \rho^{-\alpha_j}$ and for a fixed i , there are $l-i$ possible values for j . Consequently

$$p(\alpha) \leq p'(\alpha) = K e^{-\sum_{i=1}^l \rho^{-\alpha_i} - \sum_{i=1}^l \alpha_i N_i} (\log \rho)^l \quad (9)$$

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

$$P_e = \int P_e(\alpha) p(\alpha) d\alpha \leq \int \mathbb{P}\left\{\|W\|^2 > \frac{\rho^{\delta_k(\alpha, s)}}{4}\right\} p(\alpha) d\alpha.$$

Finally, we get $\forall k = 1, \dots, l$,

$$P_e \leq \int_{\mathcal{A}} p'(\alpha) \Phi(d_H^2) d\alpha \leq \int_{\mathcal{A}} p'(\alpha) \Phi(\rho^{\delta_k(\alpha, s)}) d\alpha \quad (10)$$

where $\mathcal{A} = \{\alpha : \alpha_1 \leq \dots \leq \alpha_l\}$, and

$$\Phi(d) = \mathbb{P}\left\{\|W\|^2 > \frac{d}{4}\right\} = e^{-\frac{d}{4}} \sum_{j=0}^{2mn-1} \left(\frac{d}{4}\right)^j \frac{1}{j!}. \quad (11)$$

The following Lemma is proven in Appendix B:

Lemma 3:

$$\begin{aligned} & \min_{k=1, \dots, l} \left(-\lim_{\rho \rightarrow \infty} \frac{1}{\log \rho} \log \int_{\mathcal{A}} p'(\alpha) \Phi(\rho^{\delta_k(\alpha, s)}) d\alpha \right) \\ & \geq \inf_{\alpha \in \mathcal{A}_0} \sum_{i=1}^l N_i \alpha_i, \end{aligned}$$

where \mathcal{A}_0 is defined in (7).

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

IV. QUATERNION LATTICE CODES

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

$$Y_c = \sqrt{\frac{\rho}{n}} H_c \bar{X} + W_c, \quad (12)$$

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

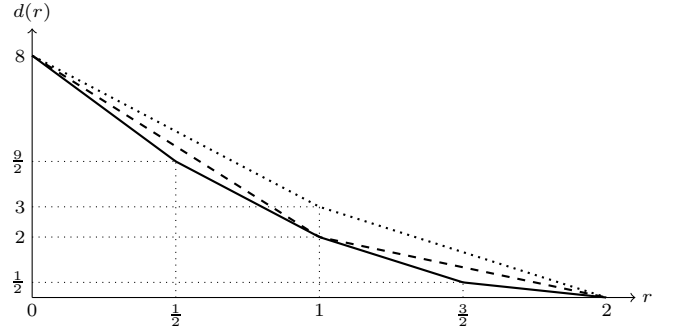


Fig. 1. DMT upper bounds for real (solid) and quaternion (dashed) codes for $n = 4$ and $m = 2$. The dotted lines correspond to the optimal DMT.

A. Equivalent quaternion channel

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

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

and we have the equivalent “quaternionic channel”:

$$\underbrace{\begin{pmatrix} Y_1 & Y_2 \\ -Y_2^* & Y_1^* \end{pmatrix}}_Y = \sqrt{\rho} \underbrace{\begin{pmatrix} H_1 & H_2 \\ -H_2^* & H_1^* \end{pmatrix}}_H \underbrace{\begin{pmatrix} A & -B^* \\ B & A^* \end{pmatrix}}_X + \underbrace{\begin{pmatrix} W_1 & W_2 \\ -W_2^* & W_1^* \end{pmatrix}}_W$$

B. General DMT upper bound for quaternion codes

Theorem 3: 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

$$\begin{pmatrix} Y_1 \\ -Y_2^* \end{pmatrix} = \sqrt{\frac{\rho}{n}} \begin{pmatrix} H_1 & H_2 \\ -H_2^* & H_1^* \end{pmatrix} \begin{pmatrix} A \\ B \end{pmatrix} + \begin{pmatrix} W_1 \\ -W_2^* \end{pmatrix} \quad (13)$$

If r is the multiplexing gain of the original system (12), then the multiplexing gain of this channel is $2r$, since the same number of symbols is transmitted using half the frame length. Consider the eigenvalues $\lambda_1 = \lambda'_1 \geq \lambda_2 = \lambda'_2 \geq \dots \geq \lambda_p = \lambda'_p \geq 0$ 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 [5]

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

The joint eigenvalue density $p(\lambda) = p(\lambda_1, \dots, \lambda_l)$ of a quaternion Wishart matrix is [7]³

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

³The quaternion case corresponds to taking $\beta = 4$ in [7, 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.

for some constant K . Considering the change of variables $\lambda_i = \rho^{-\alpha_i} \forall i = 1, \dots, l$, the distribution of $\alpha = (\alpha_1, \dots, \alpha_l)$ is

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

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

$$\begin{aligned} P_{\text{out}}(R) &\doteq \mathbb{P} \left\{ 2 \sum_{i=1}^l \log(1 + \rho \lambda_i) < 2r \log \rho \right\} \\ &= \mathbb{P} \left\{ \prod_{i=1}^l (1 + \rho^{1-\alpha_i}) < \rho^r \right\} \doteq \mathbb{P} \left\{ \prod_{i=1}^l \rho^{(1-\alpha_i)^+} < \rho^r \right\} \geq \mathbb{P}(\mathcal{A}_0) \end{aligned}$$

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

$$\begin{aligned} P_{\text{out}}(R) &\geq \int_{\mathcal{A}_0 \cap S_\delta} e^{-\sum_{i=1}^l \rho^{-\alpha_i}} \rho^{-2 \sum_{i=1}^l \alpha_i (\Delta+1)} \prod_{i < j} (\rho^{-\alpha_i} - \rho^{-\alpha_j})^4 d\alpha \\ &\geq \frac{(1 - \rho^{-\delta})^l}{e^l} \int_{\mathcal{A}_0 \cap S_\delta} \rho^{-2 \sum_{i=1}^l N_i \alpha_i} d\alpha \end{aligned}$$

where $N_i = 2(\Delta + 2l - 2i + 1)$. Let $f(\alpha) = \sum_{i=1}^l \alpha_i N_i$. Using the Laplace principle, $\lim_{\rho \rightarrow \infty} -\frac{\log P_{\text{out}}(R)}{\log \rho} \geq 2 \inf_{\mathcal{A}_0 \cap S_\delta} f(\alpha) \forall \delta > 0$. Using Lemma 2 with $s = r$, $q = \Delta + l$, we find that $2 \inf_{\alpha \in \mathcal{A}_0} f(\alpha) = 2f(\alpha^*)$ is the piecewise linear function $d_2(r)$ connecting the points $(r, [2(p-r)(m-r)]^+) = (r, [(n-2r)(m-r)]^+)$ for $r \in \mathbb{Z}$. Note that $\forall \delta$, the point α_δ such that $\alpha_{\delta,i} = \alpha_i^* + \frac{\delta_i}{l}$ is in $\mathcal{A}_0 \cap S_\delta$ and when $\delta \rightarrow 0$, $\alpha_\delta \rightarrow \alpha^*$. By continuity of f , $2 \lim_{\delta \rightarrow 0} \inf_{\mathcal{A}_0 \cap S_\delta} f(\alpha) = 2f(\alpha^*) = d_2(r)$. \square

C. DMT of quaternionic lattice codes with NVD

We now show that quaternionic lattice codes with NVD achieve the upper bound of Theorem 3. This result extends Proposition 4.3 in [3].

Theorem 4: Let L be an n^2 -dimensional lattice in $M_{n/2}(\mathbb{H})$, and consider the spherically shaped code $\mathcal{C}(\rho) = \rho^{-\frac{n}{2}} L(\rho^{\frac{n}{2}})$. If L has the NVD property, then the DMT of the code $\mathcal{C}(\rho)$ is the piecewise linear function $d_2(r)$ connecting the points $(r, [(m-r)(n-2r)]^+)$ for $r \in \mathbb{Z}$.

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

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

Let $\Delta X = X - X'$. We denote by $\lambda_1 = \lambda'_1 \geq \lambda_2 = \lambda'_2 \geq \dots \geq \lambda_p = \lambda'_p \geq 0$ the eigenvalues of $H^\dagger H$, and by $0 \leq \mu_1 = \mu'_1 \leq \dots \leq \mu_p = \mu'_p$ 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 inequality as in [1], we find that for all $k = 1, \dots, l$,

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

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

As before, for all $i = 1, \dots, n$, $\mu_i \leq \|\Delta X\|^2 \leq 4\rho^{\frac{2r}{n}}$, and $\prod_{i=1}^n \mu_i = \det(\Delta X \Delta X^\dagger)^{\frac{1}{2}} \geq 1$ using the NVD property of the code. Consequently, for all $k = 1, \dots, l$

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

With the change of variables $\lambda_i = \rho^{-\alpha_i} \forall i = 1, \dots, l$, we have $\forall k = 1, \dots, l$

$$d_H^2 \geq 2\rho^{1-\frac{r}{p}} \rho^{-\frac{1}{k} \sum_{i=1}^k \alpha_i} \rho^{-\frac{r(p-k)}{p}} = 2\rho^{-\frac{1}{k} \left(\sum_{i=1}^k \alpha_i + r - k \right)} = 2\rho^{\delta_k(\alpha)}$$

where $\alpha = (\alpha_1, \dots, \alpha_l)$ and $\delta_k(\alpha) = -\frac{1}{k} \left(\sum_{i=1}^k \alpha_i + r - k \right)$.

Since $2\|W\|^2 \sim 2\chi^2(2mp)$, we have

$$\begin{aligned} P_e(H) &\leq \mathbb{P} \left\{ \|W\|^2 > \frac{\rho^{\delta_k(\alpha)}}{2} \right\} \\ &= \sum_{j=0}^{mp-1} e^{-\frac{\rho^{\delta_k(\alpha)}}{4}} \left(\frac{\rho^{\delta_k(\alpha)}}{4} \right)^j \frac{1}{j!} = \Phi(\delta_k(\alpha, r)). \end{aligned}$$

By averaging with respect to the distribution $p(\alpha)$, we get

$$P_e \leq \int_{\mathcal{A}} p(\alpha) \Phi(\delta_k(\alpha, r)) d\alpha \leq \int_{\mathcal{A}} p'(\alpha) \Phi(\delta_k(\alpha, r)) d\alpha$$

where $\mathcal{A} = \{\alpha : \alpha_1 \leq \dots \leq \alpha_l\}$, and

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

where $N_i = 2(\Delta + 2l - 2i + 1)$. Note that $p'(\alpha)$ and $\Phi(\delta_k(\alpha, r))$ have the same form as in (9) and (11). From Lemma 3 we find $d(r) \geq \inf_{\alpha \in \mathcal{A}_0} 2 \sum_{i=1}^l \alpha_i (\Delta + 2l - 2i + 1)$, which by Lemma 2 is the piecewise linear function connecting the points $(r, [(n-2r)(m-r)]^+)$ for $r \in \mathbb{Z}$. \square

APPENDIX

A. Proof of Lemma 2

Let $\bar{d}(s) = (-q - l + 2[s] + 1)s + ql - [s]([s] + 1)$. Without loss of generality, we can suppose that $k-1 \leq s < k$ for some $k \in \mathbb{N}$, i.e. $k-1 = [s]$, $k = [s] + 1$.

First, we show that $\forall \alpha \in \mathcal{A}_0$, we have $f(\alpha) \geq \bar{d}(s)$. In fact

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

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

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

B. Proof of Lemma 3

The proof closely follows [8], which is a preliminary version of [1]. Note that $\Phi(\rho^{\delta_k(\alpha, s)}) \leq 1$ since it is a probability. Given $\varepsilon > 0$, we can bound the integral (10) as follows

$$P_e \leq \int_{\bar{\mathcal{A}}} p'(\alpha) \Phi(\rho^{\delta_k(\alpha, s)}) d\alpha + \sum_{j=1}^l \int_{\mathcal{A}_j} p'(\alpha) \Phi(\rho^{\delta_k(\alpha, s)}) d\alpha, \quad (14)$$

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

$$\begin{aligned} \int_{\mathcal{A}_j} p'(\alpha) \Phi(\rho^{\delta_k(\alpha, s)}) d\alpha &\leq \int_{\mathcal{A}_j} p'(\alpha) d\alpha \\ &\leq \left(\prod_{i \neq j} \int_{-\infty}^{\infty} e^{-\rho^{-\alpha_i}} \rho^{-\alpha_i N_i} d\alpha_i \right) \int_{-\infty}^{\varepsilon} e^{-\rho^{-\alpha_j}} \rho^{-\alpha_j N_j} d\alpha_j \\ &= \left(\prod_{i \neq j} \int_0^{\infty} \frac{e^{-\lambda_i} \lambda_i^{N_i-1}}{\log \rho} d\lambda_i \right) \int_{\rho^\varepsilon}^{\infty} \frac{\lambda_j e^{-\lambda_j}}{\log \rho} d\lambda_j \\ &\doteq \rho^0 \int_{\rho^\varepsilon}^{\infty} \frac{\lambda_j e^{-\lambda_j}}{\log \rho} d\lambda_j \end{aligned}$$

which vanishes exponentially fast as a function of ρ . For the first term in (14), we have

$$\begin{aligned} \int_{\bar{\mathcal{A}}} p'(\alpha) \Phi(\rho^{\delta_k(\alpha, s)}) d\alpha &\leq \int_{\substack{\alpha > -\varepsilon \\ \delta(\alpha, s) < \varepsilon}} p'(\alpha) \Phi(\rho^{\delta_k(\alpha, s)}) d\alpha \\ &\quad + \sum_{j=1}^n \int_{\substack{\alpha > -\varepsilon, \\ \delta_j(\alpha, s) \geq \varepsilon}} p'(\alpha) \Phi(\rho^{\delta_k(\alpha, s)}) d\alpha, \end{aligned}$$

where the notation $\alpha > -\varepsilon$ means $\alpha_i > -\varepsilon \ \forall i = 1, \dots, l$. We have

$$\begin{aligned} &\int_{\substack{\alpha > -\varepsilon, \\ \delta_j(\alpha, s) \geq \varepsilon}} p'(\alpha) \Phi(\rho^{\delta_k(\alpha, s)}) d\alpha \quad (15) \\ &\leq \int_{\substack{\alpha > -\varepsilon, \\ \delta_j(\alpha, s) \geq \varepsilon}} e^{-\frac{\rho^{\delta_j(\alpha, s)}}{4}} \sum_{t=0}^{2mn-1} \left(\frac{\rho^{\delta_j(\alpha, s)}}{4} \right)^t \frac{1}{t!} \prod_{i=1}^l \rho^{-\alpha_i N_i} d\alpha \\ &\leq \left(\prod_{i=j+1}^l \int_{\alpha_i > -\varepsilon} \rho^{-\alpha_i N_i} d\alpha_i \right) \end{aligned}$$

$$\cdot \int_{\substack{\alpha_1, \dots, \alpha_j > -\varepsilon \\ \delta_j(\alpha, s) \geq \varepsilon}} e^{-\frac{\rho^{\delta_j(\alpha, s)}}{4}} \sum_{t=0}^{2mn-1} \left(\frac{\rho^{\delta_j(\alpha, s)}}{4} \right)^t \frac{1}{t!} \rho^{-\sum_{i=1}^j N_i} d\alpha_1 \dots d\alpha_j$$

since $\delta_j(\alpha, s)$ is independent of α_i for $i > j$. As $\delta_j(\alpha, s) \geq \varepsilon$, $\alpha_i > -\varepsilon$ implies $\alpha_i \leq -j\varepsilon - s + j$, 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, (15) tends to zero exponentially fast.

Finally, the SNR exponent of (10) is determined by the behavior of

$$\begin{aligned} &\int_{\substack{\alpha > -\varepsilon \\ \delta(\alpha, s) < \varepsilon}} p'(\alpha) \Phi(\rho^{\delta_k(\alpha, s)}) d\alpha \leq \int_{\substack{\alpha > -\varepsilon \\ \delta(\alpha, s) < \varepsilon}} p'(\alpha) d\alpha \\ &\leq \int_{\substack{\alpha > -\varepsilon \\ \delta(\alpha, s) < \varepsilon}} \rho^{-\sum_{i=1}^n N_i \alpha_i} d\alpha \end{aligned}$$

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

$$\begin{aligned} \mathcal{A}_0 &= \left\{ \alpha \in \mathcal{A} : \alpha_j \geq 0, \sum_{i=1}^j (1 - \alpha_i) \leq s \ \forall j = 1, \dots, l \right\} \\ &= \{ \alpha : \alpha_j \geq 0, \delta_j(\alpha, s) \leq 0 \ \forall j = 1, \dots, l \}. \quad \square \end{aligned}$$

REFERENCES

- [1] 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, 2006.
- [2] R. Vehkalahti, H.-F. Lu, and L. Luzzi, "Inverse determinant sums and connections between fading channel information theory and algebra," *IEEE Trans. Inform. Theory*, vol. 59, pp. 6060–6082, Sept 2013.
- [3] L. Luzzi, R. Vehkalahti, and A. Gorodnik, "Towards a complete DMT classification of division algebra codes," in *IEEE International Symposium on Information Theory (ISIT)*, July 2016, pp. 2993–2997.
- [4] 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.
- [5] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Europ. Trans. Telecomm.*, vol. 10, no. 6, pp. 585–595, Nov.-Dec. 1999.
- [6] A. Edelman, "Eigenvalues and condition numbers of random matrices," Ph.D. dissertation, Dept. Math., Massachusetts Inst. Technol., Cambridge, MA, USA, 1989.
- [7] A. Edelman and N. R. Rao, "Random matrix theory," *Acta Numerica*, vol. 14, pp. 233–297, 2005.
- [8] 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.