MUTUALLY ORTHOGONAL MATRICES FROM DIVISION ALGEBRAS

B. A. SETHURAMAN

ABSTRACT. Matrices A and B in $M_n(\mathbb{C})$ are said to be mutually orthogonal if $AB^* + BA^* = 0$, where * denotes the conjugate transpose. We study cardinalities of certain $\mathbb{R}$-linearly independent families of matrices arising from matrix embeddings of a division algebra of index m with center a number field Z, satisfying the property that matrices from different families are mutually orthogonal. The question is of importance in the context of coding for certain wireless channels, where the cardinalities of such sets is connected to the maximum code rate consistent with low decoding complexity. It follows from our results that the maximum code rate for the codes we consider is severely limited.

1. INTRODUCTION

This paper deals with a question that arises from certain coding and decoding issues in wireless communication. Let D be a division algebra of index m, and center a number field Z. Suppose that we have an embedding $\phi : D \to M_n(\mathbb{C})$ for some n. Thus, ϕ is a (necessarily injective) ring homomorphism, which by definition takes 1_D to the identity matrix. We will work exclusively with the embedded forms $\phi(D)$ and $\phi(Z)$, and by abuse of notation, will continue to write D and Z respectively for $\phi(D)$ and $\phi(Z)$. We will call two matrices A and B in $M_n(\mathbb{C})$ *mutually orthogonal* if $AB^* + BA^* = 0$, where * denotes the conjugate transpose. Suppose Γ_1, Γ_2, Γ_3, and Γ_4 are four (nonempty) families of matrices in D such that any two matrices from distinct families are mutually orthogonal and such that the matrices in $\Gamma_1 \cup \Gamma_2 \cup \Gamma_3 \cup \Gamma_4$ are $\mathbb{R}$-linearly independent. Assume that $|\Gamma_1| = |\Gamma_2| = |\Gamma_3| = |\Gamma_4| = k$. The question we study is the following: What is the maximum value of k? Under the assumption that $Z = Z^*$, which arises quite naturally in the application to wireless communication,

1991 *Mathematics Subject Classification.* 11C20, 11R52, 17C60.

Key words and phrases. Mutually Orthogonal Matrices, Division Algebras. Space-Time Block Codes, Fast Decodability.

The author is grateful to the U.S. National Science Foundation grant CCF-1318260 for support during this research.

we show that this maximum is $md/2$, where d is the degree of the minimal polynomial of α as a matrix in $M_n(\mathbb{C})$, α a generator of Z over $\mathbb{Q}$. Here, m is necessarily even, and we identify $\mathbb{Q}$ with its image $\phi\colon q \mapsto \mathrm{diag}(q, \ldots, q)$ in $M_n(\mathbb{C})$. We give examples to show that this maximum is actually attained.

Our main theorem is the following:

Theorem 1. *With notation and assumptions as above:*

(1) *The index m of D is even.*
(2) *We have $k \leq \frac{mt}{2}$, where t is the maximum number of $\mathbb{R}$-linearly independent Hermitian matrices in Z. Further, $t \leq d$, where d is the degree of the minimal polynomial (as a matrix in $M_n(\mathbb{C})$) of any $\alpha \in Z$ such that $Z = \mathbb{Q}(\alpha)$. Thus, $k \leq \frac{md}{2}$.*
(3) *$md \leq n$, so $k \leq \frac{n}{2}$.*

We begin our considerations in the next section, but we first describe briefly how this question arises. In the field of multiple-antenna communication, division algebras embedded in $M_n(\mathbb{C})$ form natural candidates for constructing *space-time block codes,* which for our purpose are matrices $X(\underline{s})$ arising from the embedded division algebra, whose entries depend linearly on a $2l$-tuple $\underline{s} = (s_1, \ldots, s_l, s_1^*, \ldots, s_l^*)$, $l \leq n^2$. Here, the s_i take values in a finite subset $\mathcal{S}$ of the nonzero complex numbers. The l-tuple $(s_1, \ldots, s_l)$ carries the message to be transmitted, and the matrix size n signifies both the number of antennas used as also the number of uses of the transmission channel in one block of transmission. (See [8], [9] for instance. Note that these references mainly focus on the situation where $X(\underline{s})$ depends only on $s_1, \ldots, s_l,$, but we can just as easily allow the more general case where $X(\underline{s})$ also depends on the complex conjugates s_i^*.) Writing each s_i as $a_{2i-1} + \beta a_{2i}$, where a_{2i-1} and a_{2i} are real and β is non-real, the code matrices can be written in the form

$$X = X(a_1, \ldots, a_{2l}) = \sum_{i=1}^{2l} a_i A_i, \tag{1}$$

where the A_i are fixed $n \times n$ complex matrices. The message is now carried by the *real* $2l$-tuple $(a_1, a_2, \ldots)$, where the a_i come from the set $\mathcal{R}(\mathcal{S})$ defined as $\{x \in \mathbb{C} \mid x + \beta y \in \mathcal{S}, \text{for some } y \in \mathbb{C}\}$ unioned with $\{y \in \mathbb{C} \mid x + \beta y \in \mathcal{S}, \text{for some } x \in \mathbb{C}\}$. Note that the A_i must be $\mathbb{R}$-linearly independent, else, we could write some A_i as an $\mathbb{R}$-linear combination of the remaining A_j in the right side of Equation 1, and as a result, we would effectively be transmitting fewer than $2l$ real symbols and hence less information in each matrix X.

Typically, the division algebra D from which the matrices $X(\underline{s})$ arise is taken to be an Z-central division algebra, where Z is one of $\mathbb{Q}$, $\mathbb{Q}(\imath)$, or $\mathbb{Q}(\omega)$, where ω is a primitive 3rd root of unity, and S is taken to be a subset of the nonzero elements of Z. When $Z = \mathbb{Q}(\imath)$, β above is taken to be $\imath$, and when $Z = \mathbb{Q}(\omega)$, β above is taken to be ω. In such situations, and under the assumption that $X(\underline{s}) \in D$ for all $s \in Z$, as is the situation in practice, it is easy to see that the A_i themselves are also in D. (Of course, when $Z = \mathbb{Q}$, there are no imaginary parts to the s_i, instead, for uniformity of notation, we will tacitly assume that in this case, $\underline{s}$ is really a $2l$-tuple $(a_1, \ldots, a_{2l})$, with $2l \leq 2n^2$.)

When some standard lattice-based decoding procedures are employed, the decoding process has worst-case decoding complexity of the order $\mathcal{O}(|\mathcal{R}(\mathcal{S}|)^{2l})$, which, especially when the code is "full-rate" (i.e, $l = n^2$), is prohibitively high. It is of interest to reduce the exponent of $|\mathcal{R}(\mathcal{S})|$ in the complexity, by enabling the a_i to be decoded in *parallel* groups. If this can be accomplished, and if say k is the maximum size of the groups, then the decoding complexity drops to $|\mathcal{R}(\mathcal{S}|)^k$. Suppose that the symbols $a_1, \ldots, a_{2l}$ can be decoded in parallel in groups $\Gamma_1, \ldots, \Gamma_g$, with Γ_i (after reindexing $a_1, \ldots, a_{2l}$) containing the symbols $a_{i,1}$, $a_{i,2}, \ldots$. We may rewrite Equation 1 as

$$X = \sum_{i=1}^{g} \sum_{u} a_{i,u} A_{i,u} \tag{2}$$

where the A_i are correspondingly partitioned and reindexed. An analysis of the decoding process shows that decoding can occur in such parallel groups if and only if each of the corresponding matrices $A_{i,u}$, $u = 1, 2, \ldots$, attached to the symbols $a_{i,u}$ in Γ_i is mutually orthogonal to each of the matrices $A_{j,v}$, $v = 1, 2, \ldots$, attached to the symbols $a_{j,v}$ in Γ_j, for all $1 \leq i < j \leq g$ ([2], see also [1], [5], [6], [7], [10]). Further, as [2] shows, the maximum number of groups g possible is 4. Note that since the decoding complexity is determined by the size of the largest group Γ_i, we may assume that all groups have the same cardinality: this ensures that the decoding complexity is as low as possible for a given choice of $2l = \sum_i |\Gamma_i|$. (Hence, $2l = 4k$.) We are thus led to the central question of this paper: what is the maximum possible value of the cardinality of these sets $\Gamma_1, \ldots, \Gamma_4$?

A high value of $|\Gamma_i|$ is desirable, since the higher the value of $|\Gamma_i|$, the higher the amount of information sent by the code matrix $X(\underline{s})$. In this context, see also Remark 20 at the end of the paper.

2. Commuting spaces inside division algebras

Throughout the paper, if X and Y are two subsets of a ring, we will say X and Y *commute pairwise* if $xy = yx$ for all $x \in X$ and $y \in Y$. We will say X is *commutative* if the elements of X commute with one another.

We will start with a result that is purely about division algebras:

Proposition 2. *Let E be a division algebra with center F and index m. Let V and W be two distinct F-linear subspaces of E that commute pairwise. Then at most one of $\dim_F(V)$, $\dim_F(W)$ can be greater than m.*

Proof. The result is of course true if V and W are the same space, for then, the commutativity condition shows that F and V must generate a subfield of E, whose dimension over F is necessarily bounded by m. So assume that V and W are distinct as in the statement. Not that it is sufficient to prove the theorem for $F[V]$ and $F[W]$, the F-algebras generated by V and W respectively.

Let F_1 be the center of $F[V]$. If $F[V]$ is commutative, then $F[V] = F_1$ is a field extension of F, and is hence of dimension at most m, proving the theorem for this case. Thus, we may assume that $F[V]$ is noncommutative, with center F_1. If Δ is the centralizer in E of F_1, then $\Delta \cong F[V] \otimes_{F_1} B$, where B is F_1-central, and is the centralizer in Δ of $F[V]$, which is also the centralizer in E of $F[V]$. (This is standard, see [3, Theorem III.5.1, Chapter III], or [4, Theorem 4.7, Chapter 4] for instance.) Thus, $F[W]$ is contained in B. We may further expand $F[W]$ to B (since any element of $F[V]$ commutes with any element of B) and prove our theorem for $F[V]$ and B.

Once again, if B is commutative (i.e., the centralizer of $F[V]$ in E is F_1 itself: this follows from the Double Centralizer Theorem, [3, Theorem III.5.1, Chapter III]), then as in the beginning of the previous paragraph, the theorem is proved. So we assume that B is noncommutative. Now, if $F[V]$ as an F_1 division algebra has index m_1 and B as an F_1 division algebra has index m_2, then the F-dimensions of $F[V]$ and B are $m_1^2 t$ and $m_2^2 t$ respectively, where $t = [F_1 : F]$. Suppose that both $m_1^2 t$ and $m_2^2 t$ are greater than m. If say $m_1 \geq m_2$, then $m_1 m_2 t \geq m_2^2 t > m$ by assumption. Now, if K is a maximal subfield of $F[V]$ and L a maximal subfield of B, then $K \otimes_{F_1} L$ is a subfield of Δ and of E. Since the F_1-dimensions of K and L are m_1 and m_2, we find $K \otimes_{F_1} L$ has F-dimension $m_1 m_2 t > m$. This contradicts the fact that any subfield of E must have have F-dimension bounded above by $\mathrm{ind}(E) = m$. This proves our lemma. $\square$

3. Division algebras embedded in $M_n(\mathbb{C})$.

We will retain the notation introduced in Section 1. We will prove here two results about the division algebras D of index m with center Z a number field, embedded in $M_n(\mathbb{C})$. If S and T are subrings of $M_n(\mathbb{C})$, we will write ST for the set $\{\Sigma s_i t_i, s_i \in S, t_i \in T\}$. If S and T commute, this is a subring of $M_n(\mathbb{C})$.

Proposition 3. *With D and Z as above, let α be any element in Z such that $Z = \mathbb{Q}(\alpha)$. If the minimal polynomial of α (as a matrix) has degree d, then $[\mathbb{C}Z : \mathbb{C}] = d$, and any Z-linearly independent subset of D stays $\mathbb{C}Z$-linearly independent in $\mathbb{C}D(= \mathbb{C}ZD)$. $\mathbb{C}D$ is hence a free $\mathbb{C}Z$ module of rank m^2.*

Proof. $\mathbb{C}Z = \mathbb{C}[\alpha]$, and it is clear from this that $[\mathbb{C}Z : \mathbb{C}] = d$. If the minimal polynomial of α (as a matrix) is $g(t) \in \mathbb{C}[t]$, , then $g(t)$ divides the minimal polynomial of α (as a field element) over $\mathbb{Q}$, and therefore splits in $\mathbb{C}[t]$ into d distinct linear factors $(t - \alpha_i)$. So, from $\mathbb{C}Z = \mathbb{C}[\alpha] \cong \mathbb{C}[t]/g(t)$ we find that $\mathbb{C}Z$ is a direct product of the d factors $\mathbb{C}[t]/(t - \alpha_i) \cong \mathbb{C}$. Each of these factors is a Z-algebra: α acts as multiplication by t modulo $(t-\alpha_i)$, in other words, as multiplication of $\mathbb{C}$ by α_i.

Now $\mathbb{C}D = (\mathbb{C}Z)D$, and $\mathbb{C}Z$ and D commute in $(\mathbb{C}Z)D$, so $\mathbb{C}D$ is a homomorphic image of $\mathbb{C}Z \otimes_Z D$, via $x \otimes d$ mapping to xd for $x \in \mathbb{C}Z$ and $d \in D$. Thus, $\mathbb{C}D$ is a homomorphic image of $(\mathbb{C} \times \cdots \times \mathbb{C}) \otimes_Z D$, ($d$ factors) with the $\mathbb{C}$ in the i-th slot a Z algebra as described above. In other words, $\mathbb{C}D$ is a homomorphic image of $(\mathbb{C} \otimes_Z D) \times \cdots \times (\mathbb{C} \otimes_Z D)$ We claim that this homomorphism is actually injective. Since $\mathbb{C}$ is a simple $\mathbb{Z}$ algebra, each $\mathbb{C} \otimes_Z D$ is simple. Thus, the kernel of the homomorphism is some ideal that has zeros in some slots and the corresponding factor $\mathbb{C} \otimes_Z D$ in the other slots. But note that if the kernel has $\mathbb{C} \otimes_Z D$ in the i-th slot, this means in particular that the element $(0, \dots, 1, 0, \dots) \otimes 1$ (where the 1 on the left in the i-th slot), goes to zero in $\mathbb{C}D$. Note that $\mathbb{C}Z$ embeds in $\mathbb{C}Z \otimes_Z D$ via $x \mapsto x \otimes 1$. The element $(0, \dots, 1, 0, \dots) \otimes 1$ is an element in the image of this embedding, and if it is the image of $x \in \mathbb{C}Z$, we find x goes to zero under the composition $\mathbb{C}Z \hookrightarrow \mathbb{C}Z \otimes_Z D \to \mathbb{C}D$. But the composition, which sends x to $x \otimes 1$ to $x \cdot 1 = x$, is an injection—a contradiction.

Thus, $\mathbb{C}D \cong \mathbb{C}Z \otimes_Z D$. It follows that for any Z-linearly independent subset $\{d_i, i = 1, \dots, l\}$ of D, the set $\{1 \otimes d_i, i = 1, \dots, l\}$ stays $\mathbb{C}Z$-linearly independent in the tensor product. Since D is a free Z-module of dimension m^2, the theorem follows.

□

Remark 4. We find therefore that the $\mathbb{R}$-dimension of $\mathbb{C}D$ is $2m^2d$. Thus, a trivial upper bound for the size k of the Γ_i is $\dfrac{m^2d}{2}$.

Our second result relates the minimum matrix size n to the index of D: this is thus one half of Theorem 1, Part 3.

Proposition 5. *(Theorem 1, Part 3)With D, Z and n as in the beginning of the section, and with d as in the statement of Proposition 3, we have $n \geq md$.*

Proof. We have seen in the proof of Proposition 3 that $\mathbb{C}D \cong \mathbb{C}Z \otimes_Z D \cong (\mathbb{C} \otimes_Z D) \times \cdots \times (\mathbb{C} \otimes_Z D)$ (d factors). Each $\mathbb{C} \otimes_Z D$ is simple with center $\mathbb{C}$, and of dimension m^2 over $\mathbb{C}$, and is therefore isomorphic to $M_m(\mathbb{C})$. Thus, $M_n(\mathbb{C})$ contains md orthogonal idempotents $e_{i,i}^{(k)}$, where $e_{i,i}^{(k)}$ is the (i,i) matrix unit from the k-th slot in the ring direct sum $(\mathbb{C} \otimes_Z D) \times \cdots \times (\mathbb{C} \otimes_Z D)$. The set $\sum_{i,k} e_{i,i}^{(k)} M_n(\mathbb{C})$ is a right ideal, and is actually a direct sum $\oplus_{i,k} e_{i,i}^{(k)} M_n(\mathbb{C})$, as can be seen from the orthogonality of the idempotents. Now each $e_{i,i}^{(k)} M_n(\mathbb{C})$ is itself a right ideal, and is hence a direct sum of minimal right ideals of $M_n(\mathbb{C})$, each of dimension n over $\mathbb{C}$. It follows that $\dim_{\mathbb{C}}(M_n(\mathbb{C})) = n^2 \geq \dim_{\mathbb{C}}(\sum_{i,k} e_{i,i}^{(k)} M_n(\mathbb{C})) \geq n \cdot md$, so $n \geq md$. □

4. Mutually orthogonal famllies

In this section we set up some preliminary results needed on matrices in mutually orthogonal families. First, we will say that two subsets X and Y of $M_n(\mathbb{C})$ are mutually orthogonal if x and y are mutually orthogonal for all $x \in X$ and $y \in Y$. Recall that all our code matrices are assumed invertible.

The following lemmas Lemma 6 through 9 are elementary and appeared in [2], but we will sketch their proofs for completeness:

Lemma 6. *If $A_1, \ldots, A_n$ are pairwise mutually orthogonal invertible matrices in $M_n(\mathbb{C})$, then they are $\mathbb{R}$-linearly independent.*

Proof. Assume that $r_1A_1 + \cdots + r_nA_n = 0$. For each i, multiplying this equation on the right by A_i^*, and multiplying the conjugate transpose form of this equation on the left by A_i, and then adding, we find $2r_iA_iA_i^* = 0$. Since the A_i are invertible, we find $r_i = 0$. □

Lemma 7. *If matrices A and B are mutually orthogonal, so are MA and MB for any matrix M. If M is invertible, then A and B are mutually orthogonal if and only if MA and MB are mutually orthogonal.*

Proof. This is a simple computation. □

Lemma 8. *If A and B are mutually orthogonal and A is invertible, then $A^{-1}B$ is skew-Hermitian.*

Proof. By Lemma 7 above, $A^{-1}A = I_n$ (the $n \times n$ identity matrix) and $A^{-1}B$ are mutually orthogonal. Writing down the mutual orthogonality condition for these two matrices, we find that $A^{-1}B$ is skew-Hermitian. □

Lemma 9. *The g invertible matrices $A_1 = I_n$ (the $n \times n$ identity matrix), A_2, ..., A_g in $M_n(\mathbb{C})$ are mutually orthogonal if and only if A_i is skew-Hermitian for $i \geq 2$ and A_2, ..., A_g pairwise anticommute.*

Proof. Assume that $A_1 = I_n$, A_2, ..., A_g in $M_n(\mathbb{C})$ are mutually orthogonal. Since I_n and A_i are mutually orthogonal for $i \geq 2$, we find that A_i is skew-Hermitian for $i \geq 2$. In particular, for $i, j \geq 2, i \neq j$, we may replace A_i^* by $-A_i$ and A_j^* by $-A_j$ in the orthogonality relation to obtain the anticommuting relation $A_iA_j + A_jA_i = 0$. Conversely, assume that A_i is skew-Hermitian for $i \geq 2$ and A_2, ..., A_g pairwise anticommute. We clearly have $I_nA_i^* + A_iI_n = 0$ for $i \geq 2$. Using the skew-Hermitian relation to replace the second factor in each summand of $A_iA_j + A_jA_i$ by the negative of its conjugate transpose, we find that the A_i, for $i = 2, \ldots, g$ are mutually orthogonal. □

Now let Γ_1, Γ_2, Γ_3, Γ_4 be four families of matrices from D as in the statement of Theorem 1. For the rest of the paper, we will focus on the internal algebra structure of D, and will refer to the elements in Γ_1, Γ_2, etc. by small letters, and will use 1 and I_n interchangeably for the $n \times n$ identity matrix.

Since we are only interested in the cardinality of these sets, we may pick some $w \in \Gamma_1$ (say) and multiply all matrices on the left by w^{-1}. By Lemma 7 the families $w^{-1}\Gamma_1$, $w^{-1}\Gamma_2$, $w^{-1}\Gamma_3$, and $w^{-1}\Gamma_4$ will be mutually orthogonal and since we are only multiplying through by w^{-1}, the matrices in $w^{-1}\Gamma_1 \cup w^{-1}\Gamma_2 \cup w^{-1}\Gamma_3 \cup w^{-1}\Gamma_4$ will remain $\mathbb{R}$-linearly independent. We may thus replace our original families with these new families, and we may assume that $1 \in \Gamma_1$.

Now pick some $x \in \Gamma_2$, $y \in \Gamma_3$, and $z \in \Gamma_4$. Then by the lemmas above, 1, x, y, and z are $\mathbb{R}$-linearly independent, and x, y, and z are skew-Hermitian and anticommute pairwise. The anticommutativity shows that x and y each commutes with x^2 and y^2, so x and y generate a quaternion algebra $Q_{x,y}$ over the field $Z_{x,y} := Z(x^2, y^2)$. The skew commuting relations between x and z and between y and z, show that z commutes with both x^2 and y^2, and thus, with the field $Z_{x,y}$. As is

standard (we have seen this already in the proof of Proposition 2), we may write the centralizer of $Z_{x,y}$ in D as $Q_{x,y} \otimes_{Z_{x,y}} B_{x,y}$ for some $Z_{x,y}$-central division algebra $B_{x,y}$. Hence, we may write z as $\sum_i q_i \otimes s_i$ for $q_i \in Q_{x,y}$ and s_i a $Z_{x,y}$-basis of $B_{x,y}$. We have the following:

Lemma 10. *$z = xyt$ for some $t \in B_{x,y}$, and t is Hermitian.*

Proof. The proof of this lemma is a calculation: we write $z = \sum_i q_i \otimes s_i$ as described above, and write each q_i as $Z_{x,y}$ linear combinations of 1, x, y and xy. Thus, we write $z = \sum_i (r_{i,0} + r_{i,1}x + r_{i,2}y + r_{i,3}xy) \otimes s_i)$. We use the fact that $zx + xz = 0$ to find that all $r_{i,0}$ and $r_{i,1}$ are zero. Next, the relation $zy + yz = 0$ shows that all $r_{i,2}$ are zero as well. It follows that $z = xy \otimes t = xyt$, where $t = \sum_i r_{i,3}s_i$. Since z is skew-Hermitian, we find $(xyt)^* = -xyt$. On the other had, t commutes with both x and y, so we find $(xyt)^* = (txy)^* = y^*x^*t^* = yxt^* = -xyt^*$, where the last but one equality is because x and y are skew-Hermitian, and the last equality is because x and y anticommute. We thus find $t = t^*$. □

Remark 11. Note that in the considerations above, if we had chosen to focus on the quaternion algebra generated by x and z over $Z[x^2, z^2]$, we would have found $y = xzu$, where u commutes with x and z and is Hermitian. Similarly, by focusing on the quaternion algebra generated by y and z over $Z[y^2, z^2]$, we would have found $x = yzv$ where v commutes with y and z and is Hermitian. This symmetry will be useful below.

Notation 12. *We now fix $1 \in \Gamma_1$, $x \in \Gamma_2$, $y \in \Gamma_3$ and $z \in \Gamma_4$. We list Γ_2 as $\{x_1 := x, x_2, \ldots, x_k\}$, and similarly Γ_3 as $\{y_1 := y, y_2, \ldots, y_k\}$ and Γ_4 as $\{z_1 := z, z_2, \ldots, z_k\}$. Next, we write $x_i = x_1a_i$, $y_i = y_1b_i$ and $z_i = z_1c_i$, $i = 1, \ldots, k$, for appropriate a_i, b_i and c_i in D. We write A for $\{1, a_2, \ldots, a_k\}$, B for $\{1, b_2, \ldots, b_k\}$, and C for the set $\{1, c_2, \ldots, c_k\}$.*

We have the following:

Proposition 13. *The sets A, B, and C commute pairwise. Moreover, each a_i commutes with y and z, each b_j commutes with x and z, and each c_l commutes with x and y.*

Proof. We will prove first that for each j and l, b_j and c_l commute with each other and that each b_j commutes with x and z and each c_l commutes with x and y.

We first apply the considerations of Lemma 10 above to the mutually orthogonal 4-tuple 1, x, y, and $z = z_1$, and then to 1, x, y, and z_l. Doing so, we find $z(= z_1) = (xy)t_1$, where t_1 commutes with x and y. Similarly, we find $z_l = (xy)t_l$, where t_l commutes with x and y. Thus,

$z_l = zt_1^{-1}t_l$, so we find $c_l = t_1^{-1}t_l$. We thus find c_l commutes with x and y, since both t_1 and t_l do. By symmetric arguments applied to the mutually orthogonal 4-tuple 1, x, $y = y_1$, z and then to 1, x, $y = y_j$, z (see Remark 11 above), we find b_j commutes with x and z.

By considering the mutually orthogonal 4-tuple $1, x, y_j, z_l$ we find from Lemma 9 that y_j and z_l skew-commute. Thus we find $(yb_j)(zc_l) + (zc_l)(yb_j) = 0$. In the first summand b_j commutes with z and in the second summand, c_l commutes with y. Moroever, by considering the mutually orthogonal 4-tuple 4-tuple $1, x, y, z$, we find that y and z skew-commute. Our equation thus becomes $(yz)(b_jc_l - c_lb_j) = 0$, so on canceling yz, we find that b_i and c_j commute.

The proofs for any of the pairs a_i and b_j as well as for any of the pairs a_i and c_j are similar, invoking symmetry.

□

Remark 14. Of course, since each c_l commutes with x and with each a_i, each c_l commutes with the various xa_i, $i = 2, \ldots, k$, and hence each c_l commutes with all members of Γ_2. By the same arguments, each c_l commutes with all members of Γ_3. Similarly, the members of A and Γ_3 commute pairwise, as do the members of A and Γ_4. The members of B and Γ_2 commute pairwise, as do the members of B and Γ_4. Furthermore, by considering the mutually orthogonal families $z^{-1}\Gamma_1$, $z^{-1}\Gamma_2$, $z^{-1}\Gamma_3$, $z^{-1}\Gamma_4$ (so $1 \in z^{-1}\Gamma_4$), as also the mutually orthogonal families $y^{-1}\Gamma_1$, $y^{-1}\Gamma_2$, $y^{-1}\Gamma_3$, $y^{-1}\Gamma_4$ (so $1 \in y^{-1}\Gamma_3$), and repeating the arguments above, we can see that the members of Γ_1 and A commute pairwise, as do the members of Γ_1 and B, as do the members of Γ_1 and C.

Remark 15. Note that since the elements of the family, say Γ_2 are $\mathbb{R}$-linearly independent, the elements of the family A must be $\mathbb{R}$-linearly independent, since the elements of Γ_2 are just elements of A multiplied by x_1 on the left. The same holds for the families B and C. Also note that the families A, B, and C need not be distinct. In Example 19 ahead, for instance, $A = B = C$.

We also have:

Lemma 16. *for any $a_i \in A$, and with $x_1 = x$ as in Notation 12, we have $xa_ix^{-1} = a_i^*$.*

Proof. The proof of this follows from the fact that xa_i is skew-symmetric, as is x. Write simply a for a_i. Then $(xa)^* = a^*x^* = -a^*x$. On the other hand, $(xa)^* = -xa$. We thus have $xa = a^*x$. The result now follows. □

5. Proof of Theorem 1.

In what follows, $A_0 \subseteq A$ will be a maximal set of Z-linearly independent elements in A, and similarly, $B_0 \subseteq B$ and $C_0 \subseteq C$ will be (respectively) maximal sets of Z-linearly independent elements in B and C. (Note that Z-linearly independent elements in D remain $\mathbb{C}Z$-linearly and hence $\mathbb{R}Z$- and $\mathbb{R}$-linearly independent (Proposition 3), but $\mathbb{R}$-linearly independent elements in D need not be Z-linearly independent.)

Proof of Theorem 1. We first show that $t \leq d$ (this is one part of the statement of Part 2 of of Theorem 1). As we have seen (Proposition 3), $\mathbb{C}Z$ is a d-dimension $\mathbb{C}$ space, and hence a $2d$-dimensional $\mathbb{R}$ space. Since $Z^* = Z$, $\mathbb{C}Z$ is sent to itself under conjugate transposition. Writing $\mathbb{C}Z^+$ and $\mathbb{C}Z^-$ for the set of Hermitian and skew-Hermitian matrices respectively in $\mathbb{C}Z$, it is clear that $\mathbb{C}Z \cong \mathbb{C}Z^+ \oplus \mathbb{C}Z^-$ as $\mathbb{R}$ spaces, via the mapping that sends M to $(\frac{M+M^*}{2}, \frac{M-M^*}{2})$. Moreover, multiplication by the scalar matrix $\imath$ furnishes an isomorphism between $\mathbb{C}Z^+$ and $\mathbb{C}Z^-$. Thus, the dimension of $\mathbb{C}Z^+$ as an $\mathbb{R}$-space is also d. Since t is the dimension of the $\mathbb{R}$-vector space $\mathbb{R}\langle Z^+\rangle$ generated by Z^+, and since $\mathbb{R}\langle Z^+\rangle \subseteq \mathbb{C}Z^+$, we find that $t \leq d$.

Next, let $p_1, \ldots, p_t$ be a maximal set of $\mathbb{R}$-linearly independent Hermitian matrices in Z. Suppose that $a_1, \ldots, a_l$ are the members of A_0. As observed above, the matrices in A_0, being Z-linearly independent, are also $\mathbb{C}Z$ and therefore $\mathbb{R}$-linearly independent. It follows then that the various matrices $p_j a_i$ are all $\mathbb{R}$-linearly independent. For, if say $\sum_{i,j} r_{i,j} p_j a_i = 0$, then $\sum_i (\sum_j r_{i,j} p_j) a_i = 0$. Since the a_i are $\mathbb{C}Z$ linearly independent, they are $\mathbb{R}Z$ linearly independent, so for each i, $\sum_j r_{i,j} p_j = 0$. By the choice of the p_j, each $r_{i,j}$ must be zero.

The matrices $p_j a_i$ considered above are thus a basis of the $\mathbb{R}$-space $\mathbb{R}\langle Z^+, A_0\rangle$ generated by Z^+ and A_0. We show now that the $\mathbb{R}$-space $\mathbb{R}\langle Z^+, A\rangle$ generated by Z^+ and A equals $\mathbb{R}\langle Z^+, A_0\rangle$. One direction of the containments is of course clear, we only need to show $\mathbb{R}\langle Z^+, A\rangle \subseteq \mathbb{R}\langle Z^+, A_0\rangle$. So consider any $a \in A \setminus A_0$. Since the elements of A_0 are a maximal Z-linearly independent subset of A, $a = \sum_i s_i a_i$ for $s_i \in Z$. By Lemma 16, $xax^{-1} = a^* = \sum_i a_i^* s_i^* = s_i^* a_i^*$. (The last equality is because s_i and a_i commute, so their conjugate transposes also commute with each other.) But $xax^{-1} = x(\sum_i s_i a_i)x^{-1} = \sum_i [x s_i x^{-1}] \cdot [x a_i x^{-1}]$. Invoking Lemma 16 again and the fact that the s_i are central in D, this last sum becomes $\sum_i s_i a_i^*$. We thus find $\sum (s_i^* - s_i) a_i^* = 0$, or transposing, $a_i(s_i - s_i^*) = 0$. Since $s_i^* \in Z$ by hypothesis, the Z-linear independence of the a_i shows that s_i is Hermitian. By choice of the p_j, each s_i is an $\mathbb{R}$-linear combination of the p_j. It follows immediately

that every element of A lies in the $\mathbb{R}$-space spanned by the ($\mathbb{R}$-linearly independent) matrices $p_j a_i$, which is precisely $\mathbb{R}\langle Z^+, A_0\rangle$.

It follows from the fact that the elements of A are $\mathbb{R}$-linearly independent (Remark 15) and the fact that $A \subseteq \mathbb{R}\langle Z^+, A_0\rangle$ which has $\mathbb{R}$-basis the set consisting of $p_j a_i$, that $|A| \leq t|A_0|$. But $|A| = |B| = |C|$ (as $|\Gamma_2| = |\Gamma_3| = |\Gamma_4|$), and by the same reasoning, $|B| \leq t|B_0|$ and $|C| \leq t|C_0|$. Therefore, $|A|$ is bounded above by t times the minimum of $|A_0|$, $|B_0|$, and $|C_0|$. We have the following result:

Lemma 17. *The minimum of $|A_0|$, $|B_0|$, and $|C_0|$ is at most $\frac{m}{2}$.*

Proof of Lemma 17. Since $|A_0|$ is the dimension of the Z-vector space $Z\langle A_0\rangle$ generated by A_0, and similarly for $|B_0|$ and $|C_0|$, it suffices to show that the minimum Z-space dimensions of the three *Z-algebras* $Z[A_0]$, $Z[B_0]$, and $Z[C_0]$ generated by A_0, B_0, and C_0 (respectively) is bounded above by $\frac{m}{2}$.

First consider the case where one of the families, say C_0, is commutative. The elements of the set C_0 commute with both x and y, as shown in the proof of Proposition 13. Thus, they commute with the quaternion algebra Q_{xy} generated by x and y over the field $Z_{xy} = Z(x^2, y^2)$. As before, we write the centralizer in D of Z_{xy} as $Q_{xy} \otimes_{Z_{xy}} B_{xy}$ for some Z_{xy}-central division algebra B_{xy}. Then, the algebra $Z_{xy}[C_0]$ is contained in B_{xy}. Now, if $[Z_{xy} : Z] = r$, then, the index of the centralizer of Z_{xy} is $\frac{m}{r}$, and therefore, the index of B_{xy} is $\frac{m}{2r}$. Thus, $Z_{xy}[C_0]$, being a commutative subfield of B_{xy}, has Z_{xy} dimension at most the index of B, and this is $\frac{m}{2r}$. Hence, $[Z[C_0] : Z] \leq [Z_{xy}[C_0] : Z] = [Z_{xy}[C_0] : Z_{xy}][Z_{xy} : Z] \leq \frac{m}{2r} r = \frac{m}{2}$. Thus, in the case where C_0 is commutative, we find that the minimum cardinality of A_0, B_0, and C_0 is at most $\frac{m}{2}$. Similar arguments clearly apply if A_0 or B_0 is commutative.

Now assume that one of A_0, B_0, and C_0, say C_0, is not commutative. Then $Z[C_0]$ is a division algebra of index $s \geq 2$ over some center $L \supseteq Z$. Write r for $[L : Z]$. Then the centralizer of L has index $\frac{m}{r}$, and decomposes as $Z[C_0] \otimes_L B_{C_0}$ for some L-central division algebra B_{C_0}. The index of B_{C_0} is $\frac{m}{rs}$, and this index is at most $\frac{m}{2r}$ as $s \geq 2$. Now, A_0 and B_0 are both contained in B_{C_0} as they each commute with C_0, and A_0 and B_0 commute pairwise among themselves as well (Proposition 13). If $L[A_0] = L[B_0]$, then the fact that A_0 and B_0 commute pairwise shows that A_0 is commutative, and we have already shown above that $|A_0| \leq \frac{m}{2}$ in that case. So assume $L[A_0] \neq L[B_0]$. Then $L[A_0]$ and $L[B_0]$ are two distinct subspaces of B_{C_0} that commute pairwise, so by Proposition 2, one of $[L[A_0] : L]$, $[L[B_0] : L]$ is bounded above by the index of B_{C_0}, which in turn is bounded above by $\frac{m}{2r}$. If say $[L[A_0] : L]$

is bounded above by $\frac{m}{2r}$, then $[Z[A_0] : Z] \leq [L[A_0] : Z] = [L[A_0] : L][L : Z] \leq \frac{m}{2r} r = \frac{m}{2}$.

Thus, in all cases, the minimum of $|A_0|$, $|B_0|$, and $|C_0|$ is bounded above by $\frac{m}{2}$.

□

We conclude from Lemma 17 and the arguments immediately preceding the lemma that $|A| = k \leq t \min\{|A_0|, |B_0|, |C_0|\} \leq \frac{mt}{2}$, as desired. Since we have already shown that $t \leq d$ above, we find $k \leq \frac{mt}{2} \leq \frac{md}{2}$. We have thus established Part 2 of of Theorem 1 in entirety.

To establish Part 1 of of Theorem 1, note that we have seen that the skew commuting elements x and y generate a quaternion algebra $Q_{x,y}$ with center $Z_{x,y} = Z[x^2, y^2]$. Thus, $[Q_{x,y} : Z_{x,y}] = 4$, and the containment $Z \subseteq Z_{x,y} \subseteq Q_{x,y} \subseteq D$ shows that 4 divides $[D : Z] = m^2$. It follows that m is even.

Finally, Part 3 of of Theorem 1 follows from Proposition 5: $md \leq n$ by that proposition, so indeed $k \leq \frac{md}{2} \leq \frac{n}{2}$.

We have thus proved Theorem 1. □

We end this section with a couple of examples and a remark:

Example 18. Consider the matrices $w_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $x_1 = \begin{pmatrix} \imath & 0 \\ 0 & -\imath \end{pmatrix}$, $y_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, and $z_1 = \begin{pmatrix} 0 & -\imath \\ -\imath & 0 \end{pmatrix}$. These arise from the representation of Hamilton's quaternions $\frac{(-1,-1)}{\mathbb{Q}}$ in $M_2(\mathbb{C})$, and each of them is mutually orthogonal to the other three. These matrices are $\mathbb{R}$-linearly independent, and satisfy $x_1^2 = -I_2$, $y_1^2 = -I_2$, and $x_1 y_1 = z_1 = -y_1 x_1$. Clearly $m = 2$ here, $Z = \mathbb{Q}$, and $d = 1$, and the maximum of $k = \frac{md}{2}$ is met. (This example is known as the "Alamouti Code" in the communication engineering literature.)

Example 19. More generally (we thank Nadya Markin for showing us this generalization) , let $Z = \mathbb{Q}(\alpha)$ be a totally real number field of degree d, and view $M_{2d}(\mathbb{C})$ as $M_2(\mathbb{C}) \otimes_{\mathbb{C}} M_d(\mathbb{C})$. Let $\alpha_1 = \alpha$, α_2, ..., α_d be the various conjugates of α, all real by assumption. We may embed Z into $M_{2d}(\mathbb{C})$ by sending α to I_2 tensored with the matrix M_α that has α_1, ..., α_d along the diagonal. Then, we may embed the Z-central division algebra $\frac{(-1,-1)}{Z} \cong \frac{(-1,-1)}{\mathbb{Q}} \otimes_{\mathbb{Q}} Z$ into $M_{2d}(\mathbb{C})$ via $w_1 \otimes I_d$, ..., $z_1 \otimes I_d$, and with Z embedded as above. The four families of matrices $w_1 \otimes M_\alpha^j$, $x_1 \otimes M_\alpha^j$, $y_1 \otimes M_\alpha^j$, and $z_1 \otimes M_\alpha^j$, $j = 1, \ldots, d$

are mutually orthogonal, and we have the maximum of $k = \frac{2d}{2}$ real symbols.

Remark 20. A key parameter of the code $X(\underline{s})$ described in Section 1 is the *code rate,* defined as $\frac{2l}{n}$ (this has the interpretation that it is the number of real symbols transmitted "per single use of the transmission channel"). A "full-rate" code, where l has the maximum possible value of n^2, would have a code rate of: $\frac{2n^2}{n} = 2n$; however the worst case decoding complexity of such a code is very high as we have seen. Our results in Theorem 1 show that for codes that enable parallel decoding using 4 mutually orthogonal groups, the maximum code rate drops to $4\frac{\frac{n}{2}}{n} = 2$, which is a low constant that does not grow at all with n, the number of antennas. Thus, our results show that there is a significant tradeoff between faster decodability using mutually orthogonal groups and the maximum code rate.

References

[1] Amaro Barreal, Camilla Hollanti, and Nadya Markin, "Fast-Decodable Space-Time Codes for the N-Relay and Multiple-Access MIMO Channel," *IEEE Transactions on Information Theory,* vol. 15, pp. 1754–1767, March 2016.

[2] Grégory Berhuy, Nadya Markin, and B. A. Sethuraman, "Bounds on fast decodability of space-time block codes, skew-Hermitian matrices, and Azumaya algebras," *IEEE Transactions on Information Theory,* vol. 61, pp. 1959–1970, April 2015.

[3] Grégory Berhuy and Frederique Oggier, An Introduction to Central Simple Algebras and Their Applications to Wireless Communication, American Mathematical Society, Mathematical Surveys and Monographs vol. 191, 2013.

[4] Nathan Jacobson, Basic Algebra II, W.H. Freeman, 1989.

[5] G.R. Jithamithra, B.S Rajan , Minimizing the Complexity of Fast Sphere Decoding of STBCs, *IEEE Transactions on Wireless Communications*, vol 12, no. 12, 2013.

[6] R. Vehkalahti, C. Hollanti, F. Oggier, "Fast-Decodable Asymmetric Space-Time Codes from Division Algebras," *IEEE Transactions on Information Theory*, vol. 58, no. 4, April 2012.

[7] T.P. Ren, Y.L. Guan, C. Yuen, and R.J. Shen, "Fast-group-decodable space-time block code," Proceedings IEEE Workshop (ITW 2010), 2010.

[8] B.A. Sethuraman, "Division algebras and wireless communications," *Notices of the Amer. Math. Soc.*, vol. 57, pp. 1432–1439, December 2010.

[9] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. on Information Theory*, vol. 49, no. 10, pp. 2596-2616, Oct. 2003.

[10] K. P. Srinath, B. S. Rajan, "Low ML-decoding complexity, large coding gain, full-diversity STBCs for 2×2 and 4×2 MIMO systems," *IEEE J. on Special Topics in Signal Processing: managing complexity in multi-user MIMO systems*, 2010

Department of Mathematics, California State University Northridge, Northridge, CA 91330, USA.
E-mail address: al.sethuraman@csun.edu