ARTICLE IN PRESS
JPAA:5825

Journal of Pure and Applied Algebra ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

Mutually orthogonal matrices from division algebras

B.A. Sethuraman [1]

Department of Mathematics, California State University Northridge, Northridge, CA 91330, USA

A R T I C L E I N F O

Article history:
Received 27 February 2017
Received in revised form 6 December 2017
Available online xxxx
Communicated by R. Sujatha

MSC:
11C20; 11R52; 17C60

A B S T R A C T

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, 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 ϕ: $q \mapsto \mathrm{diag}(q, \ldots, q)$ in $M_n(\mathbb{C})$. We give examples to show that this maximum is actually attained.

E-mail address: al.sethuraman@csun.edu.

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

https://doi.org/10.1016/j.jpaa.2017.12.021
0022-4049/

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 $A_{i,u}$, $u = 1, 2, \ldots,$

Please cite this article in press as: B.A. Sethuraman, Mutually orthogonal matrices from division algebras, J. Pure Appl. Algebra (2017), https://doi.org/10.1016/j.jpaa.2017.12.021