DRDO–IISc Programme on
Advanced Research in Mathematical
Engineering

Full-Rank Space-Time Block Codes from Division Algebras

(TR-PME-2002-14)

by
B.A.Sethuraman and B.Sundar Rajan
ECE. IISc, Bangalore
email: bsrajan@ece.iisc.ernet.in

October 4, 2002

Indian Institute of Science
Bangalore 560 012

Full-Rank Space-Time Block Codes from Division Algebras

B.A.Sethuraman and B.Sundar Rajan

October 4, 2002

ABSTRACT

An $n \times l$ $(l \geq n)$ space time block code (STBC) $\mathcal{C}$ consists of a finite number $|\mathcal{C}|$ of $n \times l$ matrices with entries from the complex field. If the entries of the codeword matrices take values from a complex signal set S or complex linear combinations of elements of S then the code is said to be over S. For quasi-static, flat fading channels a primary performance index of $\mathcal{C}$ is the minimum of the rank of the difference of any two codeword matrices, called the rank of the code. $\mathcal{C}$ is of full-rank if its rank is n and is of minimal-delay if $l = n$. The rate

[1]B.A.Sethuraman is with AUKBC Research Center, Anna University—M.I.T. Campus, Chennai 600044, India, and Dept. of Mathematics, California State University Northridge, CA 91330, U.S.A., email:al.sethuraman@csun.edu

[2]B.S.Rajan is with the Department of Electrical Communication Engineering and the Department of Computer Science and Automation, Indian Institute of Science, Bangalore-560 012, India, email:bsrajan@ece.iisc.ernet.in

This was partly supported by a generous grant from K.B.Chandrashekhar Family Foundation to the first author and by Academic and Research Collaboration Programme on Mathematical Engineering between the DRDO, New Delhi and IISc, Bangalore, India, to the second author.

Different parts of the content of this report appear as (i) B.A.Sethuraman and B.Sundar Rajan, "Optimal STBC over PSK Signal Sets from Cyclotomic Field Extensions," Proceedings of IEEE International Conference on Communications (ICC 2002), April 28-May 3, New York, U.S.A., vol.3, pp.1783-1787, (ii) B.A.Sethuraman and B.Sundar Rajan, "STBC from Field Extensions of the Rational Field," Proceedings of IEEE International Symposium on Information Theory, (ISIT 2002), June 30-July 5, Lausanne, Switzerland, vol.3, p.274, (iii) B.A.Sethuraman and B.Sundar Rajan, "Al Algebraic Description of Orthogonal Designs and the Uniqueness of the Alamouti Code," to appear in the Proceedings of IEEE GLOBECOM 2002, Taipai, Nov.2002 and (iv) B.A.Sethuraman and B.Sundar Rajan, "Full-rank, Full-rate STBCs from Division Algebras,“ to appear in 2002 IEEE Information Theory Workshop, to be held in Bangalore, Oct.20-25, 2002.

of the code R in symbols per channel use is given by $\frac{1}{l}\log_{|S|}(|\mathcal{C}|)$. In this paper, we present some general techniques for constructing rate 1, full-rank, minimal-delay STBCs over S using commutative division algebras (field extensions) as well as using non-commutative division algebras of the rational field $\mathbb{Q}$ embedded in matrix rings.

The first half of the paper deals with constructions using field extensions of $\mathbb{Q}$. Working primarily with cyclotomic field extensions, we construct several families of codes over a wide range of signal sets. As special cases, our method gives full-rank minimal-delay symbol-rate 1 STBCs over symmetric m-PSK signal sets (m-arbitrary) for a wide range of values of the number of antennas n, and *for arbitrary number of antennas* over (i)asymmetric PSK signal sets matched to dihedral groups, (ii) signal sets that are union of a symmetric PSK signal set and its scaled version, and (iii) rotationally invariant QAM signal sets . For completeness, we also present a method of constructing STBCs using minimal polynomials that lead to non-cyclotomic fields. In the later half of the paper, we discuss two ways of embedding non-commutative division algebras into matrices: the left regular representation, and representation over maximal cyclic subfields. We observe that the left regular representation yields codes for n^2 number of antennas where n is the degree (or index) of the division algebra and representations over maximal cyclic subfields yields codes for n number of antennas . We show that the representation over maximal cyclic subfields yields codes consisting of matrices in which the entries are twisted by powers of a field automorphism. The Alamouti's code is just a special case of this construction and we observe certain uniqueness characteristics of it in a similar way as it is the only complex orthogonal design. Also, we discuss a general principle for constructing cyclic division algebras using the n-th root of a transcendental element, and then describe a family of cyclic division algebras discovered by Brauer. We give several examples of STBCs derived from each of these constructions.

1 Introduction

It is well known that multiple-antenna wireless communication promises very high data rates, especially when the channel is known at the receiver [1, 2]. A constructive approach to design codes suitable for such systems was proposed in [3] and design criterion were developed in [4]. Two major classes of codes for multiple antenna systems are Space-Time Trellis Codes (STTC) and Space-Time Block Codes (STBC).

An $n \times l$ ($l \geq n$) space time block code (STBC) $\mathcal{C}$ is a finite number of

$n \times l$ matrices with complex entries. By STBCs over complex signal sets we mean those covered by

Definition 1. *If all the codeword matrices of a STBC $\mathcal{C}$ have some fixed subset of the slots taking values from a complex signal set S independently and entries of all other slots are complex linear combinations of the entries of this subset of slots (like in orthogonal designs), then $\mathcal{C}$ is said to be* **over** *S. If all the entries of all the codeword matrices are from S, then $\mathcal{C}$ is said to be* **completely over** *S.*

For instance, if x_0 and x_1 in the Alamouti code $\begin{bmatrix} x_0 & x_1 \\ -x_1^* & x_0^* \end{bmatrix}$ take values from a symmetric 3-PSK signal set S then the code is over S but not completely over S. It is completely over S' where S' denotes the symmetric 6-PSK signal that is the union of S and $-S$.

For quasi-static, flat fading channels a primary performance index of $\mathcal{C}$ is the minimum of the rank of the difference of any two codeword matrices, called the rank of the code. $\mathcal{C}$ is of full-rank if its rank is n and is of minimal-delay if $l = n$. The rate of the code R in symbols per channel use is given by $\frac{1}{l}\log_{|S|}(|\mathcal{C}|)$. If the rank of an $n \times l$ STBC that is completely over S is r then transmission rate of this code in bits per seconds per Hertz is bounded above by $\frac{1}{l}\log_2\left[A_{|S|^l}(n, r)\right]$, where $A_x(y, z)$ denotes the maximum size of a code of length y and minimum Hamming distance z defined over an alphabet of size x [4]. From this it follows that for full-rank codes completely over S the rate R in symbols per channel use is upper bounded by 1.

Definition 2. *A code completely over S with rate meeting the upper bound above is called a full-rate code. A minimal-delay full-rank, full-rate STBC completely over S is said to be rate-optimal over S.*

We use the term "rate-optimal" to highlight the fact that we have not optimized the coding gain among such codes. Notice that when the codeword matrices are allowed to have entries which are complex linear combinations of elements S, as in [17], then the rate of a full-rank, minimal-delay code can be more than 1 symbol per channel use.

STBCs have been studied by several authors: A simple STBC for two transmit antennas which admits a simple decoding was proposed by Alamouti [5] for arbitrary complex constellations. A generalization to Alamouti code was studied using the theory of orthogonal designs in [6]. In these codes decoupling of symbols transmitted from different antennas, which leads to simple decoding, is due to the orthogonal structure of these codes. It was also shown that for complex constellations, the only possible orthogonal design for 2 transmit antennas is the Alamouti code. A similar treatment, based on optimal SNR, of STBCs was also carried out by Ganesan and Stoica in [20, 21]. STBCs specific to PSK and QAM modulation have been studied in [7] and [8] respectively. Design of STBCs using groups and representation theory of groups have been reported in [9, 10, 11, 12] and using unitary matrices STBCs have been studied in [13, 14, 15, 16]. Hassibi and Howchwald [17] introduced codes that are linear in space and time called "Linear Dispersion Codes" which absorb STBCs from orthogonal designs as a special case. The ML decoding complexity of these codes is exponential but due to their linear structure, sub-optimal linear complexity decoding algorithms like 'successive nulling and canceling', 'square-root' and 'sphere decoding' can be used [17]. A scheme that trades diversity for simpler ML decoding is presented in [22].

In this paper, we present some general techniques for constructing rate-optimal as well as rate 1, full-rank, minimal-delay STBCs over S from field extensions (commutative division algebras) of the rational field $\mathbb{Q}$ embedded in matrix rings as well as from non-commutative division algebras embedded in matrix rings. Specializing the general technique for code construction using field extensions to cyclotomic field extensions, we construct rate-optimal STBC over symmetric m-PSK (m- arbitrary) for a wide range of values of the number of antennas n and minimal-delay full-rank rate 1 STBCs over a wide range of signal sets including certain asymmetric PSK, QAM and cross-constellations for arbitrary number of antennas. The minimal-delay STBCs obtained earlier in [6] by orthogonal designs are linearly decodable, rate 1, full-rank but unfortunately, exists for only 2,4 and 8 antennas for real signal constellations and only for 2 antennas for complex constellations. The constructions presented in [7] are only for BPSK and 4-PSK signal sets. The constructions of STBCs presented in this paper, on the other hand, are for a very wide range of signal sets and a very wide range of the number of antennas. For instance, the codes we obtain over symmetric m-PSK signal sets are valid for arbitrary m and for any number of antennas n, as long as n is not divisible by any prime that does not divide m. The constructions we present for minimal-delay full-rank rate 1 STBCs over other signal sets like asymmetric PSK, QAM and cross-constellations are valid for arbitrary number of antennas.

In the second half of the paper, we show that we can create codes of both size $n^2 \times n^2$ and of size $n \times n$ using embeddings of division algebras into matrix rings where n is the index of the division algebra. We focus primarily on cyclic division algebras, and show that Alamouti's code and real orthogonal designs of size 2 and 4 are special cases of our construction. We also point out a uniqueness property of Alamouti's code from the point of view of division algebras.

A difference between our approach and, say, Alamouti's approach, or more generally the approach of Tarokh et.al. using orthogonal designs [6], is that these authors come up with codes that will work with any signal set that is a subset of the complex field , whereas we come up with codes that will work with any signal set that is a subset of certain subfields of the complex field—in the process, however, we get enormous flexibility in terms of the number of antennas. Moreover, while we do not have linear decoding algorithms for our codes, all the codes we obtain in this paper constitute subclasses of Linear Dispersion codes [17], and hence the suboptimal decoding algorithms that apply to Linear Dispersion codes will also apply to the codes of this paper.

Throughout the paper we will have $n = l$ and hence all the matrices discussed are $n \times n$ square matrices and the codes minimal-delay codes.

The organization of the paper is as follows: In Section 2 we present the main principle underlying the code construction using embeddings of division algebras in matrix rings. The application of this principle to the case of commutative division algebras (or field extensions) is discussed in Section 3. A general technique for constructing STBCs from field extensions is presented in Section 4, and explicit code constructions over several signal sets like symmetric PSK, certain asymmetric PSK and rotationally invariant QAM signal sets are provided. Most of these are constructed using cyclotomic field extensions. A method of code construction using non-cyclotomic field extensions is also presented. In Section 5 we begin the application of the main principle given in Section 2 to the case of non-commutative division algebras by way of brief introduction to the basic structural properties of division algebras and a discussion on left regular representations of division algebras. In Section 6 we discuss cyclic division algebras and the representation of a cyclic division algebra in matrices over its maximal cyclic subfield. We show in the same section that Alamouti's code is a special case of this construction. In Section 7 we describe a technique for constructing cyclic division algebras using transcendental elements, and we describe some STBCs derived from this construction. In Section 8 we describe Brauer's division algebras and outline some explicit STBCs obtained from such algebras. Section 9 briefly describes the relationship of the codes of this paper with linear dispersion codes and orthogonal designs. Some important directions for further research constitute Section 10.

2 The Main Principle

In this section we present the basic principle used to construct STBCs throughout the paper.

All rings in this paper will be associative, and will possess a unit element 1. Recall that a division algebra[1] is simply a ring in which every nonzero element has a multiplicative inverse. A commutative division algebra, of course, is just a field, but non-commutative division algebras exist in profusion (the first such discovered was Hamilton's quaternions [18].)

Example 1. *The Hamilton's Quaternions denoted by* $\mathbb{H}$ *is the very first division algebra discovered. As is well known,* $\mathbb{H}$ *is the four dimensional vector space over the field of real numbers* $\mathbb{R}$ *with basis* $\{1, \hat{\imath}, \hat{\jmath}, \hat{k}\}$*, with multiplication given by* $\hat{\imath}^2 = \hat{\jmath}^2 = -1$ *and* $\hat{\imath}\hat{\jmath} = k = -\hat{\jmath}\hat{\imath}$*. That is,* $\mathbb{H}$ *is the set of all expressions of the form* $\{a(= a \cdot 1) + b\hat{\imath} + c\hat{\jmath} + d\hat{k} \mid a, b, c, d \in \mathbb{R}\}$*. The real numbers are identified with quaternions in which the coefficients of* $\hat{\imath}$*,* $\hat{\jmath}$*, and* $\hat{k}$ *are all zero. From the given relations, one can easily derive that* $\hat{k}^2 = -1$*, that* $\hat{\jmath}\hat{k} = \hat{\imath} = -\hat{k}\hat{\jmath}$*, and that* $\hat{k}\hat{\imath} = \hat{\jmath} = -\hat{\imath}\hat{k}$*. To multiply two quaternions* $x = a + b\hat{\imath} + c\hat{\jmath} + d\hat{k}$ *and* $y = e + f\hat{\imath} + g\hat{\jmath} + h\hat{k}$ *(where* a*, ...,* h *are real numbers), one would multiply term by term, and reduce all products of two terms using the relations above: for instance, the product of the two terms* $b\hat{\imath}f\hat{\imath}$ *would be rewritten as* $bf\hat{\imath}^2 = -bf$*, while the product* $b\hat{\imath}g\hat{\jmath}$ *would be rewritten as* $bg\hat{\imath}\hat{\jmath} = bg\hat{k}$*. One can check that the multiplicative inverse of the nonzero quaternion* $x = a + b\hat{\imath} + c\hat{\jmath} + d\hat{k}$ *is the quaternion* $(a/z) - (b/z)\hat{\imath} - (c/z)\hat{\jmath} - (d/z)\hat{k}$*, where* $z = a^2 + b^2 + c^2 + k^2$*. Thus, as every nonzero element has a multiplicative inverse,* $\mathbb{H}$ *is indeed a division algebra.*

Basic results concerning the structure of division algebras are given in Section 5. Now we discuss a very broad principle that can be used to construct full-rank minimal-delay codes from division algebras:

Let D be a division algebra, and let $f \colon D \to M_n(F)$ be a ring homomorphism from D to the set of $n \times n$ matrices over some field F. Since every element in D is invertible, D has no nontrivial two-sided ideals, so the kernel of f is either all of D or else, f is an injection. Since f does not map the unit element of D to zero, f must necessarily be an injection, and therefore, the image $f(D)$ (which is a subring of $M_n(F)$) must be isomorphic to D. (We say that $f(D)$ is an *embedding* of D in $M_n(F)$). Now let $E \subset f(D)$ be any subset of the image of f. If $M_1 = f(d_1)$ and $M_2 = f(d_2)$ are two distinct elements in E, then $M_1 - M_2 = f(d_1) - f(d_2) = f(d_1 - d_2)$. Since M_1 and M_2 are distinct and f is injective, $d_1 - d_2 \neq 0$, so it has a multiplicative inverse in D. Since D is isomorphic to its image $f(D)$, $f(d_1 - d_2) = M_1 - M_2$ must also be invertible in $f(D) \subset M_n(F)$. Hence, $M_1 - M_2$ must be of full-rank,

[1]The word "algebra" refers to the fact that such a ring is naturally a vector space over its center; this will not concern us in the first half of the paper and hence elaborated in Section 5 for use in the later half.

and our subset E must therefore have the property that the difference of any two elements in E will be of full-rank. We state this below as

Proposition 1. *Let $f\colon D \to M_n(F)$ be a ring homomorphism from a division algebra D to the set of $n \times n$ matrices over some field F. If E is any finite subset of the image of D under this map, then E will have the property that the difference of any two elements in it will be of full-rank.*

The rest of the paper essentially consists of constructing several such embeddings, first arising from field extensions of $\mathbb{Q}$, (i.e., D will be a commutative division algebra)(Sections 3 and Section 4) and then from non-commutative division algebras (Sections 5 through Section 8) and obtaining STBCs over a wide variety of signal sets using these embeddings.

3 Embedding Field Extensions into Matrices

We will recall some well-known facts (see (§7.3, [18]) for instance) about embedding field extensions into matrix algebras in this section. Let K and F be fields, with $F \subset K$, and $[K : F] = n$, i.e., K is of dimension n over F. In our application to space-time codes, F will be a suitable extension field of $\mathbb{Q}$ determined by the signal set S over which we want to construct the code and K a subfield of $\mathbb{C}$, (i.e., $\mathbb{Q} \subset F \subset K \subset \mathbb{C}$) but in this section, F can be arbitrary. Recall that K can be viewed as an n-dimensional vector space over F, and that we have a natural map L from K to $End_F(K)$, which is the set of F-linear transforms of the vector space K. This map is given by $k \mapsto \lambda_k$, where λ_k is the map on the F-vector space K that sends any $u \in K$ to the element ku. (That is, λ_k is simply multiplication by k.) It is trivial to see that λ_k is indeed in $End_F(K)$, that is, that $\lambda_k(f_1u_1 + f_2u_2) = f_1\lambda_k(u_1)+f_2\lambda_k(u_2)$. Moreover, it is easy to see that L is a *ring homomorphism* from K to $End_F(K)$, that is, $\lambda_{k_1+k_2} = \lambda_{k_1} + \lambda_{k_2}$, $\lambda_{k_1k_2} = \lambda_{k_1}\lambda_{k_2}$, and $\lambda_1 =$ (identity element). As in the discussions in the previous subsection 2 above, we find that L maps K isomorphically into $End_F(K)$, that is, K embeds in $M_n(F)$.

Notice that the image of the ground field F under L is simply the set of scalar matrices. This particular method of embedding K into $M_n(F)$ is known as the *regular representation of K in $M_n(F)$*.

For a given choice of F basis $\mathcal{B} = \{u_1, u_2, \ldots, u_n\}$ of K, one can write down the matrix corresponding to λ_k for any k as follows: for any given basis element u_i $(1 \le i \le n)$, and for any j $(1 \le j \le n)$, let $u_iu_j = \sum_{l=1}^{n} c_{ij,l}u_l$. Then, the j-th column of λ_{u_i} is simply the coefficients $c_{ij,l}$ above, $1 \le l \le n$. (Here, we use the convention that the vectors on which a matrix acts are written on the right of the matrix as a column vector, so the j-th column of the matrix just represents the image of the j-th standard basis vector under the action of the matrix.) Once the matrix corresponding to each λ_{u_i}, call it M_i, is obtained in this manner, the matrix corresponding to a general λ_k, with $k = \sum_{i=1}^{n} f_i u_i$ is just the linear combination $\sum_{i=1}^{n} f_i M_i$.

When K is generated over F by a primitive element α (this is always the case in characteristic zero, the case we will consider throughout the paper anyway), the matrices in the particular basis $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ are easier to write down. Suppose that the minimal polynomial of α over F is $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Then λ_α sends 1 to α, so the first column of the matrix of λ_α consists of zeroes everywhere except in the $(2,1)$ slot, where it has a 1. Similarly, the second column consists of zeroes everywhere except in the $(3,2)$ slot, where it has a 1. Proceeding, the $(n-1)$-th column consists of zeroes everywhere except in the $(n, n-1)$ slot, where it has a 1. The last column of the matrix is more interesting: λ_α sends α to α^n, which, from the minimal polynomial, is $-a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1}$. Thus, the last column of the matrix has the entries $-a_0, -a_1, \ldots, -a_{n-1}$. The matrices corresponding to the other powers α^i can be obtained similarly (which is a bit tedious), or else, just computed directly as the i-th power of the matrix corresponding to α.

If we write M for the matrix above, that is,

$$M = \begin{bmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 0 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \vdots & 0 & \vdots \\ 0 & 0 & 0 & 1 & -a_{n-1} \end{bmatrix}, \tag{1}$$

then the general element $k = f_0 + f_1\alpha + \ldots f_{n-1}\alpha^{n-1}$ will be mapped to the matrix $f_0 I_n + f_1 M + f_2 M^2 + \ldots + f_{n-1}M^{n-1}$. The matrix M is known as the *companion matrix* of $f(x)$. We thus have:

Proposition 2. *Let $K = F(\alpha)$ be an extension of the field F of degree n, and suppose that the minimal polynomial of α over F is $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Let M be the matrix in $M_n(F)$ defined in equation (1). Then the set of all matrices of the form $f_0 I_n + f_1 M + f_2 M^2 + \ldots + f_{n-1}M^{n-1}$, with f_0, f_1, ..., f_{n-1} coming from F is an embedding of K into $M_n(F)$. In particular, any finite subset E of such matrices will have the property that the difference of any two matrices in it will have full-rank.*

Proof. The last statement follows from Proposition 1 above. □

When the minimal polynomial of α has the special form $x^n - \gamma$ for some $\gamma \in F^*$ (non-zero elements of F), the form of the matrices simplify considerably. The matrix corresponding to α is then

$$\begin{bmatrix} 0 & 0 & \dots & \dots & 0 & \gamma \\ 1 & 0 & \dots & \dots & 0 & 0 \\ 0 & 1 & \dots & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & 1 & 0 \end{bmatrix}$$

The square of this matrix is then

$$\begin{bmatrix} 0 & 0 & \dots & \dots & \gamma & 0 \\ 0 & 0 & \dots & \dots & 0 & \gamma \\ 1 & 0 & \dots & \dots & 0 & 0 \\ \vdots & 1 & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & 0 & 0 \end{bmatrix}$$

and so on. It is now easy to see that the matrix corresponding to λ_k, where $k = f_0 + f_1\alpha + \ldots + f_{n-1}\alpha^{n-1}$, is

$$\begin{bmatrix} f_0 & \gamma f_{n-1} & \gamma f_{n-2} & \dots & \gamma f_2 & \gamma f_1 \\ f_1 & f_0 & \gamma f_{n-1} & \dots & \gamma f_3 & \gamma f_2 \\ f_2 & f_1 & f_0 & \dots & \gamma f_4 & \gamma f_3 \\ f_3 & f_2 & f_1 & \dots & \gamma f_5 & \gamma f_4 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ f_{n-1} & f_{n-2} & f_{n-3} & \dots & f_1 & f_0 \end{bmatrix} \tag{2}$$

These observations essentially prove the following special case of Proposition 2 above:

Proposition 3. *Let F be a field, and let γ be a nonzero element of F. Suppose that the polynomial $x^n - \gamma$ ($n \geq 2$) is irreducible in $F[x]$. Then, the set of all matrices of the form (2) above, with f_0, f_1, ..., f_{n-1} coming from F, forms a field, isomorphic to $F(\sqrt[n]{\gamma})$. In particular, any finite set of such matrices will have the property that the difference of any two in it will have full-rank.*

Proof. Let α be some n-th root of γ in some algebraic closure of F. Then the field $K = F(\alpha)$ has degree n over F, since the polynomial $x^n - \gamma$ is irreducible in $F[x]$. The discussions above then shows that the set of matrices of the form (2) above is isomorphic to K under the map L. The last statement follows from Proposition 1 above. $\square$

Remark 1. It is essential in the proposition above that the elements f_i all come from F. For instance, with $F = \mathbb{Q}$ and $\gamma = n = 2$, we find from the proposition that the set of matrices of the form

$$\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$$

with a and b coming from $\mathbb{Q}$ is isomorphic to $\mathbb{Q}(\sqrt{2})$. However, if a and b are allowed to be arbitrary complex numbers, the set of such matrices is no longer a field. For instance, taking $a = \sqrt{2}$ and $b = 1$, we get a nonzero matrix that is not invertible, so the set of all such matrices with arbitrary complex (or even real) entries cannot be a field.

Remark 2. Matrices of the form (2) with $\gamma = 1$ are called *circulant* matrices. It is easy to see that the set of all circulant matrices constructed from a finite set will not satisfy the full-rank criterion.

Remark 3. If $f\colon D \to M_n(F)$ is an embedding of D, then, for any invertible matrix $M \in M_n(F)$, $Mf(D)M^{-1}$, that is, f followed by conjugation by M, is another embedding of D into $M_n(F)$. So, a finite set of matrices of the form $Mf(d_i)M^{-1}$, for any choice of elements $d_i \in D$ will also be a full rank minimum delay code. (Conjugation by M merely rewrites matrices with respect to the new basis represented by M.) In particular, if M is taken to be a diagonal matrix, then the entries of $f(d_i)$, on conjugation by M, will simply be multiplied and divided by appropriate elements of (the diagonal of) M, and will thus represent a simple modification of the original code $\{f(d_i)\}$.

This scheme can be further generalized by considering all matrices of the form $Mf(D)N$, where M and N are any two invertible matrices in $M_n(K)$, where K is any extension field of F. In this generality, the matrices $Mf(D)N$ are not multiplicatively closed, and hence do not represent an embedding of D into $M_n(K)$, but the property of forming a set of matrices such that the difference of any two in it will have full rank is not destroyed: if d_1 and d_2 are two distinct elements of D, then $det(Mf(d_1)N - Mf(d_2)N) = det(M(f(d_1) - f(d_2))N) = det(M)det(f(d_1) - f(d_2))det(N) \neq 0$. While we will not explicitly follow such generalizations in this paper, it is to be understood that all codes we describe subsequently can easily be modified as just described to get new codes.

4 Constriction of STBCs using Field Extensions

In this section we will outline a simple technique to construct rate-optimal STBCs over a given finite set of nonzero complex numbers, using Propositions 2 and 3. Let S be the finite subset of the nonzero complex numbers that we wish to use as our signal set, and say $|S| = m$. Write F for the field generated by all the elements of S over $\mathbb{Q}$. (For instance, if $S = \{1, j, -1, -j\}$, then F is just the field obtained by adjoining the elements 1, j, -1, and $-j$ to $\mathbb{Q}$ or in other words, F is just $\mathbb{Q}(j)$.) Let n be the number of transmit antennas to be used ($n \geq 2$). Let K be a field extension of F of degree n. Then, by the primitive element theorem, $K = F(\alpha)$, for some element $\alpha \in K$ whose minimal polynomial is $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ for suitable $a_i \in F$. We have the following sequence of field extensions:

$$\mathbb{Q} \subset \mathbb{Q}(S) = F \subset \mathbb{Q}(S, \alpha) = F(\alpha) = K.$$

Consider all matrices of the form $f_0 I_n + f_1 M + f_2 M^2 + \ldots + f_{n-1} M^{n-1}$, where the f_0, f_1, $\ldots$, f_{n-1} come from the signal set S, and where M is the matrix in $M_n(F)$ defined in equation (1). This is a finite set of matrices of cardinality m^n, which, by Proposition 2 is a full-rank minimal-delay code over S. To be precise, the actual elements of the matrices transmitted under this scheme will not all come from the chosen signal set S, but instead, will be some simple, *linear* function of the elements of S.

Theorem 4. *The STBC code consisting of matrices of the form $f_0 I_n + f_1 M + f_2 M^2 + \ldots + f_{n-1} M^{n-1}$, where the f_0, f_1, $\ldots$, f_{n-1} come from the signal set S, and where M is the matrix in $M_n(F)$ defined in equation (1) is rate-optimal if all the codeword matrices has entries only from S and no other linear function of the elements of S (i.e., the signal set S is invariant under all linear combinations with coefficients $a_0, a_1, \cdots, a_{n-1}$).*

Proof. Follows from the fact that the resulting code is completely over S, of full-rank and from Theorem 3.3.1 of [4]. $\square$

This construction becomes simpler if we know that there is an element $\gamma \in F^*$ that has the property that the polynomial $x^n - \gamma$ is irreducible in $F[x]$. (Note that γ need not be in S.) This time, we consider matrices of the form form (2), with the f_i constrained to be in S. We get a finite set of matrices of size m^n, which, by Proposition 3 is again a full-rank minimal-delay code, and this code is over S and the entries of the codeword matrices are from the set $S \cup \gamma S$. That is, the actual entries of the matrices that are transmitted will not all be in S, but instead, some of the entries will be elements of S multiplied by γ. However, suppose that the set S and the element γ have the property that $\gamma s \in S$ for all elements $s \in S$. Then, all elements of the transmitted matrices will actually have their entries in S. When this happens, we say that S is *invariant under multiplication by* γ and the resulting code is completely over S. In many of our examples below, we will choose S and γ so that S is invariant under multiplication by γ.

A property that the element γ must have if our signal set S is to be invariant under multiplication by γ is:

Lemma 5. *Let S be a finite subset of the nonzero complex numbers, and let γ be some nonzero complex number. If S is invariant under multiplication by γ, then γ must be a root of unity.*

Proof. Let s be any element of S. By choice of γ, the elements γs, $\gamma^2 s$, ..., $\gamma^k s$, ... are all in S. Since S is a finite set, these elements cannot all be distinct, that is, for some $1 \leq i < j$, $\gamma^i s = \gamma^j s$. Canceling γ^i and s from both sides (note that the elements of S and γ are all nonzero), we find that $\gamma^{j-i} = 1$. □

4.1 Rate-optimal Codes over Symmetric m-PSK Signal Sets

In this section, we will construct (rate-optimal) STBCs over a signal set consisting of m equally spaced points on the unit circle, where m is any positive integer ($m \geq 2$), called an m-PSK signal set. (The points S_0, ..., S_7 in Fig.1 constitute an 8-PSK signal set.) The number of transmit antennas n is allowed to be any integer that has the property that the primes that appear in the factorization of n is some subset of the primes that appear in the factorization of m. (Thus, for example, with a signal set consisting of 6 equally spaced points on the unit circle, one can use 2^i antennas, or 3^j antennas, or $2^i 3^j$ antennas, with i and j being arbitrary.)

Given the integer $m \geq 2$ for which an m-PSK code has to be constructed, let ω_m denote $e^{2\pi j/m}$, which is a primitive m-th root of unity. Recall that the m-th cyclotomic field is the field generated by ω_m over $\mathbb{Q}$; $\mathbb{Q}(\omega_m)$ is of degree $\phi(m)$ over $\mathbb{Q}$, where $\phi(m)$ is the Euler totient function of m, that is, $\phi(m)$ is the number of integers i with $1 \leq i \leq m$ that are relatively prime to m. Recall that if $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the prime factorization of m, then $\phi(m) = \phi(p_1^{\alpha_1}) \cdots \phi(p_k^{\alpha_k})$. Furthermore, for any prime p and any exponent α, $\phi(p^\alpha) = p^{\alpha-1}(p-1)$. (All this is standard, see (§4.11, [18]) for instance.)

Our signal set will be the set of all m-th roots of unity, that is, $S = \{\omega_m^i,\ 0 \leq i < m\}$. Now let n be any integer such that the primes that appear in the prime factorization of n is some subset of $\{p_1, \ldots, p_k\}$, which is the set of primes that appear in the factorization of m. We first prove:

Proposition 6. *Let n and m be as above and let l be any integer such that l and m are relatively prime. Then, any of the polynomials $x^n - \omega_m^l$, with ω_m as in the discussion above, is irreducible in $\mathbb{Q}(\omega_m)$.*

Proof. Let $\omega_{mn} = e^{2\pi j/mn}$. This is a primitive mn-th root of unity. The element $\omega_{mn}^l = e^{2\pi jl/mn}$ is a root of $x^n - \omega_m^l$. The minimal polynomial of ω_{mn}^l over $\mathbb{Q}(\omega_m)$ therefore divides $x^n - \omega_m^l$ in $\mathbb{Q}(\omega_m)[x]$. It is therefore sufficient to show that the minimal polynomial of ω_{mn}^l over $\mathbb{Q}(\omega_m)$ is of degree n: this will show that $x^n - \omega_m^l$ must be the minimal polynomial of ω_{mn}^l over $\mathbb{Q}(\omega_m)$, and this will then force $x^n - \omega_m^l$ to be irreducible in $\mathbb{Q}(\omega_m)[x]$.

Note that since the prime factors of n are a subset of the prime factors of m, l is also relatively prime to nm, so ω_{mn}^l is also a primitive nm-th root of unity. Since $(\omega_{mn}^l)^n = \omega_m^l$, we have the natural containment of cyclotomic fields $\mathbb{Q} \subset \mathbb{Q}(\omega_m^l) \subset \mathbb{Q}(\omega_{mn}^l)$. Since ω_m^l is a primitive l-th root of unity, $\mathbb{Q}(\omega_m^l) = \mathbb{Q}(\omega_m)$. Similarly, $\mathbb{Q}(\omega_{mn}^l) = \mathbb{Q}(\omega_{mn})$, so our containment of fields reads $\mathbb{Q} \subset \mathbb{Q}(\omega_m) \subset \mathbb{Q}(\omega_{mn})$. The degree of $\mathbb{Q}(\omega_{mn})$ over $\mathbb{Q}$ is $\phi(mn)$, while the degree of $\mathbb{Q}(\omega_m)$ over $\mathbb{Q}$ is $\phi(m)$, so because degrees multiply in towers of field extensions, we find that the degree of $\mathbb{Q}(\omega_{mn})$ over $\mathbb{Q}(\omega_m)$ is $\phi(mn)/\phi(m)$.

It is therefore sufficient to prove that $\phi(mn) = n\phi(m)$. This will show that the degree of $\mathbb{Q}(\omega_{mn})$ over $\mathbb{Q}(\omega_m)$ is n, and since $\mathbb{Q}(\omega_{mn})$ $(= \mathbb{Q}(\omega_{mn}^l))$ is generated over $\mathbb{Q}(\omega_m)$ by ω_{mn}^l, this will show that the minimal polynomial of ω_{mn}^l over $\mathbb{Q}(\omega_m)$ is of degree n, as desired. We once again invoke the hypothesis that the primes belonging to the factorization of n appear from the set $\{p_1, \ldots, p_k\}$ (the result $\phi(mn) = n\phi(m)$ would be false without this hypothesis). Suppose that $n = p_1^{\beta_1} \cdots p_k^{\beta_k}$ (some of the β_i could possibly be zero). Then $\phi(mn) = \phi(p_1^{\alpha_1+\beta_1} \cdots p_k^{\alpha_k+\beta_k}) = p_1^{\alpha_1+\beta_1-1}(p_1-1) \cdots p_k^{\alpha_k+\beta_k-1}(p_k-1) = p_1^{\beta_1} \cdots p_k^{\beta_k} p_1^{\alpha_1-1}(p_1-1) \cdots p_k^{\alpha_k-1}(p_k-1) = n\phi(m)$, as desired. This proves the proposition. □

Now we construct the code on the signal set $S = \{\omega_m^i,\ 0 \leq i < m\}$ using matrices of the form (2) with the elements of S substituted for the f_i and with $\gamma = \omega_m^l$. This is our m-PSK code for n antennas. We get one such code for each l, $1 \leq l < n$, for which l and n are relatively prime.

Note that under this construction, since multiplication by ω_m^l takes an m-th root of unity to another m-th root of unity, the entries of the matrices transmitted will all be in S, i.e., the code is completely over S.

Moreover, the number of such matrices is $|S|^n$ and hence the rate is 1 symbol per channel use, resulting in rate-optimal codes.

Example 2. *Let us consider the* 4 *element set* $S = \{1, j, -1, -j\}$*. (This set is invariant under multiplication by* j*.) Note that* j *is a primitive* 4*-th root of unity. By Proposition 6 above, the polynomial* $x^2 - j$ *is irreducible over* $\mathbb{Q}(j)$*. We thus get the following set of* 16 2×2 *matrices with entries from* S *for our code:*

$$\begin{bmatrix} 1 & j \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ j & 1 \end{bmatrix} \begin{bmatrix} 1 & -j \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -j & 1 \end{bmatrix} \begin{bmatrix} j & j \\ 1 & j \end{bmatrix} \begin{bmatrix} j & -1 \\ i & j \end{bmatrix} \begin{bmatrix} j & -j \\ -1 & j \end{bmatrix} \begin{bmatrix} j & 1 \\ -j & j \end{bmatrix}$$

$$\begin{bmatrix} -1 & j \\ 1 & -1 \end{bmatrix} \begin{bmatrix} -1 & -1 \\ j & -1 \end{bmatrix} \begin{bmatrix} -1 & -j \\ -1 & -1 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ -j & -1 \end{bmatrix} \begin{bmatrix} -j & j \\ 1 & -j \end{bmatrix} \begin{bmatrix} -j & -1 \\ j & -j \end{bmatrix} \begin{bmatrix} -j & -j \\ -1 & -j \end{bmatrix} \begin{bmatrix} -j & 1 \\ -i & -j \end{bmatrix}$$

The Alamouti code, which is a 2×2 complex orthogonal design of size 2 over S 2 gives a code with identical parameters. In the following two examples we obtain codes with parameters that are not obtainable by orthogonal designs.

Example 3. *Let us consider the* 3*-PSK signal set* $S = \{1, \omega, \bar{\omega} = \omega^2\}$ *where* $\omega = e^{\frac{j2\pi}{3}}$ *is a primitive* 3*-rd root of unity. (This set is invariant under multiplication by* ω*.) By Proposition 6 above, the polynomial* $x^3 - \omega$ *is irreducible over* $\mathbb{Q}(j)$*. We thus get the following set of* 27 2×2 3*-PSK codeword matrices with entries from* S *for our code which is rate-optimal:*

$$\begin{bmatrix} 1 & \omega & \omega \\ 1 & 1 & \omega \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & \bar{\omega} & \omega \\ 1 & 1 & \bar{\omega} \\ \omega & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & \omega \\ 1 & 1 & 1 \\ \bar{\omega} & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & \omega & \bar{\omega} \\ \omega & 1 & \omega \\ 1 & \omega & 1 \end{bmatrix} \begin{bmatrix} 1 & \bar{\omega} & \bar{\omega} \\ \omega & 1 & \bar{\omega} \\ \omega & \omega & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & \bar{\omega} \\ \omega & 1 & 1 \\ \bar{\omega} & \omega & 1 \end{bmatrix} \begin{bmatrix} 1 & \omega & 1 \\ \bar{\omega} & 1 & \omega \\ 1 & \bar{\omega} & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & \bar{\omega} & 1 \\ \bar{\omega} & 1 & \bar{\omega} \\ \omega & \bar{\omega} & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ \bar{\omega} & 1 & 1 \\ \bar{\omega} & \bar{\omega} & 1 \end{bmatrix} \begin{bmatrix} \omega & \omega & \omega \\ 1 & \omega & \omega \\ 1 & 1 & \omega \end{bmatrix} \begin{bmatrix} \omega & \bar{\omega} & \omega \\ 1 & \omega & \bar{\omega} \\ \omega & 1 & \omega \end{bmatrix} \begin{bmatrix} \omega & 1 & \omega \\ 1 & \omega & 1 \\ \bar{\omega} & 1 & \omega \end{bmatrix} \begin{bmatrix} \omega & \omega & \bar{\omega} \\ \omega & \omega & \omega \\ 1 & \omega & \omega \end{bmatrix} \begin{bmatrix} \omega & \bar{\omega} & \bar{\omega} \\ \omega & \omega & \bar{\omega} \\ \omega & \omega & \omega \end{bmatrix}$$

$$\begin{bmatrix} \omega & 1 & \bar{\omega} \\ \omega & \omega & 1 \\ \bar{\omega} & \omega & \omega \end{bmatrix} \begin{bmatrix} \omega & \omega & 1 \\ \bar{\omega} & \omega & \omega \\ 1 & \bar{\omega} & \omega \end{bmatrix} \begin{bmatrix} \omega & \bar{\omega} & 1 \\ \bar{\omega} & \omega & \bar{\omega} \\ \omega & \bar{\omega} & \omega \end{bmatrix} \begin{bmatrix} \omega & 1 & 1 \\ \bar{\omega} & \omega & 1 \\ \bar{\omega} & \bar{\omega} & \omega \end{bmatrix} \begin{bmatrix} \bar{\omega} & \omega & \omega \\ 1 & \bar{\omega} & \omega \\ 1 & 1 & \bar{\omega} \end{bmatrix} \begin{bmatrix} \bar{\omega} & \bar{\omega} & \omega \\ 1 & \bar{\omega} & \bar{\omega} \\ \omega & 1 & \bar{\omega} \end{bmatrix} \begin{bmatrix} \bar{\omega} & 1 & \omega \\ 1 & \bar{\omega} & 1 \\ \bar{\omega} & 1 & \bar{\omega} \end{bmatrix}$$

$$\begin{bmatrix} \bar{\omega} & \omega & \bar{\omega} \\ \omega & \bar{\omega} & \omega \\ 1 & \omega & \bar{\omega} \end{bmatrix} \begin{bmatrix} \bar{\omega} & \bar{\omega} & \bar{\omega} \\ \omega & \bar{\omega} & \bar{\omega} \\ \omega & \omega & \bar{\omega} \end{bmatrix} \begin{bmatrix} \bar{\omega} & 1 & \bar{\omega} \\ \omega & \bar{\omega} & 1 \\ \bar{\omega} & \omega & \bar{\omega} \end{bmatrix} \begin{bmatrix} \bar{\omega} & \omega & 1 \\ \bar{\omega} & \bar{\omega} & \omega \\ 1 & \bar{\omega} & \bar{\omega} \end{bmatrix} \begin{bmatrix} \bar{\omega} & \bar{\omega} & 1 \\ \bar{\omega} & \bar{\omega} & \bar{\omega} \\ \omega & \bar{\omega} & \bar{\omega} \end{bmatrix} \begin{bmatrix} \bar{\omega} & 1 & 1 \\ \bar{\omega} & \bar{\omega} & 1 \\ \bar{\omega} & \bar{\omega} & \bar{\omega} \end{bmatrix}.$$

Example 4. *Let us consider the* 6*-PSK signal set* $S = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$ *where* $\omega = e^{\frac{j2\pi}{6}}$ *is a primitive* 6*-th root of unity. (This set is invariant under multiplication by* ω*.) By Proposition 6 above, the polynomial* $x^2 - \omega$ *and* $x^3 - \omega$ *are irreducible over* $\mathbb{Q}(j)$*. With* $x^2 - \omega$ *we get* 36 2×2 *codewords given by* $\begin{bmatrix} a & \omega b \\ b & a \end{bmatrix}$ *where* $a, b \in S$*, and with* $x^3 - \omega$ *we get* 216 3×3 *codewords given by* $\begin{bmatrix} a & \omega b & \omega c \\ b & a & \omega b \\ c & b & a \end{bmatrix}$ *where* $a, b, c \in S$*.*

4.2 Rate 1 Codes over Signal Sets Derived from m-SPSK Signal Sets for Arbitrary Number of Antennas

The restriction that the primes appearing in the factorization of the number of antennas, n, should be a subset of the primes appearing in the factorization of the size of the signal set, m, that we discussed in Subsection 4.1 above can be removed for signal sets that are union of a symmetric PSK and its scaled version as shown in Fig.2. and for asymmetric PSK signal sets matched to dihedral groups defined below:

Definition 3. *[24] A signal set S is said to be matched to a group G if there exists a mapping $\mu : S \mapsto G$ satisfying*

$$d(\mu(g_1), \mu(g_2)) = d(\mu(e), \mu(g_1^{-1}, g_2)); \forall g_1, g_2 \in G \tag{3}$$

where e is the identity element of G, and $d(x, y)$ denotes the squared Euclidean distance between the signal points x and y.

A dihedral group with $2m$ elements will be denoted by D_m. For different mappings that matches asymmetric $2m$-PSK signal sets to D_m see [28]. Fig.1 shows an asymmetric 8-PSK signal set (filled circles) matched to D_4 the dihedral group with 8 elements, where ϕ is the angle of asymmetry. Note that symmetric m-PSK signal sets are matched to the cyclic group with m elements. Signal sets matched to groups have been studied by several authors and constitute a basic ingredient in the construction of Euclidean space codes [23, 24, 25]. Moreover, codes over signal set matched to dihedral groups have been studied by several authors [26, 27, 28]. It is known that in fading channels asymmetric PSK can perform better than symmetric PSK [29].

The mathematical basis for construction of full-rank STBCs for the signal sets discussed in this section is the following:

Proposition 7. *Let F be a field of characteristic zero, and let z be an indeterminate. Then, for any integer $n \geq 1$, the polynomial $x^n - z$ is irreducible in the ring $F(z)[x]$. (Here, $F(z)$ is the rational function field over F in the indeterminate z, that is, it is the set of quotients of polynomials in z with entries from F.)*

Proof. It is sufficient to prove that $x^n - z$ is irreducible in $F(\omega_n, z)[x]$, where ω_n is a primitive n-th root of unity. (Note that the assumption about the characteristic guarantees the existence of a primitive n-th root of unity.) If we let ζ denote an n-th root of z (in some algebraic closure of $F(\omega_n, z)$), then

$x^n - z$ factors as $\Pi_{i=0}^{n-1}(x - \omega_n^i \zeta)$ over the field $F(\omega_n, z, \zeta) = F(\omega_n, \zeta)$. So, if f is some irreducible factor of $x^n - z$ in $F(\omega_n, z)[x]$, say of degree $k < n$, then over $F(\omega_n, \zeta)$, f must equal the product of some k of these linear factors $(x - \omega_n^i \zeta)$. Studying the constant term of this product, we find that ζ^k is in $F(\omega_n, z)$, or, taking n-th powers, that z^k is an n-th power in $F(\omega_n, z)$. But it is easy to see that when $k < n$, this is impossible: if we were to write $z^k = (g(z)/h(z))^n$, where g and h are polynomials in z with coefficients in $F(\omega_n)$, then, $h(z)^n z^k$ should equal $g(z)^n$. Comparing the highest degree (in z) on both sides gives us the contradiction. Hence, k must equal n, that is, $x^n - z$ must be irreducible in $F(\omega_n, z)[x]$. $\square$

We will use this proposition as follows. Let S be the set of m-th roots of unity, and let us pretend that we are working over the field $\mathbb{Q}(\omega_m, z)$, where z is any transcendental number, for instance, e, or π, or e^{ju}, for any algebraic real number u, even $u = 1$. (The transcendentality of numbers of the form e^{ju}, where u is any algebraic real number, is guaranteed by the Lindemann-Weierstrass theorem, see (§4.12, [18]; see Section 8 below for the statement of this theorem.). Then over that field, the polynomial $x^n - z$ is irreducible, since the transcendental element z acts just as an indeterminate over $\mathbb{Q}(\omega_m)$. (Note a standard fact: if z is transcendental over $\mathbb{Q}$, it remains transcendental over an algebraic extension of $\mathbb{Q}$ such as $\mathbb{Q}(\omega_m)$. This follows from the fact that if z were algebraic over $\mathbb{Q}(\omega_m)$, then $[\mathbb{Q}(\omega_m, z) : \mathbb{Q}(\omega_m)]$ would be finite, so $[\mathbb{Q}(\omega_m, z) : \mathbb{Q}] = [\mathbb{Q}(\omega_m, z) : \mathbb{Q}(\omega_m)][\mathbb{Q}(\omega_m) : \mathbb{Q}]$ would also be finite, contradicting the transcendentality of z over $\mathbb{Q}$.) We may then consider the various $n \times n$ matrices of the form (2), with $\gamma = z$.

Note that there is no limitation under this scheme on n: the number of antennas can therefore be arbitrary. Also note that if we take z to be of the form $e^{ju} = \cos(u) + j\sin(u)$ for some real algebraic number, for example, $u = 1$, then the entries will consist of the original m equally spaced points on the unit circle, and a copy of these points multiplied by e^{ju}, that is, rotated counter clockwise by u radians, which is same as a signal set matched to the dihedral group $D_{|S|}$.

In the following example we construct a code over the signal set matched to D_4 shown in Fig.1.

Example 5. *In Example 2 the codewords are* $\begin{bmatrix} f_0 & \gamma f_1 \\ f_1 & f_0 \end{bmatrix}$ *where* γ *was chosen to be* j *corresponding to the irreducible polynomial* $x^2 - j$ *and* $f_0, f_1 \in S = \{1, -1, j, -j\}$. *Now for some* θ *that is a real algebraic number we can take the irreducible polynomial* $x^3 - e^{j\theta}$, *use the same* S, *and construct code for* 3 *antennas (note that* 3 *is a prime not appearing in the prime power factorization of* 4*). We obtain the following full-rank code over the asymmetric*

8-PSK signal set shown in Fig.1, for 3 *antennas containing the following 64 codewords using Proposition 7:*

$$\begin{bmatrix} 1 & e^{j\theta} & e^{j\theta} \\ 1 & 1 & e^{j\theta} \\ 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & -e^{j\theta} & e^{j\theta} \\ 1 & 1 & -e^{j\theta} \\ -1 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & je^{j\theta} & e^{j\theta} \\ 1 & 1 & je^{j\theta} \\ j & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & -je^{j\theta} & e^{j\theta} \\ 1 & 1 & -je^{j\theta} \\ -j & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & e^{j\theta} & -e^{j\theta} \\ -1 & 1 & e^{j\theta} \\ 1 & -1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -e^{j\theta} & -e^{j\theta} \\ -1 & 1 & -e^{j\theta} \\ -1 & -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & je^{j\theta} & -e^{j\theta} \\ -1 & 1 & je^{j\theta} \\ j & -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & -je^{j\theta} & -e^{j\theta} \\ -1 & 1 & -je^{j\theta} \\ -j & -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & e^{j\theta} & je^{j\theta} \\ j & 1 & e^{j\theta} \\ 1 & j & 1 \end{bmatrix}\begin{bmatrix} 1 & -e^{j\theta} & je^{j\theta} \\ j & 1 & -e^{j\theta} \\ -1 & j & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & je^{j\theta} & je^{j\theta} \\ j & 1 & je^{j\theta} \\ j & j & 1 \end{bmatrix}\begin{bmatrix} 1 & -je^{j\theta} & je^{j\theta} \\ j & 1 & -je^{j\theta} \\ -j & j & 1 \end{bmatrix}\begin{bmatrix} 1 & e^{j\theta} & -je^{j\theta} \\ -j & 1 & e^{j\theta} \\ 1 & -j & 1 \end{bmatrix}\begin{bmatrix} 1 & -e^{j\theta} & -je^{j\theta} \\ -j & 1 & -e^{j\theta} \\ -1 & -j & 1 \end{bmatrix}\begin{bmatrix} 1 & je^{j\theta} & -je^{j\theta} \\ -j & 1 & je^{j\theta} \\ j & -j & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -je^{j\theta} & -je^{j\theta} \\ -j & 1 & -je^{j\theta} \\ -j & -j & 1 \end{bmatrix}\begin{bmatrix} -1 & e^{j\theta} & e^{j\theta} \\ 1 & -1 & e^{j\theta} \\ 1 & 1 & -1 \end{bmatrix}\begin{bmatrix} -1 & -e^{j\theta} & e^{j\theta} \\ 1 & -1 & -e^{j\theta} \\ -1 & 1 & -1 \end{bmatrix}\begin{bmatrix} -1 & je^{j\theta} & e^{j\theta} \\ 1 & -1 & je^{j\theta} \\ j & 1 & -1 \end{bmatrix}\begin{bmatrix} -1 & -je^{j\theta} & e^{j\theta} \\ 1 & -1 & -je^{j\theta} \\ -j & 1 & -1 \end{bmatrix}$$

$$\begin{bmatrix} -1 & 1e^{j\theta} & -e^{j\theta} \\ -1 & -1 & e^{j\theta} \\ 1 & -1 & -1 \end{bmatrix}\begin{bmatrix} -1 & -e^{j\theta} & -e^{j\theta} \\ -1 & -1 & -e^{j\theta} \\ -1 & -1 & -1 \end{bmatrix}\begin{bmatrix} -1 & je^{j\theta} & -e^{j\theta} \\ -1 & -1 & je^{j\theta} \\ j & -1 & -1 \end{bmatrix}\begin{bmatrix} -1 & -je^{j\theta} & -e^{j\theta} \\ -1 & -1 & -je^{j\theta} \\ -j & -1 & -1 \end{bmatrix}\begin{bmatrix} -1 & 1e^{j\theta} & je^{j\theta} \\ j & -1 & e^{j\theta} \\ 1 & j & -1 \end{bmatrix}$$

$$\begin{bmatrix} -1 & -e^{j\theta} & je^{j\theta} \\ j & -1 & -e^{j\theta} \\ -1 & j & -1 \end{bmatrix}\begin{bmatrix} -1 & je^{j\theta} & je^{j\theta} \\ j & -1 & je^{j\theta} \\ j & j & -1 \end{bmatrix}\begin{bmatrix} -1 & -je^{j\theta} & je^{j\theta} \\ j & -1 & -je^{j\theta} \\ -j & j & -1 \end{bmatrix}\begin{bmatrix} -1 & e^{j\theta} & -je^{j\theta} \\ -j & -1 & e^{j\theta} \\ 1 & -j & -1 \end{bmatrix}\begin{bmatrix} -1 & -e^{j\theta} & -je^{j\theta} \\ -j & -1 & -e^{j\theta} \\ -1 & -j & -1 \end{bmatrix}$$

$$\begin{bmatrix} -1 & je^{j\theta} & -je^{j\theta} \\ -j & -1 & je^{j\theta} \\ j & -j & -1 \end{bmatrix}\begin{bmatrix} -1 & -je^{j\theta} & -je^{j\theta} \\ -j & -1 & -je^{j\theta} \\ -j & -j & -1 \end{bmatrix}\begin{bmatrix} j & e^{j\theta} & e^{j\theta} \\ 1 & j & e^{j\theta} \\ 1 & 1 & j \end{bmatrix}\begin{bmatrix} j & -e^{j\theta} & e^{j\theta} \\ 1 & j & -e^{j\theta} \\ -1 & 1 & j \end{bmatrix}\begin{bmatrix} j & je^{j\theta} & 1e^{j\theta} \\ 1 & j & je^{j\theta} \\ j & 1 & j \end{bmatrix}$$

$$\begin{bmatrix} j & -je^{j\theta} & e^{j\theta} \\ 1 & j & -je^{j\theta} \\ -j & 1 & j \end{bmatrix}\begin{bmatrix} j & e^{j\theta} & -e^{j\theta} \\ -1 & j & e^{j\theta} \\ 1 & -1 & j \end{bmatrix}\begin{bmatrix} j & -e^{j\theta} & -e^{j\theta} \\ -1 & j & -e^{j\theta} \\ -1 & -1 & j \end{bmatrix}\begin{bmatrix} j & je^{j\theta} & -e^{j\theta} \\ -1 & j & je^{j\theta} \\ j & -1 & j \end{bmatrix}\begin{bmatrix} j & -je^{j\theta} & -e^{j\theta} \\ -1 & j & -je^{j\theta} \\ -j & -1 & j \end{bmatrix}$$

$$\begin{bmatrix} j & e^{j\theta} & je^{j\theta} \\ j & j & e^{j\theta} \\ 1 & j & j \end{bmatrix}\begin{bmatrix} j & -e^{j\theta} & je^{j\theta} \\ j & j & -e^{j\theta} \\ -1 & j & j \end{bmatrix}\begin{bmatrix} j & je^{j\theta} & je^{j\theta} \\ j & j & je^{j\theta} \\ j & j & j \end{bmatrix}\begin{bmatrix} j & -je^{j\theta} & je^{j\theta} \\ j & j & -je^{j\theta} \\ -j & j & j \end{bmatrix}\begin{bmatrix} j & e^{j\theta} & -je^{j\theta} \\ -j & j & e^{j\theta} \\ 1 & -j & j \end{bmatrix}$$

$$\begin{bmatrix} j & -e^{j\theta} & -je^{j\theta} \\ -j & j & -e^{j\theta} \\ -1 & -j & j \end{bmatrix}\begin{bmatrix} j & je^{j\theta} & -je^{j\theta} \\ -j & j & je^{j\theta} \\ j & -j & j \end{bmatrix}\begin{bmatrix} j & -je^{j\theta} & -je^{j\theta} \\ -j & j & -je^{j\theta} \\ -j & -j & j \end{bmatrix}\begin{bmatrix} -j & e^{j\theta} & e^{j\theta} \\ 1 & -j & 1e^{j\theta} \\ 1 & 1 & -j \end{bmatrix}\begin{bmatrix} -j & -1e^{j\theta} & e^{j\theta} \\ 1 & -j & -e^{j\theta} \\ -1 & 1 & -j \end{bmatrix}$$

$$\begin{bmatrix} -j & je^{j\theta} & e^{j\theta} \\ 1 & -j & je^{j\theta} \\ j & 1 & -j \end{bmatrix}\begin{bmatrix} -j & -je^{j\theta} & e^{j\theta} \\ 1 & -j & -je^{j\theta} \\ -j & 1 & -j \end{bmatrix}\begin{bmatrix} -j & e^{j\theta} & -e^{j\theta} \\ -1 & -j & e^{j\theta} \\ 1 & -1 & -j \end{bmatrix}\begin{bmatrix} -j & -e^{j\theta} & -e^{j\theta} \\ -1 & -j & -e^{j\theta} \\ -1 & -1 & -j \end{bmatrix}\begin{bmatrix} -j & je^{j\theta} & -e^{j\theta} \\ -1 & -j & je^{j\theta} \\ j & -1 & -j \end{bmatrix}$$

$$\begin{bmatrix} -j & -je^{j\theta} & -e^{j\theta} \\ -1 & -j & -je^{j\theta} \\ -j & -1 & -j \end{bmatrix}\begin{bmatrix} -j & e^{j\theta} & je^{j\theta} \\ j & -j & e^{j\theta} \\ 1 & j & -j \end{bmatrix}\begin{bmatrix} -j & -e^{j\theta} & je^{j\theta} \\ j & -j & -e^{j\theta} \\ -1 & j & -j \end{bmatrix}\begin{bmatrix} -j & je^{j\theta} & je^{j\theta} \\ j & -j & je^{j\theta} \\ j & j & -j \end{bmatrix}\begin{bmatrix} -j & -je^{j\theta} & je^{j\theta} \\ j & -j & -je^{j\theta} \\ -j & j & -j \end{bmatrix}$$

$$\begin{bmatrix} -j & e^{j\theta} & -je^{j\theta} \\ -j & -j & e^{j\theta} \\ 1 & -j & -j \end{bmatrix}\begin{bmatrix} -j & -e^{j\theta} & -je^{j\theta} \\ -j & -j & -e^{j\theta} \\ -1 & -j & -j \end{bmatrix}\begin{bmatrix} -j & je^{j\theta} & -je^{j\theta} \\ -j & -j & je^{j\theta} \\ j & -j & -j \end{bmatrix}\begin{bmatrix} -j & -je^{j\theta} & -je^{j\theta} \\ -j & -j & -je^{j\theta} \\ -j & -j & -j \end{bmatrix}$$

These are essentially the matrices $\begin{bmatrix} a & ce^{j\theta} & be^{j\theta} \\ b & a & ce^{j\theta} \\ c & b & a \end{bmatrix}$ *where* $a, b, c \in S$.

On the other hand, when the transcendental element z is real, the entries will be the original m equally spaced points on the unit circle, and these same points shifted *radially* to the circle at radius $|z|$. Fig.2 shows one such signal set. Note too that by choosing different real transcendentals (for example, αe for any nonzero rational number α), we can get different radius for the second circle.

Example 6. *For instance, let us take* $m = 8$, $n = 3$, *and* $z = e^j = \cos(1) + j\sin(1)$. *Since the group of* 8*th roots of unity is generated by* $e^{j2\pi/4}$, *we get the following set of* $8^3 = 512$ *matrices for our code:*

$$\begin{bmatrix} e^{ju_0 2\pi/4} & e^{j(1+u_2 2\pi/4)} & e^{j(1+u_1 2\pi/4)} \\ e^{ju_1 2\pi/4} & e^{ju_0 2\pi/4} & e^{j(1+u_2 2\pi/4)} \\ e^{ju_2 2\pi/4} & e^{ju_1 2\pi/4} & e^{ju_0 2\pi/4} \end{bmatrix}$$

where u_0, u_1, and u_2 are arbitrary integers in the range $0 \leq u_i \leq 7$. On the other hand, if we took $m = 8$ and $n = 3$, but $z = e$, we get the following matrices instead for our code:

$$\begin{bmatrix} e^{ju_0 2\pi/4} & e^{1+ju_2 2\pi/4} & e^{1+ju_1 2\pi/4} \\ e^{ju_1 2\pi/4} & e^{ju_0 2\pi/4} & e^{1+ju_2 2\pi/4} \\ e^{ju_2 2\pi/4} & e^{ju_1 2\pi/4} & e^{ju_0 2\pi/4} \end{bmatrix}$$

4.3 Rate-optimal Codes over Rotationally Invariant Signal Sets

If we take our set S to consist of points in $\mathbb{Q}(j)$ (not all on the real axis), then $\mathbb{Q}(S)$ will just be $\mathbb{Q}(j)$, and the polynomial $x^n - j$ will be irreducible over this field for any n that is a power of 2, by Proposition 6. Thus, we can construct codes over finite subsets S of $\mathbb{Q}(j)$, using matrices of the form (2) with $\gamma = j$, and with the elements f_i chosen from S. As special cases of this, we can choose our points to come from finite subsets of the standard integer lattice $\{a + jb|\ a, b \in \mathbb{Z}\}$, and furthermore, we can even choose our subset to be invariant under multiplication by j, that is, invariant under rotation by 90°. We get codes over several well-known signal sets consisting of square and rectangular arrays in this manner: for example, codes on QAM signal sets, and codes on cross-constellations.

Example 7. *Let $a \geq b > 2$ be odd integers, and let S consist of the union of the two sets $S_1 = \{(a - 2k) + j(b - 2l)|0 \leq k \leq a,\ 0 \leq l \leq b\}$ and $S_2 = jS_1 = \{-(b - 2l) + j(a - 2k)|0 \leq k \leq a,\ 0 \leq l \leq 2b\}$. Fig.3 shows such a signal set for $m = n = 5$ and Fig.4 for $m = 7$ and $n = 3$. Note that both S_1 and S_2 are invariant under multiplication by -1. When $n = m$, S_1 is already invariant under multiplication by j, so $S_1 = S_2$, and we have a square constellation. When $m > n$, S is the union of one rectangle and another copy of this rectangle rotated by 90°, and the union $S_1 \cup S_2$ is then invariant under multiplication by j. This is a* cross constellation. *In both cases, can create our codes from this signal set S for any n a power of 2 by taking matrices of the form (2) with $\gamma = j$, and with the elements f_i chosen from S. Of course, we can construct our codes on just the set S_1 using this same procedure. The entries of the matrices will then come from $S_1 \cup S_2$.*

Instead of codes from signal sets invariant under rotation by 90°, we can choose sets that are invariant under rotation by other angles $2\pi/k$, that is, invariant under multiplication by $\omega_k = e^{2\pi/k}$. One would start from a set that is a subset of $\mathbb{Q}(\omega_k)$ and then construct codes for n antennas using the extension given by the n-th root of ω_k. (Of course, n has to satisfy the condition that the prime factorization of n should only involve primes that appear in the prime factorization of k.) For instance, when $k = 3$ (so our angle of rotation is 120°), we can let S_1 be any finite set of nonzero complex numbers contained in the cyclotomic extension $\mathbb{Q}(\omega_3)$, and let $S = S_1 \cup \omega_3 S_1 \cup \omega_3^2 S_1$. Then S is invariant under multiplication by ω_3, and we can construct a code on S for n transmit antennas, where n is any power of 3, using matrices of the form (2) with $\gamma = \omega_3$.

As a specific example, let us take $S = \{1, \omega_3, \omega_3^2, -1, -\omega_3, -\omega_3^2, \omega_3 - \omega_3^2, -1+\omega_3^2, 1-\omega_3\}$, which is shown in Fig.5. Note that $S = \omega_3 S = \omega_3^2 S$, so S is already invariant under rotation by 120°. We can use this set to construct codes for transmission on $n = 3^l$ antennas for arbitrary l as described above.

4.4 Codes From Other Minimal Polynomials

All our examples in the previous three subsections have arisen from application of Proposition 3, where the minimal polynomial of the element α was of the form $x^n - \gamma$. For the sake of completeness, we will give an example in this section of a code constructed by applying Proposition 2, that is, where the minimal polynomial has other terms besides the constant term and the highest degree term. Of course, the entries of the matrices involved, in this general situation, will be linear combinations of the elements of the signal set.

First, a well-known result that will help us construct irreducible polynomials over fields other than the rationals:

Lemma 8. *Let $f(x)$ be an irreducible polynomial over $\mathbb{Q}$ of degree n. Suppose that F is an extension field of $\mathbb{Q}$ of degree m, and suppose that n and m are relatively prime. Then, $f(x)$ remains irreducible over F.*

Proof. This is standard. If α is a root of $f(x)$, then $\mathbb{Q}(\alpha)$ is an extension of $\mathbb{Q}$ of degree n. The field $F(\alpha)$ contains $\mathbb{Q}(\alpha)$, so $[F(\alpha) : \mathbb{Q}]$ is divisible by $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. Similarly, $F(\alpha)$ contains F, so $[F(\alpha) : \mathbb{Q}]$ is divisible by $[F : \mathbb{Q}] = m$. Since n and m are relatively prime, $F[(\alpha) : \mathbb{Q}]$ is divisible by nm, and hence, $F[(\alpha) : F] = [F(\alpha) : \mathbb{Q}]/[F : \mathbb{Q}]$ is divisible by $nm/m = n$. On the other hand, the minimal polynomial of α over F divides $f(x)$, so the degree of this minimal polynomial is at most n. It follows that $F[(\alpha) : F]$ is exactly n, and that $f(x)$ is the minimal polynomial of α over F, and in particular, that $f(x)$ remains irreducible over F. □

We now give a class of codes constructed from minimal polynomials that are one step more complicated than those of the form $x^n - \gamma$: Let $f(x)$ be of the form $x^n - px - p$, for some prime p. By Eisenstein's Criterion (§2.16,

[18]), $f(x)$ is irreducible over the rationals. Let m be any integer such that $\phi(m)$ and n are relatively prime. Let ω_m be a primitive m-th root of unity, and consider $\mathbb{Q}(\omega_m)$, the m-th cyclotomic field. This is of degree $\phi(m)$ over the rationals, so, by the lemma above and the assumption about n and $\phi(m)$, $f(x)$ remains irreducible over $\mathbb{Q}(\omega_m)$. Hence, if M is the matrix (1) (with $a_0 = a_1 = p$, and $a_2 = \cdots = a_{n-1} = 0$), then, for S equal to the m-th roots of unity, the set of all matrices of the form $s_0 + s_1 M + s_2 M^2 + \cdots + s_{n-1} M^{n-1}$, where the s_i are allowed to be arbitrary members of S, is an rate-optimal code of size m^n.

Example 8. *Consider $f(x) = x^3 - 2x - 2$. This is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion. Let us work over $\mathbb{Q}(j)$, a field extension of $\mathbb{Q}$ of degree 2 (note that 2 and 3 are relatively prime). Then, since*

$$M = \begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 2 \\ 0 & 1 & 0 \end{bmatrix}$$

and

$$M^2 = \begin{bmatrix} 0 & 2 & 0 \\ 0 & 2 & 2 \\ 1 & 0 & 2 \end{bmatrix}$$

our code consists of all 3×3 matrices of the form

$$\begin{bmatrix} s_0 & 2s_2 & 2s_1 \\ s_1 & s_0 + 2s_2 & 2s_1 + 2s_2 \\ s_2 & s_1 & s_0 + 2s_2 \end{bmatrix}$$

where the s_i are arbitrary members of the set $\{1, j, -1, -j\}$. Of course, the same set of matrices above also forms a code if the s_i are allowed to come from the set of 2^r-th roots of unity, for any $r \geq 2$, since the 2^r-th cyclotomic field has degree 2^{r-1}, which is relatively prime to 3.

5 STBCs from non-commutative division algebras

In this section we begin the STBC construction using embeddings of non-commutative division algebras in matrix rings. First we present the basic structural properties of division algebras in the following subsection. Then we discuss the left regular representation of division algebras which is the counterpart of Section 3 for the case of field extensions.

5.1 Division Algebras: An Introduction

Given a division algebra D, its *center* $Z(D)$ is the set $\{x \in D | xd = dx \forall d \in D\}$. It is easy to see that $Z(D)$ is a field; D therefore has a natural structure as a $Z(D)$ vector space. In this paper, we will only consider division algebras that are finite dimensional as a vector space over their center. (Such algebras are referred to as *finite dimensional division algebras*.) Good references for division algebras are [31], [32], and [34].

If F is any field, by an F *division algebra*, or a *division algebra over* F, we will mean a division algebra D whose center is precisely F. It is well known that the dimension $[D : F]$ is always a perfect square. If $[D : F] = n^2$, the square root of the dimension, n, is known as the *degree* or the *index* of the division algebra. It Example 1 the center of the quaternions is just the set $\{a(= a \cdot 1) + 0\hat{\imath} + 0\hat{\jmath} + 0\hat{k}\}$, that is, under the identification described above, the center of $\mathbb{H}$ is just $\mathbb{R}$. Notice that $\mathbb{H}$ is four $(= 2^2)$ dimensional over its center $\mathbb{R}$, that is, $\mathbb{H}$ is of degree (or "index") 2.

By a *subfield* of a division algebra, we will mean a field K, such that $F \subseteq K \subseteq D$. Note that D can have other subfields K such that $F \not\subseteq K$, but we will not consider such subfields. If K is a subfield of D, then K is a subspace of the F-vector space D, and $[K : F]$ divides $[D : F] = n^2$. It is known that the maximum possible value of $[K : F]$ is n; such a subfield is called a *maximal subfield* of D. It is known that maximal subfields exist in profusion. (Further, it is known that there exist maximal subfields that are separable over F; of course, in characteristic zero, this is automatic.)

While non-commutative division algebras exist in profusion, they are not always easy to construct. Given a field F, it is relatively easy to construct close cousins of division algebras: the *F-central simple algebras*. An F-central simple algebra is simply a ring A whose center (defined analogously as the set of all $x \in A$ such that $xy = yx$ for all $y \in A$) is precisely F, and which has no nontrivial two-sided ideals, i.e., other than $\{0\}$ and A. Thus, the key distinction between an F-central simple algebra and an F division algebra is that in a division algebra, we further require that every nonzero element be invertible. (An example of an F-central simple algebra is $M_n(F)$: this ring has no nontrivial two-sided ideals, and there are nonzero matrices that are not invertible—the ones whose determinant is zero). It is indeed quite easy to write down several examples of F-central simple algebras, but determining if any one such example has the further property that every nonzero element is invertible can be extremely difficult. Several arithmetic techniques need to be brought to bear on this problem (such as class field theory when F is an algebraic number field, and non-commutative valuation theory when F is a general valued field), and the calculations can be quite subtle and involved. Nevertheless, division algebras are very interesting mathematical objects, so, to explore their use in the construction of space time codes, we will outline one special technique (Proposition 10 ahead) for constructing division algebras that works in a wide variety of situations. We will also explore a family of division algebras first introduced by Brauer, in Section 8 ahead.

But first, we will define one easy embedding of division algebras into matrices in the following subsection:

5.2 Codes From The Left Regular Representation of Division Algebras

The material in this section parallels the material in Section 3. Given an F division algebra D of degree n, D is naturally an F-vector space of dimension n^2. We thus have a map $L\colon D \to End_F(D)$, where $End_F(D)$ is the set of F linear transforms of the vector space D. This map is given by left multiplication: it takes any $d \in D$ to λ_d, where λ_d is *left* multiplication by d, that is, $\lambda_d(e) = de$ for all $e \in D$. It is easy to check that λ_d is indeed an F-linear transform of D, that is, $\lambda_d(f_1e_1 + f_2e_2) = f_1\lambda_d(e_1) + f_2\lambda_d(e_2)$. (Notice that it is crucial that F be the center of D, otherwise, the map λ_d will not be F linear, that is, $\lambda_d(fe)$ will not equal $f\lambda_d(e)$!) One also checks that L is a ring homomorphism from D to $End_F(D)$, that is, $\lambda_{d_1+d_2} = \lambda_{d_1} + \lambda_{d_2}$, $\lambda_{d_1d_2} = \lambda_{d_1}\lambda_{d_2}$, and $\lambda_1 = 1$. Since D has no two sided ideals, L is an injection, and on choosing a basis for D as an F vector space, we will get an embedding of D in $M_{n^2}(F)$. Notice that the size of the matrices involved is n^2 and not n. (An analogous game can be played with right multiplication maps ρ_d, but there we would have $\rho_{d_1d_2} = \rho_{d_2}\rho_{d_1}$, and thus we would have a ring *anti-homomorphism* from D to $End_F(D)$. We will not pursue this further here.)

Exactly as in the field case in Section 3, we write down the matrix corresponding to λ_d with respect to a given basis $\mathcal{B} = \{u_1, u_2, \ldots, u_{n^2}\}$ as follows: For any given basis element u_i $(1 \le i \le n^2)$, and for any j $(1 \le j \le n^2)$, let $u_iu_j = \sum_{l=1}^{n^2} c_{ij,l}u_l$. Then, the j-th column of λ_{u_i} is simply the coefficients $c_{ij,l}$ above, $1 \le l \le n^2$. (Here, we use the convention that the vectors on which a matrix acts are written on the right of the matrix as a column vector, so the j-th column of the matrix just represents the image of the j-th standard basis vector under the action of the matrix.) Once the matrix corresponding to each λ_{u_i}, call it M_i, is obtained in this manner, the matrix corresponding to a general λ_d, with $d = \sum_{i=1}^{n^2} f_iu_i$ is just the linear combination $\sum_{i=1}^{n^2} f_iM_i$.

Example 9. *Let us consider the left regular representation of* $\mathbb{H}$ *with respect to the basis* $\{1, \hat{\imath}, \hat{\jmath}, \hat{k}\}$. *The defining relations* $\hat{\imath}^2 = \hat{\jmath}^2 = -1$, $\hat{\imath}\hat{\jmath} = \hat{k} = -\hat{\imath}\hat{\jmath}$, *etc. show that for* $x = a + b\hat{\imath} + c\hat{\jmath} + d\hat{k}$, *the matrix corresponding to* λ_x *is* $\begin{bmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{bmatrix}$ *which is precisely the (transpose of) the 4 dimensional orthogonal real design of the paper [6, §III-A] of Tarokh, et. al.*

In the sections ahead, we will construct other division algebras besides the quaternions, and we can apply the left regular representation to these algebras to get codes of size m^{n^2}, where m is the size of the signal set, and n is the index of the division algebra. One such concrete example is given in Example (13) ahead. In what follows, however, we will construct another embedding of division algebras of index n that yields matrices of size n instead of n^2.

6 Cyclic Division Algebras

We describe in this section a fundamental class of division algebras, the class of cyclic division algebras. All our examples of codes will be constructed from cyclic division algebras (although, our machinery for constructing codes can certainly be extended, with appropriate modifications, for other division algebras as well).

A *cyclic division algebra* D over the field F is a division algebra that has a maximal subfield K that is Galois over F, with $Gal(K/F)$ being cyclic.

Example 10. *Hamilton's quaternions* $\mathbb{H}$ *is a cyclic division algebra! For, notice that the subset* $\{a + 0\hat{\imath} + c\hat{\jmath} + 0\hat{k} \mid a, b \in \mathbb{R}\}$ *is isomorphic to the complex numbers* $\mathbb{C}$. *Let us identify the complex numbers with this subset and write (by abuse of notation)* $\mathbb{C}$ *for this subset. Notice that* $\mathbb{C}$ *is of dimension* 2 *over the center* $\mathbb{R}$, *that is,* $\mathbb{C}$ *is a maximal subfield of* $\mathbb{H}$. *Now notice that* $\mathbb{C}/\mathbb{R}$ *is indeed a Galois extension, whose Galois group is* $\{1, \sigma\}$, *where* σ *stands for complex conjugation. This is of course a cyclic group! Thus,* $\mathbb{H}$ *is a cyclic division algebra.*

Now, given a cyclic division algebra D with center F, of index n, and with maximal cyclic subfield K/F, let $Gal(K/F)$ be generated by σ. Then $\sigma^n = 1$, of course. D is naturally a *right* vector space over K, with the product of the (scalar) $k \in K$ on the vector $d \in D$ defined to be dk. (Note the definition: the action of scalars is defined via multiplication on the right—if one were to define the action of scalars via multiplication from the left, one would get a different K vector space structure on D.) It is well known that we have the following decomposition of D as right K spaces:

$$D = K \oplus zK \oplus z^2K \oplus \cdots \oplus z^{n-1}K, \tag{4}$$

where z is some element of D that satisfies the relations

$$kz \quad = z\sigma(k)\ \forall k \in K \tag{5}$$
$$z^n \ = \delta, \quad \text{for some} \quad \delta \in F^* \tag{6}$$

where F^* is the set F excluding the zero element and z^iK stands for the set of all elements of the form z^ik for $k \in K$. (Note that the element δ above is actually in F, the center.)

Equations (4) and (5) above provide a very convenient handle into the division algebra: all the non-commutativity is concentrated just in the way in which the element z interacts with elements of K: pulling z from the right of $k \in K$ to the left just induces σ on k. Also, the field generated by the element z over F is of a particularly nice kind: it is given by just adjoining an n-th root of the element δ. It is the existence of such a decomposition that makes cyclic division algebras a very manageable class of division algebras.

The division algebra D, with its decomposition above, is often written as $(K/F, \sigma, \delta)$.

Example 11. *One sees easily that in the case of $\mathbb{H}$, one can regroup the $\mathbb{R}$ space decomposition $\mathbb{H} = \{a + b\hat{\imath} + c\hat{\jmath} + d\hat{k} \mid a, b, c, d \in \mathbb{R}\}$ as $\mathbb{H} = \mathbb{C} \oplus i\mathbb{C}$, where, as in Example 10, we have identified $\mathbb{C}$ with the subset $\{a+0\hat{\imath}+c\hat{\jmath}+0\hat{k}\}$ of $\mathbb{H}$. This gives the decomposition of $\mathbb{H}$ as a right $\mathbb{C}$ vector space, with the element $\hat{\imath}$ playing the role of "z" above. Moreover, since $\hat{\imath}^2 = -1$, the element δ above is -1 in this example.*

6.1 Embedding Cyclic Division Algebras Into Matrices Over the Maximal Cyclic Subfield

Let D be a cyclic division algebra over F of index n, with maximal cyclic subfield K. As we have seen above, D is a right K space, of dimension n (each summand z^iK in Equation (4) above is a one-dimensional K space, and there are n such). To emphasize the right K structure, let us write D_K for D viewed

[1] We wish to mention in passing here perhaps the most sought after open question in the theory of division algebras today: Is every division algebra of index a prime p ($p \geq 5$) necessarily cyclic?

as a right K vector space. Now note that D acts on D_K by multiplication on the *left* as follows: given $d \in D$, it sends an arbitrary $e \in D_K$ to de. Since this action is from the left, while the scalar action of K on D_K is from the right, these two actions commute. That is, $d(ek) = (de)k$, something that is, of course obvious, but crucial. Let us write λ_d for the map from D_K to D_K that sends $e \in D$ to de. Then, the fact that the action of λ_d and that of the scalars commute means that λ_d is a K-linear transform of D_K. In other words, we have a map $f\colon D \to End_K(D_K)$ that sends d to λ_d. One checks that this is a ring homomorphism, that is $\lambda_{d_1+d_2} = \lambda_{d_1} + \lambda_{d_2}$, and $\lambda_{d_1 d_2} = \lambda_{d_1}\lambda_{d_2}$. (For this second relation, note that $\lambda_{d_1 d_2}(e) = (d_1 d_2)e = d_1(d_2 e) = \lambda_{d_1}(\lambda_{d_2}(e))$.)

We thus have an embedding of D into $End_K(D_K)$, which, once one chooses a K basis for D_K, translates into the embedding of D into $M_n(K)$ that is needed for Proposition 1. A natural basis, of course, is given by the decomposition in Equation (4) above: we choose the basis $\{1, z, z^2, \ldots, z^{n-1}\}$. A typical element $d = k_0 + zk_1 + \ldots + z^{n-1}k_{n-1}$ sends 1 to $d = k_0 + zk_1 + \ldots z^{n-1}k_{n-1}$, so the first column of the matrix corresponding to λ_d in this basis reads k_0, k_1, …, k_{n-1}. For the second column, note that $dz = (k_0 + zk_1 + \ldots z^{n-1}k_{n-1})z = k_0 z + zk_1 z + \ldots z^{n-1}k_{n-1}z = z\sigma(k_0) + z^2\sigma(k_1) + \ldots z^{n-1}\sigma(k_{n-2}) + \delta\sigma(k_{n-1})$, where we've used the relations in Equation (5) to pull z from the right to the left. So, the second column reads $\delta\sigma(k_{n-1}), \sigma(k_0), \sigma(k_1), \ldots, \sigma(k_{n-2})$. Similarly, $dz^2 = (k_0 + zk_1 + \ldots z^{n-1}k_{n-1})z^2 = z^2\sigma^2(k_0) + z^3\sigma^2(k_1) + \cdots \delta\sigma^2(k_{n-2}) + z\delta\sigma^2(k_{n-1})$. Proceeding thus, we find that the matrix corresponding to λ_d is the following:

$$\begin{bmatrix} k_0 & \delta\sigma(k_{n-1}) & \delta\sigma^2(k_{n-2}) & \ldots & \delta\sigma^{n-2}(k_2 & \delta\sigma^{n-1}(k_1) \\ k_1 & \sigma(k_0) & \delta\sigma^2(k_{n-1}) & \ldots & \delta\sigma^{n-2}(k_3) & \delta\sigma^{n-1}(k_2) \\ k_2 & \sigma(k_1) & \sigma^2(k_0) & \ldots & \delta\sigma^{n-2}(k_4) & \delta\sigma^{n-1}(k_3) \\ k_3 & \sigma(k_2) & \sigma^2(k_1) & \ldots & \delta\sigma^{n-2}(k_5) & \delta\sigma^{n-1}(k_4) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ k_{n-1} & \sigma(k_{n-2}) & \sigma^2(k_{n-3}) & \ldots & \sigma^{n-2}(k_1) & \sigma^{n-1}(k_0) \end{bmatrix} \quad (7)$$

Notice that K does not embed as scalar matrices under this map, since, for any $k \in K$, λ_k represents multiplication by k on the left, whereas, the scalar matrix with k on the diagonal represents multiplication by k on the right. In fact, λ_k is the matrix with k, $\sigma(k)$, …, $\sigma^{n-1}(k)$ along the diagonal. Also, notice that the matrices (7) above are very similar to the matrices (2); the difference is in the twist by powers of the automorphism σ.

We thus have the following corollary to Proposition 1:

Corollary 9. *Let F be a subfield of the complex numbers, and let D be a cyclic division algebra over F of index n. Let K be a maximal cyclic subfield of D. Let δ be defined by the cyclic decomposition given in Equations (4)* *and (5). Then, any finite subset E of matrices of the form (7) above, with the k_i coming from K, will have the property that the difference of any two elements in E will be of full-rank.*

6.2 Alamouti's Codes

Let us go back to the examples of the quaternions: we saw above in Example 10 that $\mathbb{H}$ is cyclic: the subfield $\mathbb{C}$ (under the identification described in that example) is a cyclic extension of $\mathbb{R}$, with Galois group generated by complex conjugation. Let us write k^* for the complex conjugate of $k \in \mathbb{C}$. In Example 11, we saw that we have the decomposition $\mathbb{H} = \mathbb{C} \oplus i\mathbb{C}$, as a right $\mathbb{C}$ space, with the role of the element "z" of the discussion above played by the quaternion $\hat{\imath}$. We also saw that since $\hat{\imath}^2 = -1$, the element δ of the discussion above is just -1. Thus, by Corollary 9 above, any finite set of matrices of the form
$\begin{bmatrix} k_0 & -k_1^* \\ k_1 & k_0^* \end{bmatrix}$ is a full rank minimum delay code. But these are precisely Alamouti's matrices!

Alamouti's construction has a certain uniqueness from the point of view of division algebras. (Of course, in [6], the authors have also studied the uniqueness of these codes from the point of view of orthogonal designs.) One has the following: Hamilton's quaternions $\mathbb{H}$ is the only (non-commutative) division algebra which has $\mathbb{C}$ as a maximal subfield. This arises from two well known facts: first, the only subfield F (up to a suitable isomorphism) of $\mathbb{C}$ such that $[\mathbb{C} : F]$ is finite is the $\mathbb{R}$ (a theorem of Artin and Schreier, see [19, Theorem 11.14], and second, the only non-commutative (and associative) division algebra over the $\mathbb{R}$ is the quaternions (a theorem of Frobenius, see [34, Chapter 13, Corollary C] for instance). Thus, the only possible set of matrices of the form (7) in which the k_i are allowed to be arbitrary complex numbers that forms a division algebra is the one corresponding to the quaternions: matrices of the form (6.2) where $n = 2$, $\delta = -1$ and σ given by complex conjugation.

Remark 4. Notice that the only $2x2$ real orthogonal design is a special case of Alamouti code where the entries take values from the subfield ($\mathbb{R}$) of the complex field $\mathbb{C}$.

Note that we will come up with several examples below where we will embed suitable division algebras D into $M_n(\mathbb{C})$ for various values of n other than $n = 2$ and thus obtain space time codes for more than 2 transmit antennas. The key distinction is that these division algebras will not have $\mathbb{C}$ as a maximal subfield, and therefore, the entries of the corresponding matrices will not be allowed to take on arbitrary complex values (in contrast with Alamouti's example).

7 A Principle for Constructing Cyclic Division Algebras Using n-th Roots of Transcendental Elements

To apply the general machinery of Corollary 9 above for constructing space time codes, we need to generate concrete division algebras over suitable subfields of $\mathbb{C}$. A natural candidate for this is the following technique: Let us take a known cyclic Galois extension K/F, whose Galois group is generated by some σ. Suppose that $[K : F] = n$, so that $\sigma^n = 1$. Let us pick a nonzero element $\delta \in F^*$, and let us construct abstractly the algebra

$$(K/F, \sigma, \delta) = K \oplus zK + \oplus z^2 K + \cdots + \oplus z^{n-1} K,$$

where z is some symbol that satisfies the two relations given in Equation 5, namely, $kz = z\sigma(k)$ for all $k \in K$, and $z^n = \delta$. It would be tempting to assume that this technique would automatically give us a division algebra, but unfortunately, this is not true. What is known is that we get an algebra whose center is F, and which is *simple,* that is, it has no nontrivial two sided ideals. Not every nonzero element in this algebra need be invertible, however. Fortunately, we have the following *sufficient* criterion to help us ([34, Chapter 15, Corollary d], or [19, Theorem 8.14]):

Proposition 10. *In the construction above,*

$$A = (K/F, \sigma, \delta)$$

is a division algebra if the smallest positive integer t such that δ^t is the norm of some element in K^* is n. (The norm of an element $k \in K^*$ is the product $k\sigma(k)\sigma^2(k)\ldots\sigma^{n-1}(k)$; this is clearly invariant under σ and is hence in F. Note that for any $a \in F^*$, the norm of a is just a^n, and hence, δ^n is the norm of δ. Thus, n is an upper bound for the integer t of the proposition above, and the content of the proposition is that if t is the maximum it can be, then A is definitely a division algebra.)

Remark 5. It is worth pointing out that this is by no means a necessary condition.

We can use Proposition 10 to construct cyclic division algebras very easily over fields of the form $F(\delta)$, where F is a suitable algebraic number field (for instance, when F is a finite extension of $\mathbb{Q}$), and where δ is some transcendental number, for example, e, or π, or $e^{ju} = \cos(u) + j\sin(u)$ for any real algebraic number u. (The fact that e^{ju} is transcendental for any real algebraic number u follows from the Lindemann-Weierstrass Theorem ([18, pp. 277, Vol. 1]); see Section 8 below for the statement of this theorem.) Suppose that F has a cyclic extension K of degree n, whose Galois group is generated by some σ. We have the following:

Proposition 11. *With F, K, n, z, and σ as above, the algebra*

$$(K(\delta)/(F(\delta), \sigma, \delta)$$

is a division algebra.

(Here, δ remains transcendental over K as K is also algebraic over $\mathbb{Q}$. Hence, in the field $K(\delta)$, δ simply behaves as an indeterminate. We extend the action of σ on K to the field $K(\delta)$ by defining $\sigma(\delta) = 1$. Thus, σ acts on any quotient of polynomials in δ by acting only on the coefficients and leaving all powers of δ fixed. We continue to use σ for this extended action on $K(\delta)$.)

Proof. Suppose that δ^t is the norm from K to F of some f/g, where f and g are polynomials in δ with coefficients in K. We rewrite this as

$$\delta^t N_{K/F}(g) = N_{K/F}(f),$$

where we have written $N_{K/F}$ for the norm of an element from K to F. It is clear from the action of σ on $K(\delta)$ that the degree of $\sigma(f)$ is the same as the degree of f (as polynomials in δ). Since $N_{K/F}(f) = f\sigma(f)\cdots\sigma^{n-1}(f)$, it follows that the degrees of $N_{K/F}(f)$ and $N_{K/F}(g)$ are multiples of n, so t must also be a multiple of n. The smallest possible positive t is therefore n (and as discussed before, δ^n is already a norm, so the smallest positive t is exactly n). It follows from Proposition 10 that $(K(\delta)/(F(\delta), \sigma, \delta)$ is a division algebra. $\square$

Corollary 12. *Continuing with the notation of Proposition 11, any finite subset E of matrices of the form (7) above, with the k_i coming from K, will have the property that the difference of any two matrices in E will be of full rank.*

Proof. This follows from Corollary 9. $\square$

In the following subsection we will construct STBCs over certain SPSK signal sets by way of illustration of Proposition 11.

7.1 Rate-1 STBCs over SPSK signal sets

Let $m = p^\alpha$, where p is an *odd* prime, and let $n = p^\beta$, for any $\alpha > 0$ and $\beta > 0$. Let ω_m be a primitive m-th root of unity, and let $F = \mathbb{Q}(\omega_m)$. As we saw in Proposition (6) above, the polynomial $x^n - \omega_m$ is irreducible in $F[x]$. If ω_{mn} is a primitive mn-th root of unity which is a root of this polynomial, then $K = \mathbb{Q}(\omega_{mn})$ is of degree n over F. Moreover, K/F is actually a cyclic Galois extension. This follows from two well know facts: The Galois group of $\mathbb{Q}(\omega_k)/\mathbb{Q}$, where ω_k is a primitive k-th root of unity for some k, is isomorphic to the group of units of the ring $\mathbb{Z}/k\mathbb{Z}$, and when k is a power of an odd prime (in our case, $p^{\alpha+\beta}$), the group of units of $\mathbb{Z}/k\mathbb{Z}$ is a cyclic group. Hence, the Galois group of K/F, which is a subgroup of the Galois group of $K/\mathbb{Q}$, is also cyclic.

We may use this field extension K/F to construct our codes: for instance, our signal set could be the set of mn-th roots of unity, which would be mn equally spaced points on the circle. For the Galois action on K, note that we have an isomorphism between the group of units of the ring $\mathbb{Z}/mn\mathbb{Z}$ and $Gal(K/\mathbb{Q})$ given as follows: one fixes a generator $[l]$ of the group of units of the ring $\mathbb{Z}/mn\mathbb{Z}$ $(0 < l < n)$, and one considers the map that sends ω_{mn} to ω_{mn}^l. One shows that this map is indeed in the Galois group of $K/\mathbb{Q}$, and in fact, generates the group. Now, since the group $\mathbb{Z}/mn\mathbb{Z}^*$ is cyclic, we find that the Galois group of K/F is the unique cyclic subgroup of this group of order n, and this is generated by $[l]^{\phi(nm)/n} = [l]^{\phi(m)}$. (Note that because m and n are both powers of the same prime, $\phi(nm) = n\phi(m)$.) Hence, once we fix a generator $[l]$ of $\mathbb{Z}/mn\mathbb{Z}^*$, our map σ is the one that sends ω_{mn} to $\omega_{mn}^{l^{\phi(m)}} = \omega_{mn}^{l^{p^{\alpha-1}(p-1)}}$.

When $n \leq m$ (so that ω_n is already contained in F) the map σ is a little easier to describe. It is easy to see that $1+m$ has order exactly n in $\mathbb{Z}/mn\mathbb{Z}^*$ (one observes using the binomial theorem and the fact that $n = p^\beta \leq m = p^\alpha$ that $(1+m)^t = 1 + tm$ in $\mathbb{Z}/mn\mathbb{Z}$). Hence, our map σ is the one that sends ω_{mn} to $\omega_{mn}^{1+m} = \omega_n \omega_{mn}$.

Example 12. *Suppose that* $m = 3^2 = 9$, *and* $n = 3$. *Then,* $mn = 27$, *so our signal set will consist of* 27 *equally spaced points as shown in Fig.6 by the points marked by* $a_0, a_1, \cdots, a_{26}$. *Take* $\omega_9 == e^{2\pi j/9}$, *a primitive* 9-*th root of unity. The number* $e^{2\pi j/27}$ *is a primitive* 27*th root of unity, and satisfies* $(e^{2\pi j/27})^3 = e^{2\pi j/9}$. *We may take* $e^{2\pi j/27}$ *to be our* ω_{27}. *Note that* $(e^{2\pi j/27})^9 = e^{2\pi j/3}$, *a primitive* 3*rd root of unity. Our map* σ *therefore sends* ω_{27} *to* $\omega_{27}^{1+9} = e^{2\pi j/3}\omega_{27} = e^{20\pi j/27}$, *and in general,* ω_{27}^k *to* $e^{20k\pi j/27}$. *So, the set of* 3×3 *matrices*

$$\begin{pmatrix} \omega_{27}^{k} & \delta\cdot\sigma(\omega_{27})^{m} & \delta\cdot\sigma^{2}(\omega_{27})^{l} \\ \omega_{27}^{l} & \sigma(\omega_{27})^{k} & \delta\cdot\sigma^{2}(\omega_{27})^{m} \\ \omega_{27}^{m} & \sigma(\omega_{27})^{l} & \sigma^{2}(\omega_{27})^{k} \end{pmatrix}$$

where δ is any transcendental number, where k, l, and m can be any of $\{0,1,2,\ldots,26\}$, and where the action of σ on these roots of unity is as described, (shown in Fig.6 by points $b_0, b_1, \cdots, b_{26}$) forms a full rank minimum delay space time code.

Suppose instead we'd taken $m = 3^2$ but had taken $n = 3^3$. Since $n > m$, we would compute the Galois action a little differently. We'd first find a generator for the group of units of $\mathbb{Z}/3^5\mathbb{Z}$, a group of order $2\cdot 3^4$. Since the possible orders of our elements are 2, 3, 6, 9, 18, 27, 54, 81, and 162, we only need to find an element $[x]$ in $\mathbb{Z}/3^5\mathbb{Z}$ such that $[x^k]$ is not $[1]$ for any k in this list except for $k = 162$. One checks that $[2]$ is such an element, so $[2]$ is a generator of the group of units of $\mathbb{Z}/3^5\mathbb{Z}$. Hence, our map σ is the one that sends ω_{243} to $\omega_{243}^{2^{\phi(m)}} = \omega_{243}^{2^6} = e^{128\pi j/243}$, and in general, ω_{243}^{k} to $e^{128k\pi j/243}$.

Example 13. *As noted in Subsection 5.2 earlier, we will use the material of this section to construct a code using the left regular representation instead of the representation on maximal subfields. In fact, we will work out the left regular representation of the division algebra in Example 12 above where $m = 3^2 = 9$, and $n = 3$. This is the cyclic division algebra $(\mathbb{Q}(\omega_{27})/\mathbb{Q}(\omega_9), \sigma, \delta)$, where ω_{27}, ω_9 and δ are as defined in that example. The center of this algebra is $\mathbb{Q}(\omega_9)$. A $\mathbb{Q}(\omega_9)$ basis for this algebra is the set $\{1, \omega_{27}, \omega_{27}^2, z, z\omega_{27}, z\omega_{27}^2, z^2, z^2\omega_{27}, z^2\omega_{27}^2\}$, where z is the usual element that appears in the cyclic decomposition of the algebra and satisfies the relations Equation 5. One checks, given all the relations in this algebra, and given that $\sigma(\omega_{27}) = \omega_3\omega_{27}$ (where $\omega_3 = e^{2\pi j/3}$), that the representation of the element $a_0 + a_1\omega_{27} + a_2\omega_{27}^2 + a_3 + a_4 z\omega_{27} + a_5 z\omega_{27}^2 + a_6 z^2 + a_7 z^2\omega_{27} + a_8 z^2\omega_{27}^2$ is given by the following 9×9 matrix:*

$$\begin{pmatrix} a_0 & \omega_9 a_2 & \omega_9 a_1 & \delta a_6 & \delta\omega_3^2\omega_9 a_8 & \delta\omega_3\omega_9 a_7 & \delta a_3 & \delta\omega_3\omega_9 a_5 & \delta\omega_3^2\omega_9 a_4 \\ a_1 & a_0 & \omega_9 a_2 & \delta\omega_3 a_7 & \delta a_6 & \delta\omega_3^2\omega_9 a_8 & \delta\omega_3^2 a_4 & \delta a_3 & \delta\omega_3\omega_9 a_5 \\ a_2 & a_1 & a_0 & \delta\omega_3^2 a_8 & \delta\omega_3 a_7 & \delta a_6 & \delta\omega_3 a_5 & \delta\omega_3^2 a_4 & \delta a_3 \\ a_3 & \omega_9 a_5 & \omega_9 a_4 & a_0 & \omega_3^2\omega_9 a_2 & \omega_3\omega_9 a_1 & \delta a_6 & \delta\omega_3\omega_9 a_8 & \delta\omega_3^2\omega_9 a_7 \\ a_4 & a_3 & \omega_9 a_5 & \omega_3 a_1 & a_0 & \omega_3^2\omega_9 a_2 & \delta\omega_3^2 a_7 & \delta a_6 & \delta\omega_3\omega_9 a_8 \\ a_5 & a_4 & a_3 & \omega_3^2 a_2 & \omega_3 a_1 & a_0 & \delta\omega_3 a_8 & \delta\omega_3^2 a_7 & \delta a_6 \\ a_6 & \omega_9 a_8 & \omega_9 a_7 & a_3 & \omega_3^2\omega_9 a_5 & \omega_3\omega_9 a_4 & a_0 & \omega_3\omega_9 a_2 & \omega_3^2\omega_9 a_1 \\ a_7 & a_6 & \omega_9 a_8 & \omega_3 a_4 & a_3 & \omega_3^2\omega_9 a_5 & \omega_3^2 a_1 & a_0 & \omega_3\omega_9 a_2 \\ a_8 & a_7 & a_6 & \omega_3^2 a_5 & \omega_3 a_4 & a_3 & \omega_3 a_2 & \omega_3^2 a_1 & a_0 \end{pmatrix}$$

Here, the entries a_0, a_1, …, a_8 can be arbitrary elements of the field $\mathbb{Q}$ adjoined with $e^{2\pi j/9}$. (In particular, we may take them to come from just the nine ninth roots of unity $e^{2\pi kj/9}$, $k = 0, \ldots, 8$.) The element δ can be any transcendental, such as e or π, or e^{ju}, where u is any algebraic real number.

8 Brauer's Division Algebras

We present here a different class of examples; this is a construction due to Brauer ([30], see also [33, §2.8]). Let l and n be any two integers such that l and n have *exactly* the same prime factors, and such that l divides n (so the exponent of every prime factor of l is not more than the exponent of the same prime factor of n). Let ω_l be a primitive l-th root of unity, and let k be the field $\mathbb{Q}(\omega_l)$. Let x_1, …, x_n be indeterminates, and consider the rational function field $K = k(x_1, \ldots, x_n)$, which is the set of all quotients of polynomials in the variables x_1, …, x_n with coefficients from k. Let σ be the automorphism of this field that takes x_1 to x_2, x_2 to x_3, …, x_{n-1} to x_n, and x_n to x_1, and that acts as the identity on k. (Thus, σ takes a polynomial $f(x_1, x_2, \ldots, x_n)$ to the polynomial $f(x_2, x_3, \ldots, x_1)$.) Let F be the fixed field of σ (so $[K : F] = n$). As in the beginning of Section 7, we may abstractly construct the algebra $(K/F, \sigma, \omega_l) = K \oplus zK + \oplus z^2K + \cdots + \oplus z^{n-1}K$, where z is some symbol that satisfies the two relations given in Equation 5, namely $zk = \sigma(k)z$ and $z^n = \omega_l$. In general, we are only guaranteed that we will get a simple algebra, but Brauer ([30], [33, §2.8]) proved the following:

Theorem 13. *With notation as above, the algebra $(K/F, \sigma, \omega_l)$ is a division algebra. It is of index n, and is clearly cyclic.*

8.1 STBCs using Brauer's division algebras

We can use Theorem 13to construct STBCs as follows. Let n and l be as above, and let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be algebraically independent transcendental numbers. (We will address the issue of finding such numbers momentarily). Let m be given. Assume that $m \geq n$. Take as the signal set these n transcendental numbers α_1, …, α_n, along with as many powers α_i^j ($i = 1, \ldots, n$, $j = 2, 3, \ldots$) as necessary to get a signal set of size exactly m. View the signal set as elements of the field $k(\alpha_1, \ldots, \alpha_n)$, where k, as above, is $\mathbb{Q}(\omega_l)$. Note that because the α_i are chosen to be algebraically independent transcendental elements, the α_i just act as indeterminates over k. The automorphism σ then sends α_1 to α_2, α_2 to α_3, and so on, and α_n to α_1. (Similarly, σ sends α_1^j to α_2^j, and so on.) Embedding the cyclic division algebra $(K/F, \sigma, \omega_l)$ into $M_n(k(\alpha_1, \ldots, \alpha_n))$ as in Section 6.1, we find that the set of matrices of the form (7), with the k_i coming from the signal set, with $\delta = \omega_l$ and with σ acting on the α_i (and their powers) as above, is a full rank rate-optimal space time block code, with m^n elements. The entries of the matrices will either be elements of the signal set or will be elements of the signal set multiplied by ω_l.

If $m < n$, then we may take our signal set to be any subset of $\alpha_1, \ldots, \alpha_n$ of cardinality m. The same procedure as above will give us a full rank rate-optimal space time block code of size m^n. The entries of the matrices will not be restricted to the signal set, but will either be elements from the larger set $\alpha_1, \ldots, \alpha_n$, or will be one of these elements multiplied by ω_l.

We now address the issue of finding n algebraically independent transcendental numbers. For this, we have the following (see [18, pp 277, Vol 1]):

Theorem 14. *(Lindemann-Weierstrass) If $u_1, u_2, \ldots, u_n$ are algebraic numbers that are linearly independent over $\mathbb{Q}$, then the complex exponentials e^{u_1}, $e^{u_2}, \ldots, e^{u_n}$ are algebraically independent over the field of algebraic numbers.*

We can use this theorem as follows to get a signal set, all of whose elements are on the unit circle: Pick $u_1, \ldots, u_n$ to be *real* algebraic numbers that are linearly independent over $\mathbb{Q}$ (for example, $1, \sqrt{2}, \sqrt{3}, \ldots$). Then $ju_1, \cdots ju_n$ will also be linearly independent over $\mathbb{Q}$. Hence, we may take $\alpha_1 = e^{ju_1}$, $\alpha_2 = e^{ju_2}, \ldots, \alpha_n = e^{ju_n}$ to be our algebraically independent transcendental elements, all of which are on the unit circle.

Note that since the only requirement on the u_i is that they be linearly independent over $\mathbb{Q}$, we can choose the u_i so that the points e^{ju_i} can be essentially in any region of the unit circle.

Example 14. *Suppose we wish to construct a code for 2 antennas, with a signal set of size 2^k for some $k \geq 1$. We take $n = 2$, and then the only choice for l is also 2, and ω_l is -1. We take $u_1 = 1$ and $u_2 = \sqrt{2}$, so $\alpha_1 = e^j$ and $\alpha_2 = e^{j\sqrt{2}}$. We take our signal set to be the set $S = \{\alpha_1^j \| \ j = 1, \ldots, 2^{k-1}\} \cup \{\alpha_2^j \| \ j = 1, \ldots, 2^{k-1}\}$. Then S has 2^k elements, and since $\sigma(\alpha_1^j) = \alpha_2^j$ and $\sigma(\alpha_2^j) = \alpha_1^j$, we find that our code consists of all possible matrices of the following four forms, with s and t each ranging from 1 to 2^{k-1}.*

$$\begin{bmatrix} e^{js} & -e^{jt} \\ e^{j\sqrt{2}t} & e^{j\sqrt{2}s} \end{bmatrix}, \begin{bmatrix} e^{j\sqrt{2}s} & -e^{j\sqrt{2}t} \\ e^{jt} & e^{js} \end{bmatrix}, \begin{bmatrix} e^{js} & -e^{j\sqrt{2}t} \\ e^{jt} & e^{j\sqrt{2}s} \end{bmatrix}, \begin{bmatrix} e^{j\sqrt{2}s} & -e^{jt} \\ e^{j\sqrt{2}t} & e^{js} \end{bmatrix}$$

Note that the total number of matrices above is indeed $(2^k)^2$. Note, too, that this code is quite different from Alamouti's code.

Example 15. *Using these same ideas, let us construct a code for three antennas, using a signal set of six elements. We take* $\alpha_1 = e^j$, $\alpha_2 = e^{j\sqrt{2}}$, *and* $\alpha_3 = e^{j\sqrt{3}}$, *and we take our signal set to be* α_1, α_1^2, α_2, α_2^2, α_3, *and* α_3^2. *We take* l *to be* 3, *that is, the "*ω_l*" in the example is the primitive third root of unity* $\omega_3 = e^{2\pi j/3}$. *Thus, our code will consist of all* $6^3 = 216$ *matrices of the form*

$$\begin{pmatrix} \alpha_p^k & \omega_3 \cdot \sigma(\alpha_r)^m & \omega_3 \cdot \sigma^2(\alpha_q)^l \\ \alpha_q^l & \sigma(\alpha_p)^k & \omega_3 \cdot \sigma^2(\alpha_r)^m \\ \alpha_r^m & \sigma(\alpha_q)^l & \sigma^2(\alpha_p)^k \end{pmatrix}$$

where k, l, *and* m *can be any of* $\{1, 2\}$, *where* p, q, *and* r *can be any of* $\{1, 2, 3\}$, *and where* $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_3$, *and* $\sigma(\alpha_3) = \alpha_1$ *(and so* $\sigma^2(\alpha_1) = \alpha_3$, *etc.).*

9 Relation to Linear Dispersion Codes and Orthogonal Designs

In this section we highlight the relationship of the codes obtained in this paper using division algebras with Linear Dispersion codes of [17] and Orthogonal Designs of [6].

9.1 Special case of Linear Dispersion codes

A Linear Dispersion code consists of $n \times l$ matrices of the form

$$C = \sum_{q=1}^{Q} s_q A_q + s_q^* B_q \tag{8}$$

where s_q belongs to a signal set S and A_q, B_q where $q = 1, 2, \cdots, Q$ are $2Q$ number of $n \times l$ complex matrices that define the code. In [17] these matrices are chosen to optimize an information theoretic criterion and not the rank of the code. Observe that the codeword matrices consist of entries that are complex linear combinations of signal points and their conjugates.

The codes of this paper can easily be seen to constitute a special case of Linear Dispersion codes where $n = l = Q$, all the matrices $B_q, q = 1, 2, \cdots, Q$ are zero matrices and $A_q = M^q, q = 1, 2, \cdots, n$ where M is given by equation (1). Hence, the efficient suboptimal decoding algorithms mentioned in [17] for the general class of Linear Dispersion codes can be used to decode the codes of this paper.

9.2 Relationship with Orthogonal Designs

Orthogonal Designs for real constellations exist only for $n = 2, 4, 8$ and for complex complex constellations exist only for $n = 2$ which is the Alamouti code [6]. The Example 9 shows that the real orthogonal design with $n = 4$ is obtainable from left regular representation of the Quaternion algebra. In Subsection 6.2 it was shown that the only complex orthogonal design can be obtained from representation over maximal cyclic subfield of the Quaternion algebra. The real orthogonal design with $n = 2$ is nothing but the Alamouti code with the variables taking values only from the real field. What about the real orthogonal design with $n = 8$?

It can be shown that the 8×8 real orthogonal design of [6, §III-A] is the one that arises from the left regular representation of the Octonion algebra (see [18, §7.6] for instance for the definition of this algebra). This is an 8 dimension algebra over the reals that is *not* associative; every nonzero element however possesses a multiplicative inverse. We have not covered this design in our discussion since we deal with only associative division algebras in this paper.

10 Scope for further work

The construction of full-rank codes using the both commutative and non-commutative division algebras have been studied. Some of the possible directions for further research are:

- It is shown in [17] that the codes obtained by Orthogonal designs generally fall short of achieving capacity (except the Alamouti code for 2 transmit and 1 receive antenna) and it will be interesting to see capacity that the codes presented in this paper achieve.
- Though we have constructed the full-rank codes for various signal sets and a large number of antennas it is not clear what will be coding gain that these codes offer.
- Do some of the codes constructed admit simpler decoding?
- In the first half of the paper where we construct codes using field extensions we have studied primarily cyclotomic field extensions. Code constructions using non-cyclotomic field extensions may yield some interesting codes.

- The construction of STBCs using non-commutative division algebras has yielded all Orthogonal designs as special cases except the real orthogonal design with $n = 8$. However, it is not at all clear what does "twisting" by σ in equation (7) buy? This aspect is worth investigating further.

References

[1] E.Teletar, "Capacity of multi-antenna Gaussian channels," AT&T Bell Labs., Tech. Report, June 1995 and European Transactions on Telecommunications, Vol.10, pp.585-595, Nov. 1999.

[2] G.J.Foschini and M.Gans, "On the limits of wireless communication in a fading environment when using multiple antennas," Wireless Personal Communication, March 1998.

[3] 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.

[4] Vahid Tarokh, Nambi Seshadri and A.R.Calderbank, "Space-time codes for high data rate wireless communication: Performance Criterion and Code Construction," *IEEE Transactions on Information Theory,* Vol. 44 No. 2, pp. 744–765 March 1998.

[5] S. M. Alamouti, "A simple transmit diversity technique for wireless communication," IEEE J. on Selected Areas in Communications, Vol.16, No.8, pp.1451-1458, Oct. 1998.

[6] Vahid Tarokh, H.Jafarkhani and A.R.Calderbank, "Space-Time block codes from orthogonal designs," *IEEE Transactions on Information Theory,* Vol.45, pp.1456-1467, July 1999.

[7] A. Roger Hammons and Hesham El Gamal, "On the Theory of Space-Time Codes for PSK Modulation," *IEEE Transactions on Information Theory,* Vol.46, No.2, pp.524-542, March 2000.

[8] Y.Liu, M.P.Fitz and O.Y.Takeshita, "A Rank Criterion for QAM Space-Time Codes," Private communication.

[9] B.Hassibi, B.M.Hochwald, A.Shokrollahi and W.Sweldens, "Representation Theory for High-Rate Multiple-Antenna Code Design," *IEEE Transactions on Information Theory,* Vol.47, No.6, pp.2335-2367, 2001.

[10] B.Hasssibi and M.Khorrami, "Fully-Diverse Multiple-Antenna Signal Constellations and Fixed-Point-Free Lie Groups," Mathematical Science Research Center, Bell Labs., Lucent Technologies, Download available from *http://mars.bell-labs.com.*

[11] A. Shokrollahi, Design of Unitary Space-Time Codes from Representations of SU(2)," Mathematical Science Research Center, Bell LAbs., Lucent Technologies, Download available from *http://mars.bell-labs.com.*

[12] B.Hughes, "Optimal Space-Time constellations from groups," submitted to IEEE Transactions on Information Theory.

[13] B.Hochwald, T.Marzetta, T.Richardson, W.Sweldens and R.Urbanke, "Systematic Design of unitary space-time constellations," IEEE Transactions on Information Theory, Vol.46, 2000, pp.1692-1973.

[14] B.M.Hochwald and T.L.Marzetta, " Unitary space-time modulation for multiple antenna communication in Rayleigh flat-fading," IEEE Transactions on Information Theory, Vol.46, 2000, pp.543-564.

[15] T.M.Marzetta, B.Hassibi and B.M.Hochwald, "Structured Unitary Space-Time Auto-coding Constellations," Mathematical Science Research Center, Bell LAbs., Lucent Technologies, Download available from *http://mars.bell-labs.com.*

[16] B.M.Hochwald and M.Sweldens, "Differential Unitary Space-Time modulation," Mathematical Science Research Center, Bell LAbs., Lucent Technologies, Download available from *http://mars.bell-labs.com.*

[17] B. Hassibi and B. Hochwald, "High-rate codes that are linear in space and time," submitted to IEEE Transactions on Information Theory. Download available from *http://mars.bell-labs.com.*

[18] N. Jacobson, "Basic Algebra I," Second Edition, W.H. Freeman and Company, New York, 1985.

[19] N. Jacobson, Basic Algebra II, Second Edition, W.H. Freeman and Company, New York, 1985.

[20] G. Ganesan and P. Stoica,"Space-time diversity using orthogonal and amicable orthogonal designs," *in Proc. of IEEE VTC'2000*, pp. 2561-2564.

[21] G. Ganesan and P. Stoica,"Space-time diversity," *Signal Processing Advances in Wireless and Mobile Communications*,Vol. 1, ch. 2, pp. 59-87, Prentice Hall PTR, 2001.

[22] H. Jafarkhani,"A Quasi-Orthogonal Space-Time Block Code," *ÌEEE Transactions on Communications* Vol.49, No.1, pp.1-4, Jan 2001.

[23] G.D.Forney, Jr., "Geometrically uniform codes," IEEE Trans. Inform. Theory, Vol.37, pp.1241-1260, 1991.

[24] H.A.Loeliger, "Signal sets matched to groups," IEEE Trans. Inform. Theory, Vol.37, pp.1675-1682, 1991.

[25] H.A.Loeliger, "On Euclidean Space Group Codes," Ph.D. dissertation, Swiss Federal Inst. Technol., Zurich, Switzerland, 1992.

[26] D.Divsalar, M.K.Simon and J.H.Yuen, "Trellis coding with asymmetric modulations," IEEE Trans. Communications, Vol. COM-35, pp.130-141, 1987.

[27] R.Garello and S.Benedetto, "Multilevel construction of block and trellis group codes," IEEE Trans. Inform. Theory, Vol.41, pp.1257-1264, 1995.

[28] Jyoti Bali and B.Sundar Rajan, "Block-Coded PSK modulation using two-level group codes over dihedral groups," IEEE Trans. Inform. Theory, Vol.44, pp.1620-1631, 1998.

[29] L.Venkata Subramaniam, B.Sundar Rajan and R.Bahl, "Performance of 4- and 8-State TCM Schemes with Asymmetric 8-PSK in Fading Channels," IEEE Trans. Vehicular Technology, Vol.49, pp.211-219, Jan. 2000.

[30] Richard Brauer, Über den index und den exponenten von divisionalgebren, Tohuku Math. J., **37** 1933, 77–87.

[31] P.K. Draxl, Skew Fields, Cambridge University Press, 1983.

[32] I.N. Herstein, Non-commutative Rings, Carus Mathematical Monographs, Math. Assocn. of America, 1968.

[33] N. Jacobson, Finite-Dimensional Division Algebras over Fields, Springer-Verlag, New York, 1996.

[34] Richard S. Pierce, Associative Algebras, Springer-Verlag, Grad Texts in Math number 88, 1982.

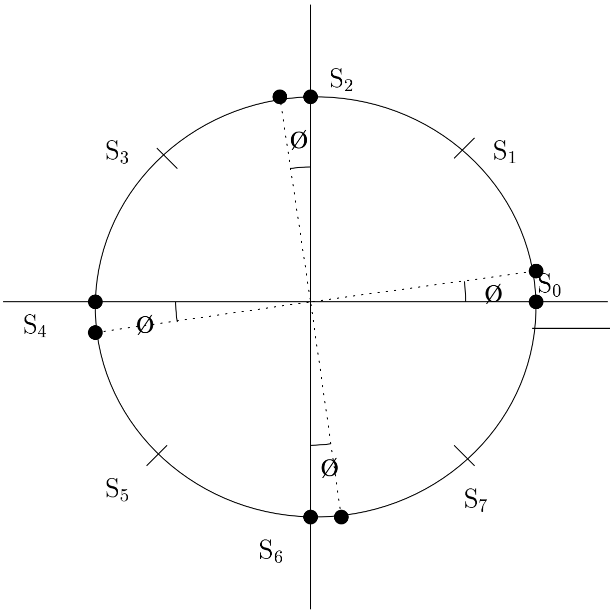

Figure 1: Asymmetric 8-PSK signal set matched to a dihedral group with 8 elements

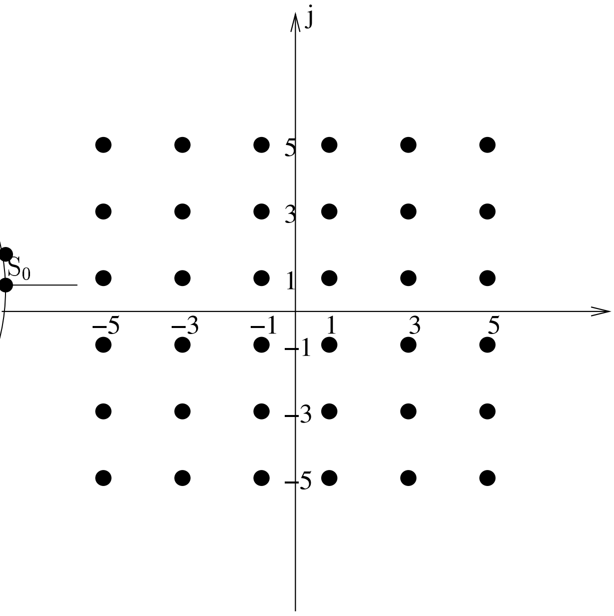

Figure 3: The square constellation with $a = b = 5$ in Example 7

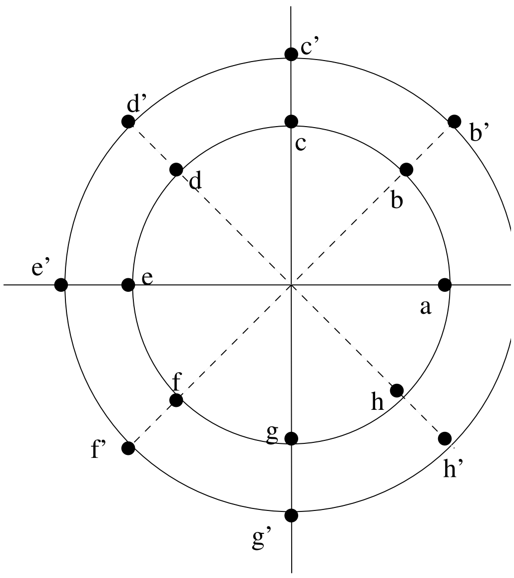

Figure 2: The symmetric 8-PSK signal set with radially shifted points included

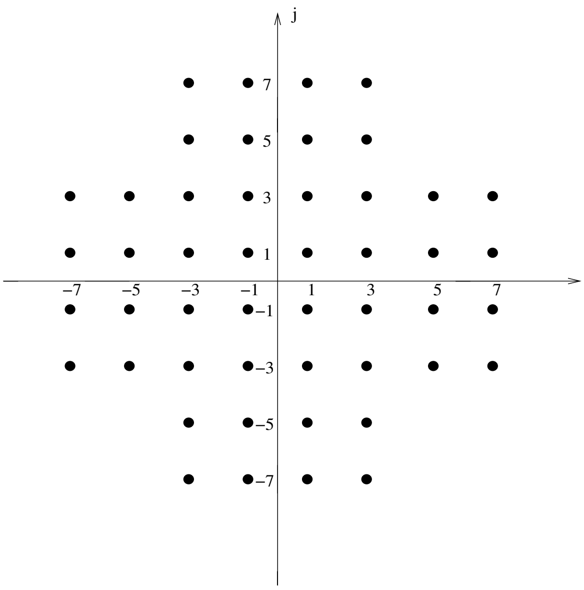

Figure 4: The cross constellation with $a = 7, b = 5$ in Example 7

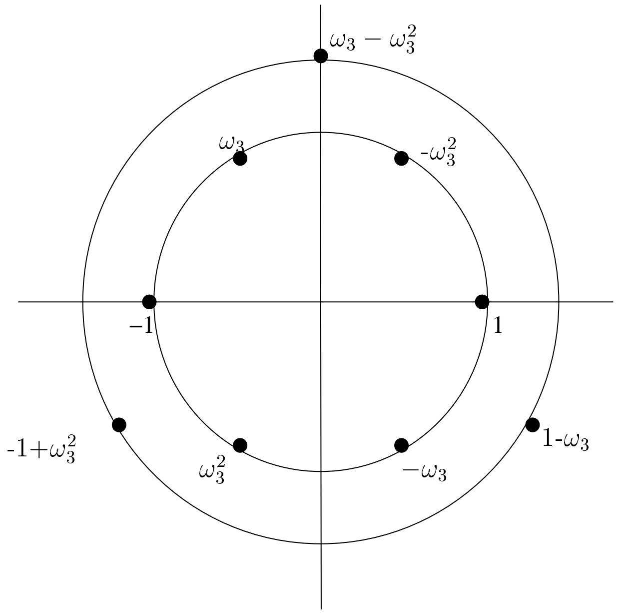

Figure 5: Double-PSK constellation

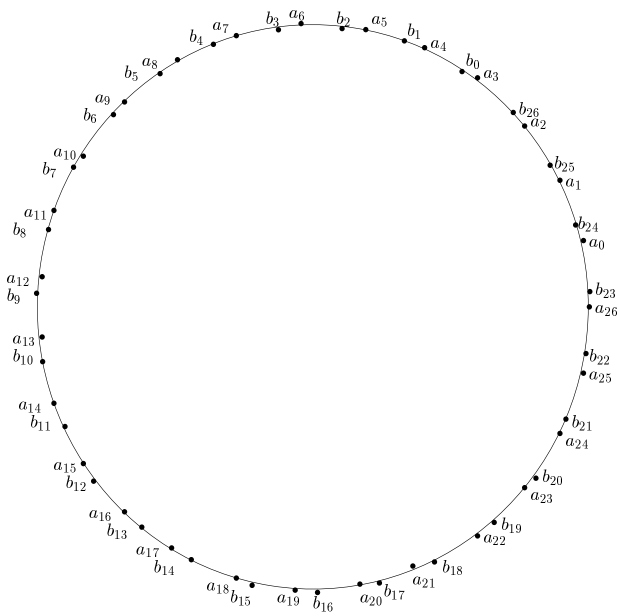

Figure 6: The PSK constellation for Example 12