FULL-DIVERSITY, HIGH-RATE SPACE-TIME BLOCK CODES FROM DIVISION ALGEBRAS

B.A.Sethuraman, B.Sundar Rajan, Senior Member, IEEE, V.Shashidhar

Abstract: We present some general techniques for constructing full-rank, minimal-delay, rate at least one Space-Time Block Codes (STBCs) over a variety of signal sets for arbitrary number of transmit antennas 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 with cyclotomic field extensions, we construct several families of STBCs over a wide range of signal sets that are of full-rank, minimal-delay and rate at least one appropriate for any number of transmit antennas. We study the coding gain and capacity of these codes. Using transcendental extensions we construct arbitrary rate codes that are full-rank for arbitrary number of antennas. Also we present a method of constructing STBCs using non-cyclotomic field extensions. 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. The 4×4 real orthogonal design is obtained by the left regular representation of Quaternions. The Alamouti's code is just a special case of the construction using representation over maximal cyclic subfields and we observe certain algebraic uniqueness characteristics of it. Also, we discuss a general principle for constructing cyclic division algebras using the n-th root of a transcendental element and study the capacity of the STBCs obtained from this construction. Another family of cyclic division algebras discovered by Brauer is discussed and several examples of STBCs derived from each of these constructions are presented.

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

[2] B.S.Rajan and V.Shashidhar are with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore- 560 012, India, emails:bsrajan@ece.iisc.ernet.in, Shashidhar@protocol.ece.iisc.ernet.in.

[3] This work was partly supported by a generous grant from K.B.Chandrashekhar Family Foundation to B.A.Sethuraman and by the IISc-DRDO Program on Advanced Research in Mathematical Engineering to B.S.Rajan.

[4] The material in this paper was presented in part at International Conference on Communications, New York, April 2002, IEEE International Symposium on Information Theory, Lausanne, June 2002, IEEE Information Theory Workshop, Bangalore, India, Oct.2002, IEEE GLOBECOM, Taipei, Nov. 2002, IEEE International Symposium on Information Theory, Yokohama, Japan June/July 2003 and to be presented in IEEE GLOBECOM, San Francisco, Dec. 2003.

1 Introduction and Preliminaries

It is well known that multiple-antenna wireless communication promises very high data rates, especially when the channel is known at the receiver [1–3]. The design criterion for such systems were developed in [4] and in [5] a constructive approach to design Space-Time Trellis Codes (STTC) suitable for such systems was given. Another major class of codes for multiple antenna systems is 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 the entries of all the codeword matrices of a STBC $\mathcal{C}$ are complex linear combinations of the elements of a signal set S, 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 $\left[\begin{array}{cc} x_0 & x_1 \\ -x_1^* & x_0^* \end{array}\right]$ 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 [5]. 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. Notice that when the codeword matrices are allowed to have entries which are complex linear combinations of elements of S, as in [6], then the rate of a full-rank, minimal-delay code can be more than 1 symbol per channel use.

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 these codes need not be of largest coding gain among such codes.

STBCs have been studied by several authors: STBCs that admit a simple decoding for arbitrary complex constellations have been studied using the theory of orthogonal designs in [7, 8]. A similar treatment of STBCs using orthogonal designs, based on optimal SNR, was also carried out by Ganesan and Stoica in [9, 10]. STBCs specific to PSK and QAM modulation have been studied in [11] and [12] respectively. Design of STBCs using groups and representation theory of groups have been reported in [13–16] and using unitary matrices STBCs have been studied in [17–20]. Hassibi and Hochwald [6] 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, linear complexity decoding algorithms like 'successive nulling and canceling', 'square-root' and 'sphere decoding' can be used [6, 21, 22]. A scheme that trades diversity for simpler ML decoding (double-symbol decoding) is presented in [23] for four and eight antennas and with certain restrictions on the signal constellation that the variables take values from it has been shown by several authors [24–29] that rate and/or diversity can be improved from those of [23]. In [30], Damen *et al.* constructed Diagonal Algebraic STBCs (DAST) which have rate one symbol per channel use and full rank if the signal set is a subset of integer lattice. These codes were extended to give rates upto n symbols per channel use, where n is the number of transmit antennas in [31], using the concept of layering. In [32], a space-time code for 2 transmit antennas was constructed which maximizes the mutual information for any number of receive antennas. However, it is not full rank for singal sets other than QAM constellations. Galliou *et al.* in [33] have used Galois theory to construct full-rate, fully diverse STBCs over QAM signals and claim to maximize the mutual information.

In this paper, we present some general techniques for constructing rate-optimal as well as rate greater than 1 (in some cases arbitrary rate), full-rank, minimal-delay STBCs over a variety of signal sets (all finite subsets of certain subfields of $\mathbb{C}$) for arbitrary number of antennas 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. The minimal-delay STBCs obtained earlier in [8] by orthogonal designs are single-symbol 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 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. The classes of codes reported in [34] are proper subclass of those obtained in the first half of this paper. 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 an algebraic uniqueness property of Alamouti's code. A difference between our approach and the approach of Tarokh et.al. using orthogonal designs [8], is that these authors come up with codes that will work with any signal set that is an arbitrary 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 rate and the number of antennas. Moreover, while we do not have simple decoding algorithms for our codes, all the codes we obtain in this paper constitute subclasses of Linear Dispersion codes [6], and hence the decoding algorithms that apply to Linear Dispersion codes will also apply to the codes of this paper. In Section 9 we show that high rate STBCs obtained in this paper perform better than LD codes at high SNRs.

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 also discussed. A general technique for constructing STBCs from field extensions is presented in Section 3, for various rates and signal sets. We discuss the coding gain and capacity of the resulting STBCs in Section 4. 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 and show 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 and also study their mutual information. In Section 8 we describe Brauer's division algebras and outline some explicit STBCs obtained from such algebras. Section 9 briefly describes the decoding aspects of these codes and presents simulation results. Several directions for further research and concluding remarks constitute Section 10.

2 The Main Principle

In this section we first present the basic principle used to construct STBCs throughout the paper and in the Subsection 2.1 describe the embedding of field extensions into matrices. All rings in this paper will be associative, and will possess a unit element 1. Recall that a division algebra 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 [35]. 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. Basic results concerning the structure of division algebras are given in Section 5.

The following proposition gives a very broad principle that is used to construct full-rank minimal-delay codes from division algebras in this paper:

Proposition 1. *Let $f: D \to M_n(F)$ 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.*

Proof. 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, i.e., $f(D)$ 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, and our subset E must therefore have the property that the difference of any two elements in E 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 2.1 and Section 3) 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.

2.1 Embedding Field Extensions into Matrices

We will recall some well-known facts (see (§7.3, [35]) 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 left multiplication by k.) As in the discussions in the previous section 2, L maps K isomorphically into $End_F(K)$, that is, K embeds in $M_n(F)$. 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 $(1 \leq i \leq n)$, and for any j $(1 \leq j \leq n)$, let $u_i u_j = \sum_{l=1}^{n} c_{ij,l} u_l$. Then, the j-th column of λ_{u_i} is simply the coefficients $c_{ij,l}$ above, $1 \leq l \leq n$. 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. 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), 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 the matrix corresponding to λ_α is simply its companion matrix M given by

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

and the matrices corresponding to the other powers α^i can be computed directly as the i-th power of M and the general element $k = f_0 + f_1\alpha + \ldots f_{n-1}\alpha^{n-1}$ will be mapped to the matrix $f_0 I_n + f_1 M + f_2 M^2 + \ldots + f_{n-1} M^{n-1}$. 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 (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. $\square$

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 same as (1) with $-a_0 = \gamma, \;\; a_1 = a_2 = \cdots = a_{n-1} = 0$ and the matrix corresponding to λ_k, where $k = f_0 + f_1\alpha + \ldots + f_{n-1}\alpha^{n-1}$, is

$$\left[\begin{array}{cccccc} f_0 & \gamma f_{n-1} & \gamma f_{n-2} & \cdots & \gamma f_2 & \gamma f_1 \\ f_1 & f_0 & \gamma f_{n-1} & \cdots & \gamma f_3 & \gamma f_2 \\ f_2 & f_1 & f_0 & \cdots & \gamma f_4 & \gamma f_3 \\ f_3 & f_2 & f_1 & \cdots & \gamma f_5 & \gamma f_4 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ f_{n-1} & f_{n-2} & f_{n-3} & \cdots & f_1 & f_0 \end{array}\right]. \tag{2}$$

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 $\left[\begin{array}{cc} a & 2b \\ b & a \end{array}\right]$ 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.

3 Construction of STBCs using Field Extensions

In this section we will outline a simple technique to construct STBCs of various rates 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 (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. 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 (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 $S \cup \gamma S$. 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. Then 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. It is easily verified that a property that the element γ must have if our signal set S is to be invariant under multiplication by γ is:

Lemma 4. *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.*

3.1 Construction of STBCs using cyclotomic field extensions

In this section we construct STBCs using cyclotomic field extensions over different classes of signal sets of various rates and number of antennas.

3.1.1 Rate-optimal Codes over Rotationally Invariant Signal Sets

We will construct rate-optimal STBCs over rotational invariant signal sets. But first, we will look at the construction of rate-optimal STBCs over m-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. For example, with 6-PSK signal set one can use 2^i antennas, or 3^j antennas, or 2^i3^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. We denote the m-PSK signal set by S_m, that is, $S_m = \{\omega_m^i,\ 0 \leq i < m\}$. 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 5. *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 ω_{mn}^l 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 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. □

Now we construct the code on the signal set $S_m = \{\omega_m^i,\ 0 \leq i < m\}$ using matrices of the form (2) with the elements of S_m 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_m, i.e., the code is completely over S_m. Moreover, the number of such matrices is $|S_m|^n$ and hence the rate is 1 symbol per channel use, resulting in rate-optimal codes.

Example 1. *Let us consider the* 4 *element set* $S_4 = \{1, j, -1, -j\}$. *(This set is invariant under multiplication by* j.*) Note that* j *is a primitive* 4*-th root of unity. By Proposition* 5 *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_4 *for our code:*

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

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

The Alamouti code, which is a 2×2 complex orthogonal design of size 2 over S_4, Example 1 gives a code with identical parameters. In the following two examples we obtain codes with parameters that are not obtainable by orthogonal designs.

Example 2. *Let us consider the* 6*-PSK signal set* $S_6 = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$ *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* 5 *above, the polynomial* $x^2 - \omega$ *and* $x^3 - \omega$ *are irreducible over* $\mathbb{Q}(\omega)$. *With* $x^2 - \omega$ *we get* 36 2×2 *codewords given by* $\begin{bmatrix} a & \omega b \\ b & a \end{bmatrix}$ *where* $a, b \in S_6$, *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* $a, b, c \in S_6$.

Instead of codes from m-PSK signal sets, which are invariant under rotation by ω_m, we will now consider the codes over any signal set invariant under rotation of $2\pi/k$, 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 $\gamma = \omega_3$. The following example gives a code over signal sets invariant under 90° rotation.

Example 3. *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 $S_2 = jS_1 = \{-(b-2l) + j(a-2k) | 0 \leq k \leq a,\ 0 \leq l \leq 2b\}$. Note that both S_1 and S_2 are invariant under multiplication by -1. When $n = m$, we have a square constellation. When $m > n$, S 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 $S_1 \cup S_2$.*

As an another 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. 2. 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.

3.1.2 Rate 1 codes over arbitrary finite subsets of $\mathbb{Q}(\omega_m)$ for arbitrary number of antennas

In the previous subsubsection for a given m the number of antennas n is restricted to have only those primes that are in m also *only* if we need rate-optimal codes. If rate-optimality is not a constraint then over any finite subset (including S_m) of subfields of the form $\mathbb{Q}(\omega_m)$ (cyclotomic subfields) of $\mathbb{C}$ full-rank STBCs can be constructed for arbitrary number of antennas, as follows:

Suppose we need to construct codes over symmetric M-PSK for n antennas then choose m such that it contains all the primes of both M and n. Now $\mathbb{Q}(\omega_m)$ contains S_M and the conditions of Proposition 5 are satisfied. Hence we obtain the code

$$\mathcal{C} = \left\{ \begin{pmatrix} f_0 & \gamma f_{n-1} & \cdots & \gamma f_1 \\ f_1 & f_0 & \cdots & \gamma f_2 \\ \vdots & \vdots & \ddots & \vdots \\ f_{n-1} & f_{n-2} & \cdots & f_0 \end{pmatrix} \mid f_i \in S_M \subset \mathbb{Q}(\omega_m), i = 0, 1, \ldots, n-1 \right\} \tag{3}$$

where $\gamma = \omega_m^l$ with $(m, l) = 1$, which is a full-rank rate-one code over S_M and **not** completely over S_M if m contains a prime that is not in M, in which case the code is not rate-optimal.

It is important to notice that for S any finite subset of $\mathbb{Q}(\omega_m)$ the code given by (3) with S_M replaced by S is a full-rank, rate-one code over S. In particular, if m is a multiple of 4 then $\mathbb{Q}(\omega_m)$ contains the entire lattice $\mathbb{Q}(j)$ and by choosing S to be any lattice constellation we get full-rank rate-one code over that lattice constellation. The following example illustrates these observations.

Example 4. *Suppose we need STBCs over the* 6*-PSK signal set* $S_6 = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$ *where* $\omega = e^{\frac{j2\pi}{6}}$ *is a primitive* 6*-th root of unity for five antennas (n=5). Now we can choose* $m = 30$*, then we get the code given by (3) where* $n = 5$*,* γ *is a primitive 30-th root of unity and* $f_i, i = 0, 1, 2, 3, 4 \in S_6$*. Notice that this code is not rate optimal since* γ *is not in* S_6*. Now, we wish to have code over a lattice constellation, say 16-QAM, then our choice of* $m = 30$ *is not sufficient since it is not a multiple of 4 and hence* $\mathbb{Q}(\omega_m)$ *does not contain the 16-QAM. The choice* $m = 60$ *will include the entire lattice in* $\mathbb{Q}(\omega_m)$ *(where now* γ *is a 60-th primitive root of unity) and hence this code is of full-rank rate-one STBC over any lattice constellations from which* $f_i, i = 0, 1, 2, 3, 4$ *come from.*

Another general mathematical basis for construction of full-rank STBCs for arbitrary number of antennas is the following:

Proposition 6. *Let* F *be a field of characteristic zero, and let* z *be an indeterminate. Also, let* $F(z)$ *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*. Then, for any integer* $n \geq 1$*, the polynomial* $x^n - z$ *is irreducible in the ring* $F(z)[x]$*.*

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 $F(\omega_n, z)[x]$. □

We will use this proposition as follows. Let S_m 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, [35]; 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 $\mathbb{Q}(\omega_m)$. (It follows from the well known fact that if z is transcendental over $\mathbb{Q}$, it remains transcendental over an algebraic extension of $\mathbb{Q}$ such as $\mathbb{Q}(\omega_m)$.) 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.

In the following example we construct a code over such a signal set with 8 elements shown in Fig. 1.

Example 5. *In Example 1 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 full-rank code over the asymmetric 8-PSK signal set shown in Fig. 1, for* 3 *antennas containing the 64 codewords given by* $\begin{bmatrix} a & ce^{j\theta} & be^{j\theta} \\ b & a & ce^{j\theta} \\ c & b & a \end{bmatrix}$ *where* $a, b, c \in S$, *using Proposition 6.*

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 $|z|$. 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.

3.1.3 High-rate (>1) codes from cyclotomic field extensions

Consider a rate-one code for n antennas over $\mathbb{Q}(\omega_m)$ and let $\mathbb{Q}(\omega_l) \subset \mathbb{Q}(\omega_m)$, where l divides m. Then, every element of $\mathbb{Q}(\omega_m)$ can be written as $\sum_{b \in B} l_b b$, where B is the basis of the field $\mathbb{Q}(\omega_m)$ seen as vector space over $\mathbb{Q}(\omega_l)$ and $l_b \in \mathbb{Q}(\omega_l)$. In (3), replacing f_i with $\sum_{b \in B} f_{i,b} b$, we have

$$\mathcal{C} = \left\{ \begin{pmatrix} \sum_{b \in B} f_{0,b} b & \gamma \sum_{b \in B} f_{n-1,b} b & \cdots & \gamma \sum_{b \in B} f_{1,b} b \\ \sum_{b \in B} f_{1,b} b & \sum_{b \in B} f_{0,b} b & \cdots & \gamma \sum_{b \in B} f_{2,b} b \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{b \in B} f_{n-1,b} b & \sum_{b \in B} f_{n-2,b} b & \cdots & \sum_{b \in B} f_{0,b} b \end{pmatrix} \mid f_{i,b} \in \mathbb{Q}(\omega_l), i \in [0, n-1] \right\} \qquad (4)$$

Clearly, $\mathcal{C}$ is a rate $|B|$ code over any finite subset of $\mathbb{Q}(\omega_l)$. For example if $m = 8$ and $l = 4$, we get 2×2, rate 2, full rank STBC's over any finite subset of $\mathbb{Q}(\omega_4)$, i.e., over lattice constellations. Thus, if we want a rate $R > 1$, (R-an integer) $n \times n$, full rank STBC over a signal set S_M, then we do the following:

- Choose m such that it has all primes of R. Then, using the irreducible polynomial $x^R - \omega_m$, extend the field $\mathbb{Q}(\omega_m)$ to the field $\mathbb{Q}(\omega_{mR})$.

- Construct the $n \times n$ full rank STBC over $\mathbb{Q}(\omega_{mR})$ using the constructions given in the previous section, i.e., construct a $n \times n$ full rank rate-one STBC over S_{mR}.

- Replace each entry of the codeword matrices with a linear combination of the basis of $\mathbb{Q}(\omega_{mR})$ over $\mathbb{Q}(\omega_m)$. Thus, we have a rate R, full rank code over S_Mi, as follows:

$$\mathcal{C} = \left\{ \begin{pmatrix} \sum_{i=0}^{R-1} f_{0,i} \omega_{mR}^i & \gamma \sum_{i=0}^{R-1} f_{n-1,i} \omega_{mR}^i & \cdots & \gamma \sum_{i=0}^{R-1} f_{1,i} \omega_{mR}^i \\ \sum_{i=0}^{R-1} f_{1,i} \omega_{mR}^i & \sum_{i=0}^{R-1} f_{0,i} \omega_{mR}^i & \cdots & \gamma \sum_{i=0}^{R-1} f_{2,i} \omega_{mR}^i \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=0}^{R-1} f_{n-1,i} \omega_{mR}^i & \sum_{i=0}^{R-1} f_{n-2,i} \omega_{mR}^i & \cdots & \sum_{b \in B} f_{0,i} \omega_{mR}^i \end{pmatrix} \mid f_{k,i} \in \mathbb{Q}(\omega_l) \right\} \qquad (5)$$

  where $k \in [0, n-1]$, $i \in [0, R-1]$ and γ is an m_R-th primitive root of unity, where m_R is a positive integer such that it has all the primes of n.

Clearly, with the above constructions, the rate is upper bounded by the degree of the polynomial $x^R - \omega_m$ and also the value of γ depends on the value of R. In the rest of this subsection, we give another method of constructing STBC's with arbitrary rate, where γ is independent of the rate R and hence, as will be seen in the sequel, we can have better coding gain.

Consider the rational function field $\mathbb{Q}(\omega_m, z)$ over $\mathbb{Q}(\omega_m)$ in the indeterminate z. The elements of $\mathbb{Q}(\omega_m, z)$ are of the form $a(z)/b(z)$, where $a(z)$ and $b(z) \neq 0$ are polynomials over $\mathbb{Q}(\omega_m)$. Then, from Theorem 6 we have that $x^n - z$ is irreducible over $\mathbb{Q}(\omega_m, z)$. Hence we have the STBC obtained by using the polynomial $x^n - z$ as

$$\mathcal{C} = \left\{ \begin{pmatrix} f_0(z) & zf_{n-1}(z) & \cdots & zf_1(z) \\ f_1(z) & f_0(z) & \cdots & zf_2(z) \\ \vdots & \vdots & \ddots & \vdots \\ f_{n-1}(z) & f_{n-2}(z) & \cdots & f_0(z) \end{pmatrix} \mid f_i(z) \in \mathbb{Q}(\omega_m)[z], i = 0, 1, \ldots, n-1 \right\} \quad (6)$$

Note that, in the above STBC the entries in the matrices are polynomials instead of the rational functions of polynomials. Now each of $f_i(z) = \sum_{k=0}^{R-1} f_{i,k} z^k$, where $f_{i,k} \in \mathbb{Q}(\omega_m)$. Here, R can be any integer and hence the rate which is equal to R is arbitrary (this is because we can have polynomials with any degree as the extension of $\mathbb{Q}$ to $\mathbb{Q}(z)$ is infinite dimensional). z can be any transcendental number. If θ is an algebraic number, then from [35] (§4.12), $e^{j\theta}$ is a transcendental number. Thus, we can take $e^{j\theta}$ as z in the above construction. The following example shows that we can achieve better performance in terms of coding gain with codes with rate larger than one.

Example 6. *Consider a rate 2, 2×2 full rank STBC $\mathcal{C}$ over 4-PSK signal set.*

$$\mathcal{C} = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} f_{0,0} + f_{0,1}z & f_{1,0}z + f_{1,1}z^2 \\ f_{1,0} + f_{1,1}z & f_{0,0} + f_{0,1}z \end{pmatrix} | f_{i,k} \in 4 - PSK, i, k = 0, 1 \right\}$$

The size of the code is 256 and hence the bit rate is 4 bits per channel use. The scaling factor $1/\sqrt{2}$ is used to make the average power per antenna per channel use equal to one. Coding gain of this code is at least equal to 0.136 ($z \approx e^{j0.52}$, coding gain might be more than this for some other z). Now consider a rate 1, 2×2 full rank STBC $\mathcal{C}'$ over M-PSK signal set. Then, to obtain bit rate 4 bits per channel use, M should be equal to 16. Coding gain of this rate-one code is 0.052 approximately. Clearly, the coding gain of the rate 2 code is about 2.5 times the coding gain of rate-one code.

Consider the rate 2 STBC over 4-PSK for 2 antennas, obtained from algebraic extensions. We have $m = 4$ and $R = 2$. So, $\gamma = \omega_8$. By manually computing the coding gain, it is found *that coding gain of this code is at most 0.13, which is lesser than the coding gain obtained from transcendental extensions.*

The above example motivates not only the use of high rate codes to improve the coding gain but also high rate codes obtained from transcendental extensions.

3.2 Construction of STBCs using non-cyclotomic field extensions

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 7. *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, [35]), $f(x)$ 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 7. *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, 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.*

4 Coding gain and capacity of STBCs from Field Extensions

In this section we discuss the coding gain of STBCs obtained from both the cyclotomic and noncyclotomic field extensions and present capacity of STBCs from cyclotomic extensions.

4.1 Coding gain

Let $A(\mathbf{c}, \mathbf{e})$ be the difference of the two codeword matrices $\mathbf{c}$, $\mathbf{e}$ in a STBC $\mathcal{C}$ and let $B(\mathbf{c}, \mathbf{e}) = A(\mathbf{c}, \mathbf{e})^* A(\mathbf{c}, \mathbf{e})$. Let $a_k, k = 0, 1, \ldots, K$ denote the K non-zero eigen values of $B(\mathbf{c}, \mathbf{e})$, where K is the rank of $A(\mathbf{c}, \mathbf{e})$. In our case $B(\mathbf{c}, \mathbf{e})$ have full rank, $K = n$. Then, the coding gain of a STBC $\mathcal{C}$ is given by the minimum of $\mid \prod_{k=0}^{n-1} a_k \mid^{1/n}$ for all possible pairs $\mathbf{c}$ and $\mathbf{e}$ of codeword matrices of the code. That is,

$$G = \min_{\mathbf{c}, \mathbf{c}' \in \mathcal{C}} \mid det(B(\mathbf{c}, \mathbf{c}')) \mid^{1/n} \tag{7}$$

Theorem 8. *If $\mathcal{C} = \{f_0 I + f_1 M + f_2 M^2 + \cdots + f_{n-1} M^{n-1} | f_i \in S \subset F\}$, where M is an (1), then coding gain is*

$$G = \min_{\mathbf{c}, \mathbf{c}' \in \mathcal{C}} \left| N_{K/F} \left(\sum_{i=0}^{n-1} (f_i - f_i') \alpha^i \right) \right|^{2/n}$$

where $N_{K/F}(x)$ denotes the norm of the element x from K to F, $\mathbf{c} = \sum_{i=0}^{n-1} f_i M^i$ and $\mathbf{c}' = \sum_{i=0}^{n-1} f_i' M^i$.

Proof. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be the minimal polynomial of α over F. Let L be a normal closure of K/F and σ_i, $i = 0, 1, \ldots, n-1$ be the distinct $F-$ homomorphisms from K to L. Let $p(x)$ be the minimal polynomial of $k = \sum_{i=0}^{n-1}(f_i - f_i')\alpha^i$ over F of degree $m \leq n$. Then, it is easy to see that m divides n and that every root of $p(x)$ is of the form $\sigma_i(k)$ for some $0 \leq i < n$. Thus, the polynomial $g(x) = \prod_{i=0}^{n-1}(x - \sigma_i(a))$ and the polynomial $p(x)$ have same roots. Since, $g(x) \in F[x]$, the only irreducible factor of $g(x)$ is $p(x)$ and hence we have $g(x) = p(x)^{n/m}$. Now, since the minimal polynomial of k divides the characteristic polynomial $\chi(x)$ of $\lambda_k = (f_0 - f_0')I + (f_1 - f_1')M + (f_2 - f_2')M^2 + \cdots + (f_{n-1} - f_{n-1}')M^{n-1}$, and share the same irreducible factors over F, $\chi(x)$ must have $p(x)$ as the only irreducible factor. Thus, $\chi(x) = p(x)^{n/m} = g(x)$ (since degree of $\chi(x)$ is n). And since determinant of λ_k is the coefficient of the constant term in the characteristic polynomial, we get

$$\det \lambda_k = \prod_{i=0}^{n-1} \sigma_i(k) = N_{K/F}(k).$$

Thus, the coding gain is $\quad G = \min_{\mathbf{c},\mathbf{c}' \in \mathcal{C}} \mid N_{K/F}(k) \mid^{2/n}.$ □

The above theorem gives coding gain expression for STBCs obtained using arbitrary field extensions. When, the field extension is a cyclotomic extension, we have the following corollary to the above theorem.

Corollary 9. *If the code $\mathcal{C}$ is as in the (3), then*

$$G = \min_{\mathbf{c},\mathbf{c}' \in \mathcal{C}} \left| \prod_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} (f_i - f_i')\gamma_j^i \right) \right|^{2/n}$$

where γ_i for $i = 0, 1, \ldots, n-1$ are the n^{th} roots of γ, $\mathbf{c} = c([f_0, f_1, \ldots, f_{n-1}], \gamma)$ (the codeword matrix with $(i,1)$-th component as f_{i-1}) and $\mathbf{c}' = c([f_0', f_1', \ldots, f_{n-1}'], \gamma)$ (the codeword matrix with $(i,1)$-th component as f_{i-1}').

Proof. The F-homomorphisms of K into the normal closure of K/F are given as $\sigma_i : \gamma_0 \mapsto \gamma_i$ for all $i = 0, 1, 2, \ldots, n-1$, where γ_i are the n-th roots of γ. Thus, from Theorem 8, we have $G = \min_{\mathbf{c},\mathbf{c}' \in \mathcal{C}} \left| N_{K/F}(\sum_{i=0}^{n-1}(f_i - f_i')\gamma_0^i) \right|^{2/n} = \min_{\mathbf{c},\mathbf{c}' \in \mathcal{C}} \left| \prod_{j=0}^{n-1} \sum_{i=0}^{n-1} (f_i - f_i')\gamma_j^i \right|^{2/n}.$ □

From the above theorem, if $\mathbf{c}$ and $\mathbf{c}'$ have $f_k = f'_k$ for all k except for some $k' \in [0, n-1]$ then we have the coding gain as

$$G \leq \left| \prod_{i=0}^{n-1} (f_{k'} - f'_{k'}) \gamma_i^{k'} \right|^{2/n} \leq \mid f_{k'} - f'_{k'} \mid^2 \quad \text{(since } \gamma_i \text{ are roots of unity).}$$

Thus, the main factor which dominates the coding gain is the selection of S. From the above theorem the coding gain for the STBC in Example 1 is

$$G = \min_{\mathbf{c}, \mathbf{c}' \in \mathcal{C}} \left| \prod_{i=0}^{n-1} \left(\sum_{k=0}^{n-1} (f_k - f'_k) \gamma_i^k \right) \right|^{2/n} = 2.$$

Now, let us see the how the coding gain depends on γ. Let m_{opt} be the smallest m such that the prime factors of n are a subset of the prime factors of m and the signal set, S_M is subset of $\mathbb{Q}(\omega_{m_{opt}})$. Therefore, $m_{opt} = xM$ for some integer x. Now let $m' \neq m_{opt}$ be another integer such that the prime factors of n are subset of the prime factors of m' and the signal set is subset of $\mathbb{Q}(\omega_{m'})$. Clearly, $m_{opt} < m'$. The codeword matrices have the entries of the form f_i and γf_i, where $f_i \in S$. If x is not equal to one, then it is easy to see that the minimum distance (which happens to be the distance between any $f_i \in S$ and γf_i) of the resulting signal set decreases if we add the points γS to the signal set. Now, if we let γ to be $\omega_{m_{opt}}$, the we claim that the decrease in the minimum distance is minimum possible. This can be seen in the following way : as m increases from m_{opt}, the point $\omega_m f_i$ gets closer to the point f_i and hence the minimum distance decreases more as m increases. Though, the minimum distance is not the coding gain of the STBC, it is intuitive enough to choose γ which keeps the minimum distance of the $S \cup \gamma S$ as maximum as possible. For instance, in Example 1 we have $m_{opt} = 4$ and the corresponding coding gain is 2. However, if we let $m = 8$ (or 12), the coding gain falls down to 1.53 (or 1.0). The same holds true for QAM constellations too.

In codes with rate larger than one obtained from transcendental extensions, the degree n of the irreducible polynomial $x^n - z$ is independent of the signal set we choose and hence m should be chosen such that the signal set is invariant under the multiplication of ω_m so that the minimum distance of the signal set remains same. However, the entries of the codeword matrices are polynomials in z (any transcendental number), and hence, the coding gain depends on z also. It is very difficult to see how the coding gain and z are related. In example 6, the coding gains as a function of z are as follows : $G(e^{j0.1}) = 0.001$, $G(e^{j0.3}) = 0.027$, $G(e^{j0.5}) = 0.121$, $G(e^{j0.52}) = 0.136$, $G(e^{j0.7}) = 0.019$, $G(e^{j0.9}) = 0.116$, $G(e^{j1.1}) = 0.093$, $G(e^{j1.3}) =$

0.073, $G(e^{j1.5}) = 0.005$, $G(e^{j1.7}) = 0.017$, $G(e^{j1.9}) = 0.107$, $G(e^{j2.1}) = 0.01$, $G(e^{j2.3}) = 0.014$, $G(e^{j2.7}) = 0.084$, $G(e^{j2.9}) = 0.015$ and $G(e^{j3.1}) = 0.0001$.

It is shown in [36] that the coding gain of the STBCS constructed in the previous sections, is equal to the minimum squared Euclidean distance for QAM and some other specific signal sets when the minimal polynomial is over the set of integers.

4.2 Capacity of STBC's from cyclotomic extensions

One says that a design is information lossless or achieves capacity if the capacity of the new equivalent channel obtained by considering the design as part of the channel, has the same capacity of the original channel [32]. Notice that our constructions basically give a design and along with a signal set for the variables we obtain a STBC. However, the information losslessness or capacity of the design will be referred to as that of the associated STBC also. In this subsection we study the capacity of the STBCs obtained from cyclotomic field extensions.

Let r be the number of receive antennas. Then, the received signal $\mathbf{x}$, when the transmitted signal is $\mathbf{f}$, is given by

$$\mathbf{x} = \sqrt{\frac{\rho}{n}} H\mathbf{f} + \mathbf{v} \tag{8}$$

where $\mathbf{x} \in \mathbb{C}^r$, $\mathbf{f} \in \mathbb{C}^n$, $H \in \mathbb{C}^{r\times n}$ is the channel matrix, $\mathbf{v} \in \mathbb{C}^r$ is the additive white Gaussian noise and ρ is the signal to noise ratio at each receive antenna. The entries in the channel matrix and the transmitted vector are assumed to have unit variance, i.e.,

$$\mathrm{E}tr(HH^*) = nr \text{ and } \mathrm{E}\mathbf{f}^*\mathbf{f} = n$$

When the channel is known at the receiver, the resulting channel capacity is [1]

$$C(\rho, n, r) = \mathrm{E} \log \det \left(I_r + \frac{\rho}{n} HH^* \right) \tag{9}$$

If $\mathbf{F}$ is the transmitted codeword matrix, then

$$\mathbf{X} = \sqrt{\frac{\rho}{n}} \mathbf{F}H + \mathbf{V}$$

The transmitted signal matrix in our STBC constructions is as in (3). And if $H = (h_{i,j})_{i\in[0,n-1], j\in[0,r-1]}$, we have

$$\hat{\mathbf{X}} = \sqrt{\frac{\rho}{n}} \hat{H} [f_0 \ f_1 \ \cdots \ f_{n-1}]^T + \hat{\mathbf{V}}$$

where $\hat{\mathbf{X}} = vec(\mathbf{X})$, $\hat{\mathbf{V}} = vec(\mathbf{V})$ and

$$\hat{H} = \left(\begin{array}{c} c_0 = c([h_{0,0}, h_{1,0}, \ldots, h_{n-1,0}], \gamma) \\ c_1 = c([h_{0,1}, h_{1,1}, \ldots, h_{n-1,1}], \gamma) \\ \vdots \\ c_{r-1} = c([h_{0,r-1}, h_{1,r-1}, \ldots, h_{n-1,r-1}], \gamma) \end{array} \right)$$

In the above equation, recall that c_j are $n \times n$ matrices as in (3), with $f_i = h_{i,j}$. It can be checked easily that eigen values $a_{i,k}$ of c_i are given by

$$a_{i,k} = \sum_{l=0}^{n-1} h_{l,i} \gamma_k^l, \text{ for } k = 0, 1, 2, \ldots, n-1$$

Then, the c_i can be written as $P_i \Lambda_i P_i^{-1}$, where P_i is the eigenvector matrix and Λ_i is the eigenvalue matrix. It can be easily seen that,

$$P_i = diag(1, \gamma_0, \gamma_0^2, \ldots, \gamma_0^{n-1}) DFT_n \tag{10}$$

Now, the capacity, denoted by $C_\gamma(\rho, n, r)$, of these codes is given by replacing H with $\hat{H}$ and $R_f = I_{nr}$ in (9), which is

$$C_\gamma(\rho, n, r) = \frac{1}{n} \mathrm{E} \log \det \left(I_{nr} + \frac{\rho}{n} \hat{H} \hat{H}^* \right) \tag{11}$$

where the normalizing factor $1/n$ in front of the expectation is for the n channels uses we have in our STBC. The term $\hat{H}\hat{H}^*$ in the capacity expression is equal to $(c_i^* c_j)_{i,j \in [0, r-1]}$. Computing the determinant of $I_{nr} + \sqrt{\frac{\rho}{n}} \hat{H}\hat{H}^*$ is very difficult for any r number of receive antennas. So, let us see the case when we have only one receive antenna. Then, removing the subscript corresponding to the receive antennas in $\hat{H}$, we have $\hat{H}\hat{H}^* = P \Lambda P^{-1} P^{-1*} \Lambda^* P^*$. From (10), we have $\hat{H}\hat{H}^* = (1/n) P |\Lambda|^2 P^*$. Thus,

$$\det \left(I_n + \sqrt{\frac{\rho}{n}} \hat{H}\hat{H}^* \right) = \det \left(P^{-1} \right) \det \left(I_n + \sqrt{\frac{\rho}{n}} \hat{H}\hat{H}^* \right) \det (P) = \det \left(I_n + \sqrt{\frac{\rho}{n}} |\Lambda|^2 \right)$$

Thus, the capacity is

$$\begin{aligned} C_\gamma(\rho, n, r = 1) &= \mathrm{E} \log \left(\prod_{k=0}^{n-1} \left(1 + \left| \sum_{i=0}^{n-1} h_i \gamma_k^i \right|^2 \right) \right)^{1/n} \qquad (12) \\ &\leq \mathrm{E} \log \left(\prod_{k=0}^{n-1} \left(1 + \sum_{i=0}^{n-1} |h_i|^2 \right) \right)^{1/n} = C(\rho, n, r = 1) \end{aligned}$$

Now, let us see what the capacity is for rate more than one codes. In this case the transmitted signal matrix $\mathbf{F}$ is given as in either (5) or (6). Thus, assuming the signal points the constellation to be independent and to ensure unit power transmitted per antenna per channel use, we have $R_f = \frac{1}{R} I_{nR}$. Let $\hat{f} = [f_0(z) f_1(z) \ldots f_{n-1}(z)]^T$. Then, $R_{\hat{f}} = I_n$. Since, the covariance matrix is same in both the cases (rate-one and rate more than one), the capacity remains unchanged. Indeed, the capacity remains unchanged, as we have computed it for the input distribution to have $R_f = I_n$, and in both the cases the codeword matrices remain same in the sense of their structure. However, we have already seen in Example 6 that by going to higher rates, we achieve more coding gain.

We have plotted the capacity for the 2×2 code from cyclotomic extensions and the capacity for Alamouti's code as a function of SNR in Fig. 3. From this plot it can be seen that the Alamouti code has more capacity (by about 1/2 a bit at 30dB SNR with one receive antenna). However, as number of receive antennas increase, one sees that the difference is coming down from the Fig. 4.

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 2.1 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 [37–40].

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.

The Hamilton's Quaternions denoted by $\mathbb{H}$ 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. 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. Clearly, the center of $\mathbb{H}$ 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 $F \nsubseteq K$, 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. If E is any subfield of D, then viewing D as an E-space, we can obtain an embedding of D into $M_{n_e}(E)$ where n_e is $[D : E]$. In particular, we give, in the following subsections embeddings of D into $M_{n^2}(F)$ and $M_n(K)$.

5.2 Codes From The Left Regular Representation of Division Algebras

The material in this section parallels the material in Section 2.1. 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 $\rho_{d_1 d_2} = \rho_{d_2}\rho_{d_1}$, 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 2.1, 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 $(1 \leq i \leq n^2)$, and for any j $(1 \leq j \leq n^2)$, let $u_i u_j = \sum_{l=1}^{n^2} c_{ij,l} u_l$. Then, the j-th column of λ_{u_i} is simply the coefficients $c_{ij,l}$ above, $1 \leq l \leq n^2$. (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 $d = \sum_{i=1}^{n^2} f_i u_i$ is just the linear combination $\sum_{i=1}^{n^2} f_i M_i$.

Example 8. *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 4 dimensional orthogonal real design of the paper [8, §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.

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 9. *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. It is well known that we have the following decomposition of D as right K spaces:

$$D = K \oplus zK \oplus z^2K \oplus \cdots \oplus z^{n-1}K, \tag{13}$$

where z is some element of D that satisfies the relations

$$kz \qquad = z\sigma(k)\ \forall k \in K \tag{14}$$

$$z^n \quad = \delta, \quad \text{for some} \quad \delta \in F^* \tag{15}$$

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 (13) and (14) 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 10. *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 9, 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 (13) 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 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. 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 (13) 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, $\ldots$, k_{n-1}. For the second column, note that $dz = (k_0 + zk_1 + \ldots z^{n-1}k_{n-1})z = k_0z + zk_1z + \ldots z^{n-1}k_{n-1}z = z\sigma(k_0) + z^2\sigma(k_1) + \ldots z^{n-1}\sigma(k_{n-2}) + \delta\sigma(k_{n-1})$, where we've used the relations in (14) 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:

$$\begin{bmatrix} k_0 & \delta\sigma(k_{n-1}) & \delta\sigma^2(k_{n-2}) & \ldots & \delta\sigma^{n-2}(k_2 & \delta\sigma^{n-1}(k_1) \\ k_1 & \sigma(k_0) & \delta\sigma^2(k_{n-1}) & \ldots & \delta\sigma^{n-2}(k_3) & \delta\sigma^{n-1}(k_2) \\ k_2 & \sigma(k_1) & \sigma^2(k_0) & \ldots & \delta\sigma^{n-2}(k_4) & \delta\sigma^{n-1}(k_3) \\ k_3 & \sigma(k_2) & \sigma^2(k_1) & \ldots & \delta\sigma^{n-2}(k_5) & \delta\sigma^{n-1}(k_4) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ k_{n-1} & \sigma(k_{n-2}) & \sigma^2(k_{n-3}) & \ldots & \sigma^{n-2}(k_1) & \sigma^{n-1}(k_0) \end{bmatrix} \qquad (16)$$

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, $\sigma(k)$, $\ldots$, $\sigma^{n-1}(k)$ along the diagonal. Also, notice that the matrices (16) above are very similar to the matrices (2); the difference is in the twist by powers of the automorphism σ.

Now, we highlight an algebraic uniqueness property of the Alamouti code [7]. In Example 9 we have seen 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 $k \in \mathbb{C}$. Thus, the STBC obtained using the division algebra $\mathbb{H}$ is given by (16) with $\delta = -1$, σ as the complex conjugation, i.e., the codeword matrices are of the form $\begin{bmatrix} k_0 & -k_1^* \\ k_1 & k_0^* \end{bmatrix}$. But this is precisely the Alamouti code [7]. And in fact this is the only rate-1 STBC which is full rank over any finite set of $\mathbb{C}$. This uniqueness of Alamouti is due to the fact that set of quaernions $\mathbb{H}$ is the only division algebra which has the entire complexes as its maximal subfield [41, Theorem 11.14].

Now, considering the fact that the field K is a cyclic extension of the field F, every k_i in the above matrix can be written as a F-linear combination of the basis of K seen as a F-vector space. Thus, if $K = F(t)$ for some $t \in K$, then the matrix (16) can be written as

$$\begin{bmatrix}
\sum_{i=0}^{n-1} f_{0,i}t^i & \delta\sigma\left(\sum_{i=0}^{n-1} f_{n-1,i}t^i\right) & \delta\sigma^2\left(\sum_{i=0}^{n-1} f_{n-2,i}t^i\right) & \cdots & \delta\sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{1,i}t^i\right) \\
\sum_{i=0}^{n-1} f_{1,i}t^i & \sigma\left(\sum_{i=0}^{n-1} f_{0,i}t^i\right) & \delta\sigma^2\left(\sum_{i=0}^{n-1} f_{n-1,i}t^i\right) & \cdots & \delta\sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{2,i}t^i\right) \\
\sum_{i=0}^{n-1} f_{2,i}t^i & \sigma\left(\sum_{i=0}^{n-1} f_{1,i}t^i\right) & \sigma^2\left(\sum_{i=0}^{n-1} f_{0,i}t^i\right) & \cdots & \delta\sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{3,i}t^i\right) \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\sum_{i=0}^{n-1} f_{n-1,i}t^i & \sigma\left(\sum_{i=0}^{n-1} f_{n-2,i}t^i\right) & \sigma^2\left(\sum_{i=0}^{n-1} f_{n-3,i}t^i\right) & \cdots & \sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{0,i}t^i\right)
\end{bmatrix} \tag{17}$$

We thus have the following corollary to Proposition 1:

Corollary 10. *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 (13) and (14). Then, any finite subset E of matrices of the form (16) and (17) 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.*

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

To apply the general machinery of Corollary 10 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

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

where z is some symbol that satisfies the two relations given in (14), 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 ([40, Chapter 15, Corollary d], or [41, Theorem 8.14]):

Proposition 11. *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.)*

We can use Proposition 11 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 ([35, 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 12. *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 11 that $(K(\delta)/(F(\delta), \sigma, \delta)$ is a division algebra. □

A detailed version of the contents of the rest of this section can be found in [42, 43]. We will always assume that δ lies on unit circle and since there are infinite transcendental numbers on unit circle (e^{ju} lies on unit circle and is transcendental for any algebraic u), we always have at least one such δ. So, the task now is to construct the field $F(\delta)$ and its cyclic extension $K(\delta)$, where δ is a transcendental over K. To do this, we use the following theorem from [44].

Theorem 13. *Let F be a field containing a primitive n^{th} root of unity. Then, K/F is cyclic of degree n if and only if K is the splitting field over F of an irreducible polynomial $x^n - a \in F[x]$.*

In the following two subsections, we use some algebraic extensions of the field of rational numbers, $\mathbb{Q}$ to construct designs and in then we show that these designs achieve capacity.

7.1 $F/\mathbb{Q}$ is finite

Let S be the signal set of interest, i.e., we want STBCs over S. Let $F = \mathbb{Q}(S, \omega_m)$, where m is a multiple of n, in such a way that $x^n - \omega_m$ is irreducible in $F[x]$. Clearly, F has a n^{th} root of unity. Let $K = F(\omega_{mn})$. To be able to use Theorem 13 it is sufficient to show that K is the splitting field of $x^n - \omega_m$. The roots of this polynomial are $\omega_{mn}\omega_n^i$ for $i = 0, 1, \ldots, n-1$. Since K contains ω_{mn}, all these roots also lie in K. Thus, K contains the splitting field of $x^n - \omega_m$. Since K is the smallest subfield containing F and ω_{mn}, K itself is the splitting field of $x^n - \omega_m$. Thus, by Theorem 13 K/F is a cyclic extension. We give some examples to illustrate the above construction.

Example 11. *Let $n = 2$ and $F = \mathbb{Q}(j)$, $K = F(\sqrt{j})$. Clearly, K is the splitting field of the polynomial $x^2 - j \in F[x]$ and hence K/F is cyclic of degree 2. Note that $x^2 - j$ is irreducible* *over F, since its only roots are $\pm\sqrt{j}$ and none of them is in F. The generator of the Galois group is given by $\sigma : \sqrt{j} \mapsto -\sqrt{j}$. Now, let δ be any transcendental element over K. Then, $(K(\delta)/F(\delta), \sigma, \delta)$ is a cyclic division algebra. Thus, we have the STBC $\mathcal{C}$ given by*

$$\mathcal{C} = \left\{ \begin{bmatrix} k_0 & \delta\sigma(k_1) \\ k_1 & \sigma(k_0) \end{bmatrix} | k_0, k_1 \in K \right\}$$

However, viewing K as a vector space over F, with the basis $\{1, \sqrt{j}\}$, we have a STBC over any finite subset of F with codewords as follows

$$\frac{1}{\sqrt{2}} \begin{bmatrix} f_{0,0} + f_{0,1}\sqrt{j} & \delta\sigma(f_{1,0} + f_{1,1}\sqrt{j}) \\ f_{1,0} + f_{1,1}\sqrt{j} & \sigma(f_{0,0} + f_{0,1}\sqrt{j}) \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} f_{0,0} + f_{0,1}\sqrt{j} & \delta(f_{1,0} - f_{1,1}\sqrt{j}) \\ f_{1,0} + f_{1,1}\sqrt{j} & (f_{0,0} - f_{0,1}\sqrt{j}) \end{bmatrix}$$

where $f_{ij} \in S \subset F$ for $i, j = 0, 1$ and the scaling factor $1/\sqrt{2}$ is to ensure that the average power transmitted by each antenna per channel use is one.

In the above example S can be any finite subset of F and hence, we have an STBC over any QAM constellation (since $F = \mathbb{Q}(j)$). From the structure of this STBC, we can see that it has a structure similar to the STBC proposed in [32]. Indeed, these two are similar in the sense of their capability of achieving the capacity, which will be shown in the next section. The code presented in [32] is full rank for QAM constellations, as is the case with our code. However, we get STBC's for 2 antennas over any signal set, by choosing appropriate m. Say for instance, we want codes over 8PSK. In this case, we can take $m = 8$. However, the restriction on the choice of m affects the coding gain. This restriction on m is due to the signal set and n. And moreover, finding m such that the polynomial $x^n - \omega_m$ is irreducible over F depends on S, which might turn out to be involved sometimes. So, in the next subsection, we give constructions which do not depend on the signal set and n.

Example 12. *Let $n = 3$ and suppose, we want S to be a QAM signal constellation. So, let $F = \mathbb{Q}(j, \omega_3)$ and $K = F(\omega_9)$. Clearly, K is the splitting field of the polynomial $x^3 - \omega_3 \in F[x]$. The polynomial $x^3 - \omega_3$ is irreducible in $F[x]$ because, otherwise, it would have linear factor in $F[x]$, which would correspond to a root of $x^3 - \omega_3$, but this polynomial has no roots in F. Thus, K/F is cyclic and $\sigma : \omega_9 \mapsto \omega_9\omega_3$ is a generator of the Galois group. Now, let δ be any transcendental over K. Then, $(K(\delta)/F(\delta), \sigma, \delta)$ is a cyclic division algebra. Thus, we have the STBC $\mathcal{C}$ with codewords as follows (obtained in a similar way as in the previous example)*

$$\frac{1}{\sqrt{3}} \begin{bmatrix} g_{0,0} & \delta g_{1,2} & \delta g_{2,1} \\ g_{0,1} & g_{1,0} & \delta g_{2,2} \\ g_{0,2} & g_{1,1} & g_{2,0} \end{bmatrix}$$

where $g_{i,j} = \sum_{l=0}^{2} f_{j,l}(\omega_9^i\omega_3)^l = \sum_{l=0}^{2} f_{j,l}\omega_9^{(3+i)l}$ *and* $f_{i,j} \in S \subset F$ *for* $i, j = 0, 1, 2.$

7.2 $F/\mathbb{Q}$ is infinite

In the last subsection, we have seen that the constructions depend on the signal set and the number of antennas, which affects the coding gain of the STBC's. In this subsection, we use transcendental extensions of $\mathbb{Q}$ to overcome this restriction. First, we have the following corollary to Theorem 13.

Corollary 14. *Let* $F = \mathbb{Q}(S, t, \omega_n)$*, where* t *is a transcendental element over* $\mathbb{Q}(S)$*. Then,* $K = F(t_n = t^{1/n})$ *is a cyclic extension of* F*, and the degree of extension is* n*.*

The above corollary gives us a cyclic extension for any n and signal set S. The irreducible polynomial used to obtain the extension in the above corollary is $x^n - t$ and that this is a irreducible polynomial over F is easy to prove. So, the difficulty of finding an irreducible polynomial over F of degree n is overcome. Using the above corollary, we give some examples.

Example 13. *Let* $n = 2$ *and* $F = \mathbb{Q}(S, t)$*, where* t *is transcendental over* $\mathbb{Q}(S)$*. Then,* $K = F(t_2 = \sqrt{t})$ *is a cyclic extension of* F *of degree 2. The generator of the Galois group is given by* $\sigma : t_2 \mapsto -t_2$*. Now, let* δ *be any transcendental over* K*. Then,* $(K(\delta)/F(\delta), \sigma, \delta)$ *is a cyclic division algebra. Thus, we have the STBC* $\mathcal{C}$ *with the codewords as follows (obtained in a similar way as in the previous example):*

$$\frac{1}{\sqrt{2}}\begin{bmatrix} f_{0,0} + f_{0,1}t_2 & \delta\sigma(f_{1,0} + f_{1,1}t_2) \\ f_{1,0} + f_{1,1}t_2 & \sigma(f_{0,0} + f_{0,1}t_2) \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} f_{0,0} + f_{0,1}t_2 & \delta(f_{1,0} - f_{1,1}t_2) \\ f_{1,0} + f_{1,1}t_2 & (f_{0,0} - f_{0,1}t_2) \end{bmatrix}$$

where $f_{0,0}, f_{0,1}, f_{1,0}, f_{1,1} \in S \subset F$*.*

Example 14. *Let* $n = 5$ *and* S *be the signal set. Then, with* $F = \mathbb{Q}(\omega_5, S, t)$ *and* $K = F(t_5 = t^{1/5})$*, we have* K/F *cyclic and* $\sigma : t_5 \mapsto \omega_5 t_5$ *is a generator of the Galois group. Thus, we have a STBC for 5 antennas as follows :*

$$\mathcal{C} = \left\{ \frac{1}{\sqrt{5}} \begin{bmatrix} g_{0,0} & \delta g_{1,4} & \delta g_{2,3} & \delta g_{3,2} & \delta g_{4,1} \\ g_{0,1} & g_{1,0} & \delta g_{2,4} & \delta g_{3,3} & \delta g_{4,2} \\ g_{0,2} & g_{1,1} & g_{2,0} & \delta g_{3,4} & \delta g_{4,3} \\ g_{0,3} & g_{1,2} & g_{2,1} & g_{3,0} & \delta g_{4,4} \\ g_{0,4} & g_{1,3} & g_{2,2} & g_{3,1} & g_{4,0} \end{bmatrix} \right\}$$

where $g_{i,j} = \sum_{l=0}^{4} f_{j,l}(\omega_5^i t_5)^l$ *and* $f_{i,j} \in S \subset F$ *for* $i, j = 0, 1, 2, 3, 4.$

7.3 Mutual Information

In this section we show that our STBC's maximize the mutual information for any number of transmit and receive antennas. Continuing the discussion of capacity from the Subsection 4.2, we have

$$\mathbf{X} = \sqrt{\frac{\rho}{n}}\mathbf{H}\mathbf{F} + \mathbf{W} \tag{18}$$

where $\mathbf{W}(r \times n)$ is the noise, $\mathbf{X}(r \times n)$ is the received matrix and $\mathbf{F}$ is our codeword matrix which is of the form given in (17). Then, we can rewrite the above equation as

$$\widehat{\mathbf{X}} = \sqrt{\frac{\rho}{n}} \underbrace{\begin{bmatrix} \mathbf{H} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{H} & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{H} \end{bmatrix}}_{\mathcal{H}} \Phi \begin{bmatrix} f_{0,0} \\ f_{0,1} \\ f_{0,2} \\ \vdots \\ \vdots \\ f_{n-1,n-1} \end{bmatrix} + \widehat{\mathbf{W}} \tag{19}$$

where $\widehat{\mathbf{X}}$ and $\widehat{\mathbf{W}}$ are $vec(\mathbf{X})$ and $vec(\mathbf{W})$ respectively ($vec(x)$ arranges all the columns of x in one column, one after another) and $\mathbf{0}$ is a $r \times n$ zero matrix. The matrix Φ is

$$\Phi = \frac{1}{\sqrt{n}} \left[\Phi_0^T \Phi_1^T \Phi_2^T \cdots \Phi_{n-1}^T\right]^T$$

where Φ_i for $i = 1, 2, \ldots, n-1$, is

$$\Phi_i = \left[\begin{array}{ccccccccc} & \text{Starts at} & & & \text{Starts at} & \text{Starts at} & \text{Starts at} & & \\ & 0^{th} \text{ col} & & & n(n-i-1)^{th} \text{ col} & n(n-i)^{th} \text{ col} & n(n-i+1)^{th} \text{ col} & & \\ & \downarrow & & & \downarrow & \downarrow & \downarrow & & \\ 0^{th} \text{ row} \rightarrow & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \delta\sigma^i(\mathbf{t}_n) & \mathbf{0} & \cdots & \mathbf{0} \\ & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \delta\sigma^i(\mathbf{t}_n) & \cdots & \mathbf{0} \\ & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \delta\sigma^i(\mathbf{t}_n) \\ i^{th} \text{ row} \rightarrow & \sigma^i(\mathbf{t}_n) & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ & \mathbf{0} & \sigma^i(\mathbf{t}_n) & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ & \mathbf{0} & \mathbf{0} & \cdots & \sigma^i(\mathbf{t}_n) & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \end{array} \right] \tag{20}$$

and $\Phi_0 = diag_n\left(\mathbf{t}_n\right)$, where $diag_n(x)$ denotes the $n \times n$ block diagonal matrix with the block x as each diagonal entry. $\mathbf{0}$ denotes the n-length zero vector, $\mathbf{t}_n$ is the vector $[1 \; t_n \; t_n^2 \; \ldots \; t_n^{n-1}]$ and $\sigma^i(\mathbf{t}_n) = \left(\sigma^i(t_n^j)\right)_{j=0}^{n-1}$. Note that Φ_is are $n \times n^2$ matrices and Φ is a $n^2 \times n^2$ matrix.

To see it more clearly, consider the STBC of Example 11. We have Φ as

$$\Phi = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & \sqrt{j} & 0 & 0 \\ 0 & 0 & 1 & \sqrt{j} \\ 0 & 0 & \delta & -\delta\sqrt{j} \\ 1 & -\sqrt{j} & 0 & 0 \end{bmatrix}$$

and for the Example 12, we have Φ as

$$\Phi = \begin{bmatrix} 1 & \omega_9 & \omega_9^2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \omega_9 & \omega_9^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \omega_9 & \omega_9^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & \delta & \delta\omega_9^4 & \delta\omega_9^8 \\ 1 & \omega_9^4 & \omega_9^8 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \omega_9^4 & \omega_9^8 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta & \delta\omega_9^7 & \delta\omega_9^5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \delta & \delta\omega_9^7 & \delta\omega_9^5 \\ 1 & \omega_9^7 & \omega_9^5 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Lemma 15. *Let K/F be a cyclic extension of degree n, where $K = F(t_n = t^{1/n})$, $t, \omega_n \in F$, $|t| = 1$ and $\sigma : t_n \mapsto \omega_n t_n$ be a generator of the Galois group. Then,*

$$\sum_{i=0}^{n-1} t_n^i \left(\sigma^k(t_n^i)\right)^* = \begin{cases} n & \textit{if } k = 0 \\ 0 & \textit{if } k \neq 0 \end{cases}$$

Proof. Note that $t^* = t^{-1}$ by the choice of t. If $k = 0$, it is trivial. So, let $k \neq 0$. Then, proving that $\sum_{i=0}^{n-1} t_n^i \left(\sigma^k(t_n^i)\right)^* = 0$ is same as proving $\sum_{i=0}^{n-1} (t_n^*)^i \left(\sigma^k(t_n^i)\right) = 0$. So, we have $\sum_{i=0}^{n-1} (t_n^*)^i \left(\sigma^k(t_n^i)\right) = \sum_{i=0}^{n-1} \left[(t_n^*)\left(\sigma^k(t_n)\right)\right]^i = \sum_{i=0}^{n-1} \left[(t_n^*)\left(\omega_n^k t_n\right)\right]^i = \sum_{i=0}^{n-1} \left(\omega_n^k\right)^i = 0.$ □

We have the following theorem

Theorem 16. *Let K/F be a cyclic extension of degree n with $K = F(t_n = t^{1/n})$, $t, \omega_n \in F, |t| = 1$ and σ be a generator of the Galois group. Let δ ($|\delta| = 1$) be a transcendental element over K. Then, the design given in (17), arising from the division algebra $(K(\delta)/F(\delta), \sigma, \delta)$, achieves the capacity. i.e., the capacity of the new channel $\mathcal{H}\Phi$ is $C(\rho, n, r)$.*

Proof. We have the capacity of the equivalent channel $\mathcal{H}\Phi$, denoted by $C_{DA}(\rho, n, r)$ (DA standing for Division algebras), as

$$C_{DA}(\rho, n, r) = \frac{1}{n} E_{\mathbf{H}} \log_2 \left(\det\left(I_{nr} + \frac{\rho}{n}(\mathcal{H}\Phi)(\mathcal{H}\Phi)^H\right)\right)$$

The factor $\frac{1}{n}$ is to compensate the n channel uses. Using the above lemma and the fact that δ lies on the unit circle, it is easy to see that $\Phi\Phi^H = I_{n^2}$. Simplifying the above, we have $C_{DA}(\rho, n, r) = \frac{1}{n} E_{\mathbf{H}} \log_2 \left(\left(\det \left(I_r + \frac{\rho}{n} \mathbf{H}\mathbf{H}^H \right) \right)^n \right) = E_{\mathbf{H}} \log_2 \left(\det \left(I_r + \frac{\rho}{n} \mathbf{H}\mathbf{H}^H \right) \right) = C(\rho, n, r)$.

□

8 Brauer's Division Algebras

We present here a different class of examples; this is a construction due to Brauer ([45], see also [39, §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 $(K/F, \sigma, \omega_l) = K \oplus zK + \oplus z^2 K + \cdots + \oplus z^{n-1} K$, where z is some symbol that satisfies the two relations given in (14), 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 ([45], [39, §2.8]) proved the following:

Theorem 17. *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 17to construct STBCs as follows. Let n and l be as above, and let α_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 $M_n(k(\alpha_1, \dots, \alpha_n))$ as in Section 6.1, we find that the set of matrices of the form (16), 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 α_1, ..., α_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 α_1, ..., α_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 [35, pp 277, Vol 1]):

Theorem 18. *(Lindemann-Weierstrass) If u_1, u_2, ..., u_n are algebraic numbers that are linearly independent over $\mathbb{Q}$, then the complex exponentials e^{u_1}, e^{u_2}, ..., 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, ..., u_n to be *real* algebraic numbers that are linearly independent over $\mathbb{Q}$ (for example, 1, $\sqrt{2}$, $\sqrt{3}$, ...). Then $ju_1, \cdots ju_n$ will also be linearly independent over $\mathbb{Q}$. Hence, we may take $\alpha_1 = e^{ju_1}$, $\alpha_2 = e^{ju_2}$, ..., $\alpha_n = e^{ju_n}$ 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 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 Decoding and Simulation results

9.1 Decoding

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

$$C = \sum_{q=1}^{Q} s_q A_q + s_q^* B_q \tag{21}$$

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 [6] 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 (1). Hence, the efficient suboptimal decoding algorithms mentioned in [6] for the general class of Linear Dispersion codes can be used to decode the codes of this paper. In particular, the sphere decoding [21] can be used effectively for decoding the STBCs obtained from both commutative and non-commutative division algebras, under some conditions on the rate and number of receive antennas. However, we can employ the generalized sphere decoder [22] for decoding STBCs for arbitrary rate and arbitrary number of receive antennas.

9.2 Simulation Results

In this section, we present the simulation results for space time block codes constructed using field extensions as well as cyclic division algebras. We also point out the performance of STBCs from cyclic division algebras in terms of how close they are to the actual capacity of the MIMO channel. We have employed the sphere decoding algorithm [21] for our simulations.

9.2.1 STBCs from field extensions

We use the rate-1 STBC $\begin{bmatrix} f_0 & jf_1 \\ f_1 & f_0 \end{bmatrix}$, with f_0, f_1 coming from 16-QAM signal set for 4 bits per channel use and from 256-QAM for 8 bits per channel use. And for rate-2 STBCs we used the one constructed in Example 6 with $f_{i,j}$ coming from 4-QAM for 4 bits per channel use and from

16-QAM for 8 bits per channel use. Figure 5 shows plots for 2 transmit and 2 receive antenna system with 4 bits per channel use. From the plot, it can be seen that the though the LD code performs at better than rate-1 code, the rate-2 code performs better than LD code at high SNRs. This is because, the LD codes are constructed to maximize the mutual information and not the diversity. And from Figure 6, it is clear that though the rate-1 code performs better than LD code only at very high SNRs, rate-2 code outperforms the LD code at medium and high SNRs. This motivates the use of high rate codes.

9.2.2 STBCs from cyclic division algebras

We use the code of Example 11 with 4 QAM and 16 QAM for 4 and 8 bits per channel use respectively. The value of δ has been arbitrarily chosen to be $e^{j0.5}$. Figure 7 shows the BER vs SNR for 2 transmit and 2 receive antennas. It can be seen that at 10^{-6} BER, STBC from division algebras outperforms the Damen's rate-2 STBC ($B_{2,\phi}$) by 0.5 dB for 4 bits per channel and by 0.75 dB for 8 bits per channel use. Comparing the BER curves corresponding to the LD code in Figure 5 and Figure 6 with the BER curves in Figure 7, we can see that our code from cyclic division algebras performs better than LD code by about 3 dB at 10^{-5} BER. From the capacity calculations of [46], it can be seen that for 4 and 8 bits per channel use, i.e., with 4 QAM and 16 QAM our code is less than 1 dB away from the capacity. Figure 8 gives the BER vs SNR for 2 transmit and 10 receive antennas. Here also, it can be seen that we outperform the Damen's rate-2 STBC by 0.25 dB for both 4 and 8 bits per channel use. In this case, our code is less than 0.25 dB away from the capacity of the channel and coincides with capacity of channel used with 4 QAM and 16 QAM as given in [46].

10 Discussion

The construction of full-rank codes using the both commutative and non-commutative division algebras have been studied. For STBCs obtained using commutative division algebras, we have studied the coding gains achieved by them and for some special cases, we have studied the capacity of these codes. We have proved that the STBCs obtained from cyclic division algebras are information lossless. Though Brauer algebra is a cyclic division algebra, the construction of STBCs from them in this paper does not give information lossless STBCs. Another construction, a lengthy and complicated one, of STBCs from Brauer division algebras which yields information lossless STBCs, is given in [43].

Some of the possible directions for further research are:

- It is shown in [6] 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. Note that we have discussed this aspect only for codes from cyclotomic extensions.
- 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.
- One of the advantages of the "twisting" by σ in (16) is that it makes the STBCs information lossless under some conditions. What are the possible advantages due to this "twisting" ? Is it possible to have simpler decoding algorithm in this case? These aspects is worth investigating further.
- It would be interesting to see how the codes constructed in this paper perform when the channel is fast fading.

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 Commun.*, vol.6, no.3, pp.311-335, 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] J.-C.Guey, M.P.Fitz, M.R.Bell and W.Y.Kuo, "Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels," *Proc. IEEE Vehicular Technology Conf.*, 1996, pp.136-140. Also in *IEEE Trans. Commun.*, vol.47, no.4, pp.527-537, April 1999.

[5] Vahid Tarokh, Nambi Seshadri and A.R.Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Inform. Theory,* vol.44, no.2, pp.744-765, March 1998.

[6] B. Hassibi and B. Hochwald, “High-rate codes that are linear in space and time,” *IEEE Trans. Inform. Theory*, vol.48, no.7, pp.1804-1824, July 2002.

[7] S. M. Alamouti, “A simple transmit diversity technique for wireless communication,” *IEEE J. on Select. Areas in Commun.*, vol.16, no.8, pp.1451-1458, Oct. 1998.

[8] Vahid Tarokh, H.Jafarkhani and A.R.Calderbank, “Space-Time block codes from orthogonal designs,” *IEEE Trans. Inform. Theory,* vol.45, pp.1456-1467, July 1999. Also “Correction to “Space-time block codes from orthogonal designs”,”*IEEE Trans. Inform. Theory*, vol. 46, no.1, p.314, Jan. 2000.

[9] G. Ganesan and P. Stoica, ”Space-time diversity using orthogonal and amicable orthogonal designs,” in *Proc. of IEEE Vehicular Technology Conf.*, 2000, pp. 2561-2564.

[10] 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.

[11] A. Roger Hammons and Hesham El Gamal, “On the theory of space-time codes for PSK modulation,” *IEEE Trans. Inform. Theory,* vol.46, no.2, pp.524-542, March 2000.

[12] Y.Liu, M.P.Fitz and O.Y.Takeshita, “A rank criterion for QAM space-time codes,”*IEEE Trans. Inform. Theory*, vol.48 no.12, pp.3062-3079, Dec. 2002

[13] B.Hassibi, B.M.Hochwald, A.Shokrollahi and W.Sweldens, “Representation theory for high-rate multiple-antenna code design,” *IEEE Trans. Inform. Theory,* vol.47, no.6, pp.2335-2367, Sept. 2001.

[14] B.Hasssibi and M.Khorrami, “Fully-diverse multiple-antenna signal constellations and fixed-point-free Lie groups,” in *Proc. IEEE Int. Symp. Information Theory (ISIT 2001)*, Washington D.C., June 2001, p.199. Download available from *http://mars.bell-labs.com.*

[15] A. Shokrollahi, “Design of unitary space-time codes from representations of SU(2),” in *Proc. IEEE. Int. Symp. Information Theory (ISIT 2001)*, Washington D.C., June 2001, p.241. Download available from *http://mars.bell-labs.com.*

[16] B.Hughes, “Optimal space-time constellations from groups,” *IEEE Trans. Inform. Theory,* vol.49, no.2, pp.401-410, Feb.2003.

[17] B.Hochwald, T.Marzetta, T.Richardson, W.Sweldens and R.Urbanke, “Systematic design of unitary space-time constellations,” *IEEE Trans. Inform. Theory,* vol.46, no.6, pp.1692-1973, Sept. 2000.

[18] B.M.Hochwald and T.L.Marzetta, “Unitary space-time modulation for multiple antenna communication in Rayleigh flat-fading,” *IEEE Trans. Inform. Theory,* vol.46, no.2, pp.543-564, March 2000.

[19] T.M.Marzetta, B.Hassibi and B.M.Hochwald, “Structured unitary space-time auto-coding constellations,” *IEEE Trans. Inform. Theory*, vol.48, no.4, pp.942-950, Apr. 2002.

[20] B.M.Hochwald and M.Sweldens, “Differential unitary space-time modulation,” *IEEE Trans. Commun.*, vol.48, no.12, pp.2041-2052 , Dec. 2000.

[21] M.O.Damen, A.Chkeif and J.-C.Belfiore, “Lattice codes decoder for space-time codes,” *IEEE Commun. Lett*, vol.4, pp.161-163, May 2000.

[22] M.O.Damen, K.Abed-Meraim and J.-C.Belfiore, “A generalized sphere decoder for asymmetrical space-time communication architecture,” *IEE Electron. Lett.*, p.166, Jan. 2000.

[23] H. Jafarkhani,“A quasi-orthogonal space-time block code,” *ÌEEE Trans. Commun.*, vol.49, no.1, pp.1-4, Jan. 2001.

[24] Weifung-Su and Xiang-Gen Xia, “Quasi-orthogonal space-time block codes with full Diversity,” in *Proc. IEEE GLOBECOM*, vol.2, 2002, pp.1098-1102.

[25] Olav Tirkkonen and Ari Hottinen, “Complex space-time block codes for four Tx antennas,” in *Proc. IEEE GLOBECOM*, vol.2, 2000, pp.1005-1009.

[26] Naresh Sharma and C.B.Papadias, “Improved quasi-orthogonal Codes,” in *Proc. IEEE Wireless Communications and Networking Conference (WCNC 2002),* March 17-21, vol.1, pp.169-171.

[27] Zafar Ali Khan and B.Sundar Rajan, “ Space-time block codes from co-ordinate interleaved orthogonal designs,” in *Proc. IEEE Int. Symp. Information Theory (ISIT 2002)*, Lausanne, Switzerland, June 2002, p.275.

[28] Zafar Ali Khan, B.Sundar Rajan and Moon Ho Lee, “ On single-symbol and double-symbol decodbale designs,” in *Proc. IEEE Int. Symp. Information Theory (ISIT 2003)*, Yokohama, Japan, June 29-July 4, p.127.

[29] Weifung Su and Xiang-Gen Xia, “Two generalized complex orthogonal space-time block codes of rates 7/11 and 3/5 for 5 and 6 transmit antennas”, *IEEE Trans. Inform. Theory*, vol.49, no.1, pp.313 -316, Jan. 2003.

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

[31] Hesham El Gamal and M.O.Damen, “Universal space-time coding,”, *IEEE Trans. Inform. Theory*, vol.49, no.5, pp.1097-1119, May 2003.

[32] M.O.Damen, Ahmed Tewfik and J-C.Belfiore, “A construction of a space-time code based on number theory”, *IEEE Trans. Inform. Theory*, vol.48, no.3, pp.753-760, Mar.2002.

[33] S.Galliou and J-C.Belfiore, “A new family of full rate fully diverse space-time codes based on Galois theory”, in *Proc. IEEE Int. Symp. Information Theory (ISIT 2002)*, Lausanne, Switzerland, 2002, p.419.

[34] Y.Xin, Z.Wang and G.B.Giannakis, “Space-time constellation-rotating codes maximizing diversity and coding gains,” in *Proc. IEEE GLOBECOM*, vol.1, 2001, pp.455-459.

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

[36] V.Shashidhar, K.Subrahmanyam, R.Chandrasekharan, B.Sundar Rajan and B.A.Sethuraman, “High-rate, full-diversity STBCs from field extensions”, in *Proc. IEEE Int. Symp. Information Theory (ISIT 2003)*, Yokohama, Japan, June 29-July 4, p.126.

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

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

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

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

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

[42] V.Shashidhar, B.Sundar Rajan and B.A.Sethuraman,“STBCs using capacity achieving designs from cyclic division algebras”, accepted for presentation at Communication Theory Symoposium, GLOBECOM 2003, San Francisco.

[43] V.Shashidhar, B.Sundar Rajan and B.A.Sethuraman,“Space-time block codes from division algebras”, manuscript under preparation.

[44] Paul J. McCarthy, *Algebraic extensions of fields*, Dover Publications Inc., New York.

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

[46] Bertrand M.Hochwald and Stephan ten Brink , “Achieving near-capacity on a multiple-antenna channel,” Mathematical Science Research Center, Bell labs, Lucent technologies, Download available from *http://mars.bell-labs.com.*

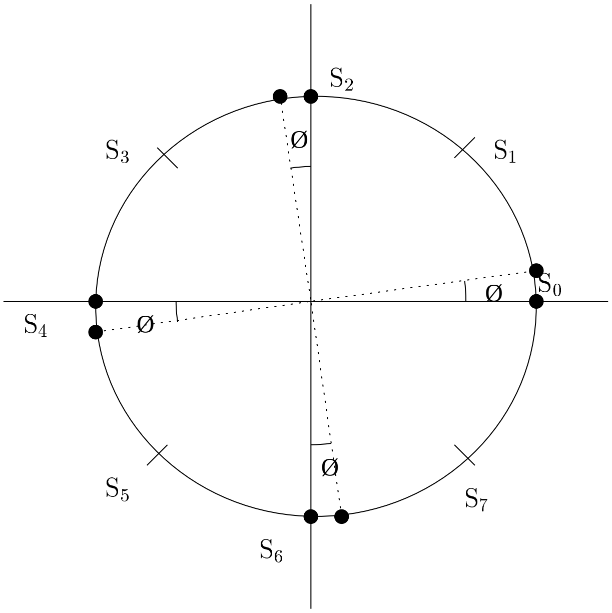

Figure 1: Asymmetric 8-PSK signal set matched to a dihedral group with 8 elements

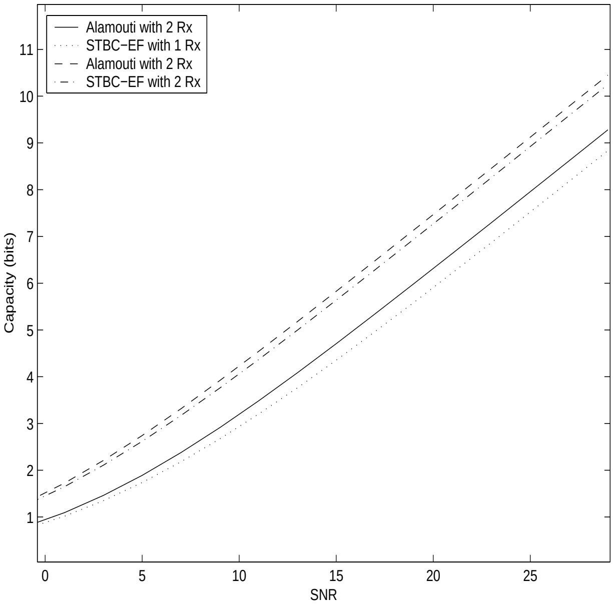

Figure 3: Capacity of the Alamouti code and of the 2×2 STBC of Example 1 as a function of SNR

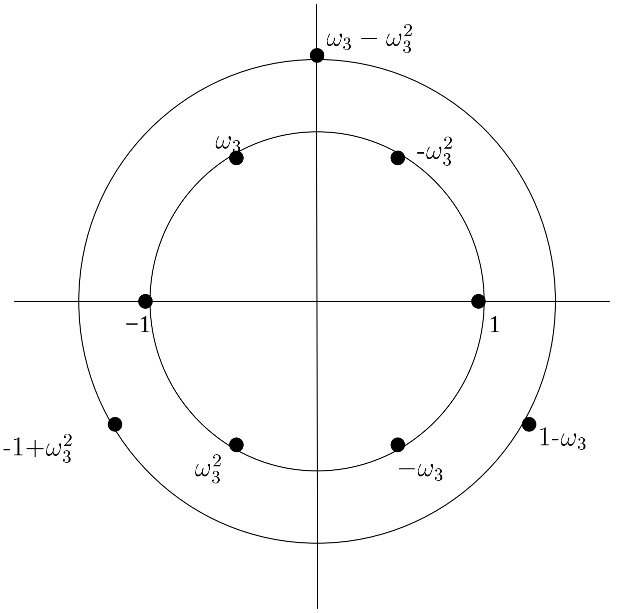

Figure 2: Double-PSK constellation

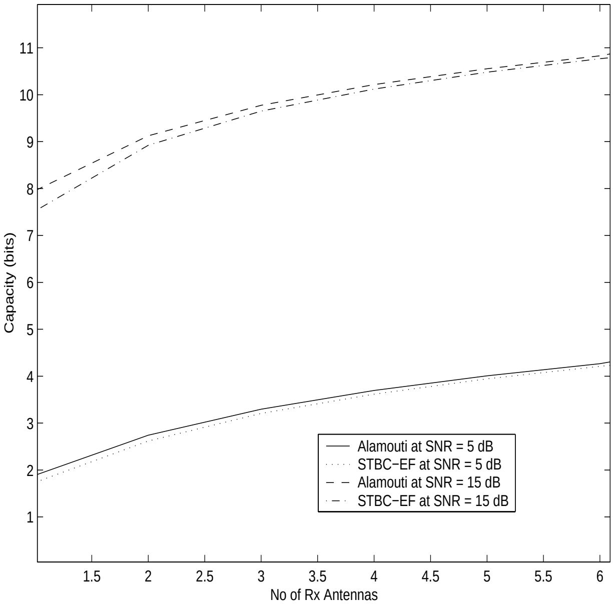

Figure 4: Capacity of the Alamouti code and of the 2×2 STBC of Example 1 as a function of Rx Antennas for two values of SNR

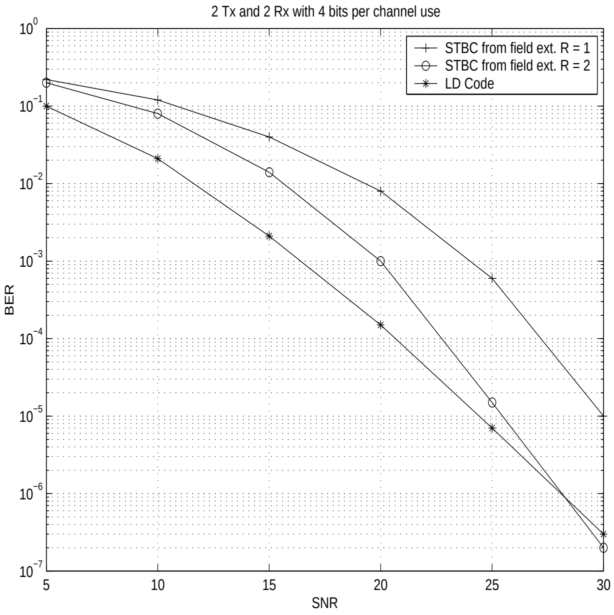

Figure 5: Comparison of STBCs from field extensions with LD codes for 2-Tx and 2-Rx with 4 bits per channel use.

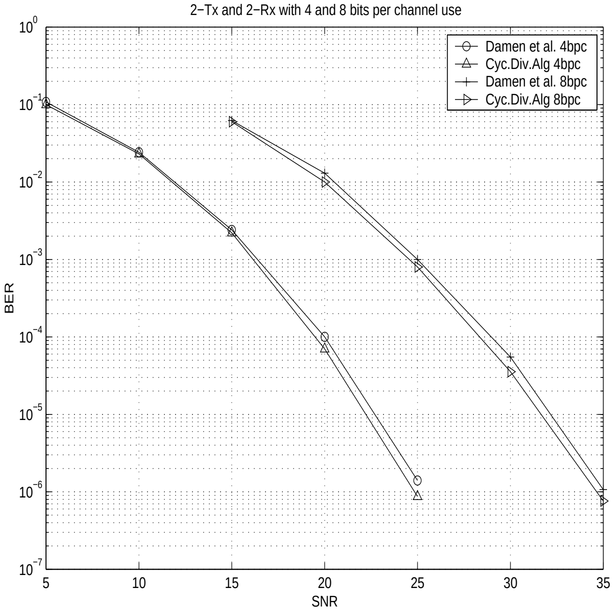

Figure 7: Comparison of STBCs from cyclic division algebras with Damen et al. code with 4 and 8 bits per channel use.

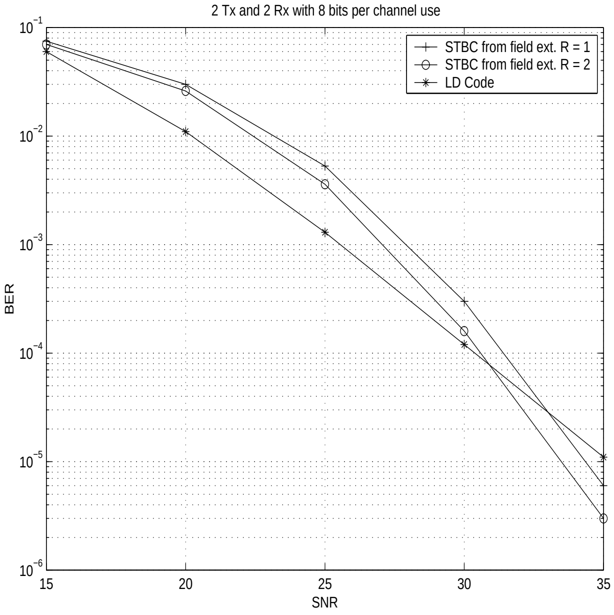

Figure 6: Comparison of STBCs from field extensions with LD codes for 2-Tx and 2-Rx with 8 bitsper channel use.

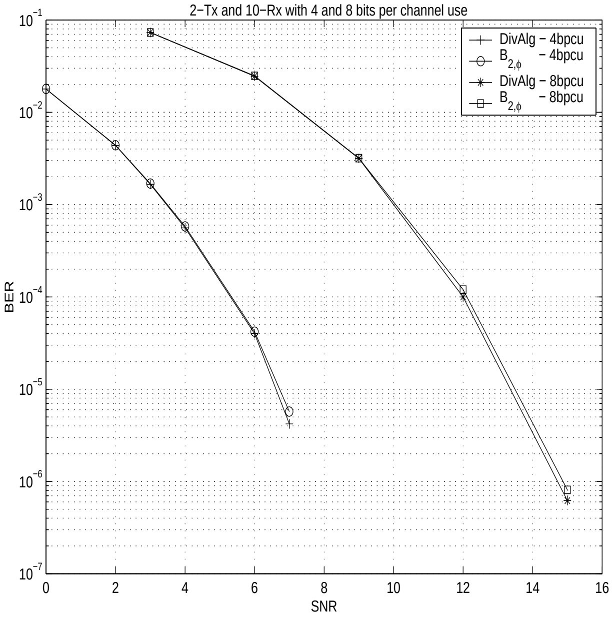

Figure 8: Comparison of STBCs from cyclic division algebras with Damen et al. code with 4 and 8 bits per channel use.