STBCs using Capacity Achieving Designs from Cyclic Division Algebras

Shashidhar V
ECE Department
Indian Institute of Science
Bangalore - 560012 INDIA
Email: shashidhar@protocol.ece.iisc.ernet.in

B.Sundar Rajan
ECE Department
Indian Institute of Science
Bangalore - 560012 INDIA
Email: bsrajan@ece.iisc.ernet.in

B.A.Sethuraman
Dept. of Mathematics
California State University, Northridge
CA 91330, USA
Email:al.sethuraman@csun.edu

***Abstract*— It is known that the Alamouti code is the only complex orthogonal design (COD) which achieves capacity and that too for the case of two transmit and one receive antenna only. Damen *et al.*, gave a design for 2 transmit antennas, which achieves capacity for any number of receive antennas, calling it *an information lossless STBC*. In this paper, we construct capacity achieving designs using cyclic division algebras for arbitrary number of transmit and receive antennas. For the STBCs obtained using these designs we present simulation results for those number of transmit and receive antennas for which Damen *et al.* also give and show that our STBCs perform better than their's.**

I. Introduction

A Space-Time Block Code (STBC) $\mathcal{C}$ over a complex signal set S, for n transmit antennas, is a finite set of $n \times l$, $(n \leq l)$ matrices with entries from S or complex linear combination of the elements of S and their complex conjugates. An important performance criteria for $\mathcal{C}$ is the minimum of ranks of difference of any two codewords ($n \times l$ matrices) of $\mathcal{C}$, called the rank of $\mathcal{C}$. The code $\mathcal{C}$ is said to be of full-rank if the rank is n and minimal delay if $n = l$. We call $\mathcal{C}$, a rate-R (in complex symbols per channel use) STBC, where $R = \frac{1}{l}\log_{|S|}|\mathcal{C}|$.

A rate-k/n, $n \times n$ design over a field F, is an $n \times n$ matrix with entries as functions of k variables which are allowed to take values from the field F. If we restrict the k variables to take values from a finite subset of F, we get a STBC over that finite subset. For example, the Alamouti code [1] is a rate-1 design over the complex field $\mathbb{C}$, where the entries are functions of two variables and we get a STBC when we restrict these two variables to some finite set, say QAM or PSK signal set. Similarly, the 4×4 real orthogonal design is a design over the real field. Complex Orthogonal Designs and their variations have been extensively studied in [2]–[6]. In the next section we construct rate-n, $n \times n$ designs over subfields F of the complex field $\mathbb{C}$ and obtain full-rank, rate-n STBCs over finite subsets of F.

In [7], it is shown that among the orthogonal designs, the Alamouti code is the only one which maximizes the mutual information and that too only for one receive antenna only. In the same paper, codes called Linear-Dispersion codes that have maximum mutual information are constructed by solving a nonlinear optimization problem using gradient approach. For less number of transmit and receive antennas, the mutual information of their codes is very close to the actual channel capacity, but as the number of antennas increase, the difference increases. Damen *et al.*, in [8], have proposed a STBC for 2 transmit antennas, which maximizes the mutual information for any number of receive antennas. However, this STBC is of full-rank only over QAM signal constellations. In [9], iterative decoding techniques are used to achieve near-capacity performance on a multiple-antenna system. Galliou and Belfiore, in [10], have constructed full rate, fully diverse STBCs for QAM constellations only using Galois theory, and claim that these codes maximize mutual information.

In this paper we present **capacity achieving designs** (*information lossless*) for **arbitrary number of transmit and receive antennas** using division algebras for any **a priori specified arbitrary complex constellation**. Familiarity with prior results obtained using division algebras available in [11]–[15] will be helpful (in particular, in [13] it is shown that the Alamouti code is obtainable using division algebra and has certain algebraic uniqueness). However, the presentation in this paper is self-contained.

II. Main Principle

A division ring D is a ring in which every nonzero element has an inverse. Let F be the center of the division ring D. Then F is a field, and D is an algebra over F and hence D is also called an F-division algebra. The vector space dimension of D over F is called the degree of the division algebra, and is denoted $[D : F]$. It is well known that when $[D : F]$ is finite, it is always a perfect square [16]. The square root of $[D : F]$ is called the index of D. By a subfield K of D, we mean a field K such that $F \subset K \subset D$. Let $[D : F] = n^2$ and K be a maximal subfield of D. Then, it is well known that $[K : F] = n$, the index of the division algebra D. We call D a cyclic division algebra if it has some maximal subfield K such that K/F is a cyclic extension. For examples of division algebras see [13], [15].

Throughout this paper we consider cyclic division algebras to construct our STBCs. Let D be a cyclic division algebra

[1]This work was partly funded by the DRDO-IISc Program on Mathematical Engineering through a grant to B.S.Rajan.

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

with center F, of index n, and with maximal cyclic subfield K. Let the Galois group $G_{K/F}$ be generated by σ, so $\sigma^n = 1$. We have the following well known decomposition of D [16]:

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

where z is some element of D which satisfies the relations

$$\begin{aligned} kz &= z\sigma(k) \ \ \forall k \in K & (2) \\ z^n &= \delta, \text{ for some } \delta \in F^* & (3) \end{aligned}$$

where F^* is the set $F\backslash\{0\}$ and z^iK denotes the set $\{z^ik | k \in K\}$. Then, we have the following theorem proved in [13], [15].

Theorem 1: Any finite set of matrices of the form

$$\begin{bmatrix} k_0 & \delta\sigma(k_{n-1}) & \delta\sigma^2(k_{n-2}) & \cdots & \delta\sigma^{n-1}(k_1) \\ k_1 & \sigma(k_0) & \delta\sigma^2(k_{n-1}) & \cdots & \delta\sigma^{n-1}(k_2) \\ k_2 & \sigma(k_1) & \sigma^2(k_0) & \cdots & \delta\sigma^{n-1}(k_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{n-1} & \sigma(k_{n-2}) & \sigma^2(k_{n-3}) & \cdots & \sigma^{n-1}(k_0) \end{bmatrix} \tag{4}$$

where $k_i \in K$, for $i = 0, 1, \ldots, n-1$, has the property that the difference of any two matrices has full rank.

From the above theorem, it is clear that we get full-rank, rate-one STBCs for n antennas, over any finite subset of K. If we write every k_i in the matrix of (4) as an F-linear combination of some fixed basis of K, we get a full-rank, rate-n STBC over any finite subset of F. Equation (1) gives an example of such codewords in the special case when K has an F-basis the set $\{1, t, t^2, \ldots, t^{n-1}\}$ for some $t \in K^*$. Here, $f_{i,j} \in S \subset F$, for $i, j = 0, 1, \ldots, n-1$, where S is some finite subset of F.

In the rest of this section, we will construct a class of cyclic division algebras which will give us full-rank, rate-n STBCs for any, n, number of transmit antennas.

Let F be a field and K an extension of F, such that $[K : F] = n$. Also, let the extension K/F be a cyclic extension, i.e., the Galois group of the extension be a cyclic group generated by some σ. Let δ be a transcendental element over K. Then, $K(\delta)/F(\delta)$ is also cyclic, with σ acting as identity on δ. Consider the following algebra:

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

where z is some symbol which satisfies the relations

$$kz = z\sigma(k) \text{ for all } k \in K \text{ and } z^n = \delta.$$

The above algebra has $F(\delta)$ as its center, $K(\delta)$ as a maximal subfield and has no nontrivial two sided ideals, but it is not a priori obvious that it is a division algebra. However, from [13], [15], we have the following theorem.

Theorem 2: With F, K, n, z, δ and σ as above, the algebra $D = (K(\delta)/F(\delta), \sigma, \delta)$ is a cyclic division algebra.

We will always assume that δ lies on the unit circle and since there are infinite transcendental numbers on the unit circle (e^{ju} lies on the unit circle and is transcendental for any algebraic u [17]), we always have at least one such δ. Henceforth, we will assume δ to be such transcendental element over K unless specified explicitly. So, the task now is to construct the field $F(\delta)$ and its cyclic extension $K(\delta)$, where δ is a transcendental element over K. To do this, we use the following theorem from [18].

Theorem 3: 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 subsection, we use some algebraic extensions of the field of rational numbers, $\mathbb{Q}$ to construct designs and in the next section we show that these designs achieve capacity. In Section III, we present simulation results for the STBCs obtained from these designs and compare with the known curves.

A. STBCs from algebraic extensions of $\mathbb{Q}$

Throughout, ω_k stands for $e^{2\pi j/k}$, a primitive k-th root of unity. Let S be the signal set of interest, i.e., we want STBCs over S. Then, we take $F = \mathbb{Q}(S, \omega_m)$, 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 primitive n^{th} root of unity. Let $K = F(\omega_{mn})$. To be able to use Theorem 3 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 3 K/F is a cyclic extension. We give some examples to illustrate the above construction.

Example 1: 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 $\sigma : \sqrt{j} \mapsto -\sqrt{j}$. Then, $(K(\delta)/F(\delta), \sigma, \delta)$ is a cyclic division algebra. Thus, we have the STBC $\mathcal{C}$ given by

$$\mathcal{C} = \left\{ \left[\begin{array}{cc} k_0 & \delta\sigma(k_1) \\ k_1 & \sigma(k_0) \end{array} \right] | k_0, k_1 \in K \right\}.$$

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

$$\frac{1}{\sqrt{2}} \left[\begin{array}{cc} f_{0,0} + f_{0,1}\sqrt{j} & \delta\sigma(f_{1,0} + f_{1,1}\sqrt{j}) \\ f_{1,0} + f_{1,1}\sqrt{j} & \sigma(f_{0,0} + f_{0,1}\sqrt{j}) \end{array} \right] =$$
$$\frac{1}{\sqrt{2}} \left[\begin{array}{cc} f_{0,0} + f_{0,1}\sqrt{j} & \delta(f_{1,0} - f_{1,1}\sqrt{j}) \\ f_{1,0} + f_{1,1}\sqrt{j} & (f_{0,0} - f_{0,1}\sqrt{j}) \end{array} \right]$$

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. Note that from Theorem 1, the STBC with codewords as above is of full-rank over any finite subset of F.

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 [8]. 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 [8] is of full-rank for QAM constellations, as is the case with our code. However, we get STBCs 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 2: 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. Then, $(K(\delta)/F(\delta), \sigma, \delta)$ is a cyclic division algebra. Thus, we have a full-rank STBC $\mathcal{C}$ with codewords as follows (obtained in a similar way as in the previous example)

$$\frac{1}{\sqrt{3}} \left[\begin{array}{ccc} g_{0,0} & \delta g_{1,2} & \delta g_{2,1} \\ g_{0,1} & g_{1,0} & \delta g_{2,2} \\ g_{0,2} & g_{1,1} & g_{2,0} \end{array} \right]$$

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 $i, j = 0, 1, 2$.

B. STBCs from transcendental extensions of $\mathbb{Q}$

In the last subsection, we have seen that the STBC constructions depend on the signal set and the number of antennas, which affects the coding gain of the STBCs. In this subsection, we use transcendental extensions of $\mathbb{Q}$ to overcome this restriction to a large extent. First, we have the following corollary to Theorem 3.

Corollary 1: 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 [15]. So, the difficulty of finding an irreducible polynomial over F of degree n is overcome. Notice that the selection of t still depends on the signal set S, but this dependence is of little effect as there are infinite transcendental elements over $\mathbb{Q}$ and S is a finite signal set. However, in the case when F is an algebraic extension of $\mathbb{Q}$, any transcendental number is a valid δ, i.e., any transcendental number is a transcendental element over K. But in the case when F is a transcendental extension of $\mathbb{Q}$, any transcendental number need not be a valid δ. The value δ can take now is that of a transcendental number algebraically independent of t. But this restriction is very small, as there are infinite transcendental numbers and any two transcendental numbers of the form e^{ju_1} and e^{ju_2} are algebraically independent if u_1 and u_2 are algebraic numbers that are linearly independent over $\mathbb{Q}$.

Using the above corollary, we give some examples.

Example 3: 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 $\sigma : t_2 \mapsto -t_2$. Then, $(K(\delta)/F(\delta), \sigma, \delta)$ is a cyclic division algebra. Thus, we have a full-rank STBC $\mathcal{C}$ with the codewords as follows (obtained in a similar way as in the previous examples):

$$\frac{1}{\sqrt{2}} \left[\begin{array}{cc} f_{0,0} + f_{0,1}t_2 & \delta\sigma(f_{1,0} + f_{1,1}t_2) \\ f_{1,0} + f_{1,1}t_2 & \sigma(f_{0,0} + f_{0,1}t_2) \end{array} \right]$$
$$= \frac{1}{\sqrt{2}} \left[\begin{array}{cc} f_{0,0} + f_{0,1}t_2 & \delta(f_{1,0} - f_{1,1}t_2) \\ f_{1,0} + f_{1,1}t_2 & (f_{0,0} - f_{0,1}t_2) \end{array} \right]$$

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

In the STBC of the above example, we have two degrees of freedom, namely t and δ. On the other hand the STBC of Example 1 has only one degree of freedom, namely δ. Thus, the STBC of the above example will have a coding gain at least that of the STBC obtained in Example 1. This is another advantage of using the transcendental extensions of $\mathbb{Q}$ for obtaining STBCs.

Example 4: Let $n = 4$ and S be the signal set. Then, with $F = \mathbb{Q}(\omega_4 = j, S, t)$ and $K = F(t_4 = t^{1/4})$, we have K/F cyclic and $\sigma : t_4 \mapsto jt_4$ is a generator of the Galois group.

$$
\Phi_i = \left[\begin{array}{ccccccccc}
 & \begin{matrix}\text{Starts at}\\ 0^{th}\text{ col}\\ \downarrow\end{matrix} & & & \begin{matrix}\text{Starts at}\\ n(n-i-1)^{th}\text{ col}\\ \downarrow\end{matrix} & \begin{matrix}\text{Starts at}\\ n(n-i)^{th}\text{ col}\\ \downarrow\end{matrix} & \begin{matrix}\text{Starts at}\\ n(n-i+1)^{th}\text{ col}\\ \downarrow\end{matrix} & & \\
0^{th}\text{ row} \rightarrow & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \delta\sigma^i(\mathbf{t}_n) & \mathbf{0} & \cdots & \mathbf{0} \\
 & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \delta\sigma^i(\mathbf{t}_n) & \cdots & \mathbf{0} \\
 & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
 & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \delta\sigma^i(\mathbf{t}_n) \\
i^{th}\text{ row} \rightarrow & \sigma^i(\mathbf{t}_n) & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\
 & \mathbf{0} & \sigma^i(\mathbf{t}_n) & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\
 & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
 & \mathbf{0} & \mathbf{0} & \cdots & \sigma^i(\mathbf{t}_n) & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0}
\end{array}\right] \tag{5}
$$

Thus, we have a full-rank STBC for 4 antennas as follows :

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

where $g_{i,j} = \sum_{l=0}^{3} f_{j,l}(j^i t_4)^l$ and $f_{i,j} \in S \subset F$ for $i,j = 0,1,2,3$.

Example 5: 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 thus, we have a full-rank 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 $i,j = 0,1,2,3,4$.

III. Mutual Information

In this section we show that our STBCs maximize the mutual information for any number of transmit and receive antennas. Let n be the number of transmit antennas and r be the number of receive antennas. Then, at any given channel use, we have

$$
\mathbf{x} = \sqrt{\frac{\rho}{n}}\mathbf{H}\mathbf{f} + \mathbf{w}
$$

where $\mathbf{H}$ ($r \times n$ matrix) is the channel matrix, $\mathbf{w}(r \times 1)$ is the noise, $\mathbf{f}$ is the transmitted signal vector and $\mathbf{X}(r \times 1)$ is the received vector. The entries of $\mathbf{H}$ and $\mathbf{w}$ are complex Gaussian iid with zero mean and unit variance. The transmitted signal vector $\mathbf{f}$ is such that the average power transmitted in a channel use is equal to n, i.e., $E(f^H f) = n$. And ρ is the signal to noise ratio at each receive antenna. Then, the capacity of the channel is given as [7], [19], [20]

$$
C(\rho, n, r) = E_{\mathbf{H}} \log_2 \left(\det \left(I_r + \frac{\rho}{n}\mathbf{H}\mathbf{H}^H \right) \right). \tag{6}
$$

The above equation is obtained by assuming that for any two channel uses, the transmitted vectors are independent of each other. On the other hand when we use our STBCs, we have the transmitted vectors in the n channel uses dependent on each other (this is because of coding). So, we have

$$
\mathbf{X} = \sqrt{\frac{\rho}{n}}\mathbf{H}\mathbf{F} + \mathbf{W} \tag{7}
$$

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 (1). These codeword matrices are again normalized such that $E\left(tr(F^H F)\right) = n^2$. Then, we can rewrite the above equation as

$$
\widehat{\mathbf{X}} = \sqrt{\frac{\rho}{n}} \underbrace{\begin{bmatrix} \mathbf{H} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{H} & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{H} \end{bmatrix}}_{\mathcal{H}} \Phi \begin{bmatrix} f_{0,0} \\ f_{0,1} \\ f_{0,2} \\ \vdots \\ \vdots \\ f_{n-1,n-1} \end{bmatrix} + \widehat{\mathbf{W}} \tag{8}
$$

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 an $r \times n$ 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 shown in (5) and $\Phi_0 = diag_n(\mathbf{t}_n)$, where $diag_n(x)$ denotes the $n \times n$ block diagonal matrix with the block x as each diagonal entry. The symbol $\mathbf{0}$ denotes the n-length zero vector, $\mathbf{t}_n$ is the vector $[1 \; t_n \; t_n^2 \; \ldots \; t_n^{n-1}]$ and $\sigma^i(\mathbf{t}_n)$ is the vector $\left(\sigma^i(t_n^j)\right)_{j=0}^{n-1}$. Note that Φ_is are $n \times n^2$ matrices and Φ is an $n^2 \times n^2$ matrix.

To see it more clearly, consider the STBC of Example 1. 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 STBC of Example 2, we have Φ as

$$
\Phi = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & \omega_9 & \omega_9^2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \omega_9 & \omega_9^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \omega_9 & \omega_9^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & \delta & \delta\omega_9^4 & \delta\omega_9^8 \\ 1 & \omega_9^4 & \omega_9^8 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \omega_9^4 & \omega_9^8 & 0 & 0 & 0 \\ 0 & 0 & 0 & \delta & \delta\omega_9^7 & \delta\omega_9^5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \delta & \delta\omega_9^7 & \delta\omega_9^5 \\ 1 & \omega_9^7 & \omega_9^5 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.
$$

Lemma 1: 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,

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

Proof: Note that $t^* = t^{-1}$ by the choice of t. The case $k = 0$ 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 the same as proving $\sum_{i=0}^{n-1} (t_n^*)^i \left(\sigma^k(t_n^i)\right) = 0$. So, we have

$$\begin{aligned} \sum_{i=0}^{n-1} (t_n^*)^i \left(\sigma^k(t_n^i)\right) &= \sum_{i=0}^{n-1} \left[(t_n^*)\left(\sigma^k(t_n)\right)\right]^i \\ &= \sum_{i=0}^{n-1} \left[(t_n^*)\left(\omega_n^k t_n\right)\right]^i \\ &= \sum_{i=0}^{n-1} \left(\omega_n^k\right)^i = 0. \end{aligned}$$

■

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. And we call a STBC described with such design an information lossless STBC [8]. Then, we have the following theorem:

Theorem 4: 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 (1), 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: According to (6), 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 Lemma 1 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

$$\begin{aligned} C_{DA}(\rho, n, r) &= \frac{1}{n} E_{\mathbf{H}} \log_2 \left(\left(\det \left(I_r + \frac{\rho}{n} \mathbf{H}\mathbf{H}^H \right) \right)^n \right) \\ &= E_{\mathbf{H}} \log_2 \left(\det \left(I_r + \frac{\rho}{n} \mathbf{H}\mathbf{H}^H \right) \right) \\ &= C(\rho, n, r). \end{aligned}$$

■

From the above theorem, it is clear that the STBCs with $|t| = |\delta| = 1$ of Examples 1, 2, 3, 4 and 5 are information lossless.

IV. Simulation Results

The channel is modeled as in (7). We present simulation results for the following cases: (i) 2 transmit and 2 receive antennas with 4 and 8 bits per channel use, (ii) 2 transmit and 10 receive antennas with 4 and 8 bits per channel use and (iii) 4 transmit and 4 receive antennas with 8 and 16 bits channel use. We have used sphere decoding algorithm [21] at the receiver.

For the two 2-transmit antenna cases we use the STBC of Example 1 with 4 QAM and 16 QAM for 4 and 8 bits per channel use respectively. The value of δ is arbitrarily chosen to be $e^{j0.5}$.

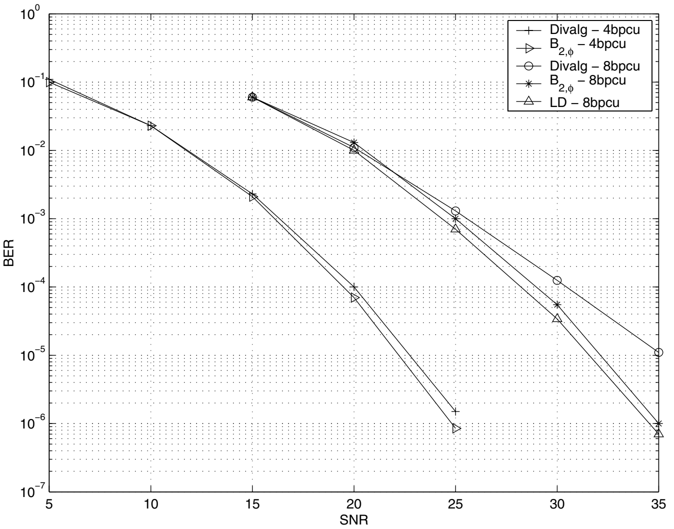

Fig. 1. Comparison of STBCs from Division algebras with Damen's rate-2 STBC and LD code from [7], for 2 transmit and 2 receive antennas

Figure 1 shows the BER vs SNR for 2 transmit and 2 receive antennas. It can be seen that at 10^{-6} BER, the 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. We also compare our code with the Linear Dispersion code in [7], obtained by maximizing the mutual information for 8 bits per channel use. It can be seen that at 8 bits per channel use, our code outperforms the LD code by

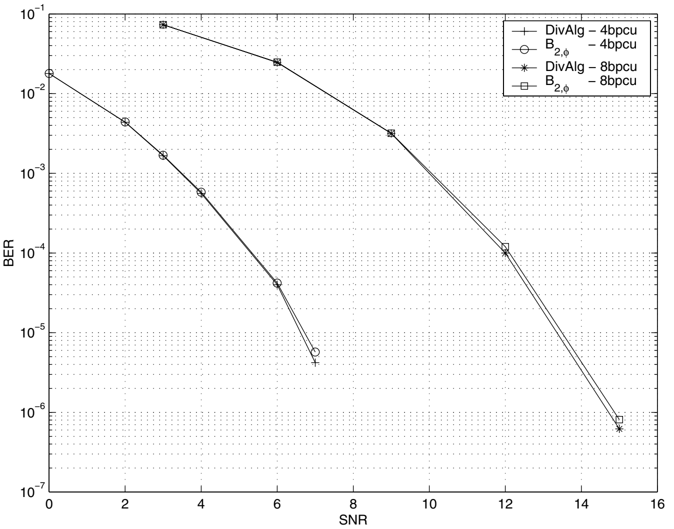

Fig. 2. Comparison of STBCs from Division algebras with Damen's rate-2 STBC, for 2 transmit and 10 receive antennas

about 4dB at BER of 10^{-5}. From the capacity calculations of [9], 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 of the channel with QAM as the input.

Figure 2 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 the capacity of the channel used with 4 QAM and 16 QAM as given in [9].

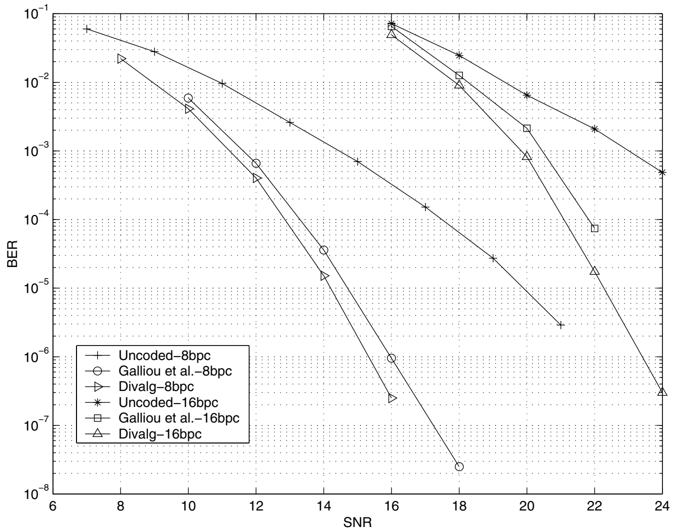

Fig. 3. Comparison of STBCs from Division algebras with Galliou's STBC, for 4 transmit and 4 receive antennas

Figure 3 shows the BER vs SNR for 4 transmit and 4 receive antennas with 8 and 16 bits per channel use. We have used the STBC of Example 4 with 4-QAM and 16-QAM for 8 and 16 bits per channel use respectively. We compare the performance of our STBC with uncoded case and the STBC obatained by Galliou *et al.* in [10] which is claimed to maximize the mutual information. For 8 bits per channel use, we can see that our STBC performs better than uncoded case by 6 dB and by 0.5 dB better than the STBC of Galliou *et al.* [10] at 10^{-5} BER. Similarly, for 16 bits per channel use our code performs better than the STBC of Galliou *et al.* by 0.75 dB at 10^{-4} BER.

V. Discussion

Using division algebras, we have constructed full-rank STBCs over any signal set S for any number of transmit antennas and have given two instances of these STBCs which are less than 1 dB away from the channel capacity. Simulations show that our STBCs outperform the Damen's rate-2 STBC of [8] by about 0.5dB at 10^{-5} BER and Galliou's STBC of [10] by about 0.75 dB at 10^{-5} BER. We can perform much better by choosing the δ and t to maximize the coding gain. One possible direction for further research is to see if there are any other cyclic division algebras which will yeild information lossless STBCs with better performance. Also one could try to obtain a closed form expression for the coding gain of the STBCs obtained in this paper.

References

[1] 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.

[2] 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.

[3] O. Tirkonen and A. Hottinen, "Square-matrix embeddable space=time block codes for complex signal constellations," *IEEE Trans. Inform. Theory*, vol.48, no.2, Feb. 2002.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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*.

[10] 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.

[11] B. A. Sethuraman and B. Sundar Rajan, "Optimal STBC over PSK Signal Sets from Cyclotomic Field Extensions," in *Proc. IEEE Int. Conf. Comm.(ICC 2002)*, April 28- May 2, New York City, U.S.A., vol.3, pp.1783-1787.

[12] B. A. Sethuraman and B. Sundar Rajan, "STBC from Field Extensions of the Rational Field," in *Proc. IEEE Int. Symp. Inform. Theory,(ISIT 2002)*, Lausanne, Switzerland, June 30-July 5, 2002, p.274.

[13] B. A. Sethuraman and B. Sundar Rajan, "An Algebraic Description of Orthogonal Designs and the Uniqueness of the Alamouti Code," in *Proc. IEEE GLOBECOM 2002*, Taipai, Nov. 17-21,2002, pp.1088-1092.

[14] 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.

[15] B. Sethuraman, B. Sundar Rajan and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," to appear in the forthcoming special issue of IEEE Trans. Inform. Theory. Available for download at *http://ece.iisc.ernet.in/˜bsrajan.*

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

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

[18] Paul J. McCarthy, *Algebraic extensions of fields*, Dover Publications Inc., New York, 1991.

[19] 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.

[20] 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.

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