STBCs using Capacity Achieving Designs from Crossed-Product Division Algebras

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

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

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

***Abstract*— We construct full-rank, rate-n Space-Time Block Codes (STBC), over any a priori specified signal set for n-transmit antennas using crossed-product division algebras and give a sufficient condition for these STBCs to be information lossless. A class of division algebras for which this sufficient condition is satisfied is identified. Simulation results are presented to show that STBCs constructed in this paper perform better than the best known codes, including those constructed from cyclic division algebras and also to show that they are very close to the capacity of the channel with QAM input.**

I. Introduction and Preliminaries

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 combinations of elements of S and their conjugates. An important performance criteria for $\mathcal{C}$, when used for a quasi-static flat fading channel, 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 STBC $\mathcal{C}$ 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 $R = \frac{1}{l}\log_{|S|}|\mathcal{C}|$. Almost all the STBCs studied in the literature so far are obtained from *designs* defined below:

Definition 1: An $n \times n$ design in k variables over a subfield F of the complex field $\mathbb{C}$ is a $n \times n$ matrix with entries that are complex linear combinations of the k variables and their complex conjugates, which are allowed to take values from the field F. If we restrict the variables to take values from a finite subset $S \subset F$, then the resulting STBC is said to be a rate-k/n linear STBC over S.

Designs over the real number field $\mathbb{R}$ and over $\mathbb{C}$ have been studied in [1] and the well known Alamouti code [2] is based on the design $\begin{bmatrix} x_0 & x_1 \\ -x_1^* & x_0^* \end{bmatrix}$ which is a rate-1, 2×2 design over $\mathbb{C}$. Designs over subfields of $\mathbb{C}$ that are neither $\mathbb{R}$ nor $\mathbb{C}$ have been studied in [3]–[8]. From now on, we describe an STBC $\mathcal{C}$ by giving the underlying design and the signal set S. Notice that the "design along with the signal set" is a compact way of describing the STBC. Thus Alamouti code is a rate-1 2×2 STBC for any complex signal set S.

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

Let n and r be the number of transmit and receive antennas respectively. Then, if $\mathbf{H} \in \mathbb{C}^{r\times n}$ is the channel matrix whose entries are iid with zero-mean, unit-variance, complex Gaussian and if the transmitted $n \times l$ matrix over l time instants is $\mathbf{S}$, then we have

$$\mathbf{X} = \sqrt{\frac{\rho}{n}}\mathbf{HS} + \mathbf{W} \tag{1}$$

where $\mathbf{X}$, $\mathbf{W}$ are the received $(r \times l)$ and additive noise $(r \times l)$ matrices respectively and ρ is the signal to noise ratio (SNR) at each receive antenna. Let the STBC used in the above equation be of rate R symbols per channel use. Then, we will have lR independent variables describing the matrix $\mathbf{S}$. Let us denote them by $f_1, f_2, \ldots, f_{lR}$ and let $\mathbf{f} = [f_1, f_2, \ldots, f_{lR}]^T$. Suppose that we can rewrite (1) as

$$\widehat{\mathbf{x}} = \sqrt{\frac{\rho}{n}}\widehat{\mathbf{H}}\mathbf{f} + \widehat{\mathbf{w}} \tag{2}$$

where $\widehat{\mathbf{x}}$ and $\widehat{\mathbf{w}}$ are the matrices $\mathbf{X}$ and $\mathbf{W}$, respectively, arranged in a single column, by serializing the columns. The maximum mutual information between the information vector $\mathbf{f}$ and the received vector $\widehat{\mathbf{x}}$ is equal to the capacity of the *equivalent channel*, $\widehat{\mathbf{H}}$, given by [9]–[11],

$$C_{\mathbf{S}}(n, r, \rho) = \frac{1}{l}E_{\mathbf{H}}\log_2\left(\det\left(I_{rR} + \frac{\rho}{n}\widehat{\mathbf{H}}^H\widehat{\mathbf{H}}\right)\right). \tag{3}$$

Definition 2: If the maximum mutual information given by (3) when an STBC $\mathcal{C}$ is used, is equal to the capacity of the channel, then we call $\mathcal{C}$ an information lossless STBC [12]. For an information lossless STBC $\mathcal{C}$ we call the design used to describe $\mathcal{C}$, a capacity achieving design.

It was shown in [11], that Alamouti code is the only complex orthogonal design which achieves capacity for 2 transmit and 1 receive antenna. In the same paper, 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. A rate-2, 2×2 design was given in [12], which achieves capacity for 2 transmit and arbitrary number of receive antennas. Galliou *et al.* in [13] have constructed

$$\frac{1}{\sqrt{P}}\begin{bmatrix} \sum_{i=0}^{n-1} f_{\sigma_0}^{(i)} t_i & \beta_0^{(1)}\sum_{i=0}^{n-1} f_{\mu_{0,1}}^{(i)}\sigma_1(t_i) & \beta_0^{(2)}\sum_{i=0}^{n-1} f_{\mu_{0,2}}^{(i)}\sigma_2(t_i) & \cdots & \beta_0^{(n-1)}\sum_{i=0}^{n-1} f_{\mu_{0,n-1}}^{(i)}\sigma_{n-1}(t_i) \\ \sum_{i=0}^{n-1} f_{\sigma_1}^{(i)} t_i & \beta_1^{(1)}\sum_{i=0}^{n-1} f_{\mu_{1,1}}^{(i)}\sigma_1(t_i) & \beta_1^{(2)}\sum_{i=0}^{n-1} f_{\mu_{1,2}}^{(i)}\sigma_2(t_i) & \cdots & \beta_1^{(n-1)}\sum_{i=0}^{n-1} f_{\mu_{1,n-1}}^{(i)}\sigma_{n-1}(t_i) \\ \sum_{i=0}^{n-1} f_{\sigma_2}^{(i)} t_i & \beta_2^{(1)}\sum_{i=0}^{n-1} f_{\mu_{2,1}}^{(i)}\sigma_1(t_i) & \beta_2^{(2)}\sum_{i=0}^{n-1} f_{\mu_{2,2}}^{(i)}\sigma_2(t_i) & \cdots & \beta_2^{(n-1)}\sum_{i=0}^{n-1} f_{\mu_{2,n-1}}^{(i)}\sigma_{n-1}(t_i) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sum_{i=0}^{n-1} f_{\sigma_{n-1}}^{(i)} t_i & \beta_{n-1}^{(1)}\sum_{i=0}^{n-1} f_{\mu_{n-1,1}}^{(i)}\sigma_1(t_i) & \beta_{n-1}^{(2)}\sum_{i=0}^{n-1} f_{\mu_{n-1,2}}^{(i)}\sigma_2(t_i) & \cdots & \beta_{n-1}^{(n-1)}\sum_{i=0}^{n-1} f_{\mu_{n-1,n-1}}^{(i)}\sigma_{n-1}(t_i) \end{bmatrix} \quad (4)$$

STBCs using Galois theory and the STBCs constructed are claimed to be information lossless. In [14], rate-n $n\times n$ designs are constructed using cyclic division algebras for 2, 3 and 4 transmit antennas.

In this paper, we construct rate-n $n \times n$ designs over subfields of $\mathbb{C}$ from crossed-product division algebras (defined in Section II) and also give a sufficient condition for these designs to be capacity achieving and the resulting STBCs to be information lossless for arbitrary number of transmit and receive antennas. Also, we identify a class of division algebras for which this condition is satisfied. The results presented in [7], [8] using cyclic division algebras follow as a special case of the results in this paper. Familiarity with [3]–[8] will be helpful. However, the presentation in this paper is self-contained.

II. STBC Construction

An F-division algebra D is a division ring with the center as the field F. It is well known [15], [16] that vector space dimension of D over F, known as the degree of D and denoted as $[D : F]$, is always a perfect square, say n^2. Let K be a maximal subfield of D. It is well known that $F \subset K$ and that $[D : K] = [K : F] = \sqrt{[D:F]} = n$. (Throughout the paper, we will be considering only those division algebras which have subfields of $\mathbb{C}$ as maximal subfields.) Assume that K/F is in addition a Galois extension and let $G = \{\sigma_0 = 1, \sigma_1, \sigma_2, \ldots, \sigma_{n-1}\}$ be the Galois group (1 is the identity map and the identity element of G) of K/F. Then, from [15], [16][Noether-Skolem theorem], there exists a set $U_G = \{u_{\sigma_i} : \sigma_i \in G\} \subset D$ such that $\sigma_i(k) = u_{\sigma_i}^{-1} k u_{\sigma_i} \quad \forall\ k \in K$ and $\sigma_i \in G$. We can always normalize the set U_G such that $u_{\sigma_0} = 1$. It can be seen easily that U_G is a basis of D seen as a right K-space, i.e.,

$$D = \bigoplus_{\sigma_i \in G} u_{\sigma_i} K. \quad (5)$$

In the above form of D, addition and equality are component-wise. And the multiplication between two elements, say $d = \sum_{i=0}^{n-1} u_{\sigma_i} k_{\sigma_i}$ and $d' = \sum_{j=0}^{n-1} u_{\sigma_j} k'_{\sigma_j}$, is

$$\left(\sum_{i=0}^{n-1} u_{\sigma_i} k_{\sigma_i}\right)\left(\sum_{j=0}^{n-1} u_{\sigma_j} k'_{\sigma_j}\right) = \sum_{l=0}^{n-1} u_{\sigma_l} k''_{\sigma_l}$$

where $k''_{\sigma_l} = \sum_{\sigma_j \in G} \phi(\sigma_l \sigma_j^{-1}, \sigma_j)\sigma_j(k_{\sigma_l \sigma_j^{-1}}) k'_{\sigma_j}$ and $\phi : G \times G \mapsto K^*$ is given by $\phi(\sigma_i, \sigma_j) = u_{\sigma_i\sigma_j}^{-1} u_{\sigma_i} u_{\sigma_j}$. From the fact that $u_{\sigma_h}\left(u_{\sigma_i} u_{\sigma_j}\right) = \left(u_{\sigma_h} u_{\sigma_i}\right) u_{\sigma_j}$ we have

$$\phi(\sigma_h, \sigma_i\sigma_j)\phi(\sigma_i, \sigma_j) = \phi(\sigma_h\sigma_i, \sigma_j)\sigma_j(\phi(\sigma_h, \sigma_i)). \quad (6)$$

The condition on the elements of G given in (6) is called a cocycle condition and any map from $G \times G$ to K^* satisfying this condition is a cocycle. With addition and multiplication as above, we denote the decomposition of D in (5) as (K, G, ϕ) and call D a **crossed-product algebra**. Let $\{t_0, t_1, \ldots, t_{n-1}\}$ be a basis of K seen as a vector space over F. Consider the set of matrices of the form (4), where $\mu_{i,j} = \sigma_i \sigma_j^{-1}$, $\beta_i^{(j)} = \phi(\sigma_i \sigma_j^{-1}, \sigma_j)$ and $f_{\sigma_i}^{(j)} \in F$ for all $i, j = 0, 1, \ldots, n-1$. The scaling factor $\frac{1}{\sqrt{P}}$ is to normalize the power transmitted by each antenna per channel use to unity. Under the assumption that σ_j preserves $|t_i|$ and $|\phi(\sigma_i, \sigma_j)| = 1$ for all $\sigma_i, \sigma_j \in G$, we have $P = \sqrt{\sum_{i=0}^{n-1} |t_i|^2}$. We have the following theorem:

Theorem 1: With D, K, F, G and ϕ as above, the set of matrices of the form as in (4) have the property that the difference of any two distinct matrices in it is invertible.

Proof: The proof follows from the fact that the set of matrices of the form as in (4) is the representation of $D = (K, G, \phi)$ seen as a right vector space over K via left multiplication. ■

From Theorem 1 it is clear that if we restrict $f_{\sigma_i}^{(j)}$ to some finite subset S of F, then all such matrices will constitute a full-rank, rate-n STBC over S. If G is cyclic with generator σ, D is called a cyclic division algebra, and the element u_{σ_i} can be chosen so that $\phi(\sigma_i, \sigma_j) = 1$ if $i+j < n$ and $\phi(\sigma_i, \sigma_j) = \delta$ if $i+j \geq n$, for some $\delta \in F^*$ ($u_\sigma^i u_\sigma^j = u_{\sigma_i}^{i+j}$ if $i+j < n$ and $u_\sigma^n = \delta$). The division algebra D is then denoted as (K, σ, δ).

Example 1: Consider the set $\mathbb{H}$ of Hamiltonians, given by $\mathbb{H} = \{a+ib+jc+kd | a, b, c, d \in \mathbb{R}\}$, with $i^2 = j^2 = k^2 = -1$ and $ij = k$. It is easy to check that $\mathbb{H}$ is a division algebra with $\mathbb{R}$ as its center and $\mathbb{C} = \mathbb{R} \oplus j\mathbb{R}$ as a maximal subfield. Since $\mathbb{C}/\mathbb{R}$ is a cyclic extension, $\mathbb{H}$ is a cyclic division algebra. With $U_G = \{u_{\sigma_0} = 1, u_{\sigma_1} = i\}$ as one of the possible bases, the cocycle with respect to this basis is $\phi(\sigma_0, \sigma_0) = \phi(\sigma_1, \sigma_0) = \phi(\sigma_0, \sigma_1) = 1$ and $\phi(\sigma_1, \sigma_1) = -1$. Then, from Theorem 1, we have that the difference of any two matrices of the form

$$\begin{bmatrix} f_{\sigma_0}^{(0)} + j f_{\sigma_0}^{(1)} & -(f_{\sigma_1}^{(0)} - j f_{\sigma_1}^{(1)}) \\ f_{\sigma_1}^{(0)} + j f_{\sigma_1}^{(1)} & f_{\sigma_0}^{(0)} - j f_{\sigma_0}^{(1)} \end{bmatrix} \quad (7)$$

where $f_{\sigma_i,j} \in \mathbb{R}$ for $i,j = 0,1$ is of full-rank. The STBC defined with the above matrix is nothing but the well known Alamouti code.

In general, every division algebra D need not be decomposable as in (5) and hence need not be a crossed-product algebra. However, whenever there is a maximal subfield of D Galois over the center, D can be written as a crossed-product algebra [15], [16]. Similarly, if K is Galois over F with G as the Galois group and $\phi : G\times G \mapsto K^*$ is a map satisfying the cocycle condition ($\phi(\sigma,\tau\gamma)\phi(\tau,\gamma) = \phi(\sigma\tau,\gamma)\gamma(\phi(\sigma,\tau))\ \forall\ \sigma,\tau,\gamma \in G$), then consider the algebra given by

$$(K,G,\phi) = \bigoplus_{\sigma\in G} x_\sigma K$$

where equality and addition are component-wise and where (i) $\sigma(k) = x_\sigma^{-1} k x_\sigma$ and (ii) $x_\sigma x_\tau = x_{\sigma\tau}\phi(\sigma,\tau)$. This algebra need not be a division algebra. However, (K,G,ϕ) is a central simple algebra with center as F. Thus, if we can prove that there are no non-zero zero divisors in it, then it is a division algebra. In this paper, we will give some classes of division algebras which are crossed-product algebras. The following theorem of [7], [8] gives a crossed-product algebra which is a cyclic division algebra and this cyclic division algebra will be used in obtaining other crossed-product division algebras.

Theorem 2: [7], [8] Let K be a cyclic extension of F of degree n, with σ as the generator of the Galois group. Let δ be a transcendental element over F. Then, the algebra $D = (K(\delta),\sigma,\delta)$ is a cyclic division algebra.

The following example illustrates the use of Theorem 2 to construct STBCs.

Example 2: 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, $(K(\delta),\sigma,\delta)$ is a cyclic division algebra. Thus, we have the STBC $\mathcal{C}$ given by

$$\frac{1}{\sqrt{2}}\begin{bmatrix} f_0^{(0)} + f_0^{(1)}\sqrt{j} & \delta\sigma(f_1^{(0)} + f_1^{(1)}\sqrt{j}) \\ f_1^{(0)} + f_1^{(1)}\sqrt{j} & \sigma(f_0^{(0)} + f_0^{(1)}\sqrt{j}) \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} f_0^{(0)} + f_0^{(1)}\sqrt{j} & \delta(f_1^{(0)} - f_1^{(1)}\sqrt{j}) \\ f_1^{(0)} + f_1^{(1)}\sqrt{j} & (f_0^{(0)} - f_0^{(1)}\sqrt{j}) \end{bmatrix} \quad (8)$$

where $f_i^{(j)} \in S \subset F$ 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. We have used i for the subscript of f instead of σ_i for the sake of convinience.

We will now generalize Theorem 2.

Theorem 3: Let δ_1, δ_2, x, and y be algebraically independent elements over a field L containing n_1-th and n_2-th primitive roots of unity, where n_1 and n_2 are positive integers. Let $F = L(x,y)$ and $K = F(x_1 = x^{1/n_1}, y_1 = y^{1/n_2})$. Clearly, $K(\delta_1,\delta_2)$ is a Galois extension of $F(\delta_1,\delta_2)$, with the Galois group as $G = \langle\sigma_x,\sigma_y\rangle$, where $\sigma_x : x_1 \mapsto \omega_{n_1}x_1$ and acts as identity on the other three variables, and where similarly, $\sigma_y : y_1 \mapsto \omega_{n_2}y_1$ and acts as identity on the other three variables. Consider the associative algebra

$$D = (K(\delta_1,\delta_2),G,\phi) = \bigoplus_{\substack{0\le i<n_1 \\ 0\le j<n_2}} u_{\sigma_x}^i u_{\sigma_y}^j K(\delta_1,\delta_2)$$

where u_{σ_x} and u_{σ_y} are two symbols commuting with each other and satisfying

$$u_{\sigma_x}^{n_1} = \delta_1; \quad u_{\sigma_y}^{n_2} = \delta_2$$

$$k u_{\sigma_x} = u_{\sigma_x}\sigma_x(k) \quad and \quad k u_{\sigma_y} = u_{\sigma_y}\sigma_y(k)$$

for all $k \in K(\delta_1,\delta_2)$. Then, D is a division algebra.

If S is the signal set of interest, then we will consider $L = \mathbb{Q}(S)$. Obtaining four algebraically independent transcendental elements over L is not a difficult task as according to Lindemann-Weierstrass Theorem [17], we have that for any algebraic numbers a_i ($i = 0,1,2,\ldots$) that are linearly independent over $\mathbb{Q}$, the numbers e^{a_i} are algebraically independent transcendental numbers. In particular, given any four real numbers a_1, a_2, a_3 and a_4 that are linearly independent over $\mathbb{Q}$, we could choose $x = e^{ja_1}$, $y = e^{ja_2}$, $\delta_1 = e^{ja_3}$ and $\delta_2 = e^{ja_4}$. We will see that having all of them on the unit circle will give us information lossless STBCs.

An example to show how to obtain STBC from the division algebra of Theorem 3 follows.

Example 3: Let S be the signal set of interest, say a QAM signal set. Let $n = 4$, i.e, we want STBC for four transmit antennas. Then, we take $F = \mathbb{Q}(j,x,y)$, where x and y are two transcendentals independent over $\mathbb{Q}(j)$. Then $K = F(\sqrt{x},\sqrt{y})$ is a Galois extension of F with the Galois group as $G = \langle\sigma_x,\sigma_y\rangle$, where $\sigma_x : \sqrt{x} \mapsto -\sqrt{x}$ and $\sigma_y : \sqrt{y} \mapsto -\sqrt{y}$. The map σ_x acts as identity on $\sqrt{y}$ and σ_y acts as identity on $\sqrt{x}$. Extending the action σ_x and σ_y to $K(\delta_1,\delta_2)$ having them act trivially on δ_1 and δ_2, we have from Theorem 3, that the algebra

$$\begin{aligned}(K(\delta_1,\delta_2),G,\phi) &= K(\delta_1,\delta_2) \oplus u_{\sigma_x}K(\delta_1,\delta_2) \\ &\quad \oplus u_{\sigma_y}K(\delta_1,\delta_2) \oplus u_{\sigma_x}u_{\sigma_y}K(\delta_1,\delta_2)\end{aligned}$$

is a division algebra, where δ_1,δ_2 are independent transcendentals elements over K. And ϕ is the cocycle given by

$$\phi(\sigma_x,\sigma_x) = \phi(\sigma_x\sigma_y,\sigma_x) = \delta_1; \phi(\sigma_y,\sigma_y) = \phi(\sigma_x\sigma_y,\sigma_y) = \delta_2;$$

$$\phi(\sigma_x,\sigma_y) = 1; \text{ and } \phi(\sigma_x\sigma_y,\sigma_x\sigma_y) = \delta_1\delta_2.$$

Substituting for ϕ in (4), we have the STBC with codewords of the form

$$\frac{1}{\sqrt{P}}\begin{bmatrix} k_{0,0} & \delta_2\sigma_y(k_{0,1}) & \delta_1\sigma_x(k_{1,0}) & \delta_1\delta_2\sigma_x\sigma_y(k_{1,1}) \\ k_{0,1} & \sigma_y(k_{0,0}) & \delta_1\sigma_x(k_{1,1}) & \delta_1\sigma_x\sigma_y(k_{1,0}) \\ k_{1,0} & \delta_2\sigma_y(k_{1,1}) & \sigma_x(k_{0,0}) & \delta_2\sigma_x\sigma_y(k_{0,1}) \\ k_{1,1} & \sigma_y(k_{1,0}) & \sigma_x(k_{0,1}) & \sigma_x\sigma_y(k_{0,0}) \end{bmatrix} \quad (9)$$

where $k_{i,j} = f_{i,j}^{(0)} + f_{i,j}^{(1)}\sqrt{x} + f_{i,j}^{(2)}\sqrt{y} + f_{i,j}^{(3)}\sqrt{xy}$ and $f_{i,j}^{(l)} \in S \subset \mathbb{Q}(j) \subset F$. Thus, we have an STBC over a QAM signal set for 4 transmit antennas.

Theorem 4: Let x_i, δ_i for $i = 0,1,\ldots,s-1$, be algebraically independent transcendental elements over a

$$\frac{1}{\sqrt{6}}\begin{bmatrix} k_{0,0} & \delta_2\sigma_{x_2}(k_{0,2}) & \delta_2\sigma_{x_2}^2(k_{0,1}) & \delta_1\sigma_{x_1}(k_{1,0}) & \delta_1\delta_2\sigma_{x_1}\sigma_{x_2}(k_{1,2}) & \delta_1\delta_2\sigma_{x_2}^2\sigma_{x_1}(k_{1,1}) \\ k_{0,1} & \sigma_{x_2}(k_{0,0}) & \delta_2\sigma_{x_2}^2(k_{0,2}) & \delta_1\sigma_{x_1}(k_{1,1}) & \delta_1\sigma_{x_1}\sigma_{x_2}(k_{1,0}) & \delta_1\delta_2\sigma_{x_2}^2\sigma_{x_1}(k_{1,2}) \\ k_{0,2} & \sigma_{x_2}(k_{0,1}) & \sigma_{x_2}^2(k_{0,0}) & \delta_1\sigma_{x_1}(k_{1,2}) & \delta_1\sigma_{x_1}\sigma_{x_2}(k_{1,1}) & \delta_1\sigma_{x_2}^2\sigma_{x_1}(k_{1,0}) \\ k_{1,0} & \delta_2\sigma_{x_2}(k_{1,2}) & \delta_2\sigma_{x_2}^2(k_{1,1}) & \sigma_{x_1}(k_{0,0}) & \delta_2\sigma_{x_1}\sigma_{x_2}(k_{0,2}) & \delta_2\sigma_{x_2}^2\sigma_{x_1}(k_{0,1}) \\ k_{1,1} & \sigma_{x_2}(k_{1,0}) & \delta_2\sigma_{x_2}^2(k_{1,2}) & \sigma_{x_1}(k_{0,1}) & \sigma_{x_1}\sigma_{x_2}(k_{0,0}) & \delta_2\sigma_{x_2}^2\sigma_{x_1}(k_{0,2}) \\ k_{1,2} & \sigma_{x_2}(k_{1,1}) & \sigma_{x_2}^2(k_{1,0}) & \sigma_{x_1}(k_{0,2}) & \sigma_{x_1}\sigma_{x_2}(k_{0,1}) & \sigma_{x_2}^2\sigma_{x_1}(k_{0,0}) \end{bmatrix} \quad (10)$$

field L containing n_i-th primitive roots of unity, where $n_i, i = 0,1,2,\dots,s-1$ are positive integers. Let $F = L(x_0, x_1, \dots, x_{s-1})$ and $K = F(t_0 = x_0^{1/n_0}, t_1 = x_1^{1/n_1}, \dots, t_{s-1} = x_{s-1}^{1/n_{s-1}})$. Clearly, $K(\delta_0, \delta_1, \dots, \delta_{s-1})$ is a Galois extension of $F(\delta_0, \delta_1, \dots, \delta_{s-1})$, with the Galois group as $G = \langle \sigma_{x_0}, \sigma_{x_1}, \cdots, \sigma_{x_{s-1}} \rangle$, where $\sigma_{x_i} : t_i \mapsto w_{n_i} t_i$ and acts as identity on x_j $(j \neq i)$ and δ_j for all $0 \leq j \leq s-1$. Consider the associative algebra

$$D = (K(\delta_0, \dots, \delta_{s-1}), G, \phi) = \bigoplus_{m_0,\dots,m_{s-1}} u_{\sigma_{x_0}}^{m_0} \cdots u_{\sigma_{x_{s-1}}}^{m_{s-1}} k_{m_0,\dots,m_{s-1}}$$

where $u_{\sigma_{x_i}}$ for $i = 0,1,\dots,s-1$ are symbols commuting with each other and satisfying

$$u_{\sigma_{x_i}}^{n_i} = \delta_i \text{ and } k u_{\sigma_{x_i}} = u_{\sigma_{x_i}} \sigma_{x_i}(k) \text{ for } i = 0,1,2,\dots,s-1.$$

Then, D is a division algebra.

Example 4: Let S be the 8-PSK signal set, and $n = 6$, i.e., we want STBC for 6 transmit antennas. Then, let $F = \mathbb{Q}(\omega_8, \omega_3, x_1, x_2)$ $(|x_i| = 1)$, where x_1 and x_2 are two transcendental elements independent over F. Then $K = F(\sqrt{x_1}, \sqrt[3]{x_2})$ $(n_1 = 2, n_2 = 3)$ is a Galois extension of $F(x_1, x_2)$ with Galois group as $G = \langle \sigma_{x_1}, \sigma_{x_2} \rangle$ where $\sigma_{x_1} : \sqrt{x_1} \mapsto -\sqrt{x_1}$ and $\sigma_{x_2} : \sqrt[3]{x_2} \mapsto \omega_3 \sqrt[3]{x_2}$. Let δ_1, δ_2 $(|\delta_i| = 1)$ be two independent transcendental elements over K. Extending the action of σ_{x_1} and σ_{x_1} to $K(\delta_1, \delta_2)$ by having them act as identity maps on δ_1 and δ_2, we have from Theorem 3, that

$$D = (K(\delta_1, \delta_2), G, \phi) = \bigoplus_{0 \leq i \leq 1} \bigoplus_{0 \leq j \leq 2} u_{\sigma_{x_1}}^i u_{\sigma_{x_2}}^j K(\delta_1, \delta_2)$$

is a division algebra, where $u_{\sigma_{x_1}}$ and $u_{\sigma_{x_2}}$ are symbols satisfying

$$u_{\sigma_{x_1}}^2 = \delta_1 \text{ and } k u_{\sigma_{x_1}} = u_{\sigma_{x_1}} \sigma_{x_1}(k);$$

$$u_{\sigma_{x_2}}^3 = \delta_2 \text{ and } k u_{\sigma_{x_2}} = u_{\sigma_{x_2}} \sigma_{x_2}(k).$$

Proceeding in a similar manner as in Example 3, we get an STBC with codewords as in (10), where $k_{i,j} = f_{i,j}^{(0)} + f_{i,j}^{(1)} \sqrt[3]{x_2} + f_{i,j}^{(2)} \sqrt[3]{x_2^2} + f_{i,j}^{(3)} \sqrt{x_1} + f_{i,j}^{(4)} \sqrt[3]{x_2}\sqrt{x_1} + f_{i,j}^{(5)} \sqrt[3]{x_2^2}\sqrt{x_1}$, with $f_{i,j}^{(l)} \in 8-PSK \subset F$. Thus, we have an STBC over the 8-PSK signal set for 6 transmit antennas.

III. Mutual Information

Observe that the matrices displayed in (4),(7), (8), (9) and (10) are designs over some appropriate subfields of $\mathbb{C}$. In this section, we obtain a condition for which our designs from crossed-product division algebras to achieve capacity, i.e., the STBC's from thecrossed-product division algebras are information lossless. We will first obtain the equivalent channel matrix $\widehat{\mathbf{H}}$ for our STBC's from division algebras. Let $\mathbf{F}$ be a codeword matrix of the form given in (4). First by serializing the columns of $\mathbf{F}$, we have

$$\mathbf{HF} = \underbrace{\begin{bmatrix} \mathbf{H} & \mathbf{0}_{r\times n} & \cdots & \mathbf{0}_{r\times n} \\ \mathbf{0}_{r\times n} & \mathbf{H} & \cdots & \mathbf{0}_{r\times n} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}_{r\times n} & \mathbf{0}_{r\times n} & \cdots & \mathbf{H} \end{bmatrix}}_{\mathcal{H}} \begin{bmatrix} \mathbf{F}_0 \\ \mathbf{F}_1 \\ \vdots \\ \mathbf{F}_{n-1} \end{bmatrix}$$

where $\mathbf{F}_j$ denotes the j^{th} column of the matrix $\mathbf{F}$. The column vector $\mathbf{F}_j$ can be written as

$$\mathbf{F}_j = \frac{1}{\sqrt{P}} \Phi_j \mathbf{f} \quad (11)$$

where Φ_j is a matrix with i^{th} row as

$$\left[\mathbf{0}_{1\times n}\ \mathbf{0}_{1\times n}\ \cdots\ \mathbf{0}_{1\times n}\ \phi(\sigma_i\sigma_j^{-1}, \sigma_j)\sigma_j(\mathbf{t})\ \mathbf{0}_{1\times n} \cdots \mathbf{0}_{1\times n}\right]$$

where $\sigma_j(\mathbf{t})$ is the vector $[\sigma_j(t_0)\ \sigma_j(t_1)\ \cdots\ \sigma_j(t_{n-1})]$. The column at which the non-zero vector $\phi(\sigma_i\sigma_j^{-1}, \sigma_j)\sigma_j(\mathbf{t})$ starts depends on the Galois group G of K/F. For instance, if $\sigma_i\sigma_j^{-1} = \sigma_l$, then the column at which this non-zero vector starts is after $l-1$ blocks of the vector $\mathbf{0}_{1\times n}$, i.e., at nl^{th} column. Then, (2) becomes

$$\widehat{\mathbf{x}} = \underbrace{\sqrt{\frac{\rho}{n}} \frac{1}{\sqrt{P}} \mathcal{H}\Phi}_{\widehat{\mathbf{H}}} \mathbf{f} + \widehat{\mathbf{w}} \quad (12)$$

where $\Phi = [\Phi_0^T\ \Phi_1^T\ \cdots\ \Phi_{n-1}^T]^T$. Thus, the equivalent channel for our STBC's is $\frac{1}{\sqrt{P}}\mathcal{H}\Phi$. The following theorem characterizes the capacity achievability of a design obtained from a division algebra with the maximal subfield K with the basis $\{t_0, t_1, \dots t_{n-1}\}$ over F.

Theorem 5: The design $\mathbf{F}$, as in (4) constructed using the crossed-product division algebra $D = (K, G, \phi)$ and the basis $\{t_0, t_1, \dots, t_{n-1}\}$, with the assumptions that $|\sigma_j(t_i)| = |t_i|$, $|\phi(i,j)| = 1$ for all $0 \leq i,j \leq n-1$, achieves the channel capacity if

$$\sum_{i=0}^{n-1} \sigma_j(t_i)\,(\sigma_{j'}(t_i))^* = 0 \text{ if } j \neq j'. \quad (13)$$

Using the above theorem, one can prove the following:

Theorem 6: Let K, F, x_i, δ_i be as in Theorem 4 with $|x_i| = |\delta_i| = 1$ for all $0 \leq i \leq s-1$. Then, the STBC arising from the division algebra $D = (K(\delta_0, \delta_1, \dots, \delta_{s-1}), G, \phi)$ is information lossless.

From the above theorem, it follows that the designs of Examples 2, 3 and 4 achieve capacity.

IV. Simulation Results

In this section, we present simulation results for 4 transmit antennas and compare with some of the best known codes including the STBCs obtained from cyclic division algebras [7], [8]. Figure 1 shows the performance of the STBCs obtained

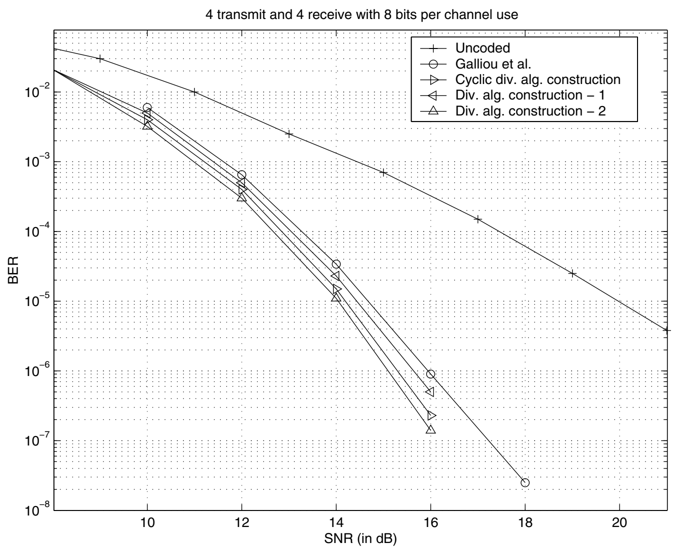

Fig. 1. Comparison of STBCs with 4 transmit and 4 receive antennas

using the division algebras of this paper and cyclic division algebras [7], [8]. The division algebra construction-1 curve is for the STBC of Example 3, with $x = e^{j\sqrt{2}}, y = e^{j\sqrt{3}}$ and $\delta_1 = e^{j\sqrt{5}}, \delta_2 = e^{j\sqrt{7}}$. These values are chosen arbitrarily. The division algebra construction-2 curve is for the same STBC with $x = e^{j\sqrt{2}}, y = e^{j\sqrt{3}}$ and $\delta_1 = e^{j\sqrt{0.23}}, \delta_2 = e^{j\sqrt{0.26}}$. The values of x and y are chosen arbitrarily, while the values of δ_1 and δ_2 are chosen to be close to the value of $\delta = e^{0.5j}$ in STBC obtained from cyclic division algebra [7]. We can see that at 10^{-6} BER, the STBC, where the parameters x, y, δ_1 and δ_2 are chosen arbitrarily, performs better than the STBC of [13] by about 0.3 dB, but is poorer than the STBC constructed from cyclic division in [7] algebra by about 0.4dB. However, the STBC, for which the x, y are chosen arbitrarily and δ_1, δ_2 are chosen close to δ, performs better than the STBC of [13] by about 0.9 dB, and better than the STBC from cyclic division algebra by about 0.2dB. We could perform even better by choosing a better x, y, δ_1 and δ_2.

V. Discussion

We have constructed rate-n, $n \times n$ designs over subfields of $\mathbb{C}$, using division algebras. And using these designs we get rate-n, full-rank STBCs over arbitrary finite subsets of subfields of $\mathbb{C}$. We gave a sufficient condition for which these designs achieve capacity. We have given two classes of division algebras and have proved that the designs constructed from these classes of division algebras achieve capacity under certain assumptions. Also, we have presented simulation results for 4 transmit and 4 receive antennas, with a transmission rate of 8 bits per channel use. The simulation results show that we perform better than the best known codes and can do even better if the best codes from division algebras are used. Also, the simulation results show that with 8 bits per channel use, we are about 0.5 dB away from the capacity of the channel with 4-QAM input [19].

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] V. Shashidhar, B. Sundar Rajan and B. A. Sethuraman,"STBCs using capacity achieving designs from cyclic division algebras", accepted for presentation in GLOBECOM 2003, San Francisco, Dec.1-5, 2003.

[8] B. Sethuraman, B. Sundar Rajan and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inform. Theory: Special Issue on Space-Time Transmission, Reception, Coding and Signal Design,* vol. 49, no. 10, pp. 2596-2616, Oct. 2003.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] J-C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding", in *Proc. IEEE Int. Workshop on Inform. Theory (ITW 2003)*, Paris, France, Mar.31 - Apr.4, 2003, pp.267-270.

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

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

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

[18] V. Shashidhar, B. Sundar Rajan and B. A. Sethuraman,"Information lossless STBCs from crossed-product algebras", manuscript under preparation.

[19] 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.*