Information-Lossless Space-Time Block Codes from Crossed-Product Algebras

Shashidhar Vummintala, *Member, IEEE,* B. Sundar Rajan, *Senior Member, IEEE,* and B. A. Sethuraman

***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.* proposed a design for 2 transmit antennas, which achieves capacity for any number of receive antennas, calling the resulting STBC when used with a signal set an information-lossless STBC. In this paper, using crossed-product central simple algebras, we construct STBCs for arbitrary number of transmit antennas over an apriori specified signal set. Alamouti code and quasi-orthogonal designs are the simplest special cases of our constructions. We obtain a condition under which these STBCs from crossed-product algebras are information lossless. We give some classes of crossed-product algebras, from which the STBCs obtained are information lossless and also of full-rank. We present some simulation results for two, three and four transmit antennas to show that our STBCs perform better than some of the best known STBCs and also that these STBCs are approximately 1 dB away from the capacity of the channel with QAM symbols as input.**

***Index Terms*— Division algebras, information-lossless, MIMO, space-time block codes.**

I. Introduction

It is known [1]–[3], that the capacity of fading channels with multiple transmit and receive antennas approximately increases linearly with the increase in the minimum of the transmit and the receive antennas. Signal design for such situations i.e., for fading channels with multiple transmit and receive antennas is called Space-Time Coding (STC) [4]. A class of STC called Space-Time Block Coding (STBC) has attracted wide attention because of the availability of low complexity decoders for them.

An $n \times l$ ($n \leq l$) Space Time Block Code (STBC) $\mathcal{C}$ is a finite set of $n \times l$ matrices (codewords) over the complex field $\mathbb{C}$. One of the main performance criteria for an STBC $\mathcal{C}$ is the minimum of the ranks of any two distinct codewords in $\mathcal{C}$, known as rank or diversity of the STBC [4], [5]. If the rank of an STBC is equal to n, then we call the STBC, a full-rank STBC. Another important criteria for an STBC is its coding gain defined as

$$C_g = \min_{\mathbf{c} \neq \mathbf{c}'} \left| \prod_i a_i \right|^{1/n}$$

where a_i are the non-zero eigen values of $(\mathbf{c}-\mathbf{c}')(\mathbf{c}-\mathbf{c}')^H$ (H denotes the Hermitian of a matrix). The following definition enables one to describe STBCs for n transmit antennas with a signal set and a matrix (in a manner similar to describing a linear code with a finite field and a generator matrix over it) which avoids exhaustive listing of codewords of an STBC.

Definition 1: A rate-k/n, $n \times l$ **linear design over a field** $F \subset \mathbb{C}$ is an $n \times l$ matrix with all its entries F-linear combinations of 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 of F, then we get an $n \times l$ STBC $\mathcal{C}$ over that finite subset S, for n transmit antennas.

For example, the Alamouti code [6] is a rate-1, 2×2 design over the field of complex numbers, $\mathbb{C}$. Similarly, the 4×4 real orthogonal design is a rate-1, 4×4 design over the real field $\mathbb{R}$ [7]. Designs over other subfields of $\mathbb{C}$ have been studied in [8]–[13]. Thus, a design and a signal set jointly constitute an STBC. In this paper we always consider the case $n = l$.

Tarokh *et al.* in [7] studied orthogonal designs (OD) over real and complex fields. These orthogonal designs have the property that the columns of the design are orthogonal to each other and using this fact the decoding complexity has been reduced from exponential increase to a linear increase with respect to the size of the signal set. This decoding has been termed as single symbol decoding in [14] as the decoding of the complete matrix codewords is broken into independent decoding of the variables in the design and STBCs admitting such decoding have been studied in [15]. In [16], ODs were constructed using Clifford algebras and an upper bound on the rate of the designs constructed is also given. Orthogonal designs were also dealt with in [17] using amicable designs. In [18] STBCs called quasi-orthogonal designs (QOD), with simple ML decoding were proposed with a transmit diversity equal to only half the number of transmit antennas. In [19]–[21], these STBCs are made fully diverse by appropriately choosing the signal sets from which the entries come from. Note that the designs in [14]–[21] are all designs over $\mathbb{R}$ and $\mathbb{C}$.

In [22], Damen *et al.* constructed Diagonal Algebraic STBCs (DAST) which have a rate of one symbol per channel use, and full rank if the signal sets chose are finite subsets of integer lattice, i.e., all QAM constellations. The DAST

This work was supported through grants to B. S. Rajan; in part by IISc-DRDO program on Advanced Research in Mathematical Engineering and in part by the Council of Scientific and Industrial Research (CISR, India) under Research Grant (22(0365)/04/EMR-II).

Shashidhar Vummintala is currently with the Beceem Communications Pvt Ltd, Bangalore, India and this work was carried out during his stay in IISc Bangalore as a Ph.D student. email:vshashidhar@beceem.com

B. Sundar Rajan is with department of Electrical Communication Engineering, Indian Institute of Science, Bangalore- 560 012, India. email:bsrajan@ece.iisc.ernet.in

B. Sethuraman is with department of Mathematics, California State University Northridge, CA 91330, USA. email:al.sethuraman@csun.edu

makes use of rotated constellations [23]. In [24], the concept of DAST was extended to a more general system called Threaded Algebraic Space-Time codes (TAST). The concept of layering is used to achieve the rates up to n symbols per channel use, where n is the number of transmit antennas. In [25], STBCs over QAM signal sets, for arbitrary number of transmit antennas are constructed using Galois theory and are claimed to maximize the mutual information. In the rest of this section, we give a brief description of the system model we use and define *equivalent channel* of an STBC and *information-lossless STBC*.

Let n and r be the number of transmit and receive antennas respectively. Let $\mathbf{f} \in \mathbb{C}^{n\times 1}$ be the transmitted vector for one time instant and $\mathbf{x} \in \mathbb{C}^{r\times 1}$ be the received vector. If $\mathbf{H} \in \mathbb{C}^{r\times n}$ is the channel matrix whose entries are iid with zero-mean, unit-variance, complex Gaussian, then we have

$$\mathbf{x} = \sqrt{\frac{\rho}{n}}\mathbf{H}\mathbf{f} + \mathbf{w} \tag{1}$$

where $\mathbf{w} \in \mathbb{C}^{r\times 1}$ is the additive noise vector whose entries are iid with zero-mean unit-variance, complex Gaussian. We assume that the vector $\mathbf{f}$ has entries with unit variance i.e., $\mathrm{E}(\mathbf{f}^H\mathbf{f}) = n$. The term ρ is the signal to noise ratio at each receive antenna. The channel matrix $\mathbf{H}$ is assumed to be known at the receiver but not at the transmitter. Then, the resulting channel capacity is given by [1], [2]

$$C(\rho, n, r) = \max_{\mathbf{R_f}\geq 0, tr(\mathbf{R_f})=n} E_{\mathbf{H}} \log_2 \left(\det\left(\mathbf{I}_r + \frac{\rho}{n}\mathbf{H}\mathbf{R_f}\mathbf{H}^H\right)\right) \tag{2}$$

where $\mathbf{R_f}$ is the covariance matrix of the vector $\mathbf{f}$ and $\mathbf{I}_r$ is the $r \times r$ identity matrix. The capacity-achieving $\mathbf{f}$ is a zero-mean complex Gaussian vector with covariance matrix say $\mathbf{R_{f,opt}}$. Under the assumption that the distribution of $\mathbf{H}$ is rotationally invariant, the optimizing covariance matrix is $\mathbf{R_{f,opt}} = \mathbf{I}_n$. Thus,

$$C(\rho, n, r) = E_{\mathbf{H}} \log_2 \left(\det\left(\mathbf{I}_r + \frac{\rho}{n}\mathbf{H}\mathbf{H}^H\right)\right). \tag{3}$$

The above expression gives channel capacity when we transmit independent vectors at every time instant i.e., there is no coding in time. However, if we use an $n\times l$ STBC, we transmit l vectors in l time instants which need not be independent of each other. So, if the transmitted $n \times l$ matrix over l time instants is $\mathbf{F}$, then we have

$$\mathbf{X} = \sqrt{\frac{\rho}{n}}\mathbf{H}\mathbf{F} + \mathbf{W} \tag{4}$$

where $\mathbf{X}$, $\mathbf{W}$ are the received $(r \times l)$ and additive noise $(r \times l)$ matrices. Let the STBC used in the above equation be of rate R symbols per channel use. Then, we have lR independent variables describing the matrix $\mathbf{F}$. 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 (4) as

$$\widehat{\mathbf{x}} = \sqrt{\frac{\rho}{n}}\widehat{\mathbf{H}}\mathbf{f} + \widehat{\mathbf{w}} \tag{5}$$

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. Notice that this can be done for any linear design. The size of the matrix $\widehat{\mathbf{H}}$ is $rl \times lR$. Then, the capacity of this new channel $\widehat{\mathbf{H}}$, known as *equivalent channel* is given by (3) with $n, r, \mathbf{H}$ replaced with $lR, lr, \widehat{\mathbf{H}}$ respectively (except for n in the term $\sqrt{\frac{\rho}{n}}$). So, by introducing coding, the maximum mutual information between the actual information vector $\mathbf{f}$ and the received matrix $\mathbf{X}$ (or $\widehat{\mathbf{x}}$) is given by

$$C_{STBC}(\rho, n, r) = \frac{1}{l} E_{\mathbf{H}} \log_2 \left(\det\left(\mathbf{I}_{lr} + \frac{\rho}{n}\widehat{\mathbf{H}}\widehat{\mathbf{H}}^H\right)\right) \tag{6}$$

where $C_{STBC}(\rho, n, r)$ denotes the maximum mutual information when the STBC is introduced. Clearly, this can at most be equal to $C(\rho, n, r)$.

Definition 2: If the maximum mutual information when an STBC $\mathcal{C}$ is used for n transmit and r receive antennas, is equal to the capacity of the channel for n transmit and r transmit antennas given by $C(\rho, n, r)$, then $\mathcal{C}$ is called an information lossless STBC [26]. We call the design used to describe $\mathcal{C}$ as a capacity achieving design.

Though, an STBC might be an information-lossless STBC, it may still be far from achieving the channel capacity. When we say an STBC is information lossless, we only mean that there is no loss in the mutual information due to the structure of the design used to describe the STBC. Note that a trivial code (e.g. V-BLAST [3]), that is, there is no dependency between the entries of the codeword matrices, is an information lossless code. But, it is known that V-BLAST doesn't achieve capacity with simple ML decoding. Thus, "information losslessness" is a necessary condition of an STBC to achieve capacity, but not a sufficient condition.

In [27], it is shown that the Alamouti code is the only rate-1, 2×2 design which achieves capacity, among all the orthogonal designs and that too only for one receive antenna. In the same paper, a class of codes namely, Linear Dispersion (LD) codes were introduced and these STBCs were constructed by optimizing for the mutual information and the designs they construct achieve 90% of the channel capacity. In [26], a rate-2, 2×2 design based on number theory was proposed which achieves capacity for 2 transmit and arbitrary number of receive antennas. In [8]–[13], full-rank, arbitrary rate STBCs were constructed for arbitrary number of transmit antennas, over any finite subsets of any subfields of $\mathbb{C}$, using commutative and non-commutative (cyclic) division algebras and have given a class of information-lossless STBCs. In [28], STBCs over QAM signal sets are constructed using cyclic division algebras for 2, 3 and 4 transmit antennas.

In this paper, we obtain designs using crossed-product algebras (defined in Section II) including division algebras and give a sufficient condition for the STBCs obtained using them to be information lossless. We give some classes of crossed-product algebras, from which the STBCs obtained are information lossless and also of full rank. The STBCs constructed in this paper include the STBCs constructed in [11], [12], [28] as a special case. The STBCS obtained in [24] which uses the concept of layering are identical to the STBCs from cyclic crossed-product algebras in this paper. However, the other classes of STBCs constructed in this paper, like STBCs from non-cyclic crossed-product algebras, are not captured by the constructions given in [24]. We present some

simulation results for two, three and four transmit antennas to show that our STBCs perform better than some of the best known codes and also that these STBCs are very close to the capacity of the channel with QAM symbols as the input. Table I summarizes the important aspects of several well known STBCs along with that of the codes of this paper. The remaining material of this paper is organized as follows: In Section II, we give a brief introduction to crossed-product central simple algebras. The main principle and construction of the STBCs from such algebras are given in Section III. Also it is shown that the well known Alamouti code and quasi-orthogonal designs can be obtained from crossed-product algebras, which in general need not be of full-rank. In Section IV, we give a sufficient condition for our STBCs to be information lossless and show that under certain conditions, the STBCs from cyclic algebras satisfy this sufficient condition, i.e., these STBCs are information lossless. In Section V, we restrict ourselves to those crossed-product algebras which are division algebras. We give some classes of division algebras using which construction of full-rank STBCs is illustrated with examples. In the same section, we show that the STBCs arising from these division algebras are information lossless. Decoding of the codes obtained in this paper is discussed in Section VI. Finally, in the same section, we present simulation results to show that our codes perform better than the best known codes and approach the capacity of the channel with QAM input.

II. Crossed-Product Algebras

In this section we give a brief introduction to crossed-product algebras. Let F be a field. Then, an associative F-algebra A is called a central simple algebra if the center of A is F and A is a simple algebra i.e., A does not have non-trivial two-sided ideals. Simple examples of central simple algebras are fields and matrix algebras over fields. Henceforth A will denote a central simple algebra. It is well known that the dimension $[A:F]$ of A over its center F is always a perfect square, say n^2 [30], [31]. The square root of $[A:F]$ is called the degree of A. The algebra A is a division algebra if every element of A is invertible in A. It is known that all division algebras are central simple algebras. By a subfield K of A, we mean $F \subset K \subset A$. Let K be a maximal subfield of A, i.e., $K \subset A$ and K is not contained in any other subfield of A. Also, let K be such that the centralizer of K in A is K itself. Then, K is called a strictly maximal subfield and it is well known that $[K:F]=n$, the degree of the algebra A. When A is a division algebra, then every maximal subfield is its own centralizer in A and thus $[K:F]=n$ for every maximal subfield K. We will always consider central simple algebras which have at least one strictly maximal subfield as a subfield of the complex field $\mathbb{C}$. In addition, let the extension K/F be a Galois extension and let $G=\{\sigma_0=1,\sigma_1,\sigma_2,\ldots,\sigma_{n-1}\}$ be the Galois group ($\sigma_0=1$ is the identity map and the identity element of G) of K/F. Then, from [30][Noether-Skolem theorem], there exists a set $U_G=\{u_{\sigma_i}:\sigma_i\in G\}\subset A$ such that

$$\sigma_i(k)=u_{\sigma_i}^{-1}ku_{\sigma_i} \quad \forall \ \ k\in K \text{ and } \ \sigma_i\in G. \tag{7}$$

We can always normalize the set U_G such that $u_{\sigma_0}=1$. It can be seen easily that the u_{σ_i} are linearly independent over K. Since $|U_G|=|G|=[K:F]=n$, U_G is a basis of A over K and called a Noether-Skolem basis. Thus, A can be seen as a right K-space of dimension n over K, i.e.,

$$A=\bigoplus_{\sigma_i\in G} u_{\sigma_i}K. \tag{8}$$

In the above form of A, addition and equality are componentwise. From (7), we have

$$\sigma_i(\sigma_j(k))=u_{\sigma_i}^{-1}u_{\sigma_j}^{-1}ku_{\sigma_j}u_{\sigma_i}=(\sigma_j\sigma_i)(k)=u_{\sigma_j\sigma_i}^{-1}ku_{\sigma_j\sigma_i}.$$

From the above expression, $u_{\sigma_j\sigma_i}(u_{\sigma_j}u_{\sigma_i})^{-1}$ commutes with every element of K and hence belongs to the centralizer of K. Since, the centralizer of K is K itself, we have $u_{\sigma_j\sigma_i}\left(u_{\sigma_j}u_{\sigma_i}\right)^{-1}\in K$, i.e., $u_{\sigma_j}u_{\sigma_i}=u_{\sigma_j\sigma_i}\phi(\sigma_j,\sigma_i)$, where $\phi(\sigma_i,\sigma_j)=u_{\sigma_i\sigma_j}^{-1}u_{\sigma_i}u_{\sigma_j}\neq 0\in K$. From the associativity of A, we have $u_{\sigma_h}(u_{\sigma_i}u_{\sigma_j})=(u_{\sigma_h}u_{\sigma_i})u_{\sigma_j}$ which implies that

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

The above condition is called the cocycle condition and any map from $G\times G$ to $K\backslash\{0\}$ satisfying the cocycle condition is a cocycle. Thus, the map $\phi: G\times G\mapsto K\backslash\{0\}$ is a cocycle. With $u_{\sigma_0}=1$, we have $\phi(\sigma_i,\sigma_0)=\phi(\sigma_0,\sigma_i)=\phi(\sigma_0,\sigma_0)=1$ for all $\sigma_i\in G$.

Now, with the above development, it is easy to see that the multiplication between two elements of A, say $a=\sum_{i=0}^{n-1}u_{\sigma_i}k_{\sigma_i}$ and $a'=\sum_{j=0}^{n-1}u_{\sigma_j}k'_{\sigma_j}$, 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 $k''_{\sigma_l}=\sum_{\sigma_i\sigma_j=\sigma_l}\phi(\sigma_i,\sigma_j)\sigma_j(k_{\sigma_i})k'_{\sigma_j}$. The algebra A with the decomposition as in (8) with addition and multiplication defined as above is called the *crossed product* of K and G with respect to ϕ and is denoted (K,G,ϕ).

Definition 3: An F-central simple algebra A is called a crossed-product algebra if it can be written as a crossed product, i.e., if it has a strictly maximal subfield Galois over the center F.

Example 1: Consider the set of Hamiltonians, given by $\mathbb{H}=\{a+ib+jc+kd|a,b,c,d\in\mathbb{R}\}$, where $\mathbb{R}$ is the real field, $i^2=j^2=k^2=-1$ and $ij=k$. Every element $h=a+ib+jc+kd\in\mathbb{H}$ has a unique inverse given by $(a-ib-jc-kd)/(a^2+b^2+c^2+d^2)$, and thus $\mathbb{H}$ is a division algebra and hence also a central simple algebra. The center of this algebra is the real field $\mathbb{R}$ and $[\mathbb{H}:\mathbb{R}]=4$. The sets $\mathbb{C}_0=\{a+ib|a,b\in\mathbb{R}\},\mathbb{C}_1=\{a+jc|a,c\in\mathbb{R}\}$ and $\mathbb{C}_2=\{a+kd|a,d\in\mathbb{R}\}$ are the maximal subfields of $\mathbb{H}$. Notice that each of the $\mathbb{C}_i$'s is an isomorphic copy of the complex field $\mathbb{C}$. Thus, we will identify one of them, say $\mathbb{C}_1$ with the complex field $\mathbb{C}$. It can be seen that $[\mathbb{C}:R]=2$ and $[\mathbb{H}:\mathbb{C}]=2$. With $\mathbb{C}$ as a maximal subfield, $\{1,i\}$ is a basis of $\mathbb{H}$ over $\mathbb{C}$. If $\{\sigma_0=1,\sigma_1=\sigma\}$ is the Galois group of $\mathbb{C}/\mathbb{R}$, then it is easy to see that (σ is the complex conjugation)

$$\sigma(c=r_1+jr_2)=i^{-1}(r_1+jr_2)i=-ir_1i-ijr_2i=r_1-jr_2.$$

Thus, $U_G = \{u_{\sigma_0} = 1, u_{\sigma_1} = i\}$ forms a Noether-Skolem basis of $\mathbb{H}$ over $\mathbb{C}$. Similarly, one can check that $\{1, k\}$ form a Noether-Skolem basis of $\mathbb{H}$ over $\mathbb{C}$. With U_G as a basis of $\mathbb{H}$ over $\mathbb{C}$, it is easy to see that $\phi(\sigma_0, \sigma_0) = \phi(\sigma_1, \sigma_0) = \phi(\sigma_0, \sigma_1) = 1$ and $\phi(\sigma_1, \sigma_1) = -1$. Thus, $\mathbb{H}$ is a crossed-product algebra.

Suppose we have a Galois extension K of a field F with the Galois group G. Then, we can construct an F-central simple algebra which has K as a strictly maximal subfield as follows: Let ϕ be a map from $G \times G$ to K^* satisfying the cocycle condition $(\phi(\sigma, \tau\gamma)\phi(\tau, \gamma) = \phi(\sigma\tau, \gamma)\gamma(\phi(\sigma, \tau))$ for all $\sigma, \tau, \gamma \in G$). Then consider the algebra

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

where equality and addition are component-wise and where u_σ are symbols such that (i) $\sigma(k) = u_\sigma^{-1} k u_\sigma$ and (ii) $u_\sigma u_\tau = u_{\sigma\tau}\phi(\sigma, \tau)$. It can be seen with simple computations that this algebra is a simple algebra with center F and hence an F-central simple algebra. And that this algebra is a crossed-product algebra is obvious from its construction.

In the next section, we construct some more crossed-product algebras and construct STBCs from these crossed-product algebras. But we shall first see a class of central simple algebras of which the set of Hamiltonians is a special case.

Example 2: Let $\mathbb{Q}$ be the field of rational numbers and F be a subfield of the complex field. Consider a four dimensional F-space $A = \{f_0 + y_1 f_1 + y_2 f_2 + y_3 f_3 | f_0, f_1, f_2, f_3 \in F\}$ with basis $y_0 = 1, y_1, y_2, y_3$. With 1 as the multiplicative identity and multiplication of any two basis elements defined as follows, it is easy to check that the space A also forms a ring:

$$y_1^2 = a, \quad y_2^2 = b, \quad y_1 y_2 = -y_2 y_1 = y_3$$

where $a,\ b$ are any two non-zero elements of F. Thus, A is an F-algebra and is called a generalized Quaternion algebra. It is easy to check that the center of this algebra is F. Now let us see whether A has any strictly maximal subfields. Clearly, if there exists one then it should be of degree 2 over F, as A is of degree 4 over F. So, it is sufficient to consider the degree 2 extensions of F contained in A. The set of elements of the form $f_0 + y_1 f_1$ forms a field, namely $F(y_1)$. Clearly, $[F(y_1) : F] = 2$. Also, the centralizer of $F(y_1)$ is $F(y_1)$. Thus, $F(y_1)$ is a strictly maximal subfield. Similarly, $F(y_2)$ and $F(y_3)$ are strictly maximal subfields of A. Also, it is easy to check that $F(y_1)/F, F(y_2)/F$ and $F(y_3)/F$ are all Galois extensions. Let $K = F(y_1)$, then the Galois group of K/F is $G = \{\sigma_0 = 1, \sigma_1 = \sigma : y_1 \mapsto -y_1\}$. Since K/F is Galois, there exists a Noether-Skolem basis of A over K. Since

$$\begin{aligned}\sigma(f_0 + y_1 f_1) &= (y_2)^{-1}(f_0 + y_1 f_1) y_2 = \frac{y_2}{b}(f_0 + y_1 f_1) y_2 \\ &= f_0 + \frac{y_2 y_1 y_2}{b} f_1 = f_0 - y_1 f_1,\end{aligned}$$

we have $U_G = \{u_{\sigma_0} = 1, u_{\sigma_1} = y_2\}$ as a basis of A over K. Also $\phi(\sigma_0, \sigma_0) = \phi(\sigma_0, \sigma_1) = \phi(\sigma_1, \sigma_0) = 1$ and $\phi(\sigma_1, \sigma_1) = b$. It would be interesting to see if this algebra is a division algebra too. It is clear that when $a = b = -1$, it is a division algebra (subset of Hamiltonians). We shall find for what other values of a and b this algebra is a division algebra. Any element x in A will be of the form $x = f_0 + y_1 f_1 + y_2 f_2 + y_3 f_3$ and we will denote the element $f_0 - y_1 f_1 - y_2 f_2 - y_3 f_3$ with $\bar{x}$. Clearly, $x\bar{x} = f_0^2 - a f_1^2 - b f_2^2 + ab f_3^2 \in F$. If $x \neq 0$ implies $x\bar{x} \neq 0$, then $x\bar{x}(x\bar{x})^{-1} = x\left(\bar{x}(x\bar{x})^{-1}\right) = 1$ which implies $x^{-1} = \bar{x}(x\bar{x})^{-1}$ and thus x is invertible. Suppose a, b are such that the equation $d_0^2 = a d_1^2 + b d_2^2$ does not have non-zero solution in F. Then $x\bar{x} = 0$ will imply that $x = 0$. Therefore, $x\bar{x} \neq 0$ if $x \neq 0$. Thus, with a, b as above, the algebra A is a division algebra. And if $d_0^2 = a d_1^2 + b d_2^2$ has a non-zero solution in F, then A is not a division algebra. With $F = \mathbb{R}$ and $a = b = -1$, we get the set of Hamiltonians.

III. STBCs from Crossed-Product Algebras

In the previous section, we have seen that if an algebra A has a strictly maximal subfield K which is Galois over the center F, then we can view A as a right K-space i.e., the action of scalar multiplication is given by right multiplication. In this section, we use this property and construct rate-n, full-rank STBCs.

Consider the map $L : A \mapsto End_K(A)$ given by $L(a) = \lambda_a$, where $\lambda_a(u) = au$ for all $u \in A$. Since, the scalar multiplication is via right and the action of λ_a gives left multiplication, these actions commute. That is $(\lambda_a(u))k = (au)k = a(uk) = \lambda_a(uk)$. This means, that λ_a is a K-linear transform of A. Clearly, L is a ring homomorphism from A to $End_K(A)$ i.e., $\lambda_{a+a'} = \lambda_a + \lambda_{a'}$ and $\lambda_{aa'} = \lambda_a \lambda_{a'}$ (this is because $\lambda_{aa'}(u) = (aa')u = a(a'u) = \lambda_a(\lambda_{a'}(u))$. Since A is a simple algebra, i.e., $\{0\}$ and A are the only ideals of A, L is injective. That is, $a - a' \neq 0 \Rightarrow \lambda_{a-a'}(u) = \lambda_a(u) - \lambda_{a'}(u) \neq 0$. If A is a division algebra, then, since $a - a'$ is invertible, say its inverse is a'', its image $\lambda_{a-a'}$ is also invertible (since $\lambda_{(a-a')a''}(u) = u$). Thus, the image of L is also a division algebra.

Now, since A is a right K-space, we can view the elements of $End_K(A)$ as matrices over K, with respect to a basis. We have seen in the previous section that the set U_G forms a basis for the algebra A over its maximal subfield K. With respect to this basis, we shall find the matrix representation of λ_a. For this, let $a = \sum_{\sigma_i \in G} u_{\sigma_i} k_{\sigma_i}$. To find the matrix representation of λ_a, it is sufficient to find the action of λ_a on each of the basis elements. Thus, $\lambda_a(u_{\sigma_j})$ is

$$\lambda_a(u_{\sigma_j}) = \sum_{\sigma_i \in G} u_{\sigma_i \sigma_j} \phi(\sigma_i, \sigma_j) \sigma_j(k_{\sigma_i}) = \sum_{\sigma_l \in G} u_{\sigma_l} k'_{\sigma_l}$$

where $k'_{\sigma_l} = \sum_{\sigma_i \sigma_j = \sigma_l} \phi(\sigma_i, \sigma_j) \sigma_j(k_{\sigma_i})$. Recall that $\phi(\sigma_i, \sigma_j) = u_{\sigma_i \sigma_j}^{-1} u_{\sigma_i} u_{\sigma_j} \in K$. From the above equation, if the rows and columns of the matrix of λ_a, denoted by $\mathbf{M}_a$, are indexed with the elements of G, then the $(\sigma_i, \sigma_j)^{th}$ entry of $\mathbf{M}_a$ is $\phi(\sigma_i \sigma_j^{-1}, \sigma_j)\sigma_j\left(k_{\sigma_i \sigma_j^{-1}}\right)$, i.e., the matrix $\mathbf{M}_a$ is given as in (9), where $\delta_{i,j} = \phi(\sigma_i \sigma_j^{-1}, \sigma_j)$. This implies, L is an embedding of the algebra A into $M_n(K)$, the set of $n \times n$ matrices over K, as shown in Figure 1. Thus, we have the following theorem:

Theorem 1: With A, K, F, G and ϕ as above and in addition if A is a division algebra, then the set of matrices

$$\mathbf{M}_a = \begin{bmatrix} k_{\sigma_0} & \delta_{0,1}\sigma_1(k_{\sigma_0\sigma_1^{-1}}) & \delta_{0,2}\sigma_2(k_{\sigma_0\sigma_2^{-1}}) & \cdots & \delta_{0,n-1}\sigma_{n-1}(k_{\sigma_0\sigma_{n-1}^{-1}}) \\ k_{\sigma_1} & \delta_{1,1}\sigma_1(k_{\sigma_1\sigma_1^{-1}}) & \delta_{1,2}\sigma_2(k_{\sigma_1\sigma_2^{-1}}) & \cdots & \delta_{1,n-1}\sigma_{n-1}(k_{\sigma_1\sigma_{n-1}^{-1}}) \\ k_{\sigma_2} & \delta_{2,1}\sigma_1(k_{\sigma_2\sigma_1^{-1}}) & \delta_{2,2}\sigma_2(k_{\sigma_2\sigma_2^{-1}}) & \cdots & \delta_{2,n-1}\sigma_{n-1}(k_{\sigma_2\sigma_{n-1}^{-1}}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{\sigma_{n-1}} & \delta_{n-1,1}\sigma_1(k_{\sigma_{n-1}\sigma_1^{-1}}) & \delta_{n-1,2}\sigma_2(k_{\sigma_{n-1}\sigma_2^{-1}}) & \cdots & \delta_{n-1,n-1}\sigma_{n-1}(k_{\sigma_{n-1}\sigma_{n-1}^{-1}}) \end{bmatrix} \tag{9}$$

$$\mathbf{M}_a = \frac{1}{\sqrt{P}} \begin{bmatrix} \sum_{i=0}^{n-1} f_{\sigma_0}^{(i)} t_i & \beta_0^{(1)} \sum_{i=0}^{n-1} f_{\mu_{0,1}}^{(i)} \sigma_1(t_i) & \beta_0^{(2)} \sum_{i=0}^{n-1} f_{\mu_{0,2}}^{(i)} \sigma_2(t_i) & \cdots & \beta_0^{(n-1)} \sum_{i=0}^{n-1} f_{\mu_{0,n-1}}^{(i)} \sigma_{n-1}(t_i) \\ \sum_{i=0}^{n-1} f_{\sigma_1}^{(i)} t_i & \beta_1^{(1)} \sum_{i=0}^{n-1} f_{\mu_{1,1}}^{(i)} \sigma_1(t_i) & \beta_1^{(2)} \sum_{i=0}^{n-1} f_{\mu_{1,2}}^{(i)} \sigma_2(t_i) & \cdots & \beta_1^{(n-1)} \sum_{i=0}^{n-1} f_{\mu_{1,n-1}}^{(i)} \sigma_{n-1}(t_i) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sum_{i=0}^{n-1} f_{\sigma_{n-1}}^{(i)} t_i & \beta_{n-1}^{(1)} \sum_{i=0}^{n-1} f_{\mu_{n-1,1}}^{(i)} \sigma_1(t_i) & \beta_{n-1}^{(2)} \sum_{i=0}^{n-1} f_{\mu_{n-1,2}}^{(i)} \sigma_2(t_i) & \cdots & \beta_{n-1}^{(n-1)} \sum_{i=0}^{n-1} f_{\mu_{n-1,n-1}}^{(i)} \sigma_{n-1}(t_i) \end{bmatrix} \tag{10}$$

of the form as in (9) have the property that the difference of any two such matrices is invertible.

Proof: The proof of the above theorem follows from the fact that the set of matrices of the form as in (9) is isomorphic to the algebra A. ∎

From the above theorem it is clear that if K is a subfield of $\mathbb{C}$ and if we restrict k_i to some finite subset S of K, we will get a finite set of $n \times n$ matrices and the STBC defined by this set of matrices will be a rate-n STBC and it will be of full-rank if A is a division algebra. We normalize these matrices with a scaling factor such that the expected power transmitted by every transmit antenna is unity per channel use. In the above case, the normalizing factor will be $n/\sqrt{\left(n + \sum_{i=0}^{n-1}\sum_{j=1}^{n-1} |\delta_{i,j}|^2\right)}$ (under the assumption that k_i have unit variance).

Example 3: Consider the set $\mathbb{H}$ of Hamiltonians of Example 1. We have seen that $\mathbb{H}$ is a division algebra with $\mathbb{R}$ as its center and $\mathbb{C}$ as a maximal subfield and hence a crossed-product 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 $\phi(\sigma_1, \sigma_1) = -1$. And the matrix representation of the map λ_d, where $d = c_{\sigma_0} + ic_{\sigma_1}$, is

$$\mathbf{M}_d = \begin{bmatrix} c_{\sigma_0} & -c_{\sigma_1}^* \\ c_{\sigma_1} & c_{\sigma_0}^* \end{bmatrix}.$$

The STBC defined with the above matrix is nothing but the well known Alamouti code.

Example 4 (Example 2 continued): Recall that the crossed-product algebra $A(a,b) = F \oplus y_1F \oplus y_2F \oplus y_3F$ is a division algebra under certain conditions on a and b. Let $F = \mathbb{Q}$. Then, $a = b = -x$, $x > 0 \in \mathbb{Q}$ satisfy the condition that $f_0^2 = af_1^2 + bf_2^2 \Rightarrow f_0 = f_1 = f_2 = 0$. Thus, the crossed-product algebra $A(a,b)$ is a division algebra with $\mathbb{Q}$ as its center and $K = \mathbb{Q}(y_1)$, $(y_1^2 = -x)$, as a maximal subfield. The Galois group of $\mathbb{Q}(y_1)/\mathbb{Q}$ is $\{1, \sigma : y_1 \mapsto -y_1\}$. The set $\{1, y_2\}$, $(y_2^2 = -x)$, forms a Noether-Skolem basis of $A(a,b)$ seen as a $\mathbb{Q}(j)-$space. With this basis, we have $\phi(1,1) = \phi(1,\sigma) = \phi(\sigma,1) = 1$ and $\phi(\sigma,\sigma) = -x$. With this ϕ, the matrix representation of $k_0 + y_2k_1 \in A(a,b)$ over K is

$$\begin{bmatrix} k_0 & -x\sigma(k_1) \\ k_1 & \sigma(k_0) \end{bmatrix}.$$

The field K can be seen as an n-dimensional F-vector space. Let $B = \{t_0, t_1, \ldots, t_{n-1}\}$ be a basis of K over F. Then, in (9), if we replace each of k_{σ_j}'s with the corresponding F-linear combination of t_i's, say $k_{\sigma j} = \sum_{i=0}^{n-1} f_{\sigma_j,i} t_i$, we get a rate-$n$ STBC for n transmit antennas, over any finite subset of F. And since F is the fixed field of G, we have $\mathbf{M}_a$ as in (10), where $\mu_{i,j} = \sigma_i\sigma_j^{-1}$, $\beta_i^{(j)} = \phi(\sigma_i\sigma_j^{-1}, \sigma_i)$ and P is a scaling factor to normalize the average total power of a codeword to n^2. It is equal to $\left(\sum_{i=0}^{n-1} |t_i|^2\right)\left(n + \sum_{i=0}^{n-1}\sum_{j=1}^{n-1} |\delta_{i,j}|^2\right)/n^2$ under the assumption that σ_j preserves the modulus of t_i. Throughout the paper, we assume that $|\phi(\sigma_i, \sigma_j)| = |t_i| = 1$ for all $0 \le i, j \le n-1$ unless specified explicitly. From now on we use this matrix for $\mathbf{M}_a$ instead of the one in (9). For instance, in Example 3, if we replace each of c_i with the corresponding linear combination over $\mathbb{R}$, i.e., $c_i = r_{i,0} + jr_{i,1}$, we have a rate-2, full-rank STBC over any finite subset of $\mathbb{R}$ whose codewords are of the form

$$\frac{1}{\sqrt{2}} \begin{bmatrix} f_{\sigma_0}^{(0)} + jf_{\sigma_0}^{(1)} & -(f_{\sigma_1}^{(0)} - jf_{\sigma_1}^{(1)}) \\ f_{\sigma_1}^{(0)} + jf_{\sigma_1}^{(1)} & f_{\sigma_0}^{(0)} - jf_{\sigma_0}^{(1)} \end{bmatrix}.$$

Now, since the crossed-product algebra (K, G, ϕ) is a central simple algebra for any K and ϕ, we get rate-n STBCs for arbitrary number of transmit antennas and over any a priori specified signal set as follows: If S is the signal set over which we want the STBC to be and n is the number of transmit antennas, then take $F = \mathbb{Q}(S)$ and let K be an n-th degree Galois extension of F, with Galois group G. Let ϕ be a map from $G \times G$ to K^* satisfying the cocycle condition, for example $\phi(\sigma, \tau) = 1$ for all $\sigma, \tau \in G$. Then, we have a crossed-product algebra using which we can construct rate-n STBCs. However, it is well known that not every crossed-product algebra is a division algebra. For instance, consider a generalized Quaternion algebra given in Example 2. If the equation $d_0^2 = ad_1^2 + bd_2^2$ has non-zero solutions for $d_0, d_1, d_2 \in F$, we have seen that it is a not a division algebra.

Thus, the rate-n STBC constructed using the crossed-product algebra A need not be of full-rank. However, by choosing the variables in the matrix given in (10) such that the element a comes from a subalgebra of A, which is a division algebra, we can make our STBC a full-rank STBC. But in this process, we might lose some of the rate. The following example illustrates one such method, from which we get rate-1, full-rank STBCs.

Example 5: Let S be the signal set of interest and n be the number of transmit antennas. Then, taking $F = \mathbb{Q}(S)$ and $K = F(\alpha)$, such that K/F is an n-th degree Galois extension, we construct the crossed-product algebra (K, G, ϕ), where ϕ is a cocycle. Thus, we get an STBC with codewords as in (10). However, this need not be of full rank, in general. So, let $f_{\sigma_0}^{(j)}$ come from S and let $f_{\sigma_i}^{(j)} = 0$, for all $i \neq 0$, then we get a rate-1, full-rank STBC over S, with codewords of the form

$$\begin{bmatrix} \sum_{i=0}^{n-1} f_{\sigma_0}^{(i)} t_i & 0 & \cdots & 0 \\ 0 & \sum_{i=0}^{n-1} f_{\mu_{1,1}}^{(i)} \sigma_1(t_i) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sum_{i=0}^{n-1} f_{\mu_{n-1,n-1}}^{(i)} \sigma_{n-1}(t_i) \end{bmatrix}$$

The coding gain of this STBC is

$$C_g = \min_{\mathbf{c} \neq \mathbf{c}'} \left| N_{K/F}(k) \right|^{2/n}$$

where $N_{K/F}(k)$ denotes the algebraic norm of the element $k \in K$ from K to F and k is the first entry on the diagonal of the difference matrix $\mathbf{c} - \mathbf{c}'$. Thus, this STBC and the STBCs constructed in [11] using field extensions, have the same rank and coding gain.

In the above example, though the crossed-product algebra is not a division algebra, we obtained a full-rank STBC by appropriately assigning the values to the variables of the design such that the resultant algebra (which is a subalgebra of the crossed-product algebra A) of the matrices is a division algebra. Another way of obtaining full-rank STBCs from crossed-product algebras is by choosing the signal sets appropriately. The next example which gives us the well known quasi-orthogonal design [20], illustrates this method of obtaining full-rank STBCs. In Section V, we construct crossed-product algebras which are division algebras and hence the resulting STBCs are full-rank STBCs.

Example 6 (Quasi-orthogonal designs): Let $F = \mathbb{R}(x)$, where x is an indeterminate and $K = F(j, \sqrt{x})$, where $j = \sqrt{-1}$. Clearly, K/F is a Galois extension, with Galois group $G = \langle \sigma_1, \sigma_2 \rangle$, where $\sigma_1 : j \mapsto -j$, $\sigma_2 : \sqrt{x} \mapsto -\sqrt{x}$. The maps σ_1 and σ_2 act as identity on $\sqrt{x}$ and j respectively. Let y_1, y_2 be two commuting symbols. Then, consider the algebra

$$A = (K, G, \phi) = K \oplus y_1 K \oplus y_2 K \oplus y_1 y_2 K$$

where $\phi(\sigma_1, \sigma_1) = \phi(\sigma_1\sigma_2, \sigma_1) = -1$ and $\phi(1, \tau) = \phi(\sigma_2, \sigma_2) = \phi(\sigma_1\sigma_2, \sigma 2) = 1$ for all $\tau \in G$. It is easy to check that this ϕ satisfies the cocycle condition. All other properties like y_i form a Noether-Skolem basis can be checked easily. Now, with this ϕ, the STBC we obtain will have codewords of the form

$$\begin{bmatrix} k_0 & -\sigma_1(k_1) & \sigma_2(k_2) & -\sigma_1(\sigma_2(k_3)) \\ k_1 & \sigma_1(k_0) & \sigma_2(k_3) & \sigma_1(\sigma_2(k_2)) \\ k_2 & -\sigma_1(k_3) & \sigma_2(k_0) & -\sigma_1(\sigma_2(k_1)) \\ k_3 & \sigma_1(k_2) & \sigma_2(k_1) & \sigma_1(\sigma_2(k_0)) \end{bmatrix}$$

where $k_i = f_i^{(0)} + f_i^{(1)} j + f_i^{(2)} \sqrt{x} + f_i^{(3)} j \sqrt{x}$. This STBC is not a full-rank STBC. Now, suppose $f_i^{(2)} = f_i^{(3)} = 0$ for $i = 0, 1, 2, 3$. Then, $\sigma_1(k_i) = k_i^*$ (complex conjugate of k_i) and $\sigma_2(k_i) = k_i$. Thus, we have a STBC with codewords of the form

$$\begin{bmatrix} k_0 & -k_1^* & k_2 & -k_3^* \\ k_1 & k_0^* & k_3 & k_2^* \\ k_2 & -k_3^* & k_0 & -k_1^* \\ k_3 & k_2^* & k_1 & k_0^* \end{bmatrix}$$

where k_i now come from arbitrary finite subset of the complex field. This is none other than the quasi-orthogonal design of the form $\begin{bmatrix} X & Y \\ Y & X \end{bmatrix}$ given in [20], where X and Y are Alamouti codes. By changing the cocycle map ϕ accordingly, we can get the other quasi-orthogonal designs too. A simple computation tells that the rank of this STBC is 2. However, if we restrict k_0, k_1 and k_2, k_3 to come from two algebraically independent signal sets, then the resulting STBC will be a full-rank STBC (in [19], the two signal sets are such that one is rotated version of the other, which is a special case of selecting two algebraically independent signal sets).

From the preceding example, it is clear that by sacrificing the division property of a division algebra, we can obtain quasi-orthogonal designs. In the rest of this section, we describe what a cyclic algebra is and construct STBCs from cyclic algebras. The cyclic algebras are important as they constitute building blocks for other crossed-product algebras constructed in this paper.

An F-central simple algebra is called a cyclic algebra, if A has a strictly maximal subfield K which is a cyclic extension of the center F. Clearly, a cyclic algebra is a crossed-product algebra. Let σ be a generator of the Galois group G. If u_{σ^i}, $i = 0, 1, \ldots, n-1$ is a Noether-Skolem basis for the algebra A over the field K, then we have

$$\sigma^i(k) = u_{\sigma^i}^{-1} k u_{\sigma^i} = u_\sigma^{-1} \left(u_{\sigma^{i-1}} k u_{\sigma^{i-1}} \right) u_\sigma = \left(u_\sigma^i \right)^{-1} k \left(u_\sigma^i \right)$$

which implies $u_{\sigma^i} = u_\sigma^i$. Also,

$$\begin{aligned} \phi(u_{\sigma^i}, u_{\sigma^j}) &= u_{\sigma^{i+j}}^{-1} u_{\sigma^i} u_{\sigma^j} \\ &= \left(u_\sigma^{i+j \ \mathit{modulo}\ n} \right)^{-1} \left(u_\sigma^{i+j} \right) \\ &= \begin{cases} 1 & \text{if } i+j < n \\ \delta & \text{if } i+j \geq n \end{cases} \end{aligned}$$

where $u_\sigma^n = \delta$. Since, the cocycle now can be described by just one element δ and similarly G can be described by σ, we denoted the crossed-product algebra (K, G, ϕ) with (K, σ, δ). Thus, with $z = u_\sigma$, we have

$$A = (K, \sigma, \delta) = \bigoplus_{i=0}^{n-1} z^i K$$

$$\frac{1}{\sqrt{n}}\begin{bmatrix} \sum_{i=0}^{n-1} f_{0,i}t^i & \delta\sigma\left(\sum_{i=0}^{n-1} f_{n-1,i}t^i\right) & \delta\sigma^2\left(\sum_{i=0}^{n-1} f_{n-2,i}t^i\right) & \cdots & \delta\sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{1,i}t^i\right) \\ \sum_{i=0}^{n-1} f_{1,i}t^i & \sigma\left(\sum_{i=0}^{n-1} f_{0,i}t^i\right) & \delta\sigma^2\left(\sum_{i=0}^{n-1} f_{n-1,i}t^i\right) & \cdots & \delta\sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{2,i}t^i\right) \\ \sum_{i=0}^{n-1} f_{2,i}t^i & \sigma\left(\sum_{i=0}^{n-1} f_{1,i}t^i\right) & \sigma^2\left(\sum_{i=0}^{n-1} f_{0,i}t^i\right) & \cdots & \delta\sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{3,i}t^i\right) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sum_{i=0}^{n-1} f_{n-1,i}t^i & \sigma\left(\sum_{i=0}^{n-1} f_{n-2,i}t^i\right) & \sigma^2\left(\sum_{i=0}^{n-1} f_{n-3,i}t^i\right) & \cdots & \sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{0,i}t^i\right) \end{bmatrix}. \tag{11}$$

where $z^n = \delta$ and $kz = z\sigma(k)$. It is easy to see that the algebras in Example 1 and 2 are cyclic algebras. Since the group multiplication is same as addition of the exponents of σ, we can replace σ^i with i, and use σ^i only if necessary. Using the above expressions, (10) reduces to (we use the notation $f_{i,j}$ for $f_i^{(j)}$ to make the notation simple) the matrix given in (11). The scaling factor before the matrix is to normalize the power transmitted by each transmit antenna per channel use to unity, under the assumptions that $|\delta| = |\sigma^j(t^i)| = |t^i| = 1$ for all $0 \leq i, j \leq n-1$.

Example 7: Let $n = 2$ and let S be a QAM signal set. Then $F = \mathbb{Q}(j)$.

(a) Clearly, the polynomial $x^2 - j$ is irreducible in $F[x]$. Thus, $K = F(\sqrt{j})$ is a cyclic extension of F. The generator of the Galois group is given by $\sigma : \sqrt{j} \mapsto -\sqrt{j}$. Now, let $\delta(|\delta| = 1)$ be any transcendental element over K. Then, it is known that the crossed-product algebra $(K(\delta), \sigma, \delta)$ is a cyclic division algebra [11], [12]. Thus, we have the STBC $\mathcal{C}$ given by

$$\mathcal{C} = \left\{ \begin{bmatrix} k_0 & \delta\sigma(k_1) \\ k_1 & \sigma(k_0) \end{bmatrix} | k_0, k_1 \in K \right\}. \tag{12}$$

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 given by

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

where $f_{i,j} \in S \subset F$ 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.

(b) In the above example, since $\{1, \sqrt{j}\}$ is a basis of K over F, every element $k \in K$ can be written as $a + b\sqrt{j}$. It is easy to see that the set $\{1 + \sqrt{j}, 1 - \sqrt{j}\}$ forms a basis of K over F, since $a + b\sqrt{j}$ can be written uniquely as

$$\frac{a+b}{2}(1 + \sqrt{j}) + \frac{a-b}{2}(1 - \sqrt{j})$$

. Thus, expanding each k_i in (12), with respect to this newly formed basis, we have a STBC with codewords given by

$$\frac{1}{2}\begin{bmatrix} f_{0,0}b_1 + f_{0,1}b_2 & \delta(f_{1,0}b_2 - f_{1,1}b_1) \\ f_{1,0}b_1 + f_{1,1}b_2 & (f_{0,0}b_2 - f_{0,1}b_1 \end{bmatrix}.$$

where $b_1 = 1 + \sqrt{j}$ and $b_2 = 1 - \sqrt{j}$.

(c) It is to check that the polynomial $x^2 - 2$ is irreducible in $F[x]$ and hence, $K = F(\sqrt{2})$ is a cyclic extension of F, of degree 2. Proceeding as above, we have a STBC with codewords of the form

$$\frac{1}{\sqrt{3}}\begin{bmatrix} f_{0,0} + f_{0,1}\sqrt{2} & \delta(f_{1,0} - f_{1,1}\sqrt{2}) \\ f_{1,0} + f_{1,1}\sqrt{2} & (f_{0,0} - f_{0,1}\sqrt{2}) \end{bmatrix}.$$

IV. Mutual Information

In this section, we give a condition under which our designs from crossed-product algebras achieve capacity, i.e., the STBCs from the crossed-product algebras are information lossless. We will first obtain the equivalent channel matrix $\widehat{\mathbf{H}}$ for our STBCs ($l = n$ and $R = n$). Let $\mathbf{F}$ be a codeword matrix of the form given in (10). First by serializing the columns of $\mathbf{F}$, we have

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

where $vec(\mathbf{HF})$ denotes the vector obtained by serializing the columns of $\mathbf{HF}$. And $\mathbf{F}_j$ denotes the j^{th} column of the matrix $\mathbf{F}$. The vector $\mathbf{F}_0$ can be written as

$$\mathbf{F}_0 = \frac{1}{\sqrt{P}}\Phi_0\mathbf{f} \tag{13}$$

where Φ_0 is an $n \times n^2$ block diagonal matrix, each of the diagonal entries is a $1 \times n$ vector $\frac{1}{\sqrt{P}}\mathbf{t} = \frac{1}{\sqrt{P}}[t_0\ t_1\ \cdots\ t_{n-1}]$ and $\mathbf{f} = [f_{\sigma_0,0}\ f_{\sigma_0,1}\ \cdots\ f_{\sigma_i,0}\ \cdots f_{\sigma_i,n-1}\ \cdots f_{\sigma_{n-1},0}\ \cdots f_{\sigma_{n-1},n-1}]^T$ is the information vector. Similarly, $\mathbf{F}_j$ can be written as

$$\mathbf{F}_j = \frac{1}{\sqrt{P}}\Phi_j\mathbf{f} \tag{14}$$

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. Note that any two rows of $\mathbf{F}_j$ have the non-zero

$$\Phi_i \;=\; \begin{array}{c} \begin{array}{cccccccc} \text{starts at} & & & \text{starts at} & \text{starts at} & \text{starts at} & & \\ \text{0-th} & & & \text{n(n-i-1)-th} & \text{n(n-i)-th} & \text{n(n-i+1)-th} & & \\ \text{col} & & & \text{col} & \text{col} & \text{col} & & \\ \downarrow & & & \downarrow & \downarrow & \downarrow & & \end{array} \\ \left[\begin{array}{cccccccc} \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \delta\sigma^i(\mathbf{t}_n) & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \delta\sigma^i(\mathbf{t}_n) & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \delta\sigma^i(\mathbf{t}_n) \\ \sigma^i(\mathbf{t}_n) & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \sigma^i(\mathbf{t}_n) & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \sigma^i(\mathbf{t}_n) & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \end{array}\right] \end{array} \begin{array}{l} \\ \\ \\ \leftarrow (i-1)^{th} \text{ row} \\ \leftarrow i^{th} \text{ row} \\ \\ \\ \end{array} \tag{15}$$

vectors in completely disjoint set of columns. Moreover, they are always separated by an integral multiple of n columns. For instance, if G is a cyclic group, then Φ_i will be as in (15). So, with $\Phi = [\Phi_0^T \;\; \Phi_1^T \;\; \cdots \Phi_{n-1}^T]^T$, we have

$$\left[\begin{array}{c} \mathbf{F}_0 \\ \mathbf{F}_1 \\ \vdots \\ \mathbf{F}_{n-1} \end{array}\right] = \frac{1}{\sqrt{P}}\Phi\mathbf{f}.$$

Then, (5) becomes

$$\widehat{\mathbf{x}} = \sqrt{\frac{\rho}{n}} \underbrace{\frac{1}{\sqrt{P}}\mathcal{H}\Phi}_{\widehat{\mathbf{H}}} \mathbf{f} + \widehat{\mathbf{w}}. \tag{16}$$

Thus, the equivalent channel for our STBCs is $\frac{1}{\sqrt{P}}\mathcal{H}\Phi$. Note that from the structure of each of Φ_j's, the k^{th} row of Φ contains the vector $\phi(\sigma_i\sigma_j^{-1},\sigma_j)\sigma_j(\mathbf{t})$ as its non-zero vector, where $k = nj+i$. And this non-zero vector starts at column nl, where $\sigma_l = \sigma_i\sigma_j^{-1}$. The following theorem characterizes the information losslessness of the STBCs from crossed-product algebras with K as a strictly maximal subfield and a basis of K over the center given as $\{t_0, t_1, \ldots t_{n-1}\}$.

Theorem 2: The design $\mathbf{M}_a$, as in (10) constructed using a crossed product algebra $A = (K, G, \phi)$ and the basis $\{t_0, t_1, \ldots, t_{n-1}\}$, 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

$$\sum_{i=0}^{n-1} \sigma_j(t_i)\left(\sigma_{j'}(t_i)\right)^* = 0 \text{ if } j \neq j'. \tag{17}$$

Proof: We will first see what $\Phi\Phi^H$ is. Since the $(k,l)^{th}$ entry of this product is the inner product between k^{th} and l^{th} rows of Φ, we have

$$(\Phi\Phi^H)_{k,l} = \sum_{a=0}^{n^2-1} \Phi_{k,a}\Phi_{a,l}^*.$$

From the structure of Φ, if the rows k and $l \neq k$ come from the same Φ_j, then their non-zero columns are disjoint and hence this inner product is zero. If k and l come from different Φ_js then either the columns of non-zero entries are disjoint or completely same. So, we have the $(k,l)-th$ element of $\Phi\Phi^H$ as

$$\sum_{a=0}^{n-1} \phi(\sigma_i\sigma_j^{-1},\sigma_j)\sigma_j(t_a)\left(\phi(\sigma_{i'}\sigma_{j'}^{-1},\sigma_{j'})\sigma_{j'}(t_a)\right)^*$$

which simplifies to

$$\phi(\sigma_i\sigma_j^{-1},\sigma_j)\phi(\sigma_{i'}\sigma_{j'}^{-1},\sigma_{j'})^* \sum_{a=0}^{n-1} \sigma_j(t_a)\left(\sigma_{j'}(t_a)\right)^*$$

which is equal to zero from the statement of the theorem. If $k = l$, then we have

$$(\Phi\Phi^H)_{k,k} = \sum_{a=0}^{n-1} |\sigma_j(t_a)|^2 = P.$$

Thus, $\Phi\Phi^H = PI_{n^2}$. Now from (6), with the equivalent channel $\widehat{\mathbf{H}}$, we have the capacity of our design as

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

■

Corollary 1: The design $\mathbf{M}_a$, as in (10) constructed using a division algebra $D = (K, G, \phi)$ and the basis $\{t_0, t_1, \ldots, t_{n-1}\}$, 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

$$\sum_{i=0}^{n-1} \sigma_j(t_i)\left(\sigma_{j'}(t_i)\right)^* = 0 \text{ if } j \neq j'. \tag{18}$$

Proof: Follows directly from Theorem 2. ■

The above theorem gives a condition on the basis of a Galois extension for which the STBC arising from the crossed-product algebra is information lossless. Also, it assumes that the basis elements have the property that $|\sigma_j(t_i)| = |t_i|$ for all $0 \leq i, j \leq n-1$. Let us now derive a sufficient condition on the basis when they don't satisfy $|\sigma_j(t_i)| = |t_i|$. Let

$\{t'_0, t'_1, \ldots, t'_{n-1}\}$ be such a basis of K over F. Now, every entry, k_i, of (9) can be written as $\sum_{j=0}^{n-1} f'_{i,j} t'_i$. Equating these two expansions of k_i, we obtain a unique representation of every $f'_{i,j}$ in terms of linear combination of $f_{i,j}$ over F. Thus, if $\mathbf{R_f} = \mathbf{I}_{n^2}$ implies $\mathbf{R_{f'}} = \mathbf{I}_{n^2}$ under the assumption that power is normalized to the same value in both the cases, the mutual information with the new basis is the same as the mutual information with the previous basis. For instance, the STBC obtained in Example 7(a) uses a basis which satisfies (17) and hence is information lossless. And the STBC obtained in Example 7(b) uses a basis which does not satisfy the property that $|\sigma(t_i)| = |t_i|$, but still the STBC obtained is information lossless, since

$$\frac{1}{2}\begin{bmatrix} f_{0,0}b_1 + f_{0,1}b_2 & \delta(f_{1,0}b_2 - f_{1,1}b_1) \\ f_{1,0}b_1 + f_{1,1}b_2 & f_{0,0}b_2 - f_{0,1}b_1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} f'_{0,0} + f'_{0,1}\sqrt{j} & \delta(f'_{1,0} - f'_{1,1}\sqrt{j}) \\ f'_{1,0} + f'_{1,1}\sqrt{j} & f'_{0,0} - f'_{0,1}\sqrt{j} \end{bmatrix}$$

where $f'_{i,0} = f_{i,0} + f_{i,1}$ and $f_{i,1} = f_{i,0} - f_{i,1}$, and $\mathbf{R_f} = \mathbf{R_{f'}}$. Note that $\{1 + \sqrt{j}, 1 - 2\sqrt{j}\}$ also forms a basis for K/F, but with this basis, $\mathbf{R_f} \neq \mathbf{R_{f'}}$ and hence the STBC obtained using this basis is not information lossless.

Consider the STBC constructed in Example 7(c). Suppose, the extension K/F has a basis $\{a_1, a_2\}$. Since a_1, a_2 are in K, let $a_1 = p_1 + q_1\sqrt{2}$ and $a_2 = p_2 + \sqrt{2}q_2$, with $p_i, q_i \in F$. Then, it is easy to check that the equation $a_1\sigma(a_1)^* + a_2\sigma(a_2)^* = 0$ does not have any solutions for p_1, q_1, p_2, q_2 in F. Thus, the extension K/F of Example 7(c) does not have any basis satisfying (17) and hence the STBC is not information lossless.

Thus, if a basis does not satisfy the property that $|\sigma_j(t_i)| = |t_i|$, for all i and j, then the STBC obtained using such a basis will be information lossless if there exists a basis satisfying all the assumptions and conditions given in Theorem 1 and such that covariance matrix is mapped to itself under the new basis. The following lemma is towards proving that the STBCs obtained in this paper are information lossless.

Lemma 1: Let F be a field containing a primitive n^{th} root of unity. Let K/F be a cyclic extension of degree n, where $K = F(t_n = t^{1/n})$, $t \in F, |t| = 1$ and σ 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: 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

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

■

Then, we have the following theorem

Theorem 3: Let $F = \mathbb{Q}(S, \omega_n, t)$, $|t| = 1$ and $K = F(t_n = t^{1/n})$ be a cyclic extension of F with $G = \langle\sigma\rangle$ as the Galois group. Let A be the crossed-product algebra (K, σ, δ) with $|\delta| = 1$. Then, the STBCs constructed using the cyclic algebra A as in Section III are information lossless.

Proof: Follows from Lemma 1 and Theorem 2. ■

From the above theorem, STBCs in the examples of Section III, namely Examples 7(a),(b) 8, 9 and 10, are information lossless with the assumption that $|t| = 1, |\delta| = 1$. However, if $|t| \neq 1$ and $|\delta| \neq 1$, the information loss increases as $||t|-1|$ and $||\delta|-1|$ increase. Figure 2 gives the capacity of the designs from cyclic algebras for various values of $|t|$ and $|\delta|$. It can be seen that the loss in the mutual information is very less compared to the information loss of 2×2 COD, namely Alamouti code. Figure 3 gives the capacity of the designs from cyclic algebras for various values of $|t|$.

V. Full-rank STBCs from Crossed-Product Division Algebras

We have seen in Section II that not all crossed-product algebras are division algebras. In this section, we identify some classes of crossed-product algebras which are division algebras and hence the STBCs from these algebras are of full-rank. We will first see when a cyclic algebra is a cyclic division algebra as cyclic division algebras constitute building blocks of other division algebras constructed in this paper. We will only give a brief introduction and for more details on them the reader can refer to [11], [12].

A. Cyclic division algebras

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 a single element, say σ. Let δ be a transcendental element over K. Then, we have the following algebra:

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

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 and has no nontrivial two sided ideals. Then, we have the following theorem.

Theorem 4 ([11], [12], [31]): With F, K, n, z and σ as above, the algebra $D = (K(\delta), \sigma, \delta)$ is a cyclic division algebra.

From the above theorem, we have a cyclic division algebra, whenever we have a cyclic extension K/F and a transcendental element δ over F. In Section III, we have already given an example of STBC from cyclic division algebra. In this section, we give some more examples of constructing STBCs using the above theorem. For details on how one obtains a cyclic extension of F appropriately, reader can refer to [11], [12].

Example 8: Let $n = 2$ and $F = \mathbb{Q}(S, t)$, where t ($|t| = 1$) is transcendental over $\mathbb{Q}(S)$. Then, $K = F(t_2 = \sqrt{t})$ is cyclic extension of F of degree 2. The generator of the Galois group is given by $\sigma : t_2 \mapsto -t_2$. Now, let $\delta(|\delta| = 1)$ be any transcendental element over K. Then, $(K(\delta)/F(\delta), \sigma, \delta)$ is a

$$\frac{1}{\sqrt{3}}\begin{bmatrix} f_{0,0}+f_{0,1}\omega_9+f_{0,2}\omega_9^2 & \delta(f_{0,0}+f_{0,1}\omega_9\omega_3+f_{0,2}\omega_9^2\omega_3^2) & \delta(f_{0,0}+f_{0,1}\omega_9\omega_3^2+f_{0,2}\omega_9^2\omega_3) \\ f_{1,0}+f_{1,1}\omega_9+f_{1,2}\omega_9^2 & f_{0,0}+f_{0,1}\omega_9\omega_3+f_{0,2}\omega_9^2\omega_3^2 & \delta(f_{0,0}+f_{0,1}\omega_9\omega_3^2+f_{0,2}\omega_9^2\omega_3) \\ f_{2,0}+f_{2,1}\omega_9+f_{2,2}\omega_9^2 & f_{0,0}+f_{0,1}\omega_9\omega_3+f_{0,2}\omega_9^2\omega_3^2 & f_{0,0}+f_{0,1}\omega_9\omega_3^2+f_{0,2}\omega_9^2\omega_3 \end{bmatrix} \quad (19)$$

cyclic division algebra. Thus, we have the STBC $\mathcal{C}$ with the codewords given by:

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

where $f_{0,0}, f_{0,1}, f_{1,0}, f_{1,1} \in S \subset F$. From the STBC construction in this example, it is clear that we have two degrees of freedom, i.e., both t_2 and δ can be chosen arbitrarily (almost), while the STBC in Example 7, we could choose only δ arbitrarily. This implies that the best coding gain possible for the STBC of Example 7, is less than the best possible with this example. Indeed, by computer search, we found that the best coding gain possible for the STBC in this example is at least 0.26 while the best coding gain possible for the STBC in Example 7 is only 0.22. Thus, this example shows that the dependence of the signal set and n have little effect on the constructions when $F/\mathbb{Q}$ is infinite, while the effect of the signal set and n is considerable when $F/\mathbb{Q}$ is finite.

Example 9: Let $n = 3$ and suppose, we want S to be a QAM signal constellation. So, let $F = \mathbb{Q}(j, \omega_3)$. Then, the polynomial $x^3 - \omega_3$ is irreducible in $F[x]$. This is because, if it is reducible, then it should have a linear factor, which implies that this polynomial has a root in F, which is not true. Thus, $K = F(\omega_9)$ is a cyclic extension of F and $\sigma : \omega_9 \mapsto \omega_9\omega_3$ is a generator of the Galois group. Now, let δ ($|\delta| = 1$) be any transcendental element over K. Then, $(K(\delta), \sigma, \delta)$ is a cyclic division algebra. Thus, we have the STBC $\mathcal{C}$ with codewords of the form (obtained in a similar way as in the previous example) given in (19), where $f_{i,j} \in S \subset F$ for $i, j = 0, 1, 2$.

Example 10: 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. 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 $i, j = 0, 1, 2, 3$.

1) STBCs from Brauer's division algebras: We give a construction of another class of cyclic division algebras due to Brauer [33], [41]. Let l and n be any two positive integers having same set of prime factors and such that l divides n. Let E be a field containing ω_l and such that $x^n - \omega_l$ is irreducible in $E[x]$. Let $K = E(x_0, x_1, \ldots, x_{n-1})$, where x_i are independent transcendental elements over E. Let $\sigma : x_i \mapsto x_{i+1 \ mod \ n}$ be an automorphism of K, fixing every element of E and F be the fixed field of σ. Since, the order of σ is n, the extension K/F is cyclic with Galois group $\langle\sigma\rangle$. Consider the following algebra

$$B = (K, \sigma, \omega_l) = \bigoplus z^i K$$

where z is some symbol satisfying $kz = z\sigma(k)$ and $z^n = \omega_l$. Then, we have the following theorem due to Brauer.

Theorem 5 ([33], [41]): With the notation as above, the algebra $B = (K, \sigma, \omega_l)$ is a cyclic division algebra of index n, with center F.

Type-I STBCs from Brauer division algebras: Let S be the signal set over which we want the STBC. Then, let $E = \mathbb{Q}(S, \omega_l)$. Assume, in addition, that $x^n - \omega_l$ is irreducible in $E[x]$. Then, F, the fixed field of σ will contain E. With $\delta = \omega_l$ and $\sigma : x_i \mapsto x_{i+1 \ mod \ n}$, we get a STBC with codewords as in (9), with $k_i \in F[x_0, x_1, \ldots, x_{n-1}]$. Since F contains E, we can restrict the coefficients of the polynomials k_i to come from E and in particular S only, to obtain a STBC over S. The STBC obtained this way is full-rank. And the symbol rate of this STBC depends on the degree of the polynomials k_i. If the degree is restricted to d, then the rate will be $\sum_{i=0}^{d} {}^{n+i-1}C_{n-1}$ symbols per channel use. We call the STBCs constructed this way type-I STBCs from Brauer division algebras. The following theorem, namely Lindemann-Weierstrass Theorem, suggests a method to find n algebraically independent transcendental numbers.

Theorem 6 ([40]): If $u_1, u_2, \ldots, u_n$ are algebraic numbers that are linearly independent over $\mathbb{Q}$, then the exponentials $e^{u_1}, e^{u_2}, \ldots, e^{u_n}$ are algebraically independent over the field of algebraic numbers.

We illustrate this construction with an example.

Example 11: Let $n = 3$ and S be a QAM signal set. Then, let $E = \mathbb{Q}(j, \omega_3)$. It is easy to see that $x^3 - \omega_3$ is irreducible in $E[x]$. Let x_0, x_1, x_2, (say $e^j, e^{j\sqrt{2}}, e^{j\sqrt{3}}$), be three independent transcendental elements over E and $K = E(x_0, x_1, x_2)$. Then, $B = (K, \sigma, \omega_3) = K + zK + z^2K$ is a cyclic division algebra of index 3. Thus, we have a STBC with codewords as follows:

$$\begin{bmatrix} k_0(x_0,x_1,x_2) & \omega_l k_2(x_2,x_0,x_1) & \omega_l k_1(x_1,x_2,x_0) \\ k_1(x_0,x_1,x_2) & \omega_l k_0(x_2,x_0,x_1) & \omega_l k_2(x_1,x_2,x_0) \\ k_2(x_0,x_1,x_2) & k_1(x_2,x_0,x_1) & k_0(x_1,x_2,x_0) \end{bmatrix}$$

where $k_i(x_0, x_1, x_2)$ is a polynomial in x_0, x_1, x_2 with coefficients from S. If we allow the degree of these polynomials to be 1, then we have a symbol rate of 4. However, if we allow the degree of the polynomials to be any positive integer d, then the symbol rate will be $\sum_{i=0}^{d} {}^{2+i}C_2$.

If $n = 2$ in the above example, it is not possible to obtain a STBC over a QAM signal set, from Brauer division algebras. This is because, our E will be $\mathbb{Q}(j)$ and the polynomial x^2+1 is not irreducible in $E[x]$, which is a necessary condition for constructing a Brauer division algebra. However, if the signal set is a 5-PSK signal set, we can obtain a STBC for 2 transmit antennas.

Type-II STBCs from Brauer division algebras: Till now, we have constructed STBCs using Brauer division algebra viewing the field K as an extension of E. However, if we view K as

an extension of F (which we have been doing till the last subsection), we get a different STBC. Let $\omega_n \in E$. Since, K/F is cyclic, there exists an element $t \in K$, such that $K = F(t)$. Let us define $t = x_0 + x_1\omega_n + \ldots + x_{n-1}\omega_n^{n-1}$. Clearly, σ maps t to $t\omega_n^{-1}$ and hence $t^n \in F$. Thus, $K = F(t)$. Now, expanding each entry k_i in (9) as $\sum_{j=0}^{n-1} f_{i,j}t^j$, we get a STBC with codewords of the form as in (11). STBCs obtained this way will be called type-II STBCs from Brauer division algebras.

Example 12 (Example 11 contd.): Expanding each k_i as $\sum_{j=0}^{2} f_{i,j}t^j$, and considering only degree zero polynomials in F, we get a STBC with codewords as follows.

$$\begin{bmatrix} \sum_{j=0}^{2} f_{0,j}t^j & \omega_3\sum_{j=0}^{2} f_{2,j}t^j\omega_3^{2j} & \omega_3\sum_{j=0}^{2} f_{1,j}t^j\omega_3^{j} \\ \sum_{j=0}^{2} f_{1,j}t^j & \sum_{j=0}^{2} f_{0,j}t^j\omega_3^{2j} & \omega_3\sum_{j=0}^{2} f_{2,j}t^j\omega_3^{j} \\ \sum_{j=0}^{2} f_{2,j}t^j & \sum_{j=0}^{2} f_{1,j}t^j\omega_3^{2j} & \sum_{j=0}^{2} f_{0,j}t^j\omega_3^{j} \end{bmatrix}$$

where $f_{i,j} \in S \subset E \subset F$.

It is shown at the end of this section that the type-I STBCs from Brauer division algebras are not information lossless if $|x_i| = 1$ and might be information lossless if $|x_i| \neq 1$, while the type-II STBCs are information lossless under certain conditions.

2) Coding gain of STBCs from cyclic division algebras: We conclude this subsection, giving a closed form expression for coding gains of STBCs constructed in this subsection. Let K/F be a cyclic extension and let $\mathcal{N}_{K/F}(k)$ denote the algebraic norm from K to F, of an element in $k \in K$.

Theorem 7: Let $\mathcal{C}$ be the rate-n STBC constructed from the cyclic division algebra $(K(\delta), \sigma, \delta)$. Let the codewords of $\mathcal{C}$ be as in (11). Then, the coding gain of the code $\mathcal{C}$ is

$$C_g = \min_{\mathbf{f}\neq\mathbf{f}'} \left|(-1)^{n-1}\mathcal{N}_{K/F}(\Delta k_{n-1}) + \ldots + \mathcal{N}_{K/F}(\Delta k_0)\right|^{2/n}$$

where $\mathbf{f} = [f_{0,0}, \ldots, f_{0,n-1}, \ldots, f_{n-1,0}, \ldots, f_{n-1,n-1}]$ and $\mathbf{f}' = [f'_{0,0}, \ldots, f'_{0,n-1}, \ldots, f'_{n-1,0}, \ldots, f'_{n-1,n-1}]$ are two distinct information vectors. And $\Delta k_i = \sum_{j=0}^{n-1}\left(f_{i,j} - f'_{i,j}\right)t^i$.

Proof: Follows from Proposition 16.2b of [31] (page 298) and the definition of coding gain. ∎

B. STBCs from tensor-product division algebras

In the last few subsections, we have seen how to construct cyclic division algebras and STBCs from them. In this section, we construct division algebras from some known division algebras and hence construct STBCs from them. One of such constructions is given by tensor product (see appendix for definitions and properties of tensor products) of two division algebras as in the following theorem:

Theorem 8 ([30]): Let D_1 and D_2 be two division algebras with the same center F. If $[D_1 : F]$ is relatively prime to $[D_2 : F]$ then $D_1 \otimes_F D_2$ is a division algebra with F as the center.

So, given any two division algebras, D_1 and D_2 with the same center and relatively prime indices, the tensor product $D_1 \otimes_F D_2$ of them is also a division algebra with the same center. So, the index of $D_1 \otimes_F D_2$ is $\sqrt{[D_1 : F][D_2 : F]}$. If both D_1 and D_2 are cyclic division algebras, then the resulting tensor product division algebra is also a cyclic division algebra. The following example illustrates the construction of STBCs from such a tensor product division algebra obtained from two cyclic division algebras.

Example 13: Suppose, we want an STBC over a QAM signal set for 6 transmit antennas. Then, let $F = \mathbb{Q}(j, \omega_3)$. Let $K_1 = F(\sqrt{j})$ and $K_2 = F(\sqrt[3]{j})$. Let δ be a transcendental element over F. Obviously, δ is a transcendental element over K_1 and K_2 also. Then, from Theorem 4, the crossed-products algebras $D_1 = (K_1(\delta), G_1, \delta) = K_1(\delta) \oplus z_1K_1(\delta)$ and $D_2 = (K_2(\delta), G_2, \delta) = K_2(\delta) \oplus z_2K_2(\delta) \oplus z_2^2K_2(\delta)$ are division algebras where G_1 and G_2, the Galois groups of $K_1(\delta)/F(\delta)$ and $K_2(\delta)/F(\delta)$, are given by $G_1 = \{\sigma_{1,0} = 1, \sigma_{1,1} : \sqrt{j} \mapsto -\sqrt{j}\}$ and $G_2 = \{\sigma_{2,0} = 1, \sigma_{2,1} : \sqrt[3]{j} \mapsto \sqrt[3]{j}\omega_3, \sigma_{2,2} : \sqrt[3]{j} \mapsto \sqrt[3]{j}\omega_3^2\}$. And z_1 and z_2 are elements of D_1 and D_2 respectively such that

$$z_1^2 = \delta \text{ and } k_1z_1 = z_1\sigma_{1,1}(k_1) \quad \forall\ k_1 \in K_1(\delta)$$

and

$$z_2^3 = \delta \text{ and } k_2z_2 = z_2\sigma_{2,1}(k_2) \quad \forall\ k_2 \in K_2(\delta).$$

It is easy to see that $K(\delta) = K_1(\delta) \otimes_F K_2(\delta)$ is a maximal subfield of $D = D_1 \otimes_F D_2$ and that the Galois group of $K(\delta)/F(\delta)$ is $G = \{\sigma_0 = 1, \sigma_1 = \sigma_{1,1}, \sigma_2 = \sigma_{2,1}, \sigma_3 = \sigma_{2,2} = \sigma_{2,1}^2, \sigma_4 = \sigma_{1,1}\sigma_{2,1}, \sigma_5 = \sigma_{1,1}\sigma_{2,2}\}$. Note that G is a cyclic group with σ_4 as a generator. Also, the set $\{u_{\sigma_0} = 1, u_{\sigma_1} = z_1 \otimes 1, u_{\sigma_2} = 1 \otimes z_2, u_{\sigma_3} = 1 \otimes z_2^2, u_{\sigma_4} = z_1 \otimes z_2, u_{\sigma_5} = z_1 \otimes z_2^2\}$ forms a Noether-Skolem basis of D over $K(\delta)$. Thus,

$$\begin{aligned} D &= K(\delta) + u_{\sigma_1}K(\delta) + u_{\sigma_2}K(\delta) + u_{\sigma_3}K(\delta) \\ &\quad + u_{\sigma_4}K(\delta) + u_{\sigma_5}K(\delta) \end{aligned}$$

And the cocycle ϕ is given in Table II. Substituting the above ϕ in (9), we get an STBC with codewords of the form as follows:

$$\frac{1}{\sqrt{6}}\begin{bmatrix} k_0 & \delta\sigma_1(k_1) & \delta\sigma_2(k_3) & \delta\sigma_3(k_2) & \delta^2\sigma_4(k_5) & \delta^2\sigma_5(k_4) \\ k_1 & \sigma_1(k_0) & \delta\sigma_2(k_5) & \delta\sigma_3(k_4) & \delta\sigma_4(k_3) & \delta\sigma_5(k_2) \\ k_2 & \delta\sigma_1(k_4) & \sigma_2(k_0) & \delta\sigma_3(k_3) & \delta\sigma_4(k_1) & \delta^2\sigma_5(k_5) \\ k_3 & \delta\sigma_1(k_5) & \sigma_2(k_2) & \sigma_3(k_0) & \delta^2\sigma_4(k_4) & \delta\sigma_5(k_1) \\ k_4 & \sigma_1(k_2) & \sigma_2(k_1) & \delta\sigma_3(k_5) & \sigma_4(k_0) & \delta\sigma_5(k_3) \\ k_5 & \sigma_1(k_3) & \sigma_2(k_4) & \sigma_3(k_1) & \sigma_4(k_2) & \sigma_5(k_0) \end{bmatrix}$$

where $k_i = f_{i,0} + f_{i,1}\sqrt{j} + f_{i,2}\sqrt[3]{j} + f_{i,3}\sqrt[3]{j}^2 + f_{i,4}\sqrt{j}\sqrt[3]{j} + f_{i,5}\sqrt{j}\sqrt[3]{j}^2$ and $f_{i,j} \in S(QAM) \in F$.

The above example shows how to construct STBCs from the tensor product division algebra of two cyclic division algebras (note that it is not necessary that we use cyclic division algebras only) with relatively prime indices. This can be extended to tensor product of any number of division algebras with relatively prime indices using the following corollary.

Corollary 2: Let D_i, $i = 0, 1, 2, \ldots, s-1$ be s F-division algebras with the index of D_i as $p_i^{\alpha_i}$, where p_i, $i = 0, 1, 2, \ldots, s-1$, are distinct primes and α_i are positive integers. Then, the algebra $D = \bigotimes_F D_i$ is an F-division algebra.

Using the above method of constructing division algebras, we cannot construct division algebras from known division algebras of not relatively prime degrees. For instance, we cannot construct division algebras of degree 4 from two division algebras of degree 2. The following theorem helps us in such cases, where we construct a division algebra which is isomorphic to the tensor product of two cyclic division algebras with some constraints. However, we do not use the language of tensor product in constructing the division algebra.

Theorem 9: 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 $K = F(x_1 = x^{1/n_1}, y_1 = y^{1/n_2}, \delta_1, \delta_2)$. 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 $\sigma_x : x_1 \mapsto x_1 \omega_{n_1} x_1$ 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.

Proof: To prove that D is a division algebra, it is sufficient to show that every non-zero element in D is invertible. Let $d = \sum_{i=0}^{n_1-1} u_{\sigma_x}^i \left(\sum_{j=0}^{n_2-1} u_{\sigma_y}^j k_{i,j} \right) \in D$ (we use i, j as the subscript of k instead of $u_{\sigma_x^i} u_{\sigma_y^j}$ to make the notations simpler). And let λ_d be the left regular representation of d over $K(\delta_1, \delta_2)$, i.e., $\lambda_d : a \mapsto da$ for all $a \in D$. Then, we have

$$\lambda_d = \begin{bmatrix} \eta_0 & \delta_1 \sigma_x(\eta_{n_1-1}) & \cdots & \delta_1 \sigma_x^{n_1-1}(\eta_1) \\ \eta_1 & \sigma_x(\eta_0) & \cdots & \delta_1 \sigma_x^{n_1-1}(\eta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \eta_{n_1-1} & \sigma_x(\eta_{n_1-2}) & \cdots & \sigma_x^{n_1-1}(\eta_0) \end{bmatrix}$$

where η_i is

$$\eta_i = \begin{bmatrix} k_{i,0} & \delta_2 \sigma_y(k_{i,n_2-1}) & \cdots & \delta_2 \sigma_y^{n_2-1}(k_{i,1}) \\ k_{i,1} & \sigma_y(k_{i,0}) & \cdots & \delta_2 \sigma_y^{n_2-1}(k_{i,2}) \\ \vdots & \vdots & \ddots & \vdots \\ k_{i,n_2-1} & \sigma_y(k_{i,n_2-2}) & \cdots & \sigma_y^{n_2-1}(k_{i,0}) \end{bmatrix}.$$

Notice that $k_{i,j}$ are rational functions of polynomials of the two variables δ_1 and δ_2. However, we can assume $k_{i,j}$ are polynomials in δ_1 and δ_2 instead of rational functions in them, as we can take the LCM of all $k_{i,j}$ and factor it out. Let $\rho_d(\delta_1, \delta_2)$ denote the determinant of λ_d. Since δ_1 and δ_2 are algebraically independent of each other, it is sufficient to show that $\rho_d(\delta_1, \delta_2)$ is not a zero polynomial to show that d is invertible, For this let us assume that there exists some j for which $k_{0,j} \neq 0$. If there doesn't exist any j for which $k_{0,j} \neq 0$, then we can factor out u_{σ_x} from d and since u_{σ_x} is invertible, it is sufficient to prove that d/u_{σ_x} is invertible. Thus, we have

$$\rho_d(0, \delta_2) = \begin{vmatrix} \eta_0 & 0 & 0 & \cdots & 0 \\ \eta_1 & \sigma_x(\eta_0) & 0 & \cdots & 0 \\ \eta_2 & \sigma_x(\eta_1) & \sigma_x^2(\eta_0) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \eta_{n_1-1} & \sigma_x(\eta_{n_1-2}) & \sigma_x^2(\eta_{n_1-3}) & \cdots & \sigma_x^{n_1-1}(\eta_0) \end{vmatrix}.$$

In the above expression, η_0 can become zero matrix when δ_1 is set to zero. This can happen only if δ_1 divides $k_{0,j}$ for all j. If $k_{i,j}$ has δ_1 as a factor for all i and j, then it is sufficient to prove that $d' = d/\delta_1$ is invertible. So, without loss of generality, we can assume that there exists a $k_{i,j}$ which does not have δ_1 as a factor. Let m be the smallest integer such that δ_1 does not divide $k_{m,j}$ for some j. Then

$$d' = u_{\sigma_x}^{n_1-m} d \delta_1^{-1} = \sum_{i=0}^{n_1-1} u_{\sigma_x}^i \left(\sum_{j=0}^{n_2-1} u_{\sigma_y}^j k'_{i,j} \right)$$

has the property that there exists some j such that δ_1 does not divide $k'_{0,j}$. Also notice that all $k'_{i,j}$ are again polynomials only and not rational functions. And to prove d is invertible it is enough to prove that d' is invertible. So we can assume that there exists a j such that δ_1 does not divide $k_{0,j}$. Now, since $(K(\delta_1, \delta_2), \sigma_2, \delta_2)$ is a cyclic division algebra with center $F(\delta_1, \delta_2, x_1)$, we have $\det(\eta_0) \neq 0$. Thus, we have

$$\rho_d(0, \delta_2) = \prod_{i=0}^{n_1-1} \det(\sigma_x^i(\eta_0)) = \prod_{i=0}^{n_1-1} \sigma_x^i(\det(\eta_0)) \neq 0.$$

This implies $\rho_d(\delta_1, \delta_2)$ is not a zero polynomial because δ_1 and δ_2 are independent transcendental elements over K. ∎

If S is the signal set of interest, then we take $L = \mathbb{Q}(S)$. Obtaining 4 algebraically independent transcendental elements over L is not a difficult task as according to Lindemann-Weierstrass Theorem [41], we have that for any two algebraic numbers a_1 and a_2 linearly independent of each other over $\mathbb{Q}$, the numbers e^{a_1} and e^{a_2} are algebraically independent transcendental numbers. Thus, we can take e^{ja_1}, e^{ja_2}, e^{ja_3} and e^{ja_4} for x, y, δ_1 and δ_2 respectively. We could use e^{a_i} instead but we will see that having all of them on the unit circle will give us information-lossless STBCs.

In Theorem 9, $K(\delta_1, \delta_2)$ is a cyclic Galois extension of $F(\delta_1, \delta_2)$, if n_1 and n_2 are relatively prime to each other. We give an example to show how to obtain STBC from the division algebra of Theorem 9.

Example 14: 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 $G = \langle \sigma_x, \sigma_y \rangle$, where $\sigma_x : \sqrt{x} \mapsto -\sqrt{x}$ and $\sigma_y : \sqrt{y} \mapsto -\sqrt{y}$. Then, from Theorem 9, the algebra

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

$$\frac{1}{\sqrt{6}}\begin{bmatrix} k_{0,0} & \delta_2\sigma_{x_2}(k_{0,2}) & \delta_2\sigma^2_{x_2}(k_{0,1}) & \delta_1\sigma_{x_1}(k_{1,0}) & \delta_1\delta_2\sigma_{x_1}\sigma_{x_2}(k_{1,2}) & \delta_1\delta_2\sigma^2_{x_2}\sigma_{x_1}(k_{1,1}) \\ k_{0,1} & \sigma_{x_2}(k_{0,0}) & \delta_2\sigma^2_{x_2}(k_{0,2}) & \delta_1\sigma_{x_1}(k_{1,1}) & \delta_1\sigma_{x_1}\sigma_{x_2}(k_{1,0}) & \delta_1\delta_2\sigma^2_{x_2}\sigma_{x_1}(k_{1,2}) \\ k_{0,2} & \sigma_{x_2}(k_{0,1}) & \sigma^2_{x_2}(k_{0,0}) & \delta_1\sigma_{x_1}(k_{1,2}) & \delta_1\sigma_{x_1}\sigma_{x_2}(k_{1,1}) & \delta_1\sigma^2_{x_2}\sigma_{x_1}(k_{1,0}) \\ k_{1,0} & \delta_2\sigma_{x_2}(k_{1,2}) & \delta_2\sigma^2_{x_2}(k_{1,1}) & \sigma_{x_1}(k_{0,0}) & \delta_2\sigma_{x_1}\sigma_{x_2}(k_{0,2}) & \delta_2\sigma^2_{x_2}\sigma_{x_1}(k_{0,1}) \\ k_{1,1} & \sigma_{x_2}(k_{1,0}) & \delta_2\sigma^2_{x_2}(k_{1,2}) & \sigma_{x_1}(k_{0,1}) & \sigma_{x_1}\sigma_{x_2}(k_{0,0}) & \delta_2\sigma^2_{x_2}\sigma_{x_1}(k_{0,2}) \\ k_{1,2} & \sigma_{x_2}(k_{1,1}) & \sigma^2_{x_2}(k_{1,0}) & \sigma_{x_1}(k_{0,2}) & \sigma_{x_1}\sigma_{x_2}(k_{0,1}) & \sigma^2_{x_2}\sigma_{x_1}(k_{0,0}) \end{bmatrix} \tag{20}$$

$$\eta_h = \begin{bmatrix} k_{h,0,0} & \delta_2\sigma_{x_2}(k_{h,0,2}) & \delta_2\sigma^2_{x_2}(k_{h,0,1}) & \delta_1\sigma_{x_1}(k_{h,1,0}) & \delta_1\delta_2\sigma_{x_1}\sigma_{x_2}(k_{h,1,2}) & \delta_1\delta_2\sigma^2_{x_2}\sigma_{x_1}(k_{h,1,1}) \\ k_{h,0,1} & \sigma_{x_2}(k_{h,0,0}) & \delta_2\sigma^2_{x_2}(k_{h,0,2}) & \delta_1\sigma_{x_1}(k_{h,1,1}) & \delta_1\sigma_{x_1}\sigma_{x_2}(k_{h,1,0}) & \delta_1\delta_2\sigma^2_{x_2}\sigma_{x_1}(k_{h,1,2}) \\ k_{h,0,2} & \sigma_{x_2}(k_{h,0,1}) & \sigma^2_{x_2}(k_{h,0,0}) & \delta_1\sigma_{x_1}(k_{h,1,2}) & \delta_1\sigma_{x_1}\sigma_{x_2}(k_{h,1,1}) & \delta_1\sigma^2_{x_2}\sigma_{x_1}(k_{h,1,0}) \\ k_{h,1,0} & \delta_2\sigma_{x_2}(k_{h,1,2}) & \delta_2\sigma^2_{x_2}(k_{h,1,1}) & \sigma_{x_1}(k_{h,0,0}) & \delta_2\sigma_{x_1}\sigma_{x_2}(k_{h,0,2}) & \delta_2\sigma^2_{x_2}\sigma_{x_1}(k_{h,0,1}) \\ k_{h,1,1} & \sigma_{x_2}(k_{h,1,0}) & \delta_2\sigma^2_{x_2}(k_{h,1,2}) & \sigma_{x_1}(k_{h,0,1}) & \sigma_{x_1}\sigma_{x_2}(k_{h,0,0}) & \delta_2\sigma^2_{x_2}\sigma_{x_1}(k_{h,0,2}) \\ k_{h,1,2} & \sigma_{x_2}(k_{h,1,1}) & \sigma^2_{x_2}(k_{h,1,0}) & \sigma_{x_1}(k_{h,0,2}) & \sigma_{x_1}\sigma_{x_2}(k_{h,0,1}) & \sigma^2_{x_2}\sigma_{x_1}(k_{h,0,0}) \end{bmatrix} \tag{21}$$

is a division algebra, where δ_1, δ_2 are independent transcendentals elements over K. And

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

Substituting for ϕ in (10), we have an STBC with codewords of the form

$$\frac{1}{\sqrt{P}}\begin{bmatrix} k_{0,0} & \delta_2\sigma_y(k_{0,1}) & \delta_1\sigma_x(k_{1,0}) & \delta_1\delta_2\sigma_x\sigma_y(k_{1,1}) \\ k_{0,1} & \sigma_y(k_{0,0}) & \delta_1\sigma_x(k_{1,1}) & \delta_1\sigma_x\sigma_y(k_{1,0}) \\ k_{1,0} & \delta_2\sigma_y(k_{1,1}) & \sigma_x(k_{0,0}) & \delta_2\sigma_x\sigma_y(k_{0,1}) \\ k_{1,1} & \sigma_y(k_{1,0}) & \sigma_x(k_{0,1}) & \sigma_x\sigma_y(k_{0,0}) \end{bmatrix} \tag{22}$$

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

Corollary 3: Let x_i, $i = 0, 1, \ldots, s-1$, be s transcendental elements over a field L containing n_i-th primitive roots of unity, where $n_i, i = 0, 1, 2, \ldots, s-1$ are positive integers. Assume in addition that $x_i, i = 0, 1, 2, \ldots, s-1$ are independent of each other. Let $F = L(x_0, x_1, \ldots, x_{s-1})$ and $K = F(t_0 = x_0^{1/n_0}, t_1 = x_1^{1/n_1}, \ldots, t_{s-1} = x_{s-1}^{1/n_{s-1}})$. Clearly, K is a Galois extension of F, with the Galois group as $G = \langle \sigma_{x_0}, \sigma_{x_1}, \cdots, \sigma_{x_{s-1}} \rangle$. Let $\delta_i, i = 0, 1, 2, \ldots, s-1$ be s commuting indeterminates (one can assume them to be transcendental elements over F, independent of each other). Also, let $u_{\sigma_{x_i}}, i = 0, 1, 2, \ldots, s-1$ be s symbols commuting with each other and satisfying

$$u^{n_i}_{\sigma_{x_i}} = \delta_i \quad \text{and} \quad k u_{\sigma_{x_i}} = u_{\sigma_{x_i}}\sigma_{x_i}(k)$$

for all $k \in K(\delta_0, \delta_1, \ldots, \delta_{s-1})$. Then, the algebra

$$D = (K(\delta_1, \delta_2, \ldots, \delta_{s-1}), G, \phi)$$

is a division algebra.

Proof: Follows from Theorem 9. ∎

Thus, given an Abelian group G, we have constructed a division algebra which is a crossed product of a field K and the group G with respect to some cocycle ϕ. Such constructions are called generic constructions of Abelian crossed-product algebras.

Example 15: 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 $G = \langle \sigma_{x_1}, \sigma_{x_2} \rangle$ 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. Then, from Theorem 9,

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

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

$$u^2_{\sigma_{x_1}} = \delta_1; \quad k u_{\sigma_{x_1}} = u_{\sigma_{x_1}}\sigma_{x_1}(k);$$
$$u^3_{\sigma_{x_2}} = \delta_2 \quad \text{and} \quad k u_{\sigma_{x_2}} = u_{\sigma_{x_2}}\sigma_{x_2}(k).$$

Proceeding in a similar manner as in Example 14, we get a STBC with codewords as in (20), where $k_{i,j} = f^{(0)}_{i,j} + f^{(1)}_{i,j}\sqrt[3]{x_2} + f^{(2)}_{i,j}\sqrt[3]{x_2^2} + f^{(3)}_{i,j}\sqrt{x_1} + f^{(4)}_{i,j}\sqrt[3]{x_2}\sqrt{x_1} + f^{(5)}_{i,j}\sqrt[3]{x_2^2}\sqrt{x_1}$, with $f^{(l)}_{i,j} \in 8-PSK \subset F$. Thus, we have an STBC over the 8-PSK signal set for 6 transmit antennas.

Example 16: Let S be the 8-PSK signal set, and $n = 12$, i.e., we want STBC for 12 transmit antennas. Then, let $F = \mathbb{Q}(\omega_8, \omega_3, x_0, x_1, x_2)$ ($|x_i| = 1$), where x_0, x_1 and x_2 are transcendental elements independent over F. Then $K = F(\sqrt{x_0}, \sqrt{x_1}, \sqrt[3]{x_2})$ ($n_0 = 2, n_1 = 2, n_2 = 3$) is a Galois extension of $F(x_0, x_1, x_2)$ with Galois group $G = \langle \sigma_{x_0}, \sigma_{x_1}, \sigma_{x_2} \rangle$ where $\sigma_{x_0} : \sqrt{x_0} \mapsto -\sqrt{x_0}$, $\sigma_{x_1} : \sqrt{x_1} \mapsto -\sqrt{x_1}$ and $\sigma_{x_2} : \sqrt[3]{x_2} \mapsto \omega_3\sqrt[3]{x_2}$. Let δ_0, δ_1 and δ_2 ($|\delta_i| = 1$) be independent transcendental elements over K. Then, from Theorem 9,

$$D = (K(\delta_1, \delta_2), G, \phi) = \bigoplus_{\substack{0\le h\le 1\\ 0\le i\le 1\\ 0\le j\le 2}} u^h_{\sigma_{x_0}} u^i_{\sigma_{x_1}} u^j_{\sigma_{x_2}} K(\delta_1, \delta_2)$$

is a division algebra, where $u_{\sigma_{x_0}}$, $u_{\sigma_{x_1}}$ and $u_{\sigma_{x_2}}$ are symbols satisfying

$$u^2_{\sigma_{x_0}} = \delta_0; \quad u^2_{\sigma_{x_1}} = \delta_1;$$
$$u^3_{\sigma_{x_2}} = \delta_2 \quad \text{and} \quad k u_{\sigma_{x_i}} = u_{\sigma_{x_i}}\sigma_{x_i}(k).$$

Proceeding in a similar manner as in Example 14, we get a STBC with codewords as $\frac{1}{\sqrt{12}}\begin{bmatrix} \eta_0 & \delta_0\sigma_{x_0}(\eta_1) \\ \eta_1 & \sigma_{x_0}(\eta_0) \end{bmatrix}$ where η_h is as given in (21) with $k_{h,i,j} = \sum_{a=0}^{1}\sum_{b=0}^{1}\sum_{c=0}^{2} f^{(a,b,c)}_{h,i,j}\sqrt{x_0}^a\sqrt{x_1}^b\sqrt[3]{x_2}^c$, with

$$\sum_{i_0,\ldots,i_{s-1}} \left[\sigma_0^{j_0}\ldots\sigma_{s-1}^{j_{s-1}}\left((x_0')^{i_0}\ldots(x_{s-1}')^{i_{s-1}}\right)\right]^* \left[\sigma_0^{j_0'}\ldots\sigma_{s-1}^{j_{s-1}'}\left((x_0')^{i_0}\ldots(x_{s-1}')^{i_{s-1}}\right)\right] = 0 \tag{23}$$

$$\sum_{i_0,\ldots,i_{s-1}} \left\{\left[(x_0')^{i_0}\omega_{n_0}^{i_0 j_0}\right]\cdots\left[(x_{s-1}')^{i_{s-1}}\omega_{n_{s-1}}^{i_{s-1}j_{s-1}}\right]\right\}^* \left\{\left[(x_0')^{i_0}\omega_{n_0}^{i_0 j_0'}\right]\cdots\left[(x_{s-1}')^{i_{s-1}}\omega_{n_{s-1}}^{i_{s-1}j_{s-1}'}\right]\right\}. \tag{24}$$

$$\sum_{i_0}\left\{\omega_{n_0}^{i_0(j_0'-j_0)}\sum_{i_1}\left[\omega_{n_1}^{i_1(j_1'-j_1)}\cdots\left(\omega_{n_{s-2}}^{i_{s-2}(j_{s-2}'-j_{s-2})}\sum_{i_{s-1}}\omega_{n_{s-1}}^{i_{s-1}(j_{s-1}'-j_{s-1})}\right)\right]\right\} = 0. \tag{25}$$

$f_{h,i,j}^{(a,b,c)} \in 8-PSK \subset F$. Thus, we have an STBC over the 8-PSK signal set for 12 transmit antennas.

C. Rates beyond n symbols per channel use

Till now, we have constructed rate-n, full-rank STBCs using division algebras. Recall that the division algebras we used are the ones with center a transcendental field over $\mathbb{Q}$. Consider the case of the STBCs from cyclic division algebras. The division algebras we considered are of the form $(K(\delta),\sigma,\delta)$ where $K(\delta)$ is a cyclic extension of $F(\delta)$, with δ a transcendental element over F. Recall that F is a field extension of $\mathbb{Q}$ such that it contains the signal set S. Now the codeword matrices with this division algebra will be of the form (11) with $f_{\sigma_i,j}$ coming from $F(\delta)$, since the center is $F(\delta)$. And an element of $F(\delta)$ will be of the form $a(\delta)/b(\delta)$, where $a(\delta)$ and $b(\delta)$ are polynomials in δ. So, each entry in (11) is of the form $a(\delta)/b(\delta)$. But since, two different pairs of $(a(\delta),b(\delta))$ can give rise to the same $a(\delta)/b(\delta)$, we assume that the entries of (11) are of the form $a(\delta)$ only. Thus, if $f_{\sigma_i,j,l}$ come from the signal set S, then our codeword matrices are of the form (11), with $f_{\sigma_i,j}=\sum_l f_{\sigma_i,j,l}\delta^l$, where the subscript l can range from 0 to any positive integer. With this, our STBC constructed from the division algebra $(K(\delta),\sigma,\delta)$ can have arbitrary rate. For instance, the STBC constructed in Example 7, will have the codewords of the form as below:

$$\begin{bmatrix} \sum_l f_{0,l}\delta^l + \sum_l f_{1,l}\delta^l\sqrt{j} & \delta\left(\sum_l f_{2,l}\delta^l - \sum_l f_{3,l}\delta^l\sqrt{j}\right) \\ \sum_l f_{2,l}\delta^l + \sum_l f_{3,l}\delta^l\sqrt{j} & \sum_l f_{0,l}\delta^l - \sum_l f_{1,l}\delta^l\sqrt{j} \end{bmatrix}.$$

In a similar way, STBCs constructed from other division algebras, as in Section V-B, can have arbitrary rate. But note that in the case of non-cyclic division algebras, each entry of the codeword matrix is a polynomial in more than one transcendental element. Though, we have arbitrary-rate STBCs, for the purpose of clarity, we concentrate only on the rate-n STBCs constructed till the previous subsection.

D. Mutual Information

In this section, we show that, under certain conditions, our designs arising from the division algebras we have discussed so far achieve capacity, i.e., the STBCs from these division algebras are information lossless.

1) Mutual information of STBCs from Brauer division algebras: We show that the type-I STBCs from Brauer division algebras are not information lossless. Recall from Subsection V-A.1, that in Brauer division algebras, i.e., (K,σ,ω_l), σ takes x_i to $x_{i+1\ mod\ n}$. Thus, the LHS of (17) is

$$\sum_{i=0}^{n-1} x_{i+j\ mod\ n}\left(x_{i+j'\ mod\ n}\right)^* = \sum_{i=0}^{n-1}\frac{x_{i+j\ mod\ n}}{x_{i+j'\ mod\ n}}$$

where we assume $|x_i|=1$. Since the x_i's are independent transcendental elements over E, the above expression will not be equal to zero and hence the type-I STBCs from Brauer division algebras are not information lossless.

The type-II STBCs from Brauer division algebras are information lossless if $|t|=1$. This condition that $|t|=1$ can be met, by choosing $x_1,x_2,\ldots,x_{n-1}$ arbitrarily and then choosing x_0 such that $t=x_0+\omega_n x_1+\cdots+\omega_n^{n-1}x_{n-1}$ lies on unit circle. Figure 4 shows the capacities of both the type-II and type-II STBCs constructed from Brauer division algebras. It can be seen from the figure that the information loss in type-I STBCs is less than the loss due to the Alamouti code.

2) Mutual information of STBCs from tensor-product division algebras: In the following theorem, we show that the STBCs constructed in Subsection V-B are information lossless.

Theorem 10: Let K,F,x_i,δ_i be as in Theorem 9 with $|x_i|=|\delta_i|=1$ for all $0\le i\le s-1$. Then, the STBC arising from the division algebra $D=(K(\delta_0,\delta_1,\ldots,\delta_{s-1}),G,\phi)$ is information lossless.

Proof: It is sufficient to prove (23) for $(j_0,j_1,\ldots,j_{s-1}) \neq (j_0',j_1',\ldots,j_{s-1}')$. Since, each of σ_i's act as identity on x_j' if $i\neq j$, and $\sigma_i(x_i')=x_i'\omega_{n_i}$, LHS of (23) can be written as in (24). Since $|x_i|=1$ for all i, the above expression can be written as

$$\sum_{i_0,\ldots,i_{s-1}}\left[\omega_{n_0}^{i_0(j_0'-j_0)}\right]\cdots\left[\omega_{n_{s-1}}^{i_{s-1}(j_{s-1}'-j_{s-1})}\right].$$

Expanding the above sum with respect to each variable, we obtain (25). Since $(j_0,j_1,\ldots,j_{s-1})\neq(j_0',j_1',\ldots,j_{s-1}')$, one of the sums in (25) becomes zero and hence the entire sum becomes zero. ■

From the above theorem, it follows that the designs of Examples 14, 15 and 16 achieve capacity.

Theorem 11: Let D_i, $i=0,1,2,\ldots,s-1$ be s number of crossed-product division algebras.Let each of the STBCs arising from these division algebras be information lossless.

Then the STBC arising from the division algebra $D = D_0 \otimes_F D_1 \otimes_F \cdots \otimes_F D_{s-1}$ is also information lossless if $|\phi_i(.,.)| = 1$ for all $i = 0, 1, 2, \ldots, s-1$, where ϕ_i is a cocycle for the division algebra D_i.

Proof: Can be proved in a similar manner as in Theorem 10. ∎

VI. Decoding and Simulation Results

Maximum Likelihood (ML) decoding of our STBCs in general involves exhaustive search which increases exponentially with the number of transmit antennas. In [36], sphere decoder was proposed, which uses the algorithm to find the closest lattice point to a given point [35]. This algorithm uses the fact that the column rank of the generator matrix of the lattice, is at least the number of dimensions in the lattice. Damen *et al.* in [37], have shown that sphere decoder can be applied for multiple antenna systems if perfect CSI is known at the receiver. If $\mathbf{f}$ is the transmitted vector from n antennas, we have

$$\mathbf{x} = \sqrt{\frac{\rho}{n}} H\mathbf{f} + \mathbf{w} \tag{26}$$

where $\mathbf{x}$ is the received $r \times 1$ vector (r receive antennas), H is the $n \times r$ channel matrix and $\mathbf{w}$ is the AWGN. Then, the lattice representation of the system model is given by

$$\mathbf{x}' = \sqrt{\frac{\rho}{n}} H'\mathbf{f}' + \mathbf{w}' \tag{27}$$

where

$$\begin{aligned} \mathbf{x}' &= [\mathcal{R}e(\mathbf{x}^T)\mathcal{I}m(\mathbf{x}^T)]^T, \\ \mathbf{f}' &= [\mathcal{R}e(\tilde{\mathbf{f}}^T)\ \mathcal{I}m(\tilde{\mathbf{f}}^T)]^T, \\ H' &= \begin{bmatrix} \mathcal{R}e(H) & -\mathcal{I}m(H) \\ \mathcal{I}m(H) & \mathcal{R}e(H) \end{bmatrix}, \\ \mathbf{w}' &= [\mathcal{R}e(\mathbf{w})^T\ \mathcal{I}m(\mathbf{w})^T]^T. \end{aligned}$$

Since, the channel matrix H is of full rank almost surely, the equivalent channel matrix, H', is also of full rank. Hence, the sphere decoder can be applied whenever f is from a constellation which is a subset of a lattice. Hence, SD achieves ML performance with a significantly reduced complexity which is roughly cubic in n at high SNRs [38]. Though PSK constellations are not a subset of any lattice, we can still use the sphere decoder, known as complex sphere decoder, as shown by Hochwald and Brink in [34]. The algorithm for the case of a PSK constellation searches through the phase angles of the constellation points instead of the lattice point coordinates and since the phase angles of the constellation points are integer multiples of $2\pi/M$ (for M-PSK), the search is over a finite set. The complexity of complex sphere decoder is less than the complexity of the sphere decoder for lattice constellations. This is because we search for n points in the case of complex sphere decoder, while we search for $2n$ points in the case of lattice sphere decoder.

In our case, the equivalent channel model is

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

Since, the rank of the matrix $\mathcal{H}$ is $\min(nr, n^2)$ and the matrix Φ is invertible, the rank of the matrix $\widehat{\mathbf{H}}$ is also the $\min(nr, n^2)$. Now, since the rate of our STBCs is n, we can use the sphere decoder efficiently if $\min(nr, n^2) \geq n^2$, which implies that the number of receive antennas is at least the number of transmit antennas. However, if the number of receive antennas is less than the number of transmit antennas, we can use the generalized sphere decoder proposed in [39], which involves more computational complexity. However, we can still use the sphere decoder if we decrease the rate of our STBC. If the number of receive antennas is r, then the rate of our STBC has to be r for efficient use of sphere decoder.

A. Simulation results

In this section, we present simulation results for 2,3 and 4 transmit antennas with 2, 3 and 4 receive antennas respectively, over 4-QAM and 16-QAM signal sets. Figure 5 shows the plots for 2 transmit and 2 receive antennas. We used the STBC of Example 7, with $\delta = e^{0.5j}$. This value of δ is chosen arbitrarily. It can be seen from the figure that with our code, we gain by about 3 dB over the uncoded case at 10^{-4} BER (bit error rate) and by about 0.75 dB, at 10^{-6} BER, over the STBC of [26](named as $B_{2,\phi}$), which is known to be one of the best codes. By choosing δ to maximize the coding gain, we can further improve the performance of our STBC.

Figure 6 shows the plots for 3 transmit and 3 receive antennas. The STBC we used is from Example 9. We gain by about 4 dB over the uncoded case at 10^{-4} BER.

Figure 7 shows the plots for 4 transmit and 4 receive antennas. We used the following STBC (obtained with $F = \mathbb{Q}(j)$ and $K = F(\omega_{16})$):

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

where $g_{i,j} = \sum_{l=0}^{3} f_{j,l}(j^i\omega_{16})^l$ and $f_{i,j} \in S \subset F$ for $i, j = 0, 1, 2, 3$ and $\delta = e^{0.5j}$ (chosen arbitrarily). We gain by about 5 dB, at 10^{-5} BER, over the uncoded and by about 0.8 dB, at 10^{-6} BER, over the STBC of [25], which is claimed to maximize the mutual information.

Figure 8 shows the performance of the STBCs obtained using the division algebras of Section V-B. The division algebra construction-1 curve is for the STBC of Example 14, with $x_1 = e^{j\sqrt{2}}, x_2 = e^{j\sqrt{3}}$ 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 $x_1 = e^{j\sqrt{2}}, x_2 = e^{j\sqrt{3}}$ and $\delta_1 = e^{j\sqrt{0.23}}, \delta_2 = e^{j\sqrt{0.26}}$. The values of x_1 and x_2 are chosen arbitrarily, while the values of δ_1 and δ_2 are chosen to be close to the value of δ in STBC used in Figure 7. We can see that the STBC, where the parameters x_1, x_2, δ_1 and δ_2 are chosen arbitrarily, performs better than the STBC of [25] by about 0.25 dB, but is poorer than the STBC constructed from cyclic division algebra by about 0.5dB. However, the STBC, for which the x_1, x_2 are chosen arbitrarily and δ_1, δ_2 are chosen close to δ, performs better than the STBC of [25] by about 0.9 dB, and better than the STBC from cyclic division

algebra by about 0.1dB. We could perform even better by choosing a better x_1, x_2, δ_1 and δ_2.

From these simulation results and [34], it can be seen that at 10^{-5} BER our code for 2 transmit and 2 receive antennas is approximately 3 dB away from the capacity of the channel with 4-QAM symbols as input and less than 0.5 dB away from the capacity of the channel with 16-QAM symbols as the input. On the other hand at 10^{-5} BER, our 3 transmit and 4 transmit codes are about less than 0.5 dB away from the capacity of the channel with QAM symbols as input.

In Figure 9, we also plot to the block error probabilities of our codes for 2 transmit and 4 antennas and compare them with outage probability. It can be seen that the gap between the block error rates of our codes and outage probability is decreasing with increasing size of the input QAM constellation.

VII. Discussion

The contributions of this paper are

- Using crossed-product algebras, we have constructed arbitrary rate STBCs over apriori specified arbitrary finite subsets of the complex field $\mathbb{C}$. In particular, when the crossed-product algebras are division algebras, we get full-rank STBCs.
- We have shown that Alamouti code and the quasi-orthogonal design of [20] are special cases of our constructions.
- We have also shown that our constructions give STBCs with rank and coding gain same as that of the STBCs obtained using field extensions [11].
- We have given a sufficient condition for our STBCs under which they are information lossless.
- We have identified two classes of division algebras that are crossed-product algebras and constructed rate-n, full-rank STBCs from these crossed-product division algebras. These STBCs include the STBCs of [11], [12] as special cases.
- We have proved that the STBCs obtained from the crossed-product division algebras in this paper, are information lossless.
- We have presented simulation results to 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 we are about 1 dB away from the capacity of the channel with QAM as the input [34].

The following are some possible directions for further research in this area:

- We have seen in Section III, that we can construct the Alamouti code and 4×4 quasi-orthogonal design of [20] using crossed-product algebras. It would be interesting to see if we can construct orthogonal designs other than Alamouti code and other quasi-orthogonal designs like $\begin{bmatrix} A & B \\ -B^* & A^* \end{bmatrix}$, using crossed-product algebras.
- It would be interesting to see if there exits a closed form expression for coding gain of the STBCs arising from non-cyclic division algebras.
- We have shown that we can use the sphere decoder to decode our codes, but as the number of transmit antennas increase, this decoding involves more complexity. It would be interesting to see if there exist any simpler decoding algorithms though suboptimal.

Appendix I
Tensor Products: Definition and some properties

To define tensor product of two algebras, we will first define tensor product of two vector spaces. Since any algebra is a vector space, we will extend the definition of tensor product of two spaces to tensor product of two algebras [31, Chap 9].

Definition 4: Let V and W be two F-vector spaces. A **tensor product** of V and W is an F-vector space $V \otimes_F W$, together with a bilinear mapping $V \times W \mapsto V \otimes_F W$ denoted by $(v, w) \mapsto v \otimes_F w$ such that

1) $V \otimes_F W$ is generated as an F-space by $\{v \otimes_F w | v \in V, w \in W\}$,
2) (Universality) if $\psi : V \times W \mapsto P$ is a bilinear map, where P is another F-space, then there is an F-linear map $\kappa : V \otimes_F W \mapsto P$ such that $\kappa(v \otimes_F w) = \psi(v, w)$.

The following sequence of theorems lists some of the useful properties of tensor products.

Theorem 12: [31] Let V and W be two F-vector spaces. Then,

1) The homomorphism κ in the definition of tensor product $V \otimes_F W$ is unique.
2) If $V \otimes_F W$ and $V \otimes'_F W$ are tensor products of V and W, then there is a unique isomorphism $\phi : V \otimes_F W \mapsto V \otimes'_F W$ such that $\phi(v \otimes_F w) = v \otimes'_F w$ for all $v \in V$ and $w \in W$.

From the above theorem, since any two tensor products of two vector spaces are isomorphic to each other, we can write "a tensor product" of two vector spaces as "the tensor product" of two vector spaces. The following theorem guarantees us the existence of the tensor product of two vector spaces.

Theorem 13: [31] The tensor product of two F-vector spaces V and W exists.

Now, since F-algebras are F-vector spaces, we can define tensor product of two F-algebras as the the tensor product of the corresponding vector spaces with a suitably defined multiplication. The following theorem assures us of such a multiplication.

Theorem 14: [31] If A and B are F-algebras, then there is a multiplication operation on $A \otimes_F B$ that satisfies

$$(x_1 \otimes_F y_1)(x_2 \otimes_F y_2) = x_1 x_2 \otimes_F y_1 y_2.$$

This multiplication is associative and $1_A \otimes_F 1_B = 1_{A \otimes_F B}$.

Theorem 15: [31] Let K be a field containing F and A be an F-algebra. Then, $A \otimes_F K$ is a K-algebra satisfying

$$(x \otimes_F k)(y \otimes_F k') = xy \otimes_F kk'$$

for all $x, y \in A$ and $k, k' \in K$. The scalar operations by elements of K on $A \otimes_F K$ is defined by

$$xk = x(1 \otimes_F k)$$

for all $x \in A \otimes_F K$ and $k \in K$.

REFERENCES

[1] E. Telatar, "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 Communications, Vol.6 pp.311-335, Mar 1998.

[3] G. J. Foschini, "Layered space-time architecture for wireless communications in a fading environment when using multi-element antennas," Bell Labs, Tech. J., Vol.1, No.2, pp.41-59, 1996.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.*

[12] V. Shashidhar, B. Sundar Rajan and B. A. Sethuraman,"STBCs using capacity achieving designs from cyclic division algebras", accepted for presentation at Communication Theory Symposium, GLOBECOM 2003, San Francisco. Available for download at *http://ece.iisc.ernet.in/˜bsrajan.*

[13] 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.

[14] 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.

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

[16] 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.

[17] G. Ganesan and P. Stoica, "Space-time diversity using orthogonal and amicable orthogonal designs," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing* (ICASSP 2000), Istanbul, Turkey, 2000, pp. 2561-2564.

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

[19] 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.

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

[21] 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.

[22] 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.

[23] J.Boutrous and E.Viterbo, "Signal Space Diversity : A power and bandwidth efficient diversity technique for the Rayleigh fading channel," *IEEE Trans. Information Theory*, vol.44, pp.1453-1467, jul 1998.

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

[25] 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.

[26] 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.

[27] 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.

[28] 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.

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

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

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

[32] Paul J. McCarthy, *Algebraic extensions of fi elds*, Dover Publications Inc., New York.

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

[34] Bertrand M. Hochwald and Stephan ten Brink , "Achieving near-capacity on a multiple-antenna channel," *IEEE Trans. Communications*, vol.51, no.3, pp.389-399, March 2003.

[35] U.Fincke and M.Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis, "*Math. Comput.*, vol.44, p.463-471, Apr.1985.

[36] E.Viterbo and J.Boutros, "A universal lattice code decoder for fading channel,"*IEEE Trans. Inform. Theory*, vol.45, pp.1639-1642, July 1999.

[37] 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.

[38] B.Hassibi and H.Vikalo, "On the expected complexity of sphere decoding," in *35th Asilomar Conf. Signals, Syst., Comput.,* vol.2, Nov 2001.

[39] M.O.Damen, K.Abed-Merriam and J.-C.Belfiore, "Generalized sphere decoder for asymmetrical space-time communication architecture," *IEE Electronics letters*, Vol.36, No.2, 20th Jan 2000.

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

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

V.Shashidhar received the B.E. degree in electronics and communications from Andhra University, India and the M.Sc(Engg) and Ph.D in electrical communication engineering from Indian Institute of Science, Bangalore, India in 1997, 2000 and 2004 respectively. Currently, he is working as staff design engineer with Beceem Communications Pvt. Ltd., Bangalore, India.

His research interests include error-control coding, coded modulation, space-time coding.

B.Sundar Rajan was born in India. He received the B.Sc. degree in mathematics from Madras University, India, the B.Tech. degree in electronics from Madras Institute of Technology and the M.Tech. and Ph.D. degrees in electrical engineering from Indian Institute of Technology, Kanpur, India, in 1979, 1982, 1984 and 1989 respectively.

He was a faculty member of Electrical Engineering at the Indian Institute of Technology, Delhi, India from 1990 to 1997. Currently, he is a professor with Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore, India. His primary research interests are in error-control coding, coded modulation, and space-time coding.

Dr.Rajan is a senior member of IEEE and a memeber of American Mathematical Society.

B.A.Sethuraman received his B.Tech. degree in mechanical engineering from Indian Institute of Technology, Chennai, India, and his Ph.D in mathematics from University of Californa at San Diego, USA, in 1980 and 1991 respectively. Currently he is a professor of mathematics at California State University, Northridge, USA.

His interests are in algebra, algebraic geometry, and their applications.

TABLE I

COMPARISON OF VARIOUS KNOWN STBCS (ONLY SQUARE)

STBC or the design	No. of transmit antennas	Rank	Rate	Capacity	Signal set (finite subset of)	Decoding
ODs [7], [16]	power of 2	full	≤ 1	achieves only for $n = 2, r = 1$	$\mathbb{C}$	single-symbol decodable
LDC [27]	arbitrary	full	≤ 1	achieves 90% of the possible	$\mathbb{Z}[j]$	sphere decodable
Damen *et al.* [26]	2	full	2	achieves for any r	$\mathbb{Z}[j]$	sphere decodable
DAST [22]	arbitrary	full	1	away from capacity	$\mathbb{Z}[j]$	sphere decodable
Sethuraman *et al.* [11], [12]	arbitrary	full	arbitrary	away from capacity	any subfield of $\mathbb{C}$	sphere decodable
TAST [24]	arbitrary	full	$\leq n$	close to capacity	depends on constituent code	sphere decodable
Galliou *et al.* [25]	arbitrary	full	n	claim to maximize mutual information	$\mathbb{Z}[j]$	sphere decodable
Belfiore *et al.* [28]	2, 3 and 4	full	n	away from capacity	$\mathbb{Z}[j]$	sphere decodable
Proposed in this paper	arbitrary	full	arbitrary	achieve capacity	any subfield of $\mathbb{C}$	sphere decodable

TABLE II

COCYCLE ϕ FOR THE CROSS-PRODUCT ALGEBRA IN EXAMPLE 13

$\phi(\sigma_i, \sigma_j)$	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5
σ_0	1	1	1	1	1	1
σ_1	1	δ	1	1	δ	δ
σ_2	1	1	1	δ	1	δ
σ_3	1	1	δ	δ	δ	δ
σ_4	1	δ	1	δ	δ	δ^2
σ_5	1	δ	δ	δ	δ^2	δ^2

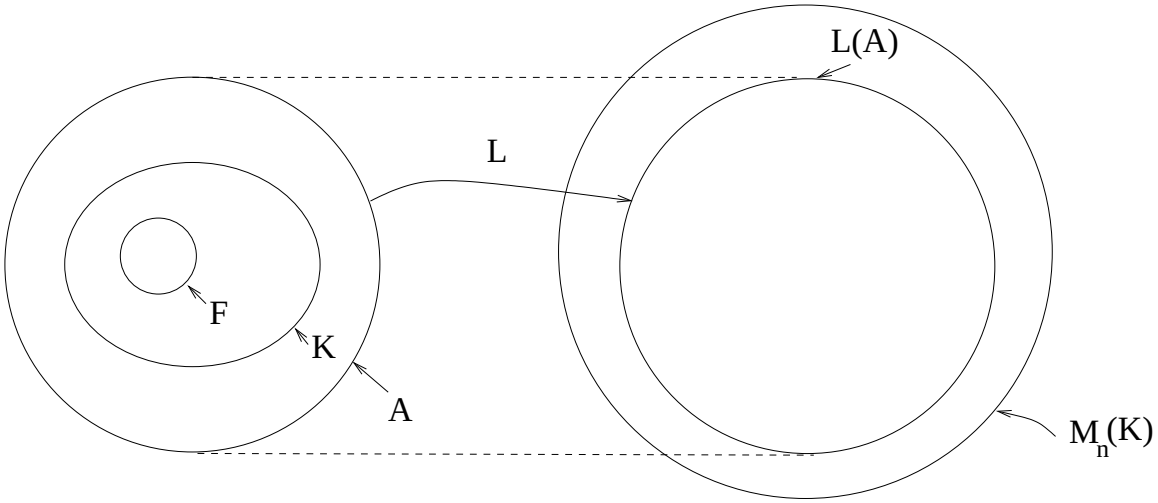

Fig. 1. Embedding of a crossed-product algebra into the set of $n \times n$ matrices over K.

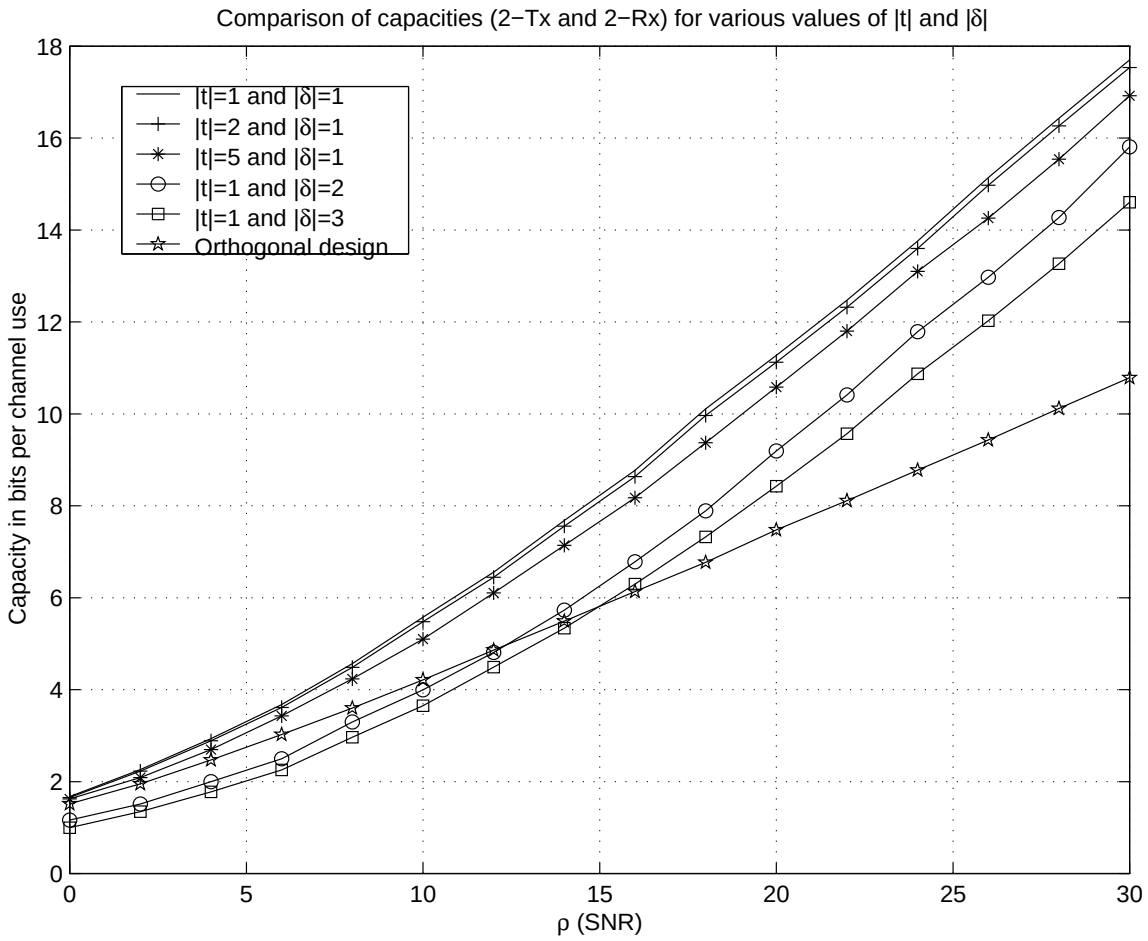

Fig. 2. Comparison of capacities for various values of $|t|$ and $|\delta|$. The plain solid curve is the capacity of the channel too. Also, $\mathbf{R_f} \neq \mathbf{R_{f'}}$ in the cases where $|t| \neq 1$ or $|\delta| \neq 1$

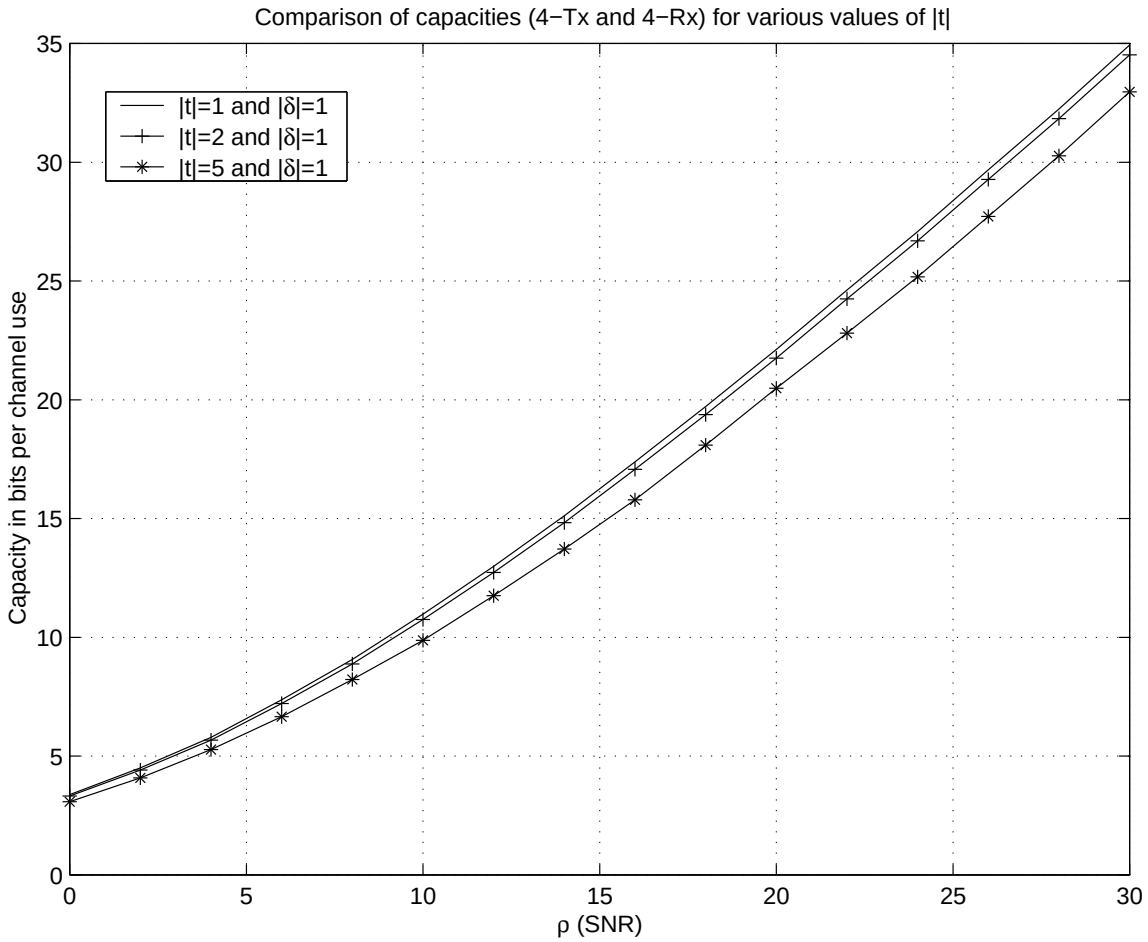

Fig. 3. Comparison of capacities for various values of $|t|$. The plain solid curve is the capacity of the channel too.

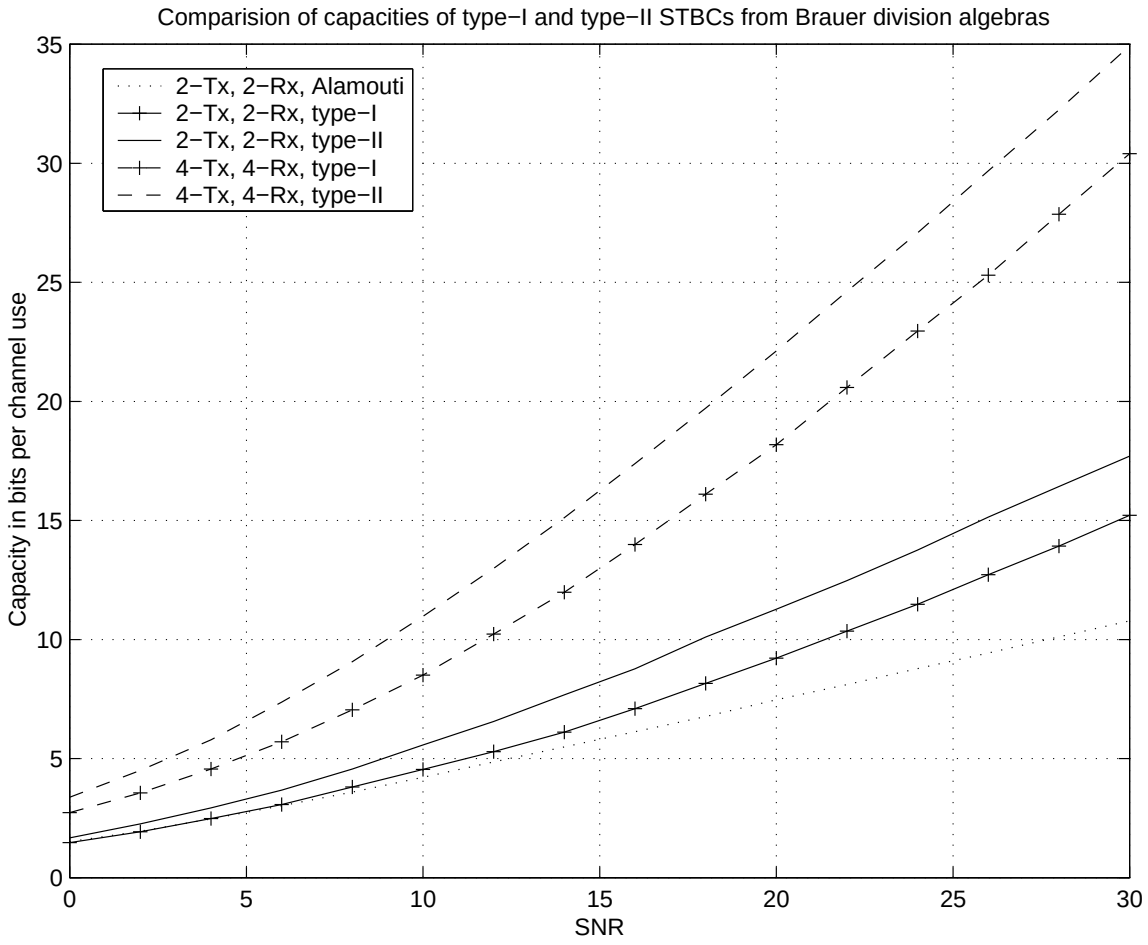

Fig. 4. Comparison of capacities of type-I and type-II STBCs from Brauer division algebras. The plain solid curve is the capacity of the channel for 2-transmit and 2-receive antennas. And the plain dashed curve is the capacity of the channel for 4-transmit and 4-receive antennas.

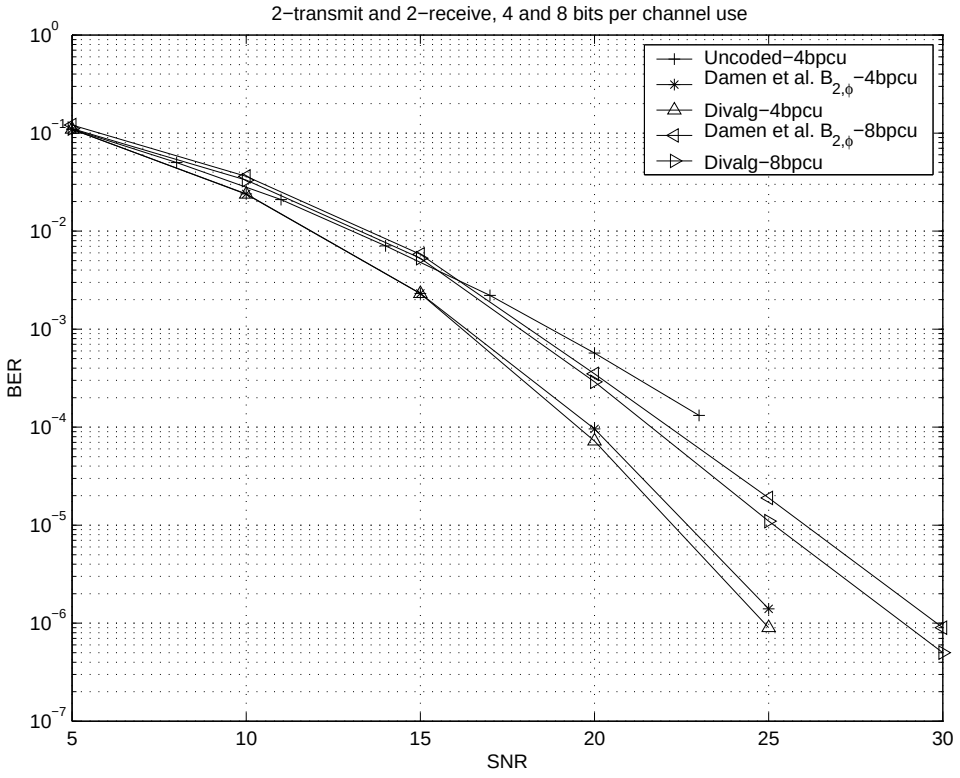

Fig. 5. Comparison of STBCs with 2 transmit and 2 receive antennas

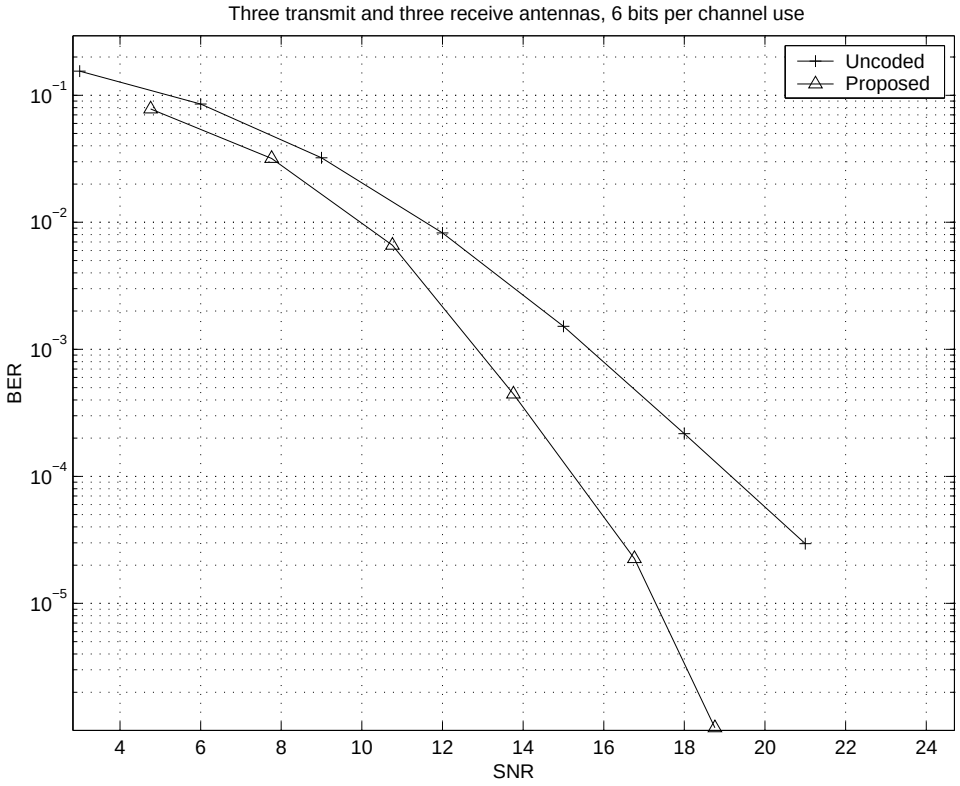

Fig. 6. Comparison of STBCs with 3 transmit and 3 receive antennas

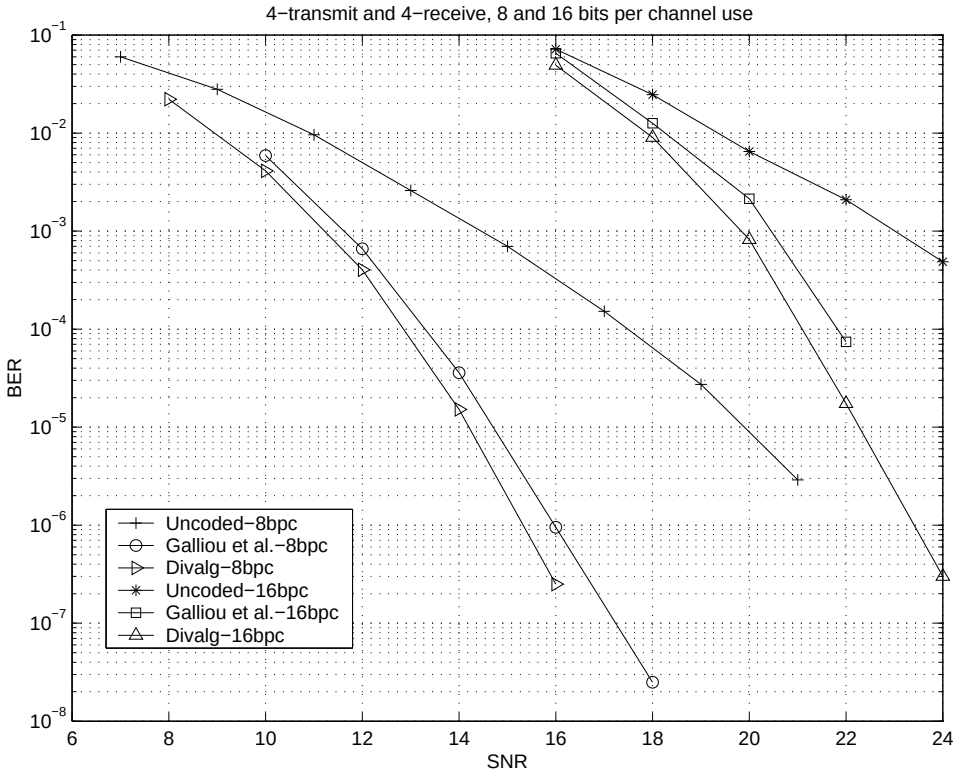

Fig. 7. Comparison of STBCs with 4 transmit and 4 receive antennas

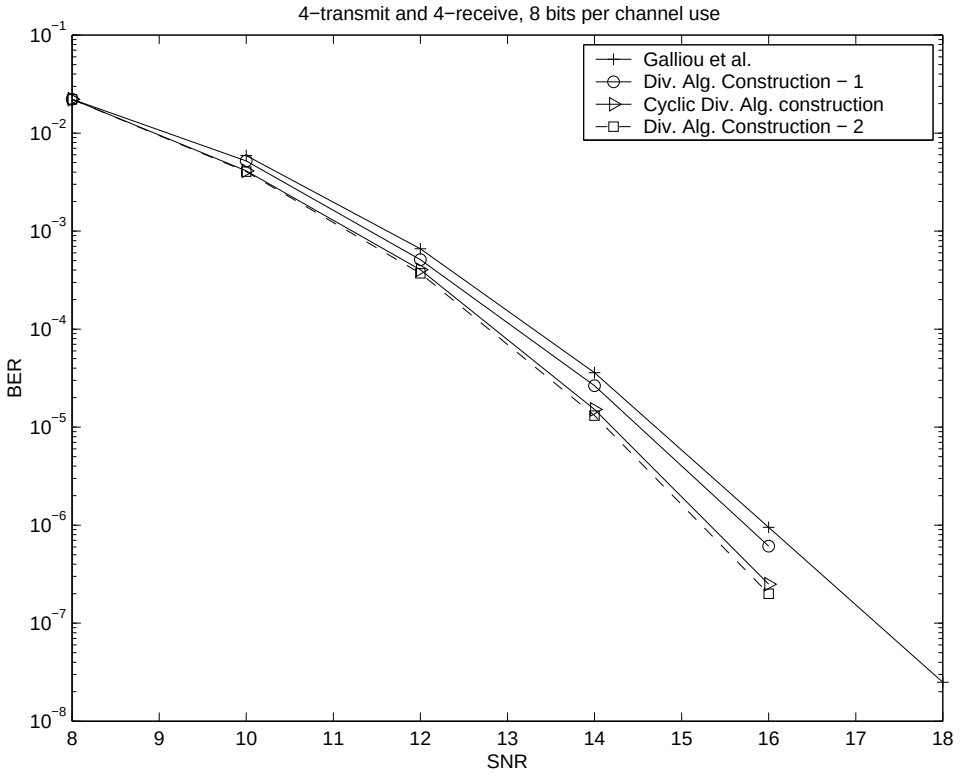

Fig. 8. Comparison of STBCs with 4 transmit and 4 receive antennas

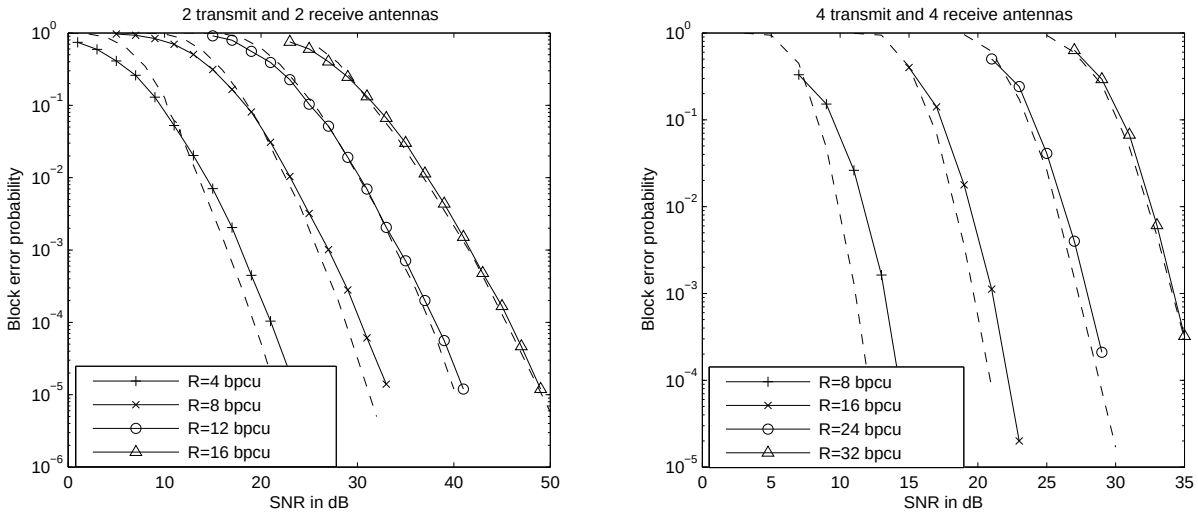

Fig. 9. Comparison of block error probabilities and outage probabilities

Table Captions

1) Comparison of various known STBCs (only square)
2) Cocycle ϕ for the cross-product algebra in Example 13

Figure Captions

1) Embedding of a crossed-product algebra into the set of $n \times n$ matrices over K.
2) Comparison of capacities for various values of $|t|$ and $|\delta|$. The plain solid curve is the capacity of the channel too. Also, $\mathbf{R_f} \neq \mathbf{R_{f'}}$ in the cases where $|t| \neq 1$ or $|\delta| \neq 1$
3) Comparison of capacities for various values of $|t|$. The plain solid curve is the capacity of the channel too.
4) Comparison of capacities of type-I and type-II STBCs from Brauer division algebras. The plain solid curve is the capacity of the channel for 2-transmit and 2-receive antennas. And the plain dashed curve is the capacity of the channel for 4-transmit and 4-receive antennas.
5) Comparison of STBCs with 2 transmit and 2 receive antennas
6) Comparison of STBCs with 3 transmit and 3 receive antennas
7) Comparison of STBCs with 4 transmit and 4 receive antennas
8) Comparison of STBCs with 4 transmit and 4 receive antennas
9) Comparison of block error probabilities and outage probabilities