Full-diversity STBCs for Block-Fading channels from Cyclic codes

U. Sripati
ECE Department
Indian Institute of Science
Bangalore - 560012 INDIA
Email: sripati@protocol.ece.iisc.ernet.in

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

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

***Abstract*— Viewing an n-length vector over F_{q^m} (the finite field of q^m elements) as an $m \times n$ matrix over F_q, by expanding each entry of the vector with respect to a basis of F_{q^m} over F_q, the rank weight of the n-length vector over F_{q^m} is the rank of the corresponding $m \times n$ matrix over F_q. Using appropriate Discrete Fourier Transform (DFT), it is known that under some conditions, n-length cyclic codes over F_{q^m}, ($n|q^m-1$ and $m \leq n$), have full-rank ($= m$). In this paper, using this result, we obtain designs for Full-diversity Space Time Block Codes (STBCs) suitable for block-fading channels from n length cyclic codes over F_{q^m}. These STBCs are suitable for m transmit antennas over signal sets matched to F_q, where $q = 2$ or q is a prime of the form $4k + 1$, $(k = 1, 2, \cdots)$. We also present simulation results which illustrate the performance of a few of these STBCs and show that our codes perform better than the well known codes for block-fading channels.**

I. Introduction

An $m \times l$ $(m \leq l)$ Space Time Block Code (STBC) $\mathcal{C}$ for m transmit antennas over a complex signal set S is a finite number of $m \times l$ matrices with entries from S. Let us consider a system with N_t transmit antennas, N_r receive antennas and codeword length l. In the block-fading model, the codeword is considered to be composed of multiple blocks. The channel fading coefficients are constant over each block and are independent from block to block. For an STBC for a block-fading channel, l is an integral multiple of the length of the block. Let M denote the number of blocks in a codeword. Then, the size of each block is $\delta \triangleq \frac{l}{M}$. When, the codeword length extends over several quasi-static blocks, as in the case of block-fading channels, El Gamal and Hammons [1] have shown that the diversity can be made to increase indefinitely with increase in length of the codeword. In [2], it was shown that the limiting performance in terms of codeword error rate can be improved by coding across multiple blocks. In particular, it was shown that the negative of the exponent of SNR in the codeword error rate for a fixed data rate can be increased to any value by coding across multiple blocks. The following base-band design criteria for block-fading channels have been derived in [1].

Design Criteria for block-fading channels [1]: Let $\mathcal{C}$ be an $n \times l$ STBC code where $\mathbf{c}' = [c'[1], c'[2], \cdots c'[M]]$ and $\mathbf{e}' = [e'[1], e'[2] \cdots e'[M]]$ are any two distinct codewords and $\mathbf{c}'[\tau], \mathbf{e}'[\tau], 1 \leq \tau \leq M$ are the τ^{th} blocks of codewords $\mathbf{c}', \mathbf{e}'$ respectively. The pairwise probability of error is

$$P(\mathbf{c}' \rightarrow \mathbf{e}') \leq \prod_{\tau=1}^{M} \left(\frac{\mu_\tau E_s}{4N_0} \right)^{-d_\tau N_r} \tag{1}$$

where

$$\mu_\tau = (\lambda_1[\tau]\lambda_2[\tau] \cdots \lambda_{d_\tau}[\tau])^{\frac{1}{d_\tau}}, \tag{2}$$

$$d_\tau = rank(c'[\tau] - e'[\tau]) \tag{3}$$

and $\lambda_1[\tau], \lambda_2[\tau], \cdots \lambda_{d_\tau}[\tau]$ are the non zero eigen values of $\mathbf{A}[\tau] = (\mathbf{c}'[\tau] - \mathbf{e}'[\tau])(\mathbf{c}'[\tau] - \mathbf{e}'[\tau])^H$, Hence the generalized diversity and product distance criteria for STBCs over MIMO block-fading channels can be stated as follows :

(i) Block-fading sum of ranks criterion : Maximize the transmit diversity advantage,

$$d = \sum_{\tau=1}^{M} d_\tau = \sum_{\tau=1}^{M} rank(\mathbf{c}'[\tau] - \mathbf{e}'[\tau]) \tag{4}$$

over all pairs of distinct codewords $\mathbf{c}', \mathbf{e}' \in \mathcal{C}$.

From this criterion, it follows that the diversity advantage increases rapidly with increase in the number of blocks M in the codeword if, for all pairwise differences of codewords, the difference blocks $(\mathbf{c}'(\tau) - \mathbf{e}'(\tau)), 1 \leq \tau \leq M$ have full-rank.

(ii) Block-fading Product distance criterion : Maximise the coding advantage,

$$\prod_{\tau=1}^{M} \mu_\tau = \prod_{\tau=1}^{M} \left\{ (\lambda_1[\tau]\lambda_2[\tau] \cdots \lambda_{d_\tau}[\tau])^{\frac{1}{d_\tau}} \right\} \tag{5}$$

over all pairs of distinct codewords $\mathbf{c}', \mathbf{e}' \in \mathcal{C}$.

In [1], full-diversity codes over BPSK and QPSK signal sets have been constructed. In these codes, the coding is done across 2, 3 and 4 blocks. In [3], full-diversity codes with coding across 2, 3 and 4 blocks were constructed for QPSK signal set.

Let $\mathbf{C}$ be an [n,k] linear code over F_{q^m}. For any pair of codewords, $\mathbf{c}$, $\mathbf{e} \in \mathbf{C}$, the rank distance between them is defined to be the rank over F_q of the $m \times n$ matrix corresponding

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

to $\mathbf{c}-\mathbf{e}$ obtained by expanding each entry of $\mathbf{c}-\mathbf{e}$ as an m-tuple along a basis of F_{q^m} over F_q. The rank of $\mathbf{C}$, denoted by $rank_q(\mathbf{C})$ is defined as the minimum of $rank_q(\mathbf{c}-\mathbf{e})$ over all possible pairs of distinct codewords. The rank distance between two codewords $\mathbf{c} \neq \mathbf{e}$ is at most equal to the Hamming distance between them. Combining this with the Singleton bound one gets, $rank_q(\mathbf{C}) \leq min\ \{m, n-k+1\}$. The case where $rank_q(\mathbf{C}) = n-k+1$ has been studied in [4], [5], and are called Maximum Rank distance (MRD) codes. The rank properties of (n,k) cyclic codes over finite fields $F_{q^m},\ (n|q^m-1,\ (n,q)=1)$ have been studied in [6], [7]. In these, exact expressions and tight bounds for the rank of the code have been derived by making use of the Discrete Fourier Transform (DFT) description of these codes.

In this paper, we derive $m \times n$ STBCs having diversity equal to n, suitable for use over block fading channels, from n-length cyclic codes over F_{q^m} where $n|q^m-1,\ m \leq n$ by making use of the rank characterization for cyclic codes [6], [7]. This characterization has been performed by making use of the DFT domain description of cyclic codes [8].

The rest of the content in the paper is organized as follows: In the next section, we will briefly state the theorems associated with the characterization of cyclic codes for the rank metric. In Section III, we obtain $m \times n$ STBCs with diversity equal to n for block-fading channels. In section IV, we present simulation results to show that our codes perform better than the well known codes in terms of codeword error probability and conclude the paper in Section V.

II. Characterisation of Cyclic codes for the Rank metric

We summarize the results relevant to the design of STBCs in Theorems 2.1, 2.2 and 2.3. The proofs of the first two theorems are given in [6], [7] and that of the third is omitted due to space limitations.

Theorem 2.1: Let $\mathbf{C}$ be a cyclic code of length $n|q^m-1,\ (m \leq n)$ over F_{q^m} such that the transform component $A_{jq^s} \in A_{[j]}, |[j]| = e_j, e_j|m$ is free and all other transform components are constrained to zero. Then $rank_q(\mathbf{C}) = e_j$. In other words, for a length $n|q^m-1$ cyclic code over F_{q^m} with only one transform component non zero, the rank of the code is equal to the size of the q-cyclotomic coset to which the free transform component belongs.

In practice, we choose the free transform domain component $A_{jq^s} \in A_{[j]}$ where $e_j = |[j]| = m$ from a full size q-cyclotomic coset. Then from Theorem 2.1 it follows that the rank of the resulting code is m. This code has q^m codewords. These codes are defined over F_{q^m}, have length equal to n and dimension equal to 1.

Theorem 2.2: Let $\mathbf{C}$ be a cyclic code of length $n|q^m-1$ over F_{q^m} whose free transform domain components are A_{jq^r} and $A_{jq^{r+s}}$. (the indices of the free transform domain components belong to the same q- cyclotomic coset and s denotes the seperation between them. $(1 \leq s \leq e_j-1),\ (0 \leq r \leq e_j-2)$. Let all other transform components be constrained to zero. Then, $rank_q(\mathbf{C}) = (e_j - gcd(s, e_j))$.

This Theorem shows that if we try to increase the number of codewords by considering codes with two free transform components from the same q-cyclotomic coset and constraining all other transform components to zero, we can no longer obtain full-rank cyclic codes. Hence, in our search for full-rank STBCs for block-fading channels, we shall confine our study to one dimensional cyclic codes of length n over $F_{q^m}, (n|q^m-1)$.

Theorem 2.3: Let $\mathcal{C}$ be a cyclic code of length $n|q^m-1$ over F_{q^m} such that the transform domain component $A_{jq^s} \in A_{[j]}$ is free and all other transform components are constrained to zero. Let $|[j]| = e_j$. Consider any non zero codeword $\mathbf{a} \in \mathcal{C}$.

$\mathbf{a} = (a_0, a_1, \cdots a_{e_j-1}, \cdots, a_{ke_j}, \cdots a_{(k+1)e_j-1}, \cdots a_{n-1})$

There are two cases:

(i) e_j *divides* n : If $e_j|n$, the $\frac{n}{e_j}$ sets $\{a_0, \cdots a_{e_j-1},\}, \{a_{e_j}, \cdots a_{2e_j-1}\} \cdots \{a_{n-e_j} \cdots a_{n-1})\}$ are linearly independent sets over F_q. If these sets are viewed as $m \times e_j$ matrices over F_q, then each matrix has F_q-rank equal to e_j.

(ii) e_j does not divide n: If e_j does not divide n, the $\lfloor \frac{n}{e_j} \rfloor$ sets $\{a_0, \cdots a_{e_j-1}\}, \{a_{e_j}, \cdots a_{2e_j-1}\}, \cdots$ $\left\{a_{n-\lfloor \frac{n}{e_j} \rfloor - e_j} \cdots a_{n-\lfloor \frac{n}{e_j} \rfloor - 1}\right\}$ are linearly independent and have rank e_j when viewed as $m \times e_j$ matrices over F_q. The last set $\left\{a_{n-\lfloor \frac{n}{e_j} \rfloor} \cdots a_{n-1}\right\}$ consisting of $n - \lfloor \frac{n}{e_j} \rfloor e_j$ terms is also linearly independent and has F_q-rank equal to $n - \lfloor \frac{n}{e_j} \rfloor e_j$ when viewed as a $m \times \left(n - \lfloor \frac{n}{e_j} \rfloor e_j\right)$ matrix over F_q.

This theorem is particularly useful in deriving STBCs suitable for block-fading channels from cyclic codes. Also, it follows that a codeword of length n over F_{q^m} can be divided into several blocks of length e_j, each of which can be viewed as a full-rank $m \times e_j$ matrix over F_q. If the length of the fading block is equal to e_j, it follows from the block-fading sum of ranks criterion, that the effective diversity advantage offered by the code is increased.

We shall use Theorems 2.1 and 2.3 to derive STBCs for block-fading channels from n-length cyclic codes over F_{q^m}.

III. Designs for Block-Fading channels from cyclic Codes

Definition 1: A rate-k/n, $n \times l$ linear design over a field $F \in \mathbb{C}$ is an $n \times l$ matrix with all its entries F-linear combinations of k complex variables and their conjugates which are allowed to take values from the field F.

Let $(n,q) = 1$ and $n|q^m-1$, where q is either 2 or a prime of the form $4k+1$. Let $[j]_n$ be a q-cyclotomic coset of I_n of size m. By restricting $A_j,\ j \in [j]_n$, to F_{q^m} and constraining all other transform components to zero, we have a n-length cyclic code over F_{q^m} whose codewords are of the form,

$$\left[\ A_j, \quad \beta^{-j}A_j, \quad \beta^{-2j}A_j, \quad \cdots \quad \beta^{-(n-1)j}A_j\ \right]$$

where β is a primitive n-th root of unity in F_{q^m} and $A_j \in F_{q^m}$. Viewing A_j as a m-length column vector over F_q, the codewords can be viewed as $m \times n$ matrices over F_q

given by,

$$\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & \cdots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & a_{1,2} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m-1,0} & a_{m-1,1} & a_{m-1,2} & \cdots & a_{m-1,n-1} \end{bmatrix} \quad (6)$$

where $\beta^{-kj}A_j = \sum_{i=0}^{m-1} a_{i,k}\alpha^i$, $a_{i,k} \in F_q$ and α is a primitive element of F_{q^m}. Notice that (6) is a design over F_q. Also, note that this is in general, possible for any linear code, however, we have information about the rank, only in the case of cyclic codes.

Example 1: Let the number of transmit antennas $N_t = 2$. We take $n = 3$. The 2-cyclotomic coset of 1 modulo 3 is $\{1, 2\}$. With A_1 taking all of F_4 and other transform components constrained to zero, we have a rank-2 cyclic code $\mathbf{C}_1$ over F_4. Let α be a cube root of unity in F_4. With x^2+x+1 as the minimal polynomial of α, the codewords of $\mathbf{C}$ are of the form,

$$\begin{bmatrix} a_0 & a_0 + a_1 & a_1 \\ a_1 & a_0 & a_0 + a_1 \end{bmatrix} \quad (7)$$

where $a_0, a_1 \in F_2$.

This is an example of a rate $2/3$ design. A design based on a cyclic code of length n over F_{q^m} is used over a block-fading channel where the channel is known to remain invariant over m successive signalling intervals. These m successive signalling intervals constitute a block. Therefore, we have two cases.

(i) m *divides* n : In this case, each codeword encompasses an integral number of fading blocks. As these codes, can be decomposed into $\frac{n}{m}$ blocks, the components of each of which are linearly independent, we have a $m \times n$ matrix over F_q, which can be decomposed into $\frac{n}{m}$ submatrices, each of F_q-rank m.

(ii) m does not divide n : In this case, we can either delete $\left(n - \lfloor \frac{n}{m} \rfloor m\right)$ columns or add $m - \left(n - \lfloor \frac{n}{m} \rfloor m\right)$ columns such that the last block also consists of linearly independent elements. In the first case, we gain in code rate at the expense of diversity and in the second case we loose in rate and gain in diversity.

To obtain STBCs from the above designs, we have to map the elements of F_q into the complex field such that the full-rank property of the finite field design is preserved. We call a signal set, which is a finite subset of the complex field, as a signal set matched to F_q, if there exists a map from F_q to the signal set which is an isometry for the F_q-rank to the complex field rank. There are two methods for obtaining maps, the Hammons and El Gamal map [9] (suitable for codes over extension fields of F_2) and the map proposed by Lusina, Gabidulin and Bossert [10].

An n-length cyclic code over F_{2^m} will give rise to an $m \times n$ STBC with 2^m codewords for m transmit antennas. Hence, the code rate in bits per channel use is $\frac{1}{n}\log_2(2^m) = m/n$. Now, assuming that we want full-rank STBCs, we have the condition $m \leq n$. Therefore, for the case of cyclic codes over F_{2^m}, the data rate is always upper bounded by 1 bit per channel use and we will not consider the Hammons and El Gamal map here. To achieve higher code rates, we derive STBCs from non binary cyclic codes by making use of the Lusina *et al.* map.

A. $q = 4k + 1$, *Lusina, Gabidulin and Bossert[10]*

Let q be a prime of the form $q = 4k + 1$. By definition a Gaussian integer w is a complex number defined as $w = a + ib,\ a,\ b\ \in \mathbf{Z},\ i = \sqrt{-1}$. From number theory, it is known that every prime number q of the form $q \equiv 1\ mod\ 4$ can be written as $q = (u + iv) \times (u - iv) = u^2 - v^2$. The number $\Pi = u + iv$ is known as Gaussian prime number where $u,\ v\ \in \mathbf{Z}$. Let $\Pi' = u - iv$. Then calculation modulo Π is defined as, $\zeta = w\ modulo\ \Pi = w - \left[\frac{w\Pi'}{\Pi\Pi'}\right]\Pi$ where [.] performs the operation of rounding to the nearest Gaussian integer. The Gaussian integers modulo Π form a field, $G_\pi = \{\zeta_0 = 0,\ \zeta_1 = 1,\ \zeta_2, \cdots, \zeta_{q-1}\}$ and the map $\xi : F_q \Rightarrow G_\Pi$ given by $\zeta_i = i\ mod\ \Pi = i - \left[\frac{i\Pi'}{\Pi\Pi'}\right]\Pi,\ i = 0,\ 1,\ 2, \cdots,\ p-1$ is an isomorphism [10]. Therefore when we map codewords from a linear cyclic code over $F_{q^m},\ q = 5, 13, 17, \cdots$ which are $m \times n$ matrices over F_q to $m \times n$ matrices over the complex Gaussian field, the full-rank property of the code over F_{q^m} is preserved. We give below, an example of the map between F_5 and the corresponding complex Gaussian field.

Example 2: The map between F_5 and G_Π where $\Pi = 1+i2$ is defined by,

$0 \mapsto 0,\ 1 \mapsto 1,\ 2 \mapsto 0 + i1,\ 3 \mapsto 0 - i1,\ 4 \mapsto -1.$

Example 3: Let $N_t = 2$ and $q = 5$. Let the length of the cyclic code be $n = 6$. The 5 -cyclotomic coset of 1 mod 6 is $\{1, 5\}$. With A_1 taking all of $F_{25} = F[x]/(x^2 + x + 1)$ and all other transform components constrained to zero, we have a rank-2 cyclic code over F_5 with 25 codewords which can be expressed as 2×6 matrices over F_5. We make use of the map proposed by Lusina et al. to derive a full-rank 2×6 STBC. From the block-fading sum of ranks criteria, the diversity of this code is 6. The codewords of the STBC are of the form given in (8), where $a_0, a_1 \in F_5$. $\xi : F_5 \mapsto G_{1+2i}$. The code rate of this code in bits per channel use is, $\frac{log_2(25)}{6} = 0.774$.

Example 4: Let $N_t = 2$ and $q = 13$. Let the length of the cyclic code be $n = 7$. The 13 -cyclotomic coset of 1 mod 13 is $\{1, 6\}$. With A_1 taking all of F_{169} generated by $F[x]/(x^2 + x + 2)$ and all other transform components constrained to zero, we have a rank-2 cyclic code over F_{13} with 169 codewords which can be expressed as 2×7 matrices over F_{13}. To increase the rate of STBC derived from this cyclic code, we will delete the last column and then map the resulting 2×6 matrices over F_{13} using the map $\xi : F_{13} \mapsto G_{2+3i}$. This yeilds a full-rank 2×6 STBC with 169 codewords. The diversity of this code is 6. The codewords of this code are of the form given in (9). The code rate in bits per channel use is $\frac{log_2(169)}{6} = 1.233$.

Example 5: Let $N_t = 2$ and $q = 17$. Let the length of the cyclic code be $n = 6$. The 17 -cyclotomic coset of 1 mod 6 is $\{1, 5\}$. With A_1 taking all of $F_{289} = F[x]/(x^2 + x + 3)$ and all other transform components constrained to zero, we have a rank-2 cyclic code over F_{17} with 289 codewords which can

$$\begin{bmatrix} \xi(a_0) & \xi(4a_0+a_1) & \xi(3a_0+a_1) & \xi(4a_0) & \xi(a_0+4a_1) & \xi(2a_0+4a_1) \\ \xi(a_1) & \xi(2a_0+2a_1) & \xi(2a_0+a_1) & \xi(4a_1) & \xi(3a_0+3a_1) & \xi(3a_0+4a_1) \end{bmatrix} \tag{8}$$

$$\begin{bmatrix} \xi(a_0) & \xi(3a_0+5a_1) & \xi(4a_0+11a_1) & \xi(7a_0+a_1) & \xi(a_0+12a_1) & \xi(3a_0+2a_1) \\ \xi(a_1) & \xi(9a_0+3a_1) & \xi(a_0+3a_1) & \xi(6a_0+a_1) & \xi(7a_0+7a_1) & \xi(12a_0+4a_1) \end{bmatrix} \tag{9}$$

$$\begin{bmatrix} \xi(a_0) & \xi(15a_0+12a_1) & \xi(14a_0+8a_1) & \xi(16a_0+5a_1) & \xi(2a_0+a_1) & \xi(3a_0+2a_1) \\ \xi(a_1) & \xi(12a_0+7a_1) & \xi(12a_0+7a_1) & \xi(3a_1) & \xi(5a_0+a_1) & \xi(5a_0+4a_1) \end{bmatrix} \tag{10}$$

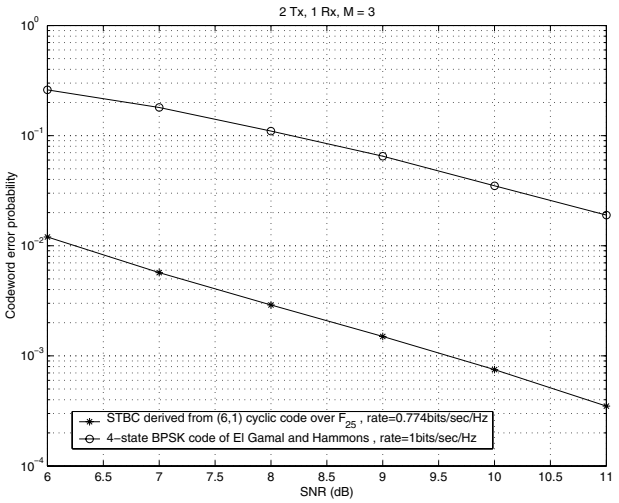

Fig. 1. Performance comparison of length 6 full-rank STBC with diversity of 6 derived from $(6,1)$ cyclic code over F_{5^2} with the best 4 state BPSK space time code derived by El Gamal and Hammons.

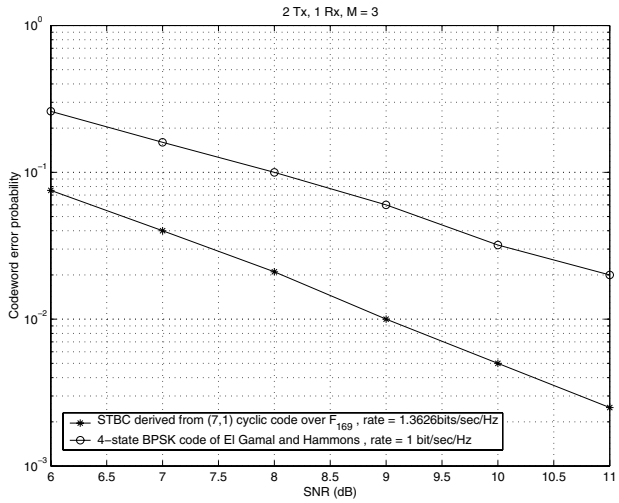

Fig. 2. Performance comparison of length 6 full-rank STBC with diversity of 6 derived from $(7,1)$ cyclic code over F_{13^2} with the best 4 state BPSK space time trellis code derived by El Gamal and Hammons.

be expressed as 2×6 matrices over F_{17}. We make use of the map $\xi : F_{17} \mapsto G_{4+i}$ to derive a full-rank 2×6 STBC. From the block-fading sum of ranks criteria, we conclude that the diversity of this code is 6. The code rate in bits per channel use is $\frac{log_2(289)}{6} = 1.3626$. The codewords of this code are as in (10). We can increase the rate of this code by deleting the last two columns. By doing this we obtain a code with diversity of 4. The code rate in bits per channel use is $\frac{log_2(289)}{4} = 2.043$.

IV. Simulation Results

In this section, we present simulation results and compare the performance of our codes with some well known codes for block-fading channels. These include the codes proposed by El Gamal and Hammons [1], Tarokh, Sheshadri and Calderbank [11] and the Turbo Space Time Code proposed by Stefanov and Duman [3].

In Figure 1, we have compared the error performance of our length 6, full-rank STBC with diversity 6, rate 0.774 derived from a $(6,1)$ cyclic code over F_{5^2} (Example 3), with the 4-state BPSK Space Time Trellis code (STTC) derived by El Gamal and Hammons [1] which has a rate of 1. This happens to be the best performing El Gamal and Hammons code with rate $1bit/sec/Hz$. This is the four state $(5,7)$ optimal free distance space time trellis code with diversity equal to 4. The parameters of this code are, $N_t = 2$, $N_r = 1$, number of fading blocks per codeword M = 3, rate=1. Our code also has the same operational parameters but has rate equal to .774. While the rate of our code is less by about 0.226, we observe that we are able to obtain any given probability of error with a much reduced value of SNR (at least 5 dB less).

In Figure 2, we have compared the error performance of our length 6, full-rank STBC with diversity 6, rate 1.233 derived from a $(7,1)$ cyclic code over F_{13^2} (Example 4), with the 4-state BPSK STTC derived by El Gamal and Hammons. This is the same El Gamal and Hammons code referred to in the context of Figure 1. We observe that our code outperforms this code in both rate and in error performance. (This code is able to achieve any given probability of error at a SNR which is at least 2.5 dB less than that required by the El Gamal and Hammons code). The number of blocks, $M = 3$ for both the codes.

In Figure 3, we have compared the error performance of our length 4, full-rank STBC with diversity 4, rate 2.043 derived from a $(6,1)$ cyclic code over F_{17^2} (Example 5), with the following:

• The linear $\mathbf{Z}_4$ code obtained by lifting the binary $(6,7)$ code with QPSK modulation [1] with parameters, $N_t = 2$, $M = 2$, rate = $2bits/sec/Hz$.

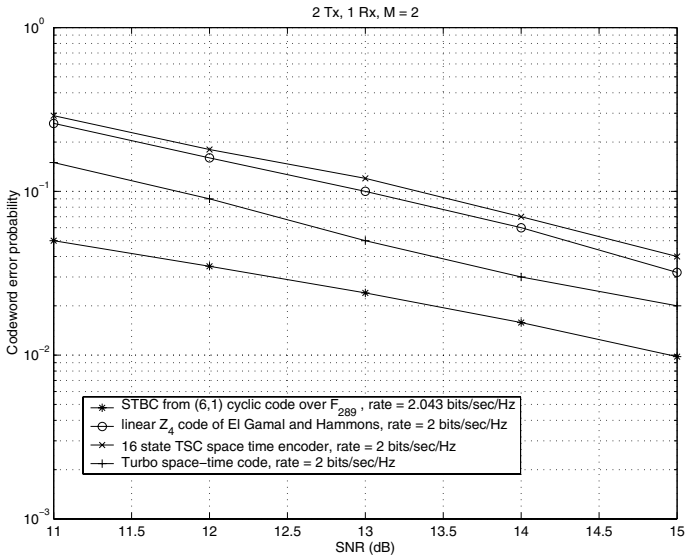

Fig. 3. Performance comparison of length 4 full-rank STBC with diversity of 4 derived from $(6, 1)$ cyclic code over F_{17^2} with the best 16 state QPSK space time code derived by El Gamal and Hammons.

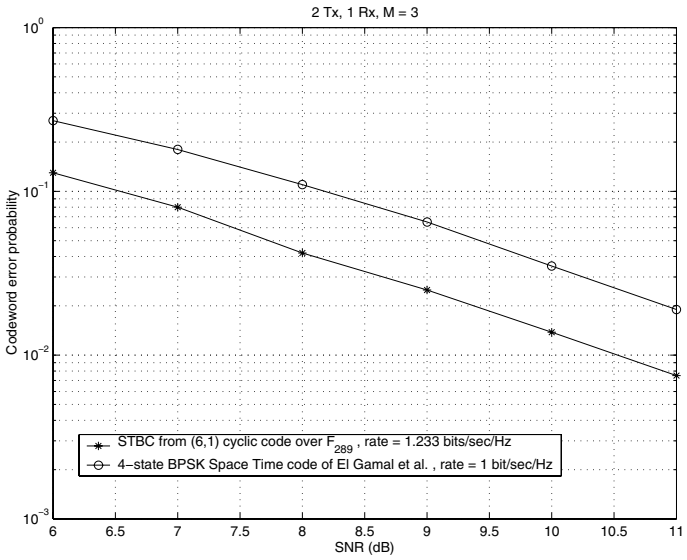

Fig. 4. Performance comparison of length 6 full-rank STBC with diversity of 6 derived from $(6, 1)$ cyclic code over F_{17^2} with the best 4 state BPSK space time code derived by El Gamal and Hammons.

• The 16 state code derived by Tarokh, Sheshadri and Calderbank (TSC) code [11] with rate $2bits/sec/Hz$.

• New Turbo Space Time code [3] with interleaver size $N = 260$, rate=$2bits/sec/Hz$. The path gains are assumed to be constant for a period of 65 transmissions. We observe that our code outperforms all of the above in rate as well as error performance.

In Figure 4, we compare the error performance of our length 6 full-rank STBC with diversity 6, rate 1.3626 derived from $(6, 1)$ cyclic code over F_{17^2} (Example 5), with the 4 state BPSK space time trellis code proposed by El Gamal and Hammons which has a rate of 1. This is the same El Gamal and Hammons code referred to in the context of the Figure 1. The number of blocks $M = 3$ for both the codes. We observe that our codes outperform the codes proposed by El Gamal and Hammons in both rate and error performance.

V. Discussion

We have shown that it is possible to obtain designs for full-rank STBCs matched to MIMO block-fading channels from length $n|q^m - 1$ cyclic codes over F_{q^m}. We have derived performance curves (codeword probability of error as a function of signal to noise ratio) for some of these codes. From the simulation results, we see that these codes offer superior performance as compared to the codes derived in [1], [11] and the Turbo Space time code proposed in [3].

References

[1] H. El Gamal and A. R Hammons, Jr., "On the Design of Algebraic Space-Time Codes for MIMO Block-Fading Channels ," *IEEE Trans. on Inform. Theory*, vol.49, No.1, Jan.-2003, pp. 151-163.

[2] E. Biglieri, G. Caire and G. Taricco, "Limiting performance of block-fading channels with multiple antennas," *IEEE Trans. Inform. Theory*, vol.47, no.4 , May 2001, pp.1273 - 1289

[3] A. Stefanov and T. Duman,"Turbo coded modulation for systems with transmit and receive diversity over Block-fading channels: System model, decoding approaches and practical considerations," *IEEE J. Select Areas Commun.,* vol. 19, pp 958-968, May 2001.

[4] E. M. Gabidulin, "Theory of Codes with Maximum Rank Distance," *Problemy Peredachy Informatsii*, 21, 99.3-14, Jan.-Mar. 1985.

[5] R. M. Roth, "Maximum Rank Array Codes and their application to Criss Cross Error Correction," *IEEE Trans. Inform. Theory,* vol.37, pp.328-336, March 1991.

[6] U. Sripati and B. Sundar Rajan, " On the Rank Distance of Cyclic Codes," *Proc. IEEE Int. Symp. Inform. Theory*, Yokohoma, Japan, June-July 2003, p.72.

[7] B. Sundar Rajan and U. Sripati, "On the Rank Distance of Cyclic Codes," Technical Report no. TR-PME-2003-04 Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore-560012. Available for download at http://ece.iisc.ernet.in/ bsrajan.

[8] R. E. Blahut, *Theory and Practise of Error Control Codes*, Addison Wesley, 1983.

[9] A. Roger Hammons Jr. and Hesham El Gamal, "On the Theory of Space Time Codes for PSK modulation," *IEEE Trans. on Inform. Theory*, vol.46, No.2, pp.524-542, March-2000.

[10] Paul Lusina, E. Gabidulin and Martin Bossert, "Maximum Rank Distance Codes as Space Time Codes," *IEEE Trans. on Inform. Theory*, vol.49, No.10, Oct. 2003, pp. 2757-2760.

[11] V. Tarokh, N. 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, pp.744-765, Mar-1998.