Designs and Full-Rank STBCs from DFT Domain Description of Cyclic Codes

U. Sripati, V. Shashidhar and B. Sundar Rajan
Dept. of Electrical Communication Engineering
Indian Institute of Science, Bangalore 560012, INDIA
{sripati@protocol.,shashidhar@protocol.,bsrajan@}ece.iisc.ernet.in

Abstract — **Viewing an n length vector over F_{q^m} 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. 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. In this paper, using this result we obtain a design using which we construct full-rank Space-Time Block Codes (STBCs) for m transmit antennas over signal sets matched to F_q where $q=2$ or q is a prime of the form $4k+1$. We also propose a construction of STBCs using n-length cyclic codes over F_{q^m}, for r transmit antennas, where $r \leq n$ and $r|m$.**

I. Extended Summary

The characterization of cyclic codes using the Rank metric has been studied in [1]. In this paper, we use the main result of [1] to obtain full-rank STBCs.

Definition 1 *A rate-k/n, $n \times l$* **linear design** *over a field F is an $n \times l$ matrix with all its entries F-linear combinations of k variables 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 code over F_{q^m} whose codewords are of the form, $\begin{bmatrix} A_j & \alpha^{-j}A_j & \alpha^{-2j}A_j & \cdots & \alpha^{-(n-1)j}A_j \end{bmatrix}$ where α 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

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

where $\alpha^{-kj}A_j = \sum_{i=0}^{m-1} A_{i,k}\beta^i$, $A_{i,k} \in F_q$ and β is a primitive element of F_{q^m}. Notice that (1) is a design over F_q and the variables are allowed to take values from a signal set matched to F_q. Also, note that this is possible for any linear code, however only for cyclic codes we have information about the rank. To obtain an STBC from the above design, we have to map the elements of F_q into the complex field such that the rank is preserved. The following maps have been proposed for the same:

Case 1. $q=2$**, Hammons et al. [2]**: A rank preserving map given by Hammons et al.[2] is as follows : $0 \mapsto +1$, $1 \mapsto -1$. Thus, by using the above map, we obtain STBCs over BPSK signal sets.

Case 2. $q=4k+1$**, Lusina et al. [3]**: Let q be a prime of the form $q=4k+1$. Then, it is known that $q=u^2+v^2$ for some integers u and v. Let $\Pi' = u - iv$. Then w modulo Π of any integer w 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 number. In [3], it is proved that the Gaussian numbers modulo Π form a field, $G_\Pi = \{\zeta_0 = 0, \zeta_1 = 1, \zeta_2, \cdots, \zeta_{q-1}\}$ where $\zeta_i = i \bmod \Pi$.

Example 1 *Let the number of transmit antennas be 2 and $q=5$. Then, we take $n=3$ and $m=2$. The 5-cyclotomic coset of 1 is $\{1,2\}$. Thus, allowing only A_1 to take values from F_{25} and constraining other components to zero, we have a full-rank 2×3 STBC with codewords of the form* $\begin{bmatrix} \xi(a_0) & \xi(3a_0+a_1) & \xi(a_0+4a_1) \\ \xi(a_1) & \xi(a_0+2a_1) & \xi(3a_0+3a_1) \end{bmatrix}$ *where $a_0, a_1 \in F_5$ and $\xi : F_5 \mapsto G_{1+2i}$.*

STBCs for r transmit antennas, $r|m$**:** Let q be a prime of the form $4k+1$. Then, we have the map $\xi : F_q \mapsto G_\pi$. Now, let $F_{q^r} = F_q[\beta]$, where β is a root of a polynomial f irreducible over F_q and of degree r.

Theorem 1 *Consider the map $\xi' : F_{q^r} \mapsto G_\pi[\gamma]$ given by $\xi'|_{F_q} = \xi$ and $\xi'(\beta) = \gamma$, where γ is a root of the polynomial $\xi(f)$ in the complex field. Then, the map ξ' is a ring isomorphism. And hence $V \in F_{q^r}^{n \times n}$ is non-singular in F_{q^r} if and only if $\xi'(V)$ is non-singular in the complex field.*

The usage of the above theorem to construct full-rank STBCs is illustrated in the following example.

Example 2 *Let $n=5$ and $q=17$. Then, we have $m=4$. The 17-cyclotomic coset of 1 is $\{1,2,3,4\}$. So, allowing A_1 to take values from F_{17^4} and constraining all other components to zero, we get a length 5 cyclic code* $\mathbf{C}$ *over F_{17^4}. Expand each component into a 2-length column vector over F_{17^2}. The F_{17^2}-rank of this code is equal to 2 because, the size of the 17^2-cyclotomic coset $\{1,4\}$ of 1 is 2. The entries of the codewords over F_{17^2} will be of the form $a_0 + a_1\beta$, where β is a primitive element of F_{17^2} and a root of an irreducible polynomial polynomial $f \in F_{17}[x]$ of degree 2. Let γ be a root of the polynomial $\xi(f)$ in the complex field. Then, using the map ξ', we obtain a full-rank STBC for 2 transmit antennas.*

References

[1] U.Sripati and B.Sundar Rajan, " On the Rank Distance of Cyclic Codes," Proc. IEEE International Symposium on Information Theory, Yokohoma, Japan, June-July 2003, p.72.

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

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

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

0-7803-8280-3/04/$20.00 ©2004 IEEE