DFT CHARACTERIZATION OF MINIMAL QUASICYCLIC CODES

Bikash Kumar Dey and B. Sundar Rajan
Department of Electrical Communication Engineering
Indian Institute of Science, Bangalore 560012 , India
email: bikash@protocol.ece.iisc.ernet.in, bsrajan@ece.iisc.ernet.in

Abstract

Transform domain characterization of linear cyclic codes over finite fields using Discrete Fourier Transform (DFT) over appropriate extension field is well known. In this paper, we extend this transform domain characterization for all linear minimal quasi-cyclic codes over finite fields.
Keywords: *quasicyclic codes, Discrete Fourier Transform, cyclotomic cosets.*

Introduction

A code is called m-quasicyclic if there exists an integer m such that cyclic shift of every codeword by m positions gives another codeword [12]. The class of quasicyclic codes is a generalization of cyclic codes (m=1) and has been studied by several authors in various context. The connection between quasicyclic codes and convolutional codes have been studied in [14] and [4]. In [3] the structural properties and enumeration of quasicyclic codes have been reported. The class of quasicyclic codes contain good codes in the sense of meeting a version of the Gilbert-Varshamov bound [10]. With restrictions on the parameters, quasicyclic codes have been investigated in [1] [5] [6] [7] [8] [9] [13] [15] [16] [17] and [18]. The transform domain characterization of linear cyclic codes using Discrete Fourier Transform (DFT) is well known [2]. Transform domain approach often leads to efficient encoder and decoder structures for the code [2]. A quasicyclic code is called minimal if it does not contain any proper nonzero quasicyclic subcode. It can be shown that any linear quasicyclic code can be decomposed as direct sum of linear minimal quasicyclic codes (not necessarily uniquely). In this paper we obtain transform domain characterization of all linear minimal quasicyclic codes over finite fields using appropriate DFT.

Preliminaries

Let F_{q^r} denote the finite field of cardinality q^r. We consider linear codes over F_q of length n where $(n,q) = 1$. Let m be a positive integer dividing n. Throughout the paper we discuss only linear minimal quasicyclic codes. Let r be the smallest positive integer such that $n|(q^r-1)$ and $\alpha \in F_{q^r}$ be an element of order n. DFT of a vector $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1}) \in F_q^n$ is defined to be $\mathbf{A} = (A_0, A_1, \cdots, A_{n-1}) \in F_{q^r}^n$, where

$$A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i \quad \text{for } j = 0, 1, \cdots, n-1. \tag{1}$$

For Any $j \in [0, n-1]$, the **q-cyclotomic coset modulo** n of j, denoted by $[j]_n$, is defined as

$$[j]_n = \{i \in [0, n-1] | j \equiv iq^t \bmod n \text{ for some nonnegative integer } t\}.$$

Similarly, on the same set $[0, n-1]$, we define q-**cyclotomic coset modulo** $\frac{n}{m}$ of j, denoted by $[j]_{\frac{n}{m}}$, as

$$[j]_{\frac{n}{m}} = \{i \in [0, n-1] | j \equiv iq^t \bmod \tfrac{n}{m} \text{ for some nonnegative integer } t\}.$$

We define the **length of** $[j]_{\frac{n}{m}}$ as the number of elements in it that are less than $\frac{n}{m}$. The length of $[j]_n$ is same as its size and will be denoted by r_j. Note that the length of $[j]_{\frac{n}{m}}$ is the same as the length of $[jm]_n$

and hence is denoted by r_{mj}. Clearly, a q-cyclotomic coset modulo $\frac{n}{m}$ is union of some q-cyclotomic cosets modulo n. If $J \subseteq [0, n-1]$, we write $[J]_n = \cup_{j \in J} [j]_n$ and $[J]_{\frac{n}{m}} = \cup_{j \in J} [j]_{\frac{n}{m}}$.

Example 1: In $\{0,1,2,3,4,5,6,7,8\}$, the cyclotomic cosets modulo 9 and modulo $\frac{9}{3} = 3$ are

$$[0]_9 = \{0\}; [1]_9 = \{1,2,4,5,7,8\}; [3]_9 = \{3,6\}$$

$$[0]_3 = \{0,3,6\}; [1]_3 = \{1,2,4,5,7,8\}.$$

The length of the cyclotomic cosets modulo 9 are same as the size these sets, whereas the length of $[0]_3$ is 1 and not same as its size. Similarly, the length of $[1]_3$ is 2 whereas its size is 6.

The DFT defined as above satisfy

(i) Conjugacy Constraint : $\mathbf{A} \in F_{q^r}^n$ is DFT of some vector $\mathbf{a} \in F_q^n$ if and only if $A_{jq} = A_j^q$ for all $j \in [0, n-1]$. Clearly, this constraint restricts A_j to be in the subfield $F_{q^{r_j}}$, where r_j is the length of $[j]_n$. Note that a specific value for A_j uniquely specifies the value of all the transform components $A_{j'}$ for $j' \in [j]_n$.

(ii) Cyclic Shift Property : If $\mathbf{A} = DFT(\mathbf{a})$, $\mathbf{b} \in F_q^n$ such that $b_i = a_{i-1}$, and $\mathbf{B} = DFT(\mathbf{b})$, then $B_j = \alpha^j A_j$.

Let $\mathcal{C}$ be a cyclic code and $\mathcal{C}_D = \{DFT(\mathbf{a}) | \mathbf{a} \in \mathcal{C}\}$. We shall say that A_j, the j-th transform component of $\mathbf{a}$, takes values from $\{A_j | \mathbf{A} \in \mathcal{C_D}\}$. If $S \subseteq F_{q^r}$, then we call the subcode $\{\mathbf{a} \in \mathcal{C} | A_j \in S\}$ to have been obtained by restricting the j^{th} transform component in S. If $L \subset [0, n-1]$, then the code obtained by restricting $\{A_j | j \notin L\}$ to zero is denoted as $\mathcal{C}_L$ and is called **the L-subcode of $\mathcal{C}$**.

Now, the transform domain characterization of cyclic code is the following: The set of j-th transform components of all the codewords of a linear cyclic code is either $F_{q^{r_j}}$ or $\{0\}$, and conversely the set of inverse DFT vectors of all the vectors of a subspace of $DFT(F_{q^n}) \subset F_{q^r}^n$, in which transform components in $[j]_n, \;\; j = 0, 1, ..., n-1$, of every vector take either only the zero value or all the values of $F_{q^{r_j}}$, and transform components in disjoint $[j_1]_n$ and $[j_2]_n$ take values independently, constitute a cyclic code.

From the above characterization, it is clear that to specify the cyclic code, it is sufficient to specify the set $[J]_n$ in which the transform components of all the codewords is zero. It is important to note that the transform components A_j and A_k can never be related unless $[j]_n = [k]_n$. The main result of this paper is that if transform components from different cyclotomic cosets modulo n are related appropriately one gets quasicyclic codes and all quasicyclic codes are describable in terms of these relations. Moreover, for quasicyclic codes the transform component A_j can take values from certain proper (non-trivial) subspaces of $F_{q^{r_j}}$ (viewed as vector space of F_q), which is not possible for a cyclic code. We start from describing these subspaces:

Definition 1 *For every $s \in F_{q^r}^*$, (nonzero elements of F_{q^r}), an F_q-subspace V of F_{q^r} is called an* **s-invariant subspace** *if it is closed under multiplication by s. An s-invariant subspace is said to be minimal if it does not have any proper nonzero s-invariant subspace.*

Example 2: We discuss all minimal s-invariant subspaces in F_{2^4} when s runs over all nonzero elements of F_{2^4}. Let α be a primitive element of F_{2^4}. There are five minimal α^5-invariant subspaces: $\{0, 1, \alpha^5, \alpha^{10}\}$, $\{0, \alpha, \alpha^6, \alpha^{11}\}$, $\{0, \alpha^2, \alpha^7, \alpha^{12}\}$, $\{0, \alpha^3, \alpha^8, \alpha^{13}\}$ and $\{0, \alpha^4, \alpha^9, \alpha 14\}$. All these five are minimal α^{10}-invariant subspaces also. There are fifteen minimal $\alpha^0 = 1$-invariant subspaces each consisting of the zero element and any one nonzero element of F_{2^4}. For all other values of s there is only one minimal s-invariant subspace which is F_{2^4}.

Since for quasicyclic codes several transform components from different cyclotomic cosets modulo n can be related we formalize the notion of related and free set of transform components as follows:

Definition 2 *Suppose the transform components $A_{j_1}, A_{j_2}, \cdots, A_{j_t}$ take values respectively from the sets $V_1, V_2, \cdots, V_t$. These transform components are called* **unrelated** *or* **free** *in $\mathcal{C}$ if $\{(A_{j_1}, A_{j_2}, \cdots, A_{j_t}) | \mathbf{a} \in \mathcal{C}\} = V_1 \times V_2 \times \cdots \times V_t$.*

Definition 3 *Let $I_1, I_2, \cdots, I_t$ be some disjoint subsets of $[0, n-1]$ and suppose $R_{I_l} = \left\{(A_i)_{i \in I_l} | \mathbf{a} \in \mathcal{C}\right\}$ for $l = 1, 2, \cdots, t$. The classes of transform components $\{A_i | i \in I_1\}, \{A_i | i \in I_2\}, \cdots, \{A_i | i \in I_t\}$ are called* **mutually unrelated** *if*

$\{((A_i)_{i\in I_1}, (A_i)_{i\in I_2}, \cdots, (A_i)_{i\in I_t}) \,|\mathbf{a} \in \mathcal{C}\}$
$= R_{I_1} \times R_{I_2} \times \cdots \times R_{I_t}$.

Quasicyclic Codes in Transform Domain

Let $\mathcal{C}$ be a linear m-quasicyclic code and

$$\mathcal{C}_D = \{DFT(\mathbf{a})|\mathbf{a} \in \mathcal{C}\}.$$

From the definition of linear quasicyclic codes and the cyclic shift property, it follows that $\mathcal{C}_D$ should satisfy the following two properties:

1. $\mathcal{C}_D$ is a vector space over F_q.
2. If $\mathbf{A} \in \mathcal{C}_D$ and $\mathbf{B} \in F_{q^r}^n$ such that $B_j = \alpha^{mj} A_j$ for $j = 0, 1, \cdots, n-1$, then $\mathbf{B} \in \mathcal{C}_D$.

The second property above leads to

Theorem 1 *The set of j-th transform component of all the codewords of a linear m-quasicyclic code is an α^{mj}-invariant subspace of $F_{q^{r_j}}$.*

If $\mathcal{C}$ is m-quasicyclic and $S \subset F_{q^r}$ is α^{mj} invariant, then clearly the subcode obtained by restricting the j^{th} transform component to S is also m-quasicyclic. If the nonzero transform components can be partitioned into two mutually unrelated and disjoint subsets, then clearly, the code is direct sum of the two subcodes obtained by restricting each subset of transform components to zero. In particular, if the subsets are of the form S and S^c where $S^c = [0, n-1] \setminus S$, then we have $\mathcal{C} = \mathcal{C}_S \bigoplus \mathcal{C}_{S^c}$.

Note that when specialized to m=1, Theorem 3.1 reduces to the well known fact for cyclic codes: the set of values taken by A_j is either $\{0\}$ or $F_{q^{r_j}}$. In the case of cyclic codes components of transform vectors from two different $[j_1]_n$ and $[j_2]_n$ can never be related to each other. Whereas for m-qyasicyclic codes they can be related provided $[j_1]_n$ and $[j_2]_n$ are in the same cyclotomic coset modulo $\frac{n}{m}$. Notice that when m=1, the set of cyclotomic cosets modulo n and modulo $\frac{n}{m}$ are identical and there is no room to relate transform components of different cyclotomic cosets.

Minimal Quasicyclic Codes

In a minimal quasicyclic code any nonzero A_j should take values from a minimal α^{mj}-invariant subspace, since otherwise, we can restrict A_j to a minimal α^{mj} invariant subspace to get a proper quasicyclic subcode.

Now, consider any $j, k \in [0, n-1]$ such that none of A_j and A_k are zero for all the codewords of a minimal m-quasicyclic code $\mathcal{C}$. Suppose A_j and A_k take values from the minimal α^{mj}-invariant and α^{mk}-invariant subspaces V_{mj} and V_{mk} respectively. Since the code is minimal, if A_j is restricted to $\{0\}$, then the subcode obtained is the zero code. Since the code is linear, for any other element β in V_{mj}, there is only one codeword in $\mathcal{C}$ with $A_j = \beta$. This is true for any nonzero transform component in $\mathcal{C}$. So, A_j and A_k are related by a linear invertible map of V_{mj} onto V_{mk}. But because the code is quasicyclic, any arbitrary linear invertible map can not relate two nonzero transform components.

Using the following two lemmas we obtain Theorem 4 that identifies the relations between transform components of different cyclotomic cosets modulo n that give minimal m-quasicyclic codes.

Lemma 2 *Let $\sigma : F_{q^l} \to F_{q^l}$ be an F_q-linear invertible map and β and β' two elements of F_{q^l} with cardinality of their conjugacy classes l. If $\sigma(\beta a) = \beta' \sigma(a)$ $\forall a \in F_{q^l}$, then, $\beta' = \beta^{q^t}$ for some $t < l$ and $\sigma : a \longmapsto ca^{q^t}$ $\forall a \in F_{q^l}$ for some $c \in F_{q^l}$.*

Lemma 3 *Let β and β' be two elements of F_{q^r} such that lengths of their conjugacy classes are both l, and sF_{q^l} and $s'F_{q^l}$ be two β and β' invariant subspaces in F_{q^r}. Suppose $\sigma : sF_{q^l} \longrightarrow s'F_{q^l}$ is an F_q linear invertible map. Then σ satisfies $\sigma(\beta a) = \beta' \sigma(a)$ if and only if $\beta' = \beta^{q^t}$ and $f_\sigma(X) = cX^{q^t}$ for some $c \in F_{q^r}$ and $t < l$.*

Theorem 4 *In a minimal linear m-quasicyclic code, transform components in only one cyclotomic coset modulo $\frac{n}{m}$, say $[j]_{\frac{n}{m}}$, is nonzero and any two nonzero transform components A_{j_1} and A_{j_2}, where $j_1, j_2 \in [j]_{\frac{n}{m}}$ and $[j_1]_n \neq [j_2]_n$, are related by an isomorphism σ with $f_\sigma(X) = cX^{q^t}$ for some $c \in F_{q^r}$, where t is such that $j_2 \equiv j_1 q^t$ mod $\frac{n}{m}$.*

Proof: In a minimal quasicyclic code, if A_{j_1} and A_{j_2} are nonzero, then A_{j_1} and A_{j_2} take values from minimal mj_1 and mj_2 invariant subspaces of $F_{q^{r_{j_1}}}$ and $F_{q^{r_{j_2}}}$ respectively, and A_{j_2} is dependent on A_{j_1} by an F_q-linear invertible map σ, i.e., $A_{j_2} = \sigma A_{j_1}$. Since the code is m-quasicyclic, σ should satisfy $\sigma(\alpha^{mj_1}a) = \alpha^{mj_2}\sigma(a)$. So, by using lemma (3) with $\beta = \alpha^{mj_1}$ and $\beta' = \alpha^{mj_2}$, we see that $mj_2 \equiv mj_1 q^t \bmod n$ for some $t < r_{mj_1}$, i.e., mj_2 and mj_1 are in same cyclotomic coset modulo n or equivalently, j_2 and j_1 are in same cyclotomic coset modulo $\frac{n}{m}$. So, in a minimal quasicyclic code, transform components are nonzero only in one cyclotomic coset modulo $\frac{n}{m}$. Moreover, again by lemma (3.3), if $j_2 \equiv j_1 q^t \bmod \frac{n}{m}$, then the isomorphism σ is given by $f_\sigma(X) = cX^{q^t}$ for some $c \in F_{q^r}$. $\square$

Discussion

In this paper, we have obtained a generalization of the well known DFT domain characterization of cyclic codes over finite fields. to describe linear minimal quasicyclic codes. A detailed treatment including several examples and extension to nonminimal quasicyclic codes can be seen in [19].

References

[1] V. K. Bhargava, G. E. Seguin and J. M. Stein, "Some (mk, k) Cyclic Codes in Quasi-Cyclic Form", *IEEE Trans. Inform. Theory*, vol. 24, pp. 630-632, Sep 1978.

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

[3] J. Conan and G. Seguin, "Structural Properties and Enumeration of Quasi Cyclic Codes", *Applicable Algebra in Engineering Communication and Computing*, pp. 25-39, Springer-Verlag 1993.

[4] M. Esmaeili, T. A. Gulliver, N. P. Secord and S. A. Mahmoud, "A Link Between Quasi-Cyclic Codes and Convolutional Codes", *IEEE Trans. Inform. Theory*, vol-44, pp. 431-435, Jan 1998.

[5] T. A. Gulliver and V. K. Bhargava, "Two New Rate 2/p Binary Quasi-Cyclic Codes", *IEEE Trans. Inform. Theory*, vol-40, pp. 1667-1668, Sep 1994.

[6] T. A. Gulliver and V. K. Bhargava, "Some Best Rate 1/p and Rate (p-1)/p Systematic Quasi-Cyclic Codes", *IEEE Trans. Inform. Theory*, vol-37, pp. 552-555, May 1991.

[7] T. A. Gulliver and V. K. Bhargava, "Nine Good Rate (m-1)/pm Quasi-Cyclic Codes", *IEEE Trans. Inform. Theory*, vol-38, pp. 1366-1369, Jul 1992.

[8] T. A. Gulliver and V. K. Bhargava, "Some Best Rate 1/p and Rate (p-1)/p Systematic Quasi-Cyclic Codes over GF(3) and GF(4)", *IEEE Trans. Inform. Theory*, vol-38, pp. 1369-1374, Jul 1992.

[9] T. A. Gulliver and V. K. Bhargava, "Twelve Good Rate (m-r)/pm Quasi-Cyclic Codes", *IEEE Trans. Inform. Theory*, vol-39, pp. 1750-1751, Sep 1993.

[10] T. Kasami, "A Gilbert-Varshamov Bound for Quasi-Cyclic Codes of Rate 1/2", *IEEE Trans. Inform. Theory*, vol-24, pp. 627-628, Sep 1978.

[11] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press.

[12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1988.

[13] F. J. MacWilliams, "Decomposition of Cyclic Codes of Block Lengths 3p, 5p, 7p", *IEEE Trans. Inform. Theory*, vol 25, pp. 112-118, Jan 1979.

[14] G. Solomon and Van Tilborg, "A Connection Between Block and Convolutional Codes", SIAM J. Appl. Math., vol. 37, pp. 358-369, Oct 1979.

[15] J. M. Stein and V. K. Bhargava, "Equivalent Rate $\frac{1}{2}$ Quasi-Cyclic Codes", *IEEE Trans. Inform. Theory*, vol-21, pp. 588-589, Sep 1975.

[16] J. M. Stein, V. K. Bhargava and S. E. Tavares, "Weight Distribution of Some "Best" (3m, 2m) Binary Quasi-Cyclic Codes", *IEEE Trans. Inform. Theory*, vol-21, pp. 708-711, Nov 1975.

[17] S. E. Tavares, V. K. Bhargava and S. G. S. Shiva, "Some Rare-p/(p+1) Quasi-Cyclic Codes", *IEEE Trans. Inform. Theory*, vol-20, pp. 133-135, Jan 1974.

[18] H. V. Tilborg, "On Quasi-Cyclic Codes with Rate 1/m", *IEEE Trans. Inform. Theory*, vol 24, pp. 628-630, Sep 1978.

[19] Bikash Kumar Dey and B.Sundar Rajan, "DFT Domain Characterisation of Quasicyclic Codes," Submitted to IEEE Transactions on Information Theory.