AAECC **13**, 453–474 (2003)

AAECC
Applicable Algebra in Engineering, Communication and Computing
© Springer-Verlag 2003

DFT Domain Characterization of Quasi-Cyclic Codes

Bikash Kumar Dey, B. Sundar Rajan*

Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore 560012, India (e-mail: bikash@protocol.ece.iisc.ernet.in, bsrajan@ece.iisc.ernet.in)

Received: January 17, 2002; revised version: November 30, 2002

Abstract. The transform domain characterization of linear cyclic codes over finite fields using Discrete Fourier Transform (DFT) over an appropriate extension field is well known. In this paper, we extend this transform domain characterization for linear quasi-cyclic codes over finite fields. We show how one can derive a lower bound on the minimum Hamming distance of a quasi-cyclic code and decode the code upto that minimum Hamming distance using this characterization.

Keywords: Quasi-cyclic codes, Discrete Fourier transform, Cyclotomic cosets.

1 Introduction

A code is said to be m-quasi-cyclic if the cyclic shift of every codeword by m positions gives another codeword [18]. The class of quasi-cyclic codes is a generalization of the class of cyclic codes (m=1) and has been studied by several authors in various contexts. The connection between quasi-cyclic codes and convolutional codes has been studied in [20] and [6]. The class of quasi-cyclic codes contains good codes in the sense of meeting a version of the Gilbert-Varshamov bound [14]. With restrictions on the parameters, quasi-cyclic codes have been investigated in [1, 7, 8, 9, 10, 11, 19, 21, 22, 24, 30]. Quasi-cyclic codes have been studied in terms of circulant matrices in [12] and [13].

There has been a renewed interest in quasi-cyclic codes [3, 5, 6, 15, 23] due to their close relationship with tail-biting representations of general block

* This work was partly supported by CSIR, India, through Research Grant (22(0298)/99/EMR-II) to B. S. Rajan
Part of this work was presented in ICCCD 2000, Kharagpur, India and ISIT 2001, Washington D.C., USA

codes [3]. For instance, motivated by the 64-state quasi-cyclic representation of the (24, 12, 8) Golay code, reported in [20], the theory of tail-biting representation of block codes was initiated in [3] and the minimal tail-biting trellises for several codes including the Golay code were reported.

For studying m-quasi-cyclic codes, quite often [1, 6, 7, 8, 9, 10, 11, 14, 15, 20, 21, 22, 23, 30] the co-ordinates of a codeword $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1})$ are permuted and blocked as $((a_0, a_m, a_{2m}, \cdots, a_{(\frac{n}{m}-1)m}), (a_1, a_{m+1}, a_{2m+1}, \cdots, a_{(\frac{n}{m}-1)m+1}), \cdots, (a_{m-1}, a_{2m-1}, a_{3m-1}, \cdots, a_{n-1}))$. With this co-ordinate ordering, the generator and parity check matrices (with possibly some redundant rows) can be written as matrices with $\frac{n}{m} \times \frac{n}{m}$ circulant matrices as elements. It specializes to cyclic codes with $m = 1$ resulting in only one block in the codewords and circulant matrices as the generator and parity check matrices. In the recent paper [15], Lally and Fitzpatrick consider codewords in the blocked polynomial form as $(a^{(0)}(X), a^{(1)}(X), a^{(2)}(X), \cdots, a^{(m-1)}(X))$ where $a^{(i)}(X) = a_i + a_{i+m}X + a_{i+2m}X^2 + \cdots + a_{i+(\frac{n}{m}-1)m}X^{\frac{n}{m}-1}$ and view an m-quasi-cyclic code as a submodule of $\left(\frac{F_q[X]}{(X^{\frac{n}{m}}-1)}\right)^m$. The authors then investigate the structural properties of m-quasi-cyclic codes with the help of Groebner bases of modules over $F_q[X]$. Essentially the same module structure was imposed by Conan and Seguin in [4, 25] in the unblocked forms of the codewords. They imposed an $F_q[X]$-module structure on an m-quasi-cyclic code by defining $f(X).\mathbf{a} = f(T^m)(\mathbf{a})$, where T is the cyclic shift operator. Since $(X^{\frac{n}{m}} - 1) \subseteq F_q[X]$ annihilates the code, the code can be seen as an $\frac{F_q[X]}{(X^{\frac{n}{m}}-1)}$ module. Unblocked polynomial form of a codeword can be obtained from the blocked polynomial form of a codeword as $a(X) = a^{(0)}(X^m) + Xa^{(1)}(X^m) + X^2a^{(2)}(X^m) + \cdots + X^{m-1}a^{(m-1)}(X^m))$.

In [23], Tanner gave ways to transform a block circulant binary parity check matrix into a parity check matrix over an extension field by a block wise DFT or linearized polynomial transform. He gave an interesting way to estimate a lower bound on the minimum Hamming distance from such a parity check matrix. For using the block wise DFT, one needs the condition $(\frac{n}{m}, 2) = 1$, whereas the linearized polynomial transform does not need any such condition to be satisfied. Using the block wise DFT, Ling and Solé [17] showed that in some cases quasi-cyclic codes can be constructed by well known construction methods from shorter codes.

The transform domain characterization of linear cyclic codes using DFT is well known [2]. An extension of this to abelian codes has been reported in [26] and to cyclic and abelian codes over integer residue rings in [27] and [28]. In [29] repeated-root cyclic codes have been studied in the transform domain. A transform domain approach often leads to efficient encoder and decoder structures for a code [2].

In this paper we investigate the structural properties of m-quasi-cyclic codes in transform domain using the n-length DFT of the unblocked codewords. This needs $(n, q) = 1$, an even stronger condition than $(\frac{n}{m}, q) = 1$. In a similar way

as in [23], we show how our approach can give a useful lower bound on the minimum Hamming distance.

The contents of this paper are organized as follows. In the next section we briefly describe the known DFT characterization of linear cyclic codes and introduce certain cyclotomic cosets and invariant subspaces needed for extending the characterization to quasi-cyclic codes. In Section 3, we present the DFT characterization for all minimal m-quasi-cyclic codes. In Section 4, we deal with non-minimal m-quasi-cyclic codes, and using results of Section 3, we obtain a DFT characterization of m-quasi-cyclic codes. The duals of quasi-cyclic codes and self-dual quasi-cyclic codes are discussed in Section 5. Construction of parity check equations over an extension field from the transform domain structure of an m-quasi-cyclic code is studied in Section 6. How such parity check equations can give a lower bound on the minimum Hamming distance is also discussed in this section. Finally Section 7 concludes this paper.

2 Preliminaries

Let F_q denote the finite field of cardinality q. We consider linear codes over F_q of length n where $(n, q) = 1$. Let m be a positive integer dividing n. A code is said to be *m-quasi-cyclic* if the code is closed under cyclic shift by m symbols. Obviously, m=1 gives cyclic codes. Throughout the paper we discuss only linear m-quasi-cyclic codes.

Let r be the smallest positive integer such that $n|(q^r - 1)$ and $\alpha \in F_{q^r} \setminus \{0\}$ be an element of order n. The 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

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

The inverse DFT is given by

$$a_i = n^{-1} \sum_{j=0}^{n-1} \alpha^{-ij} A_j \quad \text{for } i = 0, 1, \cdots, n-1. \tag{2}$$

For any $j \in [0, n-1]$, the *residue class modulo* $\frac{n}{m}$ of j, denoted by $(j)_{n,m}$, is defined as

$$(j)_{n,m} = \{i \in [0, n-1] | j \equiv i \bmod \tfrac{n}{m}\}.$$

Cardinality of $(j)_{n,m}$ is m for all $j \in [0, n-1]$. If a vector is cyclically shifted m times, the transform components whose indices lie in a residue class modulo $\frac{n}{m}$ are multiplied by the same scalar.

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

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

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

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

For any subset $S \subseteq [0, n-1]$, with misuse of terminology, we shall call the DFT components with indices in S as the '*DFT components in S*'. 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 the 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, $r_{mj} = r_{mk}$ if $[j]_{\frac{n}{m}} = [k]_{\frac{n}{m}}$ and $r_j = r_k$ if $[j]_n = [k]_n$. Each q-cyclotomic coset modulo $\frac{n}{m}$ of $[0, n-1]$ corresponds to a q-cyclotomic coset modulo $\frac{n}{m}$ of $[0, \frac{n}{m} - 1]$. Suppose $S = [j]_{\frac{n}{m}} \cap [0, \frac{n}{m} - 1]$. Then clearly $[j]_{\frac{n}{m}} = S \cup (S + \frac{n}{m}) \cup \cdots \cup (S + (m-1)\frac{n}{m})$. So, $|[j]_{\frac{n}{m}}| = m|S| = mr_{mj}$.

Clearly, a q-cyclotomic coset modulo $\frac{n}{m}$ is the 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 $[J]_{\frac{n}{m}} = \cup_{j \in J} [j]_{\frac{n}{m}}$. Clearly, $[j]_{\frac{n}{m}} = \left[(j)_{n,m}\right]_n$.

Example 2.1 In $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, the binary cyclotomic cosets modulo 9 and modulo $\frac{9}{3} = 3$ are respectively

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

and

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

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

The DFT defined by (1) is an F_q-linear map satisfying the following two properties.

Conjugacy constraint: $\mathbf{A} \in F_{q^r}^n$ is the 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 values of all the transform components $A_{j'}$ for $j' \in [j]_n$.

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 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 be obtained by restricting the j^{th} transform component in S. If $L \subset [0, n-1]$, then the subcode obtained by restricting $\{A_j | j \notin L\}$ to zero is called *the L-subcode of* $\mathcal{C}$ and will be denoted by $\mathcal{C}_L$.

Now, the transform domain characterization of cyclic codes 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 a cyclic code, it is sufficient to specify the set $[J]_n$ in which the transform components of all the codewords are 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 the m-quasi-cyclic codes and any m-quasi-cyclic code is describable in terms of these relations.

Moreover, for any m-quasi-cyclic code, a transform component A_j can take values from certain proper (non-trivial) subspaces of $F_{q^{r_j}}$ (viewed as a vector space over F_q) which is not possible for a cyclic code. We proceed to describe these subspaces.

Definition *For every $s \in F_{q^r}^*$ (the 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 the multiplication by s. A nonzero s-invariant subspace is said to be minimal if it does not have any proper nonzero s-invariant subspace.*

Example 2.2 We discuss all the minimal s-invariant subspaces of F_{2^4} when s runs over all the nonzero elements of F_{2^4}. Let α be a primitive element of F_{2^4}. There are five minimal α^5-invariant subspaces: $V_1 = \{0, 1, \alpha^5, \alpha^{10}\}$, $V_2 = \{0, \alpha, \alpha^6, \alpha^{11}\}$, $V_3 = \{0, \alpha^2, \alpha^7, \alpha^{12}\}$, $V_4 = \{0, \alpha^3, \alpha^8, \alpha^{13}\}$ and $V_5 = \{0, \alpha^4, \alpha^9, \alpha^{14}\}$. All these five subspaces 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 any other value of s there is only one minimal s-invariant subspace which is F_{2^4}.

If $\alpha \in F_{q^r}$ is an element of order n, then it is known that $\{\alpha^{jt} | t \geq 0\}$ spans the subfield $F_{q^{r_j}}$. So the α^j-invariant subspaces are nothing but the $F_{q^{r_j}}$-subspaces and any minimal α^j-invariant subspace of F_{q^r} is of the form $\beta F_{q^{r_j}}$ for some $\beta \in F_{q^r}^*$. So the number of minimal α^{mj}-invariant subspaces in $F_{q^{r_j}}$ is $\dfrac{q^{r_j} - 1}{q^{r_{mj}} - 1}$.

Since for an m-quasi-cyclic code several transform components from different cyclotomic cosets modulo n can be related, we formalize the notions of related and unrelated sets of transform components below.

For any subset $J = \{j_1, j_2, \cdots, j_k\} \subseteq [0, n-1]$, A_J denotes the ordered tuple $(A_{j_1}, A_{j_2}, \cdots, A_{j_k})$ where an arbitrary fixed order in J is assumed. For some ordered tuples $T_1 = (t_{11}, \cdots, t_{1,j_1}), \cdots, T_l = (t_{l,1}, \cdots, t_{l,j_l})$ the concatenated tuple $(t_{11}, \cdots, t_{1,j_1}, \cdots, t_{l,1}, \cdots, t_{l,j_l})$ is denoted by $(T_1, \cdots, T_l)$.

Definition *Let $I_1, I_2, \cdots, I_t$ be some disjoint subsets of $[0, n-1]$ and suppose $R_{I_l} = \left\{A_{I_l} | \mathbf{a} \in \mathcal{C}\right\}$ 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 said to be mutually unrelated for $\mathcal{C}$ if $\left\{\left(A_{I_1}, A_{I_2}, \cdots, A_{I_t}\right) | \mathbf{a} \in \mathcal{C}\right\} = R_{I_1} \times R_{I_2} \times \cdots \times R_{I_t}$. Otherwise they are said to be related.*

3 Quasi-Cyclic Codes in Transform Domain

Let $\mathcal{C}$ be a linear m-quasi-cyclic code and $\mathcal{C}_D = \{DFT(\mathbf{a}) | \mathbf{a} \in \mathcal{C}\}$. From the definition of a linear m-quasi-cyclic code 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 3.1 *Let $J = \{j_1, j_2, \cdots, j_m\} \subseteq [0, n-1]$ be a residue class modulo $\frac{n}{m}$ with $j_1 < j_2 < \cdots < j_m$. The set of ordered tuples of transform components $A_J = \left(A_{j_1}, A_{j_2}, \cdots, A_{j_m}\right)$ of all the codewords of a linear m-quasi-cyclic code is an $F_{q^{r m_{j_1}}}$-subspace of $F_{q^{r_{j_1}}} \times F_{q^{r_{j_2}}} \times \cdots \times F_{q^{r_{j_m}}}$.*

However A_J can not take values from any arbitrary $F_{q^{r m_{j_1}}}$-subspace. The subspace should conform with the conjugacy constraint on the components. For example, consider binary 3-quasi-cyclic codes of length 9. The set $\{0, 3, 6\}$ is a residue class modulo 3. The 3-tuple (A_0, A_3, A_6) should take values from an F_2-subspace V of $F_2 \times F_4 \times F_4$ such that any vector $x = (x_1, x_2, x_3) \in V$ satisfies $x_3 = x_2^2$.

If $\mathcal{C}$ is m-quasi-cyclic 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-quasi-cyclic. If the nonzero transform components can be partitioned into two mutually unrelated and disjoint subsets, then clearly, the code is the direct sum of the two subcodes obtained by restricting each subset of transform components to zero. In particular, for two mutually unrelated subsets of the form S and S^c where $S^c = [0, n-1] \setminus S$, we have $\mathcal{C} = \mathcal{C}_S \bigoplus \mathcal{C}_{S^c}$. An m-quasi-cyclic code is called *minimal* if it does not have any proper nonzero m-quasi-cyclic subcode.

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 the transform components from two different $[j_1]_n$ and $[j_2]_n$ can never be related to each other. Whereas for m-quasi-cyclic codes they can be related provided $[j_1]_n$ and $[j_2]_n$ are in the same q-cyclotomic coset modulo $\frac{n}{m}$ [Theorem 3.4]. Notice that when $m = 1$, the q-cyclotomic cosets modulo n and the q-cyclotomic cosets modulo $\frac{n}{m}$ are identical and there is no room to relate transform components of different q-cyclotomic cosets.

In the following subsection we discuss minimal m-quasi-cyclic codes and the general case is discussed in the next section.

3.1 Minimal Quasi-Cyclic Codes

In a minimal m-quasi-cyclic code, for any $j \in [0, n-1]$, 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 m-quasi-cyclic 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-quasi-cyclic 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 since the code is m-quasi-cyclic, an arbitrary linear invertible map can not relate two nonzero transform components.

The following two lemmas will help to identify the possible linear invertible maps, connecting two given nonzero transform components in a minimal m-quasi-cyclic code.

Lemma 3.2 *Let $\sigma : F_{q^l} \to F_{q^l}$ be an F_q-linear invertible map and β and β' be 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 unique $c \in F_{q^l}$.*

Proof. Any map of F_{q^l} into F_{q^l} is induced by a unique polynomial over F_{q^l} of degree at most $q^l - 1$ [16]. Let the polynomial $f_\sigma(X) = \sum_{i=0}^{q^l-1} c_i X^i \in F_{q^l}[X]$ be such that $\sigma(a) = f_\sigma(a)\ \forall a \in F_{q^l}$. In this case, $c_0 = 0$ since $f_\sigma(0) = \sigma(0) = 0$. For any $s \in F_{q^l}$, define the permutation $\lambda_s : F_{q^l} \longrightarrow F_{q^l}$ as $\lambda_s : a \longmapsto sa$. By hypotheses,

$$\sigma\lambda_\beta = \lambda_{\beta'}\sigma. \tag{3}$$

Clearly,

$$f_{\sigma\lambda_\beta}(X) = \sum_{i=1}^{q^l-1} c_i \beta^i X^i$$

and

$$f_{\lambda_{\beta'}\sigma}(X) = \sum_{i=1}^{q^l-1} c_i \beta' X^i.$$

Equation (3) implies

$$c_i \beta^i = c_i \beta' \text{ for } i = 1, 2, \cdots, q^l - 1$$

$$\Rightarrow \beta^i = \beta' \text{ whenever } c_i \neq 0.$$

If, for some $i_1 \leq q^l - 1$, we have $c_{i_1} \neq 0$, then $f_\sigma(X) = c_{i_1} X^{i_1} + \cdots$.
Since σ is F_q-linear, we have

$$\sigma(sa) = s\sigma(a) \quad \forall s \in F_q \text{ and } \forall a \in F_{q^l}$$

$$\Rightarrow \sigma\lambda_s = \lambda_s \sigma \quad \forall s \in F_q$$

$$\Rightarrow c_{i_1} s^{i_1} = s c_{i_1} \quad \forall s \in F_q$$

$$\Rightarrow s = s^{i_1} \quad \forall s \in F_q$$

$$\Rightarrow i_1 = q^{l_1} \text{ for some } l_1 < l.$$

Suppose, $\exists\, i_1 = q^{l_1}$, $i_2 = q^{l_2}$, $l_1, l_2 < l$, such that $c_{i_1}, c_{i_2} \neq 0$. Then,

$$\beta' = \beta^{q^{l_1}} = \beta^{q^{l_2}}$$

$$\Rightarrow l | (l_2 - l_1)$$

$$\Rightarrow l_2 = l_1.$$

So, there is only one nonzero term in $f_\sigma(X)$ and that is of degree q^t for some non-negative integer $t < l$ and thus the lemma follows.

Lemma 3.3 *Let β and β' be two elements of F_{q^r} such that the 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 $\sigma(\beta a) = \beta'\sigma(a)$ $\forall a \in sF_{q^l}$ if and only if $\beta' = \beta^{q^t}$ and $f_\sigma(X) = cX^{q^t}$ for some unique $c \in s's^{-q^t} F_{q^l}$ and $t < l$.*

Proof. The reverse implication is trivial. So we prove the forward implication only.
Let us define a map $\sigma' : F_{q^l} \longrightarrow F_{q^l}$ as $\sigma' : a \longmapsto (s')^{-1}\sigma(sa)$. Clearly, σ' is an F_q-linear map and

$$\begin{aligned}\sigma'(\beta a) &= (s')^{-1}\sigma(s\beta a)\\ &= (s')^{-1}\beta'\sigma(sa)\\ &= \beta'\sigma'(a).\end{aligned}$$

So by Lemma 3.2, $\beta' = \beta^{q^t}$ for some $t < l$ and $f_{\sigma'}(X) = c'X^{q^t}$ for some $c' \in F_{q^l}$.
By the definition of σ', $\sigma(a) = s'\sigma'(s^{-1}a)$; $\forall a \in sF_{q^l}$ and so, $f_\sigma(X) = s' f_{\sigma'}(s^{-1}X) = s's^{-q^t}c'X^{q^t} = cX^{q^t}$ where $c = s's^{-q^t}c'$.

The following theorem identifies the relations between the transform components in different q-cyclotomic cosets modulo n that give the minimal m-quasi-cyclic codes.

Theorem 3.4 *In a minimal m-quasi-cyclic code of length n, the transform components in only one q-cyclotomic coset modulo $\frac{n}{m}$, say $[j]_{\frac{n}{m}}$, are nonzero. 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 unique $c \in F_{q^r}$, where t is such that $j_2 \equiv j_1 q^t \bmod \frac{n}{m}$. If A_{j_1} and A_{j_2} take values from $sF_{q^{r_{mj}}}$ and $s'F_{q^{r_{mj}}}$ respectively, then $c \in s's^{-q^t}F_{q^{r_{mj}}}$.*

Proof. In a minimal m-quasi-cyclic code, if A_{j_1} and A_{j_2} are nonzero, then A_{j_1} and A_{j_2} take values from minimal α^{mj_1} and α^{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-quasi-cyclic, σ should satisfy $\sigma(\alpha^{mj_1}a) = \alpha^{mj_2}\sigma(a)$. So, by using Lemma (3.3) with $\beta = \alpha^{mj_1}$ and $\beta' = \alpha^{mj_2}$, we see that $mj_2 \equiv mj_1q^t \bmod n$ for some $t < r_{mj_1}$, i.e., mj_2 and mj_1 are in the same q-cyclotomic coset modulo n. Equivalently, j_2 and j_1 are in the same q-cyclotomic coset modulo $\frac{n}{m}$. So, in a minimal m-quasi-cyclic code, the transform components are nonzero only in one q-cyclotomic coset modulo $\frac{n}{m}$. Moreover, again by Lemma (3.3), if $j_2 \equiv j_1q^t \bmod \frac{n}{m}$, then the isomorphism σ is given by $f_\sigma(X) = cX^{q^t}$ for some $c \in F_{q^r}$.

Example 3.1 Consider binary (q=2) 3-quasi-cyclic codes ($m = 3$) of length $n = 9$. The binary cyclotomic cosets modulo n are $\{0\}, \{3, 6\}$ and $\{1, 2, 4, 5, 7, 8\}$ and the binary cyclotomic cosets modulo $\frac{n}{m} = 3$ are $\{0, 3, 6\}$ and $\{1, 2, 4, 5, 7, 8\}$. The number of minimal α^{mj}-invariant subspaces in $F_{q^{r_j}}$ is given by $\frac{q^{r_j}-1}{q^{r_{mj}}-1}$. For the example under consideration these values are tabulated in Table 1 for all the binary cyclotomic cosets. (The double vertical lines demarcate the cyclotomic cosets modulo $\frac{n}{m}$ and the single vertical lines further demarcate the binary cyclotomic cosets modulo n in the binary cyclotomic cosets modulo $\frac{n}{m}$.) The minimal 3-quasi-cyclic codes with non-zero transform

components only in the cyclotomic coset $\{1, 2, 4, 5, 7, 8\}$ can not be related to transform components in any other cyclotomic cosets and there are 21 such codes each corresponding to one α^3-invariant subspace of F_{2^6}. Table 2 shows all the other minimal 3-quasi-cyclic codes possible. There is one minimal 3-quasi-cyclic code ($\mathcal{C}_1$ in Table 2) with DFT components taking nonzero values only in the binary cyclotomic coset $\{0\}$ modulo 9, and there are three ($\mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4$ in Table 2) with DFT components taking nonzero values only in $\{3, 6\}$. There are three minimal 3-quasi-cyclic codes in which DFT components in $\{0\}$ and $\{3, 6\}$ are nonzero and related. These are $\mathcal{C}_5, \mathcal{C}_6, \mathcal{C}_7$ in Table 2, and the relations are given by $A_3 = cA_0^{2^t}$ where $t = 0$ and the values of c are respectively $1, \alpha^{21}$ and α^{42}. For comparison, the total number of minimal cyclic codes ($m = 1$) is given at the bottom of the table.

The relations in the above example for the codes with related transform components turn out to be simple and straightforward. To exemplify transform components in more than two q-cyclotomic cosets modulo n being related, we give the following example.

Example 3.2 Consider binary codes of length 15. We have m-quasi-cyclic codes for $m = 3$ and $m = 5$. For both these values, the binary cyclotomic cosets and possible minimal m-quasi-cyclic codes are classified in Table 1. In Table 3, we list the codewords and their transform vectors for four minimal 5-quasi-cyclic codes with transform components in different 2-cyclotomic cosets modulo n related. For the code $\mathcal{C}_1$, the transform components in 2-cyclotomic cosets $\{7, 11, 13, 14\}$ and $\{1, 2, 4, 8\}$ are related and the relation is $A_7 = \alpha^7 A_1$, that is, $t = 0$ and $c = \alpha^7$. The relations for the codes $\mathcal{C}_2$ and $\mathcal{C}_3$ are respectively $A_5 = \alpha^6 A_1^2$ and $A_7 = \alpha^3 A_5^2$. The code $\mathcal{C}_4$ is obtained by relating the transform components in three 2-cyclotomic cosets $\{1, 2, 4, 8\}, \{5, 10\}$ and $\{7, 11, 13, 14\}$. The relations are $A_5 = \alpha^{11} A_1^2$ and $A_7 = \alpha^3 A_1$.

Clearly, any nonzero vector is contained in a minimal m-quasi-cyclic code if and only if the DFT components of the vector are nonzero only in one q-cyclotomic coset modulo $\frac{n}{m}$. That minimal m-quasi-cyclic code is spanned by the m-shifts of the vector.

4 Arbitrary Quasi-Cyclic Codes

Let $\mathcal{C}$ be an arbitrary m-quasi-cyclic code and suppose A_j is nonzero for $\mathcal{C}$ and takes values from an α^{mj}-invariant subspace V of $F_{q^{r_j}}$. Let V_1 and V_2 be two α^{mj}-invariant subspaces of V such that $V = V_1 + V_2$. If $\mathcal{C}_1$ and $\mathcal{C}_2$ are the m-quasi-cyclic subcodes obtained by restricting A_j in the subspaces V_1 and V_2 respectively, then clearly, $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2$. (However if $V = V_1 \oplus V_2$,

Table 1. Details pertaining to Examples 3.1 and 3.2

	$q=2,\ n=9,\ m=3,\ \frac{n}{m}=3$			$q=2,\ n=15,\ m=3,\ \frac{n}{m}=5$					$q=2,\ n=15,\ m=5,\ \frac{n}{m}=3$				
Cyclotomic Cosets modulo $\frac{n}{m}$	$\{0,3,6\}$		$\{1,2,4,8,7,5\}$	$\{0,5,10\}$		$\{1,2,3,4,6,7,8,9,11,12,13,14\}$			$\{0,3,6,9,12\}$		$\{1,2,4,5,7,8,10,11,13,14\}$		
Length of $[j]_{\frac{n}{m}} = r_{mj}$	1		2	1		4			1		2		
Cyclotomic Cosets modulo n	$\{0\}$	$\{3,6\}$	$\{1,2,4,8,7,5\}$	$\{0\}$	$\{5,10\}$	$\{1,2,4,8\}$	$\{3,6,12,9\}$	$\{7,14,13,11\}$	$\{0\}$	$\{3,6,12,9\}$	$\{1,2,4,8\}$	$\{7,14,13,11\}$	$\{5,10\}$
Length of $[j]_n = r_j$	1	2	6	1	2	4	4	4	1	4	4	4	2
Number of min. α^{mj} -invariant subspaces in $F_{q^{r_j}}$	1	3	21	1	3	1	1	1	1	15	5	5	1
# of min. quasi-cyclic codes with unrelated transform components	1	3	21	1	3	1	1	1	1	15	5	5	1
# of min. quasi-cyclic codes with related transform components	3		0	3		270			15		330		
Total# of min. quasi-cyclic codes	28			280					372				
Total# of min. cyclic codes	3			5					5				

Table 2. Minimal 3-quasi-cyclic codes of Example 3.1

	Codewords									DFT									
	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
$\mathcal{C}_1$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
$\mathcal{C}_2$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	1	1	0	1	1	0	1	1	0	0	0	1	0	0	1	0	0
$\mathcal{C}_3$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	1	0	1	1	0	1	1	0	0	0	0	α^{21}	0	0	α^{42}	0	0
$\mathcal{C}_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	1	1	0	1	1	0	1	0	0	0	α^{42}	0	0	α^{21}	0	0
$\mathcal{C}_5$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0
$\mathcal{C}_6$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	1	0	0	1	0	0	1	1	0	0	α^{21}	0	0	α^{42}	0	0
$\mathcal{C}_7$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	1	0	0	1	0	0	1	0	1	0	0	α^{42}	0	0	α^{21}	0	0

then $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$ need not be true. In fact, $\mathcal{C}_1 \cap \mathcal{C}_2$ is the subcode of $\mathcal{C}$ obtained by restricting the transform component A_j to $\{0\}$.) By successively doing this, we can decompose the code as the sum of a family of subcodes, each of which has any nonzero transform component A_j taking values from a minimal α^{mj}-invariant subspace. Now, let us consider one such code (which is a subcode of the original code). Let $\{j_1, j_2, \cdots, j_t\}$ be a set of representatives of the cyclotomic cosets modulo n where the transform components are nonzero for the code. We construct a subset L of $\{j_1, j_2, \cdots, j_t\}$ as follows. First assign $L = \{j_1\}$. Suppose A_{j_l} takes values from the minimal α^{mj_l}-invariant subspace V_{j_l}. In the subcode obtained by restricting A_{j_1} to 0, A_{j_2} takes values from either V_{j_2} or $\{0\}$. If it takes values from 0, then clearly, A_{j_2} is related to A_{j_1} by an isomorphism. Otherwise A_{j_1} and A_{j_2} take values independently and in that case keep j_2 in L. Next, restrict all the transform components indexed by the elements of L to 0 and check a transform component A_{j_l} not yet considered. If its values vary over V_{j_l}, then put j_l in L. Continuing this way, we'll get a set L such that all the transform components indexed by its elements take values independently and the values of all the other transform components are determined by them.

Note that in the process of construction of L, the minimality of V_{j_l} is used and consequently such a subset L may not exist when V_{j_l} are not minimal α^{mj_l}-invariant subspaces. Now, we can decompose the subcode as the direct sum of $|L|$ codes, each one of which is obtained by restricting all but one transform components indexed by the elements of L to zero. Clearly, each subcode thus obtained is a minimal m-quasi-cyclic code. So, any m-quasi-cyclic code can be decomposed as the sum of some minimal m-quasi-cyclic codes. Just taking a minimal family of such minimal subcodes such that their sum is the original code, we can express the code as the direct sum of some minimal m-quasi-cyclic codes. So we have

Table 3. Codes of Example 3.2

	Codewords															DFT													
	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}
$\mathcal{C}_1$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	1	1	0	1	1	1	1	0	1	1	0	0	0	α	α^2	0	α^4	0	0	α^8	α^8	0	0	α^4	0	α^2	α
	0	1	1	1	1	0	1	1	0	0	0	0	0	1	1	0	α^6	α^{12}	0	α^9	0	0	α^{13}	α^3	0	0	α^{14}	0	α^7	α^{11}
	0	1	1	0	0	0	0	0	1	1	0	1	1	1	1	0	α^{11}	α^7	0	α^{14}	0	0	α^3	α^{13}	0	0	α^9	0	α^{12}	α^6
$\mathcal{C}_2$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	1	1	1	1	0	1	1	1	0	1	0	0	0	1	0	α^2	α^4	0	α^8	α^{10}	0	0	α	0	α^5	0	0	0	0
	0	1	1	1	0	1	0	0	0	1	1	1	1	1	1	0	α^7	α^{14}	0	α^{13}	α^5	0	0	α^{11}	0	α^{10}	0	0	0	0
	1	0	0	0	1	1	1	1	1	1	0	1	1	1	0	0	α^{12}	α^9	0	α^3	1	0	0	α^6	0	1	0	0	0	0
$\mathcal{C}_3$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	1	1	1	1	1	0	0	0	1	0	1	1	1	0	0	0	0	0	0	1	0	α^3	0	0	1	α^9	0	α^{12}	α^6
	0	1	1	1	0	1	1	1	1	1	1	0	0	0	1	0	0	0	0	0	α^5	0	α^{13}	0	0	α^{10}	α^{14}	0	α^7	α^{11}
	1	0	0	0	1	0	1	1	1	0	1	1	1	1	1	0	0	0	0	0	α^{10}	0	α^8	0	0	α^5	α^4	0	α^2	α
$\mathcal{C}_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	1	1	1	1	0	0	1	1	1	0	1	0	0	0	0	α^2	α^4	0	α^8	1	0	α^5	α	0	1	α^{10}	0	α^5	α^{10}
	0	1	0	0	0	0	1	1	1	1	0	0	1	1	1	0	α^{12}	α^9	0	α^3	α^5	0	1	α^6	0	α^{10}	1	0	1	1
	0	0	1	1	1	0	1	0	0	0	0	1	1	1	1	0	α^7	α^{14}	0	α^{13}	α^{10}	0	α^{10}	α^{11}	0	α^5	α^5	0	α^{10}	α^5

Theorem 4.1 *Any m-quasi-cyclic code can be decomposed as the direct sum of some minimal m-quasi-cyclic codes.*

Theorem 4.1 was first proved in [4]. Note that the decomposition of an m-quasi-cyclic code in terms of some minimal m-quasi-cyclic codes may not be unique, though for $m = 1$, that is for cyclic codes the decomposition is always unique.

For a minimal m-quasi-cyclic code, the transform components in different cyclotomic cosets modulo $\frac{n}{m}$ are (trivially) unrelated. So, by Theorem 4.1 it is also true for any m-quasi-cyclic code. This gives the following characterization of m-quasi-cyclic codes in the transform domain.

Theorem 4.2 *A code $\mathcal{C}$ is m-quasi-cyclic iff*

- *The transform components in different q-cyclotomic cosets modulo $\frac{n}{m}$ are mutually unrelated.*
- *For any $j \in [0, \frac{n}{m} - 1]$, $A_{(j)_{n,m}}$ takes values from an $F_{q^{r_{mj}}}$-subspace of $F_{q^{r_j}} \times F_{q^{r_{j+\frac{n}{m}}}} \times \cdots \times F_{q^{r_{j+(m-1)\frac{n}{m}}}}$.*

Though the decomposition of an m-quasi-cyclic code is not unique in general, by first part of Theorem 4.2, any m-quasi-cyclic code can be decomposed uniquely as direct sum of some m-quasi-cyclic codes, each having nonzero transform components only in certain distinct q-cyclotomic coset modulo $\frac{n}{m}$. So we have

Theorem 4.3 *Let Λ_i; $i = 1, 2, \cdots, t$ be the distinct q-cyclotomic cosets modulo $\frac{n}{m}$ of $[0, n-1]$. Then,*

$$\mathcal{C} = \bigoplus_{i=1}^{t} \mathcal{C}_{\Lambda_i} \tag{4}$$

The unique subcodes $\mathcal{C}_{\Lambda_i}$ in (4), obtained by considering each q-cyclotomic coset modulo $\frac{n}{m}$ are actually the primary components [15] or irreducible components [4] of the code. In [15], the primary components of $\mathcal{C}$ were obtained as $\frac{X^{\frac{n}{m}}-1}{f_i(X)}.\mathcal{C}$, where $f_i(X)$ are the irreducible factors of $X^{\frac{n}{m}} - 1$. To see the bridge, note that the $\frac{n}{m}$-length DFT of $\frac{X^{\frac{n}{m}}-1}{f_i(X)}$ is nonzero in exactly one q-cyclotomic coset modulo $\frac{n}{m}$, say $[0, \frac{n}{m}] \cap [j]_{\frac{n}{m}}$. So, the n-length DFT of $\frac{X^n-1}{f_i(X^m)}$ is nonzero in exactly one cyclotomic coset modulo $\frac{n}{m}$, namely $[j]_{\frac{n}{m}}$, because if $k \equiv lq^t \bmod \frac{n}{m}$, then the k-th component of the n-length DFT of $\frac{X^n-1}{f_i(X^m)}$ is the $\frac{\alpha^{kn}-1}{f_i(\alpha^{km})} = \frac{\alpha^{lq^t n}-1}{f_i(\alpha^{lq^t m})} = \frac{(\alpha^m)^{lq^t \frac{n}{m}}-1}{f_i\left((\alpha^m)^{lq^t}\right)} = lq^t$-th component of the $\frac{n}{m}$-length DFT of $\frac{X^{\frac{n}{m}}-1}{f_i(X)}$. So, multiplying $\frac{X^{\frac{n}{m}}-1}{f_i(X)}$ to $\mathcal{C}$, which is same as multiplying $\frac{X^n-1}{f_i(X^m)}$ to $\mathcal{C}$ in unblocked form, is equivalent to 'zeroing out' the transform components in all but one q-cyclotomic cosets modulo $\frac{n}{m}$, that is $[j]_{\frac{n}{m}}$. Thus $\mathcal{C}_{\Lambda_i}$ are the primary components of the code.

Ling and Solé [17] gave a construction of m-quasi-cyclic codes from shorter codes over extension fields of F_q. That construction also gives a decomposition of an m-quasi-cyclic code as the direct sum of some m-quasi-cyclic codes. However their decomposition is actually the same decomposition as in Theorem 4.3. To see this, let us first state the main theorem (Theorem 5.1) of [17] in a slightly simplified form. Here ζ is a primitive $\frac{n}{m}$-th root of unity in an appropriate extension field of F_q.

Theorem 5.1 of [17] (simplified form) *Let $F = F_q$ and $(\frac{n}{m}, q) = 1$. Then the m-quasi-cyclic codes over F of length n are precisely given by the following construction: write $Y^{\frac{n}{m}} - 1 = g_1 \cdots g_s$, where g_i are the irreducible factors of $Y^{\frac{n}{m}} - 1$. Write $F[Y]/(g_i) = G_i$. Let U_i denote the cyclotomic coset of $\mathbb{Z}/m\mathbb{Z}$ corresponding to G_i and fix $u_i \in U_i$. For each i, let $\mathcal{C}_i$ be a code of length m over G_i. For $\mathbf{x}_i \in \mathcal{C}_i$ and for each $0 \le g \le m-1$, let*

$$\mathbf{c}_g((\mathbf{x}_i)) = \left(\frac{n}{m}\right)^{-1} \sum_{i=1}^{s} Tr_{G_i/F}\left(\mathbf{x}_i \zeta^{-gu_i}\right). \tag{5}$$

Then the code

$$\mathcal{C} = \left\{\left(\mathbf{c}_0((\mathbf{x}_i)), \cdots, \mathbf{c}_{\frac{n}{m}-1}((\mathbf{x}_i))\right) | \forall \mathbf{x}_i \in \mathcal{C}_i\right\} \tag{6}$$

is an m-quasi-cyclic code over F of length n. Conversely, every m-quasi-cyclic code over F of length n is obtained through this construction.

Let us fix an 'i' and consider the subcode $\mathcal{C}^{(i)}$ obtained from

$$c_g((\mathbf{x}_i)) = \left(\frac{n}{m}\right)^{-1} Tr_{G_i/F}\left(\mathbf{x}_i \zeta^{-gu_i}\right) \tag{7}$$

and (6). Clearly, $\mathcal{C} = \sum_i \mathcal{C}^{(i)}$. We'll show that $\mathcal{C}^{(i)} = \mathcal{C}_{[u_i]_{\frac{n}{m}}}$. It is sufficient to show that each codeword of $\mathcal{C}^{(i)}$ has nonzero transform components (in the n-length DFT) only in $[u_i]_{\frac{n}{m}}$.

We can assume $\zeta = \alpha^m$. Let x_{ik} denote the k-th component of $\mathbf{x}_i$. Clearly, the degree of g_i is r_{mu_i}. Suppose $\mathbf{a} \in F_q^n$ is a codeword in $\mathcal{C}^{(i)}$ constructed as

$$a_{jm+k} = \left(\frac{n}{m}\right)^{-1} Tr_{G_i/F}\left(x_{ik}\alpha^{-jmu_i}\right)$$
$$\text{where } \mathbf{x}_i \in \mathcal{C}_i,\ 0 \le j \le \frac{n}{m} - 1,\ 0 \le k \le m-1 \tag{8}$$

and its n-length DFT is $\mathbf{A} \in F_{q^r}^n$. Then,

$$A_t = \sum_{j=0}^{\frac{n}{m}-1} \sum_{k=0}^{m-1} a_{jm+k}\alpha^{t(jm+k)}$$
$$= \left(\frac{n}{m}\right)^{-1} \sum_{j=0}^{\frac{n}{m}-1} \sum_{k=0}^{m-1} \alpha^{t(jm+k)} \sum_{v=0}^{r_{mu_i}-1} x_{ik}^{q^v} \alpha^{-mju_iq^v}$$

$$= \left(\frac{n}{m}\right)^{-1} \sum_{k=0}^{m-1} \sum_{v=0}^{r_{mu_i}-1} x_{ik}^{q^v} \alpha^{kt} \sum_{j=0}^{\frac{n}{m}-1} \alpha^{mj(t-u_i q^v)}.$$

But

$$\sum_{j=0}^{\frac{n}{m}-1} \alpha^{mj(t-u_i q^v)} = \begin{cases} \frac{n}{m} & \text{if } t = u_i q^v \bmod \frac{n}{m} \\ 0, & \text{otherwise.} \end{cases}$$

So,

$$A_t = \begin{cases} \sum_{k=0}^{m-1} x_{ik}^{q^v} \alpha^{kt} & \text{if } t \equiv u_i q^v \bmod \frac{n}{m} \text{ for some } v \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

and hence $\mathbf{a}$ has zero transform components outside $[u_i]_{\frac{n}{m}}$. So, $\mathbf{a} \in \mathcal{C}_{[u_i]_{\frac{n}{m}}}$. This shows that the decomposition $\mathcal{C} = \sum_i \mathcal{C}^{(i)}$ is actually the primary decomposition as in (4).

Let us consider one subcode $\mathcal{C}_{\Lambda_i}$. Let $j_{i,1}, j_{i,2}, \cdots, j_{i,k_i}$ be the representatives of the different q-cyclotomic cosets modulo n in Λ_i. Now, in any m-quasi-cyclic code, this set of representatives can be uniquely partitioned into some subsets such that transform components in these subsets are mutually unrelated and any subset cannot be partitioned further in the same way. Let $\left\{j_{i,1}, j_{i,2}, \cdots, j_{i,k_i}\right\} = \cup_{l=1}^{s_i} \Lambda_{i,l}$ be the partition. Then the code $\mathcal{C}_{\Lambda_i}$ can be decomposed further as the direct sum of s_i subcodes $\mathcal{C}_{\Lambda_{i,1}}, \mathcal{C}_{\Lambda_{i,2}}, \cdots, \mathcal{C}_{\Lambda_{i,s_i}}$, where $\mathcal{C}_{\Lambda_{i,l}}$ is obtained by restricting all the transform components of $\mathcal{C}_{\Lambda_i}$ except those indexed by the elements of $\left[\Lambda_{i,l}\right]_n$ to zero. Then, we have the unique decomposition

$$\mathcal{C} = \bigoplus_{i=1}^{t} \bigoplus_{l=1}^{s_i} \mathcal{C}_{\Lambda_{i,l}}. \tag{10}$$

However, the subsets $\Lambda_{i,l}$ are in general different for different codes.

Notice that in the unique decomposition of $\mathcal{C}$ in (10), the subcodes $\mathcal{C}_{\Lambda_{i,l}}$ are not necessarily minimal and moreover these are not necessarily uniquely decomposable into minimal quasi-cyclic codes. For example, consider the three binary 3-quasi-cyclic codes $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_5$ of length 9 listed in Table 2. The direct sum of any two of these three gives the same code, which has nonzero transform components in one binary cyclotomic coset modulo $\frac{n}{m}$ and is decomposable in three different ways. In [15], the authors gave a systematic way to get a decomposition of the subcodes $\mathcal{C}_{\Lambda_i}$ using Groebner bases.

Given any subset $S \subseteq F_q^n$, the intersection of all the m-quasi-cyclic codes containing S is called the m-quasi-cyclic code generated by S. A code generated by a single vector is called an one-generator m-quasi-cyclic code [10, 11, 15]. Note that for an one-generator m-quasi-cyclic code, each primary component $\mathcal{C}_{\Lambda_i}$ (recall equation (4)) is either zero or minimal, since it is generated by the vector whose DFT components in the corresponding q-cyclotomic coset modulo $\frac{n}{m}$ are the same as that of $\mathbf{a}$ and all other DFT components are zero.

If a minimal m-quasi-cyclic code has the nonzero DFT components in $[j]_{\frac{n}{m}}$, then its dimension is r_{mj}. Suppose there are t q-cyclotomic cosets modulo $\frac{n}{m}$. If $[j]_{\frac{n}{m}}$ is the i-th q-cyclotomic coset modulo $\frac{n}{m}$, then let us denote r_{mj} as t_i. Considering the dimensions, $\mathcal{C}_{\Lambda_i}$ can be direct sum of at most m minimal m-quasi-cyclic codes (or cyclic irreducible codes as are called in [4, 15]). The number of ways $\mathcal{C}_{\Lambda_i}$ of dimension $l_i t_i$ can be chosen is thus given by $\prod_{h=0}^{l_i-1} \frac{q^{mt_i}-q^{ht_i}}{q^{l_i t_i}-q^{ht_i}}$, where the empty product is assumed to be 1. So, the total number of distinct m-quasi-cyclic codes of length n is given by $\sum_{l_0=0}^{m} \sum_{l_1=0}^{m} \cdots \sum_{l_t=0}^{m} \prod_{i=1}^{t} \left(\prod_{h=0}^{l_i-1} \frac{q^{mt_i}-q^{ht_i}}{q^{l_i t_i}-q^{ht_i}} \right)$. This formula was originally derived in [4]. From the values of l_i for a code, lot of structural information can be known. For example, if $\max_i l_i = l$, then one needs at least l generators to generate the code. So, for an one-generator code, $l_i = 1$ or 0 and at least one l_i is 1. An one-generator code is minimal iff the generator has nonzero transform components in exactly one q-cyclotomic coset modulo $\frac{n}{m}$. Dimension of an one generator code is given by $\sum t_i$ where the summation is over the q-cyclotomic cosets modulo $\frac{n}{m}$ where the DFT components of the generator are not all zeros, that is, where the corresponding primary components of the code are nonzero. In [15, 25], the dimension of the m-quasi-cyclic code generated by a single generator in blocked polynomial form $(g^{(0)}(X), g^{(1)}(X), \cdots, g^{(m-1)}(X))$ is derived to be $\frac{n}{m} - deg(gcd(g^{(0)}(X), g^{(1)}(X), \cdots, g^{(m-1)}(X), X^{\frac{n}{m}} - 1))$. The fact that both the formulae are actually same can be realized just by noting that t_i are actually the degrees of the irreducible factors of $X^{\frac{n}{m}} - 1$.

5 Duals of Quasi-Cyclic Codes

For two vectors $\mathbf{a}, \mathbf{b} \in F_q^n$, the Euclidean inner product of $\mathbf{a}$ and $\mathbf{b}$ is defined as

$$E(\mathbf{a}, \mathbf{b}) = \sum_{i=0}^{n-1} a_i b_i. \tag{11}$$

Two vectors are said to be orthogonal if the Euclidean inner product of the vectors is zero. Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be duals of each other if $\mathcal{C}_2 = \left\{ \mathbf{b} \in F_q^n | E(\mathbf{a}, \mathbf{b}) = 0 \,;\, \forall \mathbf{a} \in \mathcal{C}_1 \right\}$.

Theorem 5.1 *For an m-quasi-cyclic code $\mathcal{C}$, a vector $\mathbf{b} \in F_q^n$ is orthogonal to $\mathcal{C}$ if and only if for all $\mathbf{a} \in \mathcal{C}$,*

$$\sum_{j \in [i]_{\frac{n}{m}}} A_j B_{-j} = 0 \quad \textit{for all } q\textit{-cyclotomic cosets } \left(\textit{modulo } \frac{n}{m} \right) \ [i]_{\frac{n}{m}}. \tag{12}$$

Proof. Clearly, $\mathbf{b}$ is orthogonal to $\mathcal{C}$ if and only if

$$\mathbf{a} \perp \mathbf{b}\,;\ \forall \mathbf{a} \in \mathcal{C}$$

$$\iff \sum_{j=0}^{n-1} a_j b_j = 0 \quad \forall \mathbf{a} \in \mathcal{C}$$

$$\iff \sum_{j=0}^{n-1} A_j B_{-j} = 0 \quad \forall \mathbf{a} \in \mathcal{C}$$

$$\iff \sum_{j \in [i]_{\frac{n}{m}}} A_j B_{-j} = 0 \quad \text{for each } q\text{-cyclotomic cosets } \left(\text{modulo } \frac{n}{m}\right) [i]_{\frac{n}{m}} \quad \forall \mathbf{a} \in \mathcal{C}.$$

Corollary 5.2 *There is no self-dual m-quasi-cyclic code over F_q of length n when $(n, q) = 1$ and m is odd.*

Proof. Note that $[0]_{\frac{n}{m}} = (0)_{n,m}$. Let $\{i_1, i_2, \cdots, i_l\}$ be a set of representatives of the q-cyclotomic cosets modulo n in $(0)_{n,m}$. Suppose for an m-quasi-cyclic code $\mathcal{C}$, $A_{\{i_1,i_2,\cdots,i_l\}}$ takes values from an F_q-subspace V of $F_{q^{r_{i_1}}} \times F_{q^{r_{i_2}}} \times \cdots \times F_{q^{r_{i_l}}}$. Clearly, the dimension of the F_q-subspace

$$W = \{B_{\{-i_1,-i_2,\cdots,-i_l\}} \mid Tr_1\left(A_{i_1} B_{-i_1}\right) + \cdots + Tr_l\left(A_{i_l} B_{-i_l}\right) = 0\ \forall A_{\{i_1,i_2,\cdots,i_l\}} \in V\}$$

is $m - dim_{F_q}(V)$ where

$$Tr_j : F_{q^{r_{i_j}}} \longrightarrow F_q$$

$$x \mapsto \quad x + x^q + \cdots + x^{q^{r_{i_j}-1}}.$$

If the code is self-dual, then $V = W$ and so, $2\, dim_{F_q}(V) = m$. Hence, there is no self-dual m-quasi-cyclic code over F_q of length n when $(n, q) = 1$ and m is odd.

However, this result is also true with the condition $(\frac{n}{m}, q) = 1$ instead of $(n, q) = 1$ (see Proposition 6.3 in [17]). But the condition $(n, q) = 1$ is required for the n-length DFT in our approach.

6 Parity Check Matrix and Minimum Distance Bound

Tanner used BCH like argument [23] to estimate a lower bound on the minimum Hamming distance from the parity check equations over an extension field. Given a binary parity check matrix of a binary m-quasi-cyclic code, Tan-

ner used block wise DFT or block wise linearized polynomial transform to get a set of parity check equations over an extension field of F_2.

Here, we describe how one can get a set of parity check equations over an extension field of F_q for an m-quasi-cyclic code over F_q. Before doing so, we first give the main theorem for the distance bound. This is in a slightly different form from Tanner's related theorems [23, Theorem 6,8 and 10] and the proof is analogous to Tanner's corresponding proofs. In the following, power of a vector will mean component wise power.

Theorem 6.1 *Suppose, the components of the vector* $\mathbf{v} \in F_{q^r}^n$ *are nonzero and distinct. If for each* $k = k_0, k_1, \cdots, k_{\delta-2}$, *the vectors* $\mathbf{v}^k$ *are in the span of a set of parity check equations over* F_{q^r}, *then the minimum Hamming distance of the code is at least that of the cyclic code of length* $q^r - 1$ *with roots* β^k, $k = k_0, k_1, \cdots, k_{\delta-2}$ *where* β *is a primitive element of* F_{q^r}.

Proof. Let $\mathcal{C}$ be the code, which has $\mathbf{v}^k$, $k = k_0, k_1, \cdots, k_{\delta-2}$ in the span of its parity check equations. Let the corresponding cyclic code be $\mathcal{C}_c$.
Suppose $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ with $v_i = \beta^{\lambda_i}$, where λ_i are distinct.
For any $\mathbf{a} \in \mathcal{C}$ with Hamming weight $\omega_H(\mathbf{a}) = d$, we'll show that $\exists \mathbf{a}' \in \mathcal{C}_c$, s. t. $\omega_H(\mathbf{a}') = d$.
We construct $\mathbf{a}'$ as

$$a'_{\lambda_i} = a_i \quad \text{for } i \in [0, n-1]$$

$$a'_j = 0 \quad \text{when } j \neq \lambda_i \ \ \forall i \in [0, n-1].$$

Clearly, $\omega_H(\mathbf{a}') = d$.
Now,

$$\begin{aligned}
\mathbf{a} \in \mathcal{C} &\Rightarrow \sum_{i=0}^{n-1} a_i v_i^k = 0 \ \text{ for } \ k = k_0, k_1, \cdots, k_{\delta-2} \\
&\Rightarrow \sum_{i=0}^{n-1} a'_{\lambda_i} \beta^{\lambda_i k} = 0 \ \text{ for } \ k = k_0, k_1, \cdots, k_{\delta-2} \\
&\Rightarrow \sum_{j=0}^{q^r-2} a'_j \beta^{jk} = 0 \ \text{ for } \ k = k_0, k_1, \cdots, k_{\delta-2} \\
&\Rightarrow \mathbf{a}' \in \mathcal{C}_c.
\end{aligned}$$

So, If $k_i = k_0 + i$ in the above theorem, by BCH bound we can say that the minimum distance of the code of length n is at least δ.

The idea behind this theorem is that, if a code has certain powers of $\mathbf{v}$ as parity check vectors, then the code can be seen as a shortened code (that is,

the code obtained by taking the codewords with certain positions zeros and then deleting those positions)[18] of a cyclic code of length $q^r - 1$. Not only is the minimum distance of the code guaranteed to be at least that of the cyclic code, any decoding algorithm for the cyclic code can also be used to decode the shortened code. The decoder only has to pad zeros in the deleted positions and decode from the resulting $q^r - 1$ length vector.

For an arbitrary $j \in [0, \frac{n}{m} - 1]$, suppose $A_{(j)_{n,m}}$ takes values from an $F_{q^{r_{mj}}}$-subspace V of $F_{q^{r_j}} \times F_{q^{r_{j+\frac{n}{m}}}} \times \cdots \times F_{q^{r_{j+(m-1)\frac{n}{m}}}}$. Then V is the null space of a system of $F_{q^{r_{mj}}}$-linear equations of the form

$$\sum_{i=0}^{m-1} Tr_i \left(c_i A_{j+i\frac{n}{m}}\right) = 0 \tag{13}$$

where Tr_i is the $F_{q^{r_{j+i\frac{n}{m}}}} / F_{q^{r_{mj}}}$-trace:

$$Tr_i : F_{q^{r_{j+i\frac{n}{m}}}} \longrightarrow F_{q^{r_{mj}}}$$

$$x \mapsto \quad x + x^{q^{r_{mj}}} + \cdots + x^{q^{(l_i-1)r_{mj}}}$$

where $l_i = \frac{r_{j+i\frac{n}{m}}}{r_{mj}}$. Now equation (13) can be rewritten as

$$\sum_{i=0}^{m-1} \sum_{k=0}^{l_i-1} \left(c_i A_{j+i\frac{n}{m}}\right)^{q^{kr_{mj}}} = 0$$

$$\Rightarrow \sum_{i=0}^{m-1} \sum_{k=0}^{l_i-1} c_i^{q^k} \sum_{t=0}^{n-1} \alpha^{t(j+i\frac{n}{m})q^{kr_{mj}}} a_t = 0$$

$$\Rightarrow \sum_{t=0}^{n-1} \left(\sum_{k=0}^{l_i-1} \left(\sum_{i=0}^{m-1} c_i \alpha^{t(j+i\frac{n}{m})} \right)^{q^{kr_{mj}}} \right) a_t = 0.$$

This gives a parity check equation over F_{q^r} for the code.

The component wise conjugate vectors of the parity check vectors obtained this way and the vectors in their span are also parity check vectors of the code.

Example 6.1 Consider an $m = 3$-quasi-cyclic code of length $n = 9$ over F_2 given by the frequency domain restriction $A_1 \in \beta^{-3} F_4$, where $\beta \in F_{64}$ is a primitive element with minimal polynomial $X^6 + X + 1$. (the DFT is defined over F_{64} with the DFT kernel $\alpha = \beta^7$). Note that the conjugacy constraint allows A_1 to take any value from F_{64}. But in this particular 3-quasi-cyclic code, A_1 takes values from a minimal α^3-invariant subspace. The restriction $A_1 \in \beta^{-3} F_4$ gives the parity check vector:

$$\mathbf{h} = \left(\left(\beta^3 \alpha^i\right)^4 - \beta^3 \alpha^i \right)_{i=0 \text{ to } 8}$$

$$= \left(\beta^{48}, \beta^{56}, \beta^7, \beta^6, \beta^{14}, \beta^{28}, \beta^{27}, \beta^{35}, \beta^{50}\right).$$

The components of $\mathbf{h}$ are distinct and nonzero and $\mathbf{h}^2$, being a component wise conjugate of $\mathbf{h}$, is also a parity check vector of the code. So, Theorem 6.1 guarantees a minimum Hamming distance at least 3 for the code. So, it is a $[9, 5, \geq 3]$ code. If we impose the further condition $A_0 = 0$, then we get another parity check vector $\mathbf{h}^0 = (1, 1, \cdots, 1)$ and as a result we get a $[9, 4, \geq 4]$ code.

7 Conclusion

In this paper, we have obtained a generalization of the well known DFT domain characterization of cyclic codes over finite fields. It is shown that for minimal m-quasi-cyclic codes of length n, transform components in different q-cyclotomic cosets modulo n are related (not possible for cyclic codes) and possible relations are identified. For non-minimal m-quasi-cyclic codes the decomposition in terms of minimal m-quasi-cyclic codes is discussed. A way to get a lower bound on the minimum Hamming distance for m-quasi-cyclic codes in terms of the minimum Hamming distance of a BCH code is shown. Decoding algorithm for the corresponding BCH code can be used to decode the m-quasi-cyclic code upto that minimum distance.

Acknowledgements. The authors greatfully acknowledge the anonymous reviewers for their constructive comments which helped to improve the manuscript.

References

1. Bhargava, V.K., Seguin, G.E., Stein, J.M.: Some (mk, k) Cyclic Codes in Quasi-Cyclic Form. IEEE Trans. Inform. Theory **24**, 630–632 (1978)
2. Blahut, R.E.: Theory and Practice of Error Control Codes. Reading, MA: Addison Wesley, 1983
3. Calderbank, A.R., Forney, G.D., Vardy, A.: Minimal Tail-biting Trellises: The Golay Codes and More. IEEE trans. Inform. Theory **45**, 1435–1255 (1999)
4. Conan, J., Seguin, G.: Structural Properties and Enumeration of Quasi Cyclic Codes. Applicable Algebra in Engineering Communication and Computing **4**, 25–39, (1993)
5. Esmaeili, M., Gulliver, T.A., Secord, N.P.: Quasi-cyclic Structure of Reed-Muller Codes and Their Smallest Regular Trellis Diagram. IEEE Trans. Inform. Theory **43**, 1040–1052 (1997)
6. Esmaeili, M., Gulliver, T.A., Secord, N.P., Mahmoud, S.A.: A Link Between Quasi-Cyclic Codes and Convolutional Codes. IEEE Trans. Inform. Theory **44**, 431–435 (1998)
7. Gulliver, T.A., Bhargava, V.K.: Two New Rate 2/p Binary Quasi-Cyclic Codes. IEEE Trans. Inform. Theory **40**, 1667–1668 (1994)
8. Gulliver, T.A., Bhargava, V.K.: Some Best Rate 1/p and Rate (p-1)/p Systematic Quasi-Cyclic Codes. IEEE Trans. Inform. Theory **37**, 552–555 (1991)
9. Gulliver, T.A., Bhargava, V.K.: Nine Good Rate (m-1)/pm Quasi-Cyclic Codes. IEEE Trans. Inform. Theory **38**, 1366–1369 (1992)
10. Gulliver, T.A., Bhargava, V.K.: Some Best Rate 1/p and Rate (p-1)/p Systematic Quasi-Cyclic Codes over GF(3) and GF(4). IEEE Trans. Inform. Theory **38**, 1369–1374 (1992)

11. Gulliver, T.A., Bhargava, V.K.: Twelve Good Rate (m-r)/pm Quasi-Cyclic Codes. IEEE Trans. Inform. Theory **39**, 1750–1751 (1993)
12. Karlin, M.: New Binary Coding Results by Circulants. IEEE Trans. Inform. Theory **15**, 81–92 (1969)
13. Karlin, M.: Decoding of Circulant Codes. IEEE Trans. Inform. Theory **16**, 797–802 (1970)
14. Kasami, T.: A Gilbert-Varshamov Bound for Quasi-Cyclic Codes of Rate 1/2. IEEE Trans. Inform. Theory **24**, 627–628 (1978)
15. Lally, K., Fitzpatrick, P.: Algebraic Structure of Quasicyclic Codes. Disc. Appl. Math. **111**, 157–175 (2001)
16. Lidl, R., Niederreiter, H.: Finite Fields. Encyclopedia of Mathematics and Its Applications, Vol. 20, Cambridge University Press
17. Ling, S., Solé, P.: On Algebraic Structure of Quasi-Cyclic Codes I: Finite Fields. IEEE Trans. Inform. Theory **47**, 2751–2760 (2001)
18. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. Amsterdam: North-Holland, 1988
19. MacWilliams, F.J.: Decomposition of Cyclic Codes of Block Lengths 3p, 5p, 7p. IEEE Trans. Inform. Theory **25**, 112–118 (1979)
20. Solomon, G., van Tilborg, H.: A Connection Between Block and Convolutional Codes. SIAM J. Appl. Math. **37**, 358–369 (1979)
21. Stein, J.M., Bhargava, V.K.: Equivalent Rate $\frac{1}{2}$ Quasi-Cyclic Codes. IEEE Trans. Inform. Theory **21**, 588–589 (1975)
22. Stein, J.M., Bhargava, V.K., Tavares, S.E.: Weight Distribution of Some "Best" (3m, 2m) Binary Quasi-Cyclic Codes. IEEE Trans. Inform. Theory **21**, 708–711 (1975)
23. Tanner, R.M.: A Transform Theory for a Class of Group-Invariant Codes. IEEE Trans. Inform. Theory **34**, 752–775 (1988)
24. Tavares, S.E., Bhargava, V.K., Shiva, S.G.S.: Some Rate-p/(p+1) Quasi-Cyclic Codes. IEEE Trans. Inform. Theory **20**, 133–135 (1974)
25. Seguin, G.E., Drolet, G.: The Trace Description of Irreducible Quasi-Cyclic Codes. IEEE Trans. Inform. Theory **36**, 1463–1466 (1990)
26. Sundar Rajan, B., Siddiqi, M.U.: Transform Domain Characterization of Abelian Codes. IEEE Trans. on Inform. Theory **38**, 1817–1821 (1992)
27. Sundar Rajan, B., Siddiqi, M.U.: Transform Domain Characterization of cyclic codes over Z_m. Applicable Algebra in Engineering, Communication and Computing **5**, 261–276 (1994)
28. Sundar Rajan, B., Siddiqi, M.U.: A Generalized DFT for Abelian Codes over Z_m. IEEE Trans. on Inform. Theory **40**, 2082–2090 (1994)
29. Mathys, P.: Frequency Domain Description of Repeated-Root Cyclic Codes. Proceedings of 1994 International Symposium on Information Theory, Trondheim, Norway, p.47 (1994)
30. van Tilborg, H.: On Quasi-Cyclic Codes with Rate 1/m. IEEE Trans. Inform. Theory **24**, 628–630 (1978)