F_q-Linear Cyclic Codes over F_{q^m}: DFT Characterization

Bikash Kumar Dey and B. Sundar Rajan*

Indian Instute of Science, Bangalore 560012, India
bikash@protocol.ece.iisc.ernet.in
bsrajan@ece.iisc.ernet.in

Abstract. Codes over F_{q^m} that form vector spaces over F_q are called F_q-linear codes over F_{q^m}. Among these we consider only cyclic codes and call them F_q-linear cyclic codes (F_qLC codes) over F_{q^m}. This class of codes includes as special cases (i) group cyclic codes over elementary abelian groups ($q = p$, a prime), (ii) subspace subcodes of Reed-Solomon codes and (iii) linear cyclic codes over F_q (m=1). Transform domain characterization of F_qLC codes is obtained using Discrete Fourier Transform (DFT) over an extension field of F_{q^m}. We show how one can use this transform domain structures to estimate a minimum distance bound for the corresponding quasicyclic code by BCH-like argument.

1 Introduction

A code over F_{q^m} (q is a power of a prime) is called linear if it is a vector space over F_{q^m}. We consider F_qLC codes over F_{q^m}, i.e., codes which are cyclic and form vector spaces over F_q. The class of F_qLC codes includes the following classes of codes as special cases:

1. **Group cyclic codes over elementary abelian groups:** When $q = p$ the class of F_pLC codes becomes group cyclic codes over an elementary abelian group C_p^m (a direct product of m cyclic groups of order p). A length n group code over a group G is a subgroup of G^n under componentwise operation. Group codes constitute an important ingredient in the construction of geometrically uniform codes [4]. Hamming distance properties of group codes over abelian groups is closely connected to the Hamming distance properties of codes over subgroups that are elementary abelian [5]. Group cyclic codes over C_p^m have been studied and applied to block coded modulation schemes with phase shift keying [8]. It is known [13],[19] that group cyclic codes over C_p^m contain MDS codes that are not linear over F_{p^m}.
2. **SSRS codes:** With $n = q^m - 1$, the class of F_qLC codes includes the subspace subcodes of Reed-Solomon (SSRS) codes [7], which contain codes with larger number of codewords than any previously known code for some lengths and minimum distances.

* This work was partly supported by CSIR, India, through Research Grant (22(0298)/99/EMR-II) to B. S. Rajan

S. Boztaş and I.E. Shparlinski (Eds.): AAECC-14, LNCS 2227, pp. 67–76, 2001.
© Springer-Verlag Berlin Heidelberg 2001

3. **Linear cyclic codes over finite fields:** Obviously, with $m = 1$, the F_qLC codes are the extensively studied class of linear cyclic codes.

A code is m-quasicyclic if cyclic shift of components of every codeword by m positions gives another codeword [11]. If $\{\beta_0, \beta_1, \cdots, \beta_{m-1}\}$ is a F_q-basis of F_{q^m}, then any vector $(a_0, a_1, \cdots, a_{n-1}) \in F_{q^m}^n$ can be seen with respect to this basis as $(a_{0,0}, a_{0,1}, \cdots, a_{0,m-1}, \cdots, a_{n-1,0}, a_{n-1,1}, \cdots, a_{n-1,m-1}) \in F_q^{mn}$, where $a_i = \sum_{j=0}^{m-1} a_{i,j}\beta_j$. This gives a 1-1 correspondence between the class of F_qLC codes of length n over F_{q^m} and the class of m-quasicyclic codes of length mn over F_q. Unlike in [3], which considers $(nm, q) = 1$, F_qLC codes gives rise to m-quasicyclic codes of length mn with $(n, q) = 1$.

It is well known [1], [14] that cyclic codes over F_q and over the residue class integer rings Z_m are characterizable in the transform domain using Discrete Fourier Transform (DFT) over appropriate Galois fields and Galois rings [12] respectively and so are the wider class of abelian codes over F_q and Z_m using a generalized DFT [15],[16]. The transform domain description of codes is useful for encoding and decoding [1],[17]. DFT approach for cyclic codes of arbitrary length is discussed in [6]. In this correspondence, we obtain DFT domain characterization of F_qLC codes over F_{q^m} using the notions of certain invariant subspaces of extension fields of F_{q^m}, two different kinds of cyclotomic cosets and linearized polynomials.

The proofs of all the theorems and lemmas are omitted due to space limitations.

2 Preliminaries

Suppose $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1}) \in F_{q^m}^n$, where $(n, q) = 1$. From now on, r will denote the smallest positive integer such that $n|(q^{mr} - 1)$ and $\alpha \in F_{q^{mr}}$ an element of multiplicative order n. The set $\{0, 1, \cdots, n-1\}$ will be denoted by I_n. The Discrete Fourier Transform (DFT) of $\mathbf{a}$ is defined to be $\mathbf{A} = (A_0, A_1, \cdots, A_{n-1}) \in F_{q^{mr}}^n$, where $A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i \;, \quad j \in I_n$. A_j is called the j-th DFT coefficient or the j-th transform component of $\mathbf{a}$. The vectors $\mathbf{a}$ and $\mathbf{A}$ will be referred as time-domain vector and the corresponding transform vector respectively.

For any $j \in I_n$, the **q-cyclotomic coset modulo n** of j is defined as $[j]_n^q = \{i \in I_n | j \equiv iq^t \bmod n$ for some $t \geq 0\}$, and the q^m**-cyclotomic coset modulo n** of j is defined as $[j]_n^{q^m} = \{i \in I_n | j \equiv iq^{mt} \bmod n$ for some $t \geq 0\}$. We'll denote the cardinalities of $[j]_n^q$ and $[j]_n^{q^m}$ as e_j and r_j respectively.

Example 1. Table 1 shows $[j]_{15}^2$, $[j]_{15}^{2^2}$, $[j]_{15}^{2^3}$ and $[j]_{15}^{2^4}$ for $j \in I_{15}$.

Mostly we'll have n for the modulus. So we'll drop the modulus when not necessary. Clearly, a q-cyclotomic coset is a disjoint union of some q^m-cyclotomic cosets. If $J \subseteq I_n$, we write $[J]_n^q = \cup_{j \in J} [j]_n^q$ and $[J]_n^{q^m} = \cup_{j \in J} [j]_n^{q^m}$.

If $\mathbf{b}$ is the cyclically shifted version of $\mathbf{a}$, then $B_j = \alpha^j A_j$ for $j \in I_n$. This is the **cyclic shift property** of DFT. The DFT components satisfy **conjugacy**

Table 1. Cyclotomic cosets modulo 15

$2/2^3$-cycl. cosets	$\{0\}$	$\{1,2,4,8\}$				$\{3,6,9,12\}$				$\{5,10\}$		$\{7,13,11,14\}$			
cardinality	1	4				4				2		4			
2^2-cycl. cosets	$\{0\}$	$\{1,4\}$		$\{2,8\}$		$\{3,12\}$		$\{6,9\}$		$\{5\}$	$\{10\}$	$\{7,13\}$		$\{14,11\}$	
cardinality	1	2		2		2		2		2		2		2	
2^4-cycl. cosets	$\{0\}$	$\{1\}$	$\{2\}$	$\{4\}$	$\{8\}$	$\{3\}$	$\{6\}$	$\{9\}$	$\{12\}$	$\{5\}$	$\{10\}$	$\{7\}$	$\{13\}$	$\{11\}$	$\{14\}$
cardinality	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

constraint[1], given by $A_{(q^m j) \bmod n} = A_j^{q^m}$. So, conjugacy constraint relates the transform components in same q^m-cyclotomic coset.

Let $I_1, I_2, \cdots, I_l$ be some disjoint subsets of I_n and suppose $R_{I_j} = \{(A_i)_{i \in I_j} \mid \mathbf{a} \in \mathcal{C}\}$ for $j = 1, 2, \cdots, l$. The sets of transform components $\{A_i | i \in I_j\}$; $1 \leq j \leq l$ are called **unrelated** for $\mathcal{C}$ if $\left\{\left((A_i)_{i \in I_1}, (A_i)_{i \in I_2}, \cdots, (A_i)_{i \in I_l}\right) | \mathbf{a} \in \mathcal{C}\right\} = R_{I_1} \times R_{I_2} \times \cdots \times R_{I_l}$.

For a code $\mathcal{C}$, we say, A_j takes values from $\{\sum_{i=0}^{n-1} \alpha^{ij} a_i | \mathbf{a} \in \mathcal{C}\} \subseteq F_{q^{mr}}$. For linear cyclic codes, A_j takes values from $\{0\}$ or $F_{q^{mr_j}}$ and transform components in different q^m-cyclotomiccosets are unrelated.

For any element $s \in F_{q^l}$, the set $[s]^q = \{s, s^q, s^{q^2}, \cdots, s^{q^{e-1}}\}$, where e is the smallest positive integer such that $s^{q^e} = s$, is called the q-conjugacy class of s. Note that, if $\alpha \in F_{q^l}$ is of order n and $s = \alpha^j$, then there is an 1-1 correspondence between $[j]_n^q$ and $[s]^q$, namely $jq^t \mapsto s^{q^t}$. So, $|[s]^q| = |[j]_n^q| = e_j$.

For any element $s \in F_{q^l}$, an F_q-subspace U of F_{q^l} is called **s-invariant** (or $[s,q]$-subspace in short) if $sU = U$. An $[s,q]$-subspace of F_{q^l} is called minimal if it contains no proper $[s,q]$-subspace. If U and V are two $[s,q]$-subspaces of F_{q^l}, then so are $U \cap V$ and $U + V$. If e is the exponent of $[s]^q$, then $Span_{F_q}\{s^i | i \geq 0\} \simeq F_{q^e}$. So, for any $g \in F_{q^l} \setminus \{0\}$, the minimal $[s,q]$-subspace containing g is gF_{q^e}. Clearly, if $s' \in [s]^q$, then $[s,q]$-subspaces and $[s',q]$-subspaces are same.

Example 2. The minimal $[\alpha^5, 2]$ and $[\alpha^{10}, 2]$-subspaces of F_{2^4} are $V_1 = F_4 = \{0, 1, \alpha^5, \alpha^{10}\}$, $V_2 = \alpha F_4$, $V_3 = \alpha^2 F_4$, $V_4 = \alpha^3 F_4$, $V_5 = \alpha^4 F_4$. The $[\alpha^k, 2]$-subspaces, for $k \neq 0, 5, 10$ are $\{0\}$ and F_{16}. Every subset $\{0, x \in F_{16}^*\}$ is a minimal $[\alpha^0, 2]$-subspace.

3 Transform Domain Characterization of $FqLC$ Codes

By the cyclic shift property, in an F_qLC code $\mathcal{C}$, the values of A_j constitute an $[\alpha^j, q]$-subspace of $F_{q^{mr}}$. However, this is not sufficient for $\mathcal{C}$ to be an F_qLC code.

Example 3. Consider length 15, F_2-linear codes over $F_{16} = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{14}\}$. We have $q = 2, m = 4$ and $r = 1$. In Table 2, the code $\mathcal{C}_3$ is not cyclic, though each transform component takes values from appropriate invariant subspaces. Other five codes in the same table are F_2LC codes. As DFT kernel, we have taken a primitive element $\alpha \in F_{16}$ with minimal polynomial $X^4 + X + 1$.

The characterization of F_qLC codes is in terms of certain decompositions of the codes. In the following subsection, we discuss the decomposition of F_qLC codes and in Subsection 3.2 present the characterization.

3.1 Decomposition of F_qLC Codes

We start from the following notion of minimal generating set of subcodes for F_q-linear codes.

A set of F_q-linear subcodes $\{\mathcal{C}_\lambda | \lambda \in \Lambda\}$ of a F_q-linear code $\mathcal{C}$ is said to be a generating set of subcodes if $\mathcal{C} = \Sigma_{\lambda\in\Lambda}\mathcal{C}_\lambda$. A generating set of subcodes $\{\mathcal{C}_\lambda | \lambda \in \Lambda\}$ of $\mathcal{C}$ is called a **minimal generating set of subcodes (MGSS)** if $\Sigma_{\lambda\neq\lambda'}\mathcal{C}_\lambda \neq \mathcal{C}$ for all $\lambda' \in \Lambda$. MGSS of an F_q-linear code is not unique. For example, consider the length 3 F_2-linear code over F_{2^2}, $\mathcal{C} = \{c_1 = (00,00,00), c_2 = (01,01,01), c_3 = (10,10,10), c_4 = (11,11,11)\}$. The sets of subcodes $\{\{c_1, c_2\}, \{c_1, c_3\}\}$ and $\{\{c_1, c_2\}, \{c_1, c_4\}\}$ are both MGSS for $\mathcal{C}$.

Suppose A_j takes values from $V \subset F_{q^{mr}}$, $V \neq \{0\}$ for an F_q-linear code $\mathcal{C}$. Let V_1 be an F_q-subspace of $F_{q^{mr}}$.We call $\mathcal{C}' = \{\mathbf{a} | \mathbf{a} \in \mathcal{C}, A_j \in V_1\}$ as the F_q-linear subcode obtained by restricting A_j in V_1. For example, the subcode $\mathcal{C}_1$ of Table 2 can be obtained from $\mathcal{C}_4$ by restricting A_5 to $\{0\}$. Clearly, if $\mathcal{C}$ is cyclic and V_1 is an $[\alpha^j, q]$-subspace, then $\mathcal{C}'$ is also cyclic. If $S \subseteq I_n$, then the subcode obtained by restricting the transform components A_j; $j \notin S$ to 0 is called the S-subcode of $\mathcal{C}$ and is denoted as $\mathcal{C}_S$.

Lemma 1. *Suppose in an F_q-linear code $\mathcal{C}$, A_j takes values from a subspace $V \in F_{q^{mr}}$. Let $V_1, V_2 \subseteq V$ be two subspaces of V such that $V = V_1 + V_2$. (i) If $\mathcal{C}_1$ and $\mathcal{C}_2$ are the subcodes of $\mathcal{C}$, obtained by restricting A_j in V_1 and V_2 respectively, then $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2$. (ii) If V_1 and V_2 are $[\alpha^j, q]$-subspaces, then $\mathcal{C}$ is cyclic if and only if $\mathcal{C}_1$ and $\mathcal{C}_2$ are cyclic.*

Suppose for an F_q-linear code $\mathcal{C}$, A_j takes values from a nonzero F_q-subspace V of $F_{q^{mr}}$, and V intersects with more than one minimal $[\alpha^j, q]$-subspace. Then, we have two nonzero $[\alpha^j, q]$-subspaces V_1 and V_2 such that $V \subseteq V_1 \oplus V_2$ and $V \cap V_1 \neq \phi$ and $V \cap V_2 \neq \phi$. Then, we can decompose the code as the sum of two smaller codes $\mathcal{C}_1$ and $\mathcal{C}_2$ obtained by restricting A_j to V_1 and V_2 respectively, i.e., $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2$. So by successively doing this for each j, we can decompose $\mathcal{C}$ into a generating set of subcodes, in each of which, for any $j \in I_n$, transform component A_j takes values from a F_q-subspace of a minimal $[\alpha^j, q]$-subspace. In particular, if the original code was an F_qLC code, all the subcodes obtained this way will have A_j from minimal $[\alpha^j, q]$-subspaces. The following are immediate consequences of this observation and Lemma 1.

1. In a minimal F_qLC code, any nonzero transform component A_j takes values from a minimal $[\alpha^j, q]$-subspace of $F_{q^{mr}}$. For example, for the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ in Table 2, A_5 and A_{10} take values from minimal $[\alpha^5, 2]$-subspaces.
2. A code is F_qLC if and only if all the subcodes obtained by restricting any nonzero transform component A_j in minimal $[\alpha^j, q]$-subspaces of $F_{q^{mr}}$ are F_qLC. The statement is also true without the word 'minimal'.

Suppose in an F_q-linear code $\mathcal{C}$, transform components $A_j,\ j \in I_n$ take values from F_q-subspaces V_j of $F_{q^{mr}}$. A set of transform components $\{A_l | l \in L \subseteq I_n\}$ is called a **maximal set of unrelated components (MSUC)** if they are unrelated for $\mathcal{C}$ and any other transform component $A_k,\ k \notin L$ can be expressed as $A_k = \sum_{l \in L} \sigma_{kl} A_l$ such that σ_{kl} is an F_q-homomorphism of V_l into V_k.

If some disjoint sets of transform components are unrelated in two codes $\mathcal{C}'$ and $\mathcal{C}''$, then so is true for the code $\mathcal{C}' + \mathcal{C}''$. However, the converse is not true. For instance, for the codes $\mathcal{C}_0$ and $\mathcal{C}_1$ in Table 2, A_5 and A_{10} are related but they are unrelated for the sum $\mathcal{C}_4 = \mathcal{C}_0 + \mathcal{C}_1$.

Theorem 1. *If $\mathcal{C}$ is an F_qLC code over F_{q^m} where any nonzero transform component A_j takes values from a minimal $[\alpha^j, q]$-subspace V_j of $F_{q^{mr}}$, then there is an MSUC $\{A_l | l \in L \subset I_n\}$ for $\mathcal{C}$.*

Clearly, for a code as described in Theorem 1, if $l \in L$, the code $\mathcal{C}_l = \{\mathbf{a} \in \mathcal{C} | A_j = 0 \text{ for } j \in L \setminus \{l\}\}$ is a minimal F_qLC code. So $\mathcal{C}$ can be decomposed into an MGSS as $\mathcal{C} = \oplus_{l \in L} \mathcal{C}_l$. Since any code can be decomposed into a minimal generating set of subcodes with nonzero transform components taking values from minimal invariant subspaces by restricting the components to minimal invariant subspaces, a minimal generating set of minimal F_qLC subcodes can be obtained by further decomposing each of the subcodes as above. So, we have,

Theorem 2. *Any F_qLC code can be decomposed as direct sum of minimal F_qLC codes.*

Suppose, in an F_qLC code, A_j and A_k take values from the $[\alpha^j, q]$-subspace V_1 and $[\alpha^k, q]$-subspace V_2 respectively. Suppose A_k is related to A_j by an F_q homomorphism $\sigma : V_1 \mapsto V_2$ i.e. $A_k = \sigma(A_j)$. Then, since the code is cyclic,

$$\sigma(\alpha^j v) = \alpha^k \sigma(v) \qquad \forall \quad v \in V_1. \tag{1}$$

Clearly, for such a homomorphism, $Ker(\sigma)$ is an $[\alpha^j, q]$-subspace.

Lemma 2. *Let $\mathcal{C}$ be an F_qLC code over F_{q^m} where each nonzero transform component A_j takes values from a minimal $[\alpha^j, q]$-subspace of $F_{q^{mr}}$. If $A_k = \sum_{i=1}^{t} \sigma_{j_i} A_{j_i}$, where $A_{j_i},\ i = 1, 2, \cdots, t$ take values freely from some respective minimal invariant subspaces, then $\sigma_{j_i},\ i = 1, 2, \cdots, t$ are all F_q-isomorphisms.*

3.2 Transform Characterization

The following theorem characterizes F_qLC codes in the DFT domain.

Theorem 3. *Let $\mathcal{C} \subset F_{q^m}^n$ be an n-length F_q-linear code over F_{q^m} Then, $\mathcal{C}$ is F_qLC if and only if all the subcodes of an MGSS obtained by restricting the transform components to minimal invariant subspaces satisfy the conditions:*
1. For all $j \in I_n$, the set of j^{th} transform components is α^j-invariant.
2. There is an MSUC $\{A_j | j \in J\}$ where A_j takes values from a minimal $[\alpha^j, q]$-subspace V_j and $A_k = \sum_{j \in J} \sigma_{kj} A_j$ for all $k \notin J$, where σ_{kj} is an F_q-isomorphism of V_j onto V_k satisfying

$$\sigma_{kj}(\alpha^j v) = \alpha^k \sigma_{kj}(v) \ \ \forall v \in V_j. \tag{2}$$

Example 4. In Table 2, the codes obtained by restricting A_{10} to V_5 and V_1 for the code $\mathcal{C}_5$ are respectively $\mathcal{C}_0$ and $\mathcal{C}_2$. In both $\mathcal{C}_0$ and $\mathcal{C}_2$, the nonzero transform components A_5 and A_{10} take values from minimal $[\alpha^5, 2]$ invariant subspaces and sum of $\mathcal{C}_0$ and $\mathcal{C}_2$ is $\mathcal{C}_5$. So, $\{\mathcal{C}_0, \mathcal{C}_2\}$ is an MGSS of $\mathcal{C}_5$. In both $\mathcal{C}_0$ and $\mathcal{C}_2$, A_5 and A_{10} are related by isomorphisms. It can be checked that the isomorphisms satisfy the condition (2).

Since for an F_qLC code, transform components can be related by homomorphisms satisfying (1), we characterize such homomorphisms in Section 4. We also show that for F_qLC codes, A_j and A_k can be related iff $k \in [j]_n^q$.

4 Connecting Homomorphisms for F_qLC Codes

Throughout the section an endomorphism will mean an F_q-endomorphism.

A polynomial of the form $f(X) = \sum_{i=0}^{t} c_i X^{q^i} \in F_{q^l}[X]$ is called a **q-polynomial or a linearized polynomial** [10] over F_{q^l}. Each q-polynomial of degree less than q^l induces a distinct F_q-linear map of F_{q^l}. So, considering the identical cardinalities, we have $End_{F_q}(F_{q^l}) = \{\sigma_f : x \mapsto f(x) | f(X) = \sum_{i=0}^{l-1} c_i X^{q^i} \in F_{q^l}[X]\}$

For any $y \in F_{q^l} \setminus \{0\}$, the automorphism induced by $f(X) = yX$ will be denoted by σ_y. The subset $\{\sigma_y | y \in F_{q^l} \setminus \{0\}\}$ forms a cyclic subgroup of $Aut_{F_q}(F_{q^l})$, generated by $\sigma_{\beta_{q^l}}$, where $\beta_{q^l} \in F_{q^l}$ is a primitive element of F_{q^l}. In this subgroup, $\sigma_y^i = \sigma_{y^i}$. We shall denote this subgroup as $S_{q,l}$ and $S_{q,l} \cup \{0\}$ as $\mathbf{S}_{q,l}$, where 0 denotes the zero map. Clearly, $\mathbf{S}_{q,l}$ forms a field isomorphic to F_{q^l}.

We shall denote the map $\sigma_{X^q} : y \mapsto y^q$ of F_{q^l} onto F_{q^l}, induced by the polynomial $f(X) = X^q$, as $\theta_{q,l}$. Clearly, $\theta_{q,l}\sigma_x = \sigma_x^q \theta_{q,l}$ i.e., $\theta_{q,l}\sigma_x\theta_{q,l}^{-1} = \sigma_x^q$ for all $x \in F_{q^l}$. The map induced by the polynomial $f(X) = X^{q^i}$ is $\theta_{q,l}^i$. So, for any $f(X) = \sum_{i=0}^{l-1} c_i X^{q^i}$, $\sigma_f = \sum_{i=0}^{l-1} \sigma_{c_i}\theta_{q,l}^i$ Thus we have $End_{F_q}(F_{q^l}) = \oplus_{i=0}^{l-1} \mathbf{S}_{q,l}\theta_{q,l}^i$ i.e., any endomorphism $\sigma \in End_{F_q}(F_{q^l})$ can be decomposed uniquely as $\sigma = \sum_{i=0}^{l-1} \sigma_{(i)}$ where $\sigma_{(i)} \in \mathbf{S}_{q,l}\theta_{q,l}^i$. We shall call this decomposition as canonical decomposition of σ.

Theorem 4. *Suppose* $x_1, x_2 \in F_{q^l}$. *Then,* $[x_1]^q = [x_2]^q \Leftrightarrow \exists \sigma \in Aut_{F_q}(F_{q^l})$ *such that* $\sigma(x_1 x) = x_2 \sigma(x)$ $\forall x \in F_{q^l}$.

Lemma 3. *Let* $V_1 \subseteq F_{q^l}$ *be a minimal* $[x_1, q]$*-subspace and* $\sigma : V_1 \longrightarrow F_{q^l}$ *be a nonzero homomorphism of* V_1 *into* F_{q^l}*, satisfying* $\sigma(x_1 v) = x_2 \sigma(v) \quad \forall \;\; v \in V_1$. *Then* $[x_1]^q = [x_2]^q$.

Theorem 5. *Suppose* $x_1, x_2 \in F_{q^l}$. *Let* $V_1 \subset F_{q^l}$ *be a* $[x_1, q]$*-subspace and* σ *is as in Lemma 3. Then (i)* $[x_1]^q = [x_2]^q$ *and (ii)* $\sigma(V_2)$ *is a* $[x_1, q]$*-subspace for any* $[x_1, q]$*-subspace* $V_2 \subset V_1$.

Theorem 6. *In an F_qLC code, the transform components of different q- cyclotomic cosets are mutually unrelated.*

Corollary 1. *Any minimal F_qLC code takes nonzero values only in one q-cyclotomic coset in transform domain and any minimal F_qLC code which has nonzero transform components in $[j]_n^q$ has size q^{e_j}.*

So, if $J_1, J_2, \cdots, J_t$ are the distinct q-cyclotomic cosets of I_n, then any F_qLC code $\mathcal{C}$ can be decomposed as $\mathcal{C} = \oplus_{i=1}^t \mathcal{C}_{J_i}$. Corresponding m-quasi-cyclic codes are called primary components [9] or irreducible components [2]. If $\mathbf{a} \in F_{q^m}^n$, then the intersection of all the F_qLC codes containing $\mathbf{a}$ is called the F_qLC code generated by $\mathbf{a}$. We call such F_qLC codes as one-generator F_qLC codes. Clearly, For a one-generator F_qLC code $\mathcal{C}$, each component $\mathcal{C}_{J_i}$ is minimal.

Suppose V_1 and V_2 are two subspaces of F_{q^l}. Suppose $y \in F_{q^l}$ such that V_1 is y-invariant and i is a nonnegative integer. Then, we define $Hom_{F_q}(V_1, V_2, y, i) = \left\{\sigma \in Hom_{F_q}(V_1, V_2) | \sigma y x = y^{q^i} \sigma x \ \ , \forall x \in V_1\right\}$. Clearly, $Hom_{F_q}(V_1, V_2, y, i)$ is a subspace of $Hom_{F_q}(V_1, V_2)$. Since $y^{q^{e_y+i}} = y^{q^i}$, we shall always assume $i < e_y$. We are interested in $Hom_{F_q}(V_1, V_2, y, i)$ since, if for an F_qLC code, $A_j \in V_1$ and $A_{jq^i} \in V_2$, then A_j and A_{jq^i} can be related by a homomorphism $\sigma : V_1 \rightarrow V_2$ if and only if $\sigma \in Hom_{F_q}(V_1, V_2, \alpha^j, i)$.

Theorem 7. *Any $\sigma \in Hom_{F_q}(x_1 F_{q^{e_y}}, x_2 F_{q^{e_y}}, y, l)$ is induced by a polynomial $f(X) = cX^{q^i}$ for some unique constant $c \in x_2 x_1^{-1} F_{q^{e_y}}$.*

For $y = \alpha^j$, this theorem specifies all possible homomorphisms by which A_{jq^l} can be related to A_j for an F_qLC code when A_j takes values from a minimal $[\alpha^j, q]$-subspace.

Example 5. Clearly, in the codes $\mathcal{C}_0$ and $\mathcal{C}_2$ in Table 2, A_5 is related to A_{10} by homomorphisms. Suppose $A_5 = \sigma_f(A_{10})$ where $f(X)$ is a q-polynomial over F_{q^l}. For $\mathcal{C}_0$, $f(X) = \alpha^8 X^2$ and for $\mathcal{C}_2$, $f(X) = \alpha X^2$.

The following theorem specifies the possible relating homomorphisms when A_j takes values from a nonminimal $[\alpha^j, q]$-subspace.

Theorem 8. *Suppose $V \subseteq F_{q^l}$ is a $[y, q]$-subspace and $V = \oplus_{j=0}^{t-1} V_j$ where V_j are minimal $[y, q]$-subspaces. Then, for any $\sigma \in Hom_{F_q}(V, F_{q^l}, y, i)$, there is a unique polynomial of the form $f(X) = \sum_{j=0}^{t-1} a_j X^{q^{je_y+i}}$, $a_j \in F_{q^l}$ such that $\sigma = \sigma_f$. So, $Hom_{F_q}(V, F_{q^l}, y, i) = \{\sigma_f | f(X) = \sum_{j=0}^{t-1} a_j X^{q^{je_y+i}}$, $a_j \in F_{q^l}\}$*

So, if $j_1, \cdots, j_w \in [k]_n^q$ and A_k is related to $A_{j_1}, \cdots, A_{j_w}$ by homomorphisms i.e., if $A_k = \sigma_1(A_{j_1}) + \cdots + \sigma_w(A_{j_w})$, where $\sigma_1, \cdots, \sigma_w$ are homomorphisms, then the relation can be expressed as $A_k = \sum_{h_1=0}^{l_1-1} c_{1,h_1} A_{j_1}^{q^{h_1 e_k + t_1}} + \cdots + \sum_{h_w=0}^{l_w-1} c_{w,h_w} A_{j_w}^{q^{h_w e_k + t_w}}$, where $k \equiv j_i^{q^{t_i}} \mod n$ for $i = 1, \cdots, w$.

Example 6. In the code $\mathcal{C}_5$ in Table 2, A_5 is related to A_{10} by a homomorphism induced by the polynomial $f(X) = \alpha^{14} X^2 + \alpha^8 X^8$.

5 Parity Check Matrix and Minimum Distance of Quasicyclic Codes

For linear codes, Tanner used BCH like argument [18] to estimate minimum distance bounds from the parity check equations over an extension field.

With respect to any basis of F_{q^m}, there is a 1-1 correspondence between n-length F_qLC codes and m-quasi-cyclic codes of length nm over F_q. Here we describe how in some cases one can directly get a set of parity check equations of a quasi-cyclic code from the transform domain structure of the corresponding F_qLC code. We first give a theorem from [3] for the distance bound.

Theorem 9. *[3] 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 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}*.*

So, If $k_i = k_0 + i$, BCH bound gives $d_{min} \geq \delta$.

Let us fix a basis $\{\beta_0, \beta_1, \cdots, \beta_{m-1}\}$ of F_{q^m} over F_q. By our characterization of F_qLC codes in DFT domain, we know that for any $j \in [0, n-1]$, A_j can take values from any $[\alpha^j, q]$-subspace of $F_{q^{rm_j}}$. In particular, A_j can take values from subspaces of the form $c^{-1}F_{q^l}$ where $e_j|l$ and $l|mr_j$. Then,

$$(cA_j)^{q^l} = cA_j \;\Leftrightarrow \left(c\sum_{i=0}^{n-1}\alpha^{ij}a_i\right)^{q^l} = c\sum_{i=0}^{n-1}\alpha^{ij}a_i$$

$$\Leftrightarrow \left(c\sum_{i=0}^{n-1}\alpha^{ij}\sum_{x=0}^{m-1}a_{ix}\beta_x\right)^{q^l} = c\sum_{i=0}^{n-1}\alpha^{ij}\sum_{x=0}^{m-1}a_{ix}\beta_x.$$

This gives a parity check vector $\mathbf{h} = (h_{0,0}, h_{0,1}, \cdots, h_{0,m-1}, \cdots, h_{n-1,0}, \cdots, h_{n-1,m-1})$ with $h_{i,x} = \left(c^{q^l}\alpha^{ijq^l}\beta_x^{q^l} - c\alpha^{ij}\beta_x\right)$. If $A_j = 0$, it gives a parity check vector $\mathbf{h}$ with $h_{i,x} = \beta_x$.

Now, for F_qLC code, A_k can be related to several other transform components $A_{j_1}, A_{j_2}, \cdots, A_{j_w}$ by homomorphisms, where $j_1, \cdots, j_w \in [k]_n^q$. Then, $A_k = \sum_{h_1=0}^{l_1-1} c_{1,h_1}A_{j_1}^{q^{h_1e_k+t_1}} + \cdots + \sum_{h_w=0}^{l_w-1} c_{w,h_w}A_{j_w}^{q^{h_we_k+t_w}}$ for some constants $c_{i,h_i} \in F_{q^{mr}}$. It can be checked in the same way that, this gives a parity check vector $\mathbf{h}$ with $h_{i,x} = \beta_x\alpha^{ik} - \sum_{h_1=0}^{l_1-1} c_{1,h_1}\beta_x^{q^{h_1e_k+t_1}}\alpha^{ij_1q^{h_1e_k+t_1}} - \cdots - \sum_{h_w=0}^{l_w-1} c_{w,h_w}\beta_x^{q^{h_we_k+t_w}}\alpha^{ij_wq^{h_we_k+t_w}}$.

The component wise conjugate vectors of the parity check vectors obtained in these ways and the vectors in their span are also parity check vectors of the code. However, in general for any F_qLC code, the components may not be related simply by homomorphisms or components may not take values from the subspaces of the form $c^{-1}F_{q^l}$. In those cases, the parity check vectors obtained in the above ways may not specify the code completely. But still those equations can be used for estimating a minimum distance bound by Theorem 9.

Since the DFT components in different q-cyclotomic cosets modulo n are unrelated, the set of parity check equations over $F_{q^{mr}}$ are union of the check equations corresponding to each q-cyclotomic coset modulo n. Clearly, for any one generator code, a set of parity check vectors completely specifying the code can be obtained in this way. There are however other codes for which complete set of parity check vectors can be derived. In fact, codes can be constructed by imposing simple transform domain restrictions and thus allowing derivations of a complete set of parity check equations over $F_{q^{mr}}$. We illustrate this with the following example. If β is a primitive element of $F_{q^{mr}}$, then we use $\alpha = \beta^{\frac{q^{mr}-1}{n}}$ as the DFT kernel and we take the basis $\{1, \beta, \beta^2, \cdots, \beta^{m-1}\}$.

Example 7. We consider the F_2LC code of length $n = 3$ over F_{2^4} given by the transform domain restrictions $A_0 = 0$ and $A_2 = \beta^4 A_1^2 + \beta^{10} A_1^8$. With the chosen basis, these two restrictions give the parity check vectors of the underlying 4-quasi-cyclic code $\mathbf{h_{(1)}} = \left(1, \beta, \beta^2, \beta^3, 1, \beta, \beta^2, \beta^3, 1, \beta, \beta^2, \beta^3\right)$ and $\mathbf{h_{(2)}} = \left(\beta^8, \beta^5, \beta^{12}, \beta^6, \beta^3, 1, \beta^7, \beta, \beta^{13}, \beta^{10}, \beta^2, \beta^{11}\right)$ respectively. Componentwise conjugates of these vectors are also parity check vectors. Moreover, ${\mathbf{h_{(2)}}}^3 = \left(\beta^9, 1, \beta^6, \beta^3, \beta^9, 1, \beta^6, \beta^3, \beta^9, 1, \beta^6, \beta^3\right) = \beta \mathbf{h_{(1)}} + \beta^8 {\mathbf{h_{(1)}}}^2 + \beta^6 {\mathbf{h_{(1)}}}^4 + {\mathbf{h_{(1)}}}^8$ and ${\mathbf{h_{(2)}}}^0 = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) = \beta^{11} \mathbf{h_{(1)}} + \beta^7 {\mathbf{h_{(1)}}}^2 + \beta^{15} {\mathbf{h_{(1)}}}^4 + \beta^{13} {\mathbf{h_{(1)}}}^8$. So, the underlying quasi-cyclic code is a $[12, 4, 6]$ code. This code is actually same as the $[12, 4, 6]$ code discussed in [18].

Table 2. Few Length 15 F_2-Linear Codes over F_{16}

[Only nonzero transform components are shown. The elements of F_{16}^* are represented by the corresponding power of the primitive element and 0 is represented by -1.]

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_5	A_{10}
$\mathcal{C}_0$																
-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
0	2	8	0	2	8	0	2	8	0	2	8	0	2	8	1	4
8	0	2	8	0	2	8	0	2	8	0	2	8	0	2	6	14
2	8	0	2	8	0	2	8	0	2	8	0	2	8	0	11	9
$\mathcal{C}_1$																
-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
4	9	14	4	9	14	4	9	14	4	9	14	4	9	14	-1	4
14	4	9	14	4	9	14	4	9	14	4	9	14	4	9	-1	14
9	14	4	9	14	4	9	14	4	9	14	4	9	14	4	-1	9
$\mathcal{C}_4 = \mathcal{C}_0 + \mathcal{C}_1$																
-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
4	9	14	4	9	14	4	9	14	4	9	14	4	9	14	-1	4
14	4	9	14	4	9	14	4	9	14	4	9	14	4	9	-1	14
9	14	4	9	14	4	9	14	4	9	14	4	9	14	4	-1	9
0	2	8	0	2	8	0	2	8	0	2	8	0	2	8	1	4
1	11	6	1	11	6	1	11	6	1	11	6	1	11	6	1	-1
3	10	12	3	10	12	3	10	12	3	10	12	3	10	12	1	9
7	13	5	7	13	5	7	13	5	7	13	5	7	13	5	1	14
8	0	2	8	0	2	8	0	2	8	0	2	8	0	2	6	14
5	7	13	5	7	13	5	7	13	5	7	13	5	7	13	6	9
6	1	11	6	1	11	6	1	11	6	1	11	6	1	11	6	-1
12	3	10	12	3	10	12	3	10	12	3	10	12	3	10	6	4
2	8	0	2	8	0	2	8	0	2	8	0	2	8	0	11	9
10	12	3	10	12	3	10	12	3	10	12	3	10	12	3	11	14
13	5	7	13	5	7	13	5	7	13	5	7	13	5	7	11	4
11	6	1	11	6	1	11	6	1	11	6	1	11	6	1	11	-1

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_5	A_{10}
$\mathcal{C}_2$																
-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
4	3	7	4	3	7	4	3	7	4	3	7	4	3	7	1	0
7	4	3	7	4	3	7	4	3	7	4	3	7	4	3	6	10
3	7	4	3	7	4	3	7	4	3	7	4	3	7	4	11	5
$\mathcal{C}_3$																
-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
0	2	8	0	2	8	0	2	8	0	2	8	0	2	8	1	4
5	7	13	5	7	13	5	7	13	5	7	13	5	7	13	6	9
10	12	3	10	12	3	10	12	3	10	12	3	10	12	3	11	14
$\mathcal{C}_5 = \mathcal{C}_0 + \mathcal{C}_2$																
-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
4	3	7	4	3	7	4	3	7	4	3	7	4	3	7	1	0
7	4	3	7	4	3	7	4	3	7	4	3	7	4	3	6	10
3	7	4	3	7	4	3	7	4	3	7	4	3	7	4	11	5
0	2	8	0	2	8	0	2	8	0	2	8	0	2	8	1	4
1	6	11	1	6	11	1	6	11	1	6	11	1	6	11	-1	1
9	10	13	9	10	13	9	10	13	9	10	13	9	10	13	11	2
14	12	5	14	12	5	14	12	5	14	12	5	14	12	5	6	8
8	0	2	8	0	2	8	0	2	8	0	2	8	0	2	6	14
5	14	12	5	14	12	5	14	12	5	14	12	5	14	12	11	3
11	1	6	11	1	6	11	1	6	11	1	6	11	1	6	-1	11
13	9	10	13	9	10	13	9	10	13	9	10	13	9	10	1	12
2	8	0	2	8	0	2	8	0	2	8	0	2	8	0	11	9
10	13	9	10	13	9	10	13	9	10	13	9	10	13	9	6	7
12	5	14	12	5	14	12	5	14	12	5	14	12	5	14	1	13
6	11	1	6	11	1	6	11	1	6	11	1	6	11	1	-1	6

Acknowledgement

We thank P. Fitzpatrick and R. M. Tanner for sending us preprint/unpublished versions of their work.

References

1. R. E. Blahut, *Theory and Practice of Error Control Codes*, Addison Wesley, 1983.
2. 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.
3. B. K. Dey and B. Sundar Rajan, "DFT Domain Characterization of Quasi-Cyclic Codes", Submitted to IEEE Trans. Inform. Theory.
4. G. D. Forney Jr., *Geometrically Uniform Codes*, IEEE Trans. Inform. Theory,IT-37 (1991), pp. 1241-1260.
5. G. D. Forney Jr., *On the Hamming Distance Properties of Group Codes*, IEEE Trans. Inform. Theory, IT-38 (1992), pp. 1797-1801.
6. G. Gunther, *A Finite Field Fourier Transform for Vectors of Arbitrary Length*, Communications and Cryptography: Two Sides of One Tapestry, R. E. Blahut, D. J. Costello, U. Maurer, T. Mittelholzer (Eds), Kluwer Academic Pub., 1994.
7. M. Hattori, R. J. McEliece and G. Solomon, *Subspace Subcodes of Reed-Solomon Codes*, IEEE Trans. Inform. Theory, IT-44 (1998), pp. 1861-1880.
8. M. Isaksson and L. H. Zetterberg, *Block-Coded M-PSK Modulation over $GF(M)$*, IEEE Trans. Inform. Theory, IT-39 (1993), pp. 337-346.
9. K. Lally and P. Fitzpatrick, "Algebraic Structure of Quasicyclic Codes", to appear in *Discrete Applied Mathematics.*
10. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press.
11. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1988.
12. McDonald B. R., *Finite rings with identity*, Marcel Dekker, New York, 1974.
13. M. Ran and J. Snyders, *A Cyclic [6,3,4] group code and the hexacode over $GF(4)$*", IEEE Trans. Inform. Theory, IT-42 (1996), pp. 1250-1253.
14. B. Sundar Rajan and M. U. Siddiqi, *Transform Domain Characterization of Cyclic Codes over Z_m*, Applicable Algebra in Engineering, Communication and Computing, Vol. 5, No. 5, pp. 261-276, 1994.
15. B. Sundar Rajan and M. U. Siddiqi, *A Generalized DFT for Abelian Codes overZ_m*, IEEE Trans. Inform. Theory, IT-40 (1994), pp. 2082-2090.
16. B. Sundar Rajan and M. U. Siddiqi, *Transform Domain Characterization of Abelian Codes*, IEEE Trans. Inform. Theory, IT-38 (1992), pp. 1817-1821.
17. B. Sundar Rajan and M. U. Siddiqi, *Transform Decoding of BCH Codes over Z_m*, International J. of Electronics, Vol 75, No. 6, pp. 1043-1054, 1993.
18. R. M. Tanner, "A Transform Theory for a Class of Group-Invariant Codes", *IEEE Trans. Inform. Theory*, vol. 34, pp. 752-775, July 1988.
19. A. A. Zain and B. Sundar Rajan, *Algebraic Characterization of MDS Group Codes over Cyclic Groups*, IEEE Trans. Inform. Theory, IT-41 (1995), pp. 2052-2056.