DRDO–IISc Programme on
Advanced Research in Mathematical Engineering

F_q-linear Cyclic Codes over F_{q^m} : DFT Approach

(TR-PME-2003-05)

by
Bikash Kumar Dey and B Sundar Rajan
ECE, IISc., Bangalore
E-mail: bsrajan@ece..iisc.ernet.in

May 19, 2003

Indian Institute of Science
Bangalore 560 012

F_q-linear Cyclic Codes over F_{q^m} : DFT Approach

Bikash Kumar Dey and B. Sundar Rajan

June 7, 2003

ABSTRACT

Codes over F_{q^m} that are closed under addition, and multiplication with elements from F_q are called F_q-linear codes over F_{q^m}. For $m \neq 1$, this class of codes is a subclass of nonlinear codes. Among F_q-linear codes, we consider only cyclic codes and call them F_q-linear cyclic codes (F_qLC codes) over F_{q^m}. The class of F_qLC codes includes as special cases (i) group cyclic codes over elementary Abelian groups ($q = p$, a prime), (ii) subspace subcodes of Reed-Solomon codes ($n = q^m - 1$) studied by Hattori, McEliece and Solomon (iii) linear cyclic codes over F_q (m=1) and (iv) twisted BCH codes. Moreover, with respect to any particular F_q-basis of F_{q^m}, any F_qLC code over F_{q^m} can be viewed as an m-quasi-cyclic code of length mn over F_q. In this correspondence, we obtain transform domain characterization of F_qLC codes, using Discrete Fourier Transform (DFT) over an extension field of F_{q^m}. The characterization is in terms of any decomposition of the code into certain subcodes and linearized polynomials over F_{q^m}. We show how one can use this transform domain characterization to obtain a minimum distance bound for the corresponding quasi-cyclic code. We also prove nonexistence of self dual F_qLC codes and self dual quasi-cyclic codes of certain parameters using the transform domain characterization.

Index terms: Non-linear cyclic codes, Space-Time codes, Additive codes, Discrete Fourier Transform (DFT).

1 Introduction and Motivation

The rank-distance properties are useful to construct space-time codes and also for coding for storage devices (See the reports [1, 2] and the references therein). In [1] rank-distance properties of the general class of linear codes over finite fields have been studied and toward obtaining closed form expressions, in [2], the study was restricted to the class of cyclic codes and modest progress have been reported. This study made use of the well known Discrete Fourier Transform (DFT) approach [5] for cyclic codes. To study the rank-distance properties of nonlinear cyclic codes first of all one needs to have the codes described in the DFT domain. This report essentially achieves it. In this section we first motivate inclusion of the class of certain nonlinear codes for characterization in the DFT domain.

A linear code over F_{q^m}, (q is a power of a prime p) is closed under addition, and multiplication with elements from F_{q^m}. In this report we consider the class of nonlinear codes over F_{q^m} that are closed under addition, and multiplication with elements from F_q and call them F_q-linear codes. Such codes have found practical applications in deep-space communication [18] and computer memory systems [7–11]. Among the F_q-linear codes, we restrict ourselves to cyclic codes. We refer to this class of codes as F_q-linear cyclic codes. Henceforth we write F_qL codes for

[0]This work was partly supported by DRDO-IISc Program on Mathematical Engineering through a research grant to B.S.Rajan.
A part of the content of this report has been accepted for publication in "Designs, Codes and Cryptography" by Kluwer Publishers subject to minor modifications.
A preliminary version of this report was presented at AAECC-14, (14th Symposium on Applied Algebra Algorithms and Error Correcting Codes) RMIT, Melbourne, Australia, Nov. 25-30, 2001.

F_q-linear codes over F_{q^m} and F_qLC codes for F_q-linear cyclic codes over F_{q^m}. 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 coincides with the class of group cyclic codes defined 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 component-wise operation. Group codes constitute an important ingredient in the construction of geometrically uniform codes [15]. Hamming distance properties of group codes over Abelian groups are closely connected to the Hamming distance properties of codes over subgroups that are elementary Abelian [16]. Group cyclic codes over C_p^m constructed using nonsingular circulant matrices over F_{p^m} have been studied and applied to block coded modulation schemes with phase shift keying [19]. It is known [27, 36] that the class of group cyclic codes over C_p^m contains MDS codes that are not linear over F_{p^m}.

2. **SSRS codes:** Given a Reed-Solomon code of length $n = q^m - 1$ over F_{q^m}, the subcode obtained by taking all the codewords with components from an F_q-subspace of F_{q^m} is called a subspace subcode of the Reed-Solomon (SSRS) code. These codes are also F_qLC codes and were discussed by Hattori, McEliece and Solomon in [18]. The authors derived dimension formula for this class of codes and codes with larger number of codewords than any previously known code with the same length and minimum distance have been reported. The class of SSRS codes is a subclass of subgroup subcodes, discussed in [20].

3. **Linear cyclic codes over finite fields:** Obviously, with $m = 1$, the class of F_qLC codes coincides with the extensively studied class of linear cyclic codes over finite fields [5, 24].

4. **Twisted BCH codes:** Consider a code obtained by taking the coordinate-wise image of a BCH code over F_{q^r} under an F_q-linear map $\phi : F_{q^r} \longrightarrow F_q^m$ for some $m \leq r$. Twisted BCH codes, constructed as F_q dual (see Section 4) of such codes, were introduced in [14] and is a subclass of F_qLC codes. Large number of good codes were constructed in [3, 4, 14] as twisted BCH codes and as combinations of twisted BCH codes with other codes.

A code is m-quasi-cyclic (m-QC) if the cyclic shift of components of every codeword by m positions gives another codeword [24]. Structural properties of quasi-cyclic codes were investigated in [12, 21]. There is a 1-1 correspondence between the class of F_qLC codes of length n over F_{q^m} and the class of m-QC codes of length mn over F_q. If $\{\beta_0, \beta_1, \cdots, \beta_{m-1}\}$ is an 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 $a_i = \sum_{j=0}^{m-1} a_{i,j}\beta_j$. When seen this way, any F_qLC code of length n over F_{q^m} corresponds to an m-QC code of length nm over F_q.

Transform domain approach has been employed to study various classes of codes. It is well known that cyclic codes over F_q [5] and over the residue class integer rings Z_m [29] are characterizable in the transform domain using Discrete Fourier Transform (DFT) over appropriate Galois fields and Galois rings [26] respectively and so are the wider class of Abelian codes over F_q and Z_m using a generalized DFT [30, 31]. The transform domain description of codes is useful for encoding and decoding [5, 32]. The DFT approach for cyclic codes of arbitrary length is discussed in [17] and for repeated-root cyclic codes [6, 35] in [25]. A version of transform domain approach is used by Tanner [33] to obtain minimum distance information for any group-invariant code. In [23], m-QC codes of length nm were seen as length m linear codes over the residue ring $F_q[x]/(x^n - 1)$ and DFT in $F_q[x]/(x^n - 1)$ was used to study self dual QC codes. Design of self dual QC codes were shown to be equivalent to design of difference sets in [34]. In this report,

- we obtain DFT domain characterization of F_qLC codes over F_{q^m}.
- we give transform domain condition for two vectors to be F_q-dual of each other. This is used to prove nonexistence of certain self dual F_qLC codes and equivalently nonexistence of the corresponding self dual QC codes. These results for self dual QC codes are also available in [23].
- the transform domain characterization of F_qLC codes is used to derive minimum distance bound for the corresponding QC codes.

The content of this report is organized as follows : In Section 2, after briefly reviewing the DFT domain description of linear cyclic codes over a finite field we define two different cyclotomic cosets. Also we introduce the notion of certain invariant subspaces to be used in the sequel. In Section 3, the main result of this report, i.e., the DFT domain description of F_qLC codes is given. The characterization is in terms of any decomposition of a code into subcodes, for which each nonzero transform component's values are from certain minimal invariant subspaces of the extension field. In Section 4, we derive transform domain condition for two vectors to be F_q-dual of each other w. r. t. a self dual basis of F_{q^m} and use it to prove the nonexistence of self dual F_qLC codes and self dual QC codes of certain parameters. In Section 5, we show how one can obtain a set of parity check equations over an extension field for the corresponding QC code and thus can get a bound on its minimum distance using an approach similar to Tanner's [33]. Several directions for further research and concluding remarks constitute Section 6.

2 Preliminaries

Let $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1}) \in F_{q^m}^n$, where $(n, q) = 1$. Also let r be the smallest positive integer such that $n|(q^{mr} - 1)$ and $\alpha \in F_{q^{mr}}$ be an element of multiplicative order n. The DFT of $\mathbf{a}$ is defined to be $\mathbf{A} = (A_0, A_1, \cdots, A_{n-1}) \in F_{q^{mr}}^n$, where $A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i$, $\quad j \in I_n = \{0, 1, \cdots, n-1\}$. 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.

The DFT components satisfy the **conjugacy constraint**[5]: $A_{(q^m j) \bmod n} = A_j^{q^m}$. This constraint implies $A_j \in F_{q^{mr_j}} \subseteq F_{q^{mr}}$, where r_j is the smallest positive integer such that $jq^{mr_j} \equiv j \ mod \ n$. So, the set of transform components $\{A_j, A_{q^m j}, A_{q^{2m} j}, \cdots, A_{q^{m(r_j-1)} j}\}$ are related. If $n = q^m - 1$, then $r = 1$ and a primitive element of F_{q^m} is taken as α. In this case, all the DFT coefficients are independent, i.e., there is no conjugacy constraint. This case arises for the transform domain study of Reed-Solomon codes [5]. 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 the DFT.

Let $\mathcal{C} \subseteq F_{q^m}^n$ be a code of length n over F_{q^m}. 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 $\mathcal{C}$. If A_j takes value from $\{0\}$, we say $A_j = 0$ for $\mathcal{C}$.

Definition 1. *For any $j \in I_n$, the* **q-cyclotomic coset modulo n** *of j is defined as*

$$[j]_n^q = \{i \in I_n | j \equiv iq^t \ mod \ n \ for \ some \ nonnegative \ integer \ t\} \tag{1}$$

*and the q^m-***cyclotomic coset modulo n** *of j is defined as*

$$[j]_n^{q^m} = \{i \in I_n | j \equiv iq^{mt} \ mod \ n \ for \ some \ nonnegative \ integer \ t\} \tag{2}$$

We shall denote the cardinalities, also called the exponents, of the cyclotomic cosets $[j]_n^q$ *and* $[j]_n^{q^m}$ *as* e_j *and* r_j *respectively.*

Clearly, e_j and r_j are related as $r_j = \frac{e_j}{(m,e_j)}$. A q-cyclotomic coset modulo n is a disjoint union of some q^m-cyclotomic cosets modulo n. If $J \subseteq I_n$, we write $[J]_n^q = \cup_{j\in J}[j]_n^q$ and $[J]_n^{q^m} = \cup_{j\in J}[j]_n^{q^m}$. For any $J \subseteq I_n$, we'll denote $\{A_j | j \in J\}$ as A_J. It can be easily checked that, every q-cyclotomic coset mod n is a disjoint union of some q^m-cyclotomic cosets mod n of identical exponent and the number of q^m-cyclotomic cosets mod n within a q-cyclotomic coset mod n divides m.

Example 2.1. For $n = 15$ the cyclotomic cosets $[j]_{15}^2$, $[j]_{15}^{2^2}$, $[j]_{15}^{2^3}$ and $[j]_{15}^{2^4}$ are shown in Table 1(a). Table 1(b) shows for $n = 63$ the cyclotomic cosets $[j]_{63}^{2^i}$ for $i = 1,2,3,4,5,6$. Observe that, in this case, $i = 1$ and $i = 5$ give identical set of cyclotomic cosets and the same is the case for the pair $i = 2$ and $i = 4$.

Notice that the conjugacy constraint relates only the components of the transform vector indexed by elements of the same q^m-cyclotomic coset and components indexed by elements of different q^m-cyclotomic cosets are not related by conjugacy constraints. One of the main results of this report is that if transform components indexed by elements of different q^m-cyclotomic cosets contained within a single q-cyclotomic coset are *related* appropriately one gets F_qLC codes over F_{q^m}. We formalize the notion of related/unrelated set of transform components as follows:

In the following, for a subset $I = \{i_1, i_2, \cdots, i_k\} \subseteq I_n$, $(A_i)_{i\in I}$ denotes the ordered tuple $(A_{i_1}, A_{i_2}, \cdots, A_{i_k})$ where an arbitrary fixed order in I 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 as $(T_1, \cdots, T_l)$.

Definition 2. *Let* $I_1, I_2, \cdots, I_l$ *be some disjoint subsets of* I_n *and suppose* $R_{I_j} = \{(A_i)_{i\in I_j} | \mathbf{a} \in \mathcal{C}\}$ *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* $\{\left((A_i)_{i\in I_1}, (A_i)_{i\in I_2}, \cdots, (A_i)_{i\in I_l}\right) | \mathbf{a} \in \mathcal{C}$ $R_{I_1} \times R_{I_2} \times \cdots \times R_{I_l}$. *They are called* **related** *if they are not unrelated.*

Now, the extensively studied F_{q^m}-linear cyclic codes over F_{q^m} can be characterized as follows:

- A cyclic code is the set of inverse DFT vectors of all the vectors of an F_{q^m}-subspace of $DFT(F_{q^m}^n) \subset F_{q^{mr}}^n$, in which transform components in $[j]_n^{q^m}$, $j \in I_n$, take either only the zero value or all the values of $F_{q^{mr_j}}$, and transform components in disjoint $[J_1]_n^{q^m}$ and $[J_2]_n^{q^m}$ are unrelated.

From the above characterization, it is clear that to specify a cyclic code, it is sufficient to specify the set $[J]_n^{q^m}$ in which the transform components of all the codewords is zero. It is important to note that the transform components A_j and A_k are not related by the conjugacy constraint of the DFT unless $[j]_n^{q^m} = [k]_n^{q^m}$. One of the results of this report is that in an F_qLC code, transform components take values from appropriate invariant subspaces (introduced in the following subsection). Moreover, the transform components from different q^m-cyclotomic cosets within a q-cyclotomic coset modulo n can be related for F_qLC codes by appropriate F_q-homomorphism (discussed in the next section) and all F_qLC codes are describable in terms of these relations along with the appropriate invariant subspaces.

2.1 Invariant subspaces of F_{q^l}

In this subsection we introduce the notion of invariant subspaces required for the characterization of F_qLC codes in transform domain. For any element s in a finite field 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 a 1-1 correspondence between $[j]_n^q$ and $[s]^q$, namely $jq^t \mapsto s^{q^t}$. So, $|[s]^q| = |[j]_n^q| = e_j$.

Definition 3. *For any element $s \in F_{q^l}$, a subset U of F_{q^l} is called* **s-invariant** *if $sU = U$. In addition, if U is an F_q-subspace, then it is called an s-***invariant** F_q**- subspace**. *For brevity, we shall write "$[s,q]$-subspace" instead of "s-invariant F_q-subspace". 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 s and s' are in the same q-conjugacy class, then $s' = s^{q^i}$ and $s = (s')^{q^j}$ for some i and j. So, $[s,q]$-subspaces and $[s',q]$-subspaces are the same.

Example 2.2. Consider $q = 2$, $m = 2$, $n = 15$ and $r = 2$. Let α be a primitive element of F_{16}. Since $[\alpha^5]^2 = [\alpha^{10}]^2$, we have $[\alpha^5, 2]$-subspaces to be the same as $[\alpha^{10}, 2]$-subspaces. The minimal $[\alpha^5, 2]$ subspaces of F_{2^4} are $V_1 = \{0, 1, \alpha^5, \alpha^{10}\}$, $V_2 = \{0, \alpha, \alpha^6, \alpha^{11}\}$, $V_3 = \{0, \alpha^2, \alpha^7, \alpha^{12}\}$, $V_4 = \{0, \alpha^3, \alpha^8, \alpha^{13}\}$, and $V_5 = \{0, \alpha^4, \alpha^9, \alpha^{14}\}$. These are also minimal $[\alpha^{10}, 4]$-subspaces. The $[\alpha^k, 2]$-subspaces, for $k \neq 0, 5, 10$ are $\{0\}$ and F_{16}. Every subset consisting of two elements $\{0, x\}; x \in F_{16}^*$ is a minimal $[\alpha^0, 2]$-subspace and none of these is an $[\alpha^0, 4]$-subspace. Observe that $\{1, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ is an α^3-invariant subset and not an $[\alpha^3, 2]$-subspace. The corresponding $[\alpha^3, 2]$-subspace, obtained as F_2-span of the set is F_{16}.

One can also talk about $[s, q^\lambda]$-subspaces of F_{q^l} when $\lambda | l$. The $[s, q^\lambda]$-subspaces are useful when one considers F_{q^λ}-linear codes over F_{q^m}. However, in such cases one can take q^λ to be q' and treat them as $F_{q'}$-linear codes over $F_{q'^{\frac{m}{\lambda}}}$. So, we will be concerned with only $[s,q]$-subspaces throughout the report.

Let s be an element of order t in F_{q^l}. Then, it is well known that $Span_{F_q}\{s^i | i = 0, 1, \cdots, t-1\} = F_q(s) = F_{q^e}$, where $e = [F_q(s) : F_q]$ is same as the cardinality of $[s]^q$. So, we have:

Theorem 2.1. *If e is the cardinality of $[s]^q$ and $F_{q^e} \subseteq F_{q^l}$ is the subfield of cardinality q^e, then for any $g \in F_{q^l} \setminus \{0\}$, the minimal $[s,q]$-subspace containing g is gF_{q^e}. Hence all minimal $[s,q]$-subspaces are of order q^e.*

3 Transform Domain Characterization of $FqLC$ Codes

Throughout, we consider length n codes over F_{q^m}, where n and q are relatively prime and α will denote the n-th primitive root of unity in $F_{q^{mr}}$, used as the DFT kernel.

From the cyclic shift property it follows that in an F_qLC code $\mathcal{C}$, the set of j^{th} transform components constitutes an $[\alpha^j, q]$-subspace of $F_{q^{mr}}$. However, a code need not be an F_qLC code even if each DFT component A_j takes values from an $[\alpha^j, q]$-subspace.

Example 3.1. Consider length 15, F_2L 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. We have chosen α with the minimal polynomial $X^2 + X + 1$.

The code $\mathcal{C}_3$ in Table 2 is not cyclic, since A_5 and A_{10} are related by an isomorphism which does not *correspond to cyclicity* in the time-domain. In the rest of this section we identify all the possible relations that correspond to cyclicity in the time domain leading to a characterization of F_qLC codes in the transform domain. The characterization is in terms of the component codes of a decomposition of the code under consideration. In the following subsection, we discuss the decomposition of F_qLC codes.

3.1 Decomposition of F_qLC Codes

Suppose A_j takes values from $V \subset F_{q^{mr}}$, $V \neq \{0\}$ for an F_qL 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_qL 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 $\{0\}$. If $\mathcal{C}''$ is a complement of $\mathcal{C}'$ in $\mathcal{C}$ and A_j takes values from V_2 in $\mathcal{C}''$, then V_2 is a complement of $V \bigcap V_1$ in V. 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 will be called the S-subcode of $\mathcal{C}$ and will be denoted as $\mathcal{C}_S$.

Lemma 3.1. *Suppose in an F_qL code $\mathcal{C}$, A_j takes values from a subspace $V \subseteq F_{q^{mr}}$. 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.*

Proof: We shall prove (i), then (ii) is obvious. It is sufficient to show that $\mathcal{C} \subset \mathcal{C}_1 + \mathcal{C}_2$. Consider a codeword $c_3 \in \mathcal{C}$. Suppose $A_j = v_3 \in V$ for c_3. Since $V = V_1 + V_2$, $\exists v_1 \in V_1$ and $v_2 \in V_2$ such that $v_3 = v_1 + v_2$. Let $c_1 \in \mathcal{C}_1$ such that $A_j = v_1$ for c_1. Now, for the codeword $c_2 = c_3 - c_1$, $A_j = v_3 - v_1 = v_2 \in V_2$. So, $c_2 \in \mathcal{C}_2$ and thus $c_3 = c_1 + c_2 \in \mathcal{C}_1 + \mathcal{C}_2$. □

Notice that $\mathcal{C}_2$ need not be a complement of $\mathcal{C}_1$ in $\mathcal{C}$ even if V_2 is a complement of V_1 since the intersection of $\mathcal{C}_1$ and $\mathcal{C}_2$ in that case is precisely the subcode obtained from $\mathcal{C}$ by restricting A_j to $\{0\}$.

Suppose in an F_qL code $\mathcal{C}$, a nonzero transform component A_j takes values from a nonzero F_q-subspace V of $F_{q^{mr}}$, and V intersects with more than one minimal $[\alpha^j, q]$-subspaces. Then, we have $t > 1$ minimal $[\alpha^j, q]$-subspaces $V_1, V_2, \cdots, V_t$ such that $V \subseteq \oplus_{i=1}^{t} V_i$ and $V \cap V_i \neq \phi$ for $i = 1, 2, \cdots, t$. Then, we can decompose the code as the sum of t smaller codes $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_t$ obtained by restricting A_j to $V_1, V_2, \cdots, V_t$, i.e., $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2 + \cdots + \mathcal{C}_t$. So by successively doing this for each j, we can decompose $\mathcal{C}$ into a set of subcodes, in each of which, for any $j \in I_n$, transform component A_j, if nonzero, takes values from an F_q-subspace of a minimal $[\alpha^j, q]$-subspace. In particular, if the original code was an F_qLC code, each of the subcodes obtained this way will have A_j from a minimal $[\alpha^j, q]$-subspaces or zero. The following are immediate consequences of this observation and Lemma 3.1.

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, the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ in Table 2 are minimal F_2LC codes and the nonzero transform components 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'.

3.1.1 Codes with Spectral Base

Definition 4. *Suppose in an F_qL 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* **spectral base** *if they are nonzero and 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.*

A code may not have a spectral base, since though we can always find a maximal subset of transform components which are unrelated, values of other components may not be determined by the values of those transform components.

As example, consider the code $\mathcal{C} = \mathcal{C}_5 + \mathcal{C}_6$ where $\mathcal{C}_5$ and $\mathcal{C}_6$ are from Table 2. Clearly, $\mathcal{C}_5$ and $\mathcal{C}_6$ have F_2-dimensions 4 and 2 respectively and $\mathcal{C}$ has dimension 6. In $\mathcal{C}$, both A_5 and A_{10} take values from F_{16}. So, $\{A_5, A_{10}\}$ is not a spectral base for $\mathcal{C}$ and neither of A_5 or A_{10} alone constitutes a spectral base. So, This code does not have a spectral base.

If a code has a spectral base, then it will be called a **code with spectral base**.

If some sets of transform components are unrelated in two codes $\mathcal{C}'$ and $\mathcal{C}''$, then it is unrelated in the code $\mathcal{C}' + \mathcal{C}''$. However, the converse is not true. For instance, consider the two F_2LC codes $\mathcal{C}_0$ and $\mathcal{C}_1$ and their sum $\mathcal{C}_4$ shown in Table 2. Clearly in $\mathcal{C}_0$ and $\mathcal{C}_1$, A_5 and A_{10} are related. But they are unrelated in $\mathcal{C}_4$.

If for an F_qLC code $\mathcal{C}$, A_j takes values from a minimal $[\alpha^j, q]$-subspace, then A_j is unrelated to $\{A_k | k \in K\}$ if and only if $\exists \mathbf{b} \in \mathcal{C}$ with DFT $\mathbf{B}$ such that $B_k = 0; \forall k \in K$ and $B_j \neq 0$.

Suppose, for an F_qLC code $\mathcal{C}$, A_j takes values from $[\alpha^j, q]$-subspace V_j for $j \in I_n$ and the transform components $\{A_k | k \in K\}$ are unrelated. Suppose A_j $(j \notin K)$ is fully related to $\{A_k | k \in K\}$ such that values of $\{A_k | k \in K\}$ for a codeword determines the value of A_j. By linearity of $\mathcal{C}$, this is equivalent to saying that for any codeword in $\mathcal{C}$, $A_k = 0\ \forall k \in K \ \Rightarrow A_j = 0$. For a fixed $k \in K$ and any $x \in V_k$, there is at least one codeword $\mathbf{b} \in \mathcal{C}$ with transform components $B_k = x$ and $B_l = 0\ \forall l \in K \setminus \{k\}$. For all such codewords, B_j takes a fixed value, say y, since otherwise difference of two such codewords will give a codeword $\mathbf{a} \in \mathcal{C}$ with $A_i = 0 \forall i \in K$ and $A_j \neq 0$ - a contradiction. So, $x \mapsto y$ defines a map $\sigma_k : V_k \to V_j$. By linearity of $\mathcal{C}$, σ_k is an F_q-homomorphism. Now, since $\{A_k | k \in K\}$ is unrelated, an arbitrary codeword $\mathbf{a} \in \mathcal{C}$ (with DFT $\mathbf{A}$) is sum of $|K|$ codewords $\mathbf{a}^{(k)}$; $k \in K$ (with DFTs $\mathbf{A}^{(k)}$) such that $A_k^{(k)} = A_k\ \forall k \in K$ and $A_i^{(k)} = 0\ \forall k \in K, i \in K \setminus \{k\}$. Hence $A_j^{(k)} = \sigma_k(A_k^{(k)})\ \forall k \in K \Rightarrow A_j = \sum_{k \in K} A_j^{(k)} = \sum_{k \in K} \sigma_k(A_k^{(k)}) = \sum_{k \in K} \sigma_k(A_k)$. Clearly, the argument also shows that the homomorphisms σ_ks are unique in this expression.

Theorem 3.2. *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 a spectral base $\{A_l | l \in L \subseteq I_n\}$ for $\mathcal{C}$*

Proof: We construct L iteratively as follows. First assign $L = \phi$, $L_1 = \{j \in I_n | A_j = 0 \text{ in } \mathcal{C}\}$ and do the following repeatedly until $L \cup L_1 = I_n$.

- Take any $j \in I_n \setminus (L \cup L_1)$. Consider the subcode $\mathcal{C}_1$ of $\mathcal{C}$ obtained by restricting $\{A_l | l \in L\}$ to zero. Clearly, in that subcode $\mathcal{C}_1$, either $A_j = 0$ or A_j takes values from V_j. If $A_j = 0$ in $\mathcal{C}_1$, then in $\mathcal{C}$, A_j can be expressed as $A_j = \sum_{l \in L} \sigma_l A_l$ for some F_q-homomorphisms $\sigma_l : V_l \longmapsto V_j$ and thus put j in L_1. Otherwise, $\{A_l | l \in L \cup \{j\}\}$ is a set of unrelated components in $\mathcal{C}$. So, put j in L.

Clearly, after all the iterations are over, the set L will be the indexes of a spectral base. Observe that the spectral base is not unique. □

Clearly, for a code $\mathcal{C}$ as described in Theorem 3.2, if $l \in L$, the subcode $\mathcal{C}_l$ obtained by restricting all the transform components $\{A_j | j \in L, j \neq l\}$ to zero is a minimal F_qLC code. Moreover, such a code $\mathcal{C}$ can be decomposed as $\mathcal{C} = \oplus_{l \in L} \mathcal{C}_l$. We have already seen that, any F_qLC code can be decomposed as a sum of F_qLC subcodes with nonzero transform components taking values from minimal invariant subspaces. So, each of the F_qLC subcodes $\mathcal{C}_l$ can now be further decomposed as direct sum of F_qLC minimal subcodes. So we have,

Theorem 3.3. *Any F_qLC code of length n, $(n, p) = 1$ over F_{q^m} can be decomposed as direct sum of minimal F_qLC codes.*

This theorem implies that, any m-QC code of length nm over F_q can be decomposed as direct sum of minimal m-QC codes, if $(n, q) = 1$. This was first proved in [12].

Corollary 3.1. *Let $\mathcal{C}$ be an F_qLC code of length n, $(n, p) = 1$ over F_{q^m}. For any proper F_qLC subcode $\mathcal{C}' \subsetneq \mathcal{C}$, there is an F_qLC subcode $\mathcal{C}'' \subsetneq \mathcal{C}$ such that $\mathcal{C} = \mathcal{C}' \oplus \mathcal{C}''$.*

Proof: Consider any decomposition $\mathcal{C} = \oplus_{i=1}^{t}\mathcal{C}_i$, where $\mathcal{C}_i$; $1 \leq i \leq t$ are minimal F_qLC codes. Since $\mathcal{C}' \neq \mathcal{C}$, $\exists i_1$; $1 \leq i_1 \leq t$ (take the minimum such i_1) such that $\mathcal{C}_{i_1} \nsubseteq \mathcal{C}' \Rightarrow \mathcal{C}_{i_1} \cap \mathcal{C}' = \{\mathbf{0}\}$ since $\mathcal{C}_{i_1}$ is a minimal F_qLC code and intersection of two F_qLC codes is an F_qLC code. So, $\mathcal{C}' \subsetneq \mathcal{C}' \oplus \mathcal{C}_{i_1} \subseteq \mathcal{C}$. If $\mathcal{C}' \oplus \mathcal{C}_{i_1} \neq \mathcal{C}$, we can repeat this process as many times as required to get $1 \leq i_1 < i_2 < \cdots < i_k \leq t$, such that $\mathcal{C}' \subsetneq \mathcal{C}' \oplus \mathcal{C}_{i_1} \oplus \mathcal{C}_{i_2} \oplus \cdots \oplus \mathcal{C}_{i_k} = \mathcal{C}$. Now, taking $\mathcal{C}'' = \mathcal{C}_{i_1} \oplus \mathcal{C}_{i_2} \oplus \cdots \oplus \mathcal{C}_{i_k}$, we have $\mathcal{C} = \mathcal{C}' \oplus \mathcal{C}''$. Moreover, $\{\mathbf{0}\} \subsetneq \mathcal{C}'' \subsetneq \mathcal{C}$ since $\mathcal{C} \supsetneq \mathcal{C}' \supsetneq \{\mathbf{0}\}$. $\square$

3.2 Linearized Polynomials and Induced Maps

Unlike linear cyclic codes, transform components in different q^m-cyclotomic cosets may be related in an F_qLC code as will be shown in next subsection. In particular, transform components may be related by F_q-homomorphisms. But two transform components can not be related by some arbitrary homomorphism. The allowed homomorphisms will be characterized in the next subsection in terms of linearized polynomials. In this subsection, linearized polynomials and their induced maps are discussed as a preparation to the next subsection.

Definition 5. *[22] 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 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

$$End_{F_q}(F_{q^l}) \quad = \quad \{\sigma_f : x \mapsto f(x) | f(X) = \sum_{i=0}^{l-1} c_i X^{q^i} \in F_{q^l}[X]\}. \tag{3}$$

For any $y \in F_{q^l} \setminus \{0\}$, the map $x \mapsto yx$ induced by the polynomial $f(X) = yX$ is an F_q-automorphism of F_{q^l} and will be denoted from now onwards 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 $f(X) = \sum_{i=0}^{l-1} c_i X^{q^i}$, $\sigma_f = \sum_{i=0}^{l-1} \sigma_{c_i}\theta_{q,l}^i$. So we have

$$End_{F_q}(F_{q^l}) \quad = \quad \oplus_{i=0}^{l-1}\mathbf{S}_{q,l}\theta_{q,l}^i. \tag{4}$$

That is, 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.

3.3 Transform Domain Characterization

The following theorem gives the basic condition that a homomorphism should satisfy to qualify for a possible relating homomorphism.

Theorem 3.4. *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 σ satisfies*

$$\sigma(\alpha^j v) = \alpha^k \sigma(v) \qquad\qquad \forall \quad v \in V_1. \tag{5}$$

Proof: Consider any $v \in V_1$. There is a codeword with transform pair $(A_k, A_j) = (\sigma(v), v)$. Since the code is cyclic, the cyclic shift of this vector with transform pair $(A_k, A_j) = (\alpha^k\sigma(v), \alpha^j v)$ is also a codeword. But, since $A_k = \sigma(A_j)$ holds for any codeword, $\alpha^k\sigma(v) = \sigma(\alpha^j v)$. $\square$

Clearly, kernel of such a homomorphism is an $[\alpha^j,q]$ subspace. However, for an F_qLC code, two related transform components may not be related by a homomorphism. But when each nonzero transform component A_j takes values from a minimal $[\alpha^j,q]$-subspace, then relations are by isomorphisms. To see that, let $\mathcal{C}$ be such an F_qLC code where each nonzero transform component A_j takes values from a minimal $[\alpha^j,q]$-subspace V_j of $F_{q^{mr}}$ and let $\{A_i | i \in L \subseteq I_n\}$ be a spectral base of $\mathcal{C}$. For any $k \notin L$, $A_k = \sum_{i\in L} \sigma_{ki} A_i$, for some unique F_q-homomorphisms $\sigma_{ki} : V_i \to V_k$. For a fixed $j \in L$, consider the F_qLC subcode $\mathcal{C}_1$ obtained by restricting $\{A_i | i \in L \setminus \{j\}\}$ to zero. For $\mathcal{C}_1$, $A_k = \sigma_{kj} A_j$. So, by Theorem 3.4 and the uniqueness of σ_{kj} in the expression $A_k = \sum_{k\in L} \sigma_{ki} A_i$, we have

$$\sigma_{kj}(\alpha^j v) = \alpha^k \sigma_{kj}(v) \ \forall v \in V_j \tag{6}$$

So, $Ker(\sigma_{kj})$ and $Im(\sigma_{kj})$ are $[\alpha^j,q]$ and $[\alpha^k,q]$-subspaces of V_j and V_k respectively. Then either $Ker(\sigma_{kj}) = V_j$, in which case σ_{kj} is a zero map, or $Ker(\sigma_{kj}) = \{0\}$, when σ_{kj} is injective. Also, either $Im(\sigma_{kj}) = \{0\}$, in which case σ_{kj} is a zero map, or $Im(\sigma_{kj}) = V_k$ i.e. σ_{kj} is surjective. So, σ_{kj} is either an isomorphism or a zero map. However, whenever, σ_{kj} is a zero map, we can remove the term $\sigma_{kj}A_j$ from the expression $A_k = \sum_{k\in L} \sigma_{ki} A_i$ and A_k can actually be said to be related only to those A_j; $j \in L$ for which σ_{kj} is nonzero.

In what follows, we present a sequence of results in terms of lemmas and theorems which leads to the transform domain characterization (Theorem 3.10). Recall that $Aut_{F_q}(F_{q^l})$ denotes the set of the invertible elements in $End_{F_q}(F_{q^l})$.

Lemma 3.5. *Suppose $x_1, x_2 \in F_{q^l}$. Then, $[x_1]^q = [x_2]^q$ if and only if there exists $\sigma \in Aut_{F_q}(F_{q^l})$ such that $\sigma(x_1 x) = x_2\sigma(x)$ $\forall x \in F_{q^l}$.*

Proof: ($\Rightarrow$): $[x_1]^q = [x_2]^q \Leftrightarrow x_2 \in [x_1]^q \Leftrightarrow \exists i$ s. t. $x_2 = x_1^{q^i}$. Now, clearly $\sigma = \theta^i_{q,l} \in Aut_{F_q}(F_{q^l})$ satisfies the condition $\sigma(x_1 x) = x_2 \sigma(x)$ $\forall x \in F_{q^l}$.

($\Leftarrow$): The given condition is equivalent to $\sigma\sigma_{x_1} = \sigma_{x_2}\sigma$. Let $\sigma = \sum_{i=0}^{l-1} \sigma_{(i)}$ be the canonical decomposition of σ. Then,

$$\begin{aligned}
& \sum_{i=0}^{l-1} \sigma_{(i)}\sigma_{x_1} = \sum_{i=0}^{l-1} \sigma_{x_2}\sigma_{(i)} \\
\Rightarrow \quad & \sigma_{(i)}\sigma_{x_1} = \sigma_{x_2}\sigma_{(i)} \quad \text{for} \quad 0 \le i \le l-1 \\
\Rightarrow \quad & \sigma_{x_1}^{q^i}\sigma_{(i)} = \sigma_{x_2}\sigma_{(i)} \quad \text{for} \quad 0 \le i \le l-1 \\
\Rightarrow \quad & x_1^{q^i} = x_2 \ \text{ or } \ \sigma_{(i)} = \mathbf{0} \quad \text{for} \quad 0 \le i \le l-1.
\end{aligned}$$

At least for one i, $\sigma_{(i)} \ne \mathbf{0}$ since $\sigma \ne \mathbf{0}$ and thus x_2 is in the q-conjugacy class of x_1. $\square$

Lemma 3.6. *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 satisfying*

$$\sigma(x_1 v) = x_2\sigma(v) \quad \forall \ v \in V_1. \tag{7}$$

Then $[x_1]^q = [x_2]^q$.

Proof: Since $Ker(\sigma) \subseteq V_1$ is an $[x_1, q]$ subspace, V_1 is a minimal $[x_1, q]$-subspace and σ is nonzero, $Ker(\sigma) = \{0\}$. Let $Im(\sigma) = V_2$. Then, σ is an isomorphism of V_1 onto V_2 satisfying

$$\sigma(x_1 v) = x_2 \sigma(v) \quad \forall \ v \in V_1. \tag{8}$$

V_2 is an x_2-invariant subspace, since for any $v = \sigma(v_1) \in V_2$, $x_2 v = x_2 \sigma(v_1) = \sigma(x_1 v_1) \in V_2$. Clearly, σ^{-1} satisfies

$$\sigma^{-1}(x_2 v) = x_1 \sigma^{-1}(v) \quad \forall \ v \in V_2. \tag{9}$$

If V_2 is not a minimal x_2-invariant subspace, then it can be decomposed as direct sum of some minimal x_2-invariant subspaces and restriction of σ^{-1} to at least one of the minimal x_2-invariant subspaces (say V_3) is nonzero. Then $\sigma^{-1}(V_3) \neq V_1$ is a proper x_1-invariant subspace of V_1: contradiction to minimality of V_1. So, V_2 is a minimal x_2 - invariant subspace. So, the size of the minimal x_1 - invariant subspaces and minimal x_2 - invariant subspaces are same i.e., $e_{x_1} = |[x_1]^q| = |[x_2]^q|$ and x_1-invariant subspaces and x_2 - invariant subspaces are same. Suppose $V_2 = y_1 F_{q^{e_{x_1}}}$ and $V_1 = y_2 F_{q^{e_{x_1}}}$. Then, define the map $\sigma_1 : F_{q^{e_{x_1}}} \longrightarrow F_{q^{e_{x_1}}}$ by $y \mapsto y_1^{-1}\sigma(y_2 y)$. Clearly, σ_1 is an F_q-automorphism and it satisfies $\sigma_1(x_1 v) = x_2 \sigma_1(v) \quad \forall \ v \in F_{q^{e_{x_1}}}$. So, by Lemma 3.5, $[x_1]^q = [x_2]^q$. $\square$

The fact that, the codes under consideration are F_qLC, does not allow any arbitrary sets of transform components to be related. The following theorem tells which components can be related in an F_qLC codes.

Theorem 3.7. *In an F_qLC code, the transform components of different q-cyclotomic cosets are unrelated.*

Proof: By Theorem 3.3, it is sufficient to show that the statement is true for minimal F_qLC codes. Let $J_1, J_2, \cdots, J_t$ be the distinct q-cyclotomic cosets in I_n. We need to prove that for a minimal F_qLC code, the transform component $\{A_j | j \in J_1\}, \{A_j | j \in J_2\}, \cdots, \{A_j | j \in J_t\}$ are unrelated. By Lemma 3.1, any nonzero transform component A_j takes values from a minimal $[\alpha^j, q]$-subspace for any minimal F_qLC code $\mathcal{C}$. So, for $\mathcal{C}$, there is a spectral base $\{A_l | l \in L\}$ for some $L \subseteq I_n$. From the remarks just after Theorem 3.2, L must be a singleton $\{l\}$. So, any other nonzero transform component A_k, $k \neq l$ is related to A_l as $A_k = \sigma A_l$ for some isomorphism $\sigma : V_l \to V_k$, where A_l and A_k take values from V_l and V_k respectively. By Lemma 3.6, $[\alpha^l]^q = [\alpha^k]^q \Rightarrow [l]_n^q = [k]_n^q$, i.e., for any minimal F_qLC code, transform components in only one q-cyclotomic coset modulo n can be nonzero. So, transform components in different cyclotomic cosets $J_1, J_2, \cdots, J_t$ are trivially unrelated.

Corollary 3.2. *(i) Any minimal F_qLC code has nonzero transform components only in one q-cyclotomic coset. (ii)Any minimal F_qLC code which has nonzero transform components in $[j]_n^q$ with exponent e has size q^e. (iii)Let $J_1, J_2, \cdots, J_t$ be the distinct q-cyclotomic cosets of I_n. Then any F_qLC code $\mathcal{C}$ can be decomposed as $\mathcal{C} = \oplus_{i=1}^t \mathcal{C}_{J_i}$, where the direct sum is over F_q.*

Suppose $\mathbf{b} \in F_{q^m}^n \setminus \{\mathbf{0}\}$ is such that it has nonzero transform components only in the q-cyclotomic coset of j. Then consider the F_qLC code $\mathcal{C}$ spanned by the cyclic shifts of $\mathbf{b}$. Clearly, the nonzero transform components (which are in $[j]_n^q$) take values from minimal $[\alpha^j, q]$-subspaces. Suppose, $B_j, B_{jq^l} \neq 0$. If $\mathbf{a}$ is the i times cyclic shift of $\mathbf{b}$, then $(A_j, A_{jq^l}) = (B_j \alpha^{ji}, B_{jq^l} \alpha^{ijq^l}) = \left(B_j \alpha^{ji}, (B_j^{-q^l} B_{jq^l})(B_j \alpha^{ji})^{q^l}\right) = (A_j, (B_j^{-q^l} B_{jq^l}) A_j^{q^l}) = (A_j, c A_j^{q^l})$, where $c = B_j^{-q^l} B_{jq^l}$. So, any linear combination of such codewords also has this same relation between the j-th and jq^l-th transform components, i.e., for $\mathcal{C}$, any nonzero transform component A_{jq^l} is related to A_j by isomorphism. So, $\mathcal{C}$ is of cardinality q^{e_j} and so it is a minimal F_qLC code.

For a given F_qLC code, when the corresponding m-quasi-cyclic codes are considered, $\mathcal{C}_{J_i}$, $i = 1, \cdots, t$, give the primary components [21] or irreducible components [12] of the code. But these primary components are not uniquely decomposable into minimal quasi-cyclic codes (or cyclic irreducible submodules, as is called in [12, 21]). 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 refer such F_qLC codes as one-generator F_qLC codes, whereas the corresponding quasi-cyclic codes are known as one-generator quasi-cyclic codes. For a one-generator F_qLC code $\mathcal{C}$, each component $\mathcal{C}_{J_i}$ is minimal, since otherwise, suppose $\mathcal{C}_{J_k}$ is not minimal and $\mathbf{b} \in \mathcal{C}_{J_k}$ such that $B_j = A_j \ \forall j \in J_k$ and $B_j = 0 \ \forall j \notin J_k$, such a $\mathbf{b}$ exists). The cyclic shifts of $\mathbf{b}$ span a minimal F_qLC subcode, say $\mathcal{C}_1$, of $\mathcal{C}_{J_k}$. Since $\mathcal{C}_{J_k}$ is not minimal, by Corollary 3.1, we can decompose $\mathcal{C}_{J_k}$ as $\mathcal{C}_{J_k} = \mathcal{C}_1 \oplus \mathcal{C}_2$, such that $\{\mathbf{0}\} \subsetneq \mathcal{C}_\mathbf{2} \subsetneq \mathcal{C}_{\mathbf{J_k}}$. Then clearly, $\mathcal{C}' = \mathcal{C}_1 \oplus_{i \neq k} \mathcal{C}_{J_i}$ contains $\mathbf{a}$: a contradiction, since $\mathcal{C}'$ is a proper F_qLC subcode of $\mathcal{C}$. So, $\mathcal{C}_{J_i}$; $i = 1, \cdots, t$, are minimal for any one-generator code $\mathcal{C}$. Moreover, if for an F_qLC code $\mathcal{C}$, $\mathcal{C}_{J_i}$ is direct sum of ν_i minimal F_qLC codes, then the code is generated by $max_{1 \leq i \leq t} \nu_i$ vectors and the F_q-dimension of the code is $\sum_{i=1}^{t} \nu_i |J_i|$.

Once we know which components can be related, we would like to know in what ways they can be related. The following lemma specifies all possible homomorphisms by which a transform component A_{jq^t} can be related to A_j, when A_j takes values from a minimal α^j-invariant subspace. As example, for a minimal F_qLC code, any nonzero transform component is a spectral base and it takes values from a minimal invariant subspace. The other transform components will be related by homomorphisms, specified by Lemma (3.8). For 1-generator F_qLC code, a set containing one nonzero transform component from each nonzero q-cyclotomic coset of transform components forms a spectral base and each transform component in the spectral base takes values from minimal invariant subspace. So, Lemma (3.8) gives the relations for 1-generator F_qLC codes also. In fact, any F_qLC code, where nonzero transform components takes values from minimal invariant subspaces, the relations of the other transform components with those in a spectral base are given by this lemma.

Lemma 3.8. *For some fixed $y \in F_{q^l}$, a homomorphism $\sigma : x_1 F_{q^{e_y}} \to x_2 F_{q^{e_y}}$ satisfies $\sigma(yx) = y^{q^t} \sigma(x) \ \forall x \in x_1 F_{q^{e_y}}$ iff σ is induced by a polynomial $f(X) = cX^{q^t}$ for some unique constant $c \in x_2 x_1^{-q^t} F_{q^{e_y}}$.*

Proof: Backward implication is trivial. For the forward implication, clearly σ satisfies the above condition if and only if $\sigma' : F_{q^{e_y}} \to F_{q^{e_y}}$; $x \mapsto x_2^{-1} \sigma(x_1 x)$ satisfies $\sigma'(yx) = y^{q^t} \sigma'(x) \ \forall x \in F_{q^{e_y}}$. Suppose, $f_1(X) = \sum_{i=0}^{e_y - 1} c_i' X^{q^i}$ induces the map σ'. Then, for any $x \in F_{q^{e_y}}$,

$$\begin{aligned}
& \sigma'(yx) = y^{q^t} \sigma'(x) \\
\Leftrightarrow \quad & \sum_{i=0}^{e_y - 1} c_i' y^{q^i} x^{q^i} = y^{q^t} \sum_{i=0}^{e_y - 1} c_i' x^{q^i} \quad \forall x \in F_{q^{e_y}} \\
\Leftrightarrow \quad & c_i' y^{q^i} x^{q^i} = y^{q^t} c_i' x^{q^i} \quad \forall x \in F_{q^{e_y}} \quad \text{for } i = 0, \cdots, e_y - 1 \\
\Leftrightarrow \quad & y^{q^i} x^{q^i} = y^{q^t} x^{q^i} \quad \forall x \in F_{q^{e_y}} \quad \text{whenever } c_i' \neq 0 \\
\Leftrightarrow \quad & i = t \quad \text{whenever } c_i' \neq 0.
\end{aligned}$$

So, there is at most one nonzero term $c' X^{q^l}$ in $f_1(X)$ where $c' \in F_{q^{e_y}}$. So, the map σ is induced by the polynomial $f(X) = x_2 f_1(x_1^{-1} X) = x_2 c' x_1^{-q^t} X^{q^t} = cX^{q^t}$ where $c = x_2 c' x_1^{-q^t} \in x_2 x_1^{-q^t} F_{q^{e_y}}$. ☐

For $y = \alpha^j$, this lemma specifies all possible homomorphisms by which A_{jq^t} can be related to A_j for an F_qLC

code when A_j takes values from a minimal α^j-invariant subspace.

Example 3.2. Clearly, in the minimal F_qLC 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_{2^4}.

For $\mathcal{C}_0$, $f(X) = \alpha^8 X^2$.

For $\mathcal{C}_2$, $f(X) = \alpha X^2$.

Example 3.3. Consider an F_qLC code with same parameters as in Table 2, where A_1, A_8, A_5 take values freely from F_{16}, F_{16}, and $\alpha^3 F_4$ respectively and other nonzero transform components A_2, A_4, and A_{10} are related to them as $A_2 = \alpha^2 A_1^2 + \alpha^5 A_8^4$, $A_4 = \alpha A_1^4 + \alpha^7 A_8^8$, and $A_{10} = \alpha^2 A_5^2$. This code is F_qLC but neither minimal nor 1-generator. But here the spectral base $\{A_1, A_8, A_5\}$ take values from minimal invariant subspaces and thus the other transform components relations with them are dictated by Lemma (3.8).

Even if a transform component does not take values from some minimal invariant subspace, another transform component may be related to it by homomorphism. The following theorem specifies all such homomorphisms. In particular, for a code with spectral base, the other transform components are related to those in the spectral base by homomorphisms, even though the transform components in the spectral base do not take values from minimal invariant subspaces. For a code with spectral base, the invariant subspaces of the components in a spectral base and the polynomials inducing the relating homomorphisms for other components specify the code completely.

Theorem 3.9. *Suppose $V \subseteq F_{q^l}$ is a y-invariant subspace and $V = \oplus_{j=0}^{t-1} V_j$ where V_j are minimal y-invariant subspaces. Then, for any $\sigma \in Hom_{F_q}(V, F_{q^l})$ satisfying $\sigma(yx) = y^{q^i}\sigma(x)\ \forall x \in V$, 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 $\sigma = \sigma_f$.*

Proof: By Lemma 3.8, there exists a unique $f_j(X) = b_j X^{q^i}$, $b_j \in F_{q^l}$, which induces $\sigma|_{V_j}$ i.e., $\sigma|_{V_j} = \sigma_{f_j}|_{V_j}$. Let us consider any polynomial $f(X) = \sum_{j=0}^{t-1} a_j X^{q^{je_y+i}}$ where $a_j \in F_{q^l}$. Now, $\sigma = \sigma_f \Leftrightarrow \sigma|_{V_j} = \sigma_{f_j}|_{V_j}\ \forall j$. Suppose $V_j = x_j F_{q^{e_y}}$; $x_j \neq 0$, for $j = 0, 1, \cdots, t-1$. For any $v \in V_j$, $v = x_j s$ for some $s \in F_{q^{e_y}}$. So,

$$\begin{aligned}
\sigma_f|_{V_k} = \sigma_{f_k}|_{V_k} \quad &\Leftrightarrow \quad f(x_k s) = f_k(x_k s)\ \forall s \in F_{q^{e_y}} \\
&\Leftrightarrow \quad \left(\sum_{j=0}^{t-1} a_j x_k^{q^{je_y+i}}\right) s^{q^i} = b_k x_k^{q^i} s^{q^i}\ \forall s \in F_{q^{e_y}} \\
&\Leftrightarrow \quad \sum_{j=0}^{t-1} a_j x_k^{q^{je_y+i}} = b_k x_k^{q^i}
\end{aligned}$$

So,

$$\sigma = \sigma_f \Leftrightarrow M \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} b_0 x_0^{q^i} \\ b_1 x_1^{q^i} \\ \vdots \\ b_{t-1} x_{t-1}^{q^i} \end{pmatrix} \tag{10}$$

where

$$M = \begin{pmatrix} x_0^{q^i} & x_0^{q^{e_y+i}} & x_0^{q^{2e_y+i}} & \cdots & x_0^{q^{(t-1)e_y+i}} \\ x_1^{q^i} & x_1^{q^{e_y+i}} & x_1^{q^{2e_y+i}} & \cdots & x_1^{q^{(t-1)e_y+i}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{t-1}^{q^i} & x_{t-1}^{q^{e_y+i}} & x_{t-1}^{q^{2e_y+i}} & \cdots & x_{t-1}^{q^{(t-1)e_y+i}} \end{pmatrix}$$

Now, $\{x_0, x_1, \cdots, x_{t-1}\}$ are linearly independent over $F_{q^{e_y}}$ since V is the direct sum of $x_0 F_{q^{e_y}}$, $x_1 F_{q^{e_y}}$, $\cdots$, $x_{t-1} F_{q^{e_y}}$. So, $\{x_0^{q^i}, x_1^{q^i}, \cdots, x_{t-1}^{q^i}\}$ are linearly independent over $F_{q^{e_y}}$ $\Rightarrow$ M is nonsingular [22] $\Rightarrow$ there exists unique solution of (10) for $a_0, a_1, \cdots, a_{t-1}$. $\square$

If for an F_qLC code, A_j takes values from an α^j-invariant subspace $V = \oplus_{l=0}^{t-1} V_l$ (where $V_l; l = 1, \cdots, t-1$ are minimal $[\alpha^j, q]$-subspaces) and A_{jq^i} is related to A_j by homomorphism, then the relation can be expressed as $A_{jq^i} = \sum_{l=0}^{t-1} c_l A_j^{q^{le_j+i}}$ for some constants $c_j \in F_{q^l}$. Suppose for an F_qLC code, $A_{j_1}, \cdots, A_{j_w}$ are unrelated and for $1 \le i \le w$, A_{j_i} takes values from direct sum of l_i minimal $[\alpha^{l_i}, q]$-subspaces. If A_k is related 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 3.4. In the code $\mathcal{C}_5$ in Table 2, A_5 is related to A_{10} by a homomorphism induced by the polynomial $f(X) = \alpha^{14} X^2 + \alpha^8 X^8$.

Example 3.5. Consider a code with the same parameters as in Table 2, where A_{14}, A_{13} and A_{10} take values freely from F_{16} which is not a minimal α^{10}-invariant subspace. Suppose the other nonzero transform components are related to these as $A_{11} = \alpha^6 A_{14}^4 + \alpha^4 A_{13}^2$, $A_7 = \alpha^7 A_{14}^8 + \alpha^{11} A_{13}^4$, and $A_5 = \alpha^7 A_{10}^2 + \alpha^{13} A_{10}^8$. It can be checked that the code constructed this way is an F_qLC code. $\{A_{14}, A_{13}, A_{10}\}$ is a spectral base of the code and so the other transform components are related to them by the homomorphisms as specified by Theorem 3.9.

In general, an F_qLC code may not have a spectral base and thus the relations between the transform components are not given by Theorem 3.9. For such a code, transform domain characterization can be given in terms of a decomposition of the code into F_qLC codes with spectral base. One such way of decomposing is by restricting the transform components to minimal invariant subspaces. From Theorem 3.2, Theorem 3.7 and Lemma 3.8, transform domain characterization of F_qLC codes can be stated as follows:

Theorem 3.10 (Transform Domain Characterization). *An F_qL code $\mathcal{C}$ in $F_{q^m}^n$ is an F_qLC-code iff for any $j \in I_n$, the transform components in $[j]_n^q$ and $I_n \setminus [j]_n^q$ are unrelated and for each $[j]_n^q$-subcode $\mathcal{C}_{[j]_n^q}$ the subcodes obtained by restricting the nonzero transform components to minimal α^j-invariant subspaces satisfy*

- *A_j is zero or takes values from a minimal α^j-invariant subspace.*
- *There is a maximal set L of unrelated components such that*

  $A_j = \sum_{l \in L} c_{jl} A_l^{q^{t_l}}$ for any nonzero A_j, where $c_{jl} \in F_{q^{r_j}}$ and $j \equiv l q^{t_l} \mod n$.

3.4 Special Cases

In this subsection we discuss several special cases arising out of restrictions on the values of n, q and m.

1. **No related components:** Recall that for a given n, the exponents of $[j]_n^q$ and $[j]_n^{q^m}$ are denoted by, respectively, e_j and r_j and $r_j = \frac{e_j}{(m, e_j)}$. If $(m, e_1) = 1$, i.e., m and e_1 are relatively prime, then $e_j = r_j$ for $0 \le j \le (n-1)$, and so no two q^m-cyclotomic cosets modulo n can be within one q-cyclotomic coset modulo n, since every q-cyclotomic coset modulo n is also a q^m-cyclotomic coset modulo n. In this case, no two or more transform components with indexes from different q^m-cyclotomic cosets can be related. In such cases, the F_qLC codes are completely specified by the invariant subspaces from which the nonzero transform components take values. Two such cases are $n = 15, q = 2$ and $m = 3$ and $n = 63, q = 2$ and $m = 5$.

2. m=**1:** When $m = 1$ we are considering conventional linear cyclic codes over F_q. This case is also the special case of the previous one i.e., the case for which no related components are possible.

4 Dual Codes of F_qLC Codes

In this section, we derive the equivalent condition in transform domain for two codes being dual of each other, and prove nonexistence of self dual F_qLC codes for certain cases. Unlike linear codes, dual of an F_qLC code has been defined as F_q-dual w. r. t. an F_q-basis of F_{q^m} [14]. Let $\{\gamma_1, \gamma_2, \cdots, \gamma_m\}$ be an F_q-basis of F_{q^m}. Each component a_i of $\mathbf{a} \in F_{q^m}^n$ can be uniquely decomposed as $a_i = \sum_{j=1}^{m} a_{ij}\gamma_j$. Two vectors $\mathbf{a}, \mathbf{b} \in F_{q^m}^n$ are called orthogonal to each other, if $\sum_{i=0}^{n-1}\sum_{j=1}^{m} a_{ij}b_{ij} = 0$, Henceforth, '$tr$' will always denote the F_{q^m}/F_q-trace.

Definition 6. *[22] An F_q-basis $\{\gamma_1, \gamma_2, \cdots, \gamma_m\}$ of F_{q^m} is called a* **self dual basis** *if*

$$\begin{aligned} tr(\gamma_i\gamma_j) = & \; 1 \qquad \text{if } i = j \\ = & \; 0 \qquad \text{if } i \neq j. \end{aligned}$$

Clearly, the j-th component of $\mathbf{x} \in F_{q^m}$ w. r. t. a self dual basis is given by $tr(\gamma_j x)$. It is known [28] that a self dual basis exists if and only if q is even or q and m are both odd.

We consider only the cases where a self dual basis of F_{q^m} exists and in which case define F_q duality with respect to such a basis. The following theorem gives the transform domain condition for two vectors to be F_q dual of each other.

Lemma 4.1. *For any $\mathbf{a}, \mathbf{b} \in F_{q^m}^n$, $\mathbf{a} \perp \mathbf{b}$ if and only if*

$$tr\left(\sum_{k=0}^{n-1} A_{-k}B_k\right) = 0. \tag{11}$$

Proof: Suppose $\{\gamma_1, \gamma_2, \cdots, \gamma_m\}$ is a self dual basis of F_{q^m}.

$$\begin{aligned} \mathbf{a} \perp \mathbf{b} \quad & \Leftrightarrow \quad \sum_{i=0}^{n-1}\sum_{j=1}^{m} a_{ij} tr(\gamma_j b_i) = 0 \\ & \Leftrightarrow \quad tr\left(\sum_{i=0}^{n-1}\sum_{j=1}^{m} a_{ij}\gamma_j b_i\right) = 0 \\ & \Leftrightarrow \quad tr\left(\sum_{i=0}^{n-1}\sum_{j=1}^{m} a_{ij}\gamma_j \sum_{k=0}^{n-1}\alpha^{-ik}B_k\right) = 0 \\ & \Leftrightarrow \quad tr\left(\sum_{k=0}^{n-1} B_k \sum_{i=0}^{n-1}\alpha^{-ik}\sum_{j=0}^{m} a_{ij}\gamma_j\right) = 0 \\ & \Leftrightarrow \quad tr\left(\sum_{k=0}^{n-1} B_k \sum_{i=0}^{n-1}\alpha^{-ik}a_i\right) = 0 \\ & \Leftrightarrow \quad tr\left(\sum_{k=0}^{n-1} B_k A_{-k}\right) = 0. \end{aligned}$$

□

Theorem 4.1 specializes to the case of $m = 1$ as: $\mathbf{a} \perp \mathbf{b}$ iff $\sum_{k=0}^{n-1} A_{-k}B_k = 0$.

Since for an F_qLC code $\mathcal{C}$, transform components in different q-cyclotomic cosets are unrelated, using Theorem 4.1, we can write $\mathcal{C}^\perp$ as (note that $J_1, J_2, \cdots, J_t$ are the distinct q-cyclotomic cosets of I_n):

$$\mathcal{C}^\perp = \left\{ \mathbf{b} \in F_{q^m}^n | tr\left(\sum_{k\in J_i} B_k A_{-k}\right) = 0 \text{ for } i = 1, \cdots, t \text{ and } \forall \mathbf{a} \in \mathcal{C} \right\}$$

and the J_i-subcode of $\mathcal{C}^\perp$ obtained by restricting A_j; $j \notin J_i$ to zero can be written as

$$\begin{aligned} \left(\mathcal{C}^\perp\right)_{J_i} &= \left\{ \mathbf{b} \in F_{q^m}^n | tr\left(\sum_{k\in J_i} B_k A_{-k}\right) = 0 \text{ and } B_k = 0 \text{ for } k \notin J_i \ \forall \mathbf{a} \in \mathcal{C} \right\} \\ &= \left\{ \mathbf{b} \in F_{q^m}^n | tr\left(\sum_{k\in J_i} B_k A_{-k}\right) = 0 \text{ and } B_k = 0 \text{ for } k \notin J_i \ \forall \mathbf{a} \in \mathcal{C}_{-J_i} \right\}. \end{aligned} \tag{12}$$

So, $\left(\mathcal{C}^\perp\right)_{J_i}$ is the biggest code with zero transform components outside J_i which is orthogonal to $\mathcal{C}_{-J_i}$.

Using Theorem 4.1, we get the following nonexistence result for self dual F_qLC codes.

Theorem 4.2. *There is no self dual F_qLC code over F_{q^m} when $(n, q) = 1$ and m is odd.*

Proof: For the cases under consideration, there is always a self dual basis $\{\gamma_1, \gamma_2, \cdots, \gamma_m\}$ of F_{q^m}. Suppose, in the F_qLC codes $\mathcal{C}$ and its dual $\mathcal{C}^\perp$, A_0 takes values from the F_q-subspaces $V \subseteq F_{q^m}$ and $V_1 \subseteq F_{q^m}$ respectively. Since A_0 is not related to other transform components, for any $v \in V$, there is a codeword in $\mathcal{C}$ with $A_0 = v$ and all other transform components zero. So according to Theorem (4.1), $V_1 = \{v_1 \in F_{q^m} | tr(vv_1) = 0 \ \forall v \in V\} = V^\perp$. Where $V^\perp$ is the trace dual subspace of V. If $\mathcal{C}$ is a self dual code, then $V = V^\perp \Rightarrow dim_{F_q}(V) = m - dim_{F_q}(V)$ which is impossible since m is odd. □

Note that the theorem is independent of the choice of the basis, though a self dual basis is used to prove it. If a self dual code exists w. r. t. any basis of F_{q^m}, then by change of basis we can get another code which is self dual w. r. t. a self dual basis.

Corollary 4.1. *There is no self dual m-QC code over F_q of length mn if m is odd and $(n, q) = 1$.*

Suppose q and m are even, n is odd and q-cyclotomic cosets modulo n are all singletons i.e., $n|(q-1)$. Then, by equation (12), A_0 should take values from one self dual subspace of F_{q^m} i.e., a subspace V such that

$$V = \{v \in F_{q^m} | tr(vu) = 0 \text{ for each } u \in V\}. \tag{13}$$

With respect to a self dual basis of F_{q^m}, such a subspace is image of a self dual code of length m over F_q. Since number of self dual codes of length m over F_q is $\prod_{i=1}^{\frac{m}{2}-1}(q^i+1)$ (see [24]), V can be chosen in $\prod_{i=1}^{\frac{m}{2}-1}(q^i+1)$ ways. For any other $k \in I_n$, A_k can be chosen to take values from any subspace V_k of F_{q^m} and A_{-k} should take values from it's dual subspace. So, the number of ways in which subspaces for A_k and A_{-k} can be chosen is $N(m, q)$= number of distinct subspaces of F_{q^m}. So, the total number of self dual quasi-cyclic codes with these parameters is $N(m, q)^{\frac{n-1}{2}} \prod_{i=1}^{\frac{m}{2}-1}(q^i+1)$.

Remark: Cor. 4.1 and the above expression for the total number of quasi-cyclic self dual codes are also available in [23].

5 Parity Check Matrix and Minimum Distance of Quasicyclic Codes

For linear codes, Tanner [33] used parity check equations over an extension field to derive minimum distance bound in terms of minimum distance of certain cyclic codes. Given a binary parity check matrix of a binary QC code, Tanner used block-wise DFT or block-wise linearized polynomial transform or Kronecker product of the two to get a set of parity check equations over an extension field of F_2.

An n-length F_qLC code over F_{q^m} can be considered as an m-QC code of length nm over F_q by expanding each component as F_q-linear combination of an F_q-basis of F_{q^m}. Similarly, any nm-length m-QC code can be considered as an n-length F_qLC code over F_{q^m}. Here we describe how in some cases one can directly get a set of parity check equations of a QC code over an extension field of F_q from the transform domain structure of the corresponding F_qLC code. Before doing so, we first give a theorem (Theorem 5.1) for the distance bound. This is in a slightly different form from Tanner's related theorems [33, Theorems 6,8 and 10] and the proof is also similar. Power of a vector will mean component-wise power. Note that, for a linear code, any linear combination of some parity check equations is again a parity check equation.

Theorem 5.1. *Let $\mathcal{C}$ be a linear code of length n over F_q. 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 (of $\mathcal{C}$) over F_{q^r}, then the minimum distance of the code $\mathcal{C}$ 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 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's are distinct.
For any $\mathbf{a} \in \mathcal{C}$ with 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

$$\begin{aligned} a'_{\lambda_i} &= a_i \ \text{ for } i \in I_n \\ a'_j &= 0 \ \text{ when } j \neq \lambda_i \ \ \forall i \in I_n \end{aligned}$$

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

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

□

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, a code obtained by taking the codewords with certain positions zeros and then deleting those positions)[24] 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, the decoding algorithm for the cyclic code can also be used to decode the shortened code. The decoder only have to pad zeros in the truncated positions and decode from the resulting $q^r - 1$ length vector.

[1]Theorem 5.1 has been reported in [13] in the context of DFT approach for QC codes and repeated here for the sake of completeness.

If $k_i = k_0 + i$ in Theorem 5.1, by the BCH bound we can conclude that the minimum distance of the n length code is at least δ.

Recall that the correspondence between F_qLC codes over F_{q^m} and m-QC codes over F_q is with respect to an F_q-basis of F_{q^m}. Let us take a basis $\{\beta_0, \beta_1, \cdots, \beta_{m-1}\}$. By our characterization of F_qLC codes in DFT domain, we know that for any $j \in I_n$, A_j can take values from any α^j-invariant subspace of $F_{q^{mr_j}}$. In particular, A_j can take values from subspaces of the form $c^{-1}F_{q^l}$ where $e_j|l$ and $l|mr_j$. Such a DFT domain restriction gives a parity check equation of the corresponding QC code over $F_{q^{mr}}$ as follows.

$$
\begin{aligned}
A_j \in c^{-1}F_{q^l} \quad & \Leftrightarrow cA_j \in F_{q^l} \\
& \Leftrightarrow (cA_j)^{q^l} = cA_j \\
& \Leftrightarrow \left(c\sum_{i=0}^{n-1} \alpha^{ij} a_i\right)^{q^l} = c\sum_{i=0}^{n-1} \alpha^{ij} a_i \\
& \Leftrightarrow \left(c\sum_{i=0}^{n-1} \alpha^{ij} \sum_{x=0}^{m-1} a_{ix}\beta_x\right)^{q^l} = c\sum_{i=0}^{n-1} \alpha^{ij} \sum_{x=0}^{m-1} a_{ix}\beta_x \\
& \Leftrightarrow c^{q^l} \sum_{i=0}^{n-1}\sum_{x=0}^{m-1} a_{ix}\alpha^{ijq^l}\beta_x^{q^l} = c\sum_{i=0}^{n-1}\sum_{x=0}^{m-1} a_{ix}\alpha^{ij}\beta_x \\
& \Leftrightarrow \sum_{i=0}^{n-1}\sum_{x=0}^{m-1} a_{ix}\left(c^{q^l}\alpha^{ijq^l}\beta_x^{q^l} - c\alpha^{ij}\beta_x\right) = 0.
\end{aligned}
$$

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 $h_{i,x} = \alpha^{ij}\beta_x$.

Now, for an 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, for some constants $c_{i,h_i} \in F_{q^{mr}}$,

$$
\begin{aligned}
& A_k && = \sum_{h_1=0}^{l_1-1} c_{1,h_1} A_{j_1}^{q^{h_1 e_k + t_1}} + \cdots \\
& && \quad + \sum_{h_w=0}^{l_w-1} c_{w,h_w} A_{j_w}^{q^{h_w e_k + t_w}} \\
\Leftrightarrow\quad & \textstyle\sum_{i=0}^{n-1} a_i\alpha^{ik} && = \sum_{h_1=0}^{l_1-1} c_{1,h_1} \left(\sum_{i=0}^{n-1} a_i\alpha^{ij_1}\right)^{q^{h_1 e_k + t_1}} + \cdots \\
& && \quad + \sum_{h_w=0}^{l_w-1} c_{w,h_w} \left(\sum_{i=0}^{n-1} a_i\alpha^{ij_w}\right)^{q^{h_w e_k + t_w}} \\
\Leftrightarrow\quad & \textstyle\sum_{i=0}^{n-1} a_i\alpha^{ik} && = \sum_{h_1=0}^{l_1-1} c_{1,h_1} \sum_{i=0}^{n-1} a_i^{q^{h_1 e_k + t_1}} \alpha^{ij_1 q^{h_1 e_k + t_1}} + \cdots \\
& && \quad + \sum_{h_w=0}^{l_w-1} c_{w,h_w} \sum_{i=0}^{n-1} a_i^{q^{h_w e_k + t_w}} \alpha^{ij_w q^{h_w e_k + t_w}} \\
\Leftrightarrow\quad & \textstyle\sum_{i=0}^{n-1}\sum_{x=0}^{m-1} a_{ix}\beta_x\alpha^{ik} && = \sum_{i=0}^{n-1}\sum_{x=0}^{m-1} a_{ix} \sum_{h_1=0}^{l_1-1} c_{1,h_1} \beta_x^{q^{h_1 e_k + t_1}} \alpha^{ij_1 q^{h_1 e_k + t_1}} + \cdots
\end{aligned}
$$

$$+\sum_{i=0}^{n-1}\sum_{x=0}^{m-1} a_{ix} \sum_{h_w=0}^{l_w-1} c_{w,h_w} \beta_x^{q^{h_w e_k + t_w}} \alpha^{i j_w q^{h_w e_k + t_w}}$$

$$\Leftrightarrow \quad \sum_{i=0}^{n-1}\sum_{x=0}^{m-1} a_{ix} \left(\beta_x \alpha^{ik} - \sum_{h_1=0}^{l_1-1} c_{1,h_1} \beta_x^{q^{h_1 e_k + t_1}} \alpha^{i j_1 q^{h_1 e_k + t_1}} - \cdots - \sum_{h_w=0}^{l_w-1} c_{w,h_w} \beta_x^{q^{h_w e_k + t_w}} \alpha^{i j_w q^{h_w e_k + t_w}} \right) = 0.$$

This gives a parity check vector $\mathbf{h}$ with $h_{i,x} = \left(\beta_x \alpha^{ik} - \sum_{h_1=0}^{l_1-1} c_{1,h_1} \beta_x^{q^{h_1 e_k + t_1}} \alpha^{i j_1 q^{h_1 e_k + t_1}} - \cdots - \sum_{h_w=0}^{l_w-1} c_{w,h_w} \beta_x^{q^{h_w e_k + t_w}} \alpha^{i j_w q^{h_w e_k + t_w}} \right)$.

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 5.1.

Since the DFT components in different q-cyclotomic cosets modulo n are unrelated, the set of parity check equations over F_{q^r} are union of the check equations corresponding to each q-cyclotomic coset modulo n. In a minimal code, any nonzero DFT component A_j takes values from a minimal α^j-invariant subspace and all other nonzero components (which are in the same q-cyclotomic coset modulo n) are related to A_j by an isomorphism. So, for any minimal code, a set of parity check vectors completely specifying the code can be obtained. Since for any one-generator code, $[j]_n^q$-subcode is minimal or zero for each j, a set of parity check vectors completely specifying the code can be obtained for one-generator codes also. 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 two examples. 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 $\{1, \beta, \beta^2, \cdots, \beta^{m-1}\}$ is taken as the basis.

Example 5.1. 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 corresponding 4-QC code

$$\begin{aligned} \mathbf{h_{(1)}} &= \left(1, \beta, \beta^2, \beta^3, 1, \beta, \beta^2, \beta^3, 1, \beta, \beta^2, \beta^3\right) \\ \text{and } \mathbf{h_{(2)}} &= \left(\beta^8, \beta^5, \beta^{12}, \beta^6, \beta^3, 1, \beta^7, \beta, \beta^{13}, \beta^{10}, \beta^2, \beta^{11}\right) \end{aligned}$$

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, five consecutive powers of $\mathbf{h_{(2)}}$ are parity check vectors of the corresponding QC code. Clearly, the dimension of the code is 4 since $A_1 \in F_{2^4}$. So, the corresponding QC code is a $[12, 4, 6]$ code.

Example 5.2. Consider the F_qLC code of length $n = 3$ over F_{2^3} given by the transform domain restriction $A_1 \in \beta^{62} F_{2^2}$, where the DFT is taken over F_{2^6}. With the chosen basis, this restriction in DFT domain gives the parity check vector of the corresponding 3-QC code of length 9 :

$$\mathbf{h} \quad = \quad \left(\beta^{54}, \beta^{14}, \beta^{35}, \beta^{55}, \beta^{15}, \beta^{36}, \beta^{56}, \beta^{16}, \beta^{37}\right).$$

The components of this vector are nonzero and distinct. Since $\mathbf{h}$ and it's conjugate $\mathbf{h}^2$ are both parity check equations of the QC code, this gives a minimum distance lower bound of 3. If we include the vector $\mathbf{h}^0 = (1, 1, \cdots, 1)$ as a parity check vector, we get a minimum distance bound of 4.

6 Discussion

The class of F_q-linear cyclic (F_qLC) codes over F_{q^m} have been characterized using the DFT defined over an extension field of F_{q^m}. The characterization is used to get minimum distance bound for m-quasi-cyclic codes of length mn. The characterization is also used to prove a nonexistance result for self dual quasi-cyclic codes. Some interesting special cases have been identified and discussed. The possible directions for further research include the following:

- A natural extension work is to study the rank-distance properties of the F_q-linear codes over F_{q^m} of this paper, in the same manner as has been done for cyclic codes over F_{q^m}, towards obtaining good space-time codes.
- The distance properties of F_qLC codes need to be investigated. The fact that SSRS codes and twisted BCH codes, which are subclasses of F_qLC codes, contain good codes [3, 4, 14, 14, 18] suggests that further good codes may be found in the class of F_qLC codes.
- All F_{q^m}-linear cyclic codes over F_{q^m} are F_qLC codes and not conversely. It is worth investigating to obtain a criteria/conditions under which a code can be seen as a linear code over F_{q^m} w. r. t. a different multiplication structure in F_{q^m}. In particular, this problem, when specialized to the class of group cyclic codes over elementary abelian groups is important since MDS group cyclic codes which are not linearizable have been reported [27, 36].
- It would be interesting to investigate the best choice of basis for a given F_qLC code for maximizing the minimum distance (or it's bound) of the corresponding quasicyclic code.

Table 1: Cyclotomic Cosets modulo 15 and 63

(a) Cyclotomic Cosets modulo 15

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

(b) Cyclotomic Cosets modulo 63

$2/2^5$-cyclotomic cosets	{0}	{1, 2, 4, 8, 16, 32}						{3, 6, 12, 24, 48, 33}						{5, 10, 20, 40, 17, 34}						{9, 18, 36}		
cardinality	1	6						6						6						3		
		{7, 14, 28, 56, 49, 35}						{11, 22, 44, 25, 50, 37}						{13, 26, 52, 41, 19, 38}						{27, 54, 45}		
		6						6						6						3		
		{15, 30, 60, 57, 51, 39}						{23, 46, 29, 58, 53, 43}						{31, 62, 61, 59, 55, 47}						{21, 42}		
		6						6						6						2		
$2^2/2^4$-cyclotomic cosets	{0}	{1, 4, 16}			{2, 8, 32}			{3, 12, 48}			{6, 24, 33}			{5, 20, 17}			{10, 40, 34}			{9, 18, 36}		
cardinality	1	3			3			3			3			3			3			3		
		{7, 28, 49}			{14, 56, 35}			{11, 44, 50}			{22, 25, 37}			{13, 52, 19}			{26, 41, 38}			{27, 54, 45}		
		3			3			3			3			3			3			3		
		{15, 60, 51}			{30, 57, 39}			{23, 29, 53}			{46, 58, 43}			{31, 61, 55}			{62, 59, 47}			{21}	{42}	
		3			3			3			3			3			3			1	1	
2^3-cyclotomic cosets	{0}	{1, 8}		{2, 16}		{4, 32}		{3, 24}		{6, 48}		{12, 33}		{5, 40}		{10, 17}		{20, 34}		{9}	{18}	{36}
cardinality	1	2		2		2		2		2		2		2		2		2		1	1	1
		{7, 56}		{14, 49}		{28, 35}		{11, 25}		{22, 50}		{44, 37}		{13, 41}		{26, 19}		{52, 38}		{27}	{54}	{45}
		2		2		2		2		2		2		2		2		2		1	1	1
		{15, 57}		{30, 51}		{60, 39}		{23, 58}		{46, 53}		{29, 43}		{31, 59}		{62, 55}		{61, 47}		{21, 42}		
		2		2		2		2		2		2		2		2		2		2		
2^6-cyclotomic cosets	{0}	{1}	{8}	{2}	{16}	{4}	{32}	{3}	{24}	{6}	{48}	{12}	{33}	{5}	{40}	{10}	{17}	{20}	{34}	{9}	{18}	{36}
cardinality	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
		{7}	{56}	{14}	{49}	{28}	{35}	{11}	{25}	{22}	{50}	{44}	{37}	{13}	{41}	{26}	{19}	{52}	{38}	{27}	{54}	{45}
		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
		{15}	{57}	{30}	{51}	{60}	{39}	{23}	{58}	{46}	{53}	{29}	{43}	{31}	{59}	{62}	{55}	{61}	{47}	{21}	{42}	
		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

Table 2: Few Length 15 F_2-Linear Codes over F_{16}
[Only nonzero transform components are shown. The nonzero 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}
	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
$\mathcal{C}_0$	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
	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
$\mathcal{C}_1$	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
	-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
$\mathcal{C}_4$	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
$\mathcal{C}_0$	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
$\mathcal{C}_1$	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
	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
$\mathcal{C}_6$	0	10	5	0	10	5	0	10	5	0	10	5	0	10	5	0	-1
	5	0	10	5	0	10	5	0	10	5	0	10	5	0	10	5	-1
	10	5	0	10	5	0	10	5	0	10	5	0	10	5	0	10	-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}
	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
$\mathcal{C}_2$	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
	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
$\mathcal{C}_3$	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
	-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
$\mathcal{C}_5$	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
$\mathcal{C}_0$	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
$\mathcal{C}_2$	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

References

[1] K.N.Manoj and B.Sundar Rajan, "Full Rank Distance Codes," Technical Report No:TR-PME-2002-16, Electrical Communication Engineering Department, IISc, Bangalore, India, October 4, 2002.

[2] B.Sundar Rajan and U.Sripati, "On the Rank-Distance Codes," Technical Report No:TR-PME-2003-04, Electrical Communication Engineering Department, IISc, Bangalore, India, October 4, 2003.

[3] J. Bierbrauer, The theory of cyclic codes and a generalization to additive codes, Designs, Codes and Cryptography, Vol. 25, No. 2 (2002), pp. 189-206.

[4] J. Bierbrauer, Direct constructions of additive codes, J. Combin. Designs, Vol. 10 (2002), pp. 207-216.

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

[6] G. Castagnoli, J. L. Massey, P. A. Schoeller and V. von Seemann, On repeated-root cyclic codes, IEEE Trans. Inform. Theory, Vol. 37 (1991), pp. 337-342.

[7] C. L. Chen, Byte-oriented error-correcting codes for semiconductor memory systems, IEEE Trans. on Computers, Vol. 35 (1986), pp. 646-648.

[8] C. L. Chen and L. E. Grosbach, Fault-tolerant memory design in the IBM application system/400, Digest of Papers, The 21-st International Symposium on Fault-Tolerant Computing (1991), pp. 393-400.

[9] C. L. Chen and M. Y. Hsiao, Error-correcting codes for semiconductor memory applications: a state-of-the-art review, IBM Journal Rs. Develop. Vol. 2 (1984), pp. 124-134.

[10] C. L. Chen, Symbol error-correcting codes for computer memory systems, IEEE Trans. on Computers, Vol. 35 (1986), pp. 646-648.

[11] C. L. Chen and L. E. Grosbach, Switching codes for delta-I noise reduction, IEEE Trans. on Computers, Vol. 45 (1996), pp. 1017-1021.

[12] J. Conan and G. Seguin, Structural properties and enumeration of quasi cyclic codes, Applicable Algebra in Engineering Communication and Computing, Vol. 4 (1993), pp. 25-39.

[13] B. K. Dey and B. Sundar Rajan, DFT domain characterization of quasicyclic codes, Applicable Algebra in Engineering, Communication and Computing, Vol. 13, Issue 6 (2003), pp. 453-474.

[14] Y. Edel and J. Bierbrauer, Twisted BCH-codes, J. Combin. Designs, Vol. 5 (1997), pp. 377-389.

[15] G. D. Forney Jr., Geometrically uniform uodes, IEEE Trans. Inform. Theory, Vol. 37 (1991), pp. 1241-1260.

[16] G. D. Forney Jr., On the Hamming uistance uroperties of uroup uodes, IEEE Trans. Inform. Theory, Vol. 38 (1992), pp. 1797-1801.

[17] 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).

[18] M. Hattori, R. J. McEliece and G. Solomon, Subspace subcodes of Reed-Solomon codes, IEEE Trans. Inform. Theory, Vol. 44 (1998), pp. 1861-1880.

[19] M. Isaksson and L. H. Zetterberg, Block-coded M-PSK modulation over $GF(M)$, IEEE Trans. Inform. Theory, Vol. 39 (1993), pp. 337-346.

[20] J. M. Jensen, Subgroup subcodes, IEEE Trans. Inform. Theory, Vol. 41 (1995), pp. 781-785.

[21] K. Lally and P. Fitzpatrick, Algebraic structure of quasicyclic codes, Discrete Applied Mathematics, Vol. 111, No 1-2 (2001), pp. 157-175.

[22] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, Vol. 20, Cambridge University Press (1987).

[23] S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields, IEEE Trans. Inform. Theory, Vol. 47 (2001), pp. 2751-2760.

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

[25] P. Mathys, Frequency domain description of repeated-root cyclic codes, Proceedings of 1994 International Symposium on Information Theory, Trondheim, Norway (1994), pp. 47.

[26] McDonald B. R., *Finite rings with identity*, Marcel Dekker, New York, 1974.

[27] M. Ran and J. Snyders, A cyclic [6,3,4] group code and the hexacode over $GF(4)$, IEEE Trans. Inform. Theory, Vol. 42 (1996), pp. 1250-1253.

[28] G. Seroussi and A. Lempel, Factorization of symmetric matrices and trace-orthogonal bases in finite fields, SIAM J. Computing Vol. 9 (1980), 758-767.

[29] 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 (1994), pp. 261-276.

[30] B. Sundar Rajan and M. U. Siddiqi, A generalized DFT for abelian codes over Z_m, IEEE Trans. Inform. Theory, IT-40 (1994), pp. 2082-2090.

[31] B. Sundar Rajan and M. U. Siddiqi, Transform domain characterization of abelian codes, IEEE Trans. Inform. Theory, Vol. 38 (1992), pp. 1817-1821.

[32] B. Sundar Rajan and M. U. Siddiqi, Transform decoding of BCH codes over Z_m, International J. of Electronics, Vol 75, No. 6 (1993), pp. 1043-1054.

[33] R. M. Tanner, A transform theory for a class of group-invariant codes, IEEE Trans. Inform. Theory, vol. 34 (1998), pp. 752-775.

[34] R. L. Townsend and E. J. Weldon, Jr., Self-orthogonal quasi-cyclic codes, IEEE Trans. Inform. Theory, vol. 13, No. 2 (1967), pp. 183-195.

[35] J. H. Van Lint, Repeated-root cyclic codes, IEEE Trans. Inform. Theory, Vol. 37 (1991), pp. 343-345.

[36] A. A. Zain and B. Sundar Rajan, Algebraic characterization of MDS group codes over cyclic groups, IEEE Trans. Inform. Theory, Vol. 41 (1995), pp. 2052-2056.