DFT Domain Characterization of Quasicyclic Codes

Bikash Kumar Dey
Dept. of Elect. Comm. Engg.
Indian Institute of Science
Bangalore 560012, India
e-mail: bikash@protocol.ece.iisc.ernet.in

B. Sundar Rajan[1]
Dept. of Elect. Comm. Engg.
Indian Institute of Science
Bangalore 560012, India
e-mail: bsrajan@ece.iisc.ernet.in

Abstract — **A code which is closed under m-times cyclic shift, is called m-quasicyclic code. DFT domain characterization of all linear quasicyclic codes over F_q of length relatively prime to q is obtained.**

I. Preliminaries

Let r be the smallest integer such that $n|(q^r-1)$ and $\alpha \in F_{q^r}$ is of order n. Then the DFT of $\mathbf{a}=(a_0,a_1,\cdots,a_{n-1}) \in F_q^n$ is defined to be $\mathbf{A}=(A_0,A_1,\cdots,A_{n-1}) \in F_{q^r}^n$, where

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

For Any $j \in [0,n-1]$, the **q-cyclotomic coset modulo n** of j, denoted by $[j]_n$, is defined as $[j]_n = \{i \in [0,n-1] | j \equiv iq^t \bmod n \text{ for some nonnegative integer } t\}$. Similarly, on the same set $[0,n-1]$, we define **q-cyclotomic coset modulo $\frac{n}{m}$** of j, denoted by $[j]_{\frac{n}{m}}$, as $[j]_{\frac{n}{m}} = \{i \in [0,n-1] | j \equiv iq^t \bmod \frac{n}{m} \text{ for some nonnegative integer } t\}$. Cardinality of $[j]_n$ is denoted as r_j. Clearly, $[j]_{\frac{n}{m}}$ is union of some q-cyclotomic cosets modulo n and cardinality of $[j]_{\frac{n}{m}}$ is mr_{mj}.

Any two different transform components in same q-cyclotomic coset modulo n are related by **conjugacy constraint**: $A_{jq} = A_j^q$. The main result in this paper is that, in case of quasicyclic codes the transform components can take values from certain proper subspaces of $F_{q^{r_j}}$ and components in different cyclotomic cosets modulo n can be related as long as they are in same cyclotomic coset modulo $\frac{n}{m}$. If $\mathbf{A} = DFT(\mathbf{a})$, $\mathbf{b} \in F_q^n$ such that $b_i = a_{i-1}$, and $\mathbf{B} = DFT(\mathbf{b})$, then $B_j = \alpha^j A_j$.

For any code $\mathcal{C}$ and $S \subseteq F_{q^r}$, $\{\mathbf{a} \in \mathcal{C} | A_j \in S\}$ is called the subcode obtained by restricting A_j in S. If $L \subset [0,n-1]$, then the code obtained by restricting $\{A_j | j \notin L\}$ to zero is denoted as $\mathcal{C}_L$ and is called **the L-subcode of $\mathcal{C}$.**

For every $s \in F_{q^r}^*$ $(= F_{q^r} \setminus \{0\})$, an F_q-subspace V of F_{q^r} is called an **s-invariant subspace** if it is closed under multiplication by s. An s-invariant subspace is said to be minimal if it does not have any proper s-invariant subspace.

Let $I_1, I_2, \cdots, I_t$ be some disjoint subsets of $[0,n-1]$ and suppose $R_{I_l} = \left\{(A_i)_{i \in I_l} | \mathbf{a} \in \mathcal{C}\right\}$ for $l = 1,2,\cdots,t$. The classes of transform components $\{A_i | i \in I_1\}, \{A_i | i \in I_2\}, \cdots, \{A_i | i \in I_t\}$ are called **mutually unrelated** if $\left\{\left((A_i)_{i\in I_1}, (A_i)_{i\in I_2}, \cdots, (A_i)_{i\in I_t}\right) | \mathbf{a} \in \mathcal{C}\right\} = R_{I_1} \times R_{I_2} \times \cdots \times R_{I_t}$. An m-quasicycli code is said to be minimal if it has no proper m-quasicyclic subcode.

II. Quasicyclic Codes in Transform Domain

From the definition and the cyclic shift property of DFT, we have

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

The following theorem identifies the relations between transform components of different cyclotomic cosets modulo n that give minimal m-quasicyclic codes.

Theorem 2 *In an n-length minimal linear m-quasicyclic code, transform components in only one cyclotomic coset modulo $\frac{n}{m}$, say $[j]_{\frac{n}{m}}$, is nonzero and any two nonzero transform components A_{j_1} and A_{j_2}, where $j_1, j_2 \in [j]_{\frac{n}{m}}$ and $[j_1]_n \neq [j_2]_n$, are related by an isomorphism σ with $f_\sigma(X) = cX^{q^t}$ i.e., $A_{j_2} = cA_{j_1}^{q^t}$ for some $c \in F_{q^r}$, where t is such that $j_2 \equiv j_1 q^t \bmod \frac{n}{m}$.*

For a quasicyclic code, if each transform component A_j takes values from a minimal α^{mj}-invariant subspace, then there is a subset $L \subset [0,n-1]$, such that $\{A_j | j \in L\}$ are unrelated and other transform components are determined by them. So, the code can be decomposed as direct sum of $|L|$ minimal codes, each obtained by restricting all but one of $\{A_j | j \in L\}$ to zero. Now, by restricting transform components to different minimal invariant subspaces, any quasicyclic code can be decomposed as sum of subcodes, in each of which any nonzero transform component takes values from minimal invariant subspace. So, any quasicyclic code can be decomposed as direct sum of minimal quasicyclic codes.

Since in a minimal quasicyclic code, transform components of different q-cyclotomic cosets mod n are unrelated, the same is true for any quasicyclic code. So, any quasicyclic code $\mathcal{C}$ can be written uniquely as $\mathcal{C} = \oplus_{i=1}^{l} \mathcal{C}_{[j_i]_{\frac{n}{m}}}$, where $[j_i]_{\frac{n}{m}}$ are the distinct q-cyclotomic cosets modulo $\frac{n}{m}$. These subcodes are actually the **primary components**[2] or **irreducible components** [1] of the code $\mathcal{C}$. However, these component codes can not be decomposed uniquely into direct sum of minimal quasicyclic codes. Suppose, k_i is the number of minimal quasicyclic codes, whose direct sum is $\mathcal{C}_{[j_i]_{\frac{n}{m}}}$. Then, the minimal number of generators for the code is given by $\max_{1\le i\le l} t_i$. Moreover, the dimension of the code is given by $\sum_{i=1}^{t} t_i r_{mj_i}$.

Suppose $k \equiv jq^t \bmod \frac{n}{m}$. If $A_j \in V = \oplus_{h=0}^{l-1} V_h$, where V_h are minimal α^{mj}-invariant subspaces, and if A_k is related to A_j by homomorphism, then, the relation is given by $A_k = \sum_{h=0}^{l-1} c_h A_j^{q^{hr_{mk}+t}}$ for some unique constants c_h.

References

[1] 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.

[2] K. Lally and P. Fitzpatrick, "Algebraic Structure of Quasicyclic Codes", to appear in *Discrete Applied Mathematics.*

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

0-7803-7123-2/01/$10.00 ©2001 IEEE