On the Rank Distance of Cyclic codes

U.Sripati and B.Sundar Rajan[1]
ECE Dept.,Indian Institute of Science
Bangalore,-560012,India
{sripati@protocol.,bsrajan@}ece.iisc.ernet.in

Abstract — **We study the rank-distance of primitive length ($n = q^m - 1$) linear cyclic codes over F_{q^m} using the Discrete Fourier Transform (DFT) description of these codes.**

I. Introduction

Let $\mathcal{C}$ be an $[n, k]$ linear code over F_{q^m}. For any pair of codewords $\vec{c_1}, \vec{c_2} \in \mathcal{C}$, the rank distance between them is defined to be the rank over F_q of the $m \times n$ matrix corresponding to $\vec{c_1} - \vec{c_2}$ obtained by expanding each entry of $\vec{c_1} - \vec{c_2}$ as an m-tuple along a basis of F_{q^m} over F_q and is denoted by $Rank_q(\vec{c_1} - \vec{c_2})$ [2]. The rank of $\mathcal{C}$, denoted by $Rank_q(\mathcal{C})$ is defined as the minimum of $Rank_q(\vec{c_1} - \vec{c_2})$ over all possible pairs of distinct codewords. Rank-distance codes over finite fields have been studied by several authors for applications in storage devices and more recently for applications in Space-Time coding. These studies are for the general class of linear codes and hence specific results like expressions or bounds for the rank of the code given by the description of the code are not known. In view of this, in this paper, we focus on primitive length ($n = q^m - 1$) cyclic codes over q^m and obtain expressions and upper bounds for the rank-distance of few sub classes of these codes. Note that this class of codes includes the well known Reed-Solomon codes.

DFT Description of cyclic codes:[1] Let $\vec{a} = (a_0, a_1, \cdots, a_{n-1}) \in F_{q^m}^n$ where q is power of a prime and $(n, q) = 1$ (i.e.,n and q are relatively prime-which is assumed to hold throughout the paper). Also let r be the smallest positive integer such that $n|q^{mr} - 1$ and let $\alpha \in F_{q^{mr}}$ an element of order n. The DFT of $\vec{a}$ is defined to be the vector $\vec{A} = (A_0, A_1, \cdots, A_{n-1}) \in F_{q^{mr}}^n$ given by $A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i, \quad j = 0, 1, \cdots, n-1$. Denoting the set $\{0, 1, \cdots, n-1\}$ by I_n, for any $j \in I_n$, for any divisor d of m the **q^d-cyclotomic coset of j modulo n** is defined to be the set $[j]^d = \{i \in I_n | j = iq^{dt} \pmod n \text{ for some } t \geq 0\}$ and we will denote the cardinality of this set by $e_j^{(d)}$. When $d = 1$ we denote the q-cyclotomic coset of j modulo n by $[j]$ and its cardinality by e_j. Simply by "cyclotomic coset", we mean a "q-cyclotomic coset". For a code $\mathcal{C}$ we say A_j takes values from $\{\sum_{i=0}^{n-1} \alpha^{ij} a_i | \vec{a} \in \mathcal{C}\} \subset F_{q^{mr}}$. For linear cyclic codes A_j takes values from $\{0\}$ or $F_{q^{me_j^{(m)}}}$ and transform components in different q^m-cyclotomic cosets are unrelated and within a q^m-cyclotomic coset are related by $A_{jq^m} = A_j^{q^m}$ (called **conjugacy constraints**). The transform components taking values from $F_{q^{me_j^{(m)}}}$ are called free spectral components. Note that for length $n = q^m - 1$ codes over F_{q^m} each cyclotomic coset is a singleton set and there is no conjugacy constraint. Also we will be using the following sets frequently throughout that are closely related to the cyclotomic cosets:$\alpha_{[j]^d} = \{\alpha^i | i \in [j]^d\}$ and $A_{[j]^d} = \{A_i | i \in [j]^d\}$.

[1]This work was partly supported by the DRDO-IISc program on Mathematical Engineering through a grant to B.S.Rajan

II. Rank-distance of $q^m - 1$ length cyclic codes

The following proposition is straightforward.

Proposition 1: Let $\mathcal{C}$ be a cyclic code of length n over F_{q^m} with A_0 being one of the free transform domain components. Then $Rank_q(\mathcal{C}) = 1$.

Identifying codewords with all the components from a proper subfield of F_{q^m} leads to

Proposition 2: Let a cyclic code $\mathcal{C}$ of length $n = q^m - 1$ over F_{q^m} be characterized by all the free transform domain components in the union of sets of the form $A_{[j]^d}$ for some values of j and all other transform domain components 0. Then $Rank_q(\mathcal{C}) \leq d$.

Theorem 1: Let $\mathcal{C}$ be a cyclic code of length $n = q^m - 1$ over F_{q^m} such that the transform domain component $A_{jq^s} \in A_{[j]}, (0 \leq s \leq e_j - 1)$ is the only free component and all other transform domain components are constrained to zero. Then $Rank_q(\mathcal{C}) = e_j$.

Theorem 2: Consider a cyclic code $\mathcal{C}$ of length $n = q^m - 1$ over F_{q^m} for which the two transform domain components A_{jq^r} and $A_{jq^{r+s}}$ are free, (s denotes the separation between the two free transform domain components) $(0 \leq r \leq e_j - 2), (1 \leq s \leq e_j - 1)$ and all other transform domain components be constrained to 0. Then $Rank_q(\mathcal{C}) = (e_j - gcd(s, e_j))$. Moreover, the rank weight distribution of $\mathcal{C}$ is given by $N_0 = 1$; $N_{e_j - gcd(s,e_j)} = \tau(q^m - 1)$; $N_{e_j} = q^{2m} - N_{e_j - gcd(s,e_j)} - 1$, where N_i denotes the number of codewords with rank weight i and τ is the number of elements of F_{q^m} that have their $(q^s - 1)$-th root in $F_{q^{e_j}}$.

An Upper Bound: We can make use of Theorem 2 to obtain an upper bound on the Rank of a code $\mathcal{C}$ characterized by more than two free transform domain components drawn from the same cyclotomic coset as follows:

Let $A_{jq^{s_1}}, A_{jq^{s_2}}, \cdots, A_{jq^{s_l}}, \cdots, A_{jq^{s_i}}, \cdots, A_{jq^{s_k}}$ be the k free transform domain components. Then

$$Rank_q(\mathcal{C}) \leq \min_{(i,l),(i>l)} \{e_j - gcd[(s_i - s_l), e_j]\} = e_j - \max_{(i,l),(i>l)} \{gcd[(s_i - s_j), e_j]\}.$$

The following theorem identifies certain situations leading to a tighter upper bound.

Theorem 3: Let $A_{jq^{s_1}}, A_{jq^{s_2}}, \cdots, A_{jq^{s_k}}$ be the set of all free transform domain components of $\mathcal{C}$ where $s_1, s_2, \cdots, s_k$ with $s_1 < s_2 < \cdots < s_{k-1} < s_k \leq e_j - 1$ are related by $s_2 - s_1 = s_3 - s_2 = \cdots = s_k - s_{k-1} = s_1 - s_k = s'$ modulo e_j, where s' divides e_j. Then $Rank_q(\mathcal{C}) \leq s'$.

References

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

[2] E. M. Gabidulin, "Theory of Codes with Maximum Rank Distance," Problemy Peredachi Informatsii, 21, 99.3-14, Jan.-Mar.1985.

0-7803-7728-1/03/$17.00 ©2003 IEEE.