On The Dimension of SSRS Codes

Mehta Sheetalkumar R.
Dept. of Elect. Comm. Engg.
Indian Institute of Science
Bangalore 560012, India
e-mail: mehta@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 Subspace Subcode of Reed-Solomon (SSRS)[1] code is a subcode of a Reed-Solomon (RS) code (called parent code) over F_{p^m} consisting of codewords whose components all lie in a fixed v-dimensional (over F_p; p- a prime)vector subspace V of F_{p^m}. In this paper we present a formula for the cardinality of an SSRS code by viewing V as an $[m, v]$ linear code over F_p with parity check matrix H. Our formula is in terms of H and counting the endomorphisms of F_{p^m} satisfying certain conditions resulting from the DFT domain characterization of SSRS codes.**

I. Preliminaries.

Let C be an $[n, k_0, d_0]$ RS code over F_{p^m} defined by the parity check polynomial $h(x) = \prod_{j\in J}(x - \alpha^j)$, where J is a subset of k_0 consecutive integers of $\{0, 1, \ldots, n-1\}$ and α is a primitive n-th root of unity in F_{p^m}. The **DFT** of $\mathbf{X} = (X_0, X_1, \ldots, X_{n-1}) \in F_{p^m}^n$ is defined to be $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in F_{p^m}^n$, given by $x_j = \sum_{i=0}^{n-1} \alpha^{ij} X_i$, $j = 0, 1, \ldots, n-1$. For $j \in \{0, 1, \ldots, n-1\}$, let $[j]_n^p = \{jp^i / i = 0, 1, \ldots, d_j - 1\}$ denote the **jth cyclotomic coset modulo n**, where d_j is the smallest positive integer such that $jp^{d_j} \equiv j (\mathrm{mod}\ n)$. Note that $d_j | m$ and let $f_j = m/d_j$.

Let I_n denote the set consisting of the smallest integers in each cyclotomic coset. Given the set J, for each $j \in I_n$, define $J_j = J \cap [j]_n^p$. Let $e_j = |J_j|$. Define the index set A_j as $A_j = \{i / jp^i (\mathrm{mod}\ n) \in J_j, 0 \le i \le d_j - 1\}$. Thus $|A_j| = e_j$.

Since the minimum distance of a subcode is lower bounded by that of the parent code, finding the dimension of the subcode is important. Hattori, McEliece and Solomon have given a formula for the dimension of SSRS code, for the case $p = 2$, using the notion of trace dual subspace, which we call the HMS dimension formula:

Theorem 1 *[1] (HMS Dimension Formula) Let the parent RS code be defined over the field F_{2^m}, then the binary dimension $K(C, V)$ of the SSRS code C_V is given by,*

$$K(C, V) = \sum_{j\in I_n} d_j (e_j f_j - r_j) \qquad (1)$$

where r_j is the rank of jth cyclotomic matrix Γ_j [1].

II. DFT Domain Dimension Formula

For every $s \in F_{p^m}^*$, (nonzero elements of F_{p^m}), an F_p-subspace V of F_{p^m} is called an **s-invariant F_p-subspace** if $sV = V$. If $s = \alpha^j$ we denote the invariant subspace by $[j, p]$-invariant subspace. An $[j, p]$-invariant subspace is said to be minimal if it does not have any proper nonzero $[j, p]$-invariant subspace. Let the set $V_j = \{V_{j,1}, V_{j,2}, \ldots, V_{j,v_j}\}$ denote the set of all minimal $[j, p]$-invariant subspaces, where $v_j = |V_j|$. Note $|V_{j,l}| = p^{d_j}$ for all $l \in \{0, 1, \ldots, v_j\}$ and v_j is given by, $v_j = \frac{p^m - 1}{p^{d_j} - 1}$.

SSRS codes are nonlinear and cyclic and constitute a proper subclass of F_p-Linear Cyclic (F_pLC) codes over F_{p^m} [3]. We use the DFT domain characterization of minimal F_pLC codes [2, 3]. A minimal F_pLC code has in its transform domain description, zeros in all transform components except components of one cyclotomic coset modulo n, say $[j]_n^p$, and in $[j]_n^p$ only one component is free taking values from a minimal $[j, p]$-invariant subspace, the rest are either related to this free component or zero. If related, say $x_{j_2} = \sigma_{j_2,j_1} x_{j_1}$ then $j_2 = j_1 p^\lambda$ where $\lambda \in \{0, 1, \ldots, d_j - 1\}$ and $\sigma_{j_2,j_1} \in \mathbf{S}\theta^\lambda$, where **S** is a Singer Cycle, which is a matrix realization of the multiplicative group of F_{p^m} and θ is a generator of a cyclic subgroup of order m in the Normalizer of **S** [2]. The **Defining endomorphism** [2] of a minimal F_pLC code, δ_j is given by, $\delta_j = \sum_{j_2\in J_j} \sigma_{j_2,j_1}$, where the minimal code takes nonzero values in J_j and j_1 is the free component. For $j \in I_n$, let Δ_j denote the set of all $(\frac{p^{me_j} - 1}{p^m - 1})$ defining endomorphisms of the minimal F_pLC codes taking nonzero values in J_j.

Viewing the subspace V as an $[m, v]$ linear code over F_p, let **H** denote a parity check matrix of V.

Theorem 2 *[4] The cardinality of the SSRS code C_V is given by the formula,*

$$|C_V| = \prod_{j\in I_n} \left[(p^{d_j} - 1) \left(\sum_{l=1}^{\frac{p^m-1}{p^{d_j}-1}} N_{j,l} \right) + 1 \right] \qquad (2)$$

where $N_{j,l}$ denote the number of defining endomorphisms $\delta \in \Delta_j$ such that $V_{j,l} \in ker\ (\mathbf{H}\delta)$, $l = 1, 2, \ldots, \frac{p^m-1}{p^{d_j}-1}$.

References

[1] M. Hattori, R. J. McEliece and G. Solomon, "Subspace Subcodes of Reed-Solomon Codes," *IEEE Trans. Information Theory*, Vol. 44, No. 5, September 1998, pp. 1861 – 1880.

[2] A. A. Zain, *An Algebraic Approach to MDS and Dual Group Codes over Finite Abelian Groups*, Ph.D. Thesis, Indian Institute of Technology, Delhi, April 1996.

[3] Bikash Kumar Dey and B. Sundar Rajan, "F_q-linear cyclic codes over F_{q^m}: Transform Approach," submitted to IEEE Trans. Information Theory.

[4] Mehta Sheetalkumar R., On The Dimension and Exceptional Subspaces of SSRS Codes, M.Sc.(Engg) Thesis, ECE Department, Indian Institute of Science, Bangalore, Feb.2001.

[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