Matrix Characterization of Near-MDS Codes over Z_m and Abelian Groups

G. Viswanath and B. Sundar Rajan[1]
Department of Electrical Communication Engineering
Indian Institute of Science
Bangalore, 560 012, India
email: {gviswa@protocol., bsrajan@}ece.iisc.ernet.in

Abstract — **In this paper we present a matrix characterization of $AMDS$ codes and $NMDS$ codes over Z_m and Abelian groups.**

I. $AMDS$ and $NMDS$ Codes over Z_m

A length-n linear code C over Z_m, the ring of integers modulo m, is a subset of Z_m^n closed under all Z_m-linear combinations. C is said to be information set supporting if $|C| = m^k$ for some integer $k < n$ and there are k coordinate positions such that the restriction of $|C|$ to these k positions is Z_m^k, in which case C is referred as an $[n, k, d]$ code over Z_m where d stands for the minimum Hamming distance of C.

Definition 1 *An $[n, k, d]$ code C over Z_m is said to be an Almost-MDS $(AMDS)$ code if the $d = n - k$. It is said to be Near-MDS $(NMDS)$ if $d = n-k$ and the minimum Hamming distance of the dual code of C is k.*

Theorem 1 *An $[n, k, d]$ linear code over Z_m, where $m = p_1^{r_1} p_2^{r_2} p_3^{r_3} \dots p_s^{r_s}$ (where p_i $1 \le i \le s$ are prime numbers) with systematic generator matrix $G = [I_k \;\; P_{k,n-k}]$ (after suitable column permutations) is an $AMDS$ code if and only if every $(g, g+1)$ submatrix has (g, g) submatrices such that*

- *there exists at least one (g, g) submatrix whose determinant is a unit in Z_m or*
- *if the determinants of all the (g, g) submatrices are zero divisors then the greatest common divisor of these determinants is an unit in Z_m.*

II. $AMDS$ and $NMDS$ Codes over Abelian Groups

Definition 2 *An $[n, k]$ systematic group code C of length n and dimension k over an Abelian group G is a subgroup of G^n with order $|G|^k$ consisting of n-tuples, $(x_1, x_2, \cdots, x_k, y_1, \cdots, y_{n-k})$ with $y_i = \phi_i(x_1, x_2, \dots, x_k)$ where ϕ_i are $(n-k)$ homomorphisms from G^k into G.*

Definition 3 *Consider a finite Abelian group G with cardinality m. An $[n, k = log_m(|C|), d]$ code C over G is an Almost-MDS $AMDS$ code if $d = n - k$. An $AMDS$ code C is said to be Near-MDS (NMDS) if its dual code [2] is also $AMDS$.*

Theorem 2 *A $[k+s, k]$ group code over G, defined by the homomorphisms $\{\phi_1, \phi_2, \dots, \phi_s\}$ is $AMDS$ if and only if every $(g, g+1)$ submatrix of the associated matrix of the form*

$$\Psi_{g,g+1} = \begin{bmatrix} \psi_{i_1 j_1} & \psi_{i_1 j_2} & \dots & \psi_{i_1 j_{g+1}} \\ \psi_{i_2 j_1} & \psi_{i_2 j_2} & \dots & \psi_{i_2 j_{g+1}} \\ \vdots & \vdots & \dots & \vdots \\ \psi_{i_g j_1} & \psi_{i_g j_2} & \dots & \psi_{i_g j_{g+1}} \end{bmatrix} \quad (1)$$

for $1 \le i_k \le g$, $1 \le j_k \le (g+1)$, $g = 1, 2, \dots, min\{s, k\}$, has

- *at least one (g, g) submatrix which represents an automorphism of G^g or*
- *if every (g, g) submatrix represents an endomorphism of G^g then the intersection of the kernels of the endomorphisms is only the identity element of G^g.*

We specialize to the case where the group G is a cyclic group C_m, i.e., a cyclic group of order m.

Definition 4 *An homomorphism $\phi : C_m^k \to C_m$ is called a distance non decreasing homomorphism $(DNDH)$ if either $K_\phi = \{\vec{e}\}$ or $d_{min}(K_\phi) = 1$, where $\vec{e}$ is the identity element of C_M^k, K_ϕ denotes the kernel of ϕ and d_{min} stands for minimum Hamming distance.*

Lemma 3 *A $[k+1,\, k]$ group code is $AMDS$ if and only if the defining homomorphism is an $DNDH$.*

Definition 5 *Let $\{\phi\}_{i=1}^{i=s}$ denoted as Φ_s be a set of homomorphisms from $C_m^k \to C_m$ denoted as $\Phi_{(s)}$. Let $K_{\phi_1 \phi_2 \dots \phi_s}$ denote $K_{\phi_1} \cap K_{\phi_2} \cap \dots K_{\phi_s}$ where K_{ϕ_i} is the kernel of ϕ_i. Φ_s is said to be a distance non decreasing set of homomorphisms, $(DNDSH)$, if the following conditions are satisfied:*

- *the homomorphisms do not constitute a set of $DISH$ [2]*
- *for all $1 \le r \le s$ $d_{min}(K_{\phi_{i_1} \phi_{i_2} \dots \phi_{i_r}}) \ge r$ or*
- *$K_{\phi_{i_1} \phi_{i_2} \dots \phi_{i_r}} = \{\vec{e}\}$.*

Theorem 4 *A $[k+s,\, k]$ group code is $AMDS$ if and only if the defining homomorphisms Φ_s constitute a set of $DNDSH$.*

Lemma 5 *Over C_m, where $m = p_1^{d_1} p_2^{d_2} p_3^{d_3} \dots p_r^{d_r}$, where p_i's are distinct primes, $[k+s,\, s]$ $AMDS$ group codes, for all $s, k \ge 2$, do not exist if $k \ge r + 2(p-1)$, where $p = min\{p_1, p_2, \dots, p_r\}$.*

Lemma 6 *Over C_m, where $m = p_1^{d_1} p_2^{d_2} p_3^{d_3} \dots p_r^{d_r}$, with all primes p_i distinct, the dual of $[k+s,\, s]$ $AMDS$ group codes, for all $s, k \ge 2$ do not exist if $s \ge r + 2(p-1)$, where $p = min\{p_1, p_2, \dots, p_r\}$.*

References

[1] S. M. Dodunekov and I. N. Landgev, 'On Near-MDS Codes', Technical Report, No:LiTH-ISY-R-1563, Department of Electrical Engineering, Linkoping University, February, 1994.

[2] A. A. Zain and B. Sundar Rajan, 'Algebraic Characterization of MDS Group Codes over Cyclic Groups', *IEEE Trans. Information Theory*, Vol.41, No.6, Nov., 1997, pp.2052-2056.

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