A CONSTRUCTION OF NON-REED-SOLOMON TYPE MDS CODES

RON M. ROTH, MEMBER, IEEE AND ABRAHAM LEMPEL, FELLOW, IEEE

Department of Computer Science

Technion, Israel Institute of Technology

Haifa 32000 - Israel

ABSTRACT

We present a construction of long MDS codes which are not of the generalized Reed-Solomon (GRS) type. The construction employs subsets S, $|S| = m$, of a finite field $F = GF(q)$ with the property that no t distinct elements of S add up to some fixed element of F. Large subsets of this kind are used to construct $[n = m + 2, k = t + 1]$ non-GRS MDS codes over F.

I. INTRODUCTION

An $[n, k, d]$ linear code over $F = GF(q)$ is called *maximum distance separable* (MDS) if $d = n - k + 1$ [4, Ch. 11]. Some upper bounds on the lengths of MDS codes derive from the fact that, for certain ranges of k, n, and q, every MDS code must be a *generalized Reed-Solomon* (GRS) code, i.e., generated by

$$G_{RS} = \begin{bmatrix} 1 & 1 & \cdots & 1 & 0 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{n-2} & \cdot \\ \cdot & \cdot & \cdots & \cdot & 0 \\ \cdot & \cdot & \cdots & \cdot & 0 \\ \alpha_0^{k-1} & \alpha_1^{k-1} & \cdots & \alpha_{n-2}^{k-1} & 1 \end{bmatrix} \cdot V,$$

where the $\alpha_i \in F$ are distinct and V is a diagonal, nonsingular matrix [3],[5].

A set $S \subseteq F$ of size m is called an (m, t, δ)-*set* in F if there exists an element $\delta \in F$ such that no t elements of S sum to δ. In this paper we present a construction which produces an $[m+2, t+1]$ MDS code which is *not* GRS from any given (m, t, δ)-set in F, $m \geq t + 2$. As a method for obtaining long non-GRS MDS codes, the suggested construction reduces to the combinatorial problem of finding the largest (m, t, δ)-set in $GF(q)$ for given t and q. Lower bounds on the cardinality of such sets are derived in Section III. For related work and references see, for instance, [1].

II. A CONSTRUCTION OF NON-GRS CODES

Let n and k be two integers such that $k \geq 3$ and $k + 3 \leq n \leq q + 2$. Consider the $[n, k]$ code over F generated by the matrix

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 & 0 & 0 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{n-3} & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & 0 & 0 \\ \cdot & \cdot & \cdots & \cdot & 0 & 1 \\ \alpha_0^{k-1} & \alpha_1^{k-1} & \cdots & \alpha_{n-3}^{k-1} & 1 & \delta \end{bmatrix},$$

where the α_i are distinct elements of F and $\delta \in F$. First we show that G does not generate a

GRS code; then we prove that G generates an MDS code if and only if the α_i form an $(n-2, k-1, \delta)$-set in F.

Let

$$g_i(x) = \sum_{j=0}^{k-1} g_{ij} x^j \triangleq \prod_{0 \le j \le k-1 \,:\, j \ne i} (x - \alpha_j), \quad 0 \le i \le k-1,$$

and let $P = [g_{ij}]_{0 \le i, j \le k-1}$. Consider the matrix $\bar{G} \triangleq P \cdot G = [\Lambda \; A]$, where $\Lambda = [\lambda_{ij}]_{0 \le i, j \le k-1}$ consists of the first k columns of $\bar{G}$. By the definition of P, $\lambda_{ij} = g_i(\alpha_j)$ and, therefore, Λ is a diagonal matrix with $\lambda_{ii} = g_i(\alpha_i) \ne 0$.

One can easily verify that the last three columns of A are given by

$$\bar{A} = \begin{bmatrix} \dfrac{a}{\alpha_{n-3} - \alpha_0} & 1 & b + \alpha_0 \\ \dfrac{a}{\alpha_{n-3} - \alpha_1} & 1 & b + \alpha_1 \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \dfrac{a}{\alpha_{n-3} - \alpha_{k-1}} & 1 & b + \alpha_{k-1} \end{bmatrix},$$

where $a \triangleq \prod_{i=0}^{k-1} (\alpha_{n-3} - \alpha_i) \ne 0$ and $b \triangleq \delta - \sum_{i=0}^{k-1} \alpha_i$. To prove that G does not generate a GRS code, it suffices to show that $\bar{A}$, and therefore $A = [a_{ij}]$, is not a Cauchy matrix [4, p. 323]; that is, there exist no nonzero c_i and d_j, distinct x_i, and distinct y_j such that

$$a_{ij} = \frac{c_i d_j}{x_i + y_j}, \quad 0 \le i \le k-1, \quad 0 \le j \le n-k-1,$$

possibly with one of the columns (rows) of A having the form $d_\infty (c_0 \; c_1 \cdots c_{k-1})'$ $(c_\infty (d_0 \; d_1 \cdots d_{n-k-1}))$ [6].

Lemma 1. [5]. *Given a $k \times r$ Cauchy matrix $A = [a_{ij}]$ over $F = GF(q)$, we can always assume $a_{0j} = d_j$ and $a_{1j} = d_j y_j^{-1}$, $0 \le j \le r-1$.*

Applying Lemma 1 to $\bar{A}$, after a permutation of columns and transposition, we can assume $d_j = 1$ and $y_j = a^{-1}(\alpha_{n-3} - \alpha_j)$, $0 \le j \le k-1$, so that for some $c \ne 0$ and x,

$$\frac{c \cdot d_j}{x + y_j} = b + \alpha_j , \quad 0 \le j \le k-1 ,$$

or

$$\frac{c}{a^{-1}(\alpha_{n-3} - \alpha_j) + x} = b + \alpha_j , \quad 0 \le j \le k-1 . \tag{1}$$

Regarding (1) as a quadratic equation in α_j, it has at most $2 < k$ solutions.

Now, for G to generate an MDS code, every set of k columns of G must be linearly independent. It suffices to check only sets of k columns containing $\mathbf{u} = (0\ 0 \cdots 0\ 1\ \delta)'$ but not $\mathbf{u}_\infty = (0\ 0 \cdots 0\ 1)'$. Consider a $k \times k$ matrix B consisting of $\mathbf{u}$ and any $k-1$ columns of G but $\mathbf{u}_\infty$. Without loss of generality, we may write

$$B = \begin{bmatrix} 1 & 1 & \cdots & 1 & 0 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{k-2} & \cdot \\ \cdot & \cdot & \cdots & \cdot & 0 \\ \cdot & \cdot & \cdots & \cdot & 1 \\ \alpha_0^{k-1} & \alpha_1^{k-1} & \cdots & \alpha_{k-2}^{k-1} & \delta \end{bmatrix}.$$

Let A_i be the coefficient of x^i in the polynomial $\det(B(x))$, where

$$B(x) = \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_0 & \alpha_1 & \cdots & \alpha_{k-2} & x \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \alpha_0^{k-1} & \alpha_1^{k-1} & \cdots & \alpha_{k-2}^{k-1} & x^{k-1} \end{bmatrix}.$$

Then, $\det(B) = A_{k-2} + \delta \cdot A_{k-1}$. By the Vandermonde form of $B(x)$, we have

$$\sum_{i=0}^{k-1} A_i x^i = \prod_{0 \le i < j \le k-2} (\alpha_j - \alpha_i) \prod_{i=0}^{k-2} (x - \alpha_i) .$$

Thus, $A_{k-1} \ne 0$, $A_{k-2} = -A_{k-1} \sum_{i=0}^{k-2} \alpha_i$, and $\det(B) \ne 0$ if and only if $\sum_{i=0}^{k-2} \alpha_i \ne \delta$. Therefore, G generates an MDS code if and only if the α_i form an $(n-2, k-1, \delta)$-set.

III. DERIVATION OF LOWER BOUNDS

Let $S(t, q, \delta)$ denote a largest (m, t, δ)-set in $GF(q)$, let $M(t, q, \delta) = |S(t, q, \delta)|$, and let $M(t, q) \triangleq \max_{\delta \in F} M(t, q, \delta)$. Our objective is to obtain lower bounds on $M(t, q)$ which, by the construction of Section II, provide lower bounds on the maximal length of non-GRS MDS codes.

Lemma 2. *If* $(t, q) = 1$, *then* $M(t, q, \delta) = M(t, q)$ *for all* $\delta \in GF(q)$.

Proof. Let δ_1 and δ_2 be two distinct elements of F and let S_1 be an (m, t, δ_1)-set in F, where $(t, q) = 1$. Consider the set

$$S_2 \triangleq \{ \alpha + t^{-1}(\delta_2 - \delta_1) \mid \alpha \in S_1 \} .$$

Clearly, S_2 is an (m, t, δ_2)-set, implying $M(t, q, \delta_1) \leq M(t, q, \delta_2)$. As δ_1 and δ_2 are arbitrary elements of F, the value of $M(t, q, \delta)$ is independent of δ. □

Thus, when $(t, q) = 1$, it suffices to examine the values of, say, $M(t, q, 0)$ in order to obtain lower bounds on $M(t, q)$. Note also that for every $\delta \neq 0$, $M(t, q, \delta) = M(t, q, 1)$ (regardless of the value of (t, q)), since every (m, t, δ)-set S can be transformed into an $(m, t, 1)$-set by multiplying each element of S by δ^{-1}. The inverse transformation exists as well.

Clearly, $M(1, q) = q - 1$ for every q, since we may set $S(1, q, 0) = F - \{0\}$ and no $(m, 1, 0)$-set may contain the zero element. Also, $M(q-1, q) = q - 1$ with $S(q-1, q, 0) = F - \{\alpha\}$ for any $\alpha \in F - \{0\}$. For $2 \leq t \leq q - 2$ we distinguish between even and odd q and begin with the even case.

Lemma 3. *For* $q = 2^h$, $h \geq 2$,

$$M(2, q) = q .$$

Proof. No two distinct elements of F sum to zero. □

For a set $S \subseteq F$, denote by $\sigma(S)$ the sum of elements of S. Note that every (m, t, δ)-set S, $t < m$, is also an $(m, m-t, \sigma(S)-\delta)$-set.

Lemma 4. *For* $q = 2^h$ *and* $3 \le t \le \frac{q}{2} - 2$,

$$M(t,q) \ge \begin{cases} \frac{q}{2}+1 & \text{if } \ t \in \{3, \frac{q}{2}-2\} \\ \frac{q}{2} & \text{if } \ 3 < t < \frac{q}{2}-2 \end{cases} .$$

Proof. Let $\Omega = \{\omega_i\}_{i=0}^{h-1}$ be a basis of $F = GF(q)$, when viewed as a vector-space of dimension h over $GF(2)$, and associate $(a_0\ a_1 \cdots a_{h-1}) \in GF(2)^h$ with $\alpha = \sum_{i=0}^{h-1} a_i \omega_i$. Assume, first, that t is odd. In this case the elements of odd Hamming weight form a $(\frac{q}{2}, t, 0)$-set, since the weight of the sum of any odd number of such elements must be odd and, therefore, nonzero. The same construction yields a $(\frac{q}{2}, t, \omega_0)$-set for even t. In the special case of $t \in \{3, \frac{q}{2}-2\}$, we can join the zero element to form a $(\frac{q}{2}+1, t, 0)$-set. □

Remark. Lemma 4 can be shown to hold with equality. As the full proof is rather tedious, we present here only the case $t = 3$. Suppose there exists a $(\frac{q}{2}+2, 3, \delta)$-set S. Let $\alpha \in S - \{\delta\}$ and define $T \triangleq S - \{\alpha\}$. Since $|T| > \frac{q}{2}$, there exist distinct $\beta, \gamma \in T$ such that

$$\beta + \gamma = \delta + \alpha ,$$

implying $\sigma(\{\alpha, \beta, \gamma\}) = \delta$, in contradiction to the definition of S.

Lemma 5. *For* $q = 2^h$ *and* $\frac{q}{2} - 1 \le t \le q - 2$,

$$M(t,q) = t + 2 .$$

Proof. Every $(t+2, 2, 0)$-set S is also a $(t+2, t, \sigma(S))$-set, so that $M(t,q) \ge t+2$. On the other hand, if there were a $(t+3, t, \delta)$-set S, it would also serve as a $(t+3, 3, \sigma(S)-\delta)$-set, implying $t \le M(3,q) - 3 = \frac{q}{2} - 2$, contrary to the stated range of t. □

The given lower bounds on $M(t,q)$ guarantee the existence of $[n,k]$ non-GRS MDS codes over $GF(q)$, $q=2^h$, for the following values of n and k:

k	n
3	$q+2$
4	$\frac{q}{2}+3$
$5 \le k \le \frac{q}{2}-2$	$\frac{q}{2}+2$
$\frac{q}{2}-1$	$\frac{q}{2}+3$
$\frac{q}{2} \le k \le q-1$	$k+3$

These are not necessarily the longest possible codes with the said properties. For example, when $q=2^h$, $h \ge 7$, there exists a $[q+1, 4, q-2]$ non-GRS code [3, §5(3)], which can be utilized to construct $[k+4, k, 5]$ non-GRS codes for $\frac{q}{2} \le k \le q-3$.

We turn now to finite fields of odd size.

Lemma 6. *Let q be a power of an odd prime. Then,*

$$M(2,q) = \frac{q+1}{2}\,.$$

Proof. Let $\{\alpha_i\}_{i=0}^{q-1}$ denote the elements of F so that $\alpha_0 = 0$ and $\alpha_i = -\alpha_{q-i}$, $1 \le i \le \frac{q-1}{2}$, and let $S = \{\alpha_i\}_{i=0}^{(q-1)/2}$. Clearly, S is a $(\frac{q+1}{2}, 2, 0)$-set in F, implying $M(2,q) \ge \frac{q+1}{2}$. To show equality, note that any set $S' \subseteq F$ of size greater than $\frac{q+1}{2}$ must contain both α_i and α_{q-i} for some i, $1 \le i \le \frac{q-1}{2}$. □

The following is the analog of Lemma 5 for odd values of q.

Lemma 7. *Let q be a power of an odd prime. Then, for $\frac{q-1}{2} \le t \le q-2$,*

$$M(t,q) = t+1\,.$$

Proof. Every $(t+1,1,0)$-set S is also a $(t+1,t,\sigma(S))$-set. The proof of tightness is similar to that in Lemma 5. □

It is easy to see that the construction of Section II cannot be used to obtain non-GRS MDS codes for $k \geq \frac{q+1}{2}$. There exists however an example of a $[10,5,6]$ non-GRS construction over $GF(9)$ [3] and it would be nice to have a general construction of non-GRS MDS codes also for this range of k.

Lemma 8. *Let q be a power of an odd prime. Then, for* $3 \leq t \leq \frac{q-3}{2}$,

$$M(t,q) \geq t+2 .$$

Proof. Any $(t+2,2,0)$-set S is also a $(t+2,t,\sigma(S))$-set. □

In many cases, one can do much better than that. Consider first the case $q = p$, an odd prime. Here we have

$$M(3,p) \geq \lfloor \frac{p+7}{3} \rfloor \triangleq r ,$$

by taking the set

$$S = \{ 0, 1, 2, \cdots, r-1 \} .$$

The bound $M(t,p) \geq \lfloor ((p-2)/t) + t \rfloor$ is easy to obtain also for larger t. For small p we have the following values of $M(t,p)$, $3 \leq t \leq \frac{p-3}{2}$:

t	$M(t,11)$	$M(t,13)$	$M(t,17)$	$M(t,19)$	$M(t,23)$
3	6	6	8	8	10
4	6	6	7	8	9
5		7	8	8	9
6			8	8	9
7			9	9	10
8				10	10
9					11
10					12

Considering extension fields $GF(q)$, $q = p^h$, and $t \le \frac{q}{p}$, we have $M(t,q) \ge \frac{q}{p}$ by taking the elements of $GF(q)$ whose leading coefficient is 1 when viewed as h-vectors over $GF(p)$. Furthermore, for $3 \le t \le p-1$ we have $M(t,q) \ge \lfloor \frac{p}{t} \rfloor \cdot \frac{q}{p}$ by taking all h-vectors with leading coefficients $a, 1 \le a \le \lfloor \frac{p}{t} \rfloor$.

These lower bounds on $M(t,q)$ yield non-GRS MDS constructions for the following values of n and k over $GF(q)$, q odd: for $k = 3$ we obtain a $[\frac{q+5}{2}, 3]$ non-GRS MDS code; a special case of this construction for $q \equiv 3 \pmod 4$ results in a code which is known to be a *complete arc*: appending any column to its generator matrix violates the MDS property [2, p. 215]. Applying Lemma 8, we obtain a $[k+3, k, 4]$ non-GRS code for all $4 \le k \le \frac{q-1}{2}$. For small values of k longer codes can be obtained; when $k = 4$, for instance, the non-GRS construction yields a code whose length is of the order $\frac{q}{3}$. When $GF(q)$ is an extension field of characteristic p, $[\frac{q}{p}+2, k]$ non-GRS MDS codes exist for all $k \le \frac{q}{p} - 1$.

REFERENCES

[1] G.T. Diderrich, H.B. Mann, "Combinatorial problems in finite Abelian groups", *A Survey of Combinatorial Theory,* J.N. Srivastava et al. (Ed.), North-Holland, Amsterdam, 1973.

[2] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields.* Clarendon Press, Oxford, 1979.

[3] J.W.P. Hirschfeld, "Maximal sets in finite projective spaces", *Surveys in Combinatorics,* E.K. Lloyd (Ed.), LMS Lecture Notes Series 82, Cambridge University Press, Cambridge, 1983, pp. 55-76.

[4] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam, 1977.

[5] R.M. Roth, A. Lempel, "On MDS codes via Cauchy matrices", to appear.

[6] R.M. Roth, G. Seroussi, "On generator matrices of MDS codes", *IEEE Transactions on Information Theory,* vol. IT-31, 1985, pp. 826-830.