ON MDS CODES VIA CAUCHY MATRICES

RON M. ROTH AND ABRAHAM LEMPEL, FELLOW, IEEE

Department of Computer Science

Technion, Israel Institute of Technology

Haifa 32000 - Israel

ABSTRACT

The special form of Cauchy matrices is used to obtain a tighter bound for the validity region of the MDS Conjecture and a new compact characterization of generalized Reed-Solomon codes. The latter is further used to obtain constructions and some nonexistence results of long $[2k, k]$ double-circulant MDS codes.

This work was presented in part at the IEEE International Symposium on Information Theory, Kobe, June 1988.

I. INTRODUCTION

An $[n, k, d]$ linear code over $F = GF(q)$ is called *maximum-distance-separable* (in short, MDS) if it attains the *Singleton bound* $d \le n - k + 1$ [10, Ch. 11]. A $k \times n$ matrix G over F is a generator matrix of an MDS code if and only if every k columns of G are linearly independent. If G is a *systematic* generator matrix, i.e., $G = [I \ A]$, I being the identity matrix, then G generates an MDS code if and only if every square sub-matrix of A is nonsingular. Such matrices A will be called *super-regular*.

When $k = 1$, there exist arbitrarily long MDS codes, e.g., repetition codes and, when $k \ge q$, a code is MDS only if it has minimum distance ≤ 2. Therefore, we shall deal only with codes of dimension k, $2 \le k \le q-1$. In this case, it is known that MDS codes cannot be arbitrarily long. Let $N_{\max}(k, q)$, $2 \le k \le q-1$, be the maximal length of any MDS code of dimension k over $GF(q)$. Then, $q+1 \le N_{\max}(k, q) \le q + k - 1$. Furthermore, for some special cases of k and q it can be shown that $N_{\max}(k, q) = q + 1$. The MDS Conjecture states that the same equality holds for all q and $2 \le k \le q-1$, except when q is even and $k \in \{3, q-1\}$, in which case $N_{\max}(k, q) = q + 2$.

MDS codes have the following geometric interpretation. Viewing the columns of G as points in the $(k-1)$-st dimensional projective space $PG(k-1, q)$, no k columns of G lie on a hyperplane, and so the columns of G form an *n-arc* [5, Chs. 8-10][6]. Therefore, $N_{\max}(k, q)$ is the maximal length of any n-arc in $PG(k-1, q)$.

A well-known family of MDS codes is the set of *generalized Reed-Solomon* (in short, GRS) codes. Let $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$ be distinct elements of F and let $v_0, v_1, \cdots, v_{n-1}$ be nonzero elements of F. The standard generator matrix of an $[n, k]$ GRS code takes the form

$$G = [\mathbf{u}_0 \ \mathbf{u}_1 \cdots \mathbf{u}_{n-1}], \tag{1}$$

where

$$\mathbf{u}_i = v_i(1 \ \alpha_i \cdots \alpha_i^{k-1})', \quad 0 \le i \le n-1.$$

In addition, the generator matrix of a GRS code can also contain a column of the form $(0\ 0 \cdots 0\ v)'$, $v \neq 0$. Such a column is said to correspond to the infinity "element". In geometric terms, a GRS code corresponds to a *normal rational curve* [13][14].

A matrix of the form $G = [I\ A]$ generates a GRS code if and only if $A = [a_{ij}]$ is a *Cauchy* matrix [11], i.e.,

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

where the x_i are distinct elements of F, the y_j are distinct elements of F, $x_i + y_j \neq 0$ for all i and j, and $c_i, d_j \neq 0$. In analogy with the infinity-column in a GRS standard generator matrix, a Cauchy matrix can contain either an infinity-row of the form $c \cdot (d_0\ d_1 \cdots d_{n-k-1})$, or an infinity column of the form $d \cdot (c_0\ c_1 \cdots c_{k-1})'$. This extension of the definition of Cauchy matrices preserves super-regularity.

Note that, by definition, a GRS code with $2 \le k \le q-1$ may be of length $q+1$ at most. For $2 \le k \le q-1$, let $N_{\min}(k, q)$ be the minimal integer, if any, such that every $[n, k]$ MDS code over F with $n \ge N_{\min}(k, q)$ is GRS; if no such integer exists, $N_{\min}(k, q) \triangleq q+2$. Clearly, $N_{\min}(2, q) = 2$, and so $N_{\max}(2, q) = q+1$. To obtain an upper-bound on $N_{\min}(k, q)$ for larger values of k we make use of the following result:

Theorem 1. (Segre [13]). *If q is odd, every $[n, 3]$ MDS code over $GF(q)$ with $q - \frac{1}{4}(\sqrt{q} - 7) < n \le q+1$ is GRS.*

Note that there exist $[q+1, 3]$ MDS codes over $GF(q)$, q even, which are not GRS.

II. BOUNDS ON THE LENGTHS OF MDS CODES

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

Proof. Let C be an $[r+k, k]$ GRS code with a given standard generator matrix G of the form (1). First, we show that C has another standard generator matrix $\bar{G}$ with $\mathbf{u}_0$ corresponding to infinity and $\mathbf{u}_1$ corresponding to zero. Assume that the first column of G corresponds to some element $\alpha_0 \in F$. By [10, p. 305, Problem 7], there exists a $k \times k$ nonsingular matrix T such that the i-th column in $\hat{G} = T \cdot G$ is given by

$$\hat{\mathbf{u}}_i = v_i(1 \ (\alpha_i - \alpha_0) \cdots (\alpha_i - \alpha_0)^{k-1})' ,$$

except for the infinity column of G, if any, remaining unchanged. Thus, the first column of $\hat{G}$ corresponds to the zero element. Reversing the order of the rows of $\hat{G}$, we obtain a standard generator matrix $\tilde{G}$ with its first column corresponding to infinity. As before, there exists now a linear transformation on the rows of $\tilde{G}$ yielding a standard generator matrix $\bar{G}$ with the desired first two columns.

Second, let $[I \ A]$ be the (unique) systematic generator matrix of C. Then A is a Cauchy matrix and its rows, being in a one-to-one correspondence with the first k coordinates of C, can be associated with the first k columns of any standard generator matrix of C. In particular, associating the rows of A with the first k columns of $\bar{G}$ yields $a_{0j} = c_0 d_j$ and $a_{1j} = c_1 d_j y_j^{-1}$. Now, normalizing the parameters involved, we can always set $c_0 = c_1 = 1$. □

Lemma 2. *For* $3 \le k \le q-2$,

$$N_{\min}(k+1, q) \ \le \ N_{\min}(k, q) + 1 .$$

Proof. The theorem holds trivially if $N_{\min}(k, q) \ge q+1$. Therefore we assume $N_{\min}(k, q) \le q$. Let $G = [I \ A]$ be a $(k+1) \times n$ systematic generator matrix of an MDS code with $N_{\min}(k, q) + 1 \le n \le N_{\max}(k+1, q)$ and let $\mathbf{a}_i = (a_{i0} \ a_{i1} \cdots a_{i,n-k-2})$ denote the i-th row of A, $0 \le i \le k$. For $2 \le m \le k$, let $G_m = [I \ A_m]$ be the $k \times (n-1)$ matrix obtained by deleting the m-th row and the m-th column from G. Clearly, each G_m generates an $[n-1, k]$ MDS code and, since $n-1 \ge N_{\min}(k, q)$, each such code is GRS. Therefore, each A_m is a Cauchy matrix. By Lemma 1, $a_{0j} = d_j$ and $a_{1j} = d_j y_j^{-1}$, and so the same d_j and y_j are shared by all the matrices A_m. Moreover, since each $\mathbf{a}_i$, $2 \le i \le k$, belongs to each A_m with $m \ne i$, we have $a_{ij} = c_i d_j (x_i + y_j)^{-1}$ for

some x_i and c_i, implying that A is a Cauchy matrix. □

The analogue of Lemma 2 for $N_{\max}(k, q)$ takes the form $N_{\max}(k+1, q) \le N_{\max}(k, q) + 1$, $k \ge 2$. This follows from the fact that any $k \times ((n-1)-k)$ sub-matrix of a $(k+1) \times (n-(k+1))$ super-regular matrix is itself super-regular.

Lemma 3. *Let $F = GF(q)$ and suppose that for some k, $2 \le k \le q-2$, there exists an integer N, $k+3 \le N \le q+1$, such that every $[N, k]$ MDS code over F is GRS. Then,*

(i) $N_{\min}(k, q) \le N$;

(ii) $N_{\max}(k, q) = q+1$.

Proof. (i) Let $G = [I \ A]$ generate an $[n, k]$ MDS code with $n \ge N$. By assumption, every $k \times (N-k)$ sub-matrix of A must be a Cauchy matrix. Applying the proof of Lemma 2 to the columns of A, we conclude that A is a Cauchy matrix.

(ii) The proof of this part follows immediately from part (i). □

Theorem 2. *For odd q and $3 \le k \le q-1$,*

$$N_{\min}(k, q) \ \le \ q - \lceil \tfrac{1}{4}(\sqrt{q}+1) \rceil + k \, ,$$

where $\lceil a \rceil$ stands for the least integer not smaller than a.

Proof. It is easy to verify that Theorem 1 and Lemma 3 imply

$$N_{\min}(3, q) \ \le \ q - \lceil \tfrac{1}{4}(\sqrt{q}+1) \rceil + 3 \, . \tag{2}$$

From Lemma 2, by induction on k, we obtain

$$N_{\min}(k, q) \ \le \ N_{\min}(3, q) + k - 3 \, . \tag{3}$$

The theorem now follows from (2) and (3). □

The above result was obtained by Thas in [14] via geometric arguments.

Lemma 4. *Suppose* $N_{\min}(k, q) \le q + 1$ *for some* k, $3 \le k \le q - 2$. *Then,*

$$N_{\max}(k+1, q) = q + 1 .$$

Proof. Assume that $N_{\max}(k+1, q) \ge q + 2$ and let C be a $[q+2, k+1]$ MDS code generated by $[I \;\; A]$. Since by the conditions of the lemma, every $[q+1, k]$ MDS code over $GF(q)$ is GRS, it follows that every $k \times (q+1-k)$ sub-matrix of A is a Cauchy matrix. As in the proof of Lemma 2, A must be a Cauchy matrix which is impossible since C is of length $q + 2$. □

Theorem 3. *For odd* q *and* $2 \le k < ¼(\sqrt{q} + 13)$,

$$N_{\max}(k, q) = q + 1.$$

Proof. The theorem is known to be valid for $k = 2$ and $k = 3$. Assume now that $k \ge 4$. Then,

$$4 \;\le\; k \;\le\; \lceil ¼(\sqrt{q} + 1) \rceil + 2 \;\le\; q - 1$$

and, by Theorem 2,

$$N_{\min}(k-1, q) \le q - \lceil ¼(\sqrt{q} + 1) \rceil + k - 1 \le q + 1 .$$

The theorem now follows from Lemma 4. □

Theorem 3 slightly improves the Thas bound [14] and, thus, extends the validity range of the MDS Conjecture[1].

Lemma 5. *For* $k \ge 2$,

$$N_{\max}(N_{\max}(k, q) - k, q) \ge N_{\max}(k, q) \ge N_{\max}(N_{\max}(k, q) - k + 1, q) .$$

Proof. Let $k + 1 \le N_0 \le N_{\max}(k, q) \le N_1$. Then there exist MDS codes C_0 and $C_0^{\perp}$ with parameters $[N_0, k]$ and $[N_0, N_0 - k]$, respectively. Hence,

[1] Using a recent improvement of Thas upon Theorem 1 [15], we can slightly extend the range of k stated in Theorem 3 to $k \le ¼(\sqrt{q} + 13¾)$ for odd q. However, for the sake of simplicity we shall still refer to Theorem 3 as is.

$$N_0 \le N_{\max}(N_0 - k, q)\,.$$

Now, suppose $N_1 + 1 \le N_{\max}(N_1 - k + 1, q)$. Then there exist MDS codes C_1 and $C_1^{\perp}$ with parameters $[N_1 + 1,\ N_1 - k + 1]$ and $[N_1 + 1, k]$. This implies the contradiction $N_1 < N_{\max}(k, q)$ and, hence,

$$N_1 \ge N_{\max}(N_1 - k + 1, q)\,.$$

The lemma is obtained by setting $N_0 = N_1$. □

Lemma 5 implies the following corollary.

Corollary 1. *Theorem 3 holds also for* $q - \frac{1}{4}(\sqrt{q} + 5) < k \le q - 1$.

This restores symmetry in the validity region of the MDS Conjecture.

In analogy with Lemma 5, we have:

Lemma 6. *For* $3 \le k \le N_{\min}(k, q) - 4$,

$$N_{\min}(N_{\min}(k, q) - k, q) \le N_{\min}(k, q) \le N_{\min}(N_{\min}(k, q) - k - 1, q)\,.$$

Proof. Let $k + 4 \le N_0 \le N_{\min}(k, q) \le N_1$. Suppose $N_0 - 1 \ge N_{\min}(N_0 - k - 1, q)$. Then every MDS code with parameters $[N_0 - 1,\ N_0 - k - 1]$ is GRS. Since the dual of a GRS code is GRS, every MDS code with parameters $[N_0 - 1, k]$ must be GRS as well. By Lemma 3, we obtain the contradiction $N_{\min}(k, q) \le N_0 - 1 < N_0$ and, thus,

$$N_0 \le N_{\min}(N_0 - k - 1, q)\,.$$

Now, since every MDS code with parameters $[N_1, k]$ is GRS, the same must hold for all $[N_1,\ N_1 - k]$ MDS codes. Hence, by Lemma 3,

$$N_1 \ge N_{\min}(N_1 - k, q)\,.$$

The lemma is obtained by setting $N_0 = N_1$. □

In view of Theorem 3, the values of $N_{\max}(k, q)$ for small k are given in Table 1 (see also [6]; the range for $k = 6$ is obtained using the results of [15] instead of Theorem 1).

k	range of q $(q > k)$	$N_{\max}(k, q)$
2	all q	$q+1$
3	odd q	$q+1$
3	even q	$q+2$
4	all q	$q+1$
5	all q	$q+1$
6	$q \le 11$ or odd $q \ge 107$	$q+1$
6	even q or odd $q \le 103$	$\le q+2$

Table 1: $N_{\max}(k, q)$ for some values of k.

III. APPLICATION TO SUPER-REGULAR MATRICES

The results of the previous section on MDS codes can be expressed in terms of super-regular matrices with the sub-class of Cauchy matrices corresponding to GRS codes. For instance, the analogue of Lemma 3 takes the form:

Suppose there exist integers $s \ge 1$, $t \ge 3$ such that every $s \times t$ super-regular matrix over $F = GF(q)$ is a Cauchy matrix. Then, for every $r \ge t$, each $s \times r$ matrix is a super-regular matrix if and only if it is a Cauchy matrix.

The implication of this statement, and its dual, is illustrated in Figure 1 for the case $t = 3$ and $s = N_{\min}(3, q) - 3$.

Let $A = [a_{ij}]$ be a $k \times r$ matrix over F with $a_{ij} \neq 0$ for all $0 \le i \le k-1$ and $0 \le j \le r-1$, and let $A^c = [a_{ij}^{-1}]$; that is, every entry of A^c is the inverse of the corresponding entry of A.

Lemma 7. *Let A be a $k \times r$ matrix over F with nonzero entries. Then, A is a Cauchy matrix if and only if A^c satisfies the following two conditions:*

(i) Every 2×2 sub-matrix of A^c is nonsingular.

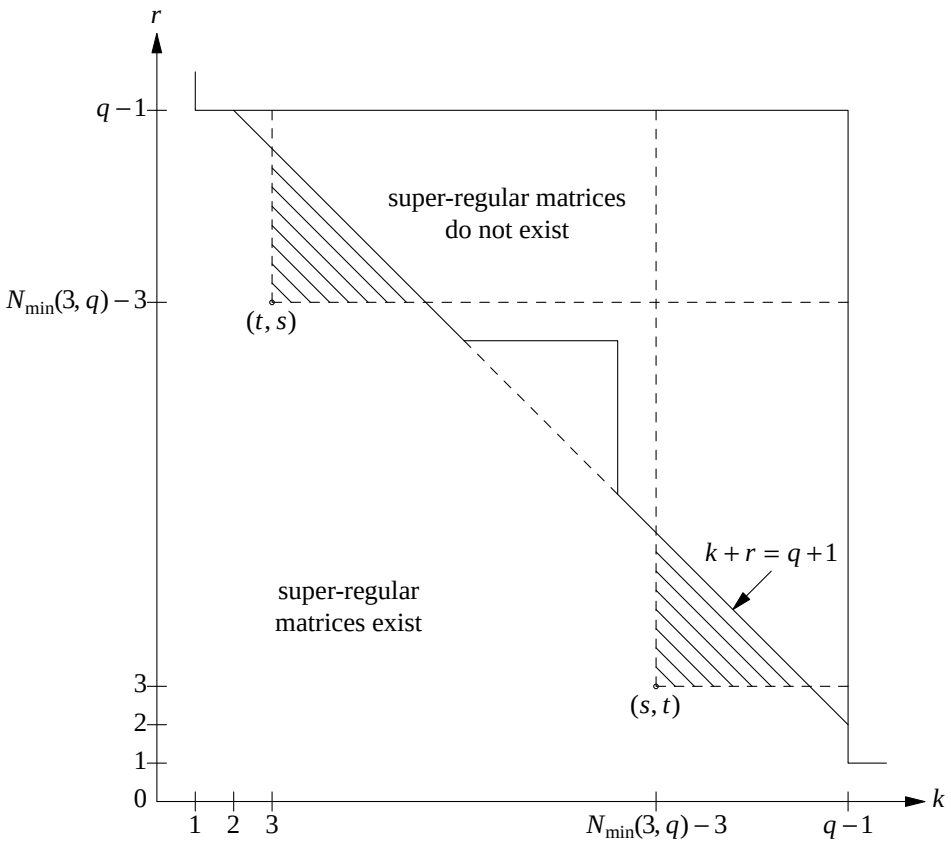

Figure 1: Existence range of $k \times r$ super-regular matrices for odd q.
Every super-regular matrix in the shaded area must be a Cauchy matrix.

(ii) Every 3×3 *sub-matrix of* A^c *is singular.*

Proof. The lemma holds trivially if $\min(k, r) \le 2$. Therefore we assume that $k, r \ge 3$. First, we prove the "only if" part. Suppose A is a Cauchy matrix. Then, the first row of A^c is given by

$$\mathbf{a}_0^c = \left(\frac{1}{d_0} \ \frac{1}{d_1} \cdots \frac{1}{d_{r-1}}\right); \tag{4}$$

the second row of A^c is given by

$$\mathbf{a}_1^c = \left(\frac{y_0}{d_0} \ \frac{y_1}{d_1} \cdots \frac{y_{r-1}}{d_{r-1}}\right); \tag{5}$$

and the i-th row of A^c, $2 \le i \le k-1$, is given by

$$\mathbf{a}_i^c = \left(\frac{x_i + y_0}{c_i d_0} \ \frac{x_i + y_1}{c_i d_1} \cdots \frac{x_i + y_{r-1}}{c_i d_{r-1}}\right).$$

Therefore,

$$\mathbf{a}_i^c = \frac{x_i}{c_i}\,\mathbf{a}_0^c + \frac{1}{c_i}\,\mathbf{a}_1^c\,, \quad 2 \le i \le k-1\,,$$

which means that every row in A^c is a linear combination of its first two rows, thus proving (ii). Condition (i) follows from the fact that a 2×2 sub-matrix of A^c is nonsingular if and only if the corresponding 2×2 sub-matrix of A is nonsingular.

For the "if" part, suppose A^c is a $k \times r$ matrix with nonzero entries satisfying (i) and (ii). Then, the first two rows of A^c are linearly independent and their entries can still be expressed as in (4) and (5), with nonzero d_j and nonzero and distinct y_j. Now, (ii) implies that every row $\mathbf{a}_i^c$, $2 \le i \le k-1$, is linearly dependent on the first two rows of A^c, i.e.,

$$a_{ij}^c = \alpha_i a_{0j}^c + \beta_i a_{1j}^c\,, \quad 2 \le i \le k-1\,, \quad 0 \le j \le r-1\,,$$

for some α_i, $\beta_i \neq 0$. Define $c_i \triangleq \beta_i^{-1}$ and $x_i \triangleq \alpha_i \beta_i^{-1}$, $2 \le i \le k-1$. Since every two rows of A^c are linearly independent, the x_i are distinct. □

Lemma 7 leads to an efficient way of verifying whether a given $k \times n$ matrix generates a GRS code. Let G_1 denote a square matrix of order k and let $G = [G_1\ G_2]$. The first step in the test of G is to verify that G_1 is nonsingular. Then, apply the transformation $G_1^{-1} \cdot G = [I\ A]$ and check that $A = [a_{ij}]$ satisfies the following two conditions: (i) the ratios a_{0j}/a_{1j}, $0 \le j \le n-k-1$, are all distinct; and (ii) the rows of A^c are pairwise independent and are all spanned by the first two rows of A^c. It can be readily verified that these two conditions are equivalent to those of Lemma 7.

Lemma 7, together with Theorem 2, imply the following result.

Theorem 4. *Let $F = GF(q)$, q odd, and let A be a $k \times r$ matrix over F with* $\max(k, r) > q - \frac{1}{4}(\sqrt{q} + 5)$. *If all the entries of A are nonzero, then A is super-regular if and only if every 2×2 sub-matrix of A^c is nonsingular and every 3×3 sub-matrix of A^c is singular.*

IV. DOUBLE-CIRCULANT MDS CODES

A $k \times k$ matrix $A = [a_{ij}]_{0 \le i,j \le k-1}$ over F is called *circulant* if $a_{ij} = a_{0,j-i} \triangleq a_{j-i}$ for all $0 \le i, j \le k-1$, where indices are taken modulo k. The polynomial $a(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}$ is called the *defining polynomial* of A. Under the correspondence $\mathbf{u} \leftrightarrow u(x)$, where $\mathbf{u} = (u_0\ u_1 \cdots u_{k-1}) \in F^k$ and $u(x) = u_0 + u_1 x + \cdots + u_{k-1} x^{k-1}$, it is easy to verify [10, p. 506] that $\mathbf{v} = \mathbf{u}\ A$ if and only if $v(x) = u(x) \cdot a(x) \pmod{x^k - 1}$ where $a(x)$ is the defining polynomial of a circulant matrix A.

A $[2k, k, d]$ linear code over F is called *double-circulant* if it is generated by a matrix $G = [I\ A]$ where A is a circulant matrix [10, p. 497]. Double-circulant codes are discussed extensively in the literature [1][2][7][8][10, Ch. 16, §7]. A sub-class of double-circulant codes approaches the Gilbert-Varshamov bound [9].

As mentioned before, there exist non-GRS $[q+1, 3]$ MDS codes over $GF(q)$ for even q. Moreover, there exists an example, obtained by Casse and Glynn [6], of a non-GRS MDS code over $GF(9)$. This is a $[10, 5, 6]$ double-circulant MDS code generated by $G = [I\ A]$, where the defining polynomial of A corresponds to

$$\mathbf{a} = (\delta^7\ \delta^5\ 1\ 1\ \delta^5),$$

and δ is a root of $x^2 + 2x + 2 = 0$. The interest in double-circulant MDS codes, in particular codes of lengths $q - 1 \le n \le q + 1$, is due, in part, to this example. In this section we apply the results derived in Section III to obtain constructions and bounds for long $[2k, k]$ double-circulant MDS codes, concentrating on the GRS case.

Lemma 8. [10, p. 319]. *An $[n, k, d]$ code C is MDS if and only if any subset of d coordinates serves as the support of a minimum-weight codeword of C.*

Lemma 9. *Every $[2k, k]$ cyclic MDS code over $F = GF(q)$ is equivalent[2] to a $[2k, k]$ dou-*

ble-circulant code.

Proof. Let C be a cyclic $[2k, k]$ MDS code over F. By Lemma 8, C contains a nonzero codeword **c** of the form

$$\mathbf{c} = (1\ c_1\ 0\ c_3\ 0\ c_5 \cdots 0\ c_{2k-1})\,.$$

That is, $c_{2i} = 0$ and $c_{2i+1} \neq 0$ for all $0 \leq i \leq k-1$ except for $c_0 = 1$. Let $c(x)$ be the polynomial corresponding to **c**. Then, under polynomial multiplication modulo $x^{2k} - 1$, $x^m c(x) \in C$ for all m. In particular, the k codewords $x^{2i}c(x)$, $0 \leq i \leq k-1$, form the matrix

$$G = \begin{bmatrix} 1 & c_1 & 0 & c_3 & \cdots & 0 & c_{2k-1} \\ 0 & c_{2k-1} & 1 & c_1 & \cdots & 0 & c_{2k-3} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & c_3 & 0 & c_5 & \cdots & 1 & c_1 \end{bmatrix},$$

which is a permuted generator matrix of a double-circulant code. □

As shown later, the converse of Lemma 9 is not true. Namely, not every double-circulant MDS code is equivalent to a cyclic code.

For code lengths in the range $q-1 \leq n \leq q+1$ there exist MDS cyclic codes with the following parameters:

(1) $n = q-1$ and $1 \leq k \leq n$. The (ordinary) Reed-Solomon codes are such.

(2) $n = q$ and $k \in \{1, q-1, q\}$. When q is not a prime, there exist no cyclic MDS codes of length q for other values of k [16][12].

(3) $n = q+1$ and either k is odd or q is even. There exist no cyclic MDS codes of length $q+1$ if q is odd and k is even, $k \leq q-1$ [10, p. 324][3].

---

[2] Two codes are *equivalent* if one can be obtained from the other by permuting the coordinates or by multiplying each coordinate by a nonzero scalar.

By Lemma 9, there exists a $[q-1, \frac{1}{2}(q-1)]$ double-circulant MDS code over an odd-size field $F = GF(q)$. We present now a construction of such codes. A similar construction using Hankel matrices is given in [11].

For odd q, let α be an element of order $\frac{q-1}{2}$ (that is, α is a square of a primitive element of F) and let b be a nonsquare in F. Consider the $\frac{1}{2}(q-1) \times (q-1)$ matrix $G = [I \ A]$, where $A = [a_{ij}]$ is a circulant matrix given by

$$a_{ij} = \frac{1}{1 - b \cdot \alpha^{j-i}}, \quad 0 \le i, j \le \frac{q-3}{2}.$$

Since α is a square, $b \cdot \alpha^m \neq 1$ for all m and so the a_{ij} are well defined. Also, note that

$$a_{ij} = \frac{\alpha^i}{\alpha^i - b \cdot \alpha^j}, \quad 0 \le i, j \le \frac{q-3}{2},$$

implying that A is a Cauchy matrix with $x_i = c_i = \alpha^i$, $y_j = -b \cdot \alpha^j$, and $d_j = 1$. Therefore, the code generated by G is GRS and, thus, MDS.

This construction can be generalized to produce any $[2k, k]$ double-circulant MDS code with k being a proper divisor of $q-1$.

Theorem 5. *Let C be a $[2k, k]$ double-circulant code over $F = GF(q)$, generated by $[I \ A]$, and let $\sum_{i=0}^{k-1} a_i x^i$ be the defining polynomial of A with $a_i \neq 0$ for all i. Then C is GRS if and only if the sequence $\sigma_j = a_j^{-1}$, $0 \le j \le k-1$, satisfies the following two conditions:*

(a) there exist $\mu, \eta \in F$ such that

$$\sigma_{j+2} + \mu\sigma_{j+1} + \eta\sigma_j = 0, \quad 0 \le j \le k-1,$$

with indices taken modulo k, and

(b) the quotients $\frac{\sigma_{j-1}}{\sigma_j}$, $0 \le j \le k-1$, are distinct.

Proof. The "only if" part is a direct corollary of Lemma 7. We can use the latter also to prove the "if" part. Clearly, (a) implies that every row of A^c is a linear combination of its first

two rows, thus yielding Condition (ii) of Lemma 7. To prove that (b) implies Condition (i) of Lemma 7, assume, to the contrary, that A^c contains a singular 2×2 matrix, that is, $\sigma_{r+l} = b \cdot \sigma_r$ and $\sigma_{s+l} = b \cdot \sigma_s$ for some $r < s$, $0 < l < k$, and a nonzero $b \in F$. Now, for any l, there exist $c, d \in F$ such that for all j, $\sigma_{j+l} = c\sigma_j + d\sigma_{j+1}$. Thus, if $d \neq 0$, the two equations obtained by letting $j = r$ and $j = s$ yield

$$\frac{\sigma_{r+1}}{\sigma_r} = \frac{\sigma_{s+1}}{\sigma_s} = \frac{b - c}{d};$$

if $d = 0$ we have for all j,

$$\frac{\sigma_{j+l}}{\sigma_{j+l+1}} = \frac{\sigma_j}{\sigma_{j+1}}.$$

In either case our assumption violates (b). □

Let $P(x) = x^2 + \mu x + \eta$ denote the characteristic polynomial of the sequence $S = \{\sigma_j\}_{j=-\infty}^{\infty}$ of period k of Theorem 5. Our next goal is to investigate the existence of such polynomials.

Case 1. *$P(x)$ is irreducible over F.* Let β be a root of $P(x)$ in $\Phi \triangleq GF(q^2)$. Clearly, the order of β in Φ equals the exponent of $P(x)$, i.e., the period k of S [4, Ch. 3]. It is easy to verify that $S = \{\sigma_j\}_{j=-\infty}^{\infty}$ satisfies Condition (a) of Theorem 5 if and only if there exists $\gamma \in \Phi$ such that, for all j,

$$\beta\sigma_j - \eta\sigma_{j-1} = \gamma \cdot \beta^j. \tag{6}$$

Thus, for any two integers r and s we have,

$$\beta^{r-s} = \frac{\beta\sigma_r - \sigma_{r-1}}{\beta\sigma_s - \sigma_{s-1}} = \frac{\sigma_r}{\sigma_s} \cdot \frac{\beta - \sigma_{r-1}/\sigma_r}{\beta - \sigma_{s-1}/\sigma_s}.$$

Hence, for S to obey Condition (b), we must have $\beta^j \in F$ if and only if $j \equiv 0 \pmod{k}$. The period k must therefore satisfy the following three conditions: (1) $(k, q-1) = 1$; (2) k divides $(q+1)(q-1)$, i.e., $k \mid q+1$; and (3) $k \leq \frac{q+1}{2}$. Therefore, in case $P(x)$ is irreducible over F, we obtain the following upper bounds on k:

$$\begin{array}{llll} \text{(7a)} & q = 2^{2m+1} \quad : \quad k \le \dfrac{q+1}{3}\,; & \text{(7c)} & q \equiv 1 \pmod 4 \quad : \quad k \le \dfrac{q+1}{2}\,; \\ \text{(7b)} & q = 2^{2m} \quad : \quad k \le \dfrac{q+1}{5}\,; & \text{(7d)} & q \equiv 3 \pmod 4 \quad : \quad k \le \dfrac{q+1}{4}\,. \end{array} \tag{7}$$

Bound (7c) is attainable with equality and, as we have indicated before, there exists even a cyclic MDS code of dimension $\dfrac{q+1}{2}$ and length $q+1$. For this value of k we have $\eta = \beta \cdot \beta^q = \beta^{q+1} = 1$ and $\mu = -(\beta + \beta^q) \triangleq -\mathrm{Tr}(\beta)$. Now, since $\beta^{½(q^2-1)} = 1$, β is a square in Φ. Setting γ to any nonsquare in Φ we have $\gamma \cdot \beta^j \notin F$ for all j and, so, the values σ_j obtained by (6) are all nonzero. In particular, we may take $\gamma = \beta - \beta^{-1}$, which can be readily verified to be a nonsquare in Φ if $q \equiv 1 \pmod 4$. Furthermore, for every nonsquare $\gamma' \in \Phi$ there exist $a \in F$ and an integer l such that $\gamma' \cdot \beta^l = a(\beta - \beta^{-1})$. It follows that for each sequence S of period $\dfrac{q+1}{2}$ obtained by this construction there exists a cyclic l-shift with $\sigma_j = \sigma_{-j}$, in which case the resulting circulant matrix A is *symmetric*. Such a shift of S yields a so-called *characteristic (or, natural) phase* of S, given by

$$\sigma_j = a \cdot \mathrm{Tr}(\beta^{-j}), \quad a \in F - \{0\}\,.$$

As an example, consider the $[10, 5, 6]$ code over $GF(9)$, generated by

$$G = [I \; A] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & \delta^7 & \delta^5 & \delta^5 & \delta^7 \\ 0 & 1 & 0 & 0 & 0 & \delta^7 & 1 & \delta^7 & \delta^5 & \delta^5 \\ 0 & 0 & 1 & 0 & 0 & \delta^5 & \delta^7 & 1 & \delta^7 & \delta^5 \\ 0 & 0 & 0 & 1 & 0 & \delta^5 & \delta^5 & \delta^7 & 1 & \delta^7 \\ 0 & 0 & 0 & 0 & 1 & \delta^7 & \delta^5 & \delta^5 & \delta^7 & 1 \end{bmatrix},$$

where δ is a root of $x^2 + 2x + 2 = 0$ and $P(x) = x^2 + \delta x + 1$ (compare with the Casse-Glynn construction). An exhaustive search has shown that for $q \in \{5, 13, 17, 25\}$ there exist no $[q+1, ½(q+1)]$ double-circulant codes over $GF(q)$ with a symmetric matrix A which are both MDS and non-GRS. This makes the Casse-Glynn construction even more interesting.

A similar construction attains bound (7a). In this case β is an element of order $k = \dfrac{q+1}{3}$ and γ may take any value in $\Phi - \{\, a \cdot \beta^j \mid a \in F, 0 \le j \le k-1 \,\}$.

Case 2. *$P(x)$ has two distinct roots in F.* In this case the period k of S must divide $q-1$ and, since $k \le \frac{q+1}{2}$, we obtain the following upper bounds on the dimension k:

$$\begin{array}{lll} \text{(8a)} \quad q = 2^{2m+1} & : & k \le \frac{q-1}{5}\,; \\ \text{(8b)} \quad q = 2^{2m} & : & k \le \frac{q-1}{3}\,; \end{array} \qquad \begin{array}{lll} \text{(8c)} \quad \text{odd } q & : & k \le \frac{q-1}{2}\,. \end{array} \tag{8}$$

Note that bound (8c) is valid also for $q = 3$. Although we have $\frac{q+1}{2} = q-1$ in this case, there exists no double-circulant MDS code of dimension 2 over $GF(3)$.

A construction attaining bound (8c) has already been described in this section, and a similar construction attains bound (8b).

Case 3. $P(x) = (x - \beta)^2$, $\beta \in F$. Here k must divide $p(q-1)$, where p is the characteristic of $GF(q)$. In this case the sequence $S = \{\sigma_j\}_{j=-\infty}^{\infty}$ takes the form

$$\sigma_j = (a + bj)\beta^j\,, \quad a, b \in F$$

and, therefore,

$$\frac{\sigma_{j+1}}{\sigma_j} = \frac{a + b(j+1)}{a + bj}\,\beta = \frac{\sigma_{j+p+1}}{\sigma_{j+p}}\,,$$

implying $k \le p$. Note that if k is strictly smaller than p, then $k \mid q-1$ as in Case 2. When $k = p$, the only instance for which k is larger than possible in Cases 1 and 2 is obtained when $q = 4$: There exists a $[4, 2, 3]$ double-circulant code over $GF(4)$, generated by

$$G = \begin{bmatrix} 1 & 0 & a_0 & a_1 \\ 0 & 1 & a_1 & a_0 \end{bmatrix},$$

where a_0 and a_1 are nonzero and distinct. Note that there is no equivalent cyclic code in this case (see our remark following Lemma 9).

The following list summarizes the maximal attainable values for the dimension of double-circulant GRS codes:

$$q = 2^{2m+1} \quad : \quad k = \frac{q+1}{3}; \qquad q \equiv 1 \pmod 4 \quad : \quad k = \frac{q+1}{2};$$
$$q = 2^{2m},\ m > 1 \quad : \quad k = \frac{q-1}{3}; \qquad q \equiv 3 \pmod 4 \quad : \quad k = \frac{q-1}{2}.$$
$$q = 4 \quad : \quad k = 2;$$

Based on these results, we may suggest some conjectures on the existence of long double-circulant MDS codes which are not necessarily GRS. An exhaustive search has shown that there are no $[q, q/2]$ double-circulant MDS codes over $GF(8)$ and $GF(16)$, suggesting:

Conjecture. *There are no* $[q, q/2]$ *double-circulant MDS codes over* $GF(q)$ *for* $q = 2^h$, $h \geq 3$.

For $q \equiv 3 \pmod 4$ we propose:

Conjecture. *When* $q \equiv 3 \pmod 4$, *there exist no* $[q+1, \frac{1}{2}(q+1)]$ *double-circulant MDS codes over* $GF(q)$.

REFERENCES

[1] V.K. Bhargava, S.E. Tavares, S.G.S. Shiva, "Difference sets of the Hadamard type and quasi-cyclic codes", *Information and Control*, vol. 26, 1974, pp. 341-350.

[2] C.L. Chen, W.W. Peterson, E.J. Weldon, Jr., "Some results on quasi-cyclic codes", *Information and Control*, vol. 15, 1969, pp. 407-423.

[3] J. Georgiades, "Cyclic $(q+1, k)$-codes of odd order q and even dimension k are not optimal", *Atti. Sem. Fis. Univ. Modena*, XXX, 1982, pp. 284-285.

[4] S.W. Golomb, *Shift Register Sequences.* Revised edition, Aegean Park Press, Laguna Hills, 1982.

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

[6] — , "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.

[7] C.W. Hoffner, II, S.M. Reddy, "Circulant bases for cyclic codes", *IEEE Transactions on Information Theory,* July 1970, pp. 511-512.

[8] M. Karlin, "New binary coding results by circulants", *IEEE Transactions on Information Theory,* vol. IT-15, 1969, pp. 81-92.

[9] T. Kasami, "A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2", *IEEE Transactions on Information Theory,* vol. IT-20, 1974, p. 679.

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

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

[12] — , "On cyclic MDS codes of length q over $GF(q)$", *IEEE Transactions on Information Theory,* vol. IT-32, 1986, pp. 284-285.

[13] B. Segre, "Curve razionali normali e k-archi negli spazi finiti", *Ann. Mat. Pura Appl.* 39, 1955, p. 357.

[14] J.A. Thas, "Normal rational curves and k-arcs in Galois spaces", *Rendiconti di Matematica,* 1, 1968, pp. 331-334.

[15] — , "Complete graphs and algebraic curves in $PG(2, q)$, preprint, Seminar of Geometry and Combinatorics, State Univ. of Ghent, Belgium, Dec. 1984.

[16] E. Zehender, "A non-existence theorem for cyclic MDS-codes", *Atti. Sem. Mat. Fis. Univ. Modena,* XXXII, 1983, pp. 203-205.