ON MDS CODES VIA CAUCHY MATRICES

by

Ron M. Roth and Abraham Lempel

Technical Report #490
January 1988
ON MDS CODES VIA CAUCHY MATRICES

RON M. ROTH AND ABRAHAM LEMPEL

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

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, \(N_{\text{max}}(k,q)\) 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

\[
G = [u_0 \ u_1 \ \cdots \ u_{n-1}],
\]

where

\[
u_i = v_i(1 \ \alpha_i \ \cdots \ \alpha_i^{k-1})', \quad 0 \leq i \leq n-1.
\]

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.,

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

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 \( \mathbf{d} \cdot (c_0 c_1 \cdots c_{k-1})' \). This extension of the definition of Cauchy matrices preserves super-regularity.

Note that, by definition, a GRS code with \( 2 \leq k \leq q - 1 \) may be of length \( q + 1 \) at most. For \( 2 \leq k \leq q - 1 \), let \( N_{\text{min}}(k,q) \) be the minimal integer, if any, such that every \( [n,k] \) MDS code over \( F \) with \( n \geq N_{\text{min}}(k,q) \) is GRS; if no such integer exists, \( N_{\text{min}}(k,q) \triangleq q + 2 \). Clearly, \( N_{\text{min}}(2,q) = 2 \), and so \( N_{\text{max}}(2,q) = q + 1 \). To obtain an upper-bound on \( N_{\text{min}}(k,q) \) 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 \( q - \frac{1}{4}(\sqrt{q} - 7) < n \leq q + 1 \) 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 \( a_{1j} = d_jy_j^{-1} \), \( 0 \leq j \leq r-1 \).

**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 \( \overline{G} \) with \( u_0 \) corresponding to infinity and \( u_1 \) 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 \( \tilde{G} = T \cdot G \) is given by

\[
\tilde{u}_i = v_i (1 - \alpha_i - \alpha_0) \cdots (\alpha_i - \alpha_0)^{k-1} y_i,
\]

except for the infinity column of \( G \), if any, remaining unchanged. Thus, the first column of \( \tilde{G} \) corresponds to the zero element. Reversing the order of the rows of \( \tilde{G} \), 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 \( 3 \leq k \leq q - 2 \),

\[
N_{\min}(k+1, q) \leq N_{\min}(k, q) + 1.
\]

**Proof.** The theorem holds trivially if \( N_{\min}(k, q) \geq q + 1 \). Therefore we assume \( N_{\min}(k, q) \leq q \). Let \( G = [I \ A] \) be a \((k+1) \times n\) systematic generator matrix of an MDS code with \( N_{\min}(k, q) + 1 \leq n \leq N_{\max}(k+1, q) \) and let \( a_i = (a_{i0} \ a_{i1} \cdots \ a_{in-k-2}) \) denote the \( i \)-th row of \( A \), \( 0 \leq i \leq k \). For \( 2 \leq m \leq k \), 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 \( n-1 \geq N_{\min}(k, q) \), 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 \( a_i \), \( 2 \leq i \leq k \), belongs to each \( A_m \) with \( m \neq i \), 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 \( N_{\max}(k+1, q) \leq N_{\max}(k, q) + 1 \), \( k \geq 2 \). This follows from the fact that any \( k \times ((n-1)-k) \) sub-matrix of a \((k+1) \times (n-(k+1))\)
Lemma 3. Let $F = GF(q)$ and suppose that for some $k$, $2 \leq k \leq q - 2$, there exists an integer $N$, $k + 3 \leq N \leq q + 1$, such that every $[N,k]$ MDS code over $F$ is GRS. Then,

(i) $N_{\min}(k,q) \leq N$;
(ii) $N_{\max}(k,q) = q + 1$.

Proof. (i) Let $G = [I \ A]$ generate an $[n,k]$ MDS code with $n \geq N$. 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 $3 \leq k \leq q - 1$,

$$N_{\min}(k,q) \leq q - \left \lfloor \frac{1}{4}(\sqrt{q} + 1) \right \rfloor + k,$$

where $\left \lfloor a \right \rfloor$ stands for the least integer not smaller than $a$.

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

$$N_{\min}(3,q) \leq q - \left \lfloor \frac{1}{4}(\sqrt{q} + 1) \right \rfloor + 3. \quad (2)$$

From Lemma 2, by induction on $k$, we obtain

$$N_{\min}(k,q) \leq N_{\min}(3,q) + k - 3. \quad (3)$$

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

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

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

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

Proof. Assume that $N_{\max}(k+1,q) \geq q + 2$ 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 \( 2 \leq k < \frac{1}{4}(\sqrt{q} + 13) \),

\[
N_{\text{max}}(k,q) = q + 1.
\]

**Proof.** The theorem is known to be valid for \( k = 2 \) and \( k = 3 \). Assume now that \( k \geq 4 \). Then,

\[
4 \leq k \leq \left\lceil \frac{1}{4}(\sqrt{q} + 1) \right\rceil + 2 \leq q - 1
\]

and, by Theorem 2,

\[
N_{\text{min}}(k-1,q) \leq q - \left\lceil \frac{1}{4}(\sqrt{q} + 1) \right\rceil + k - 1 \leq q + 1.
\]

The theorem now follows from Lemma 4. \( \Box \)

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

**Lemma 5.** For \( k \geq 2 \),

\[
N_{\text{max}}(N_{\text{max}}(k,q) - k, q) \geq N_{\text{max}}(k,q) \geq N_{\text{max}}(N_{\text{max}}(k,q) - k + 1, q).
\]

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

\[
N_0 \leq N_{\text{max}}(N_0 - k, q).
\]

Now, suppose \( N_1 + 1 \leq N_{\text{max}}(N_1 - k + 1, q) \). 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 \( N_1 < N_{\text{max}}(k,q) \) and, hence,

\[
N_1 \geq N_{\text{max}}(N_1 - k + 1, q).
\]

The lemma is obtained by setting \( N_0 = N_1 \). \( \Box \)

Lemma 5 implies the following corollary.

---

\(^1\) Recently, Thas has improved the range of \( k \) for which the MDS Conjecture holds to \( k < \frac{1}{4}(\sqrt{q} + 934) \) when \( q \) is odd.
Corollary 1. Theorem 3 holds also for \( q - \sqrt[4]{q} + 5 < k \leq q - 1 \).

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

In analogy with Lemma 5, we have:

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

\[ N_{\min}(N_{\min}(k,q) - k,q) \leq N_{\min}(k,q) \leq N_{\min}(N_{\min}(k,q) - k - 1,q) . \]

**Proof.** Let \( k + 4 \leq N_0 \leq N_{\min}(k,q) \leq N_1 \). Suppose \( N_0 - 1 \geq N_{\min}(N_0 - k - 1,q) \). 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 \( N_{\min}(k,q) \leq N_0 - 1 < N_0 \) and, thus,

\[ N_0 \leq N_{\min}(N_0 - k - 1,q) . \]

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,

\[ N_1 \geq N_{\min}(N_1 - k,q) . \]

The lemma is obtained by setting \( N_0 = N_1 \). \( \square \)

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 a former version of Theorem 1 [6, §1(8)] which appears to be better for small \( q \)).

**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 \( s \geq 1, i \geq 3 \) such that every \( s \times t \) super-regular matrix over \( F = GF(q) \) is a Cauchy matrix. Then, for every \( r \geq t \), 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 \( s = N_{\text{min}}(3,q) - 3 \).

Let \( A = [a_{ij}] \) be a \( k \times r \) matrix over \( F \) with \( a_{ij} \neq 0 \) for all \( 0 \leq i \leq k-1 \) and \( 0 \leq j \leq r-1 \), 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 non-zero entries. Then, \( A \) is a Cauchy matrix if and only if \( A^c \) satisfies the following two conditions:

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

(ii) Every \( 3 \times 3 \) sub-matrix of \( A^c \) is singular.

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

\[
a_0^c = \left( \frac{1}{d_0}, \frac{1}{d_1}, \ldots, \frac{1}{d_{r-1}} \right);
\]

the second row of \( A^c \) is given by

\[
a_1^c = \left( \frac{y_0}{d_0}, \frac{y_1}{d_1}, \ldots, \frac{y_{r-1}}{d_{r-1}} \right);
\]

<table>
<thead>
<tr>
<th>( k )</th>
<th>range of ( q ) ((q \geq k))</th>
<th>( N_{\text{max}}(k,q) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>all ( q )</td>
<td>( q + 1 )</td>
</tr>
<tr>
<td>3</td>
<td>odd ( q )</td>
<td>( q + 1 )</td>
</tr>
<tr>
<td>3</td>
<td>even ( q )</td>
<td>( q + 2 )</td>
</tr>
<tr>
<td>4</td>
<td>all ( q )</td>
<td>( q + 1 )</td>
</tr>
<tr>
<td>5</td>
<td>all ( q )</td>
<td>( q + 1 )</td>
</tr>
<tr>
<td>6</td>
<td>( q \leq 11 ) or odd ( q \geq 113 )</td>
<td>( q + 1 )</td>
</tr>
<tr>
<td>6</td>
<td>even ( q ) or odd ( q \leq 109 )</td>
<td>( \leq q + 2 )</td>
</tr>
</tbody>
</table>

Table 1: \( N_{\text{max}}(k,q) \) for some values of \( k \).
and the $i$-th row of $A^c$, $2 \leq i \leq k-1$, is given by

$$a_i^c = \left( \frac{x_i + y_0}{c_i d_0}, \frac{x_i + y_1}{c_i d_1}, \ldots, \frac{x_i + y_{r-1}}{c_i d_{r-1}} \right).$$

Therefore,

$$a_i^c = \frac{x_i}{c_i} a_0^c + \frac{1}{c_i} a_1^c, \quad 2 \leq i \leq k-1,$$

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 $2 \times 2$ sub-matrix of $A^c$ is nonsingular if and only if the corresponding $2 \times 2$ 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 $a_i^c$,
2 \leq i \leq k-1, is linearly dependent on the first two rows of \( A^c \), i.e.,
\[
a^c_{ij} = \alpha_i a^c_{0j} + \beta_i a^c_{1j}, \quad 0 \leq j \leq r-1, \quad 2 \leq i \leq k-1,
\]
for some \( \alpha_i, \beta_i \neq 0 \). Define \( c_i \triangleq \beta_i^{-1} \) and \( x_i \triangleq \alpha_i \beta_i^{-1}, \quad 2 \leq i \leq k-1 \). Since every two rows of \( A^c \) are linearly independent, the \( x_i \) are distinct. \( \square \)

This lemma, 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 \( 2 \times 2 \) sub-matrix of \( A^c \) is nonsingular and every \( 3 \times 3 \) sub-matrix of \( A^c \) is singular.

**IV. DOUBLE-CIRCULANT MDS CODES**

A \( k \times k \) matrix \( A = [a_{ij}]_{0 \leq i,j \leq k-1} \) over \( F \) is called circulant if \( a_{ij} = a_{0,j-i} \triangleq a_{j-i} \) for all \( 0 \leq i,j \leq k-1 \), 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 \( u \leftrightarrow u(x) \), where \( u = (u_0 u_1 \cdots u_{k-1}) \in F^k \) and \( u(x) = u_0 + u_1 x + \cdots + u_{k-1} x^{k-1} \), it is easy to verify [10, p. 506] that \( v = u A \) if and only if \( v(x) = u(x) \cdot a(x) \mod x^k - 1 \) where \( a(x) \) is the defining polynomial of a circulant matrix \( A \). It follows that the set of \( k \times k \) circulant matrices and the ring of polynomials modulo \( x^k - 1 \) over \( F \) are isomorphic. In particular, a circulant matrix \( A \) is invertible if and only if its defining polynomial is relatively prime to \( x^k - 1 \).

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 meets 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
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.

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 \([2k,k]\) double-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

\[
c = (1 \ 0 \ c_3 \ 0 \ c_5 \ \cdots \ 0 \ c_{2k-1})
\]

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

\[
G = \begin{bmatrix}
1 & c_1 & 0 & c_3 & \cdots & 0 & c_{2k-1} \\
0 & c_{2k-1} & 1 & c_1 & \cdots & 0 & c_{2k-3} \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & c_3 & 0 & c_5 & \cdots & 1 & c_1
\end{bmatrix}
\]

which is a permuted generator matrix of a double-circulant code. \(\square\)

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

---

\(^2\) 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.
For the lengths of interest it is known that 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 \( k \) \[15\][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 \[10, p. 324\][3].

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 \( \alpha \) be an element of order \( \frac{q-1}{2} \) (that is, \( \alpha \) 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

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

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

\[
a_{ij} = \frac{\alpha^i}{\alpha^j - b \cdot \alpha^m}, \quad 0 \leq i, j \leq \frac{q-3}{2},
\]

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 \( \sigma_j = a_j^{-1} \), \( 0 \leq j \leq k-1 \), satisfies the following two conditions:
(a) there exist $\mu, \eta \in F$ such that
\[ \sigma_{j+2} + \mu \sigma_{j+1} + \eta \sigma_j = 0, \quad 0 \leq j \leq k-1, \]
with indices taken modulo $k$, and
(b) the quotients $\frac{\sigma_{j-1}}{\sigma_j}, 0 \leq j \leq k-1$, 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 $2 \times 2$ 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). $\square$

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.

Consider the case of $q = 2^h$ and $k = \frac{q}{2}$. If $P(x)$ is irreducible over $F$, then it is easy to show that the exponent of $P(x)$, which equals the period $k$ of $S$, must divide $q^2 - 1$ [4, Ch. 3]. This can happen only if $q = 2$ and $k = 1$, corresponding to the [2,1,2] repetition code over $GF(2)$.

Assume now that $P(x)$ is reducible over $F$. If the roots of $P(x)$ are distinct, then $k | q - 1$ and, again, we must have $k = 1$; if $P(x)$ has a double root in $F$, then $k | 2(q - 1)$ and the value
$k = 2$ is also admissible, corresponding to 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). This settles the problem of existence of double-circulant GRS codes of length $q$ when $q$ is even. Regarding the more general class of MDS codes, 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 $q = 2^h$, $h \geq 3$.

Finally, we consider the case of odd $q$ and $k = \frac{q}{2}(q+1)$. First, let $q \equiv 3 \pmod{4}$. Here $k$ is even and, thus, there exist no $[q+1,\frac{1}{2}(q+1)]$ cyclic MDS codes in this case. We show that there exist no GRS double-circulant codes as well. If $P(x)$ is irreducible over $F$ and $\beta$ is a root of $P(x)$ in $\Phi \cong GF(q^2)$, $\beta$ must have order $\frac{q+1}{2}$ and $\beta^{\frac{q}{2}(q+1)} = -1$. It is easy to verify that $S = \{\sigma_j\}_{j=-\infty}^{\infty}$ is a sequence satisfying Condition (a) of Theorem 5 if and only if there exists $\gamma \in \Phi$ such that, for all $j$,

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

Hence, $\beta \sigma_0 - \eta \sigma_{-1} = \gamma$ and $\beta \sigma_{\frac{1}{2}(q+1)} - \eta \sigma_{\frac{1}{2}(q-3)} = -\gamma$, implying that $\sigma_{\frac{1}{2}(q+1)} = -\sigma_0$ and $\sigma_{\frac{1}{2}(q-3)} = -\sigma_{-1}$, thus violating Condition (b) of Theorem 5. If $P(x)$ has two distinct roots in $F$, then $\frac{1}{2}(q+1)|q-1$, implying $q = 3$, and there exist no corresponding double-circulant MDS codes. The same holds if $P(x)$ has a double root in $F$, in which case $\frac{1}{2}(q+1)|p(q-1)$, where $p$ is the characteristic of $GF(q)$. Hence, there exist no $[q+1,\frac{1}{2}(q+1)]$ double-circulant GRS codes over $GF(q)$ when $q \equiv 3 \pmod{4}$, and we propose

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

Technion - Computer Science Department - Technical Report CS0490 - 1988
The case \( q \equiv 1 \pmod{4} \) is more promising since now there exist cyclic \([q+1, \frac{1}{2}(q+1)]\) MDS codes. The following is a construction of a double-circulant GRS code for this case. Let \( \beta \in \Phi \) be an element of order \( k = \frac{q+1}{2} \). Define \( P(x) \) by setting \( \eta = \beta \cdot \beta^q = \beta^{q+1} = 1 \) and \( \mu = -(\beta + \beta^q) \neq -\text{Tr}(\beta) \). Clearly, \( P(x) \) is the minimal polynomial of \( \beta \). Since
\[
\beta^{\frac{q}{2}(q^2-1)} = \left[ \beta^{\frac{q}{2}(q+1)} \right]^{q-1} = 1,
\]
\( \beta \) is a square in \( \Phi \). Also, since \( (\frac{1}{2}(q+1), q-1) = 1 \),
\[
\beta^i \in GF(q) \text{ if and only if } i \equiv 0 \pmod{\frac{q+1}{2}}.
\] (7)
It follows that \( \{\beta^i\}_{i=0}^{k-1} \) is a subgroup of the multiplicative group of squares of \( \Phi \) with cosets
\[
H_a = \{a \cdot \beta^i\}_{i=0}^{k-1}, \ a \in GF(q) - \{0\}.
\] (8)

Let \( S = \{\sigma_j\}_{j=-\infty}^{\infty} \) be a sequence over \( F \) defined by (6), where \( \gamma \) is a nonsquare in \( \Phi - \{0\} \). Suppose \( S \) contains a zero component. Then there exists an index \( j \) such that (6) reduces to \( \beta \sigma_j = \gamma \cdot \beta^j \), or \( \gamma = \beta^{1-j} \sigma_j \). This is a contradiction, since both \( \sigma_j \) and \( \beta^{1-j} \) are squares in \( \Phi \).

Thus, all the \( \sigma_j \) are nonzero. Also, the ratios \( \frac{\sigma_{j-1}}{\sigma_j} \), \( 0 \leq j \leq k-1 \), are distinct; for if \( \sigma_{r-1}\sigma_r^{-1} = \sigma_{s-1}\sigma_s^{-1}, \ 0 \leq s < r \leq k-1 \), then from \( \beta \sigma_r - \sigma_{r-1} = \gamma \cdot \beta^r \) and \( \beta \sigma_s - \sigma_{s-1} = \gamma \cdot \beta^s \) we have
\[
\beta^{r-s} = \frac{\beta \sigma_r - \sigma_{r-1}}{\beta \sigma_s - \sigma_{s-1}} = \frac{\sigma_r}{\sigma_s} \in F,
\]
which, by (7), implies \( r \equiv s \pmod{\frac{q+1}{2}} \), namely, the contradiction \( r = s \).

It can be verified that for each sequence \( S \) obtained by the above construction there exists a cyclic 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
\[
\sigma_j = a \cdot \text{Tr}(\beta^{-j}) , \ a \in F.
\]

The construction described above can be generalized to every odd \( k \) which is a proper divisor of \( q+1 \), including the case of \( q \equiv 3 \pmod{4} \) and the case of even \( q \). In either case \( \beta \) is an ele-
ment of order $k$ in $\Phi$ and $\gamma$ is an element of $\Phi - \{0\}$ not contained in any of the cosets $H_a$ given in (8).

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

$$G = [I \ A] = \begin{bmatrix} 1 & 0 & 0 & 0 & \delta & \delta^6 & 1 & 1 & \delta^6 \\ 0 & 1 & 0 & 0 & \delta^6 & \delta & \delta^6 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & \delta^6 & \delta & \delta^6 & 1 \\ 0 & 0 & 0 & 1 & \delta^6 & 1 & 1 & \delta^6 & \delta & \delta \end{bmatrix} \tag{9}$$

where $\delta$ is a root of $x^2 + 2x + 2 = 0$ and $P(x) = x^2 + \delta^3x + 1$. This code is GRS, and it is interesting to observe that in the Casse-Glynn construction the elements of the first row of their $A$ form a permutation of those in (9) in such a way that their reciprocals do not satisfy a second-order linear recurrence. An exhaustive search has shown that for $q \in \{5,13,17,25\}$ there exist no $[q+1,\frac{q(q+1)}{2}]$ double-circulant codes over $GF(q)$ with a symmetric matrix $A$ which are both MDS and non-GRS. This makes the above example of $q = 9$ even more interesting.

REFERENCES


