On Generator Matrices of MDS Codes

Ron M. Roth[*]

and Gadiel Seroussi[**]

ABSTRACT

It is shown that the family of q-ary generalized Reed-Solomon codes is identical to the family of q-ary linear codes generated by matrices of the form $[\, I \mid A \,]$, where I is the identity matrix, and A is a generalized Cauchy matrix. Using Cauchy matrices, a construction is shown of maximal triangular arrays over GF(q), which are constant along diagonals in a Hankel matrix fashion, and with the property that every square sub-array is nonsingular. This solves an open problem posed by Singleton in [2]. By taking rectangular sub-arrays of the described triangles, it is possible to construct generator matrices $[\, I \mid A \,]$ of MDS codes, where A is a Hankel matrix. The parameters of the codes are (n, k, d), for $1 \leq n \leq q+1$, $1 \leq k \leq n$, and $d = n - k + 1$.

* Department of Electrical Engineering, Technion, Israel Institute of Technology, Haifa 32000 - Israel.
** Department of Computer Science, Technion, Israel Institute of Technology, Haifa 32000 - Israel.

I. Introduction

An (n,k,d) linear code over a finite field $F=GF(q^n)$ is *maximum distance separable* (in short, MDS) if $d=n-k+1$. MDS codes are optimal in the sense that they achieve the maximum possible minimum distance for given length and dimension. A comprehensive treatment of MDS codes, their properties, and open questions about them can be found in [1, ch. 11]. MDS codes can be characterized in terms of their systematic generator matrices as follows: let C be an (n,k,d) code with a systematic generator matrix $G=[\ I \mid A\ ]$, where I is the identity matrix of order k, and A is a $k\times(n-k)$ matrix. Then C is MDS if and only if every square submatrix of A is nonsingular [1, ch. 11, Theorem 8].

One systematic way of building matrices with the property that every square submatrix is nonsingular is the *Cauchy matrix* construction. An $r\times s$ matrix $A=(a_{ij})$ is called a Cauchy matrix if $a_{ij}=1/(x_i+y_j)$ for some elements $x_1,x_2,\cdots,x_r,y_1,y_2,\cdots,y_s$ in F. If $r=s$ then the determinant of A is given [1, p. 323] by

$$det(A)=\frac{\prod_{1\le i<j\le r}(x_j-x_i)(y_j-y_i)}{\prod_{1\le i,j\le r}(x_i+y_j)}.$$

Hence, provided that the x_i are distinct, the y_i are distinct, and $x_i+y_j\neq 0$ for all i,j, it follows that any square submatrix of a Cauchy matrix is nonsingular.

A is called an *extended Cauchy matrix* if it has a row (column) of ones, and deleting this row (column) transforms A into a Cauchy matrix $\hat{A}$. It can be readily verified that the determinant of an $r\times r$ extended Cauchy matrix A with a row of ones is given by

$$det(A)=(-1)^{n-s}\frac{\prod_{1\le i<j\le r-1}(x_j-x_i)\prod_{1\le i<j\le r}(y_j-y_i)}{\prod_{\substack{1\le i\le r-1\\ 1\le j\le r}}(x_i+y_j)},$$

where s is the index of the row of ones in A. Here $x_1,x_2,\cdots,x_{r-1},y_1,y_2,\cdots,y_r$ are the elements of F that define the Cauchy matrix $\hat{A}$. A similar expression, involving

r x_i's and $r-1$ y_j's, gives the determinant for the case where A has a column of ones. It follows that every square submatrix of an extended Cauchy matrix A is nonsingular if and only if every square submatrix of the underlying Cauchy matrix $\hat{A}$ is nonsingular.

For any vector $\mathbf{z}=(z_1, z_2, \cdots, z_t)$, we shall denote by $D(\mathbf{z})$ the diagonal matrix of order t with $D_{ii}=z_i$. An $r\times s$ matrix A is a *generalized (extended) Cauchy matrix*, in short, GC (GEC), if it has the form $A=D(\mathbf{c})\bar{A}D(\mathbf{d})$, where $\bar{A}$ is an $r\times s$ (extended) Cauchy matrix, and $\mathbf{c}=(c_1, c_2, \cdots, c_r)$ and $\mathbf{d}=(d_1, d_2, \cdots, d_s)$ are vectors of nonzero elements of F. Clearly, if all square submatrices of $\bar{A}$ are nonsingular, so are all square submatrices of A. Therefore, we can construct a systematic generator matrix for an (n,k) MDS code by concatenating the identity matrix I of order k with a suitably defined $k\times(n-k)$ GC (GEC) matrix A.

Let $\boldsymbol{\alpha}=(\alpha_1, \alpha_2, \cdots, \alpha_n)$ be a vector of distinct elements of F, and let $\mathbf{v}=(v_1, v_2, \cdots, v_n)$ be a vector of nonzero (not necessarily distinct) elements of F. C is a *generalized Reed-Solomon* (in short, GRS) *code*, denoted by $GRS(n,k,\boldsymbol{\alpha},\mathbf{v})$, if it has a generator matrix of the form

$$G=[G_1\ G_2\ \cdots\ G_n],$$

where the G_i-s are columns of the form

$$G_i=(v_i, v_i\alpha_i, v_i\alpha_i^2, \cdots, v_i\alpha_i^{k-1})^T \quad , \quad 1\le i\le n.$$

This definition includes extended GRS codes, for which one of the α_i-s is 0. A further extension which preserves the MDS property is possible by allowing a column of G of the form

$$G_\infty=(0,0,\cdots,0,v_\infty)^T,$$

where v_∞ is a nonzero element of F. In this case, the code is called a *generalized doubly extended RS code*, (in short, GDRS) and we shall keep the notation $GDRS(n+1,k,\boldsymbol{\alpha},\mathbf{v})$ in terms of the vectors $\boldsymbol{\alpha}$ and $\mathbf{v}$ by abusing notation and writing

---

[1] For any matrix M, M^T denotes the transpose of M.

$$\alpha=(\alpha_1, \alpha_2, \cdots, \alpha_{s-1}, \infty, \alpha_s, \cdots, \alpha_n),$$

and

$$\mathbf{v}=(v_1, v_2, \cdots, v_{s-1}, v_\infty, v_s, \cdots, v_n),$$

where s is the index of G_∞ in G. Reed-Solomon codes and their variants have been extensively studied, and are well known to be MDS (see for instance [1, chs. 10-11]).

In this paper we show that every GRS (GDRS) code has a systematic generator matrix of the form $[I|A]$, where A is a GC (GEC) matrix, and conversely, every systematic generator matrix of that form generates a GRS (GDRS) code. Hence, these two well-known systematic ways of constructing MDS codes yield exactly the same family of codes. The correspondence between GRS codes and GC matrices is presented in Section II, while the correspondence between GDRS codes and GEC matrices is presented in Section III. Note that the above correspondences do not cover triply-extended RS codes [1, p. 328], which exist for even values of q with $k=3$ or $k=q-1$.

In Section IV we use Cauchy matrices to show the construction over any $F=GF(q)$ of arrays S_q of the form

$$S_q: \quad \begin{array}{ccccccccc} 1 & 1 & 1 & 1 & . & . & 1 & 1 & 1 \\ 1 & a_1 & a_2 & a_3 & . & . & a_{q-3} & a_{q-2} & \\ 1 & a_2 & a_3 & . & . & . & a_{q-2} & & \\ 1 & a_3 & . & . & . & . & & & \\ . & . & . & . & . & . & & & \\ . & . & . & . & . & . & & & \\ 1 & a_{q-3} & a_{q-2} & & & & & & \\ 1 & a_{q-2} & & & & & & & \\ 1 & & & & & & & & \end{array}$$

with $a_i \in F$, $1 \le i \le q-2$, such that any square submatrix of S_q is nonsingular. Examples of these arrays were first presented by Singleton in [2] for $q=5$ and $q=7$, but no generalization was given for larger fields (see also [1, p. 322]). We show that the constructed arrays are maximal in the sense that, when q is odd, no field element can be appended to any of the rows (except, obviously, to the first row) without

creating singular submatrices. The same is true when q is even, except for one element that can be appended to each of the third and $q-1$-st rows. This corresponds to the triply-extended RS codes mentioned above.

Using a slightly more complicated variation of the construction of S_q, we also show the construction of arrays of the form

$$T_q: \quad \begin{matrix} b_0 & b_1 & b_2 & \cdots & b_{q-2} & b_{q-1} \\ b_1 & b_2 & \cdot & \cdots & b_{q-1} & \\ b_2 & \cdot & \cdot & \cdots & & \\ \cdot & \cdot & \cdot & \cdot & & \\ \cdot & \cdot & b_{q-1} & & & \\ b_{q-2} & b_{q-1} & & & & \\ b_{q-1} & & & & & \end{matrix}$$

which, as S_q, have the property that every square submatrix is nonsingular. Notice that T_q has a "pure" Hankel form (i.e.: $(T_q)_{ij}=(T_q)_{i-1,j+1}$, $1\le i\le q-1$, $0\le j\le q-i-1$), whereas S_q has a row and a column of ones that depart from the Hankel form. Taking suitable rectangular sub-arrays of either S_q or T_q, it is possible to construct generator matrices $[\, I \mid A \,]$ of MDS codes, where A is a Hankel matrix. Since A is, by construction, a generalized (extended) Cauchy matrix, the results of Sections II and III imply that we obtain generalized (doubly-extended) Reed Solomon codes.

II. Correspondence between GRS codes and GC matrices.

Theorem 1: Let C be a $GRS(n,k,\boldsymbol{\alpha},\mathbf{v})$ code defined by $\boldsymbol{\alpha}=(\alpha_1, \alpha_2, \cdots, \alpha_n)$ and $\mathbf{v}=(v_1, v_2, \cdots, v_n)$. Then C has a systematic generator matrix of the form $[\, I \mid A \,]$, where A is a $k\times(n-k)$ GC matrix such that $A_{ij}=c_i d_j/(x_i+y_j)$, with

$$x_i = -\alpha_i \ , \ 1\le i\le k, \tag{1}$$

$$y_j = \alpha_{j+k} \ , \ 1\le j\le n-k, \tag{2}$$

$$c_i = \frac{v_i^{-1}}{\prod\limits_{\substack{1\le l\le k \\ l\ne i}} (\alpha_i-\alpha_l)} \ , \ 1\le i\le k, \tag{3}$$

and

$$d_j = v_{j+k} \prod_{1\le i\le k} (\alpha_{j+k}-\alpha_i) \ , \ 1\le j\le n-k. \tag{4}$$

Conversely, if A is a $k\times(n-k)$ GC matrix defined by vectors $\mathbf{x}=(x_i)_{i=1}^{k}$, $\mathbf{y}=(y_j)_{j=1}^{n-k}$, $\mathbf{c}=(c_i)_{i=1}^{k}$, and $\mathbf{d}=(d_j)_{j=1}^{n-k}$, such that every square submatrix of A is nonsingular, then $[\ I \mid A\ ]$ generates a $GRS(n,k,\boldsymbol{\alpha},\mathbf{v})$ code with

$$\alpha_i = -x_i \ , \ 1\le i\le k, \tag{5}$$

$$\alpha_j = y_{j-k} \ , \ k+1\le j\le n, \tag{6}$$

$$v_i = \frac{c_i^{-1}}{\prod\limits_{\substack{1\le t\le k\\ t\ne i}} (x_t-x_i)} \ , \ 1\le i\le k, \tag{7}$$

$$v_j = \frac{d_j}{\prod\limits_{1\le t\le k} (x_t+y_{j-k})} \ , \ k+1\le j\le n. \tag{8}$$

Proof: Let $C=GRS(n,k,\boldsymbol{\alpha},\mathbf{v})$. Then one generator matrix of C is $G=\bar{G}D(\mathbf{v})$ where $\bar{G}_{ij}=\alpha_j^{i-1}, 1\le i\le k, \ 1\le j\le n$. Write $\bar{G}=[\ P \mid Q\ ]$, where P is the $k\times k$ Vandermonde matrix with $P_{ij}=\alpha_j^{i-1}, \ 1\le i,j\le k$, and Q is a $k\times(n-k)$ matrix with $Q_{ij}=\alpha_{j+k}^{i-1}, \ 1\le i\le k, \ 1\le j\le n-k$. The systematic generator matrix for C is $[\ I \mid A\ ]$, where

$$A = D(\mathbf{u})^{-1}P^{-1}QD(\mathbf{w}), \tag{9}$$

with $\mathbf{u}=(v_1,v_2,\cdots,v_k)$, and $\mathbf{w}=(v_{k+1},v_{k+2},\cdots,v_n)$. Consider the polynomial

$$f_i(z) = \prod_{\substack{1\le t\le k\\ t\ne i}} (z-\alpha_t) = \sum_{0\le r\le k-1} f_{ir} z^r. \tag{10}$$

The inverse of the Vandermonde matrix P is given [3, p. 36] by

$$(P^{-1})_{ij} = \frac{f_{i,j-1}}{\prod\limits_{\substack{1\le t\le k\\ t\ne i}} (\alpha_i-\alpha_t)} \ , \ 1\le i,j\le k. \tag{11}$$

Hence, it follows from equations (9) and (11) that

$$A_{ij} = v_i^{-1}\left[\sum_{r=1}^{k} (P^{-1})_{ir} Q_{rj}\right] v_{j+k}$$

$$= v_i^{-1} \frac{\sum_{r=1}^{k} f_{i,r-1} \alpha_{j+k}^{r-1}}{\prod_{\substack{1 \le t \le k \\ t \ne i}} (\alpha_i - \alpha_t)} v_{j+k}$$

$$= v_i^{-1} v_{j+k} \frac{f_i(\alpha_{j+k})}{\prod_{\substack{1 \le t \le k \\ t \ne i}} (\alpha_i - \alpha_t)}$$

$$= v_i^{-1} v_{j+k} \frac{\prod_{\substack{1 \le t \le k \\ t \ne i}} (\alpha_{j+k} - \alpha_t)}{\prod_{\substack{1 \le t \le k \\ t \ne i}} (\alpha_i - \alpha_t)}, \quad 1 \le i \le k, \ 1 \le j \le n-k. \tag{12}$$

Therefore, with **x**,**v**,**c**, and **d** as defined by equations (1)-(4), we have

$$A_{ij} = \frac{c_i d_j}{x_i + y_j}, \quad 1 \le i \le k, \ 1 \le j \le n-k, \tag{13}$$

as claimed.

Conversely, given a GC matrix A defined by the vectors **x**,**y**,**c**, and **d**, and provided that every square submatrix of A is nonsingular, we can solve equations (1)-(4) for the vectors $\boldsymbol{\alpha}$ and **v** which define a GRS code with generator matrix $[\, I \mid A \,]$. The solution is given in equations (5)-(8).

Q.E.D.

III. Correspondence between GDRS codes and GEC matrices.

Theorem 2: (i) Let C be a $GDRS(n+1,k,\boldsymbol{\alpha},\mathbf{v})$ code defined by $\boldsymbol{\alpha}=(\alpha_1, \alpha_2, \cdots, \alpha_{s-1}, \infty, \alpha_s, \cdots, \alpha_n)$, and $\mathbf{v}=(v_1, v_2, \cdots, v_{s-1}, v_\infty, v_s, \cdots, v_n)$, with $k<s\le n+1$. Then C has a generator matrix of the form $[\, I \mid \bar{A} \,]$, where $\bar{A}=[A_1, A_2, \cdots, A_{s-k-1}, A_\infty, A_{s-k}, \cdots, A_{n-k}]$ is a $k \times (n+1-k)$ GEC matrix obtained from the *GC* matrix A of Theorem 1 by inserting the column $A_\infty = d_\infty (c_1, c_2, \cdots, c_k)^T$ before the $(s-k)$-th column of A if $s<n+1$, or as the last column if $s=n+1$. Here $d_\infty = v_\infty$, and the c_i-s are as defined in (3).

(ii) Let C be a $GDRS(n+1,k+1,\boldsymbol{\alpha},\mathbf{v})$ code defined by $\boldsymbol{\alpha}$ and **v** as in (i), but with $1 \le s \le k+1$ (note also that the dimension here is $k+1$, as compared with k in (i)).

Then C has a generator matrix of the form $[\, I \mid \bar{A}\,]$, where

$$\bar{A} = \begin{bmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \vdots \\ \mathbf{a}_{s-1} \\ \mathbf{a}_\infty \\ \mathbf{a}_s \\ \vdots \\ \mathbf{a}_k \end{bmatrix}$$

is a $(k+1)\times(n-k)$ GEC matrix obtained from the GC matrix A of Theorem 1 by inserting the row $\mathbf{a}_\infty = c_\infty\,(d_1, d_2, \cdots, d_{n-k})$ before the s-th row of A if $s \le k+1$, or as the last row if $s = k+1$. Here $c_\infty = v_\infty^{-1}$, and the d_j-s are as defined in (4).

(iii) Conversely, given a GEC matrix $\bar{A}$ such that every square submatrix of $\bar{A}$ is nonsingular, there exist vectors $\boldsymbol{\alpha}$ and $\mathbf{v}$ that define a GDRS code C generated by $[\, I \mid \bar{A}\,]$.

Proof: The proof follows along the same lines as in Theorem 1, except that here we have to account for the additional column $G_\infty = (0,0,\ldots,0,v_\infty)^T$ in the generator matrix of C. We shall use the matrices A, P, Q, and the vectors $\mathbf{u}$, $\mathbf{w}$ as defined in Theorem 1 and its proof.

Part (i): Here G_∞ appears among the columns of G corresponding to the check digits, and therefore it corresponds to a column

$$A_\infty = D(\mathbf{u})^{-1}P^{-1}G_\infty = D(\mathbf{u})^{-1}(P^{-1})_k v_\infty$$

in the systematic generator matrix of C, where $(P^{-1})_k$ denotes the k-th column of P^{-1}. Using (11), we obtain

$$A_{i,\infty} = v_i^{-1}(P^{-1})_{ik}v_\infty = \frac{v_i^{-1}f_{i,k-1}}{\prod\limits_{\substack{1\le t\le k \\ t\ne i}}(\alpha_i-\alpha_t)}v_\infty, \quad 1\le i\le k.$$

Now, from (10) we have $f_{i,k-1}=1$ and, by the definitions of c_i and d_∞, we obtain $A_\infty = d_\infty\,(c_1, c_2, \cdots, c_k)^T$, as claimed.

Part (ii): Here $1\le s\le k+1$ and, hence, G_∞ is in the part of G corresponding to the

information digits. We shall assume, for the sake of clarity, that $s=k+1$, the other cases being similar. Write $G=[\ \overline{P}\ |\ \overline{Q}\ ]D(\mathbf{v})$, where

$$\overline{P} = \begin{bmatrix} & & 0 \\ & P & \vdots \\ & & 0 \\ \alpha_1^k\ \alpha_2^k & \cdots\ \alpha_k^k & 1 \end{bmatrix},$$

and

$$\overline{Q} = \begin{bmatrix} & Q & \\ \alpha_{k+1}^k\ \alpha_{k+2}^k & \cdots & \alpha_n^k \end{bmatrix}.$$

Define

$$g(z) = \prod_{i=1}^{k}(z-\alpha_i) = \sum_{r=0}^{k} g_r z^r.$$

It can be readily verified that the inverse of $\overline{P}$ is given by

$$\overline{P}^{-1} = \begin{bmatrix} & & 0 \\ & P^{-1} & \vdots \\ & & 0 \\ g_0\ g_1 & \cdots\ g_{k-1} & g_k \end{bmatrix}.$$

Let $[\ I\ |\ \overline{A}\ ]$ be the systematic generator matrix of C. Then

$$\overline{A} = D([\ \mathbf{u}\ |\ v_\infty\ ])^{-1}\overline{P}^{-1}\overline{Q}D(\mathbf{w}).$$

It follows that the first k rows of $\overline{A}$ are identical to those of A, and the $k+1$-st row of $\overline{A}$ is given by

$$\mathbf{a}_\infty = v_\infty^{-1}(g_0, g_1, \cdots, g_{k-1})\overline{QD}(\mathbf{w}) .$$

The entries of $\mathbf{a}_\infty$ are given by

$$\mathbf{a}_{\infty j} = v_\infty^{-1}\left[\sum_{r=1}^{k+1} g_{r-1}\overline{Q}_{rj}\right]v_{j+k} = v_\infty^{-1}\left[\sum_{r=1}^{k+1} g_{r-1}\alpha_{j+k}^{r-1}\right]v_{j+k}$$

$$= v_\infty^{-1}v_{j+k}g(\alpha_{j+k}) = v_\infty^{-1}v_{j+k}\prod_{1\le i\le k}(\alpha_{j+k}-\alpha_i) \ , \ 1\le j\le n-k.$$

Recalling the definition of d_j in (8), and that c_∞ is defined as $c_\infty=v_\infty^{-1}$, we obtain $\mathbf{a}_\infty=c_\infty(d_1, d_2, \cdots, d_{n-k})$, as claimed.

Part (iii): Given a GEC matrix $\overline{A}$ such that every square submatrix of $\overline{A}$ is nonsingular, we use (5)-(8) to obtain the vectors $\boldsymbol{\alpha}$ and $\mathbf{v}$ of the corresponding GDRS code, without the "infinity" entries. The index of ∞ in $\boldsymbol{\alpha}$, and of v_∞ in $\mathbf{v}$, is determined by whether the extended Cauchy matrix that underlies $\overline{A}$ has a row or a column of ones, and by the index of that row or column. The value of v_∞ is equal to the value c_∞ (or d_∞) that multiplies the row (or column) of ones in $\overline{A}$.

Q.E.D.

IV. Triangular arrays whose submatrices are nonsingular.

Theorem 3: Let $F=GF(q)$, and let S_q denote the triangular array

$$S_q: \begin{array}{ccccccccc} 1 & 1 & 1 & 1 & . & . & 1 & 1 & 1 \\ 1 & a_1 & a_2 & a_3 & . & . & a_{q-3} & a_{q-2} & \\ 1 & a_2 & a_3 & . & . & . & a_{q-2} & & \\ 1 & a_3 & . & . & . & . & & & \\ . & . & . & . & . & . & & & \\ . & . & . & . & . & . & & & \\ 1 & a_{q-3} & a_{q-2} & & & & & & \\ 1 & a_{q-2} & & & & & & & \\ 1 & & & & & & & & \end{array}$$

where

$$a_i = \frac{1}{1-\gamma^i} \ , \ 1\le i\le q-2,$$

for an arbitrary primitive element γ of F. Then, every square submatrix of S_q is

nonsingular.

Proof: Let S_q^* denote the array obtained from S_q by deleting its first and last rows, and let s_{ij}, $1 \le i \le q-2$, $0 \le j \le q-i-1$, denote the entries of S_q^*. By the definition of S_q, we have

$$s_{i0} = 1 \ , \ 1 \le i \le q-2,$$

and

$$s_{ij} = a_{i+j-1} = \frac{1}{1-\gamma^{i+j-1}}, \ 1 \le i \le q-2, \ 1 \le j \le q-1-i.$$

Note that with i and j in the above ranges, we always have $1 \le i+j-1 \le q-2$ and, hence, $\gamma^{i+j-1} \ne 1$ for γ primitive in F. Consider the vectors $\mathbf{x}=(x_1, x_2, \cdots, x_{q-2})$ and $\mathbf{y}=(y_0, y_1, \cdots, y_{q-2})$ defined by

$$x_i = -\gamma^{-(i-1)} \ , \ 1 \le i \le q-2,$$

$$y_0 = 0,$$

and

$$y_j = \gamma^j \ , \ 1 \le j \le q-2.$$

It can be readily verified that

$$s_{ij} = \frac{x_i}{x_i + y_j}, \ 1 \le i \le q-2, \ 0 \le j \le q-i-1.$$

Since all the x_i-s are distinct and nonzero, all the y_j-s are distinct, and $x_i + y_j \ne 0$ for i and j in the defined ranges, we conclude that every square submatrix of S_q^* is a nonsingular GC matrix. Now, every square submatrix of S_q is either a square submatrix of S_q^*, or a rectangular submatrix of S_q^* with an appended first row of 1's. The latter square submatrices of S_q are GEC matrices which are also nonsingular.

Q.E.D.

For $q=5$ and $q=7$, taking $\gamma=3$, which is a primitive element in both $GF(5)$ and $GF(7)$, we obtain

$$S_5:\ \begin{matrix} 1\,1\,1\,1\,1 \\ 1\,2\,3\,4 \\ 1\,3\,4 \\ 1\,4 \\ 1 \end{matrix} \quad ; \quad S_7:\ \begin{matrix} 1\,1\,1\,1\,1\,1\,1 \\ 1\,3\,6\,4\,2\,5 \\ 1\,6\,4\,2\,5 \\ 1\,4\,2\,5 \\ 1\,2\,5 \\ 1\,5 \\ 1 \end{matrix} \quad .$$

These particular examples can be found in [2] and [1, p. 322], and are presented here as applications of Theorem 3.

Notice that, by construction, every rectangular submatrix A of S_q is either a GC or a GEC matrix. Hence, by Theorems 1 and 2, the MDS code generated by $[\, I \mid A \,]$ is either a GRS or a GDRS code.

We proceed now to prove that the array S_q of Theorem 3 is, in general, maximal. First, we need the following lemma.

Lemma 1: (i) Let F be a field of characteristic other than two, and let a,b, and c be distinct elements of $F-\{1\}$ such that $c \neq 0$ and

$$\frac{1}{1-a} + \frac{1}{1-b} = \frac{2}{1-c}. \tag{14}$$

Then, the matrix

$$M = \begin{bmatrix} 1 & 1 & 1 \\ \dfrac{1}{1-a/c} & \dfrac{1}{1-b/c} & \dfrac{1}{1-1/c} \\ \dfrac{1}{1-a} & \dfrac{1}{1-b} & \dfrac{1}{1-c} \end{bmatrix}$$

is singular over F.

(ii) Let F be a field of characteristic two, and let a and b be elements of $F-\{0,1\}$ such that $ab \neq 1$. Then, the matrix

$$N = \begin{bmatrix} 1 & 1 & 1 \\ \dfrac{1}{1+ab} & \dfrac{1}{1+a^2} & \dfrac{1}{1+a} \\ \dfrac{1}{1+b} & \dfrac{1}{1+a} & \dfrac{1}{1+1/b} \end{bmatrix}$$

is singular over F.

Proof: Part (i): Solving for c in (14), it is easy to establish after some elementary algebraic manipulations that (14) implies

$$\frac{1}{1-a/c}+\frac{1}{1-b/c}=\frac{2}{1-1/c}. \tag{15}$$

Let $\mathbf{w}=(1,1,-2)^T$. We claim that $M\mathbf{w}=0$. The claim is trivial for the first row of M, and it follows from (15) and (14), respectively, for the second and third rows.

Part (ii): Let $\mathbf{u}=(1+ab,(1+a)(1+b),a+b)$. Then, again after some elementary algebraic manipulations (modulo 2), it is easy to verify that $N\mathbf{u}=0$.

Q.E.D.

Theorem 4: Let S_q be as defined in Theorem 3, and let $S_q(0),S_q(1),\cdots,S_q(q-1)$ denote the rows of S_q. If q is odd, then appending any element of F to any $S_q(k)$, $1\le k\le q-1$, creates a singular square submatrix. If q is even, then the above statement is true except for $k=2$ and $k=q-2$, in which case a unique element, equal to a_1, can be appended to $S_q(k)$ without creating singular square submatrices. This corresponds to the triply extended $(q+2,3,q)$ and $(q+2,q-1,4)$ MDS codes [1, p. 326].

(Trivially, for any q, any nonzero element of F can be added to the all-ones row $S_q(0)$ without creating any singular submatrix).

Proof: Let v be an arbitrary element of F, and assume that v is appended to $S_q(k)$, $1\le k\le q-1$. If $v=0$, then a trivial 1×1 singular matrix is formed. Hence, we assume $v\neq 0$. Moreover, due to the symmetry between rows and columns in S_q, we can assume without loss of generality that $k\le(q-1)/2$ in the case where q is odd, and $k\le q/2$ when q is even. Let $K=\{1\}\cup\{a_i\mid k\le i\le q-2\}$. Note that K contains all the entries of $S_q(k)$. If $v\in K$ then a singular submatrix of the form $\begin{bmatrix}1 & 1\\ v & v\end{bmatrix}$ is formed. Hence, it remains to consider values of v such that $v\notin K$. Since 1 and $a_1,\cdots,a_{q-2}$ exhaust all the nonzero elements of F, this implies that $v=a_r$ for some r, $1\le r<k$. We consider first the case when q is odd. Consider all unordered

pairs $\{b_1, b_2\}$ of distinct elements of F such that $b_1+b_2=2v=2a_r$. Since the cardinality of K is $q-k \geq (q+1)/2$, at least one such pair can be found among elements of K. This pair is either of the form $\{1,a_j\}$, $k \leq j \leq q-2$, or of the form $\{a_i,a_j\}$, $k \leq i < j \leq q-2$. In the first case, using $1+a_j = 2v = 2a_r$, we can apply Lemma 1(i) with $a=0$, $b=\gamma^j$, and $c=\gamma^r$, to verify that the 3×3 submatrix

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & a_{j-r} & a_{q-1-r} \\ 1 & a_j & v \end{bmatrix}$$

is singular. (Recall that $a_i = 1/(1-\gamma^i)$, $1 \leq i \leq q-2$). In the second case, using $a_i+a_j = 2v = 2a_r$, we apply Lemma 1(i) with $a=\gamma^i$, $b=\gamma^j$, and $c=\gamma^r$, to verify that the following submatrix is singular:

$$\begin{bmatrix} 1 & 1 & 1 \\ a_{i-r} & a_{j-r} & a_{q-1-r} \\ a_i & a_j & v \end{bmatrix} .$$

We consider now the case when q is even. When $k=1$, K exhausts all the nonzero elements of F. Hence, no element can be appended to $S_q(1)$ without creating a singular submatrix. When $k=2$, the only element left outside K is a_1, and indeed $v=a_1$ can be appended to $S_q(2)$ without creating singular submatrices. (This is easily verified by direct computation of the 2×2 and 3×3 determinants involving v). The $3\times(q-1)$ maximal rectangle containing v, together with a 3×3 identity matrix, form a generator matrix for the $(q+2,3,q)$ triply-extended MDS code. Symmetrically, when $v=a_1$ is appended to $S_q(q-2)$, we obtain the $(q+2,q-1,4)$ triply-extended MDS code.

Assume now that $3 \leq k \leq q/2$, and let $v=a_r$, for some $1 \leq r < k$. Let s be such that $1 \leq s < k$, and $s \neq r$ (such an s exists because $k>2$). Then, using Lemma 1(ii) with $a=\gamma^{-s}$ and $b=\gamma^{-r}$ ($ab \neq 1$ because $2 \leq r+s \leq q-2$), we obtain that the following is a singular submatrix:

$$\begin{bmatrix} 1 & 1 & 1 \\ a_{q-1-r-s} & a_{q-1-2s} & a_{q-1-s} \\ a_{q-1-r} & a_{q-1-s} & v \end{bmatrix}.$$

Q.E.D.

The row and column of ones in S_q depart from the Hankel form of the rest of the array. We now show a construction of triangular arrays T_q of the same dimensions as S_q, where this departure is avoided, while preserving the property that every square submatrix is nonsingular. Let β be an element of $\Phi=GF(q^2)$ such that β^{q+1} is the smallest positive power of β that falls into $F=GF(q)$,[2] and let $P(x)=x^2+\mu x+\eta$ be the minimal polynomial of β over F. Let $\{\sigma_i\}_{i\geq -2}$ be the sequence over F defined by the linear recursion

$$\sigma_i + \mu\sigma_{i-1} + \eta\sigma_{i-2} = 0, \quad i\geq 0,$$

with initial conditions $\sigma_{-2}=-1/\eta$, $\sigma_{-1}=0$. (Clearly, $\eta\neq 0$, $P(x)$ being irreducible).

Lemma 2: $\sigma_i\neq 0$ for $0\leq i\leq q-1$, and $\sigma_q=0$.

Proof: Using the fact that $\beta^2+\mu\beta+\eta=0$, and the definition of the recursive sequence $\{\sigma_i\}$, it is easy to prove by induction on i that

$$\beta\sigma_i - \eta\sigma_{i-1} = \beta^{i+1}, \quad i\geq -1. \tag{16}$$

Let r be the least nonnegative integer such that $\sigma_r=0$. Then, by (16), we have $\beta^{r+1}=-\eta\sigma_{r-1}$, which implies that $\beta^{r+1}\in F$. Since $r\geq 0$, this implies that $r+1\geq q+1$, or $r\geq q$. On the other hand, $\beta^{q+1}\in F$, and therefore $\beta\sigma_q=\beta^{q+1}+\eta\sigma_{q-1}\in F$, which is possible only if $\sigma_q=0$.

Q.E.D.

Lemma 3: For all $j\geq -2$ and $i\geq 0$,

$$\sigma_{i+j} = \sigma_{i-1}\sigma_{j+1} - \eta\sigma_{i-2}\sigma_j$$

---

[2] A necessary and sufficient condition is that $\beta=\lambda^t$ for some primitive element λ of Φ, with $(t,q+1)=1$. Notice that $x^{q+1}\in F$ for every $x\in\Phi$.

Proof: By induction on i, for all $j \geq -2$. For $i=0$, the claim follows from the definitions of σ_{-2} and σ_{-1}. Assume the claim is true for $0 \leq i' \leq i$. Then

$$\begin{aligned}\sigma_{(i+1)+j} &= \sigma_{i+(j+1)} = \sigma_{i-1}\sigma_{j+2} - \eta\sigma_{i-2}\sigma_{j+1} \\ &= \sigma_{i-1}(-\mu\sigma_{j+1} - \eta\sigma_j) - \eta\sigma_{i-2}\sigma_{j+1} = (-\mu\sigma_{i-1} - \eta\sigma_{i-2})\sigma_{j+1} - \eta\sigma_{i-1}\sigma_j \\ &= \sigma_i\sigma_{j+1} - \eta\sigma_{i-1}\sigma_j .\end{aligned}$$

Q.E.D.

Theorem 5: Let T_q denote the triangular array

$$T_q : \begin{array}{ccccccc} b_0 & b_1 & b_2 & \cdots & b_{q-2} & b_{q-1} \\ b_1 & b_2 & \cdot & \cdots & b_{q-1} & \\ b_2 & \cdot & \cdot & \cdots & & \\ \cdot & \cdot & \cdot & & & \\ \cdot & \cdot & b_{q-1} & & & \\ b_{q-2} & b_{q-1} & & & & \\ b_{q-1} & & & & & \end{array}$$

where $b_i = 1/\sigma_i$, $0 \leq i \leq q-1$, with σ_i as defined above. Then every square submatrix of T_q is nonsingular.

Proof: First, notice that Lemma 2 ensures that b_i, $0 \leq i \leq q-1$, is well defined. Define

$$x_i = -\eta\sigma_{i-2}\sigma_{i-1}^{-1}, \quad 1 \leq i \leq q-1,$$

$$y_j = \sigma_{j+1}\sigma_j^{-1}, \quad 0 < j < q-1,$$

$$c_0 = 1,$$

$$c_i = \sigma_{i-1}^{-1}, \quad 1 \leq i \leq q-1,$$

and

$$d_j = \sigma_j^{-1}, \quad 0 \leq j \leq q-1.$$

Let t_{ij}, $0 \leq i \leq q-1$, $0 \leq j \leq q-1-i$, denote the entries of T_q. Then, $t_{ij} = b_{i+j} = \sigma_{i+j}^{-1}$. By Lemma 3, we have

$$t_{ij} = \frac{1}{\sigma_{i-1}\sigma_{j+1} - \eta\sigma_{i-2}\sigma_j}, \quad 0 \leq i \leq q-1, \; 0 \leq j \leq q-1-i.$$

Now, using the definitions of x_i, y_j, c_i, and d_j, and the above expression for t_{ij}, it

can be readily verified that

$$t_{ij} = \frac{c_i d_j}{x_i + y_j},\ 1 \le i \le q-1,\ 0 \le j \le q-1-i,$$

and

$$t_{0j} = c_0 d_j,\ 0 \le j \le q-1.$$

Hence, every square submatrix of T_q is either a GC matrix (if it does not include entries from the first row of T_q), or a GEC matrix (if it includes entries from the first row). To prove that all the square submatrices are nonsingular, it remains to show that all the x_i-s are distinct, and that all the y_i-s are distinct. Assume $x_r = x_s$ for some $1 \le r < s \le q-1$. Then,

$$\sigma_{r-2}\sigma_{r-1}^{-1} = \sigma_{s-2}\sigma_{s-1}^{-1} = \varepsilon,$$

for some $\varepsilon \in F$. Applying Equation (16) with $i = r-1$ and with $i = s-1$, we obtain

$$\beta^r \sigma_{r-1}^{-1} = \beta^s \sigma_{s-1}^{-1} = \beta - \eta\varepsilon.$$

Therefore, $\beta^{s-r} = \sigma_{s-1}\sigma_{r-1}^{-1} \in F$, contradicting the defining property of β. A similar argument is used to prove that the y_j-s are all distinct.

Q.E.D.

We close this section with examples of T_q for $q=5$ and $q=7$. Using the primitive polynomials $P(x)=x^2+x+2$ over $GF(5)$, and $P(x)=x^2+x+3$ over $GF(7)$, we obtain

$$T_5: \begin{matrix} 1&4&4&2&4 \\ &4&4&2&4 \\ &&4&2&4 \\ &&&2&4 \\ &&&&4 \end{matrix} \quad ; \qquad T_7: \begin{matrix} 1&6&3&3&1&3&6 \\ &6&3&3&1&3&6 \\ &&3&3&1&3&6 \\ &&&3&1&3&6 \\ &&&&1&3&6 \\ &&&&&3&6 \\ &&&&&&6 \end{matrix} \quad .$$

REFERENCES

[1] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1983.

[2] R.C. Singleton, "Maximum distance q-nary codes", *IEEE Trans. Inform. Theory*, vol IT-10, pp. 116-118, 1964.

[3] D.E. Knuth, *The Art of Computer Programming*, Vol. 1: *Fundamental Algorithms*, Reading, Mass.: Addison-Wesley, 1969.