On MDS extensions of generalized Reed-Solomon codes

Gadiel Seroussi[*]

and Ron M. Roth[**]

ABSTRACT

An (n, k, d) linear code over $F = GF(q)$ is said to be *maximum distance separable* (MDS) if $d = n - k + 1$. It is shown that an $(n, k, n - k + 1)$ generalized Reed-Solomon code such that $2 \le k \le n - \lfloor (q-1)/2 \rfloor$ ($k \ne 3$ if q is even), can be extended by one digit while preserving the MDS property if and only if the resulting extended code is also a generalized Reed-Solomon code. It follows that a generalized Reed-Solomon code with k in the above range can be *uniquely* extended to a maximal MDS code of length $q+1$, and that generalized Reed-Solomon codes of length $q+1$ and dimension $2 \le k \le \lfloor q/2 \rfloor + 2$ ($k \ne 3$ if q is even), do not have MDS extensions. Hence, in cases where the $(q+1, k)$ MDS code is essentially unique, there do not exist (n, k) MDS codes with $n > q+1$.

---

[*] Department of Computer Science, Technion, Israel Institute of Technology, Haifa 32000 - Israel.

[**] Department of Computer Science, Technion, Israel Institute of Technology, Haifa 32000 - Israel. Part of this work was done while the author was an M.Sc. student at the Department of Electrical Engineering, Technion.

I. Introduction

Let q be a positive power of a prime. An (n, k, d) code C over the finite field $F = GF(q)$ is called *maximum distance separable* (in short, MDS), if $d = n - k + 1$. Since for every linear code we have $d \le n - k + 1$ (the Singleton bound, [9, p. 33]), MDS codes are optimal in the sense that they achieve the maximum possible minimum distance for given length and dimension. MDS codes and their properties are treated in [9, Ch. 11], which also presents the important connection of MDS codes to certain constructions in finite geometries. In particular, it is known that for $k > 1$, the length of MDS codes of dimension k over F is upperbounded by a maximum $m(q, k)$. For $k \ge q$, it is readily verified that $m(q, k) = k + 1$, but finding the exact value of $m(q, k)$ for $2 \le k < q$ is a well known open problem. The widely believed conjecture is that $m(q, k) = q + 1$ in the above range of k, except for the cases $k = 3$ and $k = q - 1$ with q even, in which case $m(q, k) = q + 2$. This conjecture has already been proved for some values of q and k, e.g. for $k = 2$ (trivial), or $3 \le k \le 5$ (Segre [10,11], Casse [1]), or $q \le 11$ (Maneri and Silverman [7,8], Jurick[6]), or $q > (4k - 9)^2$ (Thas [12]). Other important contributions to the determination of $m(q, k)$, and to the characterization of maximal MDS codes (in geometric terms) are the papers of Casse and Glynn [2,3], and Thas [13,14]. Extensive bibliographies can be found in [5] and [9].

Reed-Solomon codes [9, Ch. 10] are probably the best known family of MDS codes. These codes are a special case of a larger family of MDS codes, referred to as *generalized Reed-Solomon codes* (in short, GRS codes) [9, Ch.10, §8]. C is called a GRS code if it has a generator matrix $G = [\ g_{ij}\ ]$ with entries of the form

$$g_{ij} = v_j \alpha_j^{i-1}\ , 1 \le i \le k, 1 \le j \le n.$$

Here, $\alpha_1, \alpha_2, \cdots, \alpha_n$ are distinct elements of F, $v_1, v_2, \cdots, v_n$ are nonzero (not necessarily distinct) elements of F, and we define $0^0 = 1$. The elements $\alpha_1, \alpha_2, \cdots, \alpha_n$ will be referred to as the *column generators* of G (or C), while the elements $v_1, v_2, \cdots, v_n$ will be referred to as the *column multipliers.* G will be called the *canonical generator matrix* of C. Clearly, GRS codes as defined above exist for any length $n \le q$. GRS codes can be extended while preserving the MDS

property by appending to G an extra column of the form $(0,0,\ldots,v)^T$, with $v \neq 0$ [9, Ch.11, §5]. Using an abuse of notation, we shall say that the extra column has column generator ∞, and column multiplier v. The resulting code is called a *generalized doubly-extended Reed Solomon code* (in short, GDRS). The reason for using the adjective "doubly-extended" is the following: basic Reed-Solomon codes are defined having nonzero elements of F as column generators (usually, the generators are successive powers of a field element whose order is the code length, so that the code is cyclic. This is not required for GRS codes). An "extended" code is obtained by using 0 as a column generator, while a "doubly-extended" code is obtained by using the column generator ∞. In this paper, we shall refer to all of the above generalizations of the Reed-Solomon construction as GDRS codes. When necessary, we shall distinguish between *proper* GDRS codes (i.e., those that use ∞ as a column generator) and GRS codes (those that do not). GDRS codes exist for any length $n \leq q+1$.

In this paper we prove that for $2 \leq k \leq \lfloor q/2 \rfloor + 2$ (except for $k = 3$ when q is even), GDRS codes of length $q+1$ cannot be furtherly extended while preserving the MDS property. Our results imply that for $2 \leq k \leq \lfloor q/2 \rfloor + 2$, if there is a unique $(q+1, k)$ MDS code over F, then $m(q,k) = q+1$, and, by a duality argument, also $m(q, q+2-k) = q+1$. Here, uniqueness is defined up to the following equivalence relation: two codes C_1 and C_2 over F are said to be *equivalent* if there exist a permutation π on $\{1,2,\ldots,n\}$ and n nonzero constants $a_1, a_2, \cdots, a_n \in F$ such that

$$C_2 = \{ (a_1 c_{\pi(1)} \;\; a_2 c_{\pi(2)} \;\; \cdots \;\; a_n c_{\pi(n)}) \mid (c_1 c_2 \cdots c_n) \in C_1 \}.$$

Clearly, the construction of a GDRS code of length $q+1$ over F is unique up to this equivalence. For odd q, almost all known MDS codes of length $q+1$ are GDRS. A recent example, due to Casse and Glynn, and presented by Hirschfeld in [4], shows a $(10,5)$ MDS code over $GF(9)$ which is not GDRS. This example disproves the previously believed conjecture that $\forall$ MDS codes of length $q+1$ over $GF(q)$ (odd q) are GDRS.

The result on GDRS codes of length $q+1$ will be obtained as a corollary of a more general statement, presented as Theorem 1 of Section II. We prove that a GDRS code of length n and

dimension k such that $2 \le k \le n - \lfloor (q-1)/2 \rfloor$ can be extended by one digit, while preserving the MDS property, if and only if the resulting code is also GDRS. It follows that an (n, k) GDRS code over $GF(q)$, with $2 \le k \le n - \lfloor (q-1)/2 \rfloor$, can be *uniquely* extended to an MDS code of length $q+1$, which is GDRS, and which cannot be furtherly extended. Theorem 1 and its corollaries are presented in Section II, where we also show that the limitation of the range of k is necessary and tight in some cases. The proof of the theorem is presented in Section III, along with some preliminary lemmas.

The results of this paper are similar in flavor to the results of Thas in [12], once the language gap between our algebraic coding-theoretic approach and his geometric approach is closed. The results of [12] cover a much smaller range of values of k and n for a given odd q, namely, $2 \le k < n - (q - (\sqrt{q}+5)/4)$. In that range, however, the results of [12] are very strong: he proves that *every* MDS code with k in the above range is GDRS, and can be uniquely extended to a maximal GDRS code of length $q+1$. Hence, in fact, the $m(q, k) = q+1$ conjecture is proved for $2 \le k < (\sqrt{q}+9)/4$, with q odd.[1] For the sake of comparison, the results of [12] are presented in Section II, translated to the language of algebraic coding theory.

II. Statement of main results

Let C be an $(n, k, n-k+1)$ GDRS code over $F = GF(q)$. Denote by $\boldsymbol{\alpha}$ the vector of column generators of C, and by $\mathbf{v}$ the vector of column multipliers of C, i.e.

$$\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \cdots, \alpha_n),$$

and

$$\mathbf{v} = (v_1, v_2, \cdots, v_n),$$

where the α_i's, $1 \le i \le n$, are distinct elements of $F \cup \{\infty\}$, and the v_i's are nonzero elements of F. Then, we denote C by $GDRS(n, k, \boldsymbol{\alpha}, \mathbf{v})$. Let k be any positive integer, and let β be an element of F. We denote by $\mathbf{u}^k(\beta)$ the column vector

[1] Using recent results by Thas [15], it is possible to slightly extend the range of k to $2 \le k < \sqrt{q}/4 + 39/16$. The improvement being marginal, we shall still refer to the results of [12], which are more explicit.

$$\mathbf{u}^k(\beta) \quad = (1, \beta, \beta^2, \ldots, \beta^{k-1})^T.$$

This definition is extended to $\beta = \infty$ by defining

$$\mathbf{u}^k(\infty) = (0, 0, \cdots, 1)^T.$$

The canonical generator matrix G of C is

$$G = [\, v_1\mathbf{u}^k(\alpha_1) \quad v_2\mathbf{u}^k(\alpha_2) \quad \cdots \quad v_n\mathbf{u}^k(\alpha_n) \,].$$

The following theorem presents the main result of this paper.

Theorem 1: Let C be a $GDRS(n, k, \boldsymbol{\alpha}, \mathbf{v})$ code over $F = GF(q)$, such that $2 \le k \le n - \lfloor (q-1)/2 \rfloor$, let G be a k-dimensional column vector over F. Then, the extension of C generated by the matrix[2] $[\, G \mid \mathbf{g} \,]$ is MDS if and only if either

(i) $\mathbf{g} = v \cdot \mathbf{u}^k(\beta)$, where $v \in F - \{0\}$, $\beta \in F \bigcup \{\infty\}$, and β is not a column generator of C, or

(ii) q is even, $k = 3$, and $\mathbf{g} = v \cdot (0,1,0)^T$ for some $v \in F - \{0\}$.

It follows from Theorem 1 that the condition $n \ge k + \lfloor (q-1)/2 \rfloor$ is sufficient to ensure that every MDS extension of an (n, k) GDRS code must also be GDRS (except, for $k = 3$ with q even, when another well characterized extension is possible [9, p. 325]). It remains an open problem to determine, in general, whether the above sufficient condition is also a necessary one. However, this can be proved in some cases. For $k = 3$ and $q \ge 7$, with $q \not\equiv 1 (mod\ 4)$, there exist MDS codes of length $\lfloor (q+5)/2 \rfloor$, which are maximal in the sense that they do not have MDS extensions (hence, they are not GDRS), and which are extensions of GDRS codes of length $n = \lfloor (q+3)/2 \rfloor$. Noticing that for this value of n and for $k = 3$ we have $n = k - 1 + \lfloor (q-1)/2 \rfloor$, we conclude that the condition of Theorem 1 is necessary in these cases. The construction of the maximal codes mentioned above is shown in [5, Ch. 9], in the language of finite geometries. In that language, the

[2] $[\, A \mid B \,]$ denotes the concatenation of a matrix A with a matrix (or column vector) B.

columns of the generator matrix of an (n, k) MDS code over $GF(q)$ form an $n-arc$ in the finite projective geometry $PG(k-1, q)$. An n-arc that cannot be extended to an $n+1$-arc is called *complete*. An n-arc of length $n = m(q, k)$ is an *oval*. The columns of the generator matrix of a GDRS code of dimension k over $GF(q)$ are points on a *normal rational curve* in $PG(k-1, q)$ (a *conic* if $k = 3$). Reference [5] is also a good source for a wealth of geometric results on n-arcs, mostly for the case $k = 3$ (*plane* projective geometries).

The main result of Theorem 1 can be expressed in geometric terms as follows.

Theorem 1′: For $k \geq 2$, and $k \neq 3$ if q is even, an n-arc in $PG(k-1, q)$ not contained in a normal rational curve has at most $k-1+\lfloor (q-1)/2 \rfloor$ points in common with a normal rational curve.

For $k = 3$ (q odd), the result of Theorem 1′ is well known ([5, p.215, Corollary 1 of Lemma 9.4.2]).

When $n = q+1$, all the elements of $F \cup \{\infty\}$ are column generators of C. This leads to the following corollaries of Theorem 1:

Corollary 1: Let $C = GDRS(q+1, k, \boldsymbol{\alpha}, \mathbf{v})$ over $F = GF(q)$, with $2 \leq k \leq \lfloor q/2 \rfloor + 2$, and $k \neq 3$ if q is even. Then, no extension of C is MDS.

Proof: Substitute $n = q+1$ in Theorem 1, and note that, since all the elements of $F \cup \{\infty\}$ are column generators of the code, condition (i) of the theorem cannot be satisfied, while condition (ii) does not apply.

Q.E.D.

Corollary 2: Let $C = GDRS(n, k, \boldsymbol{\alpha}, \mathbf{v})$ over $F = GF(q)$, with $2 \leq k \leq n - \lfloor (q-1)/2 \rfloor$, and $k \neq 3$ if q is even. Then, C can be *uniquely* extended to a maximal MDS code of length $q+1$, which is GDRS.

Proof: By Theorem 1, the only possible MDS extensions of a $GDRS(n, k, \boldsymbol{\alpha}, \mathbf{v})$ code with $2 \leq k \leq n - \lfloor (q-1)/2 \rfloor$ and $k \neq 3$ when q is even, are also GDRS. Since the extended codes also

satisfy the hypotheses of Theorem 1, the extension process can continue until we reach the maximal GDRS code of length $q+1$ over $GF(q)$, which is unique, and, by Corollary 1, does not have any MDS extension.

Q.E.D.

In fact, Theorem 1 implies the following slightly stronger uniqueness result: under the conditions of Corollary 2, any generator matrix G of C can be uniquely extended to the generator matrix G' of a $(q+1, k)$ GDRS code. Matrix uniqueness here is up to permutation of columns and multiplication of columns by scalars. Notice that, in general, it is possible for a generator matrix G to be extended in two different ways to unequivalent matrices G' and G'', with G' and G'' generating equivalent (or even identical) codes.

Corollary 3: Let $C = GDRS(2^m+1, 3, \boldsymbol{\alpha}, \mathbf{v})$ over $F = GF(2^m)$. Then, the only possible MDS extension of C is obtained by appending to G a column of the form $(0, v, 0)^T$, $v \neq 0$.

Proof: Substitute $n = q+1$ in Theorem 1. The claim of the corollary is then equivalent to condition (ii) of the theorem.

Q.E.D.

Corollary 4: Let $2 \leq k \leq \lfloor q/2 \rfloor + 2$, and $k \neq 3$ if q is even. If the $(q+1, k)$ MDS code is unique, then $m(q, k) = q+1$, and $m(q, q+2-k) = q+1$.

Proof: Assume C is a $(q+2, k)$ MDS code over $GF(q)$. If the $(q+1, k)$ MDS code is unique, then it must be GDRS, and C is its extension. Since $2 \leq k \leq \lfloor q/2 \rfloor + 2$, this contradicts Corollary 1. Also, since the dual of a $(q+2, q+2-k)$ MDS code is a $(q+2, k)$ code [9, p. 318], nonexistence of a $(q+2, k)$ code implies nonexistence of a $(q+2, q+2-k)$ code.

Q.E.D

Using the language and methods of finite geometries, Thas [12] extended previous results by Segre [10], and proved the $m(q, k) = q+1$ conjecture for q odd and $k < (\sqrt{q}+9)/4$. The following is a restatement of the main results of [12], translated to the language of algebraic coding

theory.

Theorem 2 (Thas, [12]): Assume q is odd. Then, every (n,k) MDS code over $GF(q)$, such that $k+q-(\sqrt{q}+5)/4 < n \le q+1$, can be *uniquely* extended to a maximal $(q+1,k)$ MDS code, which is GDRS.

Similarly to the the remark following Corollary 2, the result in [12] is slightly stronger, and refers to the generator matrices rather than to the codes.

Corollary 5 (Thas, [12]): Every (n,k) MDS code over $GF(q)$, such that q is odd and $k+q-(\sqrt{q}+5)/4 < n \le q+1$, is a GDRS code.

Notice that Corollary 5 implies, in particular, that for odd q and $k < (\sqrt{q}+9)/4$, there is a unique $(q+1,k)$ MDS code over GF(q).

Theorem 3 (Thas, [12]): If q is odd, $k \ge 2$, and $(4k-9)^2 < q$, then $m(q,k) = q+1$.

III. Proofs

We start with a series of lemmas that will be used in the proof of Theorem 1.

Lemma 1: Let γ and $\alpha_1, \alpha_2, \cdots, \alpha_k$ be elements of F, and let M be the $(k+1)\times(k+1)$ matrix over F defined by

$$M = \begin{bmatrix} 0 & 1 & 1 & \dots & 1 \\ 0 & \alpha_1 & \alpha_2 & \dots & \alpha_k \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ 0 & \alpha_1^{k-2} & \alpha_2^{k-2} & \dots & \alpha_k^{k-2} \\ 1 & \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_k^{k-1} \\ \gamma & \alpha_1^{k} & \alpha_2^{k} & \dots & \alpha_k^{k} \end{bmatrix},$$

Let A_k be the $k\times k$ Vandermonde matrix at the upper right corner of M. Then, the determinant of M is given by

$$\det M = \left(\gamma - \sum_{j=1}^{k} \alpha_j \right) (-1)^k \det A_k.$$

Proof: Consider the Vandermonde matrix

$$B(x) = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ x & \alpha_1 & \alpha_2 & \dots & \alpha_k \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ x^{k-1} & \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_k^{k-1} \\ x^k & \alpha_1^k & \alpha_2^k & \dots & \alpha_k^k \end{bmatrix}, \tag{1}$$

where x is a variable. Computing the determinant of $B(x)$ by the Vandermonde determinant formula [9, p. 116], and also by cofactors of the first column, we obtain

$$\det B(x) = \left(\prod_{j=1}^{k} (\alpha_j - x) \right) \det A_k = \sum_{r=0}^{k} m_r (-x)^r, \tag{2}$$

where m_r is the minor corresponding to the element x^r in the first column of $B(x)$. From the definition of M, it follows that

$$\det M = (\gamma m_k - m_{k-1})(-1)^k, \tag{3}$$

and, by (2), we have

$$m_k = \det A_k, \tag{4}$$

$$m_{k-1} = \left(\sum_{j=1}^{k} \alpha_j \right) \det A_k. \tag{5}$$

Finally, the claim of the lemma follows by substituting (4) and (5) in (3).

Q.E.D.

Lemma 2: Let $F = GF(q)$, $q > 3$, and let S be a subset of r distinct elements of F such that $\lfloor (q-1)/2 \rfloor + 2 < r \le q$. Let $b \in F - \{0\}$, and let k be an integer such that $2 < k \le r - \lfloor (q-1)/2 \rfloor$. Then, for any subset $T = \{\alpha_1, \alpha_2, \cdots, \alpha_{k-2}\}$ of S, of cardinality $k-2$, there exist two elements α_{k-1} and α_k in S, such that the vector

$$\mathbf{w} = \mathbf{u}^k(\alpha_1) + \quad b \cdot \mathbf{u}^k(\infty)$$

lies in the linear span (over F) of the vectors $\mathbf{u}^k(\alpha_2), \cdots, \mathbf{u}^k(\alpha_k)$.

Proof: We want to prove that there exist two elements α_{k-1}, α_k in S, and $k-1$ coefficients $c_2, c_3, \cdots, c_k$ in F such that

$$\mathbf{w} = \sum_{i=2}^{k} c_i \mathbf{u}^k(\alpha_i). \tag{6}$$

Equation (6) implies that the vector $b \cdot \mathbf{u}^k(\infty)$ is in the linear span of $\mathbf{u}^k(\alpha_1), \cdots, \mathbf{u}^k(\alpha_k)$. Since $\mathbf{u}^k(\infty)$ is linearly independent of any $k-1$ such vectors, we conclude that all the α_i's, $1 \le i \le k$, should be distinct. In particular, we will require that $\alpha_{k-1} \neq \alpha_k$, and that both α_{k-1} and α_k be distinct from any of $\alpha_1, \cdots, \alpha_{k-2}$. Consider the matrix

$$W = [\ \mathbf{w}\ \ \mathbf{u}^k(\alpha_2)\ \cdots\ \ \mathbf{u}^k(\alpha_k)\ ]. \tag{7}$$

It can be readily seen that W differs from a Vandermonde matrix only by the addition of b to the entry α_1^{k-1} in the lower left corner. Hence, the determinant of W is given by

$$\det W = \left(\prod_{i=2}^{k}(\alpha_i - \alpha_1) \quad + (-1)^{k-1} b\right) \det A_{k-1} \quad = (-1)^{k-1}\left(\prod_{i=2}^{k} \ (\alpha_1 - \alpha_i) + b\right) \det A_{k-1}, \tag{8}$$

where A_{k-1} is a $(k-1)\times(k-1)$ Vandermonde matrix with entries $a_{ij} = \alpha_{j+1}^{i-1}, 1 \le i, j \le k-1$. Since $\alpha_2, \cdots, \alpha_k$ are all distinct, the vectors $\mathbf{u}^k(\alpha_2), \cdots, \mathbf{u}^k(\alpha_k)$ are linearly independent. Hence, to prove the lemma, it suffices to find α_{k-1} and α_k such that $\det W = 0$. Clearly, $\det A_{k-1} \neq 0$. Thus, we require

$$\prod_{i=2}^{k}(\alpha_1 - \alpha_i) + b = 0. \tag{9}$$

Replace both α_{k-1} and α_k in (9) by a variable x. Then, (9) becomes the quadratic equation

$$\left(\prod_{i=2}^{k-2}(\alpha_1 - \alpha_i)\right)(\alpha_1 - x)^2 + b = 0.^{3} \tag{10}$$

Equation (10) has at most two roots in F, which will be denoted β_1 and β_2. If q is even, then $\beta_1 = \beta_2$. Choose α_{k-1} such that

$$\alpha_{k-1} \neq \alpha_i, \quad 1 \leq i \leq k-2, \tag{11}$$

$$\alpha_{k-1} \neq \beta_j, \quad j = 1, 2, \tag{12}$$

and

$$\alpha_{k-1} \in S. \tag{13}$$

These constraints leave at least $r-k$ elements ($r-k+1$ if q is even) of S to choose α_{k-1} from. For a given choice of α_{k-1}, (9) is satisfied if we choose

$$\alpha_k = \alpha_1 + \frac{b}{\left(\prod_{i=2}^{k-2}(\alpha_1 - \alpha_i)\right)(\alpha_1 - \alpha_{k-1})}. \tag{14}$$

Denote the right-hand side of (14) by $f(\alpha_{k-1})$, where the function f is defined on the set $F - \{\alpha_1\}$. It can be readily verified that f is one-to-one and onto the set $F - \{\alpha_1\}$. Therefore, $\alpha_k \neq \alpha_1$, and, for α_{k-1} satisfying (12), we must have $\alpha_k \neq \alpha_{k-1}$ (otherwise, α_{k-1} would be a root of (10), contradicting (12)). Consider the (at least) $r-k$ values $\alpha_k = f(\alpha_{k-1})$ obtained by substituting values of α_{k-1} which satisfy (11)-(13). We claim that at least one of these values of α_k satisfies

$$\alpha_k \neq \alpha_i, \, 2 \leq i \leq k-2, \tag{15}$$

and

$$\alpha_k \in S. \tag{16}$$

The claim follows from the fact that there are exactly $q - r + (k-3)$ elements of F which violate either (15) or (16). By the hypotheses of the lemma, we have $k \leq r - \lfloor (q-1)/2 \rfloor$, which implies that $r - k > q - r + (k-3)$. Hence, at least one α_k satisfies both (15) and (16). Clearly, the pair α_{k-1}, α_k chosen so that α_{k-1} satisfies (11)-(13), and α_k satisfies (14)-(15), fulfills the requirements of the lemma.

---

[3] For $k = 3$, define the product to be 1.

Q.E.D.

Let G be the canonical generator matrix of a $GDRS(n, k, \boldsymbol{\alpha}, \mathbf{v})$ code over $F = GF(q)$. We say that a column $v_i\mathbf{u}^k(\alpha_i)$ is *singular* if $\alpha_i = \infty$, and *regular* otherwise. The following lemma is a direct consequence of Lemma 2.

Lemma 3: Let G be the canonical generator matrix of a $GDRS(n, k, \boldsymbol{\alpha}, \mathbf{v})$ code over F, where $2 \le k < n - \lfloor (q-1)/2 \rfloor$, and let $\mathbf{g} \in F^k$ be a column vector such that $\mathbf{g} \ne b \cdot \mathbf{u}^k(\infty)$ for any $b \in F$, and $\mathbf{g}$ can be expressed as a linear combination of $k-1$ columns of G. Then, $\mathbf{g}$ can be expressed as a linear combination of $k-1$ *regular* columns of G.

Proof: Trivially, the lemma is true if all the columns of G are regular, or if the original linear combination of columns of G giving $\mathbf{g}$ involves only regular columns. Hence, we assume that

$$\mathbf{g} = \sum_{i=1}^{k-2} a_i \mathbf{g}_i + a_\infty \mathbf{g}_\infty, \tag{17}$$

where $\mathbf{g}_1, \cdots, \mathbf{g}_{k-2}$ are regular columns of G, $\mathbf{g}_\infty$ is the singular column of G, $a_1, \cdots, a_{k-2}, a_\infty$ are scalars from F, and $a_\infty \ne 0$. Since $\mathbf{g}$ is not a scalar multiple of $\mathbf{u}^k(\infty)$, we must have $a_{i_0} \ne 0$ for some $1 \le i_0 \le k-2$, say $i_0 = 1$ (this also implies that $k > 2$). Let $r = n-1$, S be the set of generators of the regular columns of G, and T be the set of generators of the columns $\mathbf{g}_1, \cdots, \mathbf{g}_{k-2}$. Then, by Lemma 2, the vector $a_1\mathbf{g}_1 + a_\infty \mathbf{g}_\infty$ can be written as a linear combination of the columns $\mathbf{g}_2, \cdots, \mathbf{g}_{k-2}$, and two additional regular columns $\mathbf{g}_{k-1}, \mathbf{g}_k$ of G. Substituting for $a_1\mathbf{g}_1 + a_\infty \mathbf{g}_\infty$ in (17), we obtain $\mathbf{g}$ as a linear combination of $k-1$ regular columns of G.

Q.E.D.

The following lemma presents a well known property of MDS codes, a proof of which can be found in [9, Ch. 11].

Lemma 4: An (n, k, d) code C is MDS if and only if every k columns of a generator matrix G of C are linearly independent.

We can now prove Theorem 1.

Proof of Theorem 1: The "if" part corresponds to the construction of GDRS codes, which are well known to be MDS, and to the exceptional case when $k = 3$ and q is even, which is analyzed in [9, Ch. 11]. Hence, we concentrate on the proof of the "only if" part. We shall first prove it for proper GDRS codes. The proof for GRS codes will follow straightforward.

Let C be a proper $GDRS(n, k, \boldsymbol{\alpha}, \mathbf{v})$ code, with canonical generator matrix G, and such that $2 \le k \le n - \lfloor (q-1)/2 \rfloor$. We shall prove that for every column vector $\mathbf{g} \in F^k$, either

(i) $\mathbf{g} = v \cdot \mathbf{u}^k(\beta)$ where $v, \beta \in F$, $v \neq 0$, and β is not a column generator of G, or

(ii) $k = 3$, q is even, and $\mathbf{g} = (0, v, 0)^T$ for some $v \neq 0$, or

(iii) $\mathbf{g}$ can be expressed as a linear combination of $k-1$ columns of G, in which case, by Lemma 4, $[\, G \mid \mathbf{g} \,]$ does not generate an MDS code.

The proof will proceed by induction on k. The Theorem is clearly true for $k = 2$, since every nonzero $\mathbf{g} \in F^2$ is equal to $v \cdot \mathbf{u}^2(\beta)$ for some $\beta \in F \bigcup \{\infty\}$, and , if β is a column generator of G, then $\mathbf{g}$ is a scalar multiple of a column of G. The proof for $k = 2$ serves as the induction basis for the case where q is odd. When q is even, the case $k = 3$ brings the exceptional condition (ii) above, and will be treated separately. This will leave $k = 4$ as the basis for the induction. For the sake of continuity in the proof, we shall proceed now with the induction step, and we shall deal with the cases $k = 3$ and $k = 4$ (q even) later on. Thus, we assume the validity of the theorem for $k \ge 2$ when q is odd, and for $k \ge 4$ when q is even, and we prove it for $k+1$. Let G_{k+1} be the generator matrix of a $GDRS(n, k+1, \boldsymbol{\alpha}, \mathbf{v})$ code, where $k+1 \le n - \lfloor (q-1)/2 \rfloor$, and let G_k be the generator matrix of a $GDRS(n, k, \boldsymbol{\alpha}, \mathbf{v})$ code. We assume, without loss of generality, that $\alpha_n = \infty$. Notice that G_k consists of the first k rows of G_{k+1}, except in the singular column, where $v_n \mathbf{u}^k(\infty)$ replaces the first k entries (zeros) of $v_n \mathbf{u}^{k+1}(\infty)$. Let $\mathbf{g} \in F^{k+1}$ be a column vector, and let $\mathbf{g}^k \in F^k$ be the vector obtained by deleting the last coordinate of $\mathbf{g}$. Thus, we can write

$$\mathbf{g} = \begin{bmatrix} \mathbf{g}^k \\ \gamma \end{bmatrix}, \quad \gamma \in F. \tag{18}$$

We now consider three cases, which cover all possible values of $\mathbf{g}^k$.

Case 1: $\mathbf{g}^k = b \cdot \mathbf{u}^k(\infty)$ for some $b \in F$. If $b = 0$, then $\mathbf{g} = \gamma \cdot \mathbf{u}^{k+1}(\infty)$, and, trivially, $\mathbf{g}$ can be written as a linear combination of k columns of G_{k+1}. Therefore, we assume $b \neq 0$, and, hence,

$$\mathbf{g} = b \cdot [\ 0 \cdots 0\ 1\ \varepsilon\ ]^T, \tag{19}$$

where $\varepsilon = \gamma/b$. According to Lemma 1, $\mathbf{g}$ is in the linear span of the k distinct vectors $\mathbf{u}^{k+1}(\alpha_{j_1}), \cdots, \mathbf{u}^{k+1}(\alpha_{j_k})$ if and only if $\varepsilon = \sum_{i=1}^{k} \alpha_{j_i}$. Let $\alpha_{j_1}, \cdots, \alpha_{j_{k-2}}$ be $k-2$ distinct regular column generators of G_{k+1}. If q is even, we require that they do not add up to ε (it can be readily verified that such a choice is always possible). Define

$$\beta = \varepsilon - \sum_{i=1}^{k-2} \alpha_{j_i}. \tag{20}$$

We claim that there exist two distinct regular column generators $\alpha_{j_{k-1}}$ and α_{j_k} of G_{k+1}, which are not in the set $\{\alpha_{j_1}, \ldots, \alpha_{j_{k-2}}\}$, and which satisfy $\alpha_{j_{k-1}} + \alpha_{j_k} = \beta$. Hence, $\varepsilon = \sum_{i=1}^{k} \alpha_{j_i}$, and $\mathbf{g}$ is a linear combination of k columns of G_{k+1}, satisfying condition (iii) above. To prove the claim, note that the elements of F can be arranged in $\lfloor (q+1)/2 \rfloor$ pairwise disjoint unordered pairs $Q_i = \{a_i, b_i\}$ $(1 \leq i \leq \lfloor (q+1)/2 \rfloor)$, such that $a_i + b_i = \beta$. When q is odd, there is exactly one such pair in which $a_i = b_i$; when q is even, $a_i \neq b_i$ for all i, since we required $\beta \neq 0$ in this case. Now, since $k+1 \leq n - \lfloor (q-1)/2 \rfloor$, we have $(n-1) - (k-2) > \lfloor (q+1)/2 \rfloor$. By a simple counting argument, it follows that at least one of the pairs Q_i will consist of two distinct regular column generators of G_{k+1}, different from $\alpha_{j_1}, \ldots, \alpha_{j_{k-2}}$.

Case 2: $\mathbf{g}^k \neq b \cdot \mathbf{u}^k(\infty)$ for any $b \in F$, and $\mathbf{g}^k$ can be expressed as a linear combination of $k-1$ columns of G_k. Since the conditions of Lemma 3 are satisfied, we may assume that the linear combination does not include the singular column of G_k. Therefore, $\mathbf{g}$ can be expressed as a linear combination of the $k-1$ columns which give $\mathbf{g}^k$ in G_k (extended to length $k+1$), plus a suitable scalar multiple of $\mathbf{u}^{k+1}(\infty)$, chosen so that the value γ is obtained in the $k+1$-st entry.

Case 3: $\mathbf{g}^k \neq b \cdot \mathbf{u}^k(\infty)$ for any $b \in F$, and $\mathbf{g}^k$ cannot be expressed as a linear combination of $k-1$ columns of G_k. Hence, $\mathbf{g}^k$ can be appended to G_k, while preserving the MDS property. By

the induction hypothesis, $\mathbf{g}^k = v \cdot \mathbf{u}^k(\lambda)$, where $v \neq 0$, and λ is not a column generator of G_k (and, hence also not of G_{k+1}). Let $b = \gamma/v - \lambda^k$. Then, $\mathbf{g} = v \cdot [\mathbf{u}^{k+1}(\lambda) + b \cdot \mathbf{u}^{k+1}(\infty)]$. If $b = 0$, we have $\mathbf{g} = v \cdot \mathbf{u}^{k+1}(\lambda)$, and condition (i) in the claim of the theorem is satisfied. Assume $b \neq 0$. Then, using Lemma 2 with $r = n$, $S = \{\lambda, \alpha_2, \cdots, \alpha_n\}$, we obtain that $\mathbf{g}$ can be expressed as a linear combination of k columns of G_{k+1}. This completes the proof of Theorem 1 for proper GDRS codes, conditional on the proofs of the cases $k = 3$ and $k = 4$ with q even.

Consider now the case $k = 3$ with q even. Trying to apply the induction step from $k = 2$ to $k = 3$ will fail for vectors belonging to *Case 1* above, with $\varepsilon = 0$, i.e., when $\mathbf{g} = b \cdot (0,1,0)^T$. In this case, we will not be able to satisfy $\beta \neq 0$ in (20), as required in the proof. Indeed, as it is known [9, Ch. 11], such a column $\mathbf{g}$ *can* be appended to the canonical generator matrix of a $GDRS(n, 3, \boldsymbol{\alpha}, \mathbf{v})$ code over $GF(2^m)$, while preserving the MDS property. This corresponds to condition (ii) in the claim of Theorem 1 ("if" part). The "only if" part follows from the fact that the proof of Theorem 1, as presented above, fails only in the mentioned case, being correct in all other cases.

The case $k = 4$, q even, is proved by applying the induction step from $k = 3$ to $k = 4$. However, due to the singular case mentioned above, the proof that a column vector of the form $\mathbf{g} = (0, b, 0, \gamma)^T$, $b \neq 0$, is a linear combination of three columns of the generator matrix G_4, is incorrect. This case is easily handled by applying the induction step on the reversed vector $\mathbf{z} = (\gamma, 0, b, 0)^T$, and for the generator matrix G_4^* having $\alpha_1^{-1}, \cdots, \alpha_n^{-1}$ as column generators (0 goes to ∞, and ∞ goes to 0). This will use the induction hypothesis for the vector $(\gamma, 0, b)^T$, which is covered by the proof of the case $k = 3$, and will express $\mathbf{z}$ as a linear combination of three columns of G_4^*. The translation to an expression for $\mathbf{g}$ as a linear combination of three columns of G_4 is straightforward.

Finally, it remains to prove Theorem 1 for GRS codes. This is achieved by observing that any $GRS(n, k, \boldsymbol{\alpha}, \mathbf{v})$ code with canonical generator matrix G, can be extended to a proper $GDRS(n+1, k, \boldsymbol{\alpha}', \mathbf{v}')$ code, with canonical generator matrix $G' = [\ G \mid \mathbf{u}^k(\infty)\ ]$. Now, according to Lemma 3, any vector $\mathbf{g} \in F^k - \{b \cdot \mathbf{u}^k(\infty),\ b \neq 0\}$, which can be expressed as a linear

combination of $k-1$ columns of G', can be expressed as a linear combination of $k-1$ regular columns of G', which are also columns of G. Hence, G can be extended by a column $\mathbf{g}$ while preserving the MDS property if and only if either $\mathbf{g}$ is a singular column (obtaining G'), or $\mathbf{g}$ can also extend G'.

Q.E.D.

Acknowledgment. We are grateful to the anonymous referees for their thorough review of the paper, and for their useful suggestions. In particular, the geometric formulation of our main result as Theorem 1′ is due to one of the referees.

REFERENCES

[1] L.R.A. Casse, "A solution to Beniamino Segre's problem $I_{r,q}$ for q even", *Atti Accad. Naz. Lincei, Rend. Cl. Sc. Fis. Mat. Natur.,* Vol. 46, pp. 13-20, 1969.

[2] L.R.A. Casse and D.G. Glynn, "The solution to Beniamino Segre's problem $I_{r,q}$, $r = 3$, $q = 2^h$", *Geom. Dedicata,* Vol. 13, pp. 157-163, 1982.

[3] L.R.A. Casse and D.G. Glynn, "On the uniqueness of $(q+1)$-arcs of $PG(4, q)$, $q = 2^h$, $h \geq 3$", *Discrete Mathematics,* Vol. 48, pp. 173-186, 1984.

[4] J.W.P. Hirschfeld, "Maximum sets in finite projective spaces", pp. 55-76 in *Surveys in combinatorics,* LMS Lecture Notes Series 82, E.K. Lloyd, editor, Cambridge University Press, 1983.

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

[6] R.R. Jurick, "An algorithm for determining the largest maximally independent set of vectors from an r-dimensional vector space over a Galois field of n elements", Tech. Rep. ASD-TR-68-40, Air Force Systems Command, Wright-Patterson Air Force Base, Ohio, September 1968.

[7] C. Maneri and R. Silverman, "A vector-space packing problem", *J. Algebra,* Vol. 4, pp. 321-330, 1966.

[8] C. Maneri and R. Silverman, "A combinatorial problem with applications to geometry", *J. Comb. Theory,* Vol 11A, pp. 118-121, 1971.

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

[10] B. Segre, "Curve razionali normali e k-archi negli spazi finiti", *Ann. Mat. Pura Appl.,* Vol. 39, pp. 357-359, 1955.

[11] B. Segre, *Lectures in Modern Geometry,* Edizioni Cremonese, Rome, 1961.

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

[13] J.A. Thas, "Normal rational curves and $(q+2)$-arcs in a Galois space $S_{q-2,q}$ $(q=2^h)$", *Atti Accad. Naz. Lincei, Rend. Cl. Sc. Fis. Mat. Natur.*, Vol. 47, pp. 115-118, 1969.

[14] J.A. Thas, "Connection between the Grassmannian $G_{k-1;n}$ and the set of the k-arcs of the Galois space $S_{n,q}$", *Rendiconti di Matematica,* Vol. 2, pp. 121-134, 1969.

[15] J.A. Thas, "Complete arcs and algebraic curves in $PG(2, q)$", preprint, Seminar of Geometry and Combinatorics, State University of Ghent, Belgium, December 1984.