COMPOSITION OF REED-SOLOMON CODES AND GEOMETRIC DESIGNS

RON M. ROTH AND ABRAHAM LEMPEL, FELLOW, IEEE

Department of Computer Science

Technion, Israel Institute of Technology

Haifa 32000 - Israel

ABSTRACT

It is shown that good linear $[n, k, d]$ codes over a finite field $GF(q)$ can be constructed by concatenating the generator matrices of Reed-Solomon codes. For the first interesting case of $k = 3$, it is shown that many of the codes obtained via projective geometry techniques can readily be obtained via the proposed algebraic approach.

I. INTRODUCTION

Let q be a power of a prime and let F be the field $GF(q)$. An $[n, k, d]$ code C over F is a k-dimensional subspace of F^n, with d being the minimum (Hamming) distance between any two members of C [6]. To shorten notation in the sequel, we define the *(maximum) proximity* t of C as $t \triangleq n - d$; that is, t is the maximal number of coordinates in which two distinct codewords of C can have equal entries or, equivalently, the maximal number of zeroes in any nonzero codeword of C. It is easy to verify that t is also the maximal number of columns of rank $< k$ in any generator matrix G of C.

A possible approach to the construction of long codes with relatively small proximity is to form a generator matrix G by concatenating the generator matrices of several good short codes. Suitable building blocks for such a construction are generator matrices of Reed-Solomon (RS) codes and their extensions. A RS code over $GF(q)$ is a $[q-1, l, q-l]$ code generated by the matrix [6, p. 323]

$$G_{RS} = \left[\mathbf{g}_1 \ \mathbf{g}_2 \cdots \mathbf{g}_{q-1} \right],$$

where the columns of G_{RS} are of the form

$$\mathbf{g}_i = (1 \ \alpha_i \ \alpha_i^2 \cdots \alpha_i^{l-1})',$$

with the α_i ranging over the nonzero elements of $GF(q)$. Generator matrices for extended and doubly-extended RS codes are obtained from G_{RS} by appending the column $\mathbf{g}_0 = (1\ 0\ 0 \cdots 0)'$, or both $\mathbf{g}_0$ and $\mathbf{g}_\infty = (0\ 0 \cdots 0\ 1)'$, respectively, to G_{RS}.

Let G_0 denote the generator matrix of the extended RS code, i.e.,

$$G_0 = \left[G_{RS} \ \mathbf{g}_0 \right].$$

The construction proposed here employs G_0 and m matrices $T_1, T_2, \cdots, T_m$ over F such that the code generated by the matrix

$$G = \left[T_1 \cdot G_0 \quad T_2 \cdot G_0 \quad \cdots \quad T_m \cdot G_0 \right] \tag{1}$$

has small proximity. Note that in case the T_i's are nonsingular square matrices the resulting code is a concatenation of several RS codes, since each $T_i \cdot G$ serves as a generator matrix of a RS code. This will be the case in most of the constructions in the sequel. To facilitate the analysis of codes generated by (1) we need the following definitions.

Let a polynomial $v(x) = v_0 + v_1 x + \cdots + v_{l-1} x^{l-1}$, $l \geq 1$, over F be represented by the vector $\mathbf{v} = (v_0\ v_1 \cdots v_{l-1})$ of its coefficients. For a nonzero polynomial $\mathbf{v}$, let $\rho(\mathbf{v})$ denote the number of *distinct* roots of $\mathbf{v}$ in F and let $\rho^*(\mathbf{v})$ denote the number of distinct roots of $\mathbf{v}$ in $F^+ = F \bigcup \{\infty\}$, where ∞ is, by definition, a root of $\mathbf{v}$ in F^+ if $v_{l-1} = 0$.

Let $\Pi[m; k, l]$, $1 \leq k \leq l \leq q$, be a multiset of $m \geq 1$ (including multiplicity) matrices $\{T_i\}_{i=1}^m$ of order $k \times l$ and rank k over F. Define

$$\rho(\Pi[m; k, l]) \triangleq \max_{\mathbf{u} \in F^k - \{\mathbf{0}\}} \{ \sum_{i=1}^{m} \rho(\mathbf{u}\ T_i) \} .$$

$\rho^*(\Pi[m; k, l])$ is defined in a similar manner. We shall use the shorthand notation $\Pi[m; k]$ for $\Pi[m; k, k]$ and we shall omit the parameters altogether when no confusion is caused by the omission.

With each set $\Pi[m; k, l] = \{T_i\}$ we associate an $[n = m \cdot q,\ k,\ d]$ code $C(\Gamma)$ as in (1). Hence, every codeword $\mathbf{u}G$ of C, $\mathbf{u} \in F^k$, can be interpreted as a simultaneous evaluation of m polynomials $\mathbf{v}_i = \mathbf{u}\ T_i \in F^l$ at each point of F. From the definition of $\rho(\Pi[m; k, l])$ it follows that the proximity of C is given by

$$t = \rho(\Pi[m; k, l]) . \tag{2}$$

Thus, we shall refer to $\rho(\mathbf{v})$ as the proximity of $\mathbf{v}$ and to $\rho(\Gamma)$ as the proximity of Γ. Replacing G_0 in (1) by the generator matrix $G_\infty = [G_0\ \ \mathbf{g}_\infty]$ of the doubly-extended RS code yields an $[n = m(q+1),\ k,\ d^*]$ code $C^*(\Gamma)$ with $t^* = \rho^*(\Pi[m; k, l])$.

Many of the codes obtained here were previously obtained using projective geometry techniques. Let $PG(k-1,q)$ be a projective space of dimension $k-1$ over F. A multiset S of n points in $PG(k-1,q)$ is called an $(n;t)$-*arc* if t is the maximal number of points of S lying in a $(k-2)$-dimensional subspace of $PG(k-1,q)$ [2, Ch. 12][1]. Hence, a $k \times n$ matrix G of rank k, containing no zero columns, generates an $[n,k,d]$ code if and only if its columns form an $(n\,;\,t=n-d)$-arc in $PG(k-1,q)$.

It is well-known [3, §6] that the size n of an $(n;t)$-arc in $PG(k-1,q)$, $k \geq 2$, is upper-bounded by[2]

$$n \leq (t-k+2)\,q + t\,. \tag{3}$$

This bound is useful in obtaining bounds for $\rho(\Gamma)$. Clearly, $\rho(\Pi[m;1]) = 0$. For $k \geq 2$, by (3) and the definition of $C(\Gamma)$, we have

$$m \cdot q \leq (t-k+2)q + t = t(q+1) - (k-2)q$$

which, by (2), yields,

$$\frac{q}{q+1}\,(m+k-2) \leq \rho(\Pi[m;k,l]) \leq m \cdot (l-1)\,. \tag{4}$$

A similar bound holds for $\rho^*(\Pi[m;k,l])$; $\rho^*(\Pi[m;1]) = 0$ and, for $2 \leq k \leq l \leq q$, it can be readily verified that

$$m + k - 2 \leq \rho^*(\Pi[m;k,l]) \leq m \cdot (l-1)\,. \tag{5}$$

For $k = l = 2$, (5) implies $\rho^*(\Pi[m;2]) = m$. Hence, the corresponding code $C^*(\Gamma)$ attains the bound of (3). In terms of the dimension k, the first interesting case is that of $k = 3$. We present sets $\Gamma[m;3,l]$ with $\rho(\Gamma)$ close or equal to the lower bounds of (4) or (5), thus yielding codes which approach and sometimes attain the bound of (3). Some of the codes obtained in Sections III.A and III.B have already been derived using a variety of geometric arguments ([2, Ch. 12],[3,

[1] *(n;t)*-arcs are usually defined as sets; however it is easy to verify that the bound given below applies to multisets as well.

[2] A simple algebraic proof of (3) is given in Appendix A.

§2]). We believe that there is merit in an alternate derivation using a unified algebraic approach, especially, as it leads to new constructions (Section III.C) as well.

We also show that for $m = 2$, $\rho(\Gamma[2;3]) = 4$ for all $q \geq 8$. This proves that for $q \geq 8$ there exists no $[2q, 3, 2q-3]$ code obtained by concatenating the generator matrices of two extended RS codes. This result is a corollary of a stronger one, stating that there exists no $[n, 3, n-3]$ code with $n > \frac{8}{5}(q+2)$ whose generator matrix is the concatenation of generator matrices of two *maximum-distance separable* (MDS) codes [6, Ch. 11]. In terms of projective geometry this means that there exists no plane $(n;3)$-arc with $n > \frac{8}{5}(q+2)$ formed by the union of two $(\hat{n};2)$-arcs. The existence of an $(a \cdot q;3)$-arc with $a > 1$ for all q remains unresolved.

II. BACKGROUND

Let r be a power of a prime p and let $q = r^h$, $h \geq 1$. Let $F = GF(q)$ and $K = GF(r)$. The *trace* function of F over K is defined by

$$\mathrm{tr}(x) \triangleq x + x^r + x^{r^2} + \cdots + x^{r^{h-1}} .$$

The following are known properties of $\mathrm{tr}(x)$ [6, p. 116].

(i) For every $a, b \in K$ and $\alpha, \beta \in F$,

$$\mathrm{tr}(a\alpha + b\beta) = a\,\mathrm{tr}(\alpha) + b\,\mathrm{tr}(\beta) .$$

(ii) For every $\alpha \in F$,

$$\mathrm{tr}(\alpha^r) = \mathrm{tr}(\alpha) .$$

(iii) For every $\alpha \in F$, $\mathrm{tr}(\alpha) \in K$ and each value of K is the image of r^{h-1} elements of F.

Consider the polynomial equation over F:

$$v(x) \triangleq x^r - ax - b = 0 . \tag{6}$$

It is easy to determine $\rho(\mathbf{v})$, the number of distinct roots of $v(x)$ in F (see also [4, Ch. 3, §§4,5]).

If $a = 0$, then $v(x) = (x - b^{q/r})^r$ has one root of multiplicity r. Assume now that $a \neq 0$. Then, if $\rho(\mathbf{v}) \geq 2$ and x_1, x_2 are distinct roots of $v(x)$, we obtain

$$v(x_1) - v(x_2) = (x_1 - x_2)^r - a(x_1 - x_2) = 0 .$$

This implies that the polynomial $x^{r-1} - a$ has a root in F, or that a is an $(r-1)$-st power in F. Therefore, if a is not an $(r-1)$-st power, then for every $b \in F$, $\rho(\mathbf{v}) \leq 1$, which implies that $v(\alpha)$, $\alpha \in F$, is a permutation on F, or that $v(x)$ has exactly one root in F. Assume now that $a = \gamma^{r-1}$ for some $\gamma \in F - \{0\}$. Substituting $x = \gamma y$ into (6) yields

$$y^r - y - \frac{b}{\gamma^r} = 0$$

which, by (i) and (ii), implies

$$\mathrm{tr}\left(\frac{b}{\gamma^r}\right) = 0 . \tag{7}$$

Hence, if (7) does not hold, $v(x)$ has no roots in F. On the other hand, (7) is sufficient for $v(x)$ to have r roots. To see this, note first that, by (iii), for each $\gamma \in F$ there exist exactly $\frac{q}{r}$ distinct values $b \in F$ that satisfy (7). Second, when α ranges over F, $\alpha^r - a\alpha$ takes values satisfying (7); each such value is obtained exactly r times; and, the set of r α's yielding the same value $b = \alpha^r - a\alpha$ form the roots of $v(x) = x^r - ax - b$ in F.

The following is a summary of the above discussion.

Proposition 1. *Let $q = r^h$, $F = GF(q)$, and $K = GF(r)$. Let $v(x) = x^r - ax - b$ be a polynomial over F. If $a \neq 0$ is an $(r-1)$-st power in F, then either $\rho(\mathbf{v}) = r$ or $\rho(\mathbf{v}) = 0$, according to whether $\mathrm{tr}\left(\frac{b}{a^{r/(r-1)}}\right)$ is zero or nonzero; if $a = 0$ or a is not an $(r-1)$-st power in F, $\rho(\mathbf{v}) = 1$.*

Note that in the special case of $r = 2$, (6) is a quadratic equation over $F = GF(2^h)$ with one (double) root in F if and only if $a = 0$; two distinct roots in F if the discriminant $\Delta \triangleq \mathrm{tr}(b/a^2) = 0$; and, no roots in F if $\Delta = 1$ [6, p. 277].

We shall also consider quadratic equations of the form

$$x^2 + ax + b = 0 \tag{8}$$

over $F = GF(q)$ when q is odd. Here the discriminant is defined by $\Delta = a^2 - 4b$, and (8) has one root in F if $\Delta = 0$; two distinct roots if Δ is a nonzero square in F; and, no roots if Δ is a nonsquare. To facilitate the investigation of quadratic equations over finite fields of odd characteristic, we present, for later reference, several properties of the set of squares in F.

When q is odd, $F = GF(q)$ contains $\frac{q-1}{2}$ nonzero squares and the same number of nonsquares [6, p. 113]. A refinement of this property is stated in the following proposition.

Proposition 2. [6, p. 519]. *Let* $\{\theta_i\}_{i=1}^{(q-1)/2}$ *be the set of nonsquares of* F *and, for* $\alpha \in F - \{0\}$, *let* $\Theta_\alpha \triangleq \{\alpha + \theta_i\}_{i=1}^{(q-1)/2}$. *Then, (i) If* $q \equiv -1 \pmod 4$, Θ_α *contains* $\frac{q+1}{4}$ *squares; in case* α *is a square, one of the squares in* Θ_α *is zero. (ii) If* $q \equiv 1 \pmod 4$, Θ_α *contains* $\frac{q-1}{4}$ *nonzero squares; in case* α *is a nonsquare,* $0 \in \Theta_\alpha$.

A special case of interest is when $q = r^2$, r odd. Each element $a \in K = GF(r)$ is a square in F, since the polynomial $x^2 - a$ is reducible over F. Let $\beta \in F - K$. Then every element $\alpha \in F - K$ can be written uniquely as $\alpha = a \cdot (b + \beta)$ with $a, b \in K$. It follows that either both α and $b + \beta$ are squares or both are nonsquares. Therefore, if b ranges over K, $b + \beta$ takes the value of $\frac{r-1}{2}$ squares and $\frac{r+1}{2}$ nonsquares in F. On the other hand, if $\beta \in K$, then for all $b \in K$, $b + \beta$ is a square in F. Hence, we can write the following proposition.

Proposition 3. *Let $F = GF(r^2)$, r odd, and let $\beta \in F$. Then, the number of nonsquares of F among the r elements $b + \beta$, $b \in GF(r)$, does not exceed* $\frac{r+1}{2}$.

III. COMPOSITION OF REED-SOLOMON CODES

In this section we describe and analyze the composition of RS codes of dimension $k = 3$. The resulting codes approach and sometimes attain the bound of (3) which, in this case, reduces to

$$n \le (t-1)q + t\ .$$

Some of the codes constructed here have previously been obtained using various projective geometry methods. As in the geometric approach, most of the codes constructed here have $t \le q + 1$.

A. Codes over Finite Fields of Even Size

Constructions of $(n; t)$-arcs over $F = GF(2^h)$ with $t = 2^s$, $1 \le s \le h$, which attain the bound of (3) can be found in [2, Ch. 12]. Here we verify that the corresponding codes are equivalent to composite RS codes and show how these codes can be further composed to form good codes for values of t other than powers of 2. The resulting codes approach the bound of (3) as q and t tend to infinity. Throughout this subsection $F = GF(2^h)$ and the range of $\mathrm{tr}(x)$ is $GF(2)$.

Let $a \in F$ be such that $\mathrm{tr}(a) = 1$. For $1 \le s \le h$, let $\{\lambda_i\}_{i=0}^{2^s-1}$ be an s-dimensional linear subspace of F over $GF(2)$ with $\lambda_0 = 0$. Define the set $\Pi[m = 2^s - 1; 3] \triangleq \{T_i\}$ by

$$T_i = \begin{bmatrix} \lambda_i & 0 & 0 \\ a & 1 & 1 \\ 0 & 0 & \lambda_i \end{bmatrix}, \qquad 1 \le i \le 2^s - 1 .$$

We claim that $\rho^*(\Gamma) = 2^s$. To show this, let $\mathbf{u} = (u_0, u_1, u_2) \in F^3 - \{\mathbf{0}\}$ and let $\mathbf{v}_i = \mathbf{u}T_i$, $1 \le i \le 2^s - 1$, i.e.,

$$v_i(x) = (\lambda_i u_0 + a u_1) + u_1 x + (u_1 + \lambda_i u_2)x^2 , \quad 1 \le i \le 2^s - 1 . \tag{9}$$

In case $u_1 = 0$, $\rho^*(\mathbf{v}_i) \le 1$ for each i, and thus, $\sum_{i=1}^{2^s-1} \rho^*(\mathbf{v}_i) \le 2^s - 1$. Hence, we can assume $u_1 \ne 0$. The discriminant Δ_i of (9) is given by

$$\Delta_i = \mathrm{tr}\left[\frac{(\lambda_i u_0 + a u_1)(u_1 + \lambda_i u_2)}{u_1^2} \right]$$

$$= \mathrm{tr}(a) + \mathrm{tr}\left[\frac{u_0 + a u_2}{u_1} \lambda_i \right] + \mathrm{tr}\left[\frac{u_0 u_2}{u_1^2} \lambda_i^2 \right].$$

Noting that $\mathrm{tr}(x) = \mathrm{tr}(\sqrt{x})$, we obtain

$$\Delta_i = 1 + \mathrm{tr}[\delta(\mathbf{u})\, \lambda_i] , \quad 1 \le i \le 2^s - 1 , \tag{10}$$

where

$$\delta(\mathbf{u}) = \frac{u_0 + a u_2 + \sqrt{u_0 u_2}}{u_1} .$$

Since the trace is a linear operator and the λ_i form a linear subspace of dimension s, either all or exactly one half of the λ_i satisfy $\mathrm{tr}[\delta(\mathbf{u})\, \lambda_i] = 0$. Recalling that $\rho(\mathbf{v}_i) = 0$ if $\Delta_i = 1$, at least $2^{s-1} - 1$ of the polynomials $v_i(x)$ have no zeroes in F. Consequently, for each $\mathbf{u} \in F^3 - \{\mathbf{0}\}$, $\sum_{i=1}^{2^s-1} \rho(\mathbf{v}_i) \le 2^s$. Furthermore, if $u_1 + \lambda_i u_2 = 0$ for some i, $\mathbf{v}_i$, being linear, has only one root in F and, therefore, no more than two roots in $F^+ = F \cup \{\infty\}$. This implies $\sum_{i=1}^{2^s-1} \rho^*(\mathbf{v}_i) \le 2^s$. It follows that the corresponding code $C^*(\Gamma)$ has length $n = m \cdot (q+1) = (2^s - 1) \cdot (q+1)$ and proximity $t^* = \rho^*(\Gamma) = 2^s$. Recalling that when $u_1 = 0$, $\sum_{i \ge 1} \rho^*(\mathbf{v}_i) \le 2^s - 1$, we can add the column $(0,1,0)'$ to the generator matrix without affecting the proximity. This results in a code C_s^* of length $(2^s - 1)(q+1) + 1$ and proximity 2^s that attains (3).

Note that C_1^* is the exceptional triply-extended RS code [6, p. 326] and C_h^* is a $[q^2, 3, q^2 - q]$ code which corresponding to a complement of a line in $PG(2, q)$ [2, p. 325]. To carry the correspondence with geometric constructions a little further, we mention two simple modifications of C_h^* leading to other known codes. Using G_{RS} instead of G_∞ and omitting the extra column $(0,1,0)'$, an $[n = (q-1)^2, 3, n-(q-1)]$ code is obtained, whose corresponding $(n; t)$-arc is a complement of a triangle [2, p. 330]. Appending the $q+1$ columns $(0,0,1)'$ and $\{(1, 0, b)'\}_{b \in F}$ to the generator matrix of C_h^* results in an $[n = q^2 + q + 1, 3, n-(q+1)]$ code, whose generator matrix has all the points of $PG(2, q)$ as columns.

The codes C_s^* can be used for the constructions of long $[n, 3, n-t]$ codes approaching the bound of (3), where t is not necessarily a power of 2. Let $\mathbf{t} = (t_h\ t_{h-1} \cdots t_1\ 0)$ be the binary representation of a designed even proximity $t = \sum_{s=1}^{h} t_s 2^s$, $2 \le t < 2q$, and let $\mathrm{w}(t)$ be the (Hamming) weight of $\mathbf{t}$. Let G^* be the matrix obtained by concatenating all those generator matrices G_s^* of C_s^* such that $t_s = 1, 1 \le s \le h$. Clearly, the code C^*, generated by G^*, has proximity t and length

$$n = \sum_{s=1}^{h} t_s[\,(2^s - 1)(q+1) + 1\,] = t \cdot (q+1) - \mathrm{w}(t) \cdot q\,. \tag{11}$$

Codes with odd proximity $t \ge 3$, satisfying (11), can be obtained by appending a zero column to the generator matrix of a code C^* of proximity $t-1$. Since $\mathrm{w}(t) \le \log_2(t+1)$, (11) implies the existence of $[n, 3, n-t]$ codes with

$$n \ge t \cdot (q+1) - q \cdot \log_2(t+1)\,, \quad 2 \le t < 2q\,. \tag{12}$$

Note that the ratio between this lower bound on n and the upper bound of (3) approaches unity as t and q approach infinity.

B. Codes over Finite Fields of Odd Size

Let $F = GF(q)$ where q is a power of an odd prime. We begin with a construction resulting in a code over F with parameters $[n = \frac{1}{2}q(q-1)+1,\ 3,\ n-t]$, $t = \frac{q+1}{2}$. An equivalent code is given in [2, p. 330].

Let $\{\theta_i\}_{i=1}^{(q-1)/2}$ be the nonsquares of F. Consider the set $\Pi[m = \frac{q-1}{2}\ ;\ 3] = \{T_i\}$, defined by

$$T_i = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\theta_i & 0 & 1 \end{bmatrix}, \quad 1 \le i \le \frac{q-1}{2}\ .$$

Let $\mathbf{u} = (u_0\ u_1\ u_2)\ \in F^3 - \{\mathbf{0}\}$ and let $\mathbf{v}_i = \mathbf{u}T_i, 1 \le i \le m$, i.e.,

$$v_i(x) = (u_0 - \theta_i u_2) + u_1 x + u_2 x^2\ , \quad 1 \le i \le \frac{q-1}{2}\ . \tag{13}$$

If $u_2 = 0$, $\rho(\mathbf{v}_i) \le 1$ for each i and so $\sum_{i=1}^{(q-1)/2} \rho(\mathbf{v}_i) \le \frac{q-1}{2}$. Assume now that $u_2 \ne 0$ and, without loss of generality, that $u_2 = 1$. The discriminant Δ_i of (13) is given by

$$\Delta_i = u_1^2 - 4(u_0 - \theta_i) = (u_1^2 - 4u_0) + 4\theta_i \triangleq \Delta_0 + 4\theta_i\ , \quad 1 \le i \le \frac{q-1}{2}\ . \tag{14}$$

By Proposition 2, if $q \equiv -1 \pmod 4$, $\frac{q+1}{4}$ of the Δ_i are squares in F; and if $q \equiv 1 \pmod 4$, the number of the nonzero squares does not exceed $\frac{q-1}{4}$. (In the latter case it is also possible that one of the Δ_i vanishes). Thus, in either case, $\sum_{i=1}^{(q-1)/2} \rho(\mathbf{v}_i) \le \frac{q+1}{2}$ and the corresponding code $C(\Gamma)$ has proximity $\frac{q+1}{2}$. The special column $(0,0,1)'$ can also be added to the generator matrix of $C(\Gamma)$ without affecting the proximity, resulting in a code of length $n = m \cdot q + 1 = \frac{1}{2}q(q-1)+1$.

In a similar manner, an $[n = \frac{1}{2}q(q+1)+1,\ 3,\ n-\frac{q+3}{2}]$ code can be obtained by adding the matrix $T_{(q+1)/2} = I$ to the set Γ.

A different construction is possible in the special case when $q = r^2$, where r is a power of an odd prime. Let θ be a nonsquares of F, let $GF(r) = \{a_i\}_{i=1}^{r}$, and let $\Pi[r;3]$ consist of the r matrices

$$T_i = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a_i\theta & 0 & 1 \end{bmatrix}, \quad 1 \le i \le r\ . \tag{15}$$

Consider the polynomials $\mathbf{v}_i = \mathbf{u}T_i$, $\mathbf{u} = (u_0\ u_1\ u_2)\ \in F^3 - \{\mathbf{0}\}$, $1 \le i \le r$. In case $u_2 = 0$, all the $\mathbf{v}_i$ are linear polynomials and so $\sum_{i=1}^{r}\rho(\mathbf{v}_i) \le r$. Assuming that $u_2 = 1$, the discriminant Δ_i of $\mathbf{v}_i$ is given by

$$\Delta_i = u_1^2 - 4(u_0 + a_i\theta) \triangleq \Delta_0 - 4a_i\theta = \theta\left(\frac{\Delta_0}{\theta} - 4a_i\right), \quad 1 \le i \le r\ .$$

By Proposition 3, the range of $\Delta_0/\theta - 4a_i$ as a_i varies over $GF(r)$ includes no more than $\frac{r+1}{2}$ nonsquares of F. Thus, $\frac{r+1}{2}$ is the maximal number of Δ_i's which are squares and, hence, $\sum_{i=1}^{r}\rho(\mathbf{v}_i) \le r+1$. An $[rq+1,\ 3,\ rq-r]$ code $\hat{C}$ can now be obtained by appending the column $(0,0,1)'$ to the generator matrix of $C(\Gamma)$. This code has the same parameters as the one that corresponds to a Hermitian curve [2, §7.3], although the two are not equivalent[3] (see Appendix B). Concatenating M copies of the generator matrix of $\hat{C}$ we obtain a code of proximity $t = M(r+1)$ and length $n = M(rq+1) \ge (1 - \frac{1}{r+1})tq$, with the ratio between n and the bound of (3) approaching unity as r grows.

For the sake of completeness, we also mention, as in Subsection A, that an $[n = q^2,\ 3,\ n-q]$ code $C(\Gamma)$ can be constructed using $\Pi[q;3] = \{T_i\}$, where

[3] Two codes are said to be equivalent if the generator matrix of one can be obtained from that of the other by any combination of the following operations: permutation of columns, scaling of columns, and nonsingular row operations.

$$T_i = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ b_i & 0 & 1 \end{bmatrix}, \quad 1 \le i \le q\,, \quad \{b_i\} = F\,.$$

When the columns $(0,1,0)'$ and $\{(0,1,b)'\}_{b \in F}$ are added to the generator matrix of $C(\Gamma)$, we obtain an $[n = q^2 + q + 1,\ 3,\ n - (q+1)]$ code whose generator matrix contains all the points of $PG(2, q)$ as columns. Finally, an $[n = (q-1)^2,\ 3,\ n - (q-1)]$ code is obtained using G_{RS} instead of G_0 and the set $\Pi[q-1; 3] = \{T_i\}$, where

$$T_i = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b_i \end{bmatrix}, \quad 1 \le i \le q-1\,, \quad \{b_i\} = F - \{0\}\,.$$

C. Codes over Finite Extension Fields

Let $F = GF(q)$ and $K = GF(r)$, where r is a power of a prime and $q = r^h$, $h > 1$. Let $\{a_i\}_{i=1}^{r} = K$ be an ordering on the elements of K. For h integers $0 \le \delta_1 \le \delta_2 \le \cdots \le \delta_h \triangleq \delta < r$ define the h sets

$$A_j \triangleq \{a_i \mid 1 \le i \le r - \delta_j\}\,, \quad 1 \le j \le h\,.$$

Relative to a given basis $\Omega = \{\omega_1, \omega_2, \cdots, \omega_h\}$ of F over K, define the set $\Lambda \subseteq F$ as the collection of all h-vectors over K whose j-th coordinate is restricted to A_j. Note that the cardinality L of Λ is given by $\prod_{j=1}^{h}(r - \delta_j)$. By the linearity of the trace operator, for every $b \in F - \{0\}$, $\mathrm{tr}(b\omega_j) \neq 0$ for at least one ω_j. Furthermore, the same property of $\mathrm{tr}(\cdot)$ implies that $\mathrm{tr}(b\lambda)$ takes each value of K no more than $\dfrac{L}{r - \delta}$ times as λ ranges over Λ.

Given a primitive element $\beta \in F$ and an integer M, $1 \le M \le r-1$, define the set $\Pi[m = M \cdot L;\ 3,\ l = r+1] = \{T_{i,\lambda} \mid 0 \le i \le M-1,\ \lambda \in \Lambda\}$ as follows:

$$T_{i,\lambda} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \beta^i & 0 & \cdots & 0 & 0 \\ \lambda & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, \quad 0 \le i \le M-1, \ \lambda \in \Lambda .$$

Every $\mathbf{u} = (u_0\ u_1\ u_2) \in F^3 - \{\mathbf{0}\}$ defines $M \cdot L$ polynomials $\mathbf{v}_{i,\lambda} = \mathbf{u}T_{i,\lambda}$, given by

$$v_{i,\lambda}(x) = (u_0 + \lambda u_2) + \beta^i u_1 x + u_2 x^r , \quad 0 \le i \le M-1, \ \lambda \in \Lambda . \tag{16}$$

In case either $u_1 = 0$ or $u_2 = 0$, each polynomial in (16) has at most one root in F. When $u_2 \neq 0$ we may assume, without loss of generality, that $u_2 = -1$. By Proposition 1, $\rho(\mathbf{v}_{i,\lambda}) \le 1$ for every i such that $\beta^i u_1$ is not an $(r-1)$-st power in F. Since β is primitive, for a given $\mathbf{u}$ there is at most one value of i such that $\beta^i u_1$ is an $(r-1)$-st power. Therefore, there are at least $(M-1)L$ polynomials in (16) for which $\rho(\mathbf{v}_{i,\lambda}) \le 1$.

It remains to consider the case when $\beta^i u_1 = \gamma^{r-1}$ for some $\gamma \in F - \{0\}$. In this case (16) has r roots if

$$\mathrm{tr}\left(\frac{u_0 + \lambda}{\gamma^r}\right) = \mathrm{tr}\left(\frac{u_0}{\gamma^r}\right) + \mathrm{tr}\left(\frac{\lambda}{\gamma^r}\right) = 0 , \tag{17}$$

and no roots if (17) does not hold. However, as mentioned above, (17) is satisfied by at most $\frac{L}{r-\delta}$ elements $\lambda \in \Lambda$. Therefore,

$$\sum_{i,\lambda} \rho(\mathbf{v}_{i,\lambda}) \le t = (M-1) \cdot L + \frac{r}{r-\delta} L = \left[1 + \frac{\delta}{M(r-\delta)}\right] \cdot M \cdot L \tag{18}$$

$$\triangleq \tau(\delta, r, M) \cdot M \cdot L .$$

It follows that the length of $C(\Gamma)$ satisfies

$$n = M \cdot L \cdot q = \frac{1}{\tau(\delta, r, M)}\ t \cdot q . \tag{19}$$

Since $\lim_{r\to\infty} \tau(\delta, r, M) = 1$, the ratio between the length n, as given in (19), and the bound on n given by (3) approaches unity as r tends to infinity.

This last construction leads to the following asymptotic result.

Theorem 1. *For every real* $\varepsilon, \mu > 0$ *there exists an integer* $r_0(\varepsilon, \mu)$*, such that if* $r \geq r_0(\varepsilon, \mu)$*, where* r *is a power of a prime, then for all* $t \geq \mu q$ *with* $q = r^h$*,* $h > 1$*, there exists an* $[n, 3, n-t]$ *code over* $GF(q)$ *satisfying*

$$n \geq (1-\varepsilon)[(t-1)q + t] .$$

(A similar result for the special case of even h is implied by the constructions given in [3, §2(b)]).

Proof. Referring to the parameters δ_j and M of the construction, set

$$\delta_j = \delta = r - \lfloor r^{1/3} \rfloor , \quad 1 \leq j \leq h ,$$

and $M = r - 1$. This results in a code C_0 of length n_0 and proximity t_0 such that

$$\tau(\delta, r, r-1) = 1 + \frac{\delta}{M(r-\delta)} = 1 + \frac{r - \lfloor r^{1/3} \rfloor}{(r-1)\lfloor r^{1/3} \rfloor} \triangleq 1 + f_1(r) ,$$

where $\lim_{r\to\infty} f_1(r) = 0$. Also,

$$n_0 = \frac{t_0\, q}{\tau(\delta, r, r-1)} \tag{20}$$

and

$$t_0 = \tau(\delta, r, r-1)\,(r-1)\,(r-\delta)^h \leq [1 + f_1(r)]\,(r-1)\,r^{h/3} . \tag{21}$$

Given $\mu > 0$ and a designed proximity $t \geq \mu q$, define nonnegative integers ξ and η such that $t = \xi t_0 + \eta$, $\eta < t_0$. By (21) we have

$$\xi \geq \frac{t}{t_0} - 1 \geq \frac{\mu r^h}{[1 + f_1(r)](r-1)r^{h/3}} - 1$$

which, by $h > 1$, implies

$$\xi \geq \mu\, \frac{r^{\frac{2}{3}h-1}}{1 + f_1(r)} - 1 \geq \mu\, \frac{r^{1/3}}{1 + f_1(r)} - 1 \triangleq \frac{1}{f_2(r, \mu)} ,$$

where $\lim_{r\to\infty} f_2(r, \mu) = 0$.

Now, construct the matrix G by concatenating ξ copies of the generator matrix of C_0. The $[n, 3, n - t']$ code C generated by G satisfies

$$n = \xi n_0 = \xi \frac{1}{\tau(\delta, r, r-1)} t_0 q$$

and

$$t' \le t < t_0(\xi + 1) .$$

Hence, if $t \ge \mu q$ we obtain

$$\frac{n}{t \cdot q} \ge \xi \frac{1}{\tau(\delta, r, r-1)} \cdot \frac{t_0 q}{t_0(\xi+1)q} \ge \frac{1}{1 + f_1(r)} \cdot \frac{1}{1 + 1/\xi}$$

$$\ge \frac{1}{1 + f_1(r)} \cdot \frac{1}{1 + f_2(r, \mu)} ,$$

which yields,

$$\frac{n}{(t-1)q + t} = \frac{1}{1 - 1/t + 1/q} \cdot \frac{n}{t \cdot q} \ge \frac{1}{1 + 1/r^2} \cdot \frac{1}{1 + f_1(r)} \cdot \frac{1}{1 + f_2(r, \mu)} \to 1$$

as r tends to infinity. □

IV. NON-EXISTENCE RESULTS

In this section we show that if $q \ge 8$ then $\rho(\Gamma[2; 3]) = 4$ for all $\Gamma[2; 3]$. Consequently, no $[2q, 3, 2q - 3]$ code can be constructed by concatenating the generator matrices of two extended RS codes when $q \ge 8$. Actually, we prove a stronger result as stated in the following theorem.

Theorem 2. *Let C_1 and C_2 be two three-dimensional MDS codes over $GF(q)$ of lengths n_1 and n_2, respectively. Let C_0 be an $[n = n_1 + n_2, 3, n - t]$ code whose generator matrix is the concatenation of the generator matrices of C_1 and C_2. If $n > \frac{8}{5}(q + 2)$, then the proximity of C_0 is 4.*

The geometric interpretation of this result has been mentioned already in Section I. The proof of Theorem 2 is presented following the next two lemmas.

Lemma 1. (The MacWilliams identities) [5]. *Let C be an $[n, k, d]$ linear code over $GF(q)$ with weight distribution $\{A^{(i)}\}_{i=0}^{n}$ and let $C^{\perp}$ be the dual code with weight distribution $\{B^{(j)}\}_{j=0}^{n}$. Then,*

$$\sum_{i=0}^{n-r} A^{(i)} \binom{n-i}{r} = q^{k-r} \sum_{j=0}^{r} B^{(j)} \binom{n-j}{n-r}, \; r = 0, 1, \cdots, n.$$

Lemma 2. *Let C be an $[n, 3, n-3]$ linear code over $F = GF(q)$ with $n > q+3$. Then, $A^{(n-2)} \le \frac{1}{2}(2q+3-n)n(q-1)$.*

Proof. First, we observe that the generator matrix G of C cannot contain an all-zero column, for its deletion from G would result in an $[n-1, 3, n-3]$ MDS code C' with $n-1 > q+2$, contradicting (3). Hence, each column of G contains at least one nonzero element. Next, we claim that no two columns of G are linearly dependent. For, if G contains such a pair, we may assume, without loss of generality, that the first two columns of G are linearly dependent and that G has the form

$$G = \begin{bmatrix} 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdot & \cdot & \cdots & \cdot & c_1 & c_2 & \cdots & c_w \\ 1 & 1 & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdots & \cdot \end{bmatrix},$$

where $w \ge n-3 > q$. Hence, at least two of the c_i are equal. Therefore, there exists a linear combination of the first two rows of G which yields a codeword containing at least four zeroes, thus implying $t \ge 4$, a contradiction.

Since G serves as a parity-check matrix for $C^{\perp}$ and since no two of its columns are linearly dependent, the minimum distance of $C^{\perp}$ is not smaller than 3. Therefore, if $\{B^{(j)}\}_{j=0}^{n}$ is the weight distribution of $C^{\perp}$, then $B^{(0)} = 1$ and $B^{(1)} = B^{(2)} = 0$. Substituting these values in the MacWilliams

identities for $r = 1, 2$ yields:

$$\sum_{i=n-3}^{n-1} (n-i)A^{(i)} = n(q^2-1)\,,$$

and

$$\sum_{i=n-3}^{n-2} (n-i)(n-i-1)A^{(i)} = n(n-1)(q-1)\,.$$

Eliminating $A^{(n-3)}$ we obtain,

$$A^{(n-2)} + A^{(n-1)} = \frac{1}{2}(2q+3-n)n(q-1)\,.$$

Since $A^{(n-1)} \geq 0$, the lemma follows. □

Proof of Theorem 2. It is known [6, p. 320] that the weight distribution of MDS codes depends only on the code parameters. For $C_j,\ j = 1, 2$, we have

$$A_j^{(n_j-2)} = \frac{1}{2}\, n_j(n_j-1)(q-1)$$

and

$$A_j^{(n_j-1)} = [2n_j + n_j(q-n_j)](q-1)\,.$$

Assume C_0 has proximity 3. Then no codeword of C_1 of weight $n_1 - 2$ can be concatenated with a codeword of C_2 of weight $n_2 - 2$. It follows that

$$A_0^{(n-2)} \geq [A_1^{(n_1-2)} - A_2^{(n_2-1)}] + [A_2^{(n_2-2)} - A_1^{(n_1-1)}] \tag{22}$$

$$= \frac{1}{2}(q-1)[3n_1^2 + 3n_2^2 - (2q+5)(n_1+n_2)]\,.$$

On the other hand, Lemma 2 implies

$$A_0^{(n-2)} \leq \frac{1}{2}(2q+3-n_1-n_2)(n_1+n_2)(q-1)\,. \tag{23}$$

Combining (22) and (23) yields

$$3n_1^2 + 3n_2^2 - (2q+5)(n_1 + n_2) \le (2q+3 - n_1 - n_2)(n_1 + n_2)$$

or,

$$4n^2 - (4q+8)n \le 6n_1(n - n_1) \le \frac{3}{2} n^2 ,$$

obtaining

$$n \le \frac{8}{5}(q+2) . \qquad \square$$

Consider now the set $\Pi[2;3] = \{T_1, T_2\}$. Clearly, $\rho(\Pi[2;3]) = \rho(\{I, T_1^{-1} \cdot T_2\})$, where I is the identity matrix. So it suffices to examine sets of the form $\Gamma = \{I, T\}$. The case $q > 8$ is covered by the preceding theorem since here $\frac{8}{5}(q+2) < 2q$. By (4), $\rho(\Pi[2;3]) \ge 3$ for $3 \le q \le 7$ and there exist examples with $\rho(\Pi[2;3]) = 3$ (see Appendix C). An exhaustive search has shown that $\rho(\{I, T\}) = 4$ when $q = 8$. Therefore, we have

Theorem 3. *Let* $F = GF(q)$. *If* $q \ge 8$, *then* $\rho(\Pi[2;3]) = 4$ *for every set* $\Pi[2;3]$*; if* $q \in \{3, 4, 5, 7\}$, $\rho(\Pi[2;3])$ *is either 3 or 4.*

APPENDIX A

Proposition. *Let* C *be an* $[n, k \geq 2, d = n - t]$ *code over* $F = GF(q)$. *Then,* $n \leq (t - k + 2)\ q + t$.

Proof. By the generalized Griesmer bound ([1],[7]),

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil .$$

Hence,

$$n \geq d + \frac{d}{q} + k - 2$$

or

$$(n - d - k + 2) \cdot q = (t - k + 2) \cdot q \geq d\ . \qquad \square$$

APPENDIX B

Let $F = GF(q) = \{\alpha_j\}_{j=1}^{q}$ where $q = r^2$ and r is a power of an odd prime. For $\gamma \in F$ let $\bar{\gamma}$ be the *conjugate* of γ, i.e., $\bar{\gamma} \triangleq \gamma^{r}$. A *Hermitian curve* in $PG(2, q)$ is the set of all points (u, v, w) satisfying

$$u \cdot \bar{u} + v \cdot \bar{v} + w \cdot \bar{w} = 0 .$$

If we take the points of a Hermitian curve as the columns of a generator matrix, we obtain an $[rq+1, 3, rq-r]$ code C_H over $GF(q)$ [2, §7.3]. We wish to show that the construction given in (15) is not equivalent to C_H. It suffices to show that for all nonsingular 3×3 matrices T over F, the columns of $T \cdot G_0$ are not a subset of a Hermitian curve.

Suppose there exists a nonsingular 3×3 matrix T such that the points

$$\begin{pmatrix} u_j \\ v_j \\ w_j \end{pmatrix} = T \begin{pmatrix} 1 \\ \alpha_j \\ \alpha_j^2 \end{pmatrix}, \quad 1 \le j \le q ,$$

lie on a Hermitian curve. Then,

$$(u_j \; v_j \; w_j) \cdot \begin{pmatrix} \bar{u}_j \\ \bar{v}_j \\ \bar{w}_j \end{pmatrix} = (1 \; \alpha_j \; \alpha_j^2)\, T' \bar{T} \begin{pmatrix} 1 \\ \alpha_j^r \\ \alpha_j^{2r} \end{pmatrix} = 0 , \quad 1 \le j \le q ,$$

where the elements of $\bar{T}$ are the conjugates of those of T. Consider the polynomial

$$P(x) = (1 \;\; x \;\; x^2)\, T' \bar{T} \begin{pmatrix} 1 \\ x^r \\ x^{2r} \end{pmatrix}.$$

Expanding $P(x)$ yields nine terms (some possibly zero), corresponding to the following distinct powers of x: $0, 1, 2, r, r+1, r+2, 2r, 2r+1, 2r+2$, all smaller than r^2. Since $P(\alpha_j) = 0$ for all $1 \le j \le q$, we have $T' \bar{T} = 0$, contradicting the nonsingularity of T.

APPENDIX C

The following are examples of matrices T over $GF(q)$, $3 \le q \le 7$, such that the set $\Gamma[2;3] = \{I, T\}$ has proximity 3:

$GF(3)$:

$$T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

This matrix corresponds to a $[6, 3, 3]$ linear code over $GF(3)$.

$GF(4)$:

$$T = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

This matrix corresponds to an $[8, 3, 5]$ linear code over $GF(4)$.

$GF(5)$:

$$T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

This matrix corresponds to a $[10, 3, 7]$ linear code over $GF(5)$.

$GF(7)$:

$$T = \begin{bmatrix} 0 & 0 & 6 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

This matrix corresponds to a $[14, 3, 11]$ linear code over $GF(7)$.

The binary case was excluded from this paper since, when $k > q$, there is no extended Reed-Solomon code of dimension k; still, construction (1) yields a $[4,3,1]$ code over $GF(2)$ with

$$T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Furthermore, in this case the matrix

$$T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

satisfies $\rho(\{I, T\}) = 2$, thus corresponding to a $[4,3,2]$ MDS code over $GF(2)$.

REFERENCES

[1] J. H. Griesmer, "A bound for error-correcting codes", *IBM Journal*, November 1960, pp. 532-542.

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

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

[4] R. Lidl, H. Niederreiter, *Finite Fields.* Addison-Wesley, Reading, MA, 1983.

[5] F. J. MacWilliams, "A theorem on the distribution of weights in a systematic code", *Bell System Tech. J.*, vol. 42, 1963, pp. 79-94.

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

[7] G. Solomon, J. J. Stiffler, "Algebraically punctured cyclic codes", *Information and Control*, vol. 8, 1965, pp. 116-118.