COMPOSITION OF REED-SOLOMON CODES
AND GEOMETRIC DESIGNS

by

R.M. Roth and A. Lempel

Technical Report #447
February 1987
COMPOSITION OF REED-SOLÔMON CODES
AND GEOMETRIC DESIGNS

RON M. ROTH AND ABRAHAM LEMPEL

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 \( p \) 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 the (Hamming) distance between any two members of \( C \) being at least \( d \) [6]. To shorten notation in the sequel, we define the (maximum) proximity \( t \) of \( C \) as \( t \geq n - d \); 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 \([q-1,1,q-1]\) code generated by the matrix [6, p. 323]

\[
G_{RS} = \begin{bmatrix} g_1 & g_2 & \cdots & g_{q-1} \end{bmatrix},
\]

where the columns of \( G_{RS} \) are of the form

\[
g_i = (1 \ 0 \ \alpha_i^1 \ \alpha_i^2 \ \cdots \ \alpha_i^{q-1}),
\]

with the \( \alpha_i \) 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 \( g_0 = (1 \ 0 \ \cdots \ 0)' \), or both \( g_0 \) and \( g_m = (0 \ 0 \ \cdots \ 0 \ 1)' \), respectively, to \( G_{RS} \).

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

\[
G_0 = \begin{bmatrix} G_{RS} & g_0 \end{bmatrix}.
\]

The construction proposed here employs \( G_0 \) and \( m \) matrices \( T_1, T_2, \ldots, T_m \) over \( F \) such that the code generated by the matrix
\[ G = \begin{bmatrix} T_1G_0 & T_2G_0 & \cdots & T_mG_0 \end{bmatrix} \]  

(1)

has small proximity. To facilitate the analysis of codes generated by (1) we need the following definitions.

Let a polynomial \( v(x) = v_0 + v_1x + \cdots + v_{l-1}x^{l-1}, \ l \geq 1, \) over \( F \) be represented by the vector \( v = (v_0 \ v_1 \ \cdots \ v_{l-1}) \) of its coefficients. For a nonzero polynomial \( v \), let \( \rho(v) \) denote the number of distinct roots of \( v \) in \( F \) and let \( \rho^*(v) \) denote the number of distinct roots of \( v \) in \( F^+ = F \cup \{ \infty \} \), where \( \infty \) is, by definition, a root of \( v \) in \( F^+ \) if \( v_{l-1} = 0 \).

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

\[ \rho(\Gamma[m;k,l]) = \max_{u \in F^k \setminus \{ 0 \}} \left\{ \sum_{i=1}^{m} \rho(uT_i) \right\} . \]

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

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

\[ t = \rho(\Gamma[m;k,l]). \]

(2)

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

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]. 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\(^2\)

$$n \leq (t-k+2)q + t. \quad (3)$$

This bound is useful in obtaining bounds for $\rho(\Gamma)$. Clearly, $\rho(\Gamma[m;1]) = 0$. 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,

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

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

$$m + k - 2 \leq \rho^*(\Gamma[m;k,l]) \leq m \cdot (l-1). \quad (5)$$

For $k = l = 2$, (5) implies $\rho^*(\Gamma[m;2]) = m$. 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, §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.

---

\(^1\) $(n;t)$-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.
We also show that for \( m = 2 \), \( p(\Gamma[2;3]) = 4 \) 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 for sufficiently large \( q \), there exists no \([n,3,n-3]\) code with \( n > \frac{8}{5} q \) 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 \( n > \frac{8}{5} q \), formed by the union of two \((n;2)\)-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

\[
\text{tr}(x) \triangleq x + x^r + x^{r^2} + \cdots + x^{r^{h-1}}.
\]

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

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

\[
\text{tr}(a \alpha + b \beta) = a \text{tr}(\alpha) + b \text{tr}(\beta).
\]

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

\[
\text{tr}(\alpha^r) = \text{tr}(\alpha).
\]

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

Consider the polynomial equation over \( F \):

\[
v(x) \triangleq x^r - ax - b = 0.
\]
It is easy to determine $p(v)$, 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 $p(v) \geq 2$ 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 $b \in F$, $p(v) \leq 1$, 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 (ii), implies

$$\text{tr} \left[ \frac{b}{\gamma^r} \right] = 0.$$  

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 $\alpha$ ranges over $F$, $\alpha^r - a \alpha$ takes values satisfying (7); each such value is obtained exactly $r$ times; and, the set of $r$ $\alpha$'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 $p(v) = r$ or $p(v) = 0$, according to whether $\text{tr} \left[ \frac{b}{a^{1/(r-1)}} \right]$ is zero or nonzero; if $a = 0$ or $a$ is not an $(r-1)$-st power in $F$, $p(v) = 1$. 


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

We shall also consider quadratic equations of the form

\[
x^2 + ax + b = 0
\]

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 \( \Delta \) is a quadratic residue in \( F \); and, no roots if \( \Delta \) is a quadratic nonresidue. To facilitate the investigation of quadratic equations over finite fields of odd characteristic, we present, for later reference, several properties of quadratic residues.

When \( q \) is odd, \( F = GF(q) \) contains \( q^\frac{q-1}{2} \) quadratic (nonzero) residues and the same number of quadratic nonresidues [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 quadratic nonresidues of \( F \) and, for \( \alpha \in F - \{ 0 \} \), let \( \Theta_\alpha \triangleq \{ \alpha + \theta_i \}_{i=1}^{(q-1)/2} \). Then, (i) If \( q \equiv -1 \pmod{4} \), \( \Theta_\alpha \) contains \( \frac{q+1}{4} \) residues; in case \( \alpha \) is a residue, one of the residues in \( \Theta_\alpha \) is zero. (ii) If \( q \equiv 1 \pmod{4} \), \( \Theta_\alpha \) contains \( \frac{q-1}{4} \) nonzero residues; in case \( \alpha \) is a nonresidue, 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 quadratic residue 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 \( \alpha \) and \( b + \beta \) are residues or both are nonresidues. Therefore, if \( b \) ranges over \( K \), \( b + \beta \) takes the value of \( \frac{r-1}{2} \) residues and \( \frac{r+1}{2} \) nonresidues in \( F \). On the other hand, if \( \beta \in K \), then for all \( b \in K \), \( b + \beta \) is a residue 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 quadratic non-residues 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

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

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 $t \leq q + 1$.

A. Codes over Finite Fields of Even Size

Constructions of $(n; t)$-arcs over $F = GF(2^h)$ with $t = 2^s$, $1 \leq s \leq h$, 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 $\text{tr}(x)$ is $GF(2)$.

Let $a \in F$ be such that $\text{tr}(a) = 1$. For $1 \leq s \leq h$, 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 $\Gamma[m = 2^s - 1; 3] \triangleq \{ T_i \}$ by
We claim that \( p^*(r) = 2^s \). To show this, let \( u = (u_0, u_1, u_2) \in F^3 - \{0\} \) and let \( v_i = uT_i, \)
\( 1 \leq i \leq 2^s - 1, \) i.e.,
\[
v_i(x) = (\lambda_i u_0 + au_1) + u_1 x + (u_1 + \lambda_i u_2)x^2, \quad 1 \leq i \leq 2^s - 1. \tag{9}
\]
In case \( u_1 = 0, \rho^*(v_i) \leq 1 \) for each \( i, \) and thus, \( \sum_{i=1}^{2^s-1} p^*(v_i) \leq 2^s - 1. \) Hence, we can assume
\( u_1 \neq 0. \) The discriminant \( \Delta_i \) of (9) is given by
\[
\Delta_i = \text{tr} \left[ \frac{(\lambda_i u_0 + au_1)(u_1 + \lambda_i u_2)}{u_1^2} \right] = \text{tr}(a) + \text{tr} \left[ \frac{u_0 + au_2}{u_1} \right] + \text{tr} \left[ \frac{u_0 u_2}{u_1^2} \right].
\]
Noting that \( \text{tr}(x) = \text{tr}(x^*), \) we obtain
\[
\Delta_i = 1 + \text{tr}(\delta(u) \lambda_i), \quad 1 \leq i \leq 2^s - 1, \tag{10}
\]
where
\[
\delta(u) = \frac{u_0 + au_2 + \sqrt{u_0 u_2}}{u_1}.
\]
Since the trace is a linear operator and the \( \lambda_i \) form a linear subspace of dimension \( s, \) either all or
exactly one half of the \( \lambda_i \) satisfy \( \text{tr}(\delta(u) \lambda_i) = 0. \) Hence, at least \( 2^s - 1 \) of the polynomials \( v_i(x) \)
have no zeroes in \( F. \) Consequently, for each \( u \in F^3 - \{0\}, \sum_{i=1}^{2^s-1} p(v_i) \leq 2^s. \) Furthermore, if
\( u_1 + \lambda_i u_2 = 0 \) for some \( i, v_i, \) being linear, has only one root in \( F \) and, therefore, no more than
two roots in \( F^* = F \cup \{\infty\}. \) This implies \( \sum_{i=1}^{2^s-1} p(v_i) \leq 2^s. \) It follows that the corresponding
code, \( C^*(\Gamma) \) has length \( n = m \cdot (q + 1) = (2^s - 1) \cdot (q + 1) \) and proximity \( t^* = p^*(\Gamma) = 2^s. \) Récall-
ning that when \( u_1 = 0, \sum_{i \geq 1} p(v_i) \leq 2^s - 1, \) 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 $G_\infty$ 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 $(1,0,b)'$ 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 $t = (t_h t_{h-1} \cdots t_1 0)$ be the binary representation of a designed even proximity $t = \sum_{s=1}^{h} t_s 2^s$, $2 \leq t < 2q$, and let $w(t)$ be the (Hamming) weight of $t$. Let $G^*$ be the matrix obtained by concatenating all those generator matrices $G_s^*$ of $C_s^*$ such that $t_s = 1$, $1 \leq s \leq h$. Clearly, the code $C^*$, generated by $G^*$, has proximity $t$ and length

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

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

$$n \geq t \cdot (q + 1) - q \cdot \log_2(t+1), \quad 2 \leq t < 2q .$$

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 \( \{ \theta_i \} \) be the quadratic nonresidues of $F$. Consider the set $\Gamma [m = \frac{q-1}{2}; 3] = \{ T_i \}$, defined by

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

Let $u = (u_0, u_1, u_2) \in F^3 - \{ 0 \}$ and let $v_i = uT_i$, $1 \leq i \leq m$, i.e.,

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

If $u_2 = 0$, $\rho(v_j) \leq 1$ for each $i$ and so $\sum_{i=1}^{\frac{(q-1)^2}{2}} \rho(v_i) \leq \frac{q-1}{2}$. Assume now that $u_2 \neq 0$ and, without loss of generality, that $u_2 = 1$. The discriminant $\Delta_i$ of (13) is given by

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

By Proposition 2, if $q \equiv -1 \pmod{4}$, $\frac{q+1}{4}$ of the $\Delta_i$ are quadratic residues in $F$; and if $q \equiv 1 \pmod{4}$, the number of the nonzero residues does not exceed $\frac{q-1}{4}$. (In the latter case it is also possible that one of the $\Delta_i$ vanishes). Thus, in either case, $\sum_{i=1}^{\frac{(q-1)^2}{2}} \rho(v_i) \leq \frac{q+1}{2}$ 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 $n = m \cdot q + 1 = \frac{1}{2}q(q-1) + 1$. 

Technion - Computer Science Department - Technical Report CS0447 - 1987
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 \( \Gamma \).

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

\[
T_i = \begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
a_i \theta & 0 & 1
\end{bmatrix}, \quad 1 \leq i \leq r.
\]

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

\[
\Delta_i = u_1^2 - 4(u_0 + a_i \theta) \Delta_0 - 4a_i \theta = \theta \left( \frac{\Delta_0}{\theta} - 4a_i \right), \quad 1 \leq i \leq r.
\] (15)

By Proposition 3, the range of \( \Delta_0 / \theta + 4a_i \) as \( a_i \) varies over \( GF(r) \) includes no more than \( \frac{r+1}{2} \) nonresidues of \( F \). Thus, \( \frac{r+1}{2} \) is the maximal number of \( \Delta_i \)'s which are residues and, hence, \( \sum_{i=1}^r \rho(v_i) \leq r + 1 \). An \( [rq+1, 3, r+1] \) code \( \tilde{C} \) 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. Concatenating \( M \) copies of the generator matrix of \( \tilde{C} \) we obtain a code of proximity \( t = M(r+1) \) and length \( n = M(rq + 1) \geq (1 - \frac{1}{r+1})tq \), 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 \( \Gamma[q;3] = \{T_i\} \), where

---

3 Two codes are said to be equivalent if the generator matrix of one is obtained from that of the other by permuting the columns and multiplying each column by a nonzero scalar.
When the columns \((0,1,0)'\) and \(\{(0,1,\beta)'\}_\beta \in F\) 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 \(\Gamma[q-1;3] = \{ T_i \}\), where

\[
T_i = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ b_i & 0 & 1 \end{bmatrix}, \quad 1 \leq i \leq q, \quad \{ b_i \}' = F - \{ 0 \}.
\]

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 \(\{ a_i \}_i = K\) be an ordering on the elements of \(K\). For \(h\) integers \(0 \leq \delta_1 \leq \delta_2 \leq \cdots \leq \delta_h \leq \delta < r\) define the \(h\) sets

\(A_j \triangleq \{ a_i \mid 1 \leq i \leq r - \delta_j \}, \quad 1 \leq j \leq h.\)

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 \(\Lambda\) is given by \(\prod_{j=1}^{h} (r - \delta_j)\). By the linearity of the trace operator, for every \(b \in F - \{ 0 \}, \ tr(b \omega_j) \neq 0\) for at least one \(\omega_j\). Furthermore, the same property of \(tr(\cdot)\) implies that \(tr(b \lambda)\) takes each value of \(K\) no more than \(\frac{L}{r - \delta}\) times as \(\lambda\) ranges over \(\Lambda\).

Given a primitive element \(\beta \in F\) and an integer \(M, 1 \leq M \leq r-1\), define the set \(\Gamma[m = M \cdot L; 3, l = r+1] = \{ T_{i,\lambda} \mid 0 \leq i \leq M - 1, \lambda \in \Lambda \}\) as follows:
Every \( \mathbf{u} = (u_0, u_1, u_2) \in F^3 - \{ 0 \} \) defines \( M \) \( L \) polynomials \( v_{i, \lambda} = uT_{i, \lambda} \), given by

\[
v_{i, \lambda}(x) = (u_0 + \lambda u_2) + \beta^i u_1 x + u_2 x^r, \quad 0 \leq i \leq M-1, \lambda \in \Lambda.
\]

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, \( \rho(v_{i, \lambda}) \leq 1 \) for every \( i \) such that \( \beta^i u_1 \) is not an \( (r-1) \)-st power in \( F \). Since \( \beta \) is primitive, for a given \( u \) 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 \( \rho(v_{i, \lambda}) \leq 1 \).

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

\[
\text{tr} \left[ \frac{u_0 + \lambda}{\gamma^r} \right] = \text{tr} \left[ \frac{u_0}{\gamma^r} \right] + \text{tr} \left[ \frac{\lambda}{\gamma^r} \right] = 0,
\]

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,

\[
\sum_{i, \lambda} \rho(v_{i, \lambda}) \leq t = (M-1) L + \frac{r}{r-\delta} L = \left[ 1 + \frac{\delta}{M(r-\delta)} \right] M \cdot L
\]

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

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

\[
n = M \cdot L \cdot q = \frac{1}{\tau(\delta, r, M)} \cdot t \cdot q.
\]

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 \( \mathbb{GF}(q) \) satisfying

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

(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 \( \delta_j \) 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

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

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

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

and

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

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

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

which, by \( h > 1 \), implies
\[
\xi \geq \mu \left( \frac{2}{r^3} - \frac{1}{1 + f_1(r)} \right) - 1 \geq \mu \left( \frac{r^{1/3}}{1 + f_1(r)} \right) - 1 \geq \frac{1}{f_2(r, \mu)} ,
\]

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

Now, construct the matrix \( G \) by concatenating \( \xi \) 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

\[
t' \leq t < t_0(\xi + 1) .
\]

Hence, if \( t \geq \mu q \) we obtain

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

\[
\geq \frac{1}{1 + f_1(r)} \cdot \frac{1}{1 + f_2(r, \mu)} ,
\]

which yields,

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

as \( r \) tends to infinity. \( \square \)

IV. NON-EXISTENCE RESULTS

In this section we show that if \( q \geq 8 \) 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 \( q \geq 8 \). 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 $[n = n_1 + n_2, d, n-t]$ code whose generator matrix is the concatenation of the generator matrices of $C_1$ and $C_2$. Then, for every real number $a > \frac{8}{5}$, there exists an integer $Q(a)$, such that if $q > Q(a)$ and $n \geq a \cdot q$, the proximity of $C_0$ is $t = 4$.

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,

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

Lemma 2. Let $C$ be an $[n,3,n-3]$ linear code over $F = GF(q)$ with $n > q+3$. Then,

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

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

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

where $w \geq n-3 > q$. 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 \( t \geq 4 \), 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. \( \square \)

**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

\[
A_j^{(n-2)} = \frac{1}{2}n_j(n_j+1)(q-1)
\]

and

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

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
On the other hand, Lemma 2 implies

\[ A_0^{(n-2)} \leq \frac{1}{2} (q - 1)(3n_1^2 + 3n_2^2 - (2q + 5)(n_1 + n_2)) \cdot \]  

Combining (22) and (23), yields

\[ 3n_1^2 + 3n_2^2 - (2q + 5)(n_1 + n_2) \leq (2q + 3 - n_1 - n_2)(n_1 + n_2) . \]

Define \( s_1 = \frac{n_1}{q}, s_2 = \frac{n_2}{q} \), and \( s = \frac{n}{q} = s_1 + s_2 \). Then,

\[ q (2s_1^2 + 2s_2^2 + s_1s_2 - 2s_1 - 2s_2) \leq 4(s_1 + s_2) = 4s . \]

It can be readily verified that the minimum value of the real function \( f (s_1, s_2) \triangleq 2s_1^2 + 2s_2^2 + s_1s_2 - 2(s_1 + s_2) \) under the constraint \( s_1 + s_2 = s \) is attained at

\[ s_1 = s_2 = \frac{s}{2} . \]

Hence,

\[ f (s_1, s_2) \geq f \left( \frac{s}{2}, \frac{s}{2} \right) = \frac{5}{4} s^2 - 2s = \frac{1}{4} s (5s - 8) . \]

Now assume that \( n \geq a \cdot q \). Then, \( s \geq a > \frac{8}{5} \) and

\[ f (s_1, s_2) \geq \frac{1}{4} s (5a - 8) > 0 . \]

Combining (24) and (25), we obtain
Therefore, $q > Q(a)$ implies that the proximity of $C_0$ is 4. □

Consider now the set $\Gamma[2;3] = \{ T_1, T_2 \}$. Clearly, $\rho(\Gamma[2;3]) = \rho(\{ I, T_1^{-1} \cdot T_2 \})$, 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, with $a = 2$, (26) implies $\rho(\Gamma[2;3]) = 4$. By (4), $\rho(\Gamma[2;3]) \geq 3$ for $3 \leq q \leq 7$ and there exist examples with $\rho(\Gamma[2;3]) = 3$ (see Appendix B). An exhaustive search has shown that $\rho(\{ I, T \}) = 4$ when $q = 8$. Therefore, we have

**Theorem 3.** Let $F = GF(q)$. If $q \geq 8$, then $\rho(\Gamma[2;3]) = 4$. For every set $\Gamma[2;3]$, if $q \in \{ 3, 4, 5, 7 \}$, $\rho(\Gamma[2;3])$ 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]),

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

Hence,

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

or

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

\qed
APPENDIX B

The following are examples of matrices $T$ over $GF(q)$, $3 \leq q \leq 7$, 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


