A class of linear codes with good parameters

Xing, Chaoping; Ling, San

2000

Xing, C., & Ling, S. (2000). A class of linear codes with good parameters. IEEE Transactions on Information Theory, 46(6), 2184-2188.

https://hdl.handle.net/10356/96105

https://doi.org/10.1109/18.868488

Correspondence

A Class of Linear Codes with Good Parameters

Chaoping Xing and San Ling

***Abstract*—A construction of linear codes with good parameters is given. Based on Brouwer's table [1], more than 100 new codes are obtained from our construction.**

***Index Terms*—Linear codes, parameters, polynomials.**

I. Introduction

To construct a punctured Reed–Solomon code over the finite field $\boldsymbol{F}_q$, one has to choose a subset S of $\boldsymbol{F}_q$. The resulting codes are *maximum-distance separable* (MDS) codes with the length equal to the cardinality of S. This class of codes have optimal parameters. However, the length of such a code is at most q. Now we ask whether we can choose a subset in some extension of $\boldsymbol{F}_q$ to construct q-ary linear codes by using a method similar to the one used for punctured Reed–Solomon codes. If the answer is positive, we can increase the length of codes dramatically. In this correspondence, we develop the above idea to construct a class of q-ary linear codes by choosing a subset of $\boldsymbol{F}_{q^2}$. Our results show that codes from our construction have nice parameters. These codes have lengths between $(q^2-q)/2$ and $(q^2+q)/2$. Compared with Brouwer's table of the best known codes[1], we find more than 100 new codes, that is, codes that have better parameters than the corresponding codes in Brouwer's table for $q=7, 8$, and 9. In fact, we believe that our codes become better as q increases (our belief will be partially supported by Section III). Unfortunately, for $q>9$, it is difficult to compare our codes with existing codes since Brouwer's table does not contain any q-ary codes for $q>9$. Nevertheless, we still have enough new codes for $q \leq 9$ to illustrate the construction.

This correspondence is arranged as follows. In Section II, we present our construction of linear codes. In the last section, some of our codes are tabulated so that our codes can be compared with Brouwer's table [1].

II. Construction

Let $\boldsymbol{F}_q$ be the finite field with q elements and $\boldsymbol{F}_{q^2}$ the extension over $\boldsymbol{F}_q$ of degree 2.

Before discussing our construction of codes, we recall the construction of punctured Reed–Solomon codes so that the idea of our construction can be presented clearly.

Let N, K be two integers with $1<N\leq q$ and $1\leq K\leq N$, and let P_K be the set of all polynomials in $\boldsymbol{F}_q[x]$ with degree less than K.

Choose a subset $\{\alpha_1,\alpha_2,\ldots,\alpha_N\}$ of $\boldsymbol{F}_q$. Define a punctured Reed–Solomon code by

$$GRS_q(N,K)=\{(f(\alpha_1),f(\alpha_2),\ldots,f(\alpha_N))|f(x)\in P_K\}.$$

The authors are with the Department of Mathematics, National University of Singapore, Singapore 117543 (e-mail: matxcp@nus.edu.sg; matlings@nus.edu.sg).

Communicated by R. M. Roth, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(00)07005-X.

Then $GRS_q(N,K)$ is a q-ary code with parameters $[N,K,N-K+1]$, i.e., $GRS_q(N,K)$ is an MDS code over $\boldsymbol{F}_q$ (for detailed results of punctured Reed–Solomon codes, we refer to [2]).

However, for a subset S of $\boldsymbol{F}_{q^2}$, the code

$$\{(f(\alpha))_{\alpha\in S}|f(x)\in P_K\}$$

is no longer defined over $\boldsymbol{F}_q$ in general. This suggests that we should choose a set V of polynomials in $\boldsymbol{F}_q[x]$ such that $(f(\alpha))_{\alpha\in S}$ is a vector over $\boldsymbol{F}_q$ for all $f(x)\in V$.

From now on in this section, we will discuss our construction. First we list all elements of $\boldsymbol{F}_q$ as

$$\boldsymbol{F}_q=\{\alpha_1,\alpha_2,\ldots,\alpha_q\}.$$

As $\beta^q\neq\beta$ for all $\beta\in\boldsymbol{F}_{q^2}-\boldsymbol{F}_q$, we can list the elements of $\boldsymbol{F}_{q^2}$ as

$$\boldsymbol{F}_{q^2}=\{\alpha_1,\alpha_2,\ldots,\alpha_q,\beta_1,\beta_1^q,\beta_2,\beta_2^q,\ldots,\beta_r,\beta_r^q\}$$

where $r=(q^2-q)/2$.

The following lemma is clear from the Galois theory of finite fields.

Lemma 2.1: For a polynomial $f(x)\in\boldsymbol{F}_q[x]$, $f(\beta_i)=0$ if and only if $f(\beta_i^q)=0$ for all $1\leq i\leq r$.

We distinguish two cases for odd and even q.

A. q is Odd

In this subsection, we assume that q is odd.

For $i,j\geq 0$, let

$$e_{i,j}(x)=x^{qi+j}+x^{qj+i}.$$

Lemma 2.2:

1) $e_{i,j}(\beta)$ is an element of $\boldsymbol{F}_q$ for any $\beta\in\boldsymbol{F}_{q^2}$ and $i,j\geq 0$.
2) For $1\leq m\leq q$, the set $E:=\{e_{i,j}(x)|0\leq i\leq j\leq m-1\}$ is $\boldsymbol{F}_q$-linearly independent.

Proof:

1) This is obvious.
2) It is easy to show that all polynomials have distinct degree. Therefore, they are $\boldsymbol{F}_q$-linearly independent.

For $m\geq 1$, we define the $\boldsymbol{F}_q$-linear space V_m to be the $\boldsymbol{F}_q$-linear span of the set $\{e_{i,j}(x)|0\leq i\leq j\leq m-1\}$, i.e.,

$$V_m=\langle\{e_{i,j}(x)|0\leq i\leq j\leq m-1\}\rangle.$$

Then by Lemma 2.2

$$\dim(V_m)=|\{e_{i,j}(x)|0\leq i\leq j\leq m-1\}|=\frac{1}{2}m(m+1)$$

for $m\leq q-1$. Moreover, for any $\beta\in\boldsymbol{F}_{q^2}$, $f(\beta)$ is an element of $\boldsymbol{F}_q$ for all $f(x)\in V_m$ since $e_{i,j}(\beta)\in\boldsymbol{F}_q$ for all $i,j\geq 0$.

For $0\leq t\leq q$ and $1\leq m\leq q-1$, we define a linear code

$$C_q(t,m)=\{(f(\alpha_1),f(\alpha_2),\ldots,f(\alpha_t),f(\beta_1),f(\beta_2),\ldots,f(\beta_r))|f(x)\in V_m\}.$$

It is obvious that $C_q(t,m)$ is a q-ary linear code with length $n:=t+r=t+(q^2-q)/2$.

Proposition 2.3: For $0 \le t \le q$ and $1 \le m \le q-1$, the dimension of $C_q(t,m)$ is equal to $m(m+1)/2$.

Proof: For $f(x) \in V_m$, put

$$\boldsymbol{c}_f = (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_t), f(\beta_1), f(\beta_2), \ldots, f(\beta_r)).$$

If $\boldsymbol{c}_f = \boldsymbol{0}$, then $\alpha_1, \alpha_2, \ldots, \alpha_t, \beta_1, \beta_2, \ldots, \beta_r$ are roots of $f(x)$. By Lemma 2.1, $\beta_1^q, \beta_2^q, \ldots, \beta_r^q$ are also roots of $f(x)$. Hence $f(x)$ has at least $t+2r$ roots.

Notice the fact that the highest degree of polynomials in V_m is $\deg(e_{m-1,m-1}(x)) = (q+1)(m-1)$. Thus $f(x)$ equals the zero polynomial since

$$t + 2r \ge q^2 - q > (q+1)(q-2) \ge (q+1)(m-1).$$

This implies that the dimension of $C_q(t,m)$ is equal to the dimension of V_m, which is $m(m+1)/2$.

Proposition 2.4: For $0 \le t \le q$ and $1 \le m \le q-1$, the minimum distance d of $C_q(t,m)$ satisfies

$$d \ge n - \frac{1}{2}((q+1)(m-1) + \min\{2(m-1), t\})$$

where n is the length $t + (q^2-q)/2$.

Proof: Let $f(x)$ be an arbitrary nonzero polynomial of V_m. It is sufficient to prove that the weight of $\boldsymbol{c}_f$ is at least

$$n - \frac{1}{2}((q+1)(m-1) + \min\{2(m-1), t\}).$$

To find the weight of $\boldsymbol{c}_f$, we have to count the roots of $f(x)$ among $\{\alpha_1, \alpha_2, \ldots, \alpha_t, \beta_1, \beta_2, \ldots, \beta_r\}$. Let

$$f(x) = \sum_{s=0}^{2(m-1)} \sum_{\substack{i+j=s \\ 0 \le i \le j \le m-1}} a_{i,j} e_{i,j}(x)$$

for some $a_{i,j} \in \boldsymbol{F}_q$.

Case 1:

$$\sum_{\substack{i+j=s \\ 0 \le i \le j \le m-1}} a_{i,j} = 0$$

for all $0 \le s \le 2(m-1)$.

We have

$$\begin{aligned} f(x) &= \sum_{s=0}^{2(m-1)} \sum_{\substack{i+j=s \\ 0 \le i \le j \le m-1}} a_{i,j} e_{i,j}(x) \\ &= \sum_{s=0}^{2(m-1)} \sum_{\substack{i+j=s \\ 0 \le i \le j \le m-1}} a_{i,j} e_{i,j}(x) \\ &\quad - \sum_{s=0}^{2(m-1)} \left(\sum_{\substack{i+j=s \\ 0 \le i \le j \le m-1}} a_{i,j} \right) (x^s + x^{qs}) \\ &= \sum_{s=0}^{2(m-1)} \sum_{\substack{i+j=s \\ 0 \le i \le j \le m-1}} a_{i,j} (x^{qi+j} + x^{qj+i} - x^s - x^{qs}) \\ &= \sum_{s=0}^{2(m-1)} \sum_{\substack{i+j=s \\ 0 \le i \le j \le m-1}} a_{i,j} (x^{qi} - x^i)(x^j - x^{qj}). \end{aligned}$$

Hence $(x^q - x)^2$ is a divisor of $f(x)$. Put

$$g(x) := \frac{f(x)}{(x^q - x)^2} \in \boldsymbol{F}_q[x].$$

Then β_i is a root of $f(x)$ if and only if it is a root of $g(x)$ since $\beta_i^q - \beta_i \ne 0$. Thus $f(x)$ has at most $\deg(g(x))/2$ roots among $\{\beta_1, \beta_2, \ldots, \beta_r\}$, since $g(\beta_i) = 0$ if and only if $g(\beta_i^q) = 0$.

Altogether $f(x)$ has at most $t + \deg(g(x))/2$ roots among $\{\alpha_1, \alpha_2, \ldots, \alpha_t, \beta_1, \beta_2, \ldots, \beta_r\}$. Therefore, the weight of $\boldsymbol{c}_f$ satisfies

$$\begin{aligned} \mathrm{wt}(\boldsymbol{c}_f) &\ge n - \left(t + \frac{1}{2} \deg(g(x)) \right) \\ &\ge n - \left(t + \frac{1}{2}((q+1)(m-1) - 2q) \right) \\ &= n - \frac{1}{2}(q+1)(m-1) + (q-t) \\ &\ge n - \frac{1}{2}((q+1)(m-1) + \min\{2(m-1), t\}). \end{aligned}$$

Case 2:

$$\sum_{\substack{i+j=u \\ 0 \le i \le j \le m-1}} a_{i,j} \ne 0$$

for some $0 \le u \le 2(m-1)$ and

$$\sum_{\substack{i+j=s \\ 0 \le i \le j \le m-1}} a_{i,j} = 0$$

for all $u < s \le 2(m-1)$.

For an element $\alpha \in \boldsymbol{F}_q$, $f(\alpha) = 0$, i.e.,

$$\sum_{s=0}^{2(m-1)} \sum_{\substack{i+j=s \\ 0 \le i \le j \le m-1}} a_{i,j} e_{i,j}(\alpha) = 0$$

which is equivalent to

$$\sum_{s=0}^{2(m-1)} \sum_{\substack{i+j=s \\ i \le j \le m-1}} 2a_{i,j} \alpha^s = 0$$

since

$$e_{i,j}(\alpha) = \alpha^{qi+j} + \alpha^{qj+i} = 2\alpha^{i+j}.$$

Therefore, $f(\alpha) = 0$ is equivalent to

$$\sum_{s=0}^{u} \sum_{\substack{i+j=s \\ i \le j \le m-1}} 2a_{i,j} \alpha^s = 0.$$

This means that an element α of $\boldsymbol{F}_q$ is a root of $f(x)$ if and only if α is a root of the nonzero polynomial

$$\sum_{s=0}^{u} \left(\sum_{\substack{i+j=s \\ i \le j \le m-1}} a_{i,j} \right) x^s.$$

Hence $f(x)$ has at most u roots in $\boldsymbol{F}_q$. Since $u \le 2(m-1)$, $f(x)$ has at most $\min\{2(m-1), t\}$ roots among $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$.

Assume that $f(x)$ has r_1 roots among $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ and r_2 roots among $\{\beta_1, \beta_2, \ldots, \beta_r\}$. Then we have two inequalities

$$\begin{aligned} r_1 &\le \min\{2(m-1), t\} \\ r_1 + 2r_2 &\le \deg(f(x)) \le (q+1)(m-1). \end{aligned}$$

Thus

$$r_1 + r_2 = \frac{1}{2}(r_1 + 2r_2 + r_1) \leq \frac{1}{2}((q+1)(m-1) + \min\{2(m-1), t\}).$$

As $f(x)$ has $r_1 + r_2$ roots among $\{\alpha_1, \alpha_2, \ldots, \alpha_t, \beta_1, \beta_2, \ldots, \beta_r\}$, we get

$$\text{wt}\,(\boldsymbol{c}_f) = n - (r_1 + r_2) \geq n - \frac{1}{2}((q+1)(m-1) + \min\{2(m-1), t\}).$$

This completes the proof.

Combining Propositions 2.3 and 2.4 we obtain

Theorem 2.5: Let q be odd. For $0 \leq t \leq q$ and $1 \leq m \leq q-1$, the code $C_q(t,m)$ is a q-ary $[n,k,d]$ linear code with $n = t + (q^2-q)/2$, $k = m(m+1)/2$ and

$$d \geq n - \frac{1}{2}((q+1)(m-1) + \min\{2(m-1), t\}).$$

The dimension of the code $C_q(t,m)$ is uniquely determined by m. In order to obtain more codes, we want to have another parameter l such that the dimension depends on both m and l.

For $m \geq 2$ and $0 \leq l \leq m-1$, let $V_{m,l}$ be the $\boldsymbol{F}_q$-vector space generated by the set

$$\{e_{i,j}(x) | 0 \leq i \leq j \leq m-2\} \cup \{e_{i,m-1}(x) | 0 \leq i \leq l\}.$$

Then the dimension of $V_{m,l}$ is equal to

$$|\{e_{i,j}(x) | 0 \leq i \leq j \leq m-2\} \cup \{e_{i,m-1}(x) | 0 \leq i \leq l\}| = m(m-1)/2 + l + 1.$$

When $l = m-1$, $V_{m,l}$ is the same as the vector space V_m. In the same manner, we construct q-ary linear codes

$$C_q(t,m,l) = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_t), f(\beta_1), f(\beta_2), \ldots, f(\beta_r)) | f(x) \in V_{m,l}\}.$$

Theorem 2.6: Let q be odd. For $0 \leq t \leq q$, $2 \leq m \leq q-1$, and $0 \leq l \leq m-1$, the code $C_q(t,m,l)$ is a q-ary $[n,k,d]$ linear code with $n = t + (q^2-q)/2$, $k = m(m-1)/2 + l + 1$, and

$$d \geq n - \frac{1}{2}(q(m-1) + l + \min\{\max\{2(m-2), m+l-1\}, t\}).$$

Proof: The results on the length and the dimension are clear. Noting the fact that the highest degree of the polynomials in $V_{m,l}$ is $q(m-1)+l$ and the biggest sum $i+j$ for pairs (i,j) which satisfy $e_{i,j}(x) \in V_{m,l}$ is $\max\{2(m-2), m+l-1\}$, we can easily prove the result on minimum distance by employing exactly the same arguments as in the Proof of Proposition 2.4.

B. q is Even

In this subsection, we assume that q is even.

For $i, j \geq 0$, let

$$e_{i,j}(x) = \begin{cases} x^{q^i+j} + x^{q^j+i}, & \text{if } i \neq j \\ x^{q^i+j}, & \text{if } i = j. \end{cases}$$

Then, as in Lemma 2.2, it can be proven that

$$\{e_{i,j}(x) | 0 \leq i \leq j \leq m-1\}$$

is $\boldsymbol{F}_q$-linearly independent for $1 \leq m \leq q-1$.

Let V_m be the $\boldsymbol{F}_q$-vector space generated by

$$\{e_{i,j}(x) | 0 \leq i \leq j \leq m-1\}.$$

Then

$$\dim(V_m) = \frac{1}{2}m(m+1)$$

for $m \leq q-1$. Moreover, for any $\beta \in \boldsymbol{F}_{q^2}$, $f(\beta)$ are elements of $\boldsymbol{F}_q$ for all $f(x) \in V_m$ since $e_{i,j}(\beta) \in \boldsymbol{F}_q$ for all $i, j \geq 0$.

For $0 \leq t \leq q$ and $1 \leq m \leq q-1$, we define a linear code

$$C_q(t,m) = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_t), f(\beta_1), f(\beta_2), \ldots, f(\beta_r)) | f(x) \in V_m\}$$

as in the case where q is odd. It is obvious that $C_q(t,m)$ is a q-ary linear code with length $n := t + r = t + (q^2-q)/2$.

Proposition 2.7: For $0 \leq t \leq q$ and $1 \leq m \leq q-1$, the dimension of $C_q(t,m)$ is equal to $m(m+1)/2$.

Proof: Exactly as the Proof of Proposition 2.3.

Proposition 2.8: For $0 \leq t \leq q$ and $1 \leq m \leq q-1$, the minimum distance d of $C_q(t,m)$ satisfies

$$d \geq n - \frac{1}{2}((q+1)(m-1) + \max\{2t-q, \min\{m-1, t\}\})$$

where n is the length $t + (q^2-q)/2$.

Proof: Let $f(x)$ be an arbitrary nonzero polynomial of V_m. It is sufficient to prove that the weight of $\boldsymbol{c}_f$ is at least

$$n - \frac{1}{2}((q+1)(m-1) + \max\{2t-q, \min\{m-1, t\}\}).$$

To find the weight of $\boldsymbol{c}_f$, we have to count the roots of $f(x)$ among $\{\alpha_1, \alpha_2, \ldots, \alpha_t, \beta_1, \beta_2, \ldots, \beta_r\}$.

Let

$$f(x) = \sum_{0 \leq i \leq j \leq m-1} a_{i,j} e_{i,j}(x) = \sum_{i=0}^{m-1} a_{i,i} e_{i,i}(x) + \sum_{0 \leq i < j \leq m-1} a_{i,j} e_{i,j}(x)$$

for some $a_{i,j} \in \boldsymbol{F}_q$.

Case 1: $a_{0,0} = a_{1,1} = \cdots = a_{m-1,m-1} = 0$.

Then $f(\alpha) = 0$ for any $\alpha \in \boldsymbol{F}_q$ since for $0 \leq i < j \leq m-1$

$$e_{i,j}(\alpha) = \alpha^{q^i+j} + \alpha^{q^j+i} = 2\alpha^{i+j} = 0.$$

Thus $f(x)$ has at most $(\deg(f(x)) - q)/2$ roots among $\{\beta_1, \beta_2, \ldots, \beta_r\}$. It follows that $f(x)$ has at most $t + (\deg(f(x)) - q)/2$ roots among $\{\alpha_1, \alpha_2, \ldots, \alpha_t, \beta_1, \beta_2, \ldots, \beta_r\}$. Therefore, the weight of $\boldsymbol{c}_f$ satisfies

$$\begin{aligned} \text{wt}\,(\boldsymbol{c}_f) &\geq n - \left(t + \frac{1}{2}(\deg(f(x)) - q)\right) \\ &\geq n - \left(t + \frac{1}{2}((q+1)(m-1) - q)\right) \\ &= n - \frac{1}{2}((q+1)(m-1) + 2t - q) \\ &\geq n - \frac{1}{2}((q+1)(m-1) + \max\{\min\{m-1, t\}, 2t-q\}). \end{aligned}$$

Case 2: $a_{u,u} \neq 0$ for some $u \leq m-1$ and $a_{i,i} = 0$ for all $u < i \leq m-1$.

For an element $\alpha \in \boldsymbol{F}_q$, $f(\alpha) = 0$ is equivalent to

$$\sum_{i=0}^{m-1} a_{i,i} e_{i,i}(\alpha) + \sum_{0 \leq i < j \leq m-1} a_{i,j} e_{i,j}(\alpha) = 0$$

TABLE I
$q = 7$

Theorem	t	m	l	n	k	d	d_B
2.6	1	3	2	22	6	14	13
2.6	3	3	2	24	6	15	14
2.6	3	5	4	24	15	7	6

Theorem	t	m	l	n	k	d	d_B
2.6	7	3	1	28	5	19	18
2.6	7	3	2	28	6	18	17
2.6	7	4	2	28	9	14	13

TABLE II
$q = 8$

Theorem	t	m	l	n	k	d	d_B
2.9	0	2	–	28	3	24	23
2.9	0	4	–	28	10	15	14
2.9	0	6	–	28	21	6	5
2.9	1	3	–	29	6	20	19
2.9	1	5	–	29	15	11	10
2.9	2	4	–	30	10	16	15
2.9	2	6	–	30	21	7	6
2.9	3	5	–	31	15	12	11
2.9	4	6	–	32	21	8	7

Theorem	t	m	l	n	k	d	d_B
2.9	5	3	–	33	6	23	22
2.9	6	4	–	34	10	19	18
2.10	6	5	3	34	14	15	14
2.9	6	5	–	34	15	14	13
2.10	6	6	1	34	17	12	11
2.10	6	6	3	34	19	11	10
2.9	7	6	–	35	21	10	9
2.10	7	7	1	35	23	8	7
2.10	7	7	3	35	25	7	6

i.e.,

$$\sum_{i=0}^{u} a_{i,i}e_{i,i}(\alpha) + \sum_{0\le i<j\le m-1} a_{i,j}e_{i,j}(\alpha) = 0.$$

This is equivalent to

$$\sum_{i=0}^{u} a_{i,i}e_{i,i}(\alpha) = 0 \tag{1}$$

since $e_{i,j}(\alpha) = \alpha^{qi+j} + \alpha^{qj+i} = 2\alpha^{i+j} = 0$ for $i \neq j$.

As $e_{i,i}(\alpha) = \alpha^{qi+i} = \alpha^{2i}$, it follows from (1) that an element α of $\boldsymbol{F}_q$ is a root of $f(x)$ if and only if α is a root of the nonzero polynomial

$$\sum_{i=0}^{u} a_{i,i}x^{2i}.$$

Let $b_i \in \boldsymbol{F}_q$ such that $b_i^2 = a_{i,i}$ for all $0 \le i \le u$. Then

$$\sum_{i=0}^{u} a_{i,i}x^{2i} = \left(\sum_{i=0}^{u} b_i x^i\right)^2.$$

This implies that an element of $\boldsymbol{F}_q$ is a root of $f(x)$ if and only if it is a root of $\sum_{i=0}^{u} b_i x^i$.

Hence $f(x)$ has at most u roots in $\boldsymbol{F}_q$. Since $u \le m-1$, $f(x)$ has at most $\min\{m-1, t\}$ roots among $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$.

Assume that $f(x)$ has r_1 roots among $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ and r_2 roots among $\{\beta_1, \beta_2, \ldots, \beta_r\}$. Then we have the two inequalities

$$r_1 \le \min\{m-1, t\}, r_1 + 2r_2 \le \deg(f(x)) \le (q+1)(m-1).$$

Thus

$$r_1 + r_2 = \frac{1}{2}(r_1 + 2r_2 + r_1) \le \frac{1}{2}((q+1)(m-1) + \min\{m-1, t\}).$$

As $f(x)$ has $r_1 + r_2$ roots among $\{\alpha_1, \alpha_2, \ldots, \alpha_t, \beta_1, \beta_2, \ldots, \beta_r\}$, we get

$$\begin{aligned}\mathrm{wt}(\boldsymbol{c}_f) &= n - (r_1 + r_2) \ge n - \frac{1}{2}((q+1)(m-1) + \min\{m-1, t\}) \\ &\ge n - \frac{1}{2}((q+1)(m-1) + \max\{\min\{m-1, t\}, 2t-q\}).\end{aligned}$$

This completes the proof.

Combining Propositions 2.7 and 2.8, we obtain

Theorem 2.9: Let q be even. For $0 \le t \le q$ and $1 \le m \le q-1$, the code $C_q(t, m)$ is a q-ary $[n, k, d]$ linear code with $n = t + (q^2 - q)/2$, $k = m(m+1)/2$, and

$$d \ge n - \frac{1}{2}((q+1)(m-1) + \max\{\min\{m-1, t\}, 2t-q\}).$$

For $m \ge 2$ and $0 \le l \le m-1$, let $V_{m,l}$ be the $\boldsymbol{F}_q$-vector space generated by the set

$$\{e_{i,j}(x) | 0 \le i \le j \le m-2\} \cup \{e_{i,m-1}(x) | 0 \le i \le l\}.$$

Then the dimension of $V_{m,l}$ is equal to $m(m-1)/2 + l + 1$. When $l = m-1$, $V_{m,l}$ is the same as the vector space V_m. In the same manner, we construct q-ary linear codes

$$C_q(t, m, l) = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_t), f(\beta_1), f(\beta_2), \ldots, f(\beta_r)) | f(x) \in V_{m,l}\}.$$

Theorem 2.10: Let q be even. For $0 \le t \le q$, $2 \le m \le q-1$, and $0 \le l \le m-2$, the code $C_q(t, m, l)$ is a q-ary $[n, k, d]$ linear code with $n = t + (q^2 - q)/2$, $k = m(m-1)/2 + l + 1$, and

$$d \ge n - \frac{1}{2}(q(m-1) + l + \max\{\min\{m-2, t\}, 2t-q\}).$$

Proof: The results on the length and the dimension are clear. Noting the fact that the highest degree of the polynomials in $V_{m,l}$ is $q(m-1)+l$ and the biggest i which satisfies $e_{i,i}(x) \in V_{m,l}$ is $m-2$, we can easily prove the result on minimum distance by employing exactly the same arguments as in the Proof of Proposition 2.8.

III. Tables

In this section, we present tables (Tables I–III) to compare codes from our construction in Section II and codes from Brouwer's table [1]. These tables show more than 100 new codes (including codes obtained from our tables in obvious ways) compared with Brouwer's table. Of course it is not definitely certain that all of the codes in our tables are new codes since some best known codes might not be contained in Brouwer's table.

We need to explain the symbols in our tables. For odd q, Theorem 2.5 is a special case of Theorem 2.6 where l is equal to $m-1$. Hence

TABLE III
$q = 9$

Theorem	t	m	l	n	k	d	d_B
2.6	1	3	2	37	6	27	25
2.6	1	4	3	37	10	22	20
2.6	1	5	4	37	15	17	16
2.6	1	6	5	37	21	12	11
2.6	1	7	6	37	28	7	6
2.6	3	3	2	39	6	28	26
2.6	3	4	3	39	10	23	22
2.6	3	5	4	39	15	18	17
2.6	3	6	5	39	21	13	12
2.6	3	7	6	39	28	8	7

Theorem	t	m	l	n	k	d	d_B
2.6	5	4	3	41	10	24	23
2.6	5	7	6	41	28	9	8
2.6	7	5	4	43	15	20	19
2.6	7	6	5	43	21	15	14
2.6	9	3	2	45	6	33	31
2.6	9	4	1	45	8	29	28
2.6	9	4	2	45	9	28	27
2.6	9	4	3	45	10	27	26
2.6	9	6	5	45	21	16	15
-	-	-	-	-	-	-	-

we just use Theorem 2.6 in our tables. However, for even q, Theorem 2.10 does not include the case where $l = m - 1$, i.e., the result of Theorem 2.9 is not contained in Theorem 2.10.

t, m paramters in Theorems 2.6, 2.9, or 2.10.
l parameter in Theorems 2.6 or 2.10.
n, k length and dimension of codes, respectively, obtained from Theorems 2.6, 2.9, or 2.10 with given parameters t, m, l.
d lower bounds on minimum distance of codes obtained from Theroems 2.6, 2.9, or 2.10 with given parameters t, m, l.
d_B the lower bound on minimum distance of codes with given length n and dimension k quoted from Brouwer's table [1].

Remark 3.1: Besides codes directly coming from our construction, many new codes can be obtained from some codes in our tables in obvious ways. For example, in the table for $q = 7$, there is a 7-ary $[28, 6, 18]$ linear code, lengthening the code gives a new $[29, 6, 18]$ code.

ACKNOWLEDGMENT

The authors wish to thank two referees for their helpful comments on the earlier version of the correspondence. Special thanks go to one of the referees for very useful and detailed suggestions.

REFERENCES

[1] A. Brouwer. Bounds on the minimum distance of linear code. [Online]. Available: http://www.win.tue/nl/~aeb/voorlincod.html
[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
[3] M. A. Tsafasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*. Dordrecht, The Netherlands: Kluwer, 1991.