A class of linear codes with good parameters from algebraic curves

Xing, Chaoping; Ling, San

2000

Xing, C., & Ling, S. (2000). A class of linear codes with good parameters from algebraic curves. *IEEE Transactions on Information Theory*, 46(4), 1527-1532.

<https://hdl.handle.net/10356/79954>

<https://doi.org/10.1109/18.850687>

© 2000 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at:
<http://dx.doi.org/10.1109/18.850687>.

Downloaded on 26 Apr 2023 12:34:26 SGT

A Class of Linear Codes with Good Parameters from Algebraic Curves

Chaoping Xing and San Ling

Abstract—A class of linear codes with good parameters is constructed in this correspondence. It turns out that linear codes of this class are subcodes of the subfield subcodes of Goppa's geometry codes. In particular, we find 61 improvements on Brouwer's table [1] based on our codes.

Index Terms—Algebraic curves, algebraic-geometry codes, subfield subcodes.

I. INTRODUCTION

Algebraic-geometry codes constructed by Goppa [2] make use of algebraic curves with many rational points. These codes have excellent asymptotic parameters. In particular, the q -ary Gilbert–Varshamov bound was broken by Goppa's geometric codes for some sufficiently large q [8], [3].

However, for small q , it seems difficult to find many good codes by Goppa's construction. The reason is that the number of rational points of an algebraic curve over $\mathbf{F}_q$ is not satisfactory to construct good Goppa's geometric codes for small q . In order to increase the length of geometric codes, researchers have been looking for possibilities to use points over some extensions of $\mathbf{F}_q$ to construct good codes [5], [10], [11], [4], [12]. In this correspondence, we make use of curves defined over some extension of $\mathbf{F}_q$ to construct codes over $\mathbf{F}_q$ with larger length. It turns out that codes constructed in this way are subcodes of the subfield subcode of Goppa's geometric codes. It is well known that one cannot expect any good results if we just use a general lower bound (see (1) of Section II) to estimate dimensions of subfield subcodes of algebraic-geometry codes. However, by using our explicit construction, we can determine dimensions of our codes that exceed the lower bound (1) of Section II on dimensions of subfield subcodes. Consequently, we obtain some linear codes with good parameters. In particular, 61 improvements on Brouwer's table are found for $q = 8$ and 9 by using elliptic curves.

The correspondence is organized as follows. In Section II, we introduce Goppa's construction of algebraic-geometry codes and a general lower bound on dimensions of subfield subcodes. Section III is devoted to construction of a class of linear codes that are subcodes of subfield subcodes of algebraic-geometry codes. Parameters of these codes are estimated in this section. Finally, in Section IV, we list some improvements on Brouwer's table based on the codes of Section III.

II. BACKGROUND

In this section, we briefly introduce Goppa's geometric codes and subfield subcodes.

Let r be a prime power and $\mathcal{X}$ a projective, absolutely irreducible, complete algebraic curve over $\mathbf{F}_r$ (we simply express this fact by saying that $\mathcal{X}/\mathbf{F}_r$ is an algebraic curve). Let $\mathbf{F}_r(\mathcal{X})$ be the function field of $\mathcal{X}/\mathbf{F}_r$. For a divisor G (we always mean a rational divisor whenever a divisor is mentioned in this correspondence) of $\mathcal{X}/\mathbf{F}_r$, the linear space

$$\mathcal{L}(G) = \{f \in \mathbf{F}_r(\mathcal{X}) - \{0\} \mid \text{div}(f) + G \geq 0\} \cup \{0\}$$

is a finite-dimensional linear space over $\mathbf{F}_r$. Moreover, by the Riemann–Roch theorem [6], [7] have

$$\ell(G) := \dim \mathcal{L}(G) \geq \deg(G) + 1 - g$$

where g is the genus of $\mathcal{X}$. The equality holds if $\deg(G) \geq 2g - 1$.

Let $P_1, P_2, \dots, P_n$ be n distinct rational points of $\mathcal{X}$ satisfying

$$\text{Supp}(G) \cap \{P_1, P_2, \dots, P_n\} = \emptyset.$$

We denote by $C(P_1, P_2, \dots, P_n; G)$ the set

$$C(P_1, P_2, \dots, P_n; G) = \{(f(P_1), f(P_2), \dots, f(P_n)) \mid f \in \mathcal{L}(G)\}.$$

It is clear that $C(P_1, P_2, \dots, P_n; G)$ is a linear code over $\mathbf{F}_r$. Furthermore, we have

Proposition 2.1 (Goppa): Let $\mathcal{X}/\mathbf{F}_r$ be an algebraic curve with n distinct points $\{P_1, P_2, \dots, P_n\}$. Suppose G is a divisor of $\mathcal{X}$ with $\text{Supp}(G) \cap \{P_1, P_2, \dots, P_n\} = \emptyset$ and $\deg(G) < n$. Then $C(P_1, P_2, \dots, P_n; G)$ is an $[n, k, d]$ linear code over $\mathbf{F}_r$ with

$$k = \ell(G) \geq \deg(G) + 1 - g \quad d \geq n - \deg(G).$$

Next we introduce a general lower bound on dimensions of subfield subcodes of linear codes.

Let $r = q^s$ for some prime power q and a positive integer s . Suppose that C is a linear code over $\mathbf{F}_r$ with parameters $[N, K, D]$. Consider the intersection

$$C|_{\mathbf{F}_q} := C \cap \mathbf{F}_q^N.$$

It is clear that $C|_{\mathbf{F}_q}$ is a linear code over $\mathbf{F}_q$. It is called the subfield subcode of C . $C|_{\mathbf{F}_q}$ has length N and distance of at least D .

Lemma 2.2 (see [6], [7]): If C is a linear code over $\mathbf{F}_r = \mathbf{F}_{q^s}$ with parameters $[N, K, D]$, then $C|_{\mathbf{F}_q}$ is a linear code over $\mathbf{F}_q$ with parameters $[N, k, d]$ satisfying $d \geq D$ and

$$k \geq sK - (s - 1)N. \quad (1)$$

III. CONSTRUCTIONS

In this section, we construct a class of linear codes over $\mathbf{F}_q$ based on curves over $\mathbf{F}_{q^2}$. In fact, codes constructed in this section are subcodes of subfield subcodes of algebraic-geometry codes over $\mathbf{F}_{q^2}$.

First we fix some notations for this section.

q	a prime power;
$\mathcal{X}/\mathbf{F}_{q^2}$	an algebraic curve;
$g := g(\mathcal{X})$	the genus of $\mathcal{X}/\mathbf{F}_{q^2}$;
$\mathbf{F}_{q^2}(\mathcal{X})$	the function field of $\mathcal{X}/\mathbf{F}_{q^2}$;
$\mathcal{X}(\mathbf{F}_{q^2})$	the set of $\mathbf{F}_{q^2}$ -rational points of $\mathcal{X}$.

We label the elements of $\mathcal{X}(\mathbf{F}_{q^2})$ as $P_0, P_1, \dots, P_n$, where $n = |\mathcal{X}(\mathbf{F}_{q^2})| - 1$.

For $m \geq g$, we have $\ell(mP_0) \geq m + 1 - g \geq 1$ by the Riemann–Roch theorem. Therefore, we can find $m + 1 - g$ nongaps $0 = v_1 < v_2 < \dots < v_{m+1-g} \leq m$ of P_0 , i.e., there exist $m + 1 - g$ functions $f_1, f_2, \dots, f_{m+1-g}$ of $\mathcal{L}(mP_0)$ such that

$$\nu_{P_0}(f_i) = -v_i \quad (2)$$

Manuscript received July 23, 1999; revised February 14, 2000. This work was supported under the NUS Grant R-146-000-018-112.

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

Communicated by I. F. Blake, Associate Editor for Coding Theory.

for all $1 \leq i \leq m+1-g$, where ν_{P_0} denotes the normalized discrete valuation of P_0 . Since v_i are strictly increasing, we obtain

$$v_i \leq v_{m+1-g} - ((m+1-g) - i) \leq m - (m+1-g-i) = g+i-1. \quad (3)$$

Put

$$e_{ij} = f_i^q f_j + f_i f_j^q$$

for all $1 \leq i < j \leq m+1-g$, and

$$e_{ii} = f_i^{q+1}$$

for all $1 \leq i \leq m+1-g$.

Choose an element γ of $\mathbf{F}_{q^2} - \mathbf{F}_q$ and put

$$e'_{ij} = \gamma^q f_i^q f_j + \gamma f_i f_j^q$$

for all $1 \leq i < j \leq m+1-g$.

Lemma 3.1: For any $\mathbf{F}_{q^2}$ -rational point $P \neq P_0$ of $\mathcal{X}/\mathbf{F}_{q^2}$, both $e_{ij}(P)$ and $e'_{ij}(P)$ are elements of $\mathbf{F}_q$ for all i, j .

Proof: It is clear that P_0 is the unique possible pole of e_{ij} and e'_{ij} . Therefore, $e_{ij}(P)$ and $e'_{ij}(P)$ are well defined.

Considering

$$\begin{aligned} e_{ij}(P)^q &= (f_i^q(P)f_j(P) + f_i(P)f_j^q(P))^q \\ &= f_i^{q^2}(P)f_j^q(P) + f_i^q(P)f_j^{q^2}(P) \\ &= f_i(P)f_j^q(P) + f_i^q(P)f_j(P) \\ &= e_{ij}(P) \end{aligned}$$

and

$$\begin{aligned} e'_{ij}(P)^q &= (\gamma^q f_i^q(P)f_j(P) + \gamma f_i(P)f_j^q(P))^q \\ &= \gamma^{q^2} f_i^{q^2}(P)f_j^q(P) + \gamma^q f_i^q(P)f_j^{q^2}(P) \\ &= \gamma f_i(P)f_j^q(P) + \gamma^q f_i^q(P)f_j(P) \\ &= e'_{ij}(P) \end{aligned}$$

for all $1 \leq i < j \leq m+1-g$, and

$$e_{ii}(P)^q = (f_i^{q+1}(P))^q = f_i^{q^2+q}(P) = f_i^{q+1}(P) = e_{ii}(P)$$

for all $1 \leq i \leq m+1-g$, we find that both $e_{ij}(P)$ and $e'_{ij}(P)$ are elements of $\mathbf{F}_q$ for all i, j .

Let U_m be the $\mathbf{F}_q$ -linear span of the set

$$\{e_{ij} | 1 \leq i \leq j \leq m+1-g\} \cup \{e'_{ij} | 1 \leq i < j \leq m+1-g\}.$$

Lemma 3.2: The dimension of the $\mathbf{F}_q$ -linear space U_m is equal to $(m+1-g)^2$ if $m < q$.

Proof: Since the cardinality of the set

$$\{e_{ij} | 1 \leq i \leq j \leq m+1-g\} \cup \{e'_{ij} | 1 \leq i < j \leq m+1-g\}$$

is equal to $(m+1-g)^2$, we have to prove that these $(m+1-g)^2$ elements are $\mathbf{F}_q$ -linearly independent.

First, for $1 \leq i < j \leq m+1-g$, we have

$$\nu_{P_0}(f_i^q f_j) = -qv_i - v_j > -qv_j - v_i = \nu_{P_0}(f_i f_j^q).$$

Therefore, both e_{ij} and e'_{ij} are nonzero functions for all i, j .

Suppose

$$\sum_{1 \leq i \leq j \leq m+1-g} a_{ij} e_{ij} + \sum_{1 \leq i < j \leq m+1-g} a'_{ij} e'_{ij} = 0 \quad (4)$$

for some $a_{ij}, a'_{ij} \in \mathbf{F}_q$.

Rewrite (4) into the form

$$\sum_{1 \leq i < j \leq m+1-g} (a_{ij} e_{ij} + a'_{ij} e'_{ij}) + \sum_{i=1}^{m+1-g} a_{ii} e_{ii} = 0$$

i.e.,

$$\begin{aligned} \sum_{1 \leq i < j \leq m+1-g} ((a_{ij} + a'_{ij} \gamma^q) f_i^q f_j + (a_{ij} + a'_{ij} \gamma) f_i f_j^q) \\ + \sum_{i=1}^{m+1-g} a_{ii} f_i^{q+1} = 0. \end{aligned}$$

Noting the following three facts:

i) for all $1 \leq i < j \leq m+1-g$, $a_{ij} = a'_{ij} = 0$ (this is equivalent to

$$(a_{ij} + a'_{ij} \gamma^q) f_i^q f_j + (a_{ij} + a'_{ij} \gamma) f_i f_j^q = 0$$

since

$$\nu_{P_0}(f_i^q f_j) = -(qv_i + v_j) > -(qv_j + v_i) = \nu_{P_0}(f_i f_j^q)$$

and $1, \gamma$ are $\mathbf{F}_q$ -linearly independent), or

$$\nu_{P_0}((a_{ij} + a'_{ij} \gamma^q) f_i^q f_j + (a_{ij} + a'_{ij} \gamma) f_i f_j^q) = -(qv_j + v_i);$$

ii) for $1 \leq i \leq m+1-g$, $a_{ii} = 0$ or $\nu_{P_0}(a_{ii} f_i^{q+1}) = -(q+1)v_i$; and

iii) if $1 \leq i \leq j \leq m+1-g$ and $1 \leq u \leq w \leq m+1-g$ satisfy

$$-(qv_j + v_i) = -(qv_w + v_u) \quad (5)$$

then $(i, j) = (u, w)$ (Suppose $-(qv_j + v_i) = -(qv_w + v_u)$. Then $q(v_j - v_w) = v_u - v_i$. Hence $v_u - v_i \equiv 0 \pmod{q}$. By the condition $m < q$, we have $0 \leq v_i, v_u \leq m < q$. It follows that $v_i = v_u$, i.e., $i = u$. This yields $v_j = v_w$ by (5), i.e., $j = w$);

we find that all a_{ij}, a'_{ij} are equal to zero. This completes the proof.

We construct a code as follows:

$$C_m = \{(f(P_1), f(P_2), \dots, f(P_n)) | f \in U_m\}.$$

This code is defined over $\mathbf{F}_q$ by Lemma 3.1 and it is clear that C_m is a linear code of length n .

Looking at

$$\begin{aligned} \min\{\nu_{P_0}(e_{ij}) | 1 \leq i \leq j \leq m+1-g\} \\ = \min\{-(qv_j + v_i) | 1 \leq i \leq j \leq m+1-g\} \\ = -(qv_{m+1-g} + v_{m+1-g}) \geq -m(q+1) \end{aligned}$$

and

$$\begin{aligned} \min\{\nu_{P_0}(e'_{ij}) | 1 \leq i < j \leq m+1-g\} \\ = \min\{-(qv_j + v_i) | 1 \leq i < j \leq m+1-g\} \\ = -(qv_{m+1-g} + v_{m-g}) \geq -m(q+1) + 1 \end{aligned}$$

we find that all e_{ij}, e'_{ij} are elements of $\mathcal{L}(m(q+1)P_0)$, i.e., U_m is a subset of $\mathcal{L}(m(q+1)P_0)$. Hence, C_m is a subcode of the subfield subcode

$$C(P_1, P_2, \dots, P_n; m(q+1)P_0)_{\mathbf{F}_q}.$$

Theorem 3.3: Let $\mathcal{X}/\mathbf{F}_{q^2}$ be an algebraic curve of genus g with $n+1$ rational points $P_0, P_1, \dots, P_n$. Suppose $g \leq m < \min\{q, n/(q+1)\}$. Then C_m is an $[n, (m+1-g)^2, d]$ linear code over $\mathbf{F}_q$ with

$$d \geq n - m(q+1).$$

Proof: We can directly show the result on the minimum distance. However, since C_m is a subcode of the subfield subcode $C(P_1, P_2, \dots, P_n; m(q+1)P_0)|_{\mathbf{F}_q}$ and $n > \deg(m(q+1)P_0)$, it follows from Proposition 2.1 that

$$d = d(C_m) \geq C(P_1, P_2, \dots, P_n; m(q+1)P_0)|_{\mathbf{F}_q} \geq n - m(q+1).$$

In order to show that the dimension of C_m is equal to $(m+1-g)^2$, it is sufficient to show that the map

$$U_m \rightarrow \mathbf{F}_q^n, \quad f \mapsto (f(P_1), f(P_2), \dots, f(P_n))$$

is injective since $\dim_{\mathbf{F}_q}(U_m) = (m+1-g)^2$ by Lemma 3.2. Suppose $f \in U_m$ satisfies $(f(P_1), f(P_2), \dots, f(P_n)) = \mathbf{0}$, i.e.,

$$f \in \mathcal{L}(m(q+1)P_0 - \sum_{i=1}^n P_i).$$

Then, $f = 0$ as

$$\deg(m(q+1)P_0 - \sum_{i=1}^n P_i) < 0.$$

The proof is complete.

Remark: Since C_m is a subcode of $C(P_1, P_2, \dots, P_n; m(q+1)P_0)|_{\mathbf{F}_q}$, we have

$$\begin{aligned} \dim_{\mathbf{F}_q}(C(P_0, P_1, \dots, P_n; m(q+1)P_0)|_{\mathbf{F}_q}) \\ \geq \dim_{\mathbf{F}_q}(C_m) = (m+g-1)^2. \end{aligned} \quad (6)$$

On the other hand, applying the lower bound (1) in Section II, we only get

$$\begin{aligned} \dim_{\mathbf{F}_q}(C(P_0, P_1, \dots, P_n; m(q+1)P_0)|_{\mathbf{F}_q}) \\ \geq 2\ell(m(q+1)P_0) - n \\ \geq 2(m(q+1) + 1 - g) - n. \end{aligned} \quad (7)$$

For small genus g , bound (6) is obviously better than bound (7). For instance, taking $g = 0$ gives

$$\begin{aligned} (m+1-g)^2 - (2(m(q+1) + 1 - g) - n) \\ = (m+1)^2 - (2(m(q+1) + 1 - q^2)) \\ = (q-m)^2 - 1, \end{aligned}$$

and taking an elliptic curve over $\mathbf{F}_{q^2}$ with $q^2 + 2q + 1$ rational points (such an elliptic curve exists [9]) gives

$$\begin{aligned} (m+1-g)^2 - (2(m(q+1) + 1 - g) - n) \\ = m^2 - (2(m(q+1) - q^2 - 2q)) \\ = (q-m)(q-m+2). \end{aligned}$$

Corollary 3.4: If $1 \leq m < q$, then there exist

- 1) a $[q^2, (m+1)^2, d \geq q^2 - m(q+1)]$ linear code over $\mathbf{F}_q$, and
- 2) a $[q^2 + 2q, m^2, d \geq q^2 + 2q - m(q+1)]$ linear code over $\mathbf{F}_q$.

Proof:

- 1) Consider the projective line $\mathcal{X}$ over $\mathbf{F}_{q^2}$. Then

$$n = |\mathcal{X}(\mathbf{F}_{q^2})| - 1 = q^2.$$

By Theorem 3.3, there exists a $[q^2, (m+1)^2, d \geq q^2 - m(q+1)]$ linear code over $\mathbf{F}_q$.

- 2) Consider an elliptic curve $\mathcal{X}$ over $\mathbf{F}_{q^2}$ with $q^2 + 2q + 1$ rational points. Then

$$n = |\mathcal{X}(\mathbf{F}_{q^2})| = q^2 + 2q.$$

By Theorem 3.3, there exists a $[q^2 + 2q, m^2, d \geq q^2 + 2q - m(q+1)]$ linear code over $\mathbf{F}_q$.

For the code C_m , its dimension is uniquely determined by m . In order to obtain more codes, we add another parameter l to control the dimension.

For $1 \leq m \leq q$ and $1 \leq l \leq m - g$, let U_{ml} be the $\mathbf{F}_q$ -linear span of the set

$$\begin{aligned} &\{e_{ij} | 1 \leq i \leq j \leq m - g\} \\ &\cup \{e'_{ij} | 1 \leq i < j \leq m - g\} \\ &\cup \{e_{1,m+1-g}, e_{2,m+1-g}, \dots, e_{l,m+1-g}\} \\ &\cup \{e'_{1,m+1-g}, e'_{2,m+1-g}, \dots, e'_{l,m+1-g}\}. \end{aligned}$$

It is clear by the proof of Lemma 3.2 that the dimension of U_{ml} is equal to $(m-g)^2 + 2l$.

Define the code

$$C_{ml} = \{(f(P_1), f(P_2), \dots, f(P_n)) | f \in U_{ml}\}.$$

Then C_{ml} is a subcode of the subfield subcode

$$C(P_1, P_2, \dots, P_n; (qm + g + l - 1)P_0)|_{\mathbf{F}_q}$$

since

$$\begin{aligned} \min\{\nu_{P_0}(f) | f \in U_{ml}\} &= \nu_{P_0}(e_{l,m+1-g}) \\ &= -qv_{m+1-g} - v_l \\ &\geq -qm - (g + l - 1) \\ &= -qm - g - l + 1. \end{aligned}$$

Therefore, by Proposition 2.1 the minimum distance of C_{ml} is at least $n - qm - g - l + 1$ if $n > qm + g + l - 1$. In the case where $l = 1$, we have a better result on minimum distance, namely,

$$d(C_{m1}) \geq n - qm.$$

This is because C_{m1} is a subcode of $C(P_1, P_2, \dots, P_n; qmP_0)$ since

$$\begin{aligned} \min\{\nu_{P_0}(f) | f \in U_{m1}\} &= \nu_{P_0}(e_{1,m+1-g}) \\ &= -qv_{m+1-g} - v_1 \geq -qm. \end{aligned}$$

Theorem 3.5: If $g \leq m < \min\{q+1, n/(q+1)\}$ and $1 \leq l \leq m - g$, then C_{ml} is an $[n, (m-g)^2 + 2l, d]$ linear code over $\mathbf{F}_q$ with

$$d \geq \begin{cases} n - (qm + v_l) \geq n - (qm + l + g - 1), & \text{if } 2 \leq l \leq m - g \\ n - qm, & \text{if } l = 1. \end{cases}$$

Proof: From the above analysis, we know that the result on the minimum distance is true. As in the proof of Theorem 3.3, it is easy to show that the dimension of C_{ml} is equal to the dimension of U_{ml} , i.e.,

$$\dim_{\mathbf{F}_q}(C_{ml}) = (m-g)^2 + 2l.$$

Corollary 3.6:

- 1) If $1 \leq m \leq q$ and $1 \leq l \leq m$, then there exists a $[q^2, m^2 + 2l, d]$ linear code with $d \geq q^2 - qm - l + 1$.
- 2) If $1 \leq m \leq q$ and $1 \leq l \leq m - 1$, then there exists a $[q^2 + 2q, (m-1)^2 + 2l, d]$ linear code with

$$d \geq \begin{cases} q^2 + 2q - qm - l, & \text{if } 2 \leq l \leq m - 1 \\ q^2 + 2q - qm, & \text{if } l = 1. \end{cases}$$

Proof: Considering the projective line over $\mathbf{F}_{q^2}$ and an elliptic curve over $\mathbf{F}_{q^2}$ with $q^2 + 2q + 1$ rational points, respectively, yields the desired result by Theorem 3.5.

For the code C_m , the length is equal to $|\mathcal{X}(\mathbf{F}_{q^2})| - 1$. In fact, we can increase the length by one if a certain divisor exists.

We only discuss this idea for elliptic curves over $\mathbf{F}_{q^2}$ with $q^2 + 2q + 1$ rational points though it can be extended to arbitrary curves.

Lemma 3.7: Let $\mathcal{X}/\mathbf{F}_{q^2}$ with $q \geq 4$ be an elliptic curve of $q^2 + 2q + 1$ rational points and P_0 be a fixed rational point. Then for any rational point $P \in \mathcal{X}(\mathbf{F}_{q^2})$, there exists a closed point Q_P of degree 2 such that $Q_P - P_0 - P$ is a principal divisor.

Proof: By the Riemann–Roch theorem, one has $\ell(P + P_0) = 2$. Thus there are $((q^2)^2 - 1)/(q^2 - 1) = q^2 + 1$ positive divisors equivalent to $P_0 + P$. Since $g(\mathcal{X}) = 1$, $\mathcal{X}(\mathbf{F}_{q^2})$ forms an Abelian group isomorphic to the divisor class group of degree 0 of $\mathcal{X}$. Therefore, the set

$$S := \{R \in \mathcal{X}(\mathbf{F}_{q^2}) | 2R \sim P_0 + P\}$$

has at most four elements. For any rational point $P' \in \mathcal{X}(\mathbf{F}_{q^2})$, there is a unique rational point P'' such that $P' + P'' \sim P + P_0$. Hence the number of positive divisors D with $D \sim P + P_0$ and

$$\text{Supp}(D) \cap \mathcal{X}(\mathbf{F}_{q^2}) \neq \emptyset$$

is equal to

$$|S| + \frac{|\mathcal{X}(\mathbf{F}_{q^2})| - |S|}{2} = \frac{(q^2 + 2q + 1 + |S|)}{2} \leq \frac{q^2 + 2q + 5}{2}$$

that is less than $q^2 + 1$ as $q \geq 4$. This implies that there is a closed point Q_P of degree 2 equivalent to $P + P_0$, i.e., $Q_P - P - P_0$ is principal.

Lemma 3.8: Let $\mathcal{X}/\mathbf{F}_{q^2}$ be an elliptic curve with $q^2 + 2q + 1$ rational points. If $4 \leq m < q$, then there exists a function $h_m \in \mathbf{F}_{q^2}(\mathcal{X})$ such that the zero divisor of h_m is

$$(h_m)_0 := \sum_{\nu_P(h_m) > 0} \nu_P(h_m)P = mP_0$$

and the pole divisor

$$(h_m)_\infty := - \sum_{\nu_P(h_m) < 0} \nu_P(h_m)P$$

satisfies

$$\text{Supp}((h_m)_\infty) \cap \mathcal{X}(\mathbf{F}_{q^2}) = \emptyset.$$

Proof: Choose a place T of degree $m - 2 \geq 2$. Then there exists a rational point P of $\mathcal{X}$ such that $P_0 - P$ is equivalent to $T - (m - 2)P_0$ since $\mathcal{X}(\mathbf{F}_{q^2})$ is isomorphic to the class group of $\mathcal{X}$. Let Q_P be a closed point of degree 2 of $\mathcal{X}$ such that $Q_P \sim P_0 + P$ (this is possible by Lemma 3.7), then $2P_0 - Q_P \sim P_0 - P$. Hence

$$2P_0 - Q_P \sim T - (m - 2)P_0$$

i.e.,

$$T + Q_P \sim mP_0.$$

Let $h_m \in \mathbf{F}_{q^2}(\mathcal{X})$ satisfy $\text{div}(h_m) = mP_0 - (T + Q_P)$, then h_m is the desired function.

Theorem 3.9: If $4 \leq m < q$, then there exists a

$$[q^2 + 2q + 1, m^2, q^2 + 2q + 1 - m(q + 1)]$$

linear code over $\mathbf{F}_q$.

Proof: Let $\mathcal{X}/\mathbf{F}_{q^2}$ be an elliptic curve with $q^2 + 2q + 1$ rational points. By Lemma 3.8, there exists a function $h_m \in \mathbf{F}_{q^2}(\mathcal{X})$ such that

$$(h_m)_0 = mP_0, \quad \text{and} \quad \text{Supp}((h_m)_\infty) \cap \mathcal{X}(\mathbf{F}_{q^2}) = \emptyset.$$

Put

$$\overline{U}_m = h_m^{q+1}U_m = \{h_m^{q+1}f | f \in U_m\}.$$

Then $\overline{U}_m$ is an $\mathbf{F}_q$ -linear space and

$$\dim_{\mathbf{F}_q} \overline{U}_m = \dim_{\mathbf{F}_q} U_m = m^2.$$

Moreover, we have the following:

i)

$$\begin{aligned} \text{div}(h_m^{q+1}f) &= \text{div}(h_m^{q+1}) + \text{div}(f) \\ &\geq m(q+1)P_0 - (q+1)(h_m)_\infty + (f)_0 + \nu_{P_0}(e_{mm})P_0 \\ &\geq -(q+1)(h_m)_\infty \end{aligned}$$

i.e., $\overline{U}_m \subseteq \mathcal{L}((q+1)(h_m)_\infty)$, and

ii) $(h_m^{q+1}f)(P) \in \mathbf{F}_q$ for all $f \in U_m$ and $P \in \mathcal{X}(\mathbf{F}_{q^2})$.

Put

$$\overline{C}_m = \{((h_m^{q+1}f)(P_0), (h_m^{q+1}f)(P_1), \dots, (h_m^{q+1}f)(P_n)) | f \in U_m\}$$

where $n = q^2 + 2q$. Then it is easy to see that $\overline{C}_m$ is a subcode of the subfield subcode

$$C(P_0, P_1, \dots, P_n; (q+1)(h_m)_\infty)_{\mathbf{F}_q}.$$

The dimension of this code is equal to the dimension of U_m , that is, m^2 and the minimum distance satisfies

$$\begin{aligned} d(\overline{C}_m) &\geq d(C(P_0, P_1, \dots, P_n; (q+1)(h_m)_\infty)) \\ &\geq q^2 + 2q + 1 - m(q+1). \end{aligned}$$

IV. TABLES

In this section, we first list all improvements on Brouwer's table [1] for $q = 8$ and 9 by directly using the results in Section III. Then we apply some well-known propagation rules to our codes to obtain more improvements on Brouwer's table [1] for $q = 8$ and 9.

We need to explain the symbols in Tables I and II. Corollaries 3.4, 3.6 and Theorem 3.9 are used to construct in Tables I and II.

- l, m parameters in Corollaries 3.4, 3.6 and Theorem 3.9;
- n, k length and dimension of codes, respectively, obtained from Corollaries 3.4, 3.6, or Theorem 3.9 for given parameters m, l ;
- d lower bound on minimum distance obtained from Corollaries 3.4, 3.6, or Theorem 3.9;
- d_B the lower bound on minimum distance of codes with given length n and dimension k quoted from Brouwer's table.

TABLE I
 $q = 8$

Corollary or Theorem	m	l	n	k	d	d_B
3.6(2)	6	5	80	35	27	26
3.4(2)	6	-	80	36	26	25
3.6(2)	7	5	80	46	19	18
3.6(2)	7	6	80	48	18	17
3.4(2)	7	-	80	49	17	16
3.6(2)	8	1	80	51	16	15
3.9	5	-	81	25	36	35
3.9	6	-	81	36	27	26
3.9	7	-	81	49	18	17

TABLE II
 $q = 9$

Corollary or Theorem	m	l	n	k	d	d_B
3.4(2)	6	-	99	36	39	38
3.6(2)	7	6	99	48	30	29
3.4(2)	7	-	99	49	29	28
3.6(2)	8	5	99	59	22	21
3.6(2)	8	6	99	61	21	20
3.6(2)	8	7	99	63	20	19
3.4(2)	8	-	99	64	19	18
3.4(2)	9	1	99	66	18	17
3.9	6	-	100	36	40	39
3.9	7	-	100	49	30	29
3.9	8	-	100	64	20	19

TABLE III
 $q = 8$

Proposition	original code	s	n	k	d	d_B
4.1(1)	[81,49,≥18]	5	75	44	18	17
4.1(1)	[80,48,≥18]	4	76	44	18	17
4.1(1)	[81,49,≥18]	4	76	45	18	17
4.1(1)	[80,48,≥18]	3	77	45	18	17
4.1(1)	[80,51,≥16]	3	77	48	16	15
4.1(1)	[81,49,≥18]	3	77	46	18	17
4.1(1)	[80,36,≥26]	2	78	34	26	25
4.1(1)	[80,48,≥18]	2	78	46	18	17
4.1(1)	[80,49,≥17]	2	78	47	17	16
4.1(1)	[80,51,≥16]	2	78	49	16	15
4.1(1)	[80,46,≥19]	1	79	45	19	18
4.1(1)	[81,36,≥27]	2	79	34	27	26
4.1(1)	[80,36,≥26]	1	79	35	26	25
4.1(1)	[81,49,≥18]	2	79	47	18	17
4.1(1)	[80,51,≥16]	1	79	50	16	15
4.1(1)	[80,49,≥17]	1	79	48	17	16

TABLE IV
 $q = 9$

Proposition	original code	s	n	k	d	d_B
4.1(1)	[100,64,≥20]	6	94	58	20	19
4.1(1)	[99,66,≥18]	5	94	61	18	17
4.1(1)	[100,64,≥20]	5	95	59	20	19
4.1(1)	[99,64,≥19]	4	95	60	19	18
4.1(1)	[99,66,≥18]	4	95	62	18	17
4.1(1)	[100,49,≥30]	4	96	45	30	29
4.1(1)	[99,49,≥29]	3	96	46	29	28
4.1(1)	[99,61,≥21]	3	96	58	21	20
4.1(1)	[100,64,≥20]	4	96	60	20	19
4.1(1)	[99,64,≥19]	3	96	61	19	18
4.1(1)	[99,66,≥18]	3	96	63	18	17
4.1(1)	[100,49,≥30]	3	97	46	30	29
4.1(1)	[99,49,≥29]	2	97	47	29	28
4.1(1)	[99,61,≥21]	2	97	59	21	20
4.1(1)	[100,64,≥20]	3	97	61	20	19
4.1(1)	[99,64,≥19]	2	97	62	19	18
4.1(1)	[99,66,≥18]	2	97	64	18	17
4.1(1)	[100,49,≥30]	2	98	47	30	29
4.1(1)	[99,49,≥29]	1	98	48	29	28
4.1(2)	[99,49,≥29]	1	98	49	28	27
4.1(1)	[99,61,≥21]	1	98	60	21	20
4.1(1)	[100,64,≥20]	2	98	62	20	19
4.1(1)	[99,64,≥19]	1	98	63	19	18
4.1(1)	[99,66,≥18]	1	98	65	18	17
4.2	[99,63,≥20]	2	99	62	20	19

d

d_B

the lower bound on minimum distance obtained from Proposition 4.1 for given s and original code;
the lower bound on minimum distance of codes with given length n and dimension k quoted from Brouwer's table.

REFERENCES

- [1] A. Brouwer. Bounds on the minimum distance of linear code. [Online] Available: <http://www.win.tue.nl/~aeb/voorlincod.html>
- [2] V. D. Goppa, "Codes on algebraic curves" (in Russian), *Dokl. Akad. Nauk SSSR*, vol. 259, pp. 1289–1290, 1981.
- [3] H. Niederreiter and C. P. Xing, "Towers of global function fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound," *Math. Nachrichtentech.*, vol. 195, pp. 171–186, 1998.
- [4] H. Niederreiter, C. P. Xing, and K. Y. Lam, "A new construction of algebraic geometry codes," *Appl. Algebra Engrg. Comm. Comput.*, vol. 9, pp. 373–381, 1999.
- [5] F. Özbudak and H. Stichtenoth, "Constructing codes from algebraic curves," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2502–2505, Nov. 1999.
- [6] H. Stichtenoth, *Algebraic Function Fields and Codes*. Berlin, Germany: Springer-Verlag, 1993.
- [7] M. A. Tsfasman and S. G. Vlăduț, *Algebraic-Geometric Codes*. Dordrecht, The Netherlands: Kluwer, 1991.
- [8] —, "Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound," *Math. Nachrichtentech.*, vol. 109, pp. 21–28, 1982.
- [9] W. C. Waterhouse, "Abelian varieties over finite fields," *Ann. Sci. Ecole Norm. Supp.*, vol. 2, no. 4, pp. 521–560, 1969.

Next we use the propagation rules to get more improvements on Brouwer's table.

Proposition 4.1 (see [7, Exercise 1.2.24]):

- 1) If there is an $[n, k, d]$ linear code over $\mathbf{F}_q$, then there exists an $[n - s, k - s, d]$ linear code over $\mathbf{F}_q$ for any $s \leq n - d$.
- 2) If there is an $[n, k, d]$ linear code over $\mathbf{F}_q$, then there exists an $[n - s, k, d - s]$ linear code over $\mathbf{F}_q$ for any $s \leq n - k$.

By considering subcodes of a linear code, we obtain the following result.

Proposition 4.2: If there is an $[n, k, d]$ linear code over $\mathbf{F}_q$, then there exists an $[n, k - s, d]$ linear code for any $0 \leq s \leq k - 1$.

We need to explain the symbols in Tables III and IV. We use the codes in Tables I, II and Proposition 4.1 to construct the codes in Tables III and IV.

Original code linear codes from Tables II and III;

s parameters in Proposition 4.1;

n, k length and dimension of codes, respectively, obtained from Proposition 4.1 for given s and original code;

- [10] C. P. Xing and S. Ling, "A class of linear codes with good parameters," *IEEE Trans. Inform. Theory*, to be published.
- [11] C. P. Xing, H. Niederreiter, and K. Y. Lam, "Constructions of algebraic geometry codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1186–1193, May 1999.
- [12] —, "A generalization of algebraic geometry codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2498–2501, Nov. 1999.