New binary linear codes from algebraic curves

Leung, Ka Hin; Ling, San; Xing, Chaoping

2002

Leung, K. H., Ling, S., & Xing, C. (2002). New binary linear codes from algebraic curves. IEEE Transactions on Information Theory, 48(1), 285-287.

https://hdl.handle.net/10356/96426

https://doi.org/10.1109/18.971757

New Binary Linear Codes From Algebraic Curves

Ka Hin Leung, San Ling, and Chaoping Xing

***Abstract*—Many new binary linear codes (compared with Brouwer's table) are found from a construction based on algebraic curves over finite fields.**

***Index Terms*—Algebraic function fields, binary linear codes, places.**

I. Introduction

Constructing codes with good parameters is one of the important problems in coding theory. Various tools and methods from algebra, numbers theory, geometry, combinatorics, etc., are employed for the construction of linear codes. Since binary codes do not only have a longer history than codes over other fields but are also of the greatest interest in practice, much more attention has been paid to binary than nonbinary codes. Nowadays, it is believed that constructing new binary linear codes of small lengths is becoming more and more difficult.

Algebraic geometry has been extensively used in the construction of codes since the discovery of Goppa's geometry codes [2], [4], [5]. In order to get good Goppa's geometry codes, one has to find algebraic curves with as many rational points as possible. However, it seems impossible to obtain many good q-ary linear codes by directly applying Goppa's construction for small q since curves over small finite fields have few rational points compared with their genera. In recent years, several constructions using closed points of higher degrees have been proposed [6]–[8], [3] and some new nonbinary linear codes with good parameters have been found based on these constructions. Unfortunately, these constructions do not provide any new binary linear codes with good parameters even though closed points of higher degrees are used. In this correspondence, we modify the concatenation construction in [8], namely, we employ curves over extensions of the ground field and their closed points of higher degrees and apply the classical concatenation method to construct linear codes. It turns out that many new binary linear codes with good parameters are produced from this construction. The main objective of this correspondence is to find new binary codes with good parameters rather than to focus on new constructions of codes.

II. Construction of Codes

Since it is more convenient to use notations of function fields, we switch from the language of curves to that of function fields from now on.

Let q be a prime power. For the finite field $\boldsymbol{F}_q$, let F be an algebraic function field with the full constant field $\boldsymbol{F}_q$. We express this fact by simply saying that $F/\boldsymbol{F}_q$ is a function field. The genus of $F/\boldsymbol{F}_q$ is denoted by $g(F)$. A place P of F has degree m if its residue class field F_P is an extension of $\boldsymbol{F}_q$ of degree m. A place of degree 1 is also called *rational*. For Goppa's construction, one is interested in function fields with as many rational places as possible for a given genus. For our purpose, function fields with many rational places are relevant as well. However, function fields with many rational places and many places of other small degrees are more interesting for us.

For an arbitrary divisor G of F, we form the vector space

$$\mathcal{L}(G) = \{x \in F\backslash\{0\}\colon \operatorname{div}(x) + G \geq 0\} \cup \{0\}.$$

Then, $\mathcal{L}(G)$ is a finite-dimensional vector space over $\boldsymbol{F}_q$, and we denote its dimension by $\ell(G)$. By the Riemann–Roch theorem we have

$$\ell(G) \geq \deg(G) + 1 - g \tag{1}$$

and equality holds if $\deg(G) \geq 2g - 1$.

For a place P of F of degree m and a function $f \in F$ with $\nu_P(f) \geq 0$, the residue class $f(P)$ of f in the residue class field F_P of P is identified with an element of $\boldsymbol{F}_{q^m}$. For more background on curves and their function fields, we refer to the books [4], [5].

Now let $q = r^e$ for some integer $e \geq 1$ and prime power r. Let $F/\boldsymbol{F}_q$ be a function field of genus g. We choose s distinct places $P_1, \ldots, P_s$ and a divisor G of F such that

$$\operatorname{supp}(G) \cap \{P_1, \ldots, P_s\} = \emptyset.$$

For each $1 \leq i \leq s$, we also choose an r-ary linear code C_i with parameters $[n_i, ek_i, d_i]$, where $k_i = \deg(P_i)$. For each $1 \leq i \leq s$, we fix an $\boldsymbol{F}_r$-linear isomorphism π_i mapping the residue class field $F_{P_i} \simeq \boldsymbol{F}_{q^{k_i}}$ onto C_i.

Now we consider the map

$$\alpha\colon \quad \mathcal{L}(G) \longrightarrow \boldsymbol{F}_r^n$$
$$f \longmapsto (\pi_1(f(P_1)), \pi_2(f(P_2)), \ldots, \pi_s(f(P_s)))$$

where n is equal to $\sum_{i=1}^{s} n_i$. It is easy to verify that α is an $\boldsymbol{F}_r$-linear map.

The image of α is obviously a linear code over $\boldsymbol{F}_r$ of length n. We denote it by $\mathcal{C}(P_1, \ldots, P_s;\ G;\ C_1, \ldots, C_s)$.

Lemma 2.1: Let the notations be the same as above. If $\deg(G) < \sum_{i=1}^{s} k_i$ then α is injective.

Proof: Suppose that $\alpha(f) = \alpha(h)$ for $f, h \in \mathcal{L}(G)$, then

$$\pi_i(f(P_i)) = \pi_i(h(P_i)) \tag{2}$$

for all $1 \leq i \leq s$. Hence $f(P_i) = h(P_i)$ for all $1 \leq i \leq s$ since the π_i are isomorphisms. It thus follows that

$$f - h \in \mathcal{L}\left(G - \sum_{i=1}^{s} P_i\right). \tag{3}$$

By the condition $\deg(G) < \sum_{i=1}^{s} k_i$ (3) implies that $f - h = 0$, i.e., $f = h$. □

Theorem 2.2: With the notation above, suppose that $\deg(G) < \sum_{i=1}^{s} k_i$ and $d_i \leq ek_i$ for all $1 \leq i \leq s$. Then the dimension k and the minimum distance d of the code $\mathcal{C}(P_1, \ldots, P_s;\ G;\ C_1, \ldots, C_s)$ satisfy

$$k \geq e(\deg(G) - g + 1) \quad \text{and} \quad d \geq \sum_{i=1}^{s} d_i - e\deg(G).$$

Furthermore, we have $k = e(\deg(G) - g + 1)$ if $\deg(G) \geq 2g - 1$.

Proof: It directly follows from the Riemann–Roch theorem that the dimension $\dim_{\boldsymbol{F}_q} \mathcal{L}(G)$ satisfies

$$\dim_{\boldsymbol{F}_q} \mathcal{L}(G) = \ell(G) \geq \deg(G) - g + 1$$

with equality if $\deg(G) \geq 2g - 1$. By Lemma 2.1, the dimension $\dim_{\boldsymbol{F}_r} \mathcal{C}(P_1, \ldots, P_s; G;\ C_1, \ldots, C_s)$ is equal to

K. H. Leung and S. Ling are with the Department of Mathematics, National University of Singapore, Singapore 117543 (e-mail: matlkh@nus.edu.sg; matlings@nus.edu.sg).

C. Xing is with the Department of Mathematics, National University of Singapore, Singapore 117543. He is also with the Department of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, China (e-mail: matxcp@nus.edu.sg).

Communicated by J. Justesen, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(02)00035-4.

$\dim_{\boldsymbol{F}_r} \mathcal{L}(G) = e \dim_{\boldsymbol{F}_q} \mathcal{L}(G)$. Therefore, the desired result on the dimension of $\mathcal{C}(P_1, \ldots, P_s;\ G;\ C_1, \ldots, C_s)$ follows.

Choose an arbitrary nonzero function f in $\mathcal{L}(G)$ and let R be the subset of $\{1, 2, \ldots, s\}$ satisfying

$$f(P_i) = 0, \qquad \text{if and only if } \ i \in R.$$

Let T be the complement of R in $\{1, 2, \ldots, s\}$. With $\mathrm{wt}(\cdot)$ denoting the Hamming weight of a vector, it follows that

$$\begin{aligned} \mathrm{wt}(\alpha(f)) &= \sum_{i \in T} \mathrm{wt}(\pi_i(f(P_i))) \geq \sum_{i \in T} d_i \\ &= \sum_{i=1}^{s} d_i - \sum_{i \in R} d_i \geq \sum_{i=1}^{s} d_i - \sum_{i \in R} e \deg(P_i). \end{aligned} \tag{4}$$

On the other hand, it follows from $f \in \mathcal{L}(G - \sum_{i \in R} P_i)$ that

$$\deg(G) \geq \sum_{i \in R} \deg(P_i). \tag{5}$$

Adding (4) and $e \times$(5), we obtain

$$\mathrm{wt}(\alpha(f)) + e \deg(G) \geq \sum_{i=1}^{s} d_i$$

which gives the desired lower bound on d. □

Remark: We note that the construction in this section is a modification of the earlier construction of new types of algebraic-geometry codes given in [8]. We will see in the next section that this modification produces a lot of new binary linear codes with good parameters.

III. Examples

In this section, we present two examples for $r = 2$ from our construction in Section II. These examples provide many new binary linear codes compared with Brouwer's table [1], while it seems impossible to obtain such good binary linear codes from Goppa's construction and the construction in [8].

Let $F/\boldsymbol{F}_q$ be an algebraic function field of genus g. Then the zeta function of $F/\boldsymbol{F}_q$ is a rational function of the form

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)}$$

where $L(t)$ is a polynomial of degree $2g$ with integral coefficients. $L(t)$ is called the L-polynomial of $F/\boldsymbol{F}_q$. Suppose that $\{w_i\}_{i=1}^{2g}$ are all reciprocal roots of $L(t)$. Then the absolute value of each w_i is $\sqrt{q}$ and the number B_r of the places of $F/\boldsymbol{F}_q$ of degree r is given by (see [4, Proposition V.2.9])

$$B_r = \frac{1}{r} \sum_{d|r} \mu\left(\frac{r}{d}\right)(q^d - S_d) \tag{6}$$

for all $r \geq 2$, where $\mu(\cdot)$ denotes the Möbius function and S_d is given by

$$S_d := \sum_{i=1}^{2g} w_i^d.$$

If $F/\boldsymbol{F}_q$ is the rational function field, then the genus is 0. Thus, the L-polynomial is 1. In this case, $B_1 = q + 1$ and B_r $(r \geq 2)$ is the number of monic irreducible polynomials of degree r over $\boldsymbol{F}_q$.

If $F/\boldsymbol{F}_q$ is the function field of an elliptic curve, then the L-polynomial is of the form $1 + at + qt^2$ for some integer a since the genus is 1. Furthermore, we have $a = q + 1 - B_1$ by (6).

Note that for sufficiently large δ there exist places Q_δ and $Q_{\delta+1}$ of F of degrees δ and $\delta+1$, respectively [4, Corollary V.2.10(c)]. We always choose $G = m(Q_{\delta+1} - Q_\delta)$, so that $\mathrm{supp}(G) \cap \{P_1, \ldots, P_s\} = \emptyset$ for sufficiently large δ and $\deg(G) = m$.

TABLE I

n	k	$d \geq$	d_B	Example
153	32	46	44	1(a) with $m = 7$
156	32	48	45	1(b) with $m = 7$
209	24	78	76	2(a) with $m = 6$
213	24	80	78	2(b) with $m = 6$
217	20	86	85	2(c) with $m = 5$
217	24	82	80	2(c) with $m = 6$
217	28	78	76	2(c) with $m = 7$
217	32	74	72	2(c) with $m = 8$
217	36	70	68	2(c) with $m = 9$
217	40	66	64	2(c) with $m = 10$
217	44	62	60	2(c) with $m = 11$
217	48	58	56	2(c) with $m = 12$
220	24	84	82	2(d) with $m = 6$
220	28	80	78	2(d) with $m = 7$
220	32	76	73	2(d) with $m = 8$
220	36	72	70	2(d) with $m = 9$
220	40	68	65	2(d) with $m = 10$
220	44	64	61	2(d) with $m = 11$
220	48	60	58	2(d) with $m = 12$

In both examples, we write $Z(t)$ for the zeta function of the function field $F/\boldsymbol{F}_{16}$ and B_i, $i \geq 1$, for the number of places of F of degree i.

Example 3.1: Let $q = 16$, so $e = 4$. Let $F = \boldsymbol{F}_{16}(x)$ be the rational function field. Then $g(F) = 0$ and

$$Z(t) = \frac{1}{(1-t)(1-16t)}.$$

Furthermore, $B_1 = 17$ and $B_2 > 1$.

a) Take $s = 18$, $k_i = 1$ for $1 \leq i \leq 17$, and $k_{18} = 2$. For $1 \leq i \leq 17$, let the parameters of C_i be $[n_i,\ e \cdot k_i,\ d_i] = [8,\ 4,\ 4]$ and let the parameters of C_{18} be $[n_{18},\ e \cdot k_{18},\ d_{18}] = [17,\ 8,\ 6]$. Then, by Theorem 2.2, we obtain binary linear codes with parameters

$$[153,\ 4m + 4,\ \geq 74 - 4m], \qquad \text{for } 1 \leq m \leq 18.$$

b) Take $s = 18$, $k_i = 1$ for $1 \leq i \leq 17$, and $k_{18} = 2$. For $1 \leq i \leq 17$, let the parameters of C_i be $[n_i,\ e \cdot k_i,\ d_i] = [8,\ 4,\ 4]$ and let the parameters of C_{18} be $[n_{18},\ e \cdot k_{18},\ d_{18}] = [20,\ 8,\ 8]$. Then, by Theorem 2.2, we obtain binary linear codes with parameters

$$[156,\ 4m + 4,\ \geq 76 - 4m], \qquad \text{for } 1 \leq m \leq 18.$$

Example 3.2: Let $q = 16$, so $e = 4$. Let $F = \boldsymbol{F}_{16}(x, y)$ be the function field defined by

$$y^2 + y = x^3 + \alpha x$$

where α is a primitive element of $\boldsymbol{F}_4$. Then, $g(F) = 1$ and $B_1 = 25$. Thus, the zeta-function is

$$Z(t) = \frac{(4t+1)^2}{(1-t)(1-16t)}.$$

A simple calculation based on (6) shows that $B_2 > 1$.

a) Take $s = 26$, $k_i = 1$ for $1 \leq i \leq 25$, and $k_{26} = 2$. For $1 \leq i \leq 25$, let the parameters of C_i be $[n_i,\ e \cdot k_i,\ d_i] = [8,\ 4,\ 4]$ and let

TABLE II

n	k	$d \geq$	d_B	Remark
152	32	45	44	by shortening of $[153, 32, \geq 46]$
154	32	46	44	by lengthening of $[153, 32, \geq 46]$
155	32	47	44	by shortening of $[156, 32, \geq 48]$
157	32	48	46	by lengthening of $[156, 32, \geq 48]$
208	24	77	76	by shortening of $[209, 24, \geq 78]$
209	23	78	76	by taking subcode of $[209, 24, \geq 78]$
210	24	78	76	by lengthening of $[209, 24, \geq 78]$
216	32	73	72	by shortening of $[217, 32, \geq 74]$
217	31	74	72	by taking subcode of $[217, 32, \geq 74]$
218	32	74	72	by lengthening of $[217, 32, \geq 74]$
219	40	67	64	by shortening of $[220, 40, \geq 68]$
220	39	68	66	by taking subcode of $[220, 40, \geq 68]$
221	40	68	66	by lengthening of $[220, 40, \geq 68]$

the parameters of C_{26} be $[n_{26},\, e \cdot k_{26},\, d_{26}] = [9,\, 8,\, 2]$. Then, by Theorem 2.2, we obtain binary linear codes with parameters

$$[209,\, 4m,\, \geq 102 - 4m], \qquad \text{for } 1 \leq m \leq 25.$$

b) Take $s = 26$, $k_i = 1$ for $1 \leq i \leq 25$, and $k_{26} = 2$. For $1 \leq i \leq 25$, let the parameters of C_i be $[n_i,\, e \cdot k_i,\, d_i] = [8,\, 4,\, 4]$ and let the parameters of C_{26} be $[n_{26},\, e \cdot k_{26},\, d_{26}] = [13,\, 8,\, 4]$. Then, by Theorem 2.2, we obtain binary linear codes with parameters

$$[213,\, 4m,\, \geq 104 - 4m], \qquad \text{for } 1 \leq m \leq 25.$$

c) Take $s = 26$, $k_i = 1$ for $1 \leq i \leq 25$, and $k_{26} = 2$. For $1 \leq i \leq 25$, let the parameters of C_i be $[n_i,\, e \cdot k_i,\, d_i] = [8,\, 4,\, 4]$ and let the parameters of C_{26} be $[n_{26},\, e \cdot k_{26},\, d_{26}] = [17,\, 8,\, 6]$. Then, by Theorem 2.2, we obtain binary linear codes with parameters

$$[217,\, 4m,\, \geq 106 - 4m], \qquad \text{for } 1 \leq m \leq 26.$$

d) Taking $s = 26$, $k_i = 1$ for $1 \leq i \leq 25$, and $k_{26} = 2$. For $1 \leq i \leq 25$, let the parameters of C_i be $[n_i,\, e \cdot k_i,\, d_i] = [8,\, 4,\, 4]$ and let the parameters of C_{26} be $[n_{26},\, e \cdot k_{26},\, d_{26}] = [20,\, 8,\, 8]$. Then, by Theorem 2.2, we obtain binary linear codes with parameters

$$[220,\, 4m,\, \geq 108 - 4m], \qquad \text{for } 1 \leq m \leq 26.$$

The above examples produce a series of new binary linear codes. We list some new codes from Examples 3.1 and 3.2 in Table I. The numbers $n,\, k,\, d$ in Table I stand for the three parameters of binary linear codes from our examples, whereas d_B denotes the lower bound on the largest d for binary linear codes, with given length n and dimension k, from Brouwer's table [1] (as of November 4, 2000).

Note that some simple propagation rules will yield a lot of other new binary codes from those in Table I. We list only a few of these new codes in Table II as illustrations.

REFERENCES

[1] A. Brouwer. (2000, Nov.) 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] F. Özbudak and H. Stichtenoth, "Constructing codes from algebraic curves," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2502–2506, Nov. 1999.

[4] H. Stichtenoth, *Algebraic Function Fields and Codes*. Berlin, Germany: Springer-Verlag, 1993.

[5] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*. Dordrecht, The Netherlands: Kluwer, 1991.

[6] C. P. Xing and S. Ling, "A class of linear codes with good parameters from algebraic curves," *IEEE Trans. Inform. Theory*, vol. 46, pp. 1527–1532, July 2000.

[7] ——, "A class of linear codes with good parameters," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2184–2188, Sept. 2000.

[8] C. P. Xing, H. Niederreiter, and K. Y. Lam, "A generalization of algebraic geometry codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2498–2501, Nov. 1999.