A NEW CONSTRUCTION OF NONLINEAR CODES VIA ALGEBRAIC FUNCTION FIELDS

SHU LIU, LIMING MA, TING-YI WU, AND CHAOPING XING

ABSTRACT. In coding theory, constructing codes with good parameters is one of the most important and fundamental problems. Though a great many of good codes have been produced, most of them are defined over alphabets of sizes equal to prime powers. In this paper, we provide a new explicit construction of $(q + 1)$-ary nonlinear codes via algebraic function fields, where q is a prime power. Our codes are constructed by evaluations of rational functions at all rational places of the algebraic function field. Compared with algebraic geometry codes, the main difference is that we allow rational functions to be evaluated at pole places. After evaluating rational functions from a union of Riemann-Roch spaces, we obtain a family of nonlinear codes over the alphabet $\mathbb{F}_q \cup \{\infty\}$. It turns out that our codes have better parameters than those obtained from MDS codes or good algebraic geometry codes via code alphabet extension and restriction.

1. INTRODUCTION

In coding theory, constructing codes with good parameters is one of the most important and fundamental problems. For a q-ary code of length n, size M and minimum distance d, we denote it by an (n, M, d)-code. The size is a measure of its efficiency and the minimum distance represents its error-correcting capability. Hence, people hope that both the size M and minimum distance d are as large as possible. However, there is a trade-off between the size and the minimum distance of the code. One of the well-known upper bounds is the Singleton bound which says that $M \leqslant q^{n-d+1}$. A linear code achieving this bound is called a maximum distance separable (MDS) code.

Many efforts have been devoted to various constructions of good codes. Linear codes have received a lot of attention, such as Reed-Solomon codes, BCH codes, cyclic codes and so on, since they have good algebraic structures and many practical advantages. However, there are some examples showing that linear codes do not exist for some parameters that nonlinear codes can have. For example, there are no binary linear codes with parameters $[16, 8, 6]$. On the other hand, the Nordstorm-Robinson code [14] is a binary nonlinear code with parameters $(16, 2^8, 6)$. Furthermore, the Nordstrom-Robinson code can be viewed as an image under the Gray map of some algebraic geometry code over $\mathbb{Z}/4\mathbb{Z}$ in [22]. Therefore, it is also of interest to provide explicit constructions of nonlinear codes. Though a large number of nonlinear codes have been constructed, most of them are q-ary codes where q is a prime power. Less is known for

constructions of q-ary codes, where q is not a prime power. Some nonlinear codes over $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_{10}$ or $\mathbb{Z}_{12}$ were given with certain properties [7, 8, 9].

In [12], an explicit construction of $(q+1)$-ary $(q+1, q^{2m+1}+q^{2m}-2q^m+2, q+1-2m)$ nonlinear codes with q being a prime power was presented. Such codes have better parameters than those obtained from MDS codes via code alphabet restriction and extension. Another advantage of these codes is that they can be efficiently decoded. Due to rich structures of algebraic function fields over finite fields, various techniques have been employed to construct good codes from algebraic function fields [1, 11, 13, 17, 18, 23].

In this paper, we generalizes the construction of nonlinear codes via rational function fields given in [12] to algebraic function fields. Our nonlinear codes are constructed by evaluations of rational functions at all rational places of algebraic function fields. Compared with algebraic geometry codes, the main difference is that we allow rational functions to be evaluated at pole places. After evaluating rational functions from a union of Riemann-Roch spaces, we construct a family of good nonlinear codes over the alphabet $\mathbb{F}_q \cup \{\infty\}$. Note that code sizes in [12] are exactly calculated due to the nature of rational function fields, while lower bounds on code sizes in this paper are provided.

This paper is organized as follows. In Section 2, we introduce the basic facts on algebraic function fields, Riemann-Roch spaces, Zeta functions, codes and algebraic geometry codes. In Section 3, we give an explicit construction of $(q+1)$-ary nonlinear codes from algebraic function fields over the finite field $\mathbb{F}_q$. In particular, we focus on the constructions of nonlinear codes via elliptic curves in Section 4 and maximal function fields in Section 5, respectively.

2. Preliminaries

In this section, we present preliminaries on the definitions of algebraic function fields, Riemann-Roch spaces, Zeta functions, Codes and algebraic geometry codes.

2.1. **Algebraic function fields.** Let q be a prime power, let $\mathbb{F}_q$ be the finite field with q elements and let $F/\mathbb{F}_q$ be an algebraic function field with the full constant field $\mathbb{F}_q$. The set of all places of F is denoted by $\mathbb{P}_F$. Let $P \in \mathbb{P}_F$ be a place of F and let $\mathcal{O}_P$ be its corresponding valuation ring. The degree of P is defined as the degree of field extension $[\mathcal{O}_P/P : \mathbb{F}_q]$. A place of $F/\mathbb{F}_q$ with degree one is called rational. For any rational place P and $f \in \mathcal{O}_P$, we define $f(P) \in \mathcal{O}_P/P \cong \mathbb{F}_q$ to be the residue class of f modulo P; otherwise $f(P) = \infty$ for any $f \in F \setminus \mathcal{O}_P$.

A divisor G of F is a formal sum $G = \sum_{P \in \mathbb{P}_F} n_P P$ with only finitely many nonzero coefficients $n_P \in \mathbb{Z}$. The support of G is defined as $\mathrm{supp}(G) = \{P \in \mathbb{P}_F : n_P \neq 0\}$. If all coefficients of G are non-negative, then the divisor G is called effective. Let ν_P be the normalized discrete valuation of P. For any nonzero element $f \in F$, the zero

divisor of f is defined by $(f)_0 = \sum_{P \in \mathbb{P}_F, \nu_P(f)>0} \nu_P(f)P$, and the pole divisor of f is defined by $(f)_\infty = \sum_{P \in \mathbb{P}_F, \nu_P(f)<0} -\nu_P(f)P$. The principal divisor of f is given by

$$(f) := (f)_0 - (f)_\infty = \sum_{P \in \mathbb{P}_F} \nu_P(f)P.$$

For two divisors $G = \sum_{P \in \mathbb{P}_F} n_P P$ and $D = \sum_{P \in \mathbb{P}_F} m_P P$, we define the union and intersection of G and D respectively as follows

$$G \vee D := \sum_{P \in \mathbb{P}_F} \max\{n_P, m_P\}P, \qquad G \wedge D := \sum_{P \in \mathbb{P}_F} \min\{n_P, m_P\}P.$$

It is clear that $G \wedge D + G \vee D = G + D$.

2.2. **Riemann-Roch spaces.** Let $F/\mathbb{F}_q$ be an algebraic function field with genus g. For a divisor G of $F/\mathbb{F}_q$, the Riemann-Roch space of G is defined by

$$\mathcal{L}(G) := \{u \in F^* : (u) + G \geqslant 0\} \cup \{0\}.$$

From the Riemann-Roch theorem [20, Theorem 1.5.17], $\mathcal{L}(G)$ is a $\mathbb{F}_q$-vector space of dimension $\ell(G) \geqslant \deg(G) - g + 1$. Moreover, the equality holds true if $\deg(G) \geqslant 2g - 1$. For any two divisors G and H, it is straightforward to verify that

$$\mathcal{L}(G) \cap \mathcal{L}(H) = \mathcal{L}(G \wedge H) \text{ and } \mathcal{L}(G) + \mathcal{L}(H) \subseteq \mathcal{L}(G \vee H).$$

Lemma 2.1. *Let f_1, f_2 be two nonzero functions in F with pole divisors $(f_i)_\infty = G_i$ for $i = 1, 2$. If $f_1(P) = f_2(P) \in \mathbb{F}_q \cup \{\infty\}$ for some rational place $P \in \mathbb{P}_F$, then we have $f_1 - f_2 \in \mathcal{L}(G_1 + G_2 - P)$.*

Proof. **Case 1:** If $f_1(P) = f_2(P) \in \mathbb{F}_q$, then we have $(f_1 - f_2)(P) = f_1(P) - f_2(P) = 0$, i.e., P is a zero of $f_1 - f_2$. Let $G = (f_1 - f_2)_\infty$. Thus, we have $f_1 - f_2 \in \mathcal{L}(G - P)$. Since $f_1 - f_2 \in \mathcal{L}(G_1) + \mathcal{L}(G_2) \subseteq \mathcal{L}(G_1 \vee G_2)$, it follows that $f_1 - f_2 \in \mathcal{L}(G_1 \vee G_2 - P) \subseteq \mathcal{L}(G_1 + G_2 - P)$.

Case 2: If $f_1(P) = f_2(P) = \infty$, then we have $P \in \mathrm{supp}(G_1) \cap \mathrm{supp}(G_2) = \mathrm{supp}(G_1 \wedge G_2)$. From the equation $G_1 \vee G_2 = G_1 + G_2 - G_1 \wedge G_2$, we have $G_1 \vee G_2 \leqslant G_1 + G_2 - P$. Since $f_1 - f_2 \in \mathcal{L}(G_1) + \mathcal{L}(G_2) \subseteq \mathcal{L}(G_1 \vee G_2)$, it follows that $f_1 - f_2 \in \mathcal{L}(G_1 + G_2 - P)$. $\square$

2.3. **Zeta functions.** Let $F/\mathbb{F}_q$ be an algebraic function field with genus g. Let A_i be the number of all effective divisors of $F/\mathbb{F}_q$ of degree $i \geqslant 0$. The Zeta function of $F/\mathbb{F}_q$ is defined as the power series $Z(t) := \sum_{i=0}^{\infty} A_i t^i \in \mathbb{C}[[t]]$. From [20, Theorem 5.1.15], the Zeta function $Z(t)$ can be written as a rational function

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

where $L(t) = \sum_{i=0}^{2g} a_i t^i \in \mathbb{Z}[t]$ is a polynomial of degree $2g$. The polynomial $L(t)$ is called the L-polynomial of $F/\mathbb{F}_q$.

Lemma 2.2. *Let $F/\mathbb{F}_q$ be an algebraic function field with genus g. Let A_i be the number of all effective divisors of degree i. Let a_j be the coefficients of L-polynomial $L(t) = \sum_{j=0}^{2g} a_j t^j$. Then we have*

$$A_i = \sum_{j=0}^{\min\{i,2g\}} \frac{q^{i+1-j} - 1}{q-1} a_j.$$

Proof. This result follows from the equation

$$\sum_{i=0}^{\infty} A_i t^i = Z(t) = \frac{L(t)}{(1-t)(1-qt)} = \left(\sum_{j=0}^{2g} a_j t^j\right) \left(\sum_{k=0}^{\infty} t^k\right) \left(\sum_{u=0}^{\infty} q^u t^u\right)$$

$$= \left(\sum_{j=0}^{2g} a_j t^j\right) \left(\sum_{k=0}^{\infty} \frac{q^{k+1} - 1}{q-1} t^k\right).$$

$\square$

2.4. **Codes.** Let $\mathbb{F}_q$ be the finite field with q elements. We denote a q-ary (n, M, d) code as a code of length n, size M and minimum distance d. There is a well-known upper bound on the size of codes which is called the Singleton bound [14, Theorem 5.4.1].

Lemma 2.3. *For any integer $q > 1$, any positive integer n and any integer d with $1 \leqslant d \leqslant n$, let C be a q-ary (n, M, d)-code. Then we have $M \leqslant q^{n-d+1}$.*

A linear code of length n over $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$. A linear code with length n, dimension k and minimum distance d is denoted as an $[n, k, d]$-linear code. Any linear code achieving the Singleton bound, i.e., $k + d = n + 1$, is called a maximum distance separable (MDS) code.

Denote by Σ the set $\mathbb{F}_q \cup \{\infty\}$. The size of Σ is $|\Sigma| = q + 1$. In this paper, we consider nonlinear codes over the alphabet Σ. Let $\mathbf{x}, \mathbf{y}$ be words of length n over Σ. The Hamming distance of $\mathbf{x}$ and $\mathbf{y}$, denoted by $d(\mathbf{x}, \mathbf{y})$, is defined to be the number of places at which $\mathbf{x}$ and $\mathbf{y}$ differ. The minimum distance of C is defined by $d(C) = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}$. From Lemma 2.3, any (n, M, d)-code over Σ satisfies $M \leqslant (q+1)^{n-d+1}$. In order to obtain good lower bound on the size of code over Σ, one could make use of the following propagation rules given in Exercises of [14, Chapter 6].

Lemma 2.4. (1) *(Alphabet extension) Let s, r be two integers such that $s \geqslant r > 1$. We embed an alphabet A of cardinality of r into an alphabet B of cardinality s. Then any (n, M, d)-code C over A can be viewed as an (n, M, d)-code over B.*

(2) *(Alphabet restriction) Let s, r be two integers such that $s \geqslant r > 1$. We embed an alphabet A of cardinality of r into $\mathbb{Z}_s$. For an (n, M, d)-code C over $\mathbb{Z}_s$, there exists an r-ary (n, M', d')-code with $M' \geqslant M(r/s)^n$ and $d' \geqslant d$.*

(3) *(Alphabet multiplication) Let r and s be two integers bigger than 1. Let C_1 be an (n, M_1, d_1)-code over $\mathbb{Z}_r$, and let C_2 be an (n, M_2, d_2)-code over $\mathbb{Z}_s$. Then C_1 and C_2 can be viewed as codes over $\mathbb{Z}_{rs}$ by mapping $i(\bmod r) \in \mathbb{Z}_r$ and $i(\bmod s) \in \mathbb{Z}_s$ to $i(\bmod rs) \in \mathbb{Z}_{rs}$. Furthermore, the code*

$$C_1 + rC_2 := \{\mathbf{u} + r\mathbf{v} \in \mathbb{Z}_{rs}^n : \mathbf{u} \in C_1, \mathbf{v} \in C_2\}$$

is an $(n, M_1 M_2, \min\{d_1, d_2\})$-code over $\mathbb{Z}_{rs}$.

2.5. **Algebraic geometry codes.** Let $F/\mathbb{F}_q$ be an algebraic function field of genus g with $N(F)$ rational places. Let $P_1, P_2, \cdots, P_n$ be rational points of F and $D = \sum_{i=1}^{n} P_i$. For every divisor G with $0 < \deg(G) < n$ and $P_i \notin \operatorname{supp}(G)$, the algebraic geometry code $C(D, G)$ is defined as the image of evaluation map

$$\phi : \mathcal{L}(G) \to \mathbb{F}_q^n, \ \phi(f) = (f(P_1), f(P_2), \cdots, f(P_n)).$$

From the Riemann-Roch Theorem, the dimension of $C(D, G)$ is $k = \ell(G) \geqslant \deg(G) - g + 1$ and the minimum distance of $C(D, G)$ is lower bounded by $d \geqslant n - \deg(G)$. It is easy to see that $n - g + 1 \leqslant k + d \leqslant n + 1$. The following lemma gives an upper bound on the number of rational places of algebraic function fields over $\mathbb{F}_q$ from [20, Theorem 5.2.3].

Lemma 2.5. *Let $F/\mathbb{F}_q$ be an algebraic function field of genus g defined over the finite field $\mathbb{F}_q$ and let $N(F)$ be its number of rational places. Then we have*

$$|N(F) - q - 1| \leqslant 2g\sqrt{q}.$$

The above bound given in Lemma 2.5 is called the Hasse-Weil bound. Any function field $F/\mathbb{F}_q$ of genus g achieving the Hasse-Weil upper bound $q + 1 + 2g\sqrt{q}$ is called maximal. In order to construct good algebraic geometry codes, people need to use algebraic function fields with many rational places, especially maximal function fields [2, 3, 4, 5, 16].

In particular, if $F/\mathbb{F}_q$ is an elliptic function field, then the elliptic code $C(D, G)$ is an $[n, k, d]$-linear code with $n \leqslant k + d \leqslant n + 1$. Hence, the elliptic code is an almost MDS code, i.e., $k + d = n$, or an MDS code. Furthermore, the following result can be found from [15, Proposition 3.4].

Lemma 2.6. *If a nontrivial elliptic MDS code has length $n > q + 1$, then it is a $[6, 3]$ code over $\mathbb{F}_4$ arising from a curve with 9 rational points.*

Let $N_q(g)$ be the maximum number of rational places of global function fields $F/\mathbb{F}_q$ of genus g. A prime power $q = p^a$ is called exceptional if $a \geqslant 3$ is odd and p divides $\lfloor 2\sqrt{q} \rfloor$. From [10, Corollary 9.94], one has the following result.

Lemma 2.7. *The value $N_q(1)$ can be determined explicitly as follows:*

$$N_q(1) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor, & \text{if } q \text{ is exceptional,} \\ q + 1 + \lfloor 2\sqrt{q} \rfloor, & \text{otherwise.} \end{cases}$$

3. A NEW CONSTRUCTION OF NONLINEAR CODES

Let q be a prime power. Let $\mathbb{F}_q = \{\alpha_1, \alpha_2, \cdots, \alpha_q\}$ be the finite field with q elements. Denote by Σ the set $\mathbb{F}_q \cup \{\infty\}$. The size of Σ is $|\Sigma| = q + 1$. In this section, we will propose a construction of $(q + 1)$-ary nonlinear codes over the code alphabet Σ via algebraic function fields by generalizing the ideas given in [12] and [21].

Proposition 3.1. *Let $F/\mathbb{F}_q$ be an algebraic function field with genus g and D be a divisor of F with $\deg(D) = m \geqslant 2g - 1$. Let $Q_1, Q_2, \cdots, Q_t$ be distinct places of F with $\deg(Q_i) = r_i$. Let $G = \sum_{i=1}^{t} m_i Q_i$ be a divisor of F with $\deg(G) = \sum_{i=1}^{t} m_i r_i = s$ and $m_i \geqslant 1$ for $1 \leqslant i \leqslant t$. Consider the set*

$$\mathcal{L}_D(G) = \{f \in \mathcal{L}(D + G) | \nu_{Q_i}(f) = -m_i - \nu_{Q_i}(D) \text{ for all } 1 \leqslant i \leqslant t\}.$$

Then the cardinality of $\mathcal{L}_D(G)$ is

$$|\mathcal{L}_D(G)| = q^{m+s-g+1} \prod_{i=1}^{t} \left(1 - \frac{1}{q^{r_i}}\right) \geqslant q^{m-g+1}(q-1)^s.$$

Proof. From the definition of $\mathcal{L}_D(G)$, it is clear that

$$\mathcal{L}_D(G) = \mathcal{L}(D + G) - \cup_{i=1}^{t} \mathcal{L}(D + G - Q_i).$$

From the Riemann-Roch Theorem [20, Theorem 1.5.14], the size of $\mathcal{L}(D + G)$ is

$$|\mathcal{L}(D + G)| = q^{\deg(D+G)-g+1} = q^{m+s-g+1}.$$

From the inclusion-exclusion principle of combinatorics, the cardinality of $\cup_{i=1}^{t} \mathcal{L}(D + G - Q_i)$ can be calculated explicitly as follows:

$$\begin{aligned}
|\cup_{i=1}^{t} \mathcal{L}(D + G - Q_i)| &= \sum_{k=1}^{t} (-1)^{k-1} \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant t} |\cap_{j=1}^{k} \mathcal{L}(D + G - Q_{i_j})| \\
&= \sum_{k=1}^{t} (-1)^{k-1} \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant t} |\mathcal{L}(D + G - \sum_{j=1}^{k} Q_{i_j})| \\
&= \sum_{k=1}^{t} (-1)^{k-1} \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant t} q^{m+s-g+1-\sum_{i=1}^{k} r_{i_j}} \\
&= q^{m+s-g+1} \sum_{k=1}^{t} (-1)^{k-1} \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant t} q^{-\sum_{i=1}^{k} r_{i_j}} \\
&= q^{m+s-g+1} \left[1 - \prod_{i=1}^{t} \left(1 - \frac{1}{q^{r_i}}\right)\right].
\end{aligned}$$

Hence, the cardinality of $\mathcal{L}_D(G)$ is

$$|\mathcal{L}_D(G)| = q^{m+s-g+1} \prod_{i=1}^{t} \left(1 - \frac{1}{q^{r_i}}\right) \geqslant q^{m+s-g+1} \prod_{i=1}^{t} \left(1 - \frac{1}{q}\right)^{r_i}$$

$$\geqslant q^{m+s-g+1} \left(1 - \frac{1}{q}\right)^{\sum_{i=1}^{t} m_i r_i} = q^{m+s-g+1} \left(1 - \frac{1}{q}\right)^{s} = q^{m-g+1}(q-1)^s.$$

$\square$

Lemma 3.2. *Let G_1 and G_2 be two distinct positive divisors of F. Then we have $\mathcal{L}_D(G_1) \cap \mathcal{L}_D(G_2) = \emptyset$.*

Proof. Suppose that there exists an element $f \in \mathcal{L}_D(G_1) \cap \mathcal{L}_D(G_2)$. We first claim that $\mathrm{supp}(G_1) = \mathrm{supp}(G_2)$. If there exists a place $Q \in \mathrm{supp}(G_i) \backslash \mathrm{supp}(G_j)$ for $i \neq j \in \{1, 2\}$, then we have $\nu_Q(f) = -\nu_Q(G_i) - \nu_Q(D) \leqslant -\nu_Q(D) - 1$ and $\nu_Q(f) \geqslant -\nu_Q(G_j) - \nu_Q(D) = -\nu_Q(D)$. This is impossible.

If $f \in \mathcal{L}_D(G_1) \cap \mathcal{L}_D(G_2)$, then we have $\nu_Q(f) = -\nu_Q(G_1) - \nu_Q(D) = -\nu_Q(G_2) - \nu_Q(D)$ for any place $Q \in \mathrm{supp}(G_1) \cup \mathrm{supp}(G_2)$. Hence, we have $\nu_Q(G_1) = \nu_Q(G_2)$ for any place $Q \in \mathbb{P}_F$, i.e., $G_1 = G_2$, which is a contradiction to $G_1 \neq G_2$. $\square$

Construction: The construction of our nonlinear codes is given explicitly as follows. Let $F/\mathbb{F}_q$ be an algebraic function field of genus g. Let $P_1, P_2, \cdots, P_n$ be rational places of $F/\mathbb{F}_q$. Let s be a positive integer. For any positive integer $r \geqslant 4g+3$, there exist two places R_{r+1} and R_r in $\mathbb{P}_F$ with $\deg(R_{r+1}) = r+1$ and $\deg(R_r) = r$ respectively from [20, Corollary 5.2.10]. Let $D = m(R_{r+1} - R_r)$ be a divisor of F with $\deg(D) = m \geqslant 2g-1$. Consider the set

$$\mathcal{L}_s(D) := \bigcup_{G \geqslant 0, \deg(G) \leqslant s} \mathcal{L}_D(G),$$

where G runs over all effective divisors of F with $0 \leqslant \deg(G) \leqslant s$. Here we assume that $\mathcal{L}_D(0) = \mathcal{L}(D)$. Let Σ be the set $\mathbb{F}_q \cup \{\infty\}$. We define an evaluation map $\phi : \mathcal{L}_s(D) \to \Sigma^n$ by putting

$$\phi(f) = (f(P_1), f(P_2), \cdots, f(P_n))$$

for any element $f \in \mathcal{L}_s(D)$. The image of ϕ together with $\{(\infty, \infty, \cdots, \infty)\}$ is our nonlinear code $C := \phi(\mathcal{L}_s(D)) \cup \{(\infty, \infty, \cdots, \infty)\} \subseteq \Sigma^n$.

Theorem 3.3. *Let $F/\mathbb{F}_q$ be an algebraic function field of genus g with at least n rational places, and let A_i be the number of effective divisors of $F/\mathbb{F}_q$ with degree i. Let $m \geqslant 2g-1$ and let s be an non-negative integer with $n - m - 2s > 0$. Then the code C defined as above is a $(q+1)$-ary (n, M, d)-code with cardinality*

$$M = |C| \geqslant 1 + \sum_{i=0}^{s} (q-1)^i q^{m-g+1} A_i,$$

and minimum distance

$$d \geqslant n - m - 2s.$$

Proof. Under the assumption that the minimum distance of C is $d \geqslant n - m - 2s > 0$, it is clear that the evaluation map ϕ is injective. Hence, the cardinality of the code C is lower bounded by

$$M = |C| \geqslant 1 + \sum_{i=0}^{s} (q-1)^i q^{m-g+1} A_i$$

from Proposition 3.1 and Lemma 3.2. It is easy to see that the Hamming distance of $\phi(f)$ and $(\infty, \infty, \cdots, \infty)$ is at least $n - m - s$ for any $f \in \mathcal{L}_s(D)$. It will be sufficient to prove that the Hamming distance $d(\phi(f_1), \phi(f_2))$ of $\phi(f_1)$ and $\phi(f_2)$ is at least $n - m - 2s$ for any two distinct elements $f_1, f_2 \in \mathcal{L}_s(D)$.

Assume that $f_1 \in \mathcal{L}_D(G_1)$ and $f_2 \in \mathcal{L}_D(G_2)$ for effective divisors G_1, G_2 with $\deg(G_1) \leqslant s$ and $\deg(G_2) \leqslant s$ respectively, then $f_1 - f_2 \in \mathcal{L}(D + G_1 \vee G_2)$. If $P_i \in \operatorname{supp}(G_1) \cap \operatorname{supp}(G_2)$, then $f_1 - f_2 \in \mathcal{L}(D + G_1 + G_2 - P_i)$ from Lemma 2.1. Hence, we have

$$f_1 - f_2 \in \mathcal{L}\left(D + G_1 + G_2 - \sum_{P_i \in \operatorname{supp}(G_1) \cap \operatorname{supp}(G_2)} P_i\right).$$

Let Z be a subset of $\{1, 2, \cdots, n\}$ defined by

$$Z := \{1 \leqslant j \leqslant n | P_j \notin \operatorname{supp}(G_1) \cup \operatorname{supp}(G_2) \text{ and } f_1(P_j) = f_2(P_j)\}.$$

From Lemma 2.1, we have

$$0 \neq f_1 - f_2 \in \mathcal{L}\left(D + G_1 + G_2 - \sum_{P_i \in \operatorname{supp}(G_1) \cap \operatorname{supp}(G_2)} P_i - \sum_{j \in Z} P_j\right).$$

It follows that

$$m + \deg(G_1) + \deg(G_2) - |\operatorname{supp}(G_1) \cap \operatorname{supp}(G_2)| - |Z| \geqslant 0.$$

On the other hand, the Hamming distance of $\phi(f_1)$ and $\phi(f_2)$ is

$$d(\phi(f_1), \phi(f_2)) \geqslant n - |\operatorname{supp}(G_1) \cap \operatorname{supp}(G_2)| - |Z|.$$

Hence, the minimum distance d of the code C is lower bounded by

$$\begin{aligned} d &\geqslant n - |\operatorname{supp}(G_1) \cap \operatorname{supp}(G_2)| - |Z| \\ &\geqslant n - m - \deg(G_1) - \deg(G_2) \\ &\geqslant n - m - 2s. \end{aligned}$$

$\square$

Corollary 3.4. *Let $F/\mathbb{F}_q$ be an algebraic function field of genus g with at least n rational places, and let A_i be the number of effective divisors of $F/\mathbb{F}_q$ with degree i. Let m be a positive integer with $m \geqslant 2g-1$. For a fixed minimum distance $2 \leqslant d \leqslant n-m$, there exists a $(q+1)$-ary (n, M, d)-code with cardinality*

$$M \geqslant 1 + \max_{2g-1 \leqslant m \leqslant n-d} \left\{ \sum_{i=0}^{[(n-d-m)/2]} (q-1)^i q^{m-g+1} A_i \right\},$$

here $[x]$ is the integer part of $x \in \mathbb{R}$.

Proof. This corollary follows from Theorem 3.3 and [14, Theorem 6.1.1]. $\square$

4. Nonlinear codes via elliptic curves

In this section, we provide an explicit construction of nonlinear codes via elliptic curves given in Section 3.

Let $E/\mathbb{F}_q$ be an elliptic curve defined over a finite field $\mathbb{F}_q$. Let $N(E)$ be the number of rational points of elliptic curve $E/\mathbb{F}_q$. From [20, Theorem 5.1.15], the L-polynomial of the elliptic curve $E/\mathbb{F}_q$ is given by $L(t) = 1 + (N(E) - q - 1)t + qt^2 \in \mathbb{Z}[t]$, i.e., $a_0 = 1$, $a_1 = N(E) - q - 1$, $a_2 = q$ and $a_j = 0$ for $j \geqslant 3$. From Lemma 2.2, the number of effective divisors of $E/\mathbb{F}_q$ with degree i is given by $A_i = \sum_{j=0}^{i} a_j(q^{i+1-j} - 1)/(q-1)$. Let $m \geqslant 2g(E) - 1 = 1$ and s be two non-negative integers. From Theorem 3.3, there exists a $(q+1)$-ary (n, M, d) nonlinear code with length $n = N(E)$, size $M \geqslant 1 + \sum_{i=0}^{s} (q-1)^i q^m A_i$, and minimum distance $d \geqslant n-m-2s > 0$. Hence, the following proposition follows from Corollary 3.4.

Proposition 4.1. *Let $E/\mathbb{F}_q$ be an elliptic curve with $N(E)$ rational points. For $q+3 \leqslant n \leqslant N(E)$ and $2 \leqslant d \leqslant n-1$, there exists a $(q+1)$-ary (n, M, d)-nonlinear code C_E with cardinality $M = |C_E| \geqslant 1 + \sum_{i=0}^{[(n-d-m)/2]} (q-1)^i q^m A_i$ for all $1 \leqslant m \leqslant n-d$.*

In the following, we want to compare our nonlinear codes via elliptic curves with the codes obtained from propagation rules given in Lemma 2.4.

4.1. **Alphabet extension.** In this subsection, we compare our nonlinear codes via elliptic curves with the codes constructed via the alphabet extension of elliptic codes. If $q+3 \leqslant n \leqslant N(E)$, then there exists a q-ary $[n, n-d, d]$-linear code constructed from elliptic curve $E/\mathbb{F}_q$. Furthermore, the nontrivial q-ary $[n, n-d+1, d]$-elliptic MDS code doesn't exist from Lemma 2.6, i.e., the q-ary $[n, n-d, d]$-linear code is the best-known linear code for given length n and minimum distance d in the literature. From Lemma 2.4, there exists a $(q+1)$-ary (n, q^{n-d}, d)-nonlinear code via code alphabet extension.

Proposition 4.2. *Let $E/\mathbb{F}_q$ be an elliptic curve with $N(E)$ rational points. For $q+3 \leqslant n \leqslant N(E)$ and $2 \leqslant d \leqslant n-1$, there exists a $(q+1)$-ary (n, M, d)-nonlinear code C_E with cardinality bigger than q^{n-d}, i.e., the size of the $(q+1)$-ary nonlinear code C_E via*

elliptic curves is larger than the size of codes constructed from code alphabet extension of elliptic codes.

Proof. From Proposition 4.1, for $m = n-d$, there exists a $(q+1)$-ary (n, M, d)-nonlinear code C_E with cardinality

$$M = |C_E| \geqslant 1 + (q-1)^0 q^m A_0 = 1 + q^{n-d} > q^{n-d}.$$

$\square$

4.2. **Alphabet restriction.** If $q + 2$ is a prime power as well, then there exists a $(q+2)$-ary $[n, n - d, d]$-linear code from elliptic codes. From Lemma 2.4, there exists a $(q + 1)$-ary $\left(n, M' \geqslant \frac{(q+1)^n}{(q+2)^d}, d\right)$-nonlinear code via code alphabet restriction of elliptic codes. In the case where $q + 2$ is not a prime, we are not sure if there are still exists a $(q+2)$-ary $(n, (q+2)^{n-d}, d)$-code for $n > q+1$. Nevertheless, no matter whether $q + 2$ is a prime or not, we use $(q+2)$-ary $(n, (q+2)^{n-d}, d)$-codes to compare with our codes in the following proposition.

Proposition 4.3. *Let $E/\mathbb{F}_q$ be an elliptic curve with $N(E)$ rational points. If $q+1 \leqslant n \leqslant N(E)$ and $d \geqslant n \cdot \ln(1 + \frac{1}{q})/\ln(1 + \frac{2}{q})$, then there exists a $(q + 1)$-ary (n, M, d) nonlinear code C_E with cardinality larger than $\frac{(q+1)^n}{(q+2)^d}$, i.e., the size of the $(q + 1)$-ary nonlinear code C_E is larger than the size of codes constructed from code alphabet restriction of $(q + 2)$-ary $(n, (q + 2)^{n-d}, d)$-codes for sufficiently large d.*

Proof. From Proposition 4.1, there exists a $(q + 1)$-ary (n, M, d) nonlinear code C_E with cardinality

$$M = |C_E| \geqslant 1 + \sum_{i=0}^{1} (q-1)^i q^{n-d-2} A_i \geqslant 1 + q^{n-d-2}[1 + (q-1)n].$$

It is easy to verify that

$$q^{n-d-2}[1 + (q-1)n] \geqslant \frac{(q+1)^n}{(q+2)^d} \quad \Leftrightarrow \quad \frac{(q+2)^d}{q^d} \geqslant \frac{(q+1)^n}{q^n} \cdot \frac{q^2}{1 + (q-1)n}.$$

If $n \geqslant q + 1$ and $d \geqslant n \cdot \ln(1 + \frac{1}{q})/\ln(1 + \frac{2}{q})$, then we have $M > (q+1)^n/(q+2)^d$. $\square$

Remark 1. If q is a prime power, then $q + 2$ may not be a prime power. Let n be a positive integer with $q + 1 \leqslant n \leqslant N_q(1)$. Let $q + a$ be the least prime power satisfying $q + a \geqslant n - 1$. Then there exists a $(q + a)$-ary $[n, n + 1 - d, d]$-MDS code from rational algebraic geometry codes. Hence, we can obtain a $(q + 1)$-ary $\left(n, M' \geqslant \frac{(q+1)^n}{(q+a)^{d-1}}, d\right)$-nonlinear code via code alphabet restriction of the above MDS code. In particular, if $n = q + 1 + \lfloor 2\sqrt{q} \rfloor$, then we choose $a \geqslant \lfloor 2\sqrt{q} \rfloor$ to be an integer such that $q + a$ is a prime power. From Proposition 4.3, there exists a $(q + 1)$-ary (n, M, d)-nonlinear code

C_E with cardinality $M \geqslant 1 + q^{n-d-2}[1 + (q-1)n]$. It is easy to verify that

$$q^{n-d-2}[1 + (q-1)n] \geqslant (q+a)^{n-d+1} \left(\frac{q+1}{q+a} \right)^n = \frac{(q+1)^n}{(q+a)^{d-1}}$$

if and only if

$$\frac{(q+a)^d}{q^d} \geqslant \frac{(q+1)^n(q+a)}{q^n} \cdot \frac{q^2}{1 + (q-1)n}.$$

If $d \geqslant [n \cdot \ln(1 + \frac{1}{q}) + \ln(q+a)] / \ln(1 + \frac{a}{q})$, then we have

$$M > \frac{(q+1)^n}{(q+a)^{d-1}}.$$

4.3. **Numerical examples.** In this subsection, we provide numerical examples from nonlinear codes via elliptic curves and compare our nonlinear codes with other $(q+1)$-ary nonlinear codes via code alphabet extension and restriction. Although Proposition 4.3 shows that our codes are better than those obtained from alphabet restriction for sufficiently large minimum distance d, our numerical results show that even for small d, our codes still outperform those obtained from code alphabet restriction.

Example 4.4. Let $E/\mathbb{F}_5$ be the function field defined by $E = \mathbb{F}_5(x,y)$ with $y^2 = 3(x^4 + 2)$ given in [19]. All rational places of $\mathbb{F}_5(x)$ except the infinite place ∞ split completely in $E/\mathbb{F}_5(x)$, and the genus of E is one from the theory of Kummer extension [20, Proposition 3.7.3]. Hence, the elliptic function field E has 10 rational places which achieves the Serre bound, i.e., $N_5(1) = 10$. The L-polynomial of $E/\mathbb{F}_q$ is given by $L(t) = 1 + 4t + 5t^2 \in \mathbb{Z}[t]$, i.e., $a_0 = 1$, $a_1 = 4$, $a_2 = 5$ and $a_j = 0$ for $j \geqslant 3$. From Lemma 2.2, the number of effective divisors of $E/\mathbb{F}_5$ of degree i is given by $A_i = \sum_{j=0}^{i}(5^{i+1-j} - 1)a_j/4$. Let d be an integer with $2 \leqslant d \leqslant 9$. From Theorem 3.3 and Corollary 3.4, there exists a 6-ary $(10, M, d)$-nonlinear code with size

$$M \geqslant 1 + \sum_{i=0}^{[(10-d-m)/2]} 4^i \cdot 5^m A_i,$$

for any integer $1 \leqslant m \leqslant 10 - d$.

In the following table, we compare the codes given in Example 4.4 with those obtained via code alphabet extension and restriction. Note that to obtain codes via code extension and restriction, we have to start with a code of the best-known parameters. However, we are lack of nonlinear codes with the best-known parameters. Instead, we choose linear codes with the best-known parameters given in the online table [6].

We use the case where $q = 5, n = 10$ and $d = 4$ to illustrate the following table. In this case, we start with 5-ary $[10, 6, 4]$ and 7-ary $[10, 6, 4]$-linear codes and then apply code alphabet extension and restriction to obtain 6-ary codes with sizes 15625 and 25184, respectively. From the online table [6], there exist 2-ary $[10, 5, 4]$ and 3-ary $[10, 6, 4]$-linear codes and then apply code alphabet multiplication given in Lemma 2.4

to obtain a 6-ary code with size 23328. In the last column, we provide code sizes obtained from Example 4.4.

Table I

Comparison of sizes of 6-ary codes of length 10

Distance d	Alphabet extension	Alphabet restriction	Alphabet multiplication	Example 4.4
4	15625	25184	23328	**25626**
5	3125	3598	1000	**5126**
6	625	514	324	**1026**
7	125	74	18	**206**
8	25	11	6	**42**

Example 4.5. Let $E/\mathbb{F}_9$ be the function field defined by $E = \mathbb{F}_9(x, y)$ with $y^2 = x^4 + 1$ given in [19]. In fact, $E/\mathbb{F}_9$ is a maximal elliptic function field with 16 rational places from [19] and the L-polynomial of $E/\mathbb{F}_q$ is $L(t) = 1 + 6t + 9t^2 \in \mathbb{Z}[t]$, i.e., $a_0 = 1$, $a_1 = 6$, $a_2 = 9$ and $a_j = 0$ for $j \geqslant 3$. From Lemma 2.2, we have $A_i = \sum_{j=0}^{i}(9^{i+1-j} - 1)a_j/8$. Let d be an integer with $2 \leqslant d \leqslant 15$. From Theorem 3.3 and Corollary 3.4, there exists a 10-ary $(16, M, d)$ nonlinear code with size

$$M \geqslant 1 + \sum_{i=0}^{[(16-d-m)/2]} 8^i \cdot 9^m A_i,$$

for any integer $1 \leqslant m \leqslant 16 - d$.

From Example 4.4, the size of codes via code alphabet multiplication turns out to be not good enough for large minimum distance d. Hence, we only compare the codes given in Example 4.5 with those obtained via code alphabet extension and restriction in the following table. In particular, we use 11-ary $[16, k, 16 - k]$-linear codes for comparison with the codes via code alphabet restriction.

Table II

Comparison of sizes of 10-ary codes of length 16

Minimum distance d	Alphabet extension	Alphabet restriction	Example 4.5
7	$387, 420, 489$	$513, 158, 119$	**617,003,002**
8	$43, 046, 721$	$46, 650, 739$	**68,555,890**
9	$4, 782, 969$	$4, 240, 977$	**7,617,322**
10	$531, 441$	$385, 544$	**846,370**
11	$59, 049$	$35, 050$	**94,042**
12	$6, 561$	$3, 187$	**10,450**
13	729	290	**1,162**
14	81	27	**130**

5. Nonlinear codes via maximal function fields

In this section, we provide an explicit construction of nonlinear codes via maximal function fields given in Section 3.

Let $F/\mathbb{F}_q$ be a maximal function field of genus g. If $g \geqslant 1$, then q must be a square of a prime power. Otherwise, $F/\mathbb{F}_q$ is the rational function field over $\mathbb{F}_q$ for any prime power. The number of rational places of F is $N(F) = q + 1 + 2g\sqrt{q}$ and the L-polynomial of $F/\mathbb{F}_q$ is $L(t) = (1 + \sqrt{q}t)^{2g} \in \mathbb{Z}[t]$. Hence, we have $a_j = \binom{2g}{j}\sqrt{q}^j$ for $0 \leqslant j \leqslant 2g$ and $a_j = 0$ for $j \geqslant 2g + 1$. From Lemma 2.2, the number of effective divisors of $F/\mathbb{F}_q$ is $A_i = \sum_{j=0}^{i} a_j(q^{i+1-j} - 1)/(q - 1)$. Let $m \geqslant 2g - 1$ and let s be an non-negative integer with $n - m - 2s > 0$. From Theorem 3.3, there exists a $(q+1)$-ary (n, M, d)-nonlinear code with length $q + 1 \leqslant n \leqslant q + 1 + 2g\sqrt{q}$, size $M \geqslant 1 + \sum_{i=0}^{s}(q-1)^i q^{m+1-g} A_i$, and minimum distance $d \geqslant n - m - 2s$. From Corollary 3.4, there exists a $(q+1)$-ary (n, M, d)-nonlinear code C with size

$$M = |C| \geqslant 1 + \max_{2g-1 \leqslant m \leqslant n-d} \left\{ \sum_{i=0}^{[(n-d-m)/2]} (q-1)^i q^{m-g+1} A_i \right\}.$$

5.1. **Alphabet extension.** If $q + 1 \leqslant n \leqslant q + 1 + 2g\sqrt{q}$, then there exists a q-ary $[n, n-g+1-d, d]$-linear code constructed from the maximal function field $F/\mathbb{F}_q$. From Lemma 2.4, there exists a $(q+1)$-ary $(n, q^{n-g+1-d}, d)$-nonlinear code via code alphabet extension of algebraic geometry codes.

Proposition 5.1. *Let $F/\mathbb{F}_q$ be a maximal function field with genus g. For $q + 1 \leqslant n \leqslant q + 1 + 2g\sqrt{q}$ and $2 \leqslant d \leqslant n - g$, there exists a $(q+1)$-ary (n, M, d)-nonlinear code C_F with cardinality larger than $q^{n-g+1-d}$, i.e., the size of the $(q+1)$-ary nonlinear code C_F is larger than the size of codes constructed from code alphabet extension of $[n, n-g+1-d, d]$-algebraic geometry codes.*

Proof. Let $m = n - d - 2$. From Theorem 3.3 and the fact that the number of effective divisors of E degree one is $A_1 = q + 1 + 2g\sqrt{q}$, there exists a $(q+1)$-ary (n, M, d)-nonlinear code C_F with cardinality

$$M \geqslant 1 + \sum_{i=0}^{1}(q-1)^i q^{n-d-2-g+1} A_i = 1 + q^{n-g-d-1}[1 + (q-1)(q+1+2g\sqrt{q})].$$

It is easy to verify that

$$M \geqslant 1 + q^{n-g-d-1}[1 + (q-1)n] \geqslant 1 + q^{n-g-d-1}[1 + (q-1)(q+1)] > q^{n-g+1-d}.$$

$\square$

5.2. **Alphabet restriction.** If $q + 2$ is a prime power as well, then there exists a $(q+2)$-ary $[n, n-g+1-d, d]$-linear code from algebraic geometry codes. Since there may be a lack of the parameters of the optimal linear codes for given q, n and d, the algebraic geometry codes are good candidate for optimal linear codes for large length n compared with q. From Lemma 2.4, there exists a $(q+1)$-ary $\left(n, M' \geqslant \frac{(q+1)^n}{(q+2)^{d+g-1}}, d\right)$-nonlinear code via code alphabet restriction of algebraic geometry codes. Again, in the case where $q + 2$ is not a prime, we are not sure if there still exists a $(q+2)$-ary

$(n, (q+2)^{n-d-g+1}, d)$-code for $n = q+1+2g\sqrt{q}$. Nevertheless, no matter whether $q+2$ is a prime or not, we use $(q+2)$-ary $(n, (q+2)^{n-d-g+1}, d)$-codes to compare with our codes in the following proposition.

Proposition 5.2. *Let $F/\mathbb{F}_q$ be a maximal function field with genus g. If $q+1 \leqslant n \leqslant q+1+2g\sqrt{q}$ and $d \geqslant 1 - g + n \cdot \ln(1 + \frac{1}{q})/\ln(1 + \frac{2}{q})$, then there exists a $(q+1)$-ary (n, M, d)-nonlinear code C_F with cardinality larger than $\frac{(q+1)^n}{(q+2)^{d+g-1}}$, i.e., the size of the $(q+1)$-ary nonlinear code C_F is larger than the one constructed from code alphabet restriction of $(n, (q+2)^{n-d-g+1}, d)$-codes for sufficiently large d.*

Proof. From Proposition 5.1, there exists a $(q+1)$-ary (n, M, d)-nonlinear code C_F with cardinality $M = |C_F| \geqslant 1 + q^{n-g-d-1}[1 + (q-1)n]$. It is easy to verify that

$$q^{n-g-d-1}[1 + (q-1)n] \geqslant \frac{(q+1)^n}{(q+2)^{d+g-1}}$$

if and only if

$$\frac{(q+2)^{d+g-1}}{q^{d+g-1}} \geqslant \frac{(q+1)^n}{q^n} \cdot \frac{q^2}{1 + (q-1)n}.$$

If $d \geqslant 1 - g + n \cdot \ln(1 + \frac{1}{q})/\ln(1 + \frac{2}{q})$, then we have

$$M > (q+1)^n/(q+2)^{d+g-1}.$$

This completes the proof. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

5.3. **Numerical examples.** In this subsection, we provide numerical examples from our nonlinear codes via maximal function fields and compare our nonlinear codes with other $(q+1)$-ary nonlinear codes via code alphabet extension and restriction.

Example 5.3. Let $F/\mathbb{F}_q$ be the rational function field $\mathbb{F}_q(x)$. Its L-polynomial is $L(t) = 1 \in \mathbb{Z}[t]$. From Lemma 2.2, we have $A_i = (q^{i+1} - 1)/(q - 1)$ for all $i \in \mathbb{N}$. From Theorem 3.3, there exists a $(q+1)$-ary (n, M, d)-nonlinear code with length $n = q+1$ and size

$$M \geqslant 1 + q^{n+1-d} > (q+1)^n/(q+2)^{d-1}.$$

From Propositions 5.1 and 5.2, the size of our nonlinear codes via the rational function field is better than the one obtained from code alphabet extension and restriction of MDS codes. In particular, if $D = 0$, then the nonlinear code constructed in Theorem 3.3 is the same as the one given in [12]. The size of such code C has been determined explicitly as $|C| = q^{2s+1} + q^{2s} - 2q^s + 2$ and the minimum distance of C is exactly $d = q + 1 - 2s$ from [12, Theorem III.5]. Furthermore, it has been shown that $q^{2s+1} + q^{2s} - 2q^s + 2 > (q+1)^{2s}$ for $s \leqslant q/2$. Hence, the code C is a $(q+1)$-ary $(q+1, M, d)$-nonlinear code satisfying $n < \log_{q+1} M + d \leqslant n + 1$. It turns out that the code C is quite good at the trade-off between information rate and minimum distance.

Example 5.4. Let $H/\mathbb{F}_9$ be the Hermitian function field $H = \mathbb{F}_9(x, y)$ defined by $y^3 + y = x^4$. From [20, Lemma 6.4.4], H is a maximal function field of genus $g = 3$ and the number of rational places of H is $N(H) = 28$. Hence, the L-polynomial of $H/\mathbb{F}_9$ is given by $L_H(t) = (1 + 3t)^6 \in \mathbb{Z}[t]$, i.e., $a_j = \binom{6}{j} \cdot 3^j$ for $0 \leqslant j \leqslant 6$ and $a_j = 0$ for $j \geqslant 7$. From Lemma 2.2, the number of effective divisors of $H/\mathbb{F}_9$ is $A_i = \sum_{j=0}^{i} a_j(9^{i+1-j} - 1)/8$. For $2 \leqslant d \leqslant 23$, from Theorem 3.3 and Corollary 3.4, there exists a 10-ary $(28, M, d)$-nonlinear code with size $M \geqslant 1 + \sum_{i=0}^{[(28-d-m)/2]} 8^i \cdot 9^{m-2} A_i$, for any $5 \leqslant m \leqslant 28 - d$.

Table III

Comparison of sizes of 10-ary codes of length 28

Minimum distance d	Alphabet extension code size	Alphabet restriction code size	Example 5.4
6	1.22×10^{19}	4.67×10^{19}	$\mathbf{4.85 \times 10^{19}}$
7	1.35×10^{18}	4.24×10^{18}	$\mathbf{5.39 \times 10^{18}}$
8	1.50×10^{17}	3.86×10^{17}	$\mathbf{5.99 \times 10^{17}}$
9	1.67×10^{16}	3.50×10^{16}	$\mathbf{6.66 \times 10^{16}}$
10	1.85×10^{15}	3.19×10^{15}	$\mathbf{7.40 \times 10^{15}}$
11	2.06×10^{14}	2.90×10^{14}	$\mathbf{8.22 \times 10^{14}}$
12	2.29×10^{13}	2.63×10^{13}	$\mathbf{9.13 \times 10^{13}}$
13	2.54×10^{12}	2.39×10^{12}	$\mathbf{1.01 \times 10^{13}}$
14	2.82×10^{11}	2.18×10^{11}	$\mathbf{1.12 \times 10^{12}}$
15	3.14×10^{10}	1.98×10^{10}	$\mathbf{1.25 \times 10^{11}}$
16	3.49×10^{9}	1.80×10^{9}	$\mathbf{1.39 \times 10^{10}}$
17	3.87×10^{8}	1.64×10^{8}	$\mathbf{1.54 \times 10^{9}}$
18	4.30×10^{7}	1.49×10^{7}	$\mathbf{1.71 \times 10^{8}}$
19	4.78×10^{6}	1.35×10^{6}	$\mathbf{1.91 \times 10^{7}}$
20	5.31×10^{5}	1.23×10^{5}	$\mathbf{2.12 \times 10^{6}}$
21	$59,049$	$11,168$	$\mathbf{235,882}$
22	$6,561$	$1,016$	$\mathbf{26,210}$

Note that for those comparison, we are lack of the parameters of 11-ary codes from the online table [6] for code alphabet restriction, here we use 11-ary $[28, 26 - d, d]$-algebraic geometry codes.

REFERENCES

[1] A. Barg, I. Tamo, and S. Vlăduţ, *Locally recoverable codes on algebraic curves*, IEEE Trans. Inf. Theory, vol. 63, no. 8, pp. 4928–4939, Aug. 2017.

[2] A. Bassa, L. Ma, C. Xing and S. Yeo, Towards a characterization of subfields of the Deligne–Lusztig function fields, J. Combin. Theory, Series A, vol. 120, pp. 1351–1371, Sep. 2013.

[3] P. Beelen and M. Montanucci, *A new family of maximal curves*, J. London Math. Soc., vol. 98, no. 2, pp. 573–592, 2018.

[4] A. Garcia, H. Stichtenoth and C. Xing, *On subfields of the Hermitian function fields*, Compos. Math., vol. 120, pp. 137–170, 2000.

[5] M. Giulietti and G. Korchmaros, *A new family of maximal curves over a finite field*, Math. Ann., vol. 343, pp. 229–245, 2009.

[6] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, Online available at http://www.codetables.de., accessed on 2022-08-13.

[7] T. Gulliver and M. Harada, *Extremal self-dual codes over $\mathbb{Z}_6$, $\mathbb{Z}_8$ and $\mathbb{Z}_{10}$*, AKCE J. Graphs. Combin., vol. 2, no. 1, pp. 11–24, 2005.

[8] M. Harada, *On the existence of extremal Type II codes over $\mathbb{Z}_6$*, Discrete Math., vol. 223, no. 1–3, pp. 373-378, Aug. 2000.

[9] M. Harada, and T. Miezaki, *An upper bound on the minimum weight of Type II $\mathbb{Z}_{2k}$-codes*, J. Combin. Theory, Series A, vol. 118, no. 1, pp. 190–196, Jan. 2011.

[10] J.W.P. Hirschfeld, G. Korchmaros and F. Torres, *Algebraic Curves over a Finite Field*, Princeton Series in Applied Mathematics, Princeton University Press, 2008.

[11] L. Jin, L. Ma and C. Xing, *Construction of optimal locally repairable codes via automorphism groups of rational function fields*, IEEE Trans. Inf. Theory, vol. 66, no. 1, pp. 210–221, Jan. 2020.

[12] L. Jin, L. Ma and C. Xing, *A new construction of nonlinear codes via rational function fields*, IEEE Trans. Inf. Theory, vol. 67, no. 2, pp. 770–777, Feb. 2021.

[13] X. Li, L. Ma and C. Xing, *Optimal locally repairable codes via elliptic curves*, IEEE Trans. Inf. Theory, vol. 65, no. 1, pp. 108–117, Jan. 2019.

[14] S. Ling and C. Xing, *Coding Theory: A First Course*, Cambridge University Press, Cambridge, 2004.

[15] C. Munuera, *On MDS elliptic curves*, Discrete Math., vol. 117, pp. 279–286, 1993.

[16] L. Ma and C. Xing, *On subfields of the Hermitian function field involving the involution automorphism*, J. Number Theory, vol. 198, pp. 293–317, May 2019.

[17] L. Ma and C. Xing, *Constructive asymptotic bounds of locally repairable codes via function fields*, IEEE Trans. Inf. Theory, vol. 66, no. 9, pp. 5395–5403, Sep. 2020.

[18] L. Ma and C. Xing, *The group structures of automorphism groups of elliptic function fields over finite fields and optimal locally repairable codes*, arXiv:2008.12119.

[19] H. Niederreiter and C. Xing, *Cyclotomic function fields, Hilbert class fields, and global function fields with many rational places*, Acta Arith., pp. 59–38, 1997.

[20] H. Stichtenoth, *Algebraic Function Fields and Codes* (Graduate Texts in Mathematics), vol. 254, Berlin, Germany: Springer Verlag, 2009.

[21] H. Stichtenoth and C. Xing, *Excellent nonlinear codes from algebraic function fields*, IEEE Trans. Inf. Theory, vol. 51, no. 11, pp. 4044–4046, Nov. 2005.

[22] J. Walker, *The Nordstrom-Robinson code is algebraic-geometric*, IEEE Trans. Inf. Theory, vol. 43, no. 5, pp. 1588-1593, Sep. 1977.

[23] C. Xing, *Asymptotically good nonlinear codes from algebraic curves*, IEEE Trans. Inf. Theory, vol. 57, no. 9, pp. 5991–5995, Sep. 2011.

Natl Key Lab Sci and Technol Commun, University of Electronic Science and Technology of China, Chengdu, China.
Email address: shuliu@uestc.edu.cn

School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China
Email address: lmma20@ustc.edu.cn

Theory Lab, Central Research Institute, 2012 Labs, Huawei Technologies Co. Ltd., Hong Kong SAR, China
Email address: wu.ting.yi@huawei.com

School of Electronics, Information and Electric Engineering, Shanghai Jiao Tong University, China 200240
Email address: xingcp@sjtu.edu.cn