A New Construction of Nonlinear Codes via Algebraic Function Fields

Shu Liu, Member, IEEE, Liming Ma, Senior Member, IEEE, Ting-Yi Wu, and Chaoping Xing, Senior Member, IEEE

Abstract—In coding theory, constructing codes with good parameters is one of the most important and fundamental problems. A great many good codes have been constructed over alphabets of sizes equal to prime powers, however, good block codes over other alphabet sizes are rare. 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 evaluating rational functions at all rational places of an 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 \(F_q \cup \{\infty\}\). 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.

Index Terms—Nonlinear codes, Riemann-Roch spaces, rational places, algebraic geometry codes.

I. 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, one hopes 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 any block code. One of the well-known upper bounds is the Singleton bound which says that \(M \leq q^n - d + 1\). A linear code achieving this bound is called a maximum distance separable (MDS) code.

A lot of 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 other practical advantages. There are several families of nonlinear codes that are well known and important in coding theory, such as Hadamard matrix codes, Nordstrom-Robinson code, Preparata codes and Kerdock codes [12]. For some parameters, examples shows that linear codes do not exist but nonlinear codes do. For example, there are no binary \([16, 8, 6]\)-linear codes. On the other hand, the Nordstrom-Robinson code is a binary \((16, 2^6, 6)\)-nonlinear code [19], which can be viewed as an image under the Gray map of an algebraic geometry code over \(Z/4Z\) in [23]. Moreover, there exist asymptotically good \(q\)-ary nonlinear codes over \(F_q\) which exceed the Gilbert-Varshamov bound [3], [22]. Thus, 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. In [24], the author provided a family of \((q + 1)\)-ary nonlinear codes exceeding the asymptotic Gilbert-Varshamov bound. There exist many nonlinear codes over alphabets with small cardinality, such as \(Z_4\), \(Z_6\), \(Z_{10}\) or \(Z_{12}\) in [7], [8], and [9].

In [11], an explicit construction of \((q + 1)\)-ary \((q + 1, q^{2m+1} + q^m - 2q^m + 2, q + 1 - 2m)\)-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. In this paper, we generalize the construction of nonlinear codes via rational function fields to arbitrary algebraic function fields. Our codes are constructed by evaluations of rational functions from a union of Riemann-Roch spaces 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 [11] can be exactly determined since the union of chosen Riemann-Roch spaces is clear in rational function fields, while only lower bounds of code sizes are provided for arbitrary function fields. However, our nonlinear codes have better parameters than those obtained from MDS codes or good algebraic geometry codes via code alphabet extension and restriction.

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

II. Preliminaries

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

A. 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 $\mathcal{P}_F$. Let $P \in \mathcal{P}_F$ 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 $G = \sum_{P \in \mathcal{P}_F} n_P P$ with only finitely many nonzero coefficients $n_P \in \mathbb{Z}$. Its support is defined as $\text{supp}(G) = \{P \in \mathcal{P}_F : n_P \neq 0\}$. If all coefficients of $G$ are non-negative, then the divisor $G$ is called effective. Let $\nu_P$ be the normalized discrete valuation of $P$. For any nonzero element $f \in F$, the zero divisor of $f$ is defined by $(f)_0 = \sum_{P \in \mathcal{P}_F, \nu_P(f) > 0} \nu_P(f)P$, and the pole divisor of $f$ is defined by $(f)_{\infty} = \sum_{P \in \mathcal{P}_F, \nu_P(f) < 0} -\nu_P(f)P$. Hence, the principal divisor of $f$ is given by

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

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

$$G \cup D := \sum_{P \in \mathcal{P}_F} \max\{n_P, m_P\} P$$

and

$$G \cap D := \sum_{P \in \mathcal{P}_F} \min\{n_P, m_P\} P.$$ 

It is clear that $(G \cap D) + (G \cup D) = G + D$.

B. 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 given by

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

From the Riemann-Roch theorem [21, Theorem 1.5.17], $L(G)$ is an $\mathbb{F}_q$-vector space of dimension $\ell(G) = \deg(G) - q + 1$. Moreover, the equality holds true if $\deg(G) \geq 2g - 1$. For any two divisors $G$ and $H$, it is straightforward to verify that $L(G) \cap L(H) = L(G \wedge H)$ and $L(G) + L(H) \subseteq L(G \vee H)$.

Lemma 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 $P \in \mathcal{P}_F$, then we have $f_1 - f_2 \in L(G_1 + G_2 - P)$.

Proof: Let $f_1(P) = f_2(P) \in \mathbb{F}_q$, 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 $f_1 - f_2 \in L(G - P)$. Since $f_1 - f_2 \in L(G_1) + L(G_2) \subseteq L(G_1 \cup G_2)$, it follows that $f_1 - f_2 \in L(G_1 \cup G_2) \subseteq L(G_1 + G_2 - P)$.

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

C. Zeta Functions

Let $F/\mathbb{F}_q$ be an algebraic function field with genus $g$. Let $A_1$ be the number of all effective divisors of $F/\mathbb{F}_q$ of degree $i \geq 0$. 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 [21, 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: Let $F/\mathbb{F}_q$ be an algebraic function field with genus $g$. Let $A_1$ 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

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

\qed
D. 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 \( d \). The reader may refer to [12] and [14] for more details on coding theory. There is a well-known upper bound on the size of codes which is called the Singleton bound [12, Theorem 5.4.1].

**Lemma 3:** For any integer \( q > 1 \), any positive integer \( n \) and any integer \( d \) with \( 1 \leq d \leq n \), let \( C \) be a \( q \)-ary \((n, M, d)\)-code. Then we have \( M \leq q^{n-d+1} \).

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 \( \Sigma \) the set \( \mathbb{F}_q \cup \{\infty\} \). The size of \( \Sigma \) is \( |\Sigma| = q + 1 \).

In this paper, we consider nonlinear codes over the alphabet \( \Sigma \). Let \( x, y \) be words of length \( n \) over \( \Sigma \). The Hamming distance of \( x \) and \( y \), denoted by \( d(x, y) \), is defined to be the number of places at which \( x \) and \( y \) differ. The minimum distance of \( C \) is defined by \( d(C) = \min\{d(x, y) : x, y \in C, x \neq y\} \).

From Lemma 3, any \((n, M, d)\)-code over \( \Sigma \) satisfies \( M \leq (q + 1)^{n-d+1} \). In order to obtain good lower bound on the size of code over \( \Sigma \), one could make use of the following propagation rules given in Exercises of [12, Chapter 6].

**Lemma 4:** (1) (Alphabet extension) Let \( s, r \) be two integers satisfying \( s \geq r > 1 \). If \( C \) is an \( r \)-ary \((n, M, d)\)-code, then there is an \( s \)-ary \((n, M, r)\)-code.

(2) (Alphabet restriction) Let \( s, r \) be two integers satisfying \( s \geq r > 1 \). If \( C \) is an \( s \)-ary \((n, M, d)\)-code, then there is an \( r \)-ary \((n, M', d')\)-code with \( M' \geq M(r/s)^n \) and \( d' \geq d \).

(3) (Alphabet multiplication) Let \( r \) and \( s \) be two integers bigger than \( 1 \). If \( C_1 \) is an \( r \)-ary \((n_1, M_1, d_1)\)-code and \( C_2 \) is an \( s \)-ary \((n_2, M_2, d_2)\)-code, then there is an \( rs \)-ary \((n_1M_2, min\{d_1, d_2\})\)-code.

E. Algebraic Geometry Codes

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

\[
\phi : \mathcal{L}(G) \rightarrow \mathbb{F}_q^n, \quad \phi(f) = (f(P_1), f(P_2), \ldots, f(P_n)).
\]

From the Riemann-Roch Theorem, the dimension of \( C(D, G) \) is \( k = \ell(G) \geq \text{deg}(G) - g + 1 \) and the minimum distance of \( C(D, G) \) is lower bounded by \( d \geq n - \text{deg}(G) \). It is easy to see that \( n - g + 1 \leq k + d \leq n + 1 \). The following lemma gives the Hasse-Weil bound on the number of rational places of algebraic function fields over \( \mathbb{F}_q \) from [21, Theorem 5.2.3].

**Lemma 5:** Let \( \mathcal{F}/\mathbb{F}_q \) 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

\[
|N(F) - q - 1| \leq 2g\sqrt{q}.
\]

Any function field \( \mathcal{F}/\mathbb{F}_q \) 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, one needs to use algebraic function fields with many rational places, especially maximal function fields [1], [2], [4], [5], [16], [17].

If \( \mathcal{F}/\mathbb{F}_q \) is an elliptic function field, then the elliptic code \( C(D, G) \) is an \([n, k, d]\)-linear code with \( n \leq k + d \leq n + 1 \). 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 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 all function fields of genus \( g \) defined over \( \mathbb{F}_q \). A prime power \( q = p^m \) is called exceptional if \( m = 3 \) is odd and \( p \) divides \( 2\sqrt{q} \), where \( |x| \) is the integer part of \( x \in \mathbb{R} \). From [20, Theorem 2.6.3] or [10, Corollary 9.94], one has the following result.

**Lemma 7:** The value \( N_q(1) \) can be determined explicitly as follows:

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

III. A NEW CONSTRUCTION OF NONLINEAR CODES

Let \( q \) be a prime power. Let \( \mathbb{F}_q = \{\alpha_1, \alpha_2, \ldots, \alpha_q\} \) be the finite field with \( q \) elements. Denote by \( \Sigma \) the set \( \mathbb{F}_q \cup \{\infty\} \). The size of \( \Sigma \) is \( |\Sigma| = q + 1 \). In this section, we will propose a construction of \((q + 1)\)-ary nonlinear codes over the code alphabet \( \Sigma \) via algebraic function fields by generalizing the ideas given in [11], [13], and [22].

**Proposition 8:** Let \( \mathcal{F}/\mathbb{F}_q \) be an algebraic function field with genus \( g \) and \( D \) be a divisor of \( F \) with \( \text{deg}(D) = m \geq 2g - 1 \). Let \( Q_1, Q_2, \ldots, Q_t \) be distinct places of \( F \) with \( \text{deg}(Q_i) = r_i \). Let \( G = \sum_{i=1}^t m_i Q_i \) be a divisor of \( F \) with \( \text{deg}(G) = \sum_{i=1}^t m_i r_i = s \) and \( m_i \geq 1 \) for \( 1 \leq i \leq t \). Consider the set \( \mathcal{L}_D(G) = \{ f \in \mathcal{L}(D + G) | \forall Q_i, (f) = -m_i - \nu_{Q_i}(D) \text{ for all } 1 \leq i \leq t \} \).

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

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

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

\[
\mathcal{L}_D(G) = \mathcal{L}(D + G) - \bigcup_{i=1}^t \mathcal{L}(D + G - Q_i).
\]

From the Riemann-Roch Theorem [21, Theorem 1.5.14], the size of \( \mathcal{L}(D + G) \) is

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

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

\[
|\mathcal{L}(D + G - Q_i)| = q^{\text{deg}(D+G)-g+1} = q^{m-s-g+1}.
\]
\[
\begin{align*}
= & \sum_{k=1}^{t} (-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq t} q^{m+s-g+1-\sum_{i=1}^{k} r_{i_j}} \\
= & q^{m+s-g+1} \sum_{k=1}^{t} (-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq t} q^{-\sum_{i=1}^{k} r_{i_j}} \\
= & q^{m+s-g+1} \left[ 1 - \prod_{i=1}^{t} \left( 1 - \frac{1}{q^r} \right) \right].
\end{align*}
\]

Hence, the cardinality of \( \mathcal{L}_D(G) \) is
\[
|\mathcal{L}_D(G)| = q^{m+s-g+1} \prod_{i=1}^{t} \left( 1 - \frac{1}{q^r} \right)
\geq q^{m+s-g+1} \prod_{i=1}^{t} \left( 1 - \frac{1}{q} \right)^{r_i}
\geq q^{m+s-g+1} \left( 1 - \frac{1}{q} \right)^{\sum_{i=1}^{t} m_i r_i}
= q^{m+s-g+1} \left( 1 - \frac{1}{q} \right)^{s} = q^{m-g+1}(q-1)^{s}.
\]

\[\square\]

Lemma 9: 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 \( \text{supp}(G_1) = \text{supp}(G_2) \). If there exists a place \( Q \in \text{supp}(G_1) \setminus \text{supp}(G_2) \) for \( i \neq j \in \{1, 2\} \), then we have \( \nu_Q(f) = -\nu_Q(G_1) - \nu_Q(D) \leq -\nu_Q(G_2) - \nu_Q(D) = -\nu_Q(D) \) and \( \nu_Q(f) = -\nu_Q(G_2) - \nu_Q(D) = -\nu_Q(D) \). 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 \( Q \in \text{supp}(G_1) \cup \text{supp}(G_2) \). 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 \( G_1 \neq G_2 \).

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 \( P_1, P_2, \ldots, P_n \) be rational places of \( F/\mathbb{F}_q \). Let \( s \) be a positive integer. For any positive integer \( r \geq 4g + 3 \), 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 [21, Corollary 5.2.10]. Let \( D = m(R_{r+1} - R_r) \) be a divisor of \( F \) with \( \deg(D) = m \geq 2g - 1 \). Consider the set
\[
\mathcal{L}_s(D) := \bigcup_{G \geq 0, \deg(G) \leq s} \mathcal{L}_D(G),
\]
where \( G \) runs over all effective divisors of \( F \) with \( 0 \leq \deg(G) \leq s \). Here we assume that \( \mathcal{L}_D(0) = \mathcal{L}(D) \). Let \( \Sigma \) be the set \( \mathbb{P}_F \cup \{\infty\} \). We define an evaluation map \( \phi : \mathcal{L}_s(D) \to \Sigma^n \) by putting
\[
\phi(f) = (f(P_1), f(P_2), \ldots, f(P_n))
\]
for any element \( f \in \mathcal{L}_s(D) \). The image of \( \phi \) together with \( \{\infty, \infty, \cdots, \infty\} \) is our nonlinear code \( C := \phi(\mathcal{L}_s(D)) \cup \{\infty, \infty, \cdots, \infty\} \subset \Sigma^n \).

Theorem 10: 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 \( m \geq 2g - 1 \) and let \( s \) be a non-negative integer with \( n - m - 2s > 0 \). Then the code \( C \) defined as above is \( (q+1) \)-ary \((n,M,d)\)-code with cardinality
\[
M = |C| \geq 1 + \sum_{s=0}^{m} (q-1)^s q^{m-g+1} A_i,
\]
and minimum distance
\[
d \geq n - m - 2s.
\]

Proof: Under the assumption that the minimum distance of \( C \) is \( d \geq n - m - 2s > 0 \), it is clear that the evaluation map \( \phi \) is injective. Hence, the cardinality of the code \( C \) is lower bounded by
\[
M = |C| \geq 1 + \sum_{s=0}^{m} (q-1)^s q^{m-g+1} A_i
\]
from Proposition 8 and Lemma 9. 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 codewords \( \phi(f_1) \) 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 \( \deg(G_1) \leq s \) and \( \deg(G_2) \leq s \) respectively, then \( f_1 - f_2 \in \mathcal{L}(D + (G_1 \cup G_2)) \). If \( P \in \text{supp}(G_1) \cap \text{supp}(G_2) \), then \( f_1 - f_2 \in \mathcal{L}(D + G_1 + G_2 - P) \) from Lemma 1. Hence, we have
\[
f_1 - f_2 \in \mathcal{L}(D + G_1 + G_2 - \sum_{P \in \text{supp}(G_1) \cap \text{supp}(G_2)} P).
\]

Let \( Z \) be the subset of \( \{1, 2, \cdots, n\} \) defined by
\[
Z := \{1 \leq j \leq n| P_j \notin \text{supp}(G_1) \cup \text{supp}(G_2) \text{ and } f_1(P_j) = f_2(P_j)\}.
\]

From Lemma 1, we have \( 0 \neq f_1 - f_2 \in \mathcal{L}(D + G_1 + G_2 - \sum_{P \in \text{supp}(G_1) \cap \text{supp}(G_2)} P_1 - \sum_{j \in Z} P_j).
\]

It follows that
\[
m + \deg(G_1) + \deg(G_2) - |\text{supp}(G_1) \cap \text{supp}(G_2)| - |Z| \geq 0.
\]

On the other hand, the Hamming distance of \( \phi(f_1) \) and \( \phi(f_2) \) is \( d(\phi(f_1), \phi(f_2)) \geq n - |\text{supp}(G_1) \cap \text{supp}(G_2)| - |Z| \). Hence, the minimum distance \( d \) of the code \( C \) is lower bounded by
\[
d \geq n - |\text{supp}(G_1) \cap \text{supp}(G_2)| - |Z| \geq n - m - \deg(G_1) - \deg(G_2) \geq n - m - 2s.
\]

Corollary 11: 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 \( m \geq 2g - 1 \). For a fixed minimum distance \( 2 \leq d \leq n - m \), there exists a \((q+1)\)-ary \((n,M,d)\)-code with cardinality
\[
M \geq 1 + \max_{2g-1 \leq m \leq n-d} \left\{ \frac{(n-d-m/2)}{2} \sum_{i=0}^{\infty} (q-1)^i q^{m-g+1} A_i \right\}.
\]

Proof: This corollary follows from Theorem 10 and [12, Theorem 6.1.1].

\[\square\]
IV. NONLINEAR CODES VIA ELLIPTIC CURVES

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

Let $E/\mathbb{F}_q$ be an elliptic curve defined over the finite field $\mathbb{F}_q$ and $N(E)$ be its number of rational points. From [21, Theorem 5.1.15], the $L$-polynomial of the elliptic curve $E/\mathbb{F}_q$ is $L(t) = 1 + (N(E) - q - 1)t + qt^2 \in \mathbb{Z}[t]$, i.e., $a_0 = 1$, $a_1 = N(E) - q - 1$, $a_2 = q$ and $a_j = 0$ for $j \geq 3$.

From Lemma 2, the number of effective divisors of $E/\mathbb{F}_q$ with degree $i$ is $A_i = \sum_{j=0}^{i} a_j (q^{i+1-j} - 1)/(q-1)$. Let $m \geq 2(qg - 1) - 1$ and $s$ be two non-negative integers. From Theorem 10, there exists a $(q+1)$-ary $(n, M, d)$-nonlinear code with length $n = N(E)$, size $M \geq 1 + \sum_{i=0}^{s}(q - 1)^i q^{m}A_i$, and minimum distance $d \geq n - m - 2s > 0$. Hence, the following proposition follows from Corollary 11.

Proposition 12: Let $E/\mathbb{F}_q$ be an elliptic curve with $N(E)$ rational points. For $q + 3 \leq n \leq N(E)$ and $2 \leq d \leq n - 1$, there exists a $(q+1)$-ary $(n, M, d)$-nonlinear code $C_E$ with cardinality $M = |C_E| \geq 1 + \sum_{i=0}^{s}(q - 1)^i q^{m}A_i$ for all $1 \leq m \leq n - d$.

In the following, we want to compare our nonlinear codes via elliptic curves with the codes obtained from propagation rules given in Lemma 4.

A. 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 $q + 3 \leq n \leq N(E)$, 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 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 4, there exists a $(q+1)$-ary $(n, q^{n-d}, d)$-nonlinear code via alphabet extension.

Proposition 13: Let $E/\mathbb{F}_q$ be an elliptic curve with $N(E)$ rational points. For $q + 3 \leq n \leq N(E)$ and $2 \leq d \leq n - 1$, there exists a $(q+1)$-ary $(n, M, d)$-nonlinear code $C_E$ with cardinality $M = |C_E| \geq 1 + (q + 1)^{n}A_0 = 1 + q^{n-d} > q^{n-d}$.

B. Alphabet Restriction

Let $q$ be a prime power. If $q + 2$ is a prime power as well, then there exists a $(q + 2)$-ary $[n, n - d, d]$-linear code for $n \leq N_{q+2}(1)$. From Lemma 4, there exists a $(q+1)$-ary $(n, M' \geq (q+1)^{n}/(q+2)^{n-1}, d)$-nonlinear code via alphabet restriction. In the case where $q + 2$ is not a prime power, we are not sure whether there exists a $(q+2)$-ary $(n, q^{n-d}, d)$-code. Nevertheless, no matter whether $q + 2$ is a prime power or not, we use $(q+2)$-ary $(n, (q+2)^{n-d}, d)$-codes to compare with our codes in the following proposition.

Proposition 14: Let $E/\mathbb{F}_q$ be an elliptic curve with $N(E)$ rational points. If $q + 1 \leq n \leq N(E)$ and $d \geq n \cdot \ln(1 + \frac{1}{q})/\ln(1 + \frac{2}{q})$, then there exists a $(q+1)$-ary $(n, M, d)$-nonlinear code $C_E$ with cardinality larger than $(q+2)^{n}/(q+2)^{n-1}$, i.e., the size of the $(q+1)$-ary nonlinear code $C_E$ is larger than the one constructed from code alphabet restriction of a $(q+2)$-ary $(n, q^{n-d}, d)$-code for sufficiently large $d$.

Proof: From Proposition 12, there exists a $(q+1)$-ary $(n, M, d)$-nonlinear code $C_E$ with cardinality

$$M \geq 1 + \sum_{i=0}^{s}(q - 1)^i q^{m}A_i \geq 1 + q^{n-d}[1 + (q - 1)n].$$

It is easy to verify that

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

If and only if

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

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

Remark 15: If $q$ is a prime power, then $q + 2$ may not be a prime power. Let $n$ be a positive integer with $q + 1 \leq n \leq N_{q+1}(1)$. Let $q + a$ be the least prime power satisfying $q + a \geq n - 1$. 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 $(n, M' \geq [(q+1)^{n}/(q+a)^{n-1}], d)$-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 $a = \lfloor 2\sqrt{q} \rfloor$ to be an integer such that $q + a$ is a prime power. From Proposition 14, there exists a $(q+1)$-ary $(n, M, d)$-nonlinear code $C_E$ with cardinality

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

It is easy to verify that

$$q^{n-d}[1 + (q - 1)n] \geq (q + a)^{n-d+1} \frac{(q + 1)^{n}}{(q + a)^{d-1}}$$

if and only if

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

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

$$M > \frac{(q + 1)^{n}}{(q + a)^{d-1}}.$$
Hence, the elliptic function field $E$ is \( i \leq a_6 \) the best-known parameters given in the online table [6]. Instead, we choose linear codes with parameters. However, we are lack of nonlinear codes with the best-known parameters. From Theorem 10 and Corollary 11, there exists a 10-ary \((10,M,d)\)-nonlinear code with size
\[
\frac{|(10-d-m)/2|}{2} \cdot 5^m A_i,
\]
for any integer \( 1 \leq m \leq 10 - d \).

In the above table I, we compare the codes given in Example 16 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 turn out to be not good enough for large minimum distances. Hence, we only compare codes given in Example 16 with those obtained via code alphabet extension and restriction in the above table II. In particular, we use 11-ary \([16,k,16-k]\)-linear codes for comparison with the codes via code alphabet restriction.

### V. NONLINEAR CODES VIA MAXIMAL FUNCTION FIELDS

In this section, we provide an explicit construction of nonlinear codes via maximal function fields given in Section III. Let \( F/F_q \) be a maximal function field of genus \( g \). If \( g \geq 1 \), then \( q \) must be a square of a prime power. Otherwise, \( F/F_q \) is the rational function field over \( F_q \) for any prime power. The rational number of places of \( F \) is \( N(F) = q + 1 + 2g \sqrt{q} \) and the \( L \)-polynomial of \( F/F_q \) is \( L(t) = (1 + \sqrt{q}t)^2g \in \mathbb{Z}[t] \). Hence, we have \( a_j = (2g \sqrt{q})^j \) for \( 0 \leq j \leq 2g \), and \( a_j = 0 \) for \( j > 2g + 1 \). From Lemma 2, the number of effective divisors of \( F/F_q \) is \( A_i = \sum_{j=0}^{2g} a_j (q^j + 1) \) for \( 0 \leq j \leq 2g \), and \( a_j = 0 \) for \( j > 2g + 1 \). From Theorem 10, there exists a \((q+1)\)-ary \((n,M,d)\)-nonlinear code with length \( q + 1 \leq n \leq q + 1 + 2g \sqrt{q} \), size \( M \geq 1 + \sum_{i=0}^{2g} (q-1)^i q^{m+1-s} A_i \), and minimum distance \( d \geq n - m - 2s \). From Corollary 11, there exists a \((q+1)\)-ary \((n,M,d)\)-nonlinear code \( C \) with size
\[
M \geq 1 + \max_{2g-1 \leq m \leq n-d} \left\{ \sum_{i=0}^{2g} (q-1)^i q^{m+1-s} A_i \right\}.
\]
A. Alphabet Extension

If \( q + 1 \leq n \leq q + 1 + 2g\sqrt{q} \), then there exists a \( (q+1) \)-ary \([n, n-g+1-d, d] \)-linear code constructed from a maximal function field \( F/\mathbb{F}_q \). From Lemma 4, there exists a \((q+1)\)-ary \([n, q^{-g+1-d}, d] \)-nonlinear code via code alphabet extension of algebraic geometry codes.

Proposition 18: Let \( F/\mathbb{F}_q \) be a maximal function field with genus \( g \). For \( q + 1 \leq n \leq q + 1 + 2g\sqrt{q} \) and \( 2 \leq d \leq n-g \), there exists a \((q+1)\)-ary \([n, M, d] \)-nonlinear code \( C_F \) with cardinality larger than \( q^{n-g+1-d} \).

Proof: Let \( m = n - d - 2 \). From Theorem 10 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

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

It is easy to verify that

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

B. 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 candidates for optimal linear codes for large length \( n \) compared with \( q \). From Lemma 4, there exists a \((q+1)\)-ary \([n, M' \geq \frac{(q+1)^n}{(q+2)^{n-g+1}}, d] \)-nonlinear code via code alphabet restriction of algebraic geometry codes. Again, in the case where \( q+2 \) is not a prime power, we are not sure whether there still exists a \((q+2)\)-ary \([n, (q+2)^{n-d-g+1}, d] \)-code for \( n \leq q+1 + 2g\sqrt{q} \). Nevertheless, no matter whether \( q+2 \) is a prime power 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 19: Let \( F/\mathbb{F}_q \) be a maximal function field with genus \( q \). If \( q + 1 \leq n \leq q + 1 + 2g\sqrt{q} \) and \( d \geq 1 - g + n \cdot \ln(1 + \frac{1}{q}/\ln(1 + \frac{2}{q})) \), then there exists a \((q+1)\)-ary \([n, M, d] \)-nonlinear code \( C_F \) with cardinality larger than \( q^{n-g+1-d} \).

Proof: From Proposition 18, there exists a \((q+1)\)-ary \([n, M, d] \)-nonlinear code \( C_F \) with cardinality \( M = |C_F| \geq 1 + q^{n-g-d-1}[1 + (q-1)n] \). It is easy to verify that

\[
q^{n-g-d-1}[1 + (q-1)n] \geq \frac{(q+1)^n}{(q+2)^{d+g-1}}
\]
if and only if

\[
\frac{(q+2)^{d+g-1}}{q^{n-g-1}} \geq \frac{(q+1)^n}{q^n} \cdot \frac{q^2}{1 + (q-1)n}.
\]

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

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

This completes the proof.

C. 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 20: 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, we have \( A_i = (q^{i+1} - 1)/(q - 1) \) for all \( i \in \mathbb{N} \). From Theorem 10, there exists a \((q+1)\)-ary \([n, M, d] \)-nonlinear code with length \( n = q+1 \) and size

\[
M \geq 1 + q^{n+1-d} > (q+1)^n/(q+2)^{d-1}.
\]

From Propositions 18 and 19, 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 10 is the same as the one given in [11]. 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 [11, Theorem III.5]. Furthermore, it has been shown that $q^{2s+1} + q^{2s} - 2q^s + 2 > (q+1)2s$ for $s \leq q/2$. Hence, the code $C$ is a $(q+1)$-ary $(q+1, M, d)$-nonlinear code satisfying $n < \log_2(q+1) + M + d \leq n + 1$. It turns out that the code $C$ is quite good at the trade-off between information rate and minimum distance.

Example 21: Let $H/\mathbb{F}_q$ be the Hermitian function field $H = \mathbb{F}_q(x,y)$ defined by $y^3 + y = x^4$. From [21, Lemma 6.4.4], $H$ is a maximal function field of genus $3$ and the number of rational places of $H$ is $N(H) = 28$. Hence, the $L$-polynomial of $H/\mathbb{F}_q$ is given by $L_H(t) = (1 + 3t)^6 \in \mathbb{Z}[t]$, i.e., $a_j = \binom{6}{j} \cdot 3^j$ for $0 \leq j \leq 6$ and $a_j = 0$ for $j \geq 7$. From Lemma 2, the number of effective divisors of $H/\mathbb{F}_q$ is $A_i = \sum_{j=0}^{i} a_j(9i^2+1-j)/8$. For $2 \leq d \leq 23$, from Theorem 10 and Corollary 11, there exists a 10-ary $(28, M, d)$-nonlinear code with size $M \geq 1 + \sum_{i=0}^{(28-d-m)/2} 9i \cdot 9^{m-2} A_i$, for any $5 \leq m \leq 28 - d$.

Note that for these comparison, we are lack of the parameters of 11-ary codes from the online table [6] for code alphabet restriction. Hence, we use 11-ary $(28, 26, d, d)$-algebraic geometry codes in the above table III.

---

**References**

[1] A. Bassa, L. Ma, C. Xing, and S. L. Yeo, “Towards a characterization of subfields of the Deligne–Lusztig function fields,” *J. Combin. Theory A*, vol. 120, no. 7, pp. 1351–1371, Sep. 2013.

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

[3] N. D. Elkies, “Excellent codes from modular curves,” in *Proc. 33rd Annu. ACM Symp. Theory Comput.*, Crete, Greece, Jul. 2001, pp. 200–208.

[4] A. Garcia, H. Stichtenoth, and C. Xing, “On subfields of the Hermitian function fields,” *Compositio Mathemtica*, vol. 120, pp. 137–170, Jan. 2000.

[5] M. Giulietti and G. Korchmáros, “A new family of maximal curves over a finite field,” *Mathematische Annalen*, vol. 343, no. 1, pp. 229–245, Jan. 2009.

[6] M. Grassl, *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*. Accessed: Aug. 13, 2022. [Online]. Available: http://www.codetables.de

[7] T. Gulliver and M. Harada, “Extremal self-dual codes over $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_4$,” *AKCE J. Graphs Comb.*, vol. 2, no. 1, pp. 11–24, 2005.

[8] M. Harada, “On the existence of extremal type $\mathbb{I}_2$ codes over $\mathbb{Z}_9$,” *Discrete Math.*, vol. 223, nos. 1–3, pp. 373–378, Aug. 2000.

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

[10] H. P. Hirschfeld, G. Korchmaros, and F. Torres, *Algebraic Curves Over a Finite Field* (Princeton Series in Applied Mathematics). Princeton, NJ, USA: Princeton Univ. Press, 2008.

[11] 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.

[12] S. Ling and C. Xing, *Coding Theory: A First Course*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[13] S. Liu, T. Wu, and C. Xing, “Nonlinear codes exceeding the Gilbert–Varshamov and Tsfasman–Vladut–Zink bound,” in *Proc. SODA*, 2022, pp. 4104–4114.

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[15] C. Munuera, “On MDS elliptic curves,” *Discrete Math.*, vol. 117, pp. 279–286, Jan. 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] M. Montanucci and G. Zini, “The complete list of genera of quotients of the $F_2^2$-maximal Hermitian curve for $q \equiv 1 \pmod{4}$,” *J. Algebra*, vol. 550, pp. 23–53, May 2020.

[18] H. Niederreiter and C. Xing, “Cyclotomic function fields, Hilbert class fields, and global function fields with many rational places,” *Acta Arith.*, vol. 79, no. 1, pp. 38–59, 1997.

[19] A. W. Nordstrom and J. P. Robinson, “An optimal nonlinear codes,” *Inform. Control*, vol. 11, pp. 613–616, Jan. 1967.

[20] J. P. Serre, *Rational Points on Curves Over Finite Fields*, document 18, Société Mathématique de France, 2020.

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

[22] 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.

[23] J. L. Walker, “The Nordstrom–Robinson code is algebraic-geometric,” *IEEE Trans. Inf. Theory*, vol. 43, no. 5, pp. 1588–1593, Sep. 1997.

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

---

**Shu Liu** (Member, IEEE) received the Ph.D. degree from Nanyang Technological University, Singapore, in 2018. She is currently an Associate Professor with the National Key Laboratory on Wireless Communications, University of Electronic Science and Technology of China, China. Her research interests include coding theory and its applications.

**Liming Ma** received the Ph.D. degree in mathematics from Nanyang Technological University, Singapore, in 2014. From April 2014 to May 2020, he was a Lecturer with the School of Mathematical Sciences, Yangzhou University, China. Since June 2020, he has been a Research Associate Professor with the School of Mathematical Sciences, University of Science and Technology of China. His research interests include algebraic function fields over finite fields and coding theory.

**Ting-Yi Wu** received the Ph.D. degree in communication engineering from National Chiao Tung University, Hsinchu, Taiwan, in 2013. He worked as a Postdoctoral Fellow with the Network Technology Laboratory, National Chiao Tung University, until 2015. Then, he joined the Signal-Processing and Communication Laboratory, HKUST, the Coordinated Science Laboratory, SYSU, Guangzhou. He is currently a Principal Engineer with the Theory Laboratory, 2012 Labs, Central Research Institute, Huawei Technologies Company Ltd. His research interests include erasure coding for storage, networks, and communications.

**Chaoping Xing** (Senior Member, IEEE) received the Ph.D. degree from the University of Science and Technology of China in 1990. From 1990 to 1993, he was a Lecturer and an Associate Professor with the University of Science and Technology of China. He joined the University of Essen, Germany, as an Alexander von Humboldt Fellow, from 1993 to 1995. After this, he spent most time with the Institute of Information Processing, Austrian Academy of Sciences, until 1998. From March 1998 to November 2007, he was working with the National University of Singapore as an Assistant Professor/an Associate Professor/a Full Professor. Since November 2009, he has been with Shanghai Jiaotong University as a Chair Professor. His research interests include coding theory, cryptography, algebraic curves over finite fields, and quasi-Monte Carlo methods.