New Binary Codes From Rational Function Fields

Jin, Lingfei; Xing, Chaoping

2014

Jin, L., & Xing, C. (2015). New Binary Codes From Rational Function Fields. IEEE Transactions on Information Theory, 61(1), 60-65.

<https://hdl.handle.net/10356/81336>

<https://doi.org/10.1109/TIT.2014.2352306>

© 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [<http://dx.doi.org/10.1109/TIT.2014.2352306>].

Downloaded on 26 Apr 2023 20:00:02 SGT

New Binary Codes From Rational Function Fields

Lingfei Jin and Chaoping Xing

Abstract—In this paper, we present an algebraic construction of binary codes through rational function fields. We make use of certain multiplicative group of rational functions for our construction. In particular, the “point at infinity” can be employed in our construction to get codes of length up to $q + 1$, where q is the ground field size. As a result, several new binary constant-weight codes are found and many new binary nonlinear codes are presented.

I. INTRODUCTION

For a given pair (n, d) , we denote by $A(n, d)$ the largest size of binary codes of length n and minimum distance d . Similarly, for given a triple (n, d, w) , we denote by $A(n, d, w)$ the largest size of binary constant-weight codes of length n , weight w and minimum distance d . It is one of the fundamental problems in coding theory to determine the values of $A(n, d)$ and $A(n, d, w)$. In general, it is very difficult to determine exact values of $A(n, d)$ and $A(n, d, w)$. Thus, people have tried very hard to develop various upper and lower bounds on $A(n, d)$ and $A(n, d, w)$. As there is tremendous research work on this topic in literature, it would be difficult to cite all papers. Instead, we cite only most relevant ones in our paper. The reader may refer to the online tables [1], [3] for references on various constructions of binary codes and bounds.

Lower bounds are typically obtained by means of explicit code constructions. Since birth of coding theory, it has been always a great challenge to construct good binary codes from both coding and combinatorial point of view. Various constructions through combinatorics, algebra, number theory and

even geometry have been proposed (see the references in the online tables [1], [3]). However, it seems that it is still far from satisfaction to provide general lower bounds on $A(n, d)$ and $A(n, d, w)$. On the other hand, for small parameters, some reasonable lower bounds can be found from the two online tables [1], [3].

In this paper, we propose a purely algebraic construction of binary codes using rational function fields. We start with a rational function field over $\mathbb{F}_q$ and consider the point set $\mathbb{F}_q \cup \{\infty\}$, where ∞ stands for the “point at infinity”. Thus, the length of our binary codes can be up to $q + 1$. It turns out that several new binary constant-weight codes are found and many new binary nonlinear codes are provided. Note that in [1], [2], [3], [4], some constructions based on rational function fields have been studied. However, for most of these constructions, the “point at infinity” was not considered.

The paper is organized as follows. In Section 2, we introduce some preliminaries on rational function field and binary codes. Our constructions are presented in Section 3. The last section shows some examples and provides several tables in which our new codes are listed.

II. PRELIMINARIES

A. Rational function fields

Let $\mathbb{F}_q$ be the finite field of q elements and denote by $k := \mathbb{F}_q(x)$ the rational function field. For $n \leq q + 1$, choose a set S of $n - 1$ distinct elements $\{\alpha_1, \dots, \alpha_{n-1}\}$ in $\mathbb{F}_q$.

Denote by $\text{Div}_S^0(k)$ the free abelian multiplicative group generated by $\{x - \alpha_i : 1 \leq i \leq n - 1\}$. For a polynomial $f(x)$ that is co-prime with $\prod_{i=1}^{n-1} (x - \alpha_i)$, we consider the subset $K(f) := \{g(x) \in \text{Div}_S^0(k) : f(x) \mid (g(x) - 1)\}$. Note that $g(x)$ is a rational function of the form $g(x) = \prod_{i \in I} (x - \alpha_i)^{a_i} / \prod_{j \in J} (x - \alpha_j)^{a_j}$ for two disjoint subsets $I, J \subseteq \{1, 2, \dots, n - 1\}$ and non-negative integers a_i, a_j . By $f(x) \mid (g(x) - 1)$, we

The work of C. Xing was supported by the Singapore Ministry of Education under the Tier 1 Grant RG20/13.

Lingfei Jin is with Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai 200433, China. *email*: lfjin@fudan.edu.cn.

Chaoping Xing is with Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637371, Republic of Singapore. *email*: xingcp@ntu.edu.sg

mean that

$$f(x) \mid \left(\prod_{i \in I} (x - \alpha_i)^{a_i} - \prod_{j \in J} (x - \alpha_j)^{a_j} \right).$$

Lemma II.1. *Let $\deg(f(x)) \geq 1$, then the set $K(f)$ defined above is a subgroup of $\text{Div}_S^0(k)$.*

Proof: For two elements $g_1(x), g_2(x)$ in K , we consider the product $g_1(x)g_2^{-1}(x)$. We write $g_1(x) = u_1(x)/v_1(x)$ and $g_2(x) = u_2(x)/v_2(x)$ for some polynomials $u_i(x), v_i(x)$ with $\gcd(u_i(x), v_i(x)) = 1$ ($i = 1, 2$). Then $f(x) \mid (u_i(x) - v_i(x))$ for $i = 1, 2$. Thus, $f(x) \mid (u_1(x)v_2(x) - u_2(x)v_1(x))$ since

$$u_1(x)v_2(x) - u_2(x)v_1(x) = (u_1(x) - v_1(x))v_2(x) - (u_2(x) - v_2(x))v_1(x).$$

Hence, $f(x) \mid (g_1(x)g_2^{-1}(x) - 1)$. This implies that K is a subgroup of $\text{Div}_S^0(k)$. ■

Lemma II.2. *If $\deg(f(x)) \geq 1$, then the quotient group $\text{Div}_S^0(k)/K(f)$ is finite. Furthermore, if $f(x)$ has factorization $f(x) = \prod_{i=1}^m p_i(x)^{e_i}$ for distinct monic irreducible polynomials $p_i(x)$ and integers $e_i \geq 1$, then*

$$|\text{Div}_S^0(k)/K(f)| \leq \prod_{i=1}^m (q^{d_i} - 1)q^{d_i(e_i-1)},$$

where d_i is the degree of $p_i(x)$.

Proof: Consider the unit group $(\mathbb{F}_q[x]/(f(x)))^*$ of the residue ring $\mathbb{F}_q[x]/(f(x))$. By the Chinese Remainder Theorem, we have $(\mathbb{F}_q[x]/(f(x)))^* \simeq \prod_{i=1}^m (\mathbb{F}_q[x]/(p_i(x)^{e_i}))^*$. Hence, the cardinality of $(\mathbb{F}_q[x]/(f(x)))^*$ is $\prod_{i=1}^m (q^{d_i} - 1)q^{d_i(e_i-1)}$. The desired result follows from the fact that $\text{Div}_S^0(k)/K(f)$ is the subgroup of $(\mathbb{F}_q[x]/(f(x)))^*$ generated by $\{x - \alpha_i : 1 \leq i \leq n-1\}$. ■

Next we consider another subgroup of $\text{Div}_S^0(k)$.

Lemma II.3. *Let $\deg(f(x)) \geq 1$, then the set $G(f) := \{g(x) \in \text{Div}_S^0(k) : f(x) \mid (g(x) - \alpha) \text{ for some } \alpha \in \mathbb{F}_q^*\}$ is a subgroup of $\text{Div}_S^0(k)$.*

Proof: The proof is quite similar to the one of Lemma II.1. Indeed, for two elements $g_1(x), g_2(x)$ in G , we consider the product $g_1(x)g_2^{-1}(x)$. We write $g_1(x) = u_1(x)/v_1(x)$ and $g_2(x) = u_2(x)/v_2(x)$ for some polynomials $u_i(x), v_i(x)$ with $\gcd(u_i(x), v_i(x)) = 1$ ($i = 1, 2$). Then there exist $\beta_1, \beta_2 \in \mathbb{F}_q^*$ such that $f(x) \mid (u_i(x) - \beta_i v_i(x))$ for $i = 1, 2$. Thus, $f(x) \mid (u_1(x)v_2(x) - \beta_1\beta_2^{-1}u_2(x)v_1(x))$ since

$$u_1(x)v_2(x) - \beta_1\beta_2^{-1}u_2(x)v_1(x) = (u_1(x) - \beta_1v_1(x))v_2(x) - \beta_1\beta_2^{-1}(u_2(x) - \beta_2v_2(x))v_1(x). \text{ Hence, } f(x) \mid (g_1(x)g_2^{-1}(x) - \beta_1\beta_2^{-1}). \text{ This implies that } G \text{ is a subgroup of } \text{Div}_S^0(k). \quad \blacksquare$$

Lemma II.4. *If $\deg(f(x)) \geq 1$, then the quotient group $\text{Div}_S^0(k)/G(f)$ is finite. Furthermore, if $f(x)$ has factorization $f(x) = \prod_{i=1}^m p_i(x)^{e_i}$ for distinct monic irreducible polynomials $p_i(x)$ and integers $d_i \geq 1$, then*

$$|\text{Div}_S^0(k)/G(f)| \leq \frac{1}{q-1} \prod_{i=1}^m (q^{d_i} - 1)q^{d_i(e_i-1)},$$

where d_i is the degree of $p_i(x)$.

Proof: It is clear that $\mathbb{F}_q^*$ is a subgroup of the unit group $(\mathbb{F}_q[x]/(f(x)))^*$. The quotient group of $(\mathbb{F}_q[x]/(f(x)))^*$ over $\mathbb{F}_q^*$ is denoted by A . It is easy to see that $\text{Div}_S^0(k)/G(f)$ can be viewed as a subgroup of A . The desired result follows. ■

B. Binary codes

A binary code of length n is a subset of $\{0, 1\}^n$. A binary code of length n , size M and minimum distance d is denoted by (n, M, d) .

For given n and d , the maximal cardinality M of binary (n, M, d) -codes is denoted by $A(n, d)$, i.e.,

$$A(n, d) = \max\{M : \text{there exists an } (n, M, d)\text{-code}\}.$$

For every pair (n, d) , a binary $(n, A(n, d), d)$ -code is called *optimal*.

Determining the exact values of $A(n, d)$ is a challenging problem. However, there are various upper and lower bounds on $A(n, d)$. Furthermore, for binary codes of length up to 512 and minimum distance up to 30, an online table of lower bounds on $A(n, d)$ can be found at

<http://www.eng.tau.ac.il/~litsyn/tableand/>

For an integer $1 \leq w \leq n/2$, we consider the Johnson space $J(n, w) := \{\mathbf{u} \in \{0, 1\}^n : \text{wt}_H(\mathbf{u}) = w\}$ of weight w , where wt_H denotes the Hamming weight. A binary constant-weight code of length n and weight w is a subset of $J(n, w)$. A binary constant-weight code of length n , weight w , size M and minimum distance d is denoted by $(n, M, d; w)$. For given n, d, w , the maximal cardinality M of binary constant-weight $(n, M, d; w)$ -codes is denoted by $A(n, d, w)$, i.e.,

$$A(n, d, w) = \max\{M : \text{there exists an } (n, M, d; w)\text{-code}\}.$$

For every triple (n, w, d) , a binary constant-weight $(n, A(n, w, d), d; w)$ -code is called *optimal*.

Similarly, determining the exact values of $A(n, w, d)$ is a challenging problem and there are various upper and lower bounds on $A(n, w, d)$. For binary constant-weight codes of relatively small length and minimum distance, an online table of lower bounds on $A(n, w, d)$ can be found at

<http://www.research.att.com/~njas/codes/Andw>

III. CONSTRUCTION

In this section, we fix a set S of $n - 1$ distinct elements $\{\alpha_1, \dots, \alpha_{n-1}\}$ in $\mathbb{F}_q$, where $n \leq q + 1$. We also assume that S contains the zero element 0 of $\mathbb{F}_q$.

A. The first construction

Let us consider the map

$$\begin{aligned} \pi_K : J(n-1, w) &\rightarrow \text{Div}_S^0(k)/K(f); \\ \mathbf{u} = (u_1, u_2, \dots, u_{n-1}) &\mapsto (x - \alpha_1)^{-w} \prod_{i=1}^{n-1} (x - \alpha_i)^{u_i}. \end{aligned} \quad (1)$$

We claim that for every element in $\text{Div}_S^0(k)/K(f)$, its pre-image under π_K defined in (1) is a constant-weight code with minimum distance controlled by the degree of $f(x)$.

Proposition III.1. *For every element of $\text{Div}_S^0(k)/K(f)$, its pre-image under π_K is a binary constant-weight code of length $n - 1$, weight w and minimum distance at least $2\delta + 2$, where δ is the degree of $f(x)$.*

Proof: Since every pre-image under π_K is a subset of the $J(n-1, w)$, it is sufficient to prove that the minimum distance is at least $2\delta + 2$. Assume that $\mathbf{u} = (u_1, u_2, \dots, u_{n-1})$ and $\mathbf{v} = (v_1, v_2, \dots, v_{n-1})$ are two distinct elements in the same pre-image. Then $\pi_K(\mathbf{u})/\pi_K(\mathbf{v})$ is the identity of $\text{Div}_S^0(k)/K(f)$, i.e., $f(x)|(\pi_K(\mathbf{u})/\pi_K(\mathbf{v}) - 1)$. Write $\pi_K(\mathbf{u})/\pi_K(\mathbf{v}) = \prod_{i \in I} (x - \alpha_i) / \prod_{j \in J} (x - \alpha_j)$, where I, J are two disjoint subsets of $\{1, 2, \dots, n-1\}$ with the same cardinality. Then $f(x) | \prod_{i \in I} (x - \alpha_i) - \prod_{j \in J} (x - \alpha_j)$. Thus, $|I| - 1 \geq \deg(f(x)) = \delta$. Hence, $d_H(\mathbf{u}, \mathbf{v}) = |I| + |J| \geq 2\delta + 2$. This completes the proof. ■

Theorem III.2. *For any prime power q and a positive integer n with $n \leq q + 1$, let $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$*

be $n - 1$ distinct elements in $\mathbb{F}_q$. Let $f(x)$ be a polynomial in $\mathbb{F}_q[x]$ which is co-prime with $\prod_{i=1}^{n-1} (x - \alpha_i)$. If $\deg(f(x)) = \delta$ and $f(x)$ has factorization $f(x) = \prod_{i=1}^m p_i(x)^{e_i}$ for distinct monic irreducible polynomials $p_i(x)$ and integers $e_i \geq 1$, then for any positive integer w , there exists a binary constant-weight $(n - 1, M, d; w)$ -code with

$$d \geq 2\delta + 2 \quad \text{and} \quad M \geq \frac{\binom{n-1}{w}}{\prod_{i=1}^m (q^{d_i} - 1) q^{d_i(e_i-1)}}.$$

Proof: Assume that g is an element of $\text{Div}_S^0(k)/K(f)$ such that $\pi_K^{-1}(g)$ has the maximal cardinality, i.e.,

$$|\pi_K^{-1}(g)| = \max\{|\pi_K^{-1}(h)| : h \in \text{Div}_S^0(k)/K(f)\}.$$

We claim that $\pi_K^{-1}(g)$ is the desired code.

First, by Proposition III.1, $\pi_K^{-1}(g)$ is a constant-weight $(n - 1, 2\delta + 2, w)$ -code. By the Pigeonhole principle, the cardinality M of $\pi_K^{-1}(g)$ is at least $\binom{n-1}{w} / |\text{Div}_S^0(k)/K(f)|$. The desired result follows from Lemma II.2. ■

Now we extend the map π_K from $J(n-1, w)$ to a larger set

$$\begin{aligned} \mathcal{S} := & \left(\bigcup_{i=0}^a J(n-1, \lfloor (n-1)/2 \rfloor - (2\delta+2)i) \right) \\ & \cup \left(\bigcup_{i=0}^b J(n-1, \lfloor (n-1)/2 \rfloor + (2\delta+2)i) \right), \end{aligned}$$

where $\deg(f(x)) = \delta$, and

$$\begin{aligned} a &= \left\lfloor \frac{1}{2\delta+2} \left\lfloor \frac{n-1}{2} \right\rfloor \right\rfloor, \\ b &= \left\lfloor \frac{1}{2\delta+2} \left(n-1 - \left\lfloor \frac{n-1}{2} \right\rfloor \right) \right\rfloor. \end{aligned} \quad (2)$$

Extend the map π_K

$$\pi_K : \mathcal{S} \rightarrow \text{Div}_S^0(k)/K(f);$$

$$\mathbf{u} = (u_1, u_2, \dots, u_{n-1}) \mapsto (x - \alpha_1)^{-\sum_{i=1}^{n-1} u_i} \prod_{i=1}^{n-1} (x - \alpha_i)^{u_i}. \quad (3)$$

Theorem III.3. *For any prime power q and a positive integer n with $n \leq q + 1$, let $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$ be $n - 1$ distinct elements in $\mathbb{F}_q$. Let $f(x)$ be a polynomial in $\mathbb{F}_q[x]$ which is co-prime with $\prod_{i=1}^{n-1} (x - \alpha_i)$. If $\deg(f(x)) = \delta$ and $f(x)$ has factorization $f(x) = \prod_{i=1}^m p_i(x)^{e_i}$ for distinct monic irreducible polynomials $p_i(x)$ and integers $d_i \geq 1$, then there exists a binary $(n - 1, M, d)$ -code with*

$$\begin{aligned} d &\geq 2\delta + 2 \quad \text{and} \\ M &\geq \frac{\sum_{i=0}^a \binom{n-1}{\lfloor (n-1)/2 \rfloor - (2\delta+2)i} + \sum_{i=0}^b \binom{n-1}{\lfloor (n-1)/2 \rfloor + (2\delta+2)i}}{\prod_{i=1}^m (q^{d_i} - 1) q^{d_i(e_i-1)}}, \end{aligned}$$

where a, b are defined in (2).

Proof: Assume that g is an element of $\text{Div}_S^0(k)/K(f)$ such that $\pi_K^{-1}(g)$ defined in (3) has the maximal cardinality, i.e.,

$$|\pi_K^{-1}(g)| = \max\{|\pi_K^{-1}(h)| : h \in \text{Div}_S^0(k)/K(f)\}.$$

We claim that $\pi_K^{-1}(g)$ is the desired code.

First, by the Pigeonhole principle, the cardinality M of $\pi_K^{-1}(g)$ is at least $|\mathcal{S}|/|\text{Div}_S^0(k)/K(f)|$. The desired result on the size of $\pi_K^{-1}(g)$ is now clear. Next, let $\mathbf{u}$ and $\mathbf{v}$ be two distinct elements of $\pi_K^{-1}(g)$. If the weights of $\mathbf{u}$ and $\mathbf{v}$ are equal, then $d_H(\mathbf{u}, \mathbf{v}) \geq 2\delta + 2$ by Proposition III.1. If the weights of $\mathbf{u}$ and $\mathbf{v}$ are distinct, it is clear that $d_H(\mathbf{u}, \mathbf{v}) = \text{wt}_H(\mathbf{u} - \mathbf{v})$ is congruent to 0 modulo $2\delta + 2$. The result follows. ■

B. The second construction

For the second construction, we are going to map the elements of $J(n, w)$ to those in the group $\text{Div}_S^0(k)/G(f)$.

$$\begin{aligned} \pi_G : \mathbf{u} = (u_1, u_2, \dots, u_{n-1}, u_\infty) &\mapsto \\ \begin{cases} (x - \alpha_1)^{-w} \prod_{i=1}^{n-1} (x - \alpha_i)^{u_i} & \text{if } u_\infty = 0, \\ (x - \alpha_1)^{-w+1} \prod_{i=1}^{n-1} (x - \alpha_i)^{u_i} & \text{if } u_\infty = 1. \end{cases} \end{aligned} \quad (4)$$

Proposition III.4. *For every element of $\text{Div}_S^0(k)/G(f)$, its pre-image under π_G is a binary constant-weight code of length n , weight w and minimum distance at least 2δ , where δ is the degree of $f(x)$.*

Proof: Since every pre-image under π_K is a subset of the $J(n, w)$, it is sufficient to prove that the minimum distance is at least 2δ . Assume that $\mathbf{u} = (u_1, u_2, \dots, u_{n-1}, u_\infty)$ and $\mathbf{v} = (v_1, v_2, \dots, v_{n-1}, v_\infty)$ are two distinct element in the same pre-image. Then $\pi_G(\mathbf{u})/\pi_G(\mathbf{v})$ is the identity of $\text{Div}_S^0(k)/G(f)$, i.e., $f(x) | (\pi_G(\mathbf{u})/\pi_G(\mathbf{v}) - \alpha)$ for some $\alpha \in \mathbb{F}_q^*$.

If $u_\infty = v_\infty$, then we can write $\pi_G(\mathbf{u})/\pi_G(\mathbf{v}) = \prod_{i \in I} (x - \alpha_i) / \prod_{j \in J} (x - \alpha_j)$, where I, J are two disjoint subsets of $\{1, 2, \dots, n-1\}$ with $|I| = |J|$. Moreover, $d_H(\mathbf{u}, \mathbf{v}) = |I| + |J|$. In this case, we have $f(x) | (\prod_{i \in I} (x - \alpha_i) - \alpha \prod_{j \in J} (x - \alpha_j))$. Hence, $|I| \geq \deg(f(x)) = \delta$ and $d_H(\mathbf{u}, \mathbf{v}) \geq 2\delta$.

If $u_\infty \neq v_\infty$ (without loss of generality, we may assume that $u_\infty = 0$ and $v_\infty = 1$), then we can write $\pi_G(\mathbf{u})/\pi_G(\mathbf{v}) = \prod_{i \in I} (x - \alpha_i) / (\prod_{j \in J} (x - \alpha_j) (x - \alpha_1))$, where I, J are two disjoint subsets of $\{1, 2, \dots, n-1\}$ with $|I| = |J| + 1$. In this case, we have $d_H(\mathbf{u}, \mathbf{v}) = |I| + |J| + 1 = 2|I|$. Since $f(x) | (\prod_{i \in I} (x - \alpha_i) - \alpha \prod_{j \in J} (x - \alpha_j) (x - \alpha_1))$, we have $|I| \geq \delta$. Hence, $d_H(\mathbf{u}, \mathbf{v}) \geq 2\delta$. This completes the proof. ■

$\alpha_i) / (\prod_{j \in J} (x - \alpha_j) (x - \alpha_1))$, where I, J are two disjoint subsets of $\{1, 2, \dots, n-1\}$ with $|I| = |J| + 1$. In this case, we have $d_H(\mathbf{u}, \mathbf{v}) = |I| + |J| + 1 = 2|I|$. Since $f(x) | (\prod_{i \in I} (x - \alpha_i) - \alpha \prod_{j \in J} (x - \alpha_j) (x - \alpha_1))$, we have $|I| \geq \delta$. Hence, $d_H(\mathbf{u}, \mathbf{v}) \geq 2\delta$. This completes the proof. ■

Theorem III.5. *For any prime power q and a positive integer n with $n \leq q + 1$, let $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$ be $n-1$ distinct elements in $\mathbb{F}_q$. Let $f(x)$ be a polynomial in $\mathbb{F}_q[x]$ which is co-prime with $\prod_{i=1}^{n-1} (x - \alpha_i)$. If $\deg(f(x)) = \delta$ and $f(x)$ has factorization $f(x) = \prod_{i=1}^m p_i(x)^{e_i}$ for distinct monic irreducible polynomials $p_i(x)$ and integers $e_i \geq 1$, then for any positive integer w , there exists a binary constant-weight $(n, M, d; w)$ -code with*

$$d \geq 2\delta \quad \text{and} \quad M \geq \frac{(q-1) \binom{n}{w}}{\prod_{i=1}^m (q^{d_i} - 1) q^{d_i(e_i-1)}}.$$

The proof is similar to the one of Theorem III.3. We skip the detail.

Similarly we can extend the map π_G from $J(n, w)$ to a larger set

$$\mathcal{T} := \left(\bigcup_{i=0}^{a'} J(n, \lfloor n/2 \rfloor - 2\delta i) \right) \cup \left(\bigcup_{i=0}^{b'} J(n, \lfloor n/2 \rfloor + 2\delta i) \right),$$

where $\deg(f(x)) = \delta$, and

$$a' = \left\lfloor \frac{1}{2\delta} \left\lfloor \frac{n}{2} \right\rfloor \right\rfloor, \quad b' = \left\lfloor \frac{1}{2\delta} \left(n - \left\lfloor \frac{n}{2} \right\rfloor \right) \right\rfloor. \quad (5)$$

Extend the map

$$\pi_G : \mathcal{T} \rightarrow \text{Div}_S^0(k)/G(f);$$

$$\mathbf{u} \mapsto (x - \alpha_1)^{-\sum_{i=1}^{n-1} u_i} \prod_{i=1}^{n-1} (x - \alpha_i)^{u_i}, \quad (6)$$

where $\mathbf{u} = (u_1, u_2, \dots, u_{n-1}, u_\infty)$.

Theorem III.6. *For any prime power q and a positive integer n with $n \leq q + 1$, let $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$ be $n-1$ distinct elements in $\mathbb{F}_q$. Let $f(x)$ be a polynomial in $\mathbb{F}_q[x]$ which is co-prime with $\prod_{i=1}^{n-1} (x - \alpha_i)$. If $\deg(f(x)) = \delta$ and $f(x)$ has factorization $f(x) = \prod_{i=1}^m p_i(x)^{e_i}$ for distinct monic irreducible polynomials $p_i(x)$ and integers $e_i \geq 1$, then there exists a binary $(n-1, M, d)$ -code with*

$$d \geq 2\delta \quad \text{and} \quad M \geq \frac{\sum_{i=0}^{a'} \binom{n}{\lfloor n/2 \rfloor - 2\delta i} + \sum_{i=0}^{b'} \binom{n}{\lfloor n/2 \rfloor + 2\delta i}}{\prod_{i=1}^m (q^{d_i} - 1) q^{d_i(e_i-1)}},$$

where a', b' are defined in (5).

The proof of Theorem III.6 is straightforward.

IV. EXAMPLES AND NUMERICAL RESULT

Our main results of this paper are Theorems III.2, III.3, III.5 and III.6. However, it is not immediate to see how good these results are. In this section, we use some examples and numerical tables to illustrate.

Example IV.1. Let $q = 27$ and $n = 28$. Let ω be a primitive element of $\mathbb{F}_{27}$.

- (i) Consider the primitive polynomial $f(x) := x^3 + \omega x + \omega^{14}$. By Theorem III.5, we have a binary constant-weight $(28, M, 6; w)$ -code with $M \geq \lceil 26 \binom{28}{w} / (27^3 - 1) \rceil$ for all $1 \leq w \leq 28$. This bound is obtained through the average argument. To obtain the maximal size of the pre-images of π_K defined in (1), we used MAGMA to compute this maximal size and obtain lower bound on $A(28, 6, w)$ for $12 \leq w \leq 14$ given in Table 1. The first row in Table 1 provides the bound using the average argument, the second row in Table 1 shows the bound obtained from the maximal size of pre-images of π_G by MAGMA, the last rows gives the best-known bound from [1]. The table shows that the maximal size exceeds the current best-known bounds on $A(28, 6, w)$ for $12 \leq w \leq 14$.

Table 1

w	12	13	14
Ave in Theorem III.5	40188	49462	52995
Max in Theorem III.5	40237	49510	53046
Bound in [1]	40209	49482	53021

- (ii) Similarly, if we consider the polynomial $f(x) := (x - \omega^{25})^3$, we obtain the following lower bound on $A(27, 6, w)$ for $12 \leq w \leq 13$ given in Table 2. It shows that a new lower bound on $A(27, 6, 13)$ is obtained.

Table 2

w	12	13
Ave in Theorem III.2	23847	27515
Max in Theorem III.2	23898	27600
Bound in [1]	23901	27581

Example IV.2. In this example, we provide some lower bounds on $A(n, d)$ via formulas given in Theorems III.3 and III.6, respectively. Note that the lower bound given in Theorems III.3 and III.6 are obtained through the average argument. One can expect slight improvement if the maximal size is computed.

In the following tables, we list some new binary codes obtained from previous two constructions

given in Theorems III.3 and III.6. Some remarks on Tables 3 and 4:

- (i) Table 3 lists new binary codes obtained from Theorems III.3 while table 4 provides new binary codes obtained from Theorems III.6 .
- (ii) The minimum distance given in Theorems III.3 and III.6 is always even. To compare with the online table [3], we reduce to the case of odd minimum distance by using the fact that there exists a binary $(n, M, 2t)$ -code if and only if there exists a binary $(n - 1, M, 2t - 1)$ -code.
- (iii) In Tables 3 and 4, the polynomial $f(x)$ is always taken to be $a(x)^s b(x)^\varepsilon$ for some quadratic irreducible polynomial $a(x)$ and cubic irreducible polynomial $b(x)$, where $\varepsilon = 0$ or 1 depending on whether the degree of $f(x)$ is even or odd. This choice maximizes the average size of pre-images for a fixed degree.
- (iv) In Tables 3 and 4, k_{LRS} denotes $\log_2 M_{LRS}$, where M_{LRS} stands for the lower bound on $A(n, d)$ given in the online table [3], while k_{New} denotes $\log_2 M_{New}$, where M_{New} is the lower bound on $A(n, d)$ given in Theorems III.3 and III.6. Both k_{LRS} and k_{New} are rounded off to the third decimal place.
- (v) In order to compare, we use the following simple propagation rule to obtain some of the code lengths that are not listed in the online table [3]: there is a binary $(n - r, M/2^r, d)$ code whenever there is a binary (n, M, d) code for any $r \leq n$.

Table 3

n	d	k_{LRS}	k_{New}
276	9	241	241.223
280	9	245	245.14
282	9	247	247.099
316	9	280	280.445
330	9	294	294.195
336	9	300	300.092
150	11	111.17	111.238
282	11	238	238.692
288	11	244	244.541
292	11	248	248.441
306	11	262	262.105
312	11	267	267.965
316	11	271	271.873
330	11	285	285.562
336	11	291	291.432
346	11	301	301.221
348	11	303	303.18
352	11	307	307.097
162	13	115	115.145
282	13	230	230.327
288	13	236	236.145
292	13	239	240.026
306	13	253	253.621
310	13	257	257.509
312	13	259	259.454
316	13	263	263.344
330	13	276	276.969
336	13	282	282.814
346	13	292	292.56
348	13	294	294.511
352	13	298	298.412
358	13	304	304.266
360	13	306	306.218
366	13	312	312.075
166	15	111	111.421
168	15	113	113.297
172	15	117	117.053
292	15	230	231.646
306	15	244	245.173
310	15	248	249.041
312	15	250	250.976
316	15	254	254.848
330	15	267	268.41

n	d	k_{LRS}	k_{New}
336	15	273	274.228
346	15	283	283.932
348	15	285	285.874
352	15	289	289.758
358	15	295	295.588
360	15	297	297.532
366	15	303	303.365
372	15	309	309.201
172	17	109	109.542
178	17	115	115.132
192	17	128	128.232
292	17	223	223.304
306	17	235	236.759
310	17	239	240.608
312	17	241	242.533
316	17	245	246.385
330	17	259	259.882
336	17	264	265.674
346	17	274	275.334
348	17	276	277.267
352	17	280	281.135
358	17	286	286.939
360	17	288	288.875
366	17	294	294.683
372	17	300	300.495
378	17	306	306.31
382	17	310	310.189
306	19	227	228.381
310	19	231	232.21
312	19	233	234.126
316	19	237	237.958
330	19	250	251.388
336	19	256	257.152
346	19	266	266.767
348	19	268	268.692
352	19	272	272.542
358	19	278	278.321
360	19	280	280.248
366	19	286	286.031
388	19	307	307.268
306	21	219	220.038
310	21	223	223.847
312	21	225	225.752

n	d	k_{LRS}	k_{New}
316	21	228	229.565
330	21	241	242.927
336	21	247	248.663
346	21	257	258.232
348	21	259	260.148
352	21	263	263.981
358	21	269	269.733
360	21	271	271.651
366	21	277	277.41
372	21	283	283.172
388	21	298	298.557
396	21	306	306.259
400	21	310	310.122
306	23	211	211.723
310	23	215	215.512
312	23	217	217.407
316	23	220	221.200
330	23	232	234.495
336	23	238	240.202
346	23	248	249.727
348	23	250	251.633
352	23	254	255.448
358	23	260	261.174
360	23	262	263.084
366	23	268	268.816
372	23	274	274.553
378	23	280	280.295
382	23	284	284.125
388	23	289	289.873
396	23	297	297.544
400	23	301	301.382
408	23	309	309.062
306	25	203	203.43
310	25	207	207.198
312	25	209	209.084
316	25	212	212.857
330	25	224	226.086
336	25	230	231.765
346	25	239	241.244
348	25	241	243.142
352	25	245	246.939
358	25	251	252.639
360	25	253	254.54
366	25	259	260.247

n	d	k_{LRS}	k_{New}
372	25	265	265.959
378	25	271	271.676
382	25	275	275.489
388	25	280	281.213
396	25	288	288.853
400	25	292	292.675
408	25	300	300.325
316	27	204	204.529
330	27	216	217.692
336	27	222	223.344
346	27	230	232.779
348	27	232	234.668
352	27	236	238.447
358	27	242	244.122
360	27	244	246.015
366	27	250	251.696
372	27	256	257.383
378	27	262	263.075
382	27	266	266.873
388	27	271	272.573
396	27	279	280.181
400	27	283	283.988
408	27	291	291.608
418	27	301	301.143
420	27	303	303.052
306	29	186	186.879
316	29	196	196.21
330	29	208	209.309
336	29	214	214.934
346	29	222	224.325
348	29	224	226.205
352	29	228	229.968
358	29	233	235.617
360	29	235	237.501
366	29	241	243.158
372	29	247	248.821
378	29	253	254.489
382	29	257	258.27
388	29	262	263.947
396	29	270	271.524
400	29	274	275.315
408	29	282	282.905
418	29	292	292.404
420	29	294	294.305

Table 4

n	d	k_{LRS}	k_{New}
277	9	242	242.218
281	9	246	246.135
283	9	248	248.094
317	9	281	281.44
331	9	295	295.191
337	9	301	301.087
347	9	311	310.919
149	11	110	110.326
151	11	112	112.228
283	11	239	239.687
289	11	245	245.536
293	11	249	249.436
307	11	263	263.1
311	11	267	267.007
313	11	268	268.96
317	11	272	72.869
331	11	286	286.557
337	11	292	292.428
347	11	302	302.217
349	11	304	304.176
353	11	308	308.093
157	13	110.167	110.467
163	13	116	116.136
283	13	231	231.322
289	11	236.238	237.14
293	13	240	241.021
307	13	254	254.617
311	13	258	258.504
313	13	260	260.449
317	13	264	264.339
331	13	277	277.965
337	13	283	283.809
347	13	293	293.556
349	13	295	295.506
353	13	299	299.408
359	13	305	305.262
361	13	307	307.214
367	13	313	313.071
169	15	114	114.288
289	15	228.238	228.781
293	15	232	232.641

n	d	k_{LRS}	k_{New}
307	15	245	246.168
311	15	249	250.037
313	15	251	251.972
317	15	255	255.843
331	15	268	269.405
337	15	274	275.224
347	15	284	284.928
349	15	286	286.87
353	15	290	290.754
359	15	296	296.584
361	15	298	298.528
367	15	304	304.361
373	15	310	310.197
379	15	316	316.036
173	17	110	110.533
179	17	116	116.124
193	17	129	129.224
293	17	224	224.299
307	17	236	237.754
311	17	240	241.603
313	17	242	243.529
317	17	246	247.381
331	17	260	260.878
337	17	265	266.669
347	17	275	276.33
349	17	277	278.263
353	17	281	282.131
359	17	287	287.935
361	17	289	289.871
367	17	295	295.679
373	17	301	301.491
379	17	307	307.306
383	17	311	311.185
389	17	317	317.005
307	19	228	229.377
311	19	232	233.206
313	19	234	235.121
317	19	238	238.954
331	19	251	252.384
337	19	257	258.148
347	19	267	267.763

n	d	k_{LRS}	k_{New}
349	19	269	269.688
353	19	273	273.538
359	19	279	279.317
360	19	280	280.251
367	19	287	287.027
389	19	308	308.265
307	21	220	221.033
311	21	224	224.842
313	21	225.238	226.748
317	21	229	230.56
331	21	242	243.923
337	21	248	249.658
347	21	258	259.228
349	21	260	261.144
353	21	264	264.976
359	21	270	270.729
360	21	271	271.666
367	21	278	278.406
373	21	284	284.168
389	21	299	299.553
397	21	307	307.255
401	21	311	311.109
307	23	212	212.719
311	23	216	216.507
313	23	217.238	218.403
317	23	221	222.195
331	23	233	235.491
337	23	239	241.198
347	23	249	250.723
349	23	251	252.629
353	23	255	256.444
359	23	261	262.17
361	23	263	264.08
367	23	269	269.812
373	23	275	275.55
379	23	281	281.291
383	23	285	285.121
389	23	290	290.869
397	23	298	298.54
401	23	302	302.378
409	23	310	310.059

n	d	k_{LRS}	k_{New}
307	25	204	204.858
311	25	208	208.633
313	25	209.238	210.522
317	25	213	214.301
331	25	225	227.552
337	25	230.238	233.241
347	25	240	242.734
349	25	242	244.634
353	25	246	248.437
359	25	252	254.145
361	25	254	256.048
367	25	260	261.763
373	25	266	267.482
379	25	272	273.205
383	25	276	277.024
389	25	281	282.754
397	25	289	290.402
401	25	293	294.228
409	25	301	301.886
419	25	311	311.468
421	25	313	313.385
307	27	196	196.145
313	27	200.238	201.77
317	27	205	205.524
331	27	217	218.688
337	27	221.238	224.34
347	27	231	233.775
349	27	233	235.664
353	27	237	239.443
359	27	243	245.118
361	27	245	247.011
367	27	251	252.692
373	27	257	258.379
379	27	263	264.072
383	27	267	267.869
389	27	272	273.57
397	27	280	281.177
401	27	284	284.984
409	27	292	292.604
419	27	302	302.14
421	27	304	304.048

n	d	k_{LRS}	k_{New}
317	29	197	197.205
331	29	209	210.304
337	29	214.238	215.93
347	29	223	225.321
349	29	225	227.201
353	29	228.238	2230.964
359	29	234	236.613
361	29	236	238.497
367	29	242	244.154
373	29	248	249.817
379	29	254	255.485
383	29	258	259.266
389	29	263	264.943
397	29	271	272.52
401	29	275	276.312
409	29	283	283.902
419	29	293	293.401
421	29	295	295.302

this he spent most time in Institute of Information Processing, Austrian Academy of Sciences until 1998. From March of 1998 to November of 2007, he was working in National University of Singapore. Since December of 2007, he has been with Nanyang Technological University and currently is a full Professor. Dr. Xing has been working on the areas of algebraic curves over finite fields, coding theory, cryptography and quasi-Monte Carlo methods, etc.

Acknowledgment

We would like to thank Ding Yang for computation of the maximal size of binary constant-weight codes given in Tables 1 and 2.

REFERENCES

- [1] A. E. Brouwer, *Table of nonlinear binary constant-weight codes*, online table at <http://www.win.tue.nl/~aeb/codes/Andw.html>.
- [2] R. L. Graham and N. J. A. Sloane, Lower bounds for constant weight codes, *IEEE Trans. Inform. Theory*, **26**(1980), 37–43.
- [3] S. Litsyn, E. M. Rains and N. J. A. Sloane, *Table of nonlinear binary codes*, online table at <http://www.eng.tau.ac.il/~litsyn/tableand/>.
- [4] C. Xing, *Constructions of codes from residue rings of polynomials*, *IEEE Trans. Inform. Theory*, **48**(2002), 2995–2997.

Lingfei Jin received her B.A. degree in mathematics from Hefei University of Technology, China in 2009. In 2013, she received her Ph.D. degree from Nanyang Technological University, Singapore. Currently, she is an associate Professor at the School of Computer Science, Fudan University, China. Her research interests include quantum information, cryptography and coding theory.

Chaoping Xing received his Ph.D. degree in 1990 from University of Science and Technology of China. From 1990 to 1993 he was a lecturer and associate professor in the same university. He joined University of Essen, Germany as an Alexander von Humboldt fellow from 1993 to 1995. After