Low-Correlation, Large Linear Span Sequences From Function Fields

Chaoping Xing, P. Vijay Kumar, *Fellow, IEEE*, and Cunsheng Ding, *Member, IEEE*

***Abstract*—A general method of generating families of binary sequences with low correlation as well as large linear span is presented. The lower bound on the linear span is on the order of the square root of the period of each sequence within the family. The design makes use of the theory of function fields. Two example applications of this method are presented in which the underlying function fields are the rational and elliptic function fields respectively.**

***Index Terms*—Correlation, function fields, linear span, pseudorandom sequences, sequences.**

I. Introduction

A COMMONLY used method of generating low-correlation sequences is described below.

Let $q = p^e$, p prime, $e \geq 1$ and let $d \geq 1$ be a fixed integer. Let $\boldsymbol{F}_q$ denote the finite field of q elements. Let $\mathcal{F}$ be the collection of all polynomials over $\boldsymbol{F}_q$ of degree $\leq d$. Let α be a primitive element in $\boldsymbol{F}_q$. Let $\mathcal{S}$ denote the collection of sequences

$$\mathcal{S} = \left\{ \mathrm{Tr}(f(\alpha^t)) \right\}_{t \in Z} \mid f \in \mathcal{F} \}$$

where Tr denotes the trace from $\boldsymbol{F}_q \rightarrow \boldsymbol{F}_p$. The sequences in $\mathcal{S}$ all have period dividing $q-1$. Let $\mathcal{S}'$ denote the subset of $\mathcal{S}$ consisting of sequences of period $= q-1$.

Two periodic sequences are said to be cyclically equivalent if one is a cyclic shift of the other. Let $\mathcal{S}'$ be partitioned into equivalence classes where all the sequences within an equivalence class are cyclically equivalent. Let $\mathcal{S}_{cd}$ be the subset of $\mathcal{S}'$ obtained by picking one representative from each equivalence class. Let $\{f_i\}$ denote the polynomials associated to the sequences in $\mathcal{S}_{cd}$.

Manuscript received February 6, 2000; revised January 20, 2003. The work of C. P. Xing was supported in part by the MOE-ARF under Grant R-146-000-029-112 and the Hundred Talents Program of the Chinese Academy of Science.

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

P. V. Kumar is with the Department of Electrical Engineering–Systems, EEB 500, University of Southern California, Los Angeles, CA 90089-2565 USA (e-mail: vijayk@ceng.usc.edu).

C. S. Ding is with the Department of Computer Science, Hong Kong University of Science and Technology, Kowloon, Hong Kong, China (e-mail: cding@cs.ust.hk).

Communicated by A. M. Klapper, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2003.811905

Let ω be a complex, primitive pth root of unity. Then the correlation between the ith and jth sequences at shift τ is given by

$$C_{ij}(\tau) = \sum_{t=0}^{q-2} \omega^{\mathrm{Tr}(f_i(\alpha^{t+\tau}) - f_j(\alpha^t))}$$

and may be regarded as an exponential sum [5], [3] whose magnitude can be upper-bounded using the Weil–Carlitz–Uchiyama bound

$$\max_{i,j,\tau} \{ |C_{i,j}(\tau)| \mid \text{ either } i \neq j \text{ or } \tau \neq 0 \} \leq (d-1)\sqrt{q} + 1.$$

For example, setting $d = 3$, $p = 2$, e odd, in the method generates one instance of the well-known and optimal Gold sequence family. A generalization of this method to Galois rings generates the sequence families described in [4].

One disadvantage of this method, however, is that the sequences produced by this method have short linear span. (The linear span of a periodic sequence is the length of a shortest linear feedback shift register that is capable of generating the sequence.) For example, in the case of the Gold sequence family of length $2^m - 1$, m odd, the linear span is upper-bounded by $2m$. One method of increasing the linear span is to replace the polynomial f by a rational function $f(x)/g(x)$.

The present paper takes this idea one step further first by working over an arbitrary function field (the above approach can be viewed as working on the rational function field) and second by constructing families of sequences in such a way that the period, the maximum correlation value, and the minimum linear span can all be related to the number of places of degree one (rational points) on an appropriately constructed Artin–Schreier extension of the underlying function field.

The use of function fields in sequence construction is not new (see [2], [4], [9]) since the Weil–Carlitz–Uchiyma bound on exponential sums referred to above is itself based on an estimate of the number of places of degree one of an Artin–Schreier extension of the rational function field, i.e., the function field corresponding to the projective line.

Our approach makes it possible to design sequence families where the period is not necessarily of the commonly found form $p^e - 1$ for some prime p.

The parameters of two example constructions arising from the method presented here appear in Table I.

In Table I, t is an integer satisfying one of the following conditions:

1) t is an odd integer between $-2\sqrt{q} = -2^{m/2+1}$ and $2\sqrt{q} = 2^{m/2+1}$;
2) $t = 0$;

0018-9448/03$17.00 © 2003 IEEE

TABLE I

Funct. field	period	family size	max corrln	linear span
rational f.f.	2^m-1	2^{m-1}	$6\sqrt{2^m}$	$\sqrt{2^m}/4$
elliptic f.f.	2^m+1+t	2^{m-1}	$10\sqrt{2^m}$	$\sqrt{2^m}/4$

3) $t=\sqrt{q}=2^{m/2}$ if m is even, and $t=\sqrt{2q}=2^{(m+1)/2}$ if m is odd.

We now introduce some definitions.

Definition 1.1: The linear complexity of a nonzero binary periodic sequence $\boldsymbol{a}=\{a_i\}_{i=0}^{\infty}$ is defined to be the smallest positive integer k such that there exist $k+1$ binary numbers $\lambda_0, \lambda_2, \ldots, \lambda_k$ with $\lambda_0=\lambda_k=1$ satisfying

$$\sum_{i=0}^{k}\lambda_i a_{i+v}=0$$

for all $v\geq 0$. The linear complexity of $\boldsymbol{a}$ is denoted by $\ell(\boldsymbol{a})$.

Definition 1.2: Let $\boldsymbol{a}_1=\{a_{1,i}\}_{i=0}^{\infty}$ and $\boldsymbol{a}_2=\{a_{2,i}\}_{i=0}^{\infty}$ be two binary sequences of period n (it is allowed that $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ are the same). Then their correlation at shift w, with $0\leq w\leq n-1$, is given by

$$c_{\boldsymbol{a}_1,\boldsymbol{a}_2}(w)=\sum_{i=1}^{n}(-1)^{a_{1,i}+a_{2,i+w}}.$$

Definition 1.3: Let $\mathcal{S}=\{\boldsymbol{a}_i | i=1, 2, \ldots, l\}$ be a family of binary sequences of period n. We put

$$\ell_{\min}(\mathcal{S})=\min\{\ell(\boldsymbol{a})|\boldsymbol{a}\in\mathcal{S}\}$$

and

$$c_{\max}(\mathcal{S})=\max\{|c_{\boldsymbol{a}_i,\boldsymbol{a}_j}(w)||i\neq j \text{ or } w\not\equiv 0 \pmod n\}.$$

The next section of the paper presents some results on function fields that we will make use of. Section III presents the general construction. Sections IV and V present specific examples of this construction that relate to the rational and elliptic function fields, respectively.

II. Some Background on Function Fields

We first fix some notation for this section. As in the previous section, q is the power of a prime p.

F	global function field with full constant field $\boldsymbol{F}_q$ (we simply say that $F/\boldsymbol{F}_q$ is a function field);
$g=g(F)$	genus of F;
$\boldsymbol{P}_F$	set of all places of F;
$N(F)$	number of rational places of F;
ν_P	normalized discrete valuation corresponding a place P of F.

A divisor G of F is a formal sum

$$G=\sum_{P\in S}m_P P$$

where S is a finite subset of $\boldsymbol{P}_F$ and each m_P is an integer. The degree of G is defined by

$$\deg(G)=\sum_{P\in S}m_P\deg(P)\in\boldsymbol{Z}$$

and the support of G given by

$$\operatorname{Supp}(G)=\{P\in S|m_P\neq 0\}.$$

For a nonzero element f of F, let $\mathcal{Z}(f)$ and $\mathcal{N}(f)$ denote the set of zeros and poles of f, respectively. Define the zero and pole divisors of f via

$$(f)_0=\sum_{P\in\mathcal{Z}(f)}\nu_P(f)P,\qquad (f)_\infty=-\sum_{P\in\mathcal{N}(f)}\nu_P(f)P$$

respectively.

Then, $\deg(f)_0=\deg(f)_\infty$ [8, p. 18]. For a divisor G, we form the vector space

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

where $\operatorname{div}(x)=(x)_0-(x)_\infty$ is the principal divisor of x. Then $\mathcal{L}(G)$ is a finite-dimensional vector space over $\boldsymbol{F}_q$. By the Riemann–Roch theorem [8], we have

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

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

Definition 2.1: An element z is called degenerate if z can be written as the form $\alpha+h^p-h$ for some $\alpha\in\boldsymbol{F}_q$ and $h\in F$. Otherwise, z is nondegenerate.

Lemma 2.2: If there exists a place Q of F such that $\nu_Q(z)<0$ is prime to p, then z is nondegenerate.

Proof: Suppose that z is degenerate, i.e., z is of the form $\alpha+h^p-h$ for some $\alpha\in\boldsymbol{F}_q$ and $h\in F$. Then we have

$$\nu_Q(z)=\nu_Q(h^p)=p\nu_Q(h).$$

This contradicts $(p, \nu_Q(h))=1$. The proof is complete.

For a nondegenerate element z of F, we can construct an Artin–Schreier extension over F. The following results can be found in [8, Proposition VIII.2.8].

Lemma 2.3: Let z be a nondegenerate element of F, then Y^p-Y-z is an irreducible polynomial of $F[Y]$. Let y be a root of Y^p-Y-z, then $F(y)$ is cyclic extension of degree p over F, and $\operatorname{Gal}(F(y)/F)\simeq\boldsymbol{Z}/p\boldsymbol{Z}$.

Remark 2.4: If y_1 and y_2 are two roots of Y^p-Y-z, then there exists an element $a\in\boldsymbol{F}_p$ such that $y_1=y_2+a$. Hence, $F(y_1)=F(y_2)$, i.e., the field $F(y)$ is unique for any root y of Y^p-Y-z. We denote the field $F(y)$ by E_z.

The following lemma provides us with an estimate of the genus of such an Artin–Schreier extension.

Lemma 2.5: Let z be a nondegenerate element of F, then the genus of E_z satisfies

$$g(E_z)\leq pg(F)+(p-1)(d-1)$$

where d is the degree $\deg(z)_\infty$ of the pole divisor of z.

Proof: A place P of F is ramified in E_z/F only if P is a pole of z. If P is ramified, then P is totally ramified and the different exponent d_P of P is at most $(\nu_P(z)+1)(p-1)$.

It follows from the Hurwtiz formula that

$$2g(E_z) - 2 = [E_z\colon F](2g(F) - 2) + \sum_{Q \in \boldsymbol{P}_{E_z}} d_Q \deg(Q) \quad (2)$$

where $\boldsymbol{P}_{E_z}$ is the set of all places of E_z and d_Q is the different exponent of Q.

We have

$$\begin{aligned} 2g(E_z)-2 &= [E_z\colon F](2g(F)-2) + \sum_{P \in \boldsymbol{P}_F} \sum_{Q|P} d_Q \deg(Q) \\ &= p(2g(F)-2) + \sum_{P \in \mathcal{N}(z)} d_P \deg(P) \\ &\le p(2g(F)-2) + \sum_{P \in \mathcal{N}(z)} (\nu_P(z)+1)(p-1)\deg(P) \\ &= p(2g(F)-2) + (p-1)d + (p-1) \sum_{P \in \mathcal{N}(z)} \deg(P) \\ &\le p(2g(F)-2) + 2(p-1)d. \end{aligned}$$

Our result follows from the above inequality.

Next we look at the Hamming weight of trace vectors associated with nondegenerate elements and some rational places of F.

Lemma 2.6: Let $P_1, P_2, \ldots, P_n$ be n distinct rational places. Let $z \in F$ be a nondegenerate element of F such that $\nu_{P_i}(z) \ge 0$ for all $i = 1, 2, \ldots, n$. Let S_{E_z} be the set of rational places of E_z lying above those rational places of F that are outside $\{P_1, P_2, \ldots, , P_n\}$. Then the Hamming weight of the vector

$$(\mathrm{Tr}(z(P_1)), \mathrm{Tr}(z(P_2)), \ldots, \mathrm{Tr}(z(P_n)))$$

equals

$$n - \frac{N(E_z) - \#S_{E_z}}{p}$$

where $z(P_i)$ is the residue class of z modulo P_i, $N(E_z)$ denotes the number of rational places of E_z, and $\#S_{E_z}$ denotes the cardinality of the set S_{E_z}.

Proof: We refer to [8, Proposition VIII.2.8] for the proof of the special case where F is the rational function field. For a fixed i, $\mathrm{Tr}(z(P_i)) = 0$ if and only if $z(P_i)$ can be written as the form $z(P_i) = a^p - a$ for some $a \in \boldsymbol{F}_q$. This is equivalent to the fact that P_i completely splits into p rational places in $E_z = F(y)$, where y satisfies the equation

$$y^p - y = z.$$

Let r be the number of rational places in $\{P_1, P_2, \ldots, P_n\}$ which split completely in $F(y)/F$. It is clear that

$$pr + \#S_{E_z} = N(E_z)$$

and the Hamming weight of

$$(\mathrm{Tr}(z(P_1)), \mathrm{Tr}(z(P_2)), \ldots, \mathrm{Tr}(z(P_n)))$$

is equal to

$$n - r = n - \frac{N(E_z) - \#S_{E_z}}{p}.$$

Remark 2.7: It is obvious that

$$0 \le \#S_{E_z} \le p(N(F) - n).$$

The following lemma provides a sufficient condition under which a set of elements of F are $\boldsymbol{F}_q$-linearly independent.

Lemma 2.8: Let $z_1, z_2, \ldots, z_n$ be n elements of F. Suppose there exist n distinct places $P_1, P_2, \ldots, P_n$ of F such that $\nu_{P_i}(z_j) < 0$ if and only if $i = j$ for all $1 \le i, j \le n$. Then $z_1, z_2, \ldots, z_n$ are $\bar{\boldsymbol{F}}_q$-linearly independent.

Proof: Suppose that there exist k elements $\lambda_1, \lambda_2, \ldots, \lambda_k$ of $\boldsymbol{F}_q$ with $\lambda_l \ne 0$ for some $1 \le l \le k$ such that $\sum_{i=1}^{k} \lambda_i z_i = 0$, i.e.,

$$-\lambda_l z_l = \sum_{i \ne l} \lambda_i z_i. \quad (3)$$

Hence, $\nu_P(-\lambda_l z_l) < 0$ and $\nu_P(\sum_{i \ne l} \lambda_i z_i) \ge 0$. This contradicts (3).

An $\boldsymbol{F}_q$-automorphism σ is an automorphism of F keeping all elements of $\bar{\boldsymbol{F}}_q$ fixed. $\mathrm{Aut}(F/\bar{\boldsymbol{F}}_q)$ denotes the group of all $\boldsymbol{F}_q$-automorphisms of F. The following results can be easily proved.

Lemma 2.9 (see [1], [8]): Let $\sigma \in \mathrm{Aut}(F/\boldsymbol{F}_q)$, $P \in \boldsymbol{P}_F$, and $f \in F$, then

1) $\sigma(P)$ is also a place of F with $\deg(\sigma(P)) = \deg(P)$;
2) $\nu_{\sigma(P)}(\sigma(f)) = \nu_P(f)$;
3) $\sigma(f)(\sigma(P)) = f(P)$ if $\nu_P(f) \ge 0$.

In this paper, we are interested only in the rational function field and the function fields of elliptic curves. The automorphisms of these two types of function fields will be discussed in Sections IV and V.

III. The General Construction

From now on, we always assume that the characteristic p of $\boldsymbol{F}_q$ is equal to 2. We also fix some notation for this section.

- P a rational place of F;
- σ an automorphism in $\mathrm{Aut}(F/\boldsymbol{F}_q)$;
- n the least positive integer satisfying $\sigma^n(P) = P$, i.e., $\sigma^n(P) = P$ and $\sigma^i(P) \ne P$ for all $1 \le i \le n-1$.

Put $P_i = \sigma^i(P)$ for all integer $i \in \boldsymbol{Z}$. Then $P_{j+n} = P_j$ for all $j \in \boldsymbol{Z}$ and $P_l, P_{l+1}, \ldots, P_{l+n-1}$ are n pairwise distinct rational places for any fixed $l \in \boldsymbol{Z}$. For an element $z \in F$ with $\nu_{P_i}(z) \ge 0$, define the binary sequence

$$\boldsymbol{a}_z = \{\mathrm{Tr}(z(P_i))\}_{i=0}^{\infty}.$$

It is clear that n divides the period of $\boldsymbol{a}_z$. The following result provides a sufficient condition under which n equals the period of $\boldsymbol{a}_z$.

Proposition 3.1: Let $z \in F$ satisfy $\nu_{P_i}(z) \ge 0$. Suppose that Q is the unique pole of z with $(\nu_Q(z), 2) = 1$, and $Q, \sigma(Q), \sigma^2(Q), \ldots, \sigma^{n-1}(Q)$ are pairwise distinct. If $d = \deg(z)_\infty$ satisfies

$$q + 1 + 2(2g(F) + 2d - 1)\sqrt{q} < 2n$$

then the period of $\boldsymbol{a}_z$ is equal to n.

Proof: Suppose n is not the period of $\boldsymbol{a}_z$, then there exists a positive integer k with $k < n$ such that k is the period of $\boldsymbol{a}_z$. Consider the function

$$f = z - \sigma^k(z).$$

Note that Q is the unique pole of z. Hence, $\sigma^k(Q)$ is the unique pole of $\sigma^k(z)$ for all $k \in \boldsymbol{Z}$. It follows from Lemma 2.9 that f is a nonzero element. The degree of the pole divisor of f satisfies

$$\deg(f)_\infty = \deg(z - \sigma^k(z))_\infty = 2\deg(z)_\infty = 2d. \tag{4}$$

However, we have

$$\begin{aligned} f(P_{i+k}) &= z(P_{i+k}) - \sigma^k(z)(P_{i+k}) \\ &= z(P_{i+k}) - z(\sigma^{-k}(P_{i+k})) \\ &= z(P_{i+k}) - z(P_i) \end{aligned}$$

for all $i \geq 0$. Thus,

$$\mathrm{Tr}(f(P_{i+k})) = \mathrm{Tr}(z(P_{i+k}) - z(P_i)) = 0$$

since k is the period of $\boldsymbol{a}_z$. Hence,

$$(\mathrm{Tr}(f(P_1)), \mathrm{Tr}(f(P_2)), \ldots, \mathrm{Tr}(f(P_n)))$$

is the zero vector. By Lemma 2.6

$$n - \frac{N(E_f) - \#S_{E_f}}{2} = 0$$

i.e.,

$$N(E_f) = 2n + |S_{E_f}| \geq 2n. \tag{5}$$

By the Hasse–Weil theorem, we have

$$N(E_f) \leq q + 1 + 2g(E_f)\sqrt{q}. \tag{6}$$

By Lemma 2.5, we get

$$g(E_f) \leq 2g(F) + \deg(f)_\infty - 1 = 2g(F) + 2d - 1. \tag{7}$$

Combining (6) with (7) gives

$$N(E_f) \leq q + 1 + 2(2g(F) + 2d - 1)\sqrt{q}. \tag{8}$$

Combining (5) with (8) yields

$$2n \leq q + 1 + 2(2g(F) + 2d - 1)\sqrt{q}.$$

This contradicts our condition. Hence the period of $\boldsymbol{a}_z$ is equal to n.

Theorem 3.2: Let $z \in F$ satisfy $\nu_{P_i}(z) \geq 0$. Suppose that Q is the unique pole of z with $(\nu_Q(z), 2) = 1$, and $Q, \sigma(Q), \sigma^2(Q), \ldots, \sigma^{n-1}(Q)$ are pairwise distinct. Then the linear complexity of $\boldsymbol{a}_z$ satisfies

$$\ell(\boldsymbol{a}_z) \geq \frac{2n - q - 1 - 2(2g(F) + d - 1)\sqrt{q}}{2d\sqrt{q}}$$

where $d = \deg(z)_\infty$.

Proof: Denote $\ell(\boldsymbol{a}_z)$ by s. If $s = n$, we have nothing to prove. Hence, we may assume that $s < n$. Then there exist $s+1$ binary numbers $\lambda_0, \lambda_1, \ldots, \lambda_s$ such that $\lambda_0 = \lambda_s = 1$ and

$$\sum_{i=0}^{s} \lambda_i \mathrm{Tr}(z(P_{i+v})) = 0$$

for all $v \geq 0$. Put

$$u = \sum_{i=0}^{s} \lambda_i \sigma^{-i}(z)$$

then u is nondegenerate by Lemmas 2.9 and 2.2 since $\sigma^{-i}(Q)$ is the unique pole of $\sigma^{-i}(z)$ for any $0 \leq i \leq n-1$. Moreover, $\deg(u)_\infty = (s+1)\deg(z)_\infty = (s+1)d$.

Consider

$$\begin{aligned} \sum_{i=0}^{s} \lambda_i \mathrm{Tr}(z(P_{i+v})) &= \mathrm{Tr}\left(\sum_{i=0}^{s} \lambda_i z(P_{i+v})\right) \\ &= \mathrm{Tr}\left(\sum_{i=0}^{s} \lambda_i z(\sigma^i(P_v))\right) \\ &= \mathrm{Tr}\left(\sum_{i=0}^{s} \lambda_i \sigma^{-i}(z)(P_v)\right) \\ &= \mathrm{Tr}(u(P_v)). \end{aligned}$$

We obtain

$$(\mathrm{Tr}(u(P_1)), \mathrm{Tr}(u(P_2)), \ldots, \mathrm{Tr}(u(P_n))) = \boldsymbol{0}.$$

By Lemma 2.6, we have

$$0 = n - \frac{N(E_u) - \#S_{E_u}}{2} \geq n - \frac{1}{2}N(E_u).$$

Hence, by the Hasse–Weil bound and Lemma 2.5

$$\begin{aligned} 2n &\leq N(E_u) \leq q + 1 + 2g(E_u)\sqrt{q} \\ &\leq q + 1 + 2(2g(F) + d(s+1) - 1)\sqrt{q}. \end{aligned}$$

Our result follows.

The above theorem indicates that the linear complexity of $\boldsymbol{a}_z$ is good if the period n is relatively large compared with q and $2g(F)\sqrt{q}$. Now we want to look at the correlation of such sequences.

Theorem 3.3: Let z_1, z_2 be two elements of F with $d_i = \deg(z_i)_\infty$ and $\nu_{P_j}(z_i) \geq 0$ for all $1 \leq i \leq 2$ and $0 \leq j \leq n-1$ (it is allowed that $z_1 = z_2$). Suppose that $z_1 + \sigma^{-w}(z_2)$ is nondegenerate for some $w \in \boldsymbol{Z}$. Then the correlation satisfies $\left|c_{\boldsymbol{a}_{z_1}, \boldsymbol{a}_{z_2}}(w)\right| \leq 2(2g(F)+d-1)\sqrt{q} + |q+1-n| + 2(N(F)-n)$ where d is the degree of the pole divisor of $z_1 + \sigma^{-w}(z_2)$.

Proof: Put $u = z_1 + \sigma^{-w}(z_2)$. By the definition, we have

$$\begin{aligned} & c_{\boldsymbol{a}_{z_1}, a_{z_2}}(w) \\ &= \sum_{i=1}^{n} (-1)^{\mathrm{Tr}(z_1(P_i)) + \mathrm{Tr}(z_2(P_{i+w}))} \\ &= \sum_{i=1}^{n} (-1)^{\mathrm{Tr}(z_1(P_i) + z_2(P_{i+w}))} \\ &= \sum_{i=1}^{n} (-1)^{\mathrm{Tr}(z_1(P_i) + \sigma^{-w}(z_2)(P_i))} \\ &= \sum_{i=1}^{n} (-1)^{\mathrm{Tr}(u(P_i))} \\ &= n - 2wt(\mathrm{Tr}(u(P_1)), \mathrm{Tr}(u(P_2)), \ldots, \mathrm{Tr}(u(P_n))) \\ &= n - 2\left(n - \frac{N(E_u) - \#S_{E_u}}{2}\right) \\ &= N(E_u) - n - \#S_{E_u}. \end{aligned}$$

By the Hasse–Weil bound and Lemma 2.5, we have

$$|N(E_u) - (q+1)| \le 2g(E_u)\sqrt{q} \le 2(2g(F)+d-1)\sqrt{q}.$$

It is also clear that the size of S_{E_u} is at most $2(N(F)-n)$.

Hence,

$$\begin{aligned}&\left|c_{\boldsymbol{a}_{z_1}, a_{z_2}}(w)\right| \\ &\quad = |N(E_u) - n - \#S_{E_u}| \\ &\quad \le |N(E_u) - (q+1)| + |q+1-n| + \#S_{E_u} \\ &\quad \le 2(2g(F)+d-1)\sqrt{q} + |q+1-n| + 2(N(F)-n).\end{aligned}$$

The proof is complete.

IV. Example Construction Over the Rational Function Field

Assume that q is even in this section. We fix some notation again for this section:

ϵ	fixed primitive element of $\boldsymbol{F}_q$;
$F = \boldsymbol{F}_q(x)$	rational function field;
ϕ	automorphism of $F/\boldsymbol{F}_q$: $x \mapsto \epsilon x$;
P	unique zero of $x-1$.

Let P_i be the unique zero of $\phi^i(x-1) = \epsilon^i x - 1 = \epsilon^i(x-\epsilon^{-i})$ for all $i \in \boldsymbol{Z}$, and put $n = q-1$. Then $P_i, P_{i+1}, \ldots, P_{i+n-1}$ are pairwise distinct for any fixed $i \in \boldsymbol{Z}$. Moreover, $P_j = P_{j+n}$ for all $j \in \boldsymbol{Z}$ since ϕ^n is the identity. Let $\boldsymbol{P}_d(F)$ be the set of all places of degree $d \ge 2$. There is a one-to-one correspondence between $\boldsymbol{P}_d(F)$ and the set of all monic irreducible polynomials of degree d of $\boldsymbol{F}_q[x]$. Therefore, the size $I_q(d)$ of $\boldsymbol{P}_d(F)$ is equal to the number of monic irreducible polynomials of degree d of $\boldsymbol{F}_q[x]$ and is given [5] by

$$I_q(d) = \frac{1}{d}\sum_{b|d}\mu\left(\frac{d}{b}\right)q^b$$

where $\mu(\cdot)$ is the Möbius function.

Lemma 4.1: Let $Q \in \boldsymbol{P}_d(F)$. If $d \ge 2$ and $(d, q-1) = 1$, then $\phi^i(Q), \phi^{i+1}(Q), \ldots, \phi^{i+n-1}(Q))$ are pairwise distinct for any fixed $i \in \boldsymbol{Z}$.

Proof: It is sufficient to show that $\phi^l(Q) \ne Q$ for any $1 \le l \le n-1$. Let $f(x)$ be the monic irreducible polynomial with unique zero Q. Then $\phi^l(Q)$ is the unique zero of $\phi^l(f(x)) = f(\phi^l(x)) = f(\epsilon^l x)$. In order to prove that $\phi^l(Q) \ne Q$, we need to show that any roots of $f(x)$ are not roots of $\phi^l(f(x))) = f(\epsilon^l x)$. Let $\alpha \in \boldsymbol{F}_{q^d}$ be a root of $f(x)$. We want to show that α is not a root of $f(\epsilon^l x)$. This is equivalent to showing that $\epsilon^l\alpha$ is not a root of $f(x)$. Suppose that $\epsilon^l\alpha$ is a root of $f(x)$. Since all roots of $f(x)$ are $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, there exists an integer k with $1 \le k \le d-1$ such that $\epsilon^l\alpha = \alpha^{q^k}$, i.e., $\epsilon^l = \alpha^{q^k-1}$. This yields

$$1 = (\epsilon^l)^{q-1} = \alpha^{(q^k-1)(q-1)}. \tag{9}$$

Since $(d, q-1) = 1$, we have $((q^d-1)/(q-1), q-1) = 1$. Knowing $\alpha^{q^d-1} = 1$, we obtain from (9) that $\alpha^{q^k-1} = 1$, i.e., $\alpha^{q^k} = \alpha$. This contradicts the fact that $f(x)$ is an irreducible polynomial of degree d since $1 \le k \le d-1$.

By the above lemma, we find that for $d \ge 2$ with $(d, q-1) = 1$, the action of the cyclic group $\langle\phi\rangle$ of order $n = q-1$ on $\boldsymbol{P}_d(F)$ divides $\boldsymbol{P}_d(F)$ into $r = I_q(d)/n$ equivalent classes. Each class contains n places of degree d. We choose only one place from each class. Thus, we obtain r places of degree d

$$Q_1, Q_2, \ldots, Q_r.$$

It is clear that for $1 \le i \ne j \le r$

$$Q_j \notin \{\phi^s(Q_i) | s \in \boldsymbol{Z}\} = \{Q_i, \phi(Q_i), \ldots, \phi^{n-1}(Q_i)\}.$$

For each $1 \le i \le r$, let $f_i(x)$ be the monic irreducible polynomial of degree d of $\boldsymbol{F}_q[x]$ with the unique zero Q_i. Put

$$z_i = \frac{1}{f_i(x)}.$$

Then Q_i is the unique pole of z_i and $\nu_{Q_i}(z_i) = -1$. Consider the family of binary sequences

$$\mathcal{S}_d = \{\boldsymbol{a}_{z_i} | i = 1, 2, \ldots, r = I_q(d)/(q-1)\}$$

where

$$\boldsymbol{a}_{z_i} = \{\mathrm{Tr}(z_i(P_j))\}_{j=0}^{\infty} = \{\mathrm{Tr}(z_i(\epsilon^j))\}_{j=0}^{\infty}.$$

Theorem 4.2: Let $2 \le d \le ((q-7)/(2\sqrt{q})+1)/2$ and $(d, q-1) = 1$. Let $\mathcal{S}_d$ be the family of binary sequences as constructed above. Then $\mathcal{S}_d$ is of size $I_q(d)/(q-1)$ and each sequence in $\mathcal{S}_d$ is of period $n = q-1$. Moreover

$$\ell_{\min}(\mathcal{S}_d) \ge \frac{q-3-2(d-1)\sqrt{q}}{2d\sqrt{q}}$$

$$c_{\max}(\mathcal{S}_d) \le 2(2d-1)\sqrt{q} + 6.$$

Proof: By the condition $d \le ((q-7)/(2\sqrt{q})+1)/2$, we get $q + 1 + 2(2g(F) + 2d - 1)\sqrt{q} < 2n$. It follows from Proposition 3.1 that the period of each sequence in $\mathcal{S}_d$ is $n = q-1$. Let $\boldsymbol{a}_{z_i} \in \mathcal{S}_d$ for some $1 \le i \le r = I_q(d)/(q-1)$. Then Q_i is the unique pole of z_i and $Q_i, \phi(Q_i), \ldots, \phi^{n-1}(Q_i)$ are pairwise distinct. By Theorem 3.2, we have

$$\begin{aligned}\ell(\boldsymbol{a}_{z_i}) &\ge \frac{2n-q-1-2(2g(F)+d-1)\sqrt{q}}{2d\sqrt{q}} \\ &= \frac{q-3-2(d-1)\sqrt{q}}{2d\sqrt{q}}\end{aligned}$$

for all $1 \le i \le r$. This means that

$$\ell_{\min}(\mathcal{S}_d) \ge \frac{q-3-2(d-1)\sqrt{q}}{2d\sqrt{q}}.$$

Now let $\boldsymbol{a}_{z_i}$ and $\boldsymbol{a}_{z_j}$ be two sequences of $\mathcal{S}_d$ (it is allowed that $j = i$). For $w \in \boldsymbol{Z}$, consider the function

$$u = z_i + \phi^{-w}(z_j).$$

Q_i is the unique pole of z_i and $\phi^{-w}(Q_j)$ is the unique pole of $\phi^{-w}(z_j)$.

Case 1: $i \ne j$, then $Q_i \ne \phi^{-w}(Q_j)$ since

$$Q_j \notin \{\phi^s(Q_i) | s \in \boldsymbol{Z}\}$$

thus Q_i is not a pole of $\phi^{-w}(z_j)$ and

$$\nu_{Q_i}(u) = \min\{\nu_{Q_i}(z_i), \nu_{Q_i}(\phi^{-w}(z_j))\} = -1.$$

Therefore, u is nondegenerate by Lemma 2.2.

Case 2. $i = j$ and $0 < w < n$. Then $Q_i \neq \phi^{-w}(Q_i)$, thus, the same arguments as in Case 1 show that u is nondegenerate.

For both cases, $z_i + \phi^{-w}(z_j)$ is nondegenerate. By Theorem 3.3, we obtain

$$\begin{aligned}&\left|c_{\boldsymbol{a}_{z_1},\boldsymbol{a}_{z_2}}(w)\right| \\ &\quad\le 2(2g(F)+2d-1)\sqrt{q}+|q+1-n|+2(N(F)-n) \\ &\quad= 2(2d-1)\sqrt{q}+|q+1-(q-1)|+2(q+1-(q-1)) \\ &\quad= 2(2d-1)\sqrt{q}+6.\end{aligned}$$

Since $c_{\max}(\mathcal{S}_d) < n$, it is clear that sequences $\boldsymbol{a}_{z_1}, \boldsymbol{a}_{z_2}, \ldots, \boldsymbol{a}_{z_r}$ are pairwise distinct. Hence, the size of $\mathcal{S}_d$ is equal to $r = I_q(d)/(q-1)$. The proof is complete.

We rewrite Theorem 4.2 into the following form by taking $q = 2^m$.

Theorem 4.3: Let $m \geq 3$, let

$$2 \le d \le \frac{2^m-7+2^{m/2+1}}{2^{m/2+2}} \quad \text{and} \quad (d, 2^m-1) = 1.$$

Then there exists a family $\mathcal{S}_d$ of binary sequences such that

a) $\#S_d = \frac{I_{2^m}(d)}{2^m-1}$;
b) each sequence in $\mathcal{S}_d$ is of period $2^m - 1$;
c)
$$\ell_{\min}(\mathcal{S}_d) \ge \frac{2^m-3-(d-1)2^{m/2+1}}{d2^{m/2+1}};$$
d)
$$c_{\max}(\mathcal{S}_d) \le (2d-1)2^{m/2+1}+6.$$

Corollary 4.4:

i) Let $m \geq 6$, then there exists a family $\mathcal{S}_2$ of binary sequences such that
   a) $\#\mathcal{S}_2 = 2^{m-1}$;
   b) each sequence in $\mathcal{S}_2$ is of period $2^m - 1$;
   c)
   $$\ell_{\min}(\mathcal{S}_2) \ge 2^{m/2-2} - \frac{1}{2} - \frac{3}{2^{m/2+2}};$$
   d)
   $$c_{\max}(\mathcal{S}_2) \le 6(2^{m/2}+1).$$

ii) Let m be a positive integer and d a prime satisfying $(d, 2^m-1) = 1$ and $d \le ((2^m-7)/2^{m/2+1}+1)/2$. Then there exists a family $\mathcal{S}_d$ of binary sequences such that
   a)
   $$\#\mathcal{S}_d = \frac{2^{md}-2^m}{d(2^m-1)};$$
   b) each sequence in $\mathcal{S}_d$ is of period $2^m - 1$;
   c)
   $$\ell_{\min}(\mathcal{S}_d) \ge \frac{2^m-3-(d-1)2^{m/2+1}}{d\times 2^{m/2+1}};$$
   d)
   $$c_{\max}(\mathcal{S}_d) \le (2d-1)2^{m/2+1}+6.$$

Proof: Note that

$$\frac{I_{2^m}(2)}{2^m-1} = 2^{m-1}.$$

Taking $d = 2$ gives the results from Theorem 4.3.

Note that

$$\frac{I_{2^m}(d)}{2^m-1} = \frac{2^{md}-2^m}{d(2^m-1)}$$

for a prime d. Taking $d = 2$ gives the results from Theorem 4.3.

V. Example Construction Over Elliptic Function Fields

We assume that q is even again in this section. First let us review some results on elliptic curves [1], [6], [7]. Let $F/\boldsymbol{F}_q$ be the function field of an elliptic curve defined over $\boldsymbol{F}_q$ with at least one rational place O. Then all rational places of F form a finite Abelian group. Let $\boldsymbol{P}_1(F)$ be the set of all rational places. We can take O as the zero element of $\boldsymbol{P}_1(F)$. The number of rational places of F is always between $q+1-2\sqrt{q}$ and $q+1+2\sqrt{q}$. Furthermore, for any $d \geq 1$, the number of places of degree d is determined by the number of rational places. More precisely, suppose that F has $q+1+t$ rational places, then the number $B_q(d, t)$ of places of degree d of F is determined by

$$B_q(d,t) = \frac{1}{d}\sum_{b|d}\mu\left(\frac{d}{b}\right)(q^b+1-\omega_1^b-\omega_2^b)$$

where ω_1, ω_2 are two roots of the quadratic equation $X^2+tX+q = 0$. In particular

$$B_q(2,t) = \frac{q^2+q-t-t^2}{2}$$

$$B_q(3,t) = \frac{q^3-q-3qt-t+t^3}{3}.$$

For a rational place $P \in \boldsymbol{P}_1(F)$, let $[i]P$ denote the rational place

$$\underbrace{P \oplus P \oplus \cdots \oplus P}_{i}$$

where $\oplus$ stands for the addition operation of the group $\boldsymbol{P}_1(F)$.

Lemma 5.1 (see [1, pp. 194 and 195]): Let $F/\boldsymbol{F}_q$ be the function field of an elliptic curve with at least one rational place O. Then for any rational place P of F, there exists a unique automorphism σ_P of $\mathrm{Aut}(F/\boldsymbol{F}_q)$ such that for any place Q of degree d, $\sigma_P(Q) + O - Q - [d]P$ is a principal divisor. In particular, σ_O is the identity, and $\sigma_P^i = \sigma_{[i]P}$ for all $i \in \boldsymbol{Z}$.

Remark 5.2: All rational places $\boldsymbol{P}_1(F)$ of F form a finite Abelian group that is isomorphic to the divisor class group of degree zero of F. If we take O as the zero element of the group and Q is a rational place, then

$$\sigma_P(Q) = P \oplus Q.$$

An elliptic curve is called cyclic if the rational places of its function field form a cyclic group.

Lemma 5.3 (see [6, Theorem 3]): Put $q = 2^m$. Let t be an integer satisfying one of the following three conditions:

i) t is an odd integer between $-2\sqrt{q} = -2^{m/2+1}$ and $2\sqrt{q} = 2^{m/2+1}$; or

ii) $t = 0$; or

iii) $t = \sqrt{q} = 2^{m/2}$ if m is even, and $t = \sqrt{2q} = 2^{(m+1)/2}$ if m is odd.

Then there exists a cyclic elliptic curve over $\boldsymbol{F}_q$ such that its function field has $1 + q + t$ rational places.

Lemma 5.4: Let F be the function field of a cyclic elliptic curve over $\boldsymbol{F}_q$. Let R be a generator of $\boldsymbol{P}_1(F)$ and Q a place of degree d of F. Suppose the order n of $\boldsymbol{P}_1(F)$ is prime to d. Then $\sigma_R^j(Q) = \sigma_R^{j+n}(Q)$ for all $j \in \boldsymbol{Z}$ and $\sigma_R^i(Q)$, $\sigma_R^{i+1}(Q)$, $\ldots$, $\sigma_R^{i+n}(Q)$ are pairwise distinct for any fixed $i \in \boldsymbol{Z}$.

Proof: For any $j \in \boldsymbol{Z}$

$$\sigma_R^{j+n}(Q) = \sigma_R^j(\sigma_R^n(Q)) = \sigma_R^j\left(\sigma_{[n]R}(Q)\right) = \sigma_R^j(Q).$$

In order to prove that $\sigma_R^i(Q)$, $\sigma_R^{i+1}(Q)$, $\ldots$, $\sigma_R^{i+n}(Q)$ are pairwise distinct for any fixed $i \in \boldsymbol{Z}$, we only need to show that $\sigma_R^l(Q) = Q$ only if $l \equiv 0 \,(\mathrm{mod})\, n$. Suppose $\sigma_R^l(Q) = Q$, i.e., $\sigma_{[l]R}(Q) = Q$. Then

$$\sigma_{[l]R}(Q) + O - Q - [d][l]R = O - [d \cdot l]R$$

is a principal divisor. Therefore, $d \cdot l \equiv 0 \pmod{n}$ since R is a generator of $\boldsymbol{P}_1(F)$, that is, $l \equiv 0 \pmod{n}$. The proof is complete.

Let F be the function field of a cyclic elliptic curve of order $n = q + 1 + t$, R a generator of $\boldsymbol{P}_1(F)$. Put $P_i = [i]R$ for all $i \in \boldsymbol{Z}$. For $d \geq 2$, let $\boldsymbol{P}_d(F)$ be the set of all places of degree d. Assume $(d, n) = 1$. According to Lemma 5.4, the action of $\langle \sigma_R \rangle$ on $\boldsymbol{P}_d(F)$ divides $\boldsymbol{P}_d(F)$ into $r = B_q(d, t)/n = B_d(q, t)/(q + 1 + t)$ equivalent classes. Each class contains n places of degree d. We choose only one place from each class. Thus, we obtain r places of degree d

$$Q_1, Q_2, \ldots, Q_r.$$

It is clear that for $1 \leq i \neq j \leq r$

$$Q_j \notin \{\sigma^s(Q_i) | s \in \boldsymbol{Z}\} = \left\{Q_i, \sigma(Q_i), \ldots, \sigma^{n-1}(Q_i)\right\}.$$

For each $1 \leq i \leq r$, as

$$\dim_{\boldsymbol{F}_q} \mathcal{L}(Q_i) = \deg(Q_i) + 1 - g(F) = d > 1$$

we can find an element

$$z_i \in \mathcal{L}(Q_i) - \boldsymbol{F}_q.$$

It is obvious that Q_i is the unique pole of z_i and $\nu_{Q_i}(z_i) = -1$. Consider the family of binary sequences

$$\mathcal{T}_d = \{\boldsymbol{a}_{z_i} | i = 1, 2, \ldots, r = B_q(d, t)/(q + 1 + t)\}$$

where

$$\boldsymbol{a}_{z_i} = \{\mathrm{Tr}(z_i(P_j))\}_{j=0}^{\infty} = \{\mathrm{Tr}(z_i([j]R))\}_{j=0}^{\infty}.$$

Theorem 5.5: Let t be an integer satisfying one of three conditions in Lemma 5.3. Let $2 \leq d \leq ((q + 1 + 2t - 2\sqrt{q})/4\sqrt{q}$ and $(d, q+1+t) = 1$. Let $\mathcal{T}_d$ be the family of binary sequences as constructed above. Then $\mathcal{T}_d$ is of size $B_q(d, t)/(q + 1 + t)$ and each sequence in $\mathcal{T}_d$ is of period $n = q + 1 + t$. Moreover

$$\ell_{\min}(\mathcal{T}_d) \geq \frac{q + 1 + 2t - 2(d + 1)\sqrt{q}}{2d\sqrt{q}}$$

$$c_{\max}(\mathcal{S}_d) \leq 2(2d + 1)\sqrt{q} + |t|.$$

Proof: By Lemma 5.3, there exists a cyclic elliptic curve with $q + 1 + t$ rational places. Let F be the function field of the curve. Employing exactly similar arguments as in the proof of Theorem 4.2 and the results of Proposition 3.1, Theorems 3.2 and 3.3, we can get our results.

We rewrite Theorem 5.5 into the following form by taking $q = 2^m$.

Theorem 5.6: Let $m \geq 3$ be an integer, let t be an integer satisfying one of three conditions in Lemma 5.3. Let

$$2 \leq d \leq \frac{2^m + 1 + 2t - 2^{m/2+1}}{2^{m/2+2}} \quad \text{and} \quad (d, 2^m + 1 + t) = 1.$$

Then there exists a family $\mathcal{T}_d$ of binary sequences such that

a) $\#T_d = \frac{B_{2^m}(d, t)}{2^m + 1 + t}$;

b) each sequence in $\mathcal{T}_d$ is of period $2^m + 1 + t$;

c)
$$\ell_{\min}(\mathcal{T}_d) \geq \frac{2^m + 1 + 2t - (d + 1)2^{m/2+1}}{d2^{m/2+1}};$$

d)
$$c_{\max}(\mathcal{T}_d) \leq (2d + 1)2^{m/2+1} + |t|.$$

Corollary 5.7:

i) Let $m \geq 8$ and let t satisfy conditions ii) or iii) in Lemma 5.3. Then there exists a family $\mathcal{T}_2$ of binary sequences such that

a) $\#\mathcal{T}_2 = (2^m - t)/2$;

b) each sequence in $\mathcal{T}_2$ is of period $2^m + 1 + t$;

c)
$$\ell_{\min}(\mathcal{T}_2) \geq 2^{m/2-2} - \frac{3}{2} - \frac{1 + 2t}{2^{m/2+2}};$$

d)
$$c_{\max}(\mathcal{T}_2) \leq 10 \cdot 2^{m/2} + |t|.$$

ii) Let $m \geq 9$ and let t satisfy one of three conditions in Lemma 5.3. In addition, suppose $(3, t+1+(-1)^m) = 1$. Then there exists a family $\mathcal{T}_3$ of binary sequences such that

a) $\#\mathcal{T}_3 = (2^{2m} - 2^m + t2^m + t^2 - t)/3$;

b) each sequence in $\mathcal{T}_3$ is of period $2^m + 1 + t$;

c)
$$\ell_{\min}(\mathcal{T}_3) \geq 2^{m/2-2} - 2 - \frac{1 + 2t}{2^{m/2+2}};$$

d)
$$c_{\max}(\mathcal{T}_3) \leq 14 \cdot 2^{m/2} + |t|.$$

Proof: Note the fact that

$$\frac{B_q(2, t)}{q + 1 - t} = \frac{q - t}{2} = \frac{2^m - t}{2}$$

and $q+t+1$ is an odd number. Taking $d=2$ in Theorem 5.6 gives the results of part i). Note the fact that

$$\frac{B_q(3,t)}{q+1-t} = \frac{q^2-q+qt+t^2-t}{3} = \frac{(2^{2m}-2^m+t2^m+t^2-t)}{3}$$

and $(3,\, q+1+t) = (3,\, t+1+(-1)^m)$. Taking $d=3$ in Theorem 5.6 gives the results of part ii).

REFERENCES

[1] M. Eichler, *Introduction to the Theory of Algebraic Numbers and Functions*. New York: Academic, 1951.

[2] G. Gong, T. Berson, and D. Stinson, "Elliptic curve pseudo-random sequence generators," in *Proc. 6th Annual Workshop on Selected Areas in Cryptography (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1999, vol. 1758, pp. 34–48.

[3] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. Pless and C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998.

[4] P. V. Kumar, T. Helleseth, and A. R. Calderbank, "An upper bound for Weil exponential sums over Galois rings and applications," *IEEE Trans. Inform. Theory*, vol. 41, pp. 456–468, Mar. 1995.

[5] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge Univ. Press, 1997.

[6] H.-G. Rück, "A note on elliptic curves over finite fields," *Math. Comp.*, vol. 49, pp. 301–304, 1987.

[7] J. H. Silverman, *The Arithmetic of Elliptic Curves*. New York: Springer-Verlag, 1986.

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

[9] C. P. Xing and K. Y. Lam, "Sequences with almost perfect linear complexity profiles and curves over finite fields," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1267–1270, May 1999.