Multisequences with large linear and $k$-error linear complexity from a tower of Artin–Schreier extensions of function fields

Hongxi Tong$^{a,b,*}$

$^a$ Department of Mathematics, Shanghai University, Shanghai, 200444, China
$^b$ State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China

A R T I C L E   I N F O

Article history:
Received 20 December 2011
Revised 8 May 2012
Accepted 9 May 2012
Available online 30 May 2012
Communicated by Arne Winterhof

MSC:
94A60
11T71
14G50
14H05

Keywords:
Artin–Schreier extensions of function fields
Automorphisms
$k$-Error (joint) linear complexity
(Joint) linear complexity

A B S T R A C T

In this paper, we construct multisequences with both large (joint) linear complexity and $k$-error (joint) linear complexity from a tower of Artin–Schreier extensions of function fields. Moreover, these sequences can be explicitly constructed.

© 2012 Elsevier Inc. All rights reserved.

1. Introduction

A keystream generated by a stream cipher should satisfy the condition that it should be very hard to replicate the entire keystream from a part of the keystream. So one is interested to know how
hard a sequence might be to replicate. Scholars studied several complexity measures for sequences. The linear complexity is the most popular complexity measure.

Let $F_q$ denote the finite field with cardinality $q$, where $q$ is a prime power, and $k$ be a positive integer. A periodic sequence $s = s_0s_1s_2\cdots$ of elements of $F_q$ is called a $k$th-order linear recurring sequence generated by a linear feedback shift register (LFSR, for short) of length $k$ over $F_q$. If the sequence $s = s_0s_1s_2\cdots$ satisfies the following condition.

There exist $\lambda_0, \lambda_1, \ldots, \lambda_{k-1} \in F_q$ such that

$$s_j = \lambda_{k-1}s_{j-1} + \lambda_{k-2}s_{j-2} + \cdots + \lambda_0s_{j-k}$$

for all $j \geq k$.

The smallest $k$ such that a periodic sequence $s$ is generated by a $k$th-order LFSR is called the linear complexity of $s$. A set of sequences $A$ is called a multisequence of dimension $m$ over $F_q$ if it contains $m$ periodic sequences over $F_q$. The (joint) linear complexity of $A$ is the smallest $k$ such that all $m$ sequences in $A$ can be generated by a fixed $k$th-order LFSR simultaneously.

In [2], Ding et al. proved the Massey’s conjecture on synthesizing of multidimensional sequences. After that, many researchers have studied both linear complexity of periodic multisequences and linear complexity profiles of non-periodic multisequences [1,3,8,12–14]. In [6,7,9,10], many scholars introduced and studied $k$-error (joint) linear complexity of multisequences.

For our purpose in this paper, we choose the following definition.

Let $A$ be a periodic multisequence of dimension $m$ and period $N$ over $F_q$. For an integer $k$ with $0 \leq k \leq mN$, the $k$-error (joint) linear complexity of $A$ is the smallest possible linear complexity for all multisequences of dimension $m$ and period $N$ obtained by changing $k$ or fewer terms altogether in their first period of length $N$ in all $m$ sequences and then continuing the changes periodically with period $N$.

In [5,13–15], authors constructed various types of sequences from algebraic function fields. Especially Xing and Ding constructed multisequences with large linear and $k$-error linear complexity from Hermitian function fields in [15]. In this paper, we construct multisequences with various periods and dimensions from a tower of Artin–Schreier extensions of function fields. Multisequences obtained from our methods have larger $k$-error linear complexity than the $k$-error linear complexity of the multisequences in [15].

The paper is organized as follows. In Section 2, we introduce the definition of the tower of Artin–Schreier extensions of function fields and some basic properties. In Section 3, several multisequences with various periods and dimensions are constructed. Moreover we show that these multisequences have good properties. In the last section, we make some conclusions.

2. Preliminaries

In [4], Garcia and Stichtenoth gave a tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vlăduţ bound. Voss and Høholdt obtained a sequence of codes attaining the Tsfasman–Vlăduţ–Zink bound from these function fields in [16]. The function fields of this tower are defined in the following way.

**Definition 2.1.** (See [4].) Let $F_1 := F_q^q(x_1)$ be the rational function field over $F_q^q$. For $n \geq 1$, set

$$F_{n+1} := F_n(z_{n+1}),$$

where $z_{n+1}$ satisfies the equation

$$z_n^q + z_{n+1} = x_n^{q+1},$$

with

$$x_n := z_n/x_{n-1} \in F_n \quad (\text{for } n \geq 2).$$
Note that $F_2$ is the Hermitian function field.
Before we list some properties of these function fields, we fix some notations.

$\mathbb{F}_{q^2}$ the finite field of cardinality $q^2$.
$F, F_1, F_2, F_3, \ldots$ algebraic function fields of one variable over $\mathbb{F}_{q^2}$.
$g_n = g(F_n)$ the genus of $F_n/\mathbb{F}_{q^2}$.
$\mathbb{P}(F_n)$ the set of places of $F_n/\mathbb{F}_{q^2}$.
$N_n = N(F_n)$ the number of places $P \in \mathbb{P}(F_n)$ of degree one.
$v_P$ the normalized discrete valuation associated with $P$.

There are some properties of function fields $F_i/\mathbb{F}_{q^2}$ (see [4,16]).

**Lemma 2.2.** (See [4].)

1) Suppose that a place $P \in \mathbb{P}(F_n)$ is a simple pole of $x_n$ in $F_n$. Then the extension $F_{n+1}/F_n$ has degree $[F_{n+1} : F_n] = q$ and $P$ is totally ramified in $F_{n+1}/F_n$. The place $P' \in \mathbb{P}(F_{n+1})$ lying above $P$ is a simple pole of $x_{n+1}$.

2) For all $n \geq 1$, $\mathbb{F}_{q^2}$ is algebraically closed in $F_n$, and the degree of the extension $F_n/F_1$ is $[F_n : F_1] = q^{n-1}$.

3) For all $n \geq 1$, there is a unique place $Q_n \in \mathbb{P}(F_n)$ which is a common zero of the functions $x_1, z_2, z_3, \ldots, z_n$. Its degree is $\deg(Q_n) = 1$. For $1 \leq k \leq n$, the place $Q_n$ is also a zero of $x_k$, and we have $v_{Q_n}(x_k) = q^{k-1}$.

In the extension $F_{n+1}/F_n$ the place $Q_n$ splits into $q$ places of $F_{n+1}$ of degree one (one of them being $Q_n$).

**Definition 2.3.** (See [4].)

1) For $n \geq 2$, let

$$S_0^{(n)} := \{ P \in \mathbb{P}(F_n) \mid P \cap F_{n-1} = Q_{n-1} \text{ and } P \neq Q_n \}.$$

2) For $1 \leq i \leq \lfloor \frac{n-2}{2} \rfloor$, let

$$S_i^{(n)} := \{ P \in \mathbb{P}(F_n) \mid P \cap F_{n-1} \in S_{i-1}^{(n-1)} \}.$$

3) Let $P_\infty \in \mathbb{P}(F_1)$ denote the pole of $x_1$ in $F_1$, put

$$S^{(1)} := \{ P_\infty \}$$

and

$$S^{(2)} := \{ P \in \mathbb{P}(F_2) \mid P \in S_0^{(2)} \text{ or } P \cap F_1 \in S^{(1)} \}.$$

i.e., $S^{(2)}$ contains all places of $F_2$ which are either a pole of $x_1$ or a common zero of $x_1$ and $z_2 - \alpha$, for some $\alpha \in \mathbb{F}_{q^2}^*$ satisfying $\alpha^q + \alpha = 0$.

4) For $n \geq 3$ and $n \equiv 1 \mod 2$, let

$$S^{(n)} := \{ P \in \mathbb{P}(F_n) \mid P \cap F_{n-1} \in S^{(n-1)} \},$$

and for $n \geq 4$ and $n \equiv 0 \mod 2$, put

$$S^{(n)} := \{ P \in \mathbb{P}(F_n) \mid P \cap F_{n-1} \in S^{(n-1)} \cup S_{\geq n/4}^{(n-1)} \}.$$
Proposition 2.4. (See [4].)

1) Let $0 \leq i \leq \lfloor \frac{n-3}{2} \rfloor$ and $P \in S_i^{(n)}$. Then the place $P$ is unramified in the extension $F_{n+1}/F_n$.
2) Let $P \in S_i^{(n)}$ with $0 \leq i \leq \lfloor \frac{n-2}{2} \rfloor$. Then $\nu_P(x_0) = -q^{n-2i-2}$.
3) For $P \in S_i^{(n)}$, $\nu_P(x_0) = -1$.

Theorem 2.5. (See [4].) The genus $g_n = g(F_n)$ is given by the following formula:

$$
g_n = \begin{cases} 
q^n + q^{n-1} - q \frac{n+1}{2} - 2q^{\frac{n+1}{2}} + 1, & \text{if } n \equiv 1 \mod 2, \\
q^n + q^{n-1} - \frac{1}{2}q^{n+1} - \frac{3}{2}q^n - q^{n-1} + 1, & \text{if } n \equiv 0 \mod 2.
\end{cases}
$$

There are three types of places of degree one in $\mathbb{P}(F_n)$.

(A) Let $P \in \mathbb{P}(F_1)$ be the zero of $x_1 - \alpha$, with $\alpha \in F_q^*$. Then the place $P$ splits completely in $F_n/F_1$; i.e., there are exactly $q^{n-1}$ places above $P$ in $\mathbb{P}(F_n)$, all of them having degree one.

(B) The places $P \in S^{(2)}$ have degree one, and they are totally ramified in $F_n/F_2$. Hence, above each of these places there is a unique place of $F_n$, and this place has degree one.

(C) The places $P \in S_i^{(n)} \cup \{Q_n\}$ are of degree one.

There are $(q^2 - 1)q^{n-1}$ places of type (A), $q$ places of type (B) and $q$ places of type (C).

Proposition 2.6. (See [4].) For all $n \geq 3$,

$$N(F_n) \geq (q^2 - 1)q^{n-1} + 2q.$$ 

In fact, when $q$ is odd,

$$N(F_n) = (q^2 - 1)q^{n-1} + 2q \quad (\text{for } n \geq 3),$$

when $q$ is even,

$$N(F_3) = (q^2 - 1)q^2 + 2q,$$
$$N(F_4) = (q^2 - 1)q^3 + q^2 + q,$$
$$N(F_n) = (q^2 - 1)q^{n-1} + 2q^2 \quad (\text{for } n \geq 5).$$

3. Constructions

3.1. Multisequences from $F_3$

Firstly, we consider $F_3/F_{q^2}$.

Lemma 3.1.

$$N(F_3) = (q^2 - 1)q^2 + 2q$$

and

$$g_3 = g(F_3) = q^3 - 2q + 1.$$
Lemma 3.3. (See [15].) Let \( y \) be a \( \mathbb{F}^*_{q^2} \) and \( \alpha \) be totally ramified in \( \sigma \). Then deg \( (\alpha) = 1 \). Put

\[
M := \{ P_{\alpha} \mid \alpha \in \mathbb{F}^*_{q^2}, (\beta, \gamma) \in M_\alpha \}.
\]

So \(|M| = (q^2 - 1)q^2\), and these places in \( M \) are of type (A).

Proposition 3.2. Let \( P_{0\alpha} \in S_0(2) \subseteq \sigma(2) \) denote the common zero of \( x_1 - \alpha, x_2 - \beta \) and \( x_3 - \gamma \). For \( \alpha \in \mathbb{F}^*_{q^2} \) and \( \alpha^q + \alpha = 0 \), we have

\[
S(3) = \left\{ Q_{0\alpha} \mid \alpha \in \mathbb{F}^*_{q^2} \text{ and } \alpha^q + \alpha = 0, \ Q_{0\alpha} \cap F_2 = P_{0\alpha} \right\} \cup \left\{ P_{3} \mid P_{3} \cap F_1 = P_{3} \right\},
\]

and

\[
v_{Q_{0\alpha}}(z_3) = -(q + 1), \quad v_{P_{3}}(z_3) = -(q + 1).
\]

Proof. From the definition of \( S(3) \) and Proposition 2.4 3), the places \( P \in S(2) \) have degree one, and they are totally ramified in \( F_3/F_2 \). So \( v_{P_{0\alpha}}(x_2) = -1 \), and \( v_{Q_{0\alpha}}(x_2) = -q \). \( v_{Q_{0\alpha}}(x_3) = -1 \). So

\[
v_{Q_{0\alpha}}(z_3) = v_{Q_{0\alpha}}(x_3) + v_{Q_{0\alpha}}(x_2) = -(q + 1).
\]

Similarly, we have \( v_{P_{3}}(z_3) = -(q + 1) \). \( \square \)

Before we construct multisecquences, we need a lemma (see [15]).

Lemma 3.3. (See [15].) Let \( y_1, y_2, \ldots, y_k \) be \( k \) elements of \( F \). Suppose there exist \( k \) distinct places \( P_1, P_2, \ldots, P_k \) of \( F \) such that \( v_{P_i}(y_j) < 0 \) if and only if \( i = j \) for all \( 1 \leq i, j \leq k \). Then \( y_1, y_2, \ldots, y_k \) are \( \mathbb{F}_{q^2} \)-linearly independent.

For \( a \in \mathbb{F}^*_{q^2} \), \( c \in \mathbb{F}_{q^2} \) and \( c^q + c = 0 \), we define

\[
\sigma_{a,c} : F_3 \rightarrow F_3,
\]

\[
\sigma_{a,c}(x_1) = ax_1,
\]

\[
\sigma_{a,c}(z_2) = a^{q+1}z_2,
\]

\[
\sigma_{a,c}(z_3) = a^{q+1}z_3 + c,
\]

\[
\sigma_{a,c}(\alpha) = \alpha, \quad \forall \alpha \in \mathbb{F}_{q^2}.
\]

Then \( \sigma_{a,c} \in \text{Aut}(F_3/\mathbb{F}_{q^2}). \)
There are some properties on automorphisms (see [11,15]).

Proposition 3.4. (See [11].) Let \( \sigma \in \text{Aut}(F/F_{q^2}) \), \( P \in \mathbb{P}(F) \) and \( f \in F \), then:

1) \( \sigma(P) \) is also a place of \( F \) with \( \deg(\sigma(P)) = \deg(P) \).
2) \( v_P(\sigma(f)) = v_P(f) \).
3) \( \sigma(f)(\sigma(P)) = f(P) \) if \( v_P(f) \geq 0 \).

Lemma 3.5. Let \( \epsilon \) denote a generator of \( F_{q^2} \).

1) \( \sigma_{\epsilon,0} \in \text{Aut}(F/F_{q^2}) \) and \( \text{ord}(\sigma_{\epsilon,0}) = q^2 - 1 \).
2) \( \sigma_{\epsilon,0}(P^{03}) = P^{03}, \sigma_{\epsilon,0}(P_{000}) = P_{000} \).
3) Let \( \beta \in F_{q^2}, \beta^q + \beta = 0 \),

\[ \{ \sigma_{\epsilon,0}(Q_{0\beta}), i = 0, 1, \ldots, q^2 - 2 \} = \{ Q_{0\alpha} | \alpha \in F_{q^2}^*, \alpha^q + \alpha = 0 \} \].

4) Let \( \gamma \in F_{q^2}, \gamma^q + \gamma = 0 \),

\[ \{ \sigma_{\epsilon,0}(P_{00\gamma}), i = 0, 1, \ldots, q^2 - 2 \} = \{ P_{00\delta} | \delta \in F_{q^2}^*, \delta^q + \delta = 0 \} \].

5) The action of \( \sigma_{\epsilon,0} \) on all rational places in \( M \) gives rise to \( q^2 \) orbits, and each of these orbits contains \( q^2 - 1 \) elements.

Proof. From the definition of \( \sigma_{\epsilon,0} \), 1) and 2) are obviously correct.

\[ \sigma_{\epsilon,0}(x_1) = x_1, \quad \sigma_{\epsilon,0}(z_3) = \epsilon^{q+1}z_3, \]
\[ \sigma_{\epsilon,0}(z_2 - \beta) = \epsilon^{q+1}z_2 - \beta = \epsilon^{q+1}\left(z_2 - \frac{\beta}{\epsilon^{q+1}}\right). \]

\( \epsilon \) is a generator of \( F_{q^2} \), then \( \epsilon^{q+1} \) is a generator of \( F_q \).

\[ \left( \frac{\beta}{\epsilon^{q+1}} \right)^q + \frac{\beta}{\epsilon^{q+1}} = \frac{1}{\epsilon^{q+1}}(\beta^q + \beta) = 0. \]

3) is proved. Similarly, we can prove 4).

For any rational place \( P_{\alpha\beta\gamma} \in M \), the places \( \sigma_{\epsilon,0}(P_{\alpha\beta\gamma}) \) are distinct for \( i = 0, 1, \ldots, q^2 - 2 \). So the action of \( \sigma_{\epsilon,0} \) on all rational places in \( M \) gives rise to \( q^2 \) orbits, each of these orbits contains \( q^2 - 1 \) elements. \( \Box \)

The automorphism group \( \sigma_{\epsilon,0} \) divides all rational places in \( M \) into \( q^2 \) orbits, and every orbit contains \( q^2 - 1 \) elements. Let us label the elements of these \( q^2 \) orbits

\[ \{ \sigma_{\epsilon,0}^j(R) : j = 0, 1, \ldots, q^2 - 2 \} \]

and

\[ \{ P_{ij} = \sigma_{\epsilon,0}^j(P_i) : j = 0, 1, \ldots, q^2 - 2 \} \]

for \( i = 1, 2, \ldots, q^2 - 1 \).
By the Riemann–Roch theorem, the dimension of \( \mathcal{L}((2g_3 - 1)P_{\infty}^{(3)}) \) is \( g_3 \) and the dimension of \( \mathcal{L}((2g_3 - 1)P_{\infty}^{(3)} + R) \) is \( g_3 + 1 \). Thus, there exists a function \( f \in \mathcal{L}((2g_3 - 1)P_{\infty}^{(3)} + R) \) such that \( (f)_\infty = R + rP_{\infty} \) for some \( r \leq 2g_3 - 1 = 2q^3 - 4q + 1 \). For each \( 1 \leq i \leq q^2 - 1 \), put
\[
a_i(f) := \{ f(\sigma_{\epsilon,0}^i(P_i)) \}_{j=0}^{\infty},
\]
and \( q^2 - 1 \) is a period of \( a_i(f) \).

The multisequence \( A := \{a_i(f)\}_{i=1}^{q^2-1} \) over \( \mathbb{F}_{q^2} \) is dimension \( q^2 - 1 \), and \( q^2 - 1 \) is a period of \( A \).

**Theorem 3.6.** Let \( q \geq 3 \). The linear complexity of \( A \) is \( q^2 - 1 \). The period of \( A \) is also \( q^2 - 1 \).

**Proof.** Suppose that the linear complexity of \( A \) is less than \( q^2 - 1 \). Let \( k \) be the linear complexity of \( A \). Then there exist \( k + 1 \) elements \( \lambda_0, \lambda_1, \ldots, \lambda_k \in \mathbb{F}_{q^2} \) with \( \lambda_k \neq 0 \) such that
\[
\sum_{j=0}^{k} \lambda_j f(\sigma_{\epsilon,0}^{i+j}(P_i)) = 0
\]
for all \( l \geq 0 \) and \( i = 1, 2, \ldots, q^2 - 1 \).

Eq. (1) can be written into
\[
\left( \sum_{j=0}^{k} \lambda_j \sigma_{\epsilon,0}^{-j}(f)(\sigma_{\epsilon,0}^i(P_i)) \right) = 0.
\] (2)

The following facts are obvious.

1) \( \sigma_{\epsilon,0}^{-j}(R) \) are distinct for \( j = 0, 1, \ldots, k \).
2) For \( 0 \leq j, t \leq k \), \( \sigma_{\epsilon,0}^{-j}(R) \) is a pole of \( \sigma_{\epsilon,0}^{-t}(f) \) if and only if \( j = t \).
3) Hence \( \sigma_{\epsilon,0}^{-j}(R) \) is a pole of \( \sum_{j=0}^{k} \lambda_j \sigma_{\epsilon,0}^{-j}(f) \).

So the function \( \sum_{j=0}^{k} \lambda_j \sigma_{\epsilon,0}^{-j}(f) \) is a nonzero element of \( \mathcal{L}((2g_3 - 1)P_{\infty}^{(3)} + \sigma_{\epsilon,0}^{-j}(R)) \). By (2), we know that the function \( \sum_{j=0}^{k} \lambda_j \sigma_{\epsilon,0}^{-j}(f) \) belongs to
\[
\mathcal{L}((2g_3 - 1)P_{\infty}^{(3)} + \sum_{j=0}^{k} \sigma_{\epsilon,0}^{-j}(R) - \sum_{i=1}^{q^2-1} \sum_{l=0}^{q^2-2} \sigma_{\epsilon,0}^{i+l}(P_i)).
\]

So
\[
\deg((2g_3 - 1)P_{\infty}^{(3)} + \sum_{j=0}^{k} \sigma_{\epsilon,0}^{-j}(R) - \sum_{i=1}^{q^2-1} \sum_{l=0}^{q^2-2} \sigma_{\epsilon,0}^{i+l}(P_i)) \geq 0,
\]
i.e.,
\[
(2g_3 - 1) + k + 1 = 2q^3 - 4q + 1 + k + 1 \geq (q^2 - 1)^2.
\]
This is impossible. The desired result follows from this contradiction. \( \square \)
Remark 3.7. If \( q^2 - 1 \geq 2q + 1 \), i.e., \( q \geq 3 \). A multisequence consisting of any \( 2q + 1 \) sequences in \( \mathcal{A} \) has linear complexity \( q^2 - 1 \) as well. For instance, we consider the multisequence \( \mathcal{A}_1 = \{a_1(f), \ldots, a_{2q+1}(f)\} \). Suppose that the linear complexity of \( \mathcal{A}_1 \) is \( k \). Then there exist \( k + 1 \) elements \( \lambda_0, \lambda_1, \ldots, \lambda_k \in \mathbb{F}_{q^2} \) with \( \lambda_k \neq 0 \) such that

\[
\sum_{j=0}^{k} \lambda_j f(\sigma_{e,0}^{j+l}(P_i)) = 0
\]

for all \( l \geq 0 \) and \( i = 1, \ldots, 2q + 1 \). By the same argument in the proof of Theorem 3.6, we can show that \( \sum_{j=0}^{k} \lambda_j \sigma_{e,0}^{-j}(f) \) is a nonzero element of

\[
\mathcal{L}\left( (2g_3 - 1)P_\infty + \sum_{j=0}^{k} \sigma_{e,0}^{-j}(R) - \sum_{i=1}^{2q+1} \sum_{l=0}^{q^2-2} \sigma_{e,0}^{j+l}(P_i) \right).
\]

Hence,

\[
(2g_3 - 1) + k + 1 = 2q^3 - 4q + 1 + k + 1 \geq (q^2 - 1)(2q + 1).
\]

This is impossible.

Theorem 3.8. Let \( q \geq 3 \).

1) The \( l \)-error linear complexity of \( \mathcal{A} \) is still \( q^2 - 1 \) for all \( l \leq q^2 - 2q - 2 \).
2) The \( l \)-error linear complexity of \( \mathcal{A} \) is at least \( q^2 - 2q + s - 3 + \left\lfloor \frac{s^2 - (2q + 2)s + 4q}{q^2 - s} \right\rfloor \) for all \( l \leq q^2 - 1 - s \) and \( 0 < s \leq 2q + 1 \).

Proof. 1) Let a multisequence \( \mathcal{A}_1 \) be obtained from \( \mathcal{A} \) by changing \( l \) positions in the first period of length \( q^2 - 1 \) and continuing the changes periodically. Put

\[
\mathcal{A}_1 \cap \mathcal{A} := \{a_i(f) \mid a_i(f) \in \mathcal{A}_1, a_i(f) \in \mathcal{A} \}.
\]

\( l \leq q^2 - q - 2 \), so \( |\mathcal{A}_1 \cap \mathcal{A}| \geq 2q + 1 \). The linear complexity of \( \mathcal{A}_1 \cap \mathcal{A} \) is \( q^2 - 1 \). 1) is proved.

2) Let a multisequence \( \mathcal{A}_2 \) be obtained from \( \mathcal{A} \) by changing exactly \( q^2 - 1 - s \) positions in the first period of length \( q^2 - 1 \) and continuing the changing periodically.

Suppose \( |\mathcal{A} \cap \mathcal{A}_2| = t_1, 2q + 1 > t_1 \geq s \), and \( t_2 \) sequences in \( \mathcal{A}_2 \) are obtained from those in \( \mathcal{A} \) by changing exactly one position in the first period of length \( q^2 - 1 \) and continuing the changing periodically. W.l.o.g., let \( \mathcal{A} \cap \mathcal{A}_2 = \{a_1(f), \ldots, a_t(f)\} \). For each of the other sequences \( a_{t_1+1}(f), \ldots, a_{t_1+t_2}(f) \), there is exactly one position changed in the first period.

Assume that \( f(\sigma_{e,0}^{j}(P_i)) \) is changed, where \( i = t_1 + 1, \ldots, t_1 + t_2 \). Suppose that the linear complexity of \( \mathcal{A}_2 \) is \( k \), and \( \sum_{j=0}^{k} \lambda_j T^j \in \mathbb{F}_{q^2}[T] \) generates \( \mathcal{A}_2 \) with \( \lambda_k \neq 0 \). So

\[
\sum_{j=0}^{k} \lambda_j f(\sigma_{e,0}^{j+l}(P_i)) = 0
\]

for all \( l \geq 0 \), \( i = 1, \ldots, t_1 \), and

\[
\sum_{j=0}^{k} \lambda_j f(\sigma_{e,0}^{j+l}(P_i)) = 0
\]

for all \( s_i + 1 \leq l \leq q^2 - 2 + s_i - k \) and \( i = t_1 + 1, \ldots, t_1 + t_2 \).
Similarly, we can obtain that \( \sum_{j=0}^{k} \lambda_j \sigma_{e,j}^t(f) \) is a nonzero function of

\[
\mathcal{L} \left( (2g_3 - 1) P^{(2)}_{\infty} + \sum_{j=0}^{k} \sigma_{e,j}^t(R) - \sum_{i=1}^{t_1} \sum_{l=0}^{q^2 - 2} \sigma_{e,0}^j(P_i) - \sum_{i=t_1+1}^{t_1+t_2} \sum_{l=s_1+1}^{q^2 - 2 + s_1 - k} \sigma_{e,0}^j(P_i) \right).
\]

The degree of the above divisor is nonnegative, i.e.,

\[
(2g_3 - 1) + k + 1 \geq t_1(q^2 - 1) + t_2(q^2 - 2 - k),
\]

\[
k \geq \frac{(t_1 + t_2)(q^2 - 1) - 2q^3 + 4q - 2 - t_2}{t_2 + 1},
\]

and

\[
2q + 1 > t_1 \geq s,
\]

\[
qu^2 - 1 - s \geq t_2 \geq q^2 - 1 - 2q - \left\lfloor \frac{q^2 - 1 - s}{2} \right\rfloor.
\]

\[
qu^2 - 1 \geq t_1 + t_2 \geq q^2 - 1 - \left\lfloor \frac{q^2 - 1 - s}{2} \right\rfloor.
\]

So \( k \geq q^2 - 2q + s - 3 + \lfloor \frac{s^2 - (2q + 2)s + 4q}{q^2 - 5} \rfloor \). 2) is proved. \( \Box \)

**Remark 3.9.** For a multisequence \( \mathcal{A} \), there are the \( k \)-error \( \mathbb{F}_{q^2} \)-linear complexity \( L^q_{q^2 - 1,k}(\mathcal{A}) \) and the \( \overline{k} \)-error joint linear complexity \( L^q_{q^2 - 1,\overline{k}}(\mathcal{A}) \), where \( \overline{k} = (k_1, \ldots, k_{q^2 - 1}) \in \mathbb{Z}^{q^2 - 1} \) [9].

1) Let \( k = t \), the \( t \)-error \( \mathbb{F}_{q^2} \)-linear complexity \( L^q_{q^2 - 1,t}(\mathcal{A}) \) is about \( \frac{q^2 - 1}{t} - 2q \).

2) Put

\[
K_i := |\{ j | k_j = i, k_j \in [k_1, \ldots, k_{q^2 - 1}] \}|, \quad i = 0, 1, \ldots, q^2 - 1,
\]

and \( \overline{k} = (k_1, \ldots, k_{q^2 - 1}) \in \mathbb{Z}^{q^2 - 1} \).

(1) \( K_0 \geq 2q + 1, L^q_{q^2 - 1,\overline{k}}(\mathcal{A}) = q^2 - 1 \).

(2) \( K_0 < 2q + 1, L^q_{q^2 - 1,\overline{k}}(\mathcal{A}) \) is about

\[
\max \left\{ \frac{(q^2 - 1)K_0 + \cdots + q^2 - 1 - K_t - 2q^2 + 4q - 2}{K_1 + \cdots + K_t + 1}, t = 1, \ldots, q^2 - 1 \right\}.
\]

Let \( c \in \mathbb{F}^{*}_{q^2} \) and \( c^d + c = 0, \sigma_1_c \in \text{Aut}(F_3/\mathbb{F}_{q^2}) \),

\[
\sigma_1_c(x_1) = x_1, \quad \sigma_1_c(z_2) = z_2, \quad \sigma_1_c(z_3) = z_3 + c.
\]

We have the following lemma.

**Lemma 3.10.**

1) \( \text{ord}(\sigma_1_c) = p, \) where \( p \) is the characteristic of \( \mathbb{F}_{q^2} \).

2) \( \sigma_1_c(Q_{0,\alpha}) = Q_{0,\alpha}, \sigma_1_c(Q_{\infty}^{(2)}) = P_{\infty}^{(2)} \).
3) The action of $\sigma_{1,c}$ on all rational places in $M_0$ gives rise to $q/p$ orbits, and each of these orbits contains $p$ elements.
4) The action of $\sigma_{1,c}$ on all rational places in $M$ gives rise to $(q^2 - 1)q^2/p$ orbits, and every orbit contains $p$ elements.

From Lemma 3.10, we can obtain $(q^2 - 1)q^2/p + q/p$ orbits, and every orbit contains $p$ elements.

Let us label the elements of the $(q^2 - 1)q^2/p + q/p$ orbits

$$\left\{ \sigma_{1,c}^j(R): j = 0, \ldots, p - 1 \right\}$$

and

$$\left\{ \sigma_{1,c}^j(P_i): j = 0, \ldots, p - 1 \right\}$$

for $i = 1, \ldots, (q^2 - 1)q^2/p + q/p - 1$. By the Riemann–Roch theorem, the dimension of $L((2g_3 - 1)P_{\infty}^{(3)})$ is $g_3$ and the dimension of $L((2g_3 - 1)P_{\infty}^{(3)} + R)$ is $g_3 + 1$. Thus, there exists a function $f \in L((2g_3 - 1)P_{\infty}^{(3)} + R)$ such that $(f)^{\infty} = R + rP_{\infty}^{(3)}$ for some $r \leq 2g_3 - 1 = 2q^3 - 4q + 1$. For each $1 \leq i \leq (q^2 - 1)q^2/p + q/p - 1$, put

$$b_i(f) := \left\{ f(\sigma_{1,c}^j(P_i)) \right\}_{j=0}^{\infty}.$$ 

$p$ is a period of $b_i(f)$.

The multisequence $B := \{b_i(f)\}_{i=1}^{q^2q^2+q-1}$ over $\mathbb{F}_{q^2}$ is dimension $(q^2 - 1)q^2 - 1$, and $p$ is a period of $B$.

**Theorem 3.11.**

1) Let $B' \subseteq B$, and

$$|B'| \geq \frac{2q^3 - 4q}{p} + 2.$$ 

The linear complexity of $B'$ is $p$.

2) Let $l \leq \frac{q^4 - 2q^3 - q^2 + 5q}{p} - 3$, the $l$-error linear complexity of $B$ is $p$.

**Proof.** 1) Assume the linear complexity $k$ of $B$ is less than $p$. Similarly in the proof of Theorem 3.6, we have

$$2q^3 - 4q + 2 + k \geq p|B'| = 2q^3 - 4q + 2p.$$ 

This is impossible.

2) As $l \leq \frac{q^4 - 2q^3 - q^2 + 5q}{p} - 3$,

$$\frac{q^4 - q^2 + q}{p} - 1 - l \geq \frac{2q^3 - 4q}{p} + 2.$$ 

2) is proved from 1).
3.2. Multisequences from $F_n$ ($n \geq 4$)

Let $\theta \in F_{q^2}^*$ and $c \in F_{q^2}$, $c^q + c = 0$.

$$
\tau_{\theta,c} : F_n \to F_n
$$

$$
\tau_{\theta,c}(x_1) = \theta x_1,
$$

$$
\tau_{\theta,c}(z_i) = \theta^{q^i+1}z_i, \quad 2 \leq i \leq n-1,
$$

$$
\tau_{\theta,c}(z_n) = \theta^{q^1+1}z_n + c.
$$

Then it is easily checked that $\tau_{\theta,c} \in \text{Aut}(F_n/F_{q^2})$.

The situation of the rational places of $F_{n}/F_{q^2}$ is complicated, especially, when $q$ is even. From Lemma 2.2 1) and 3), we know that there are a rational place $P_{\infty}^{(n)} \in \mathbb{P}(F_n)$ and a rational place $Q_n \in \mathbb{P}(F_n)$, where $P_{\infty}^{(n)}$ is the common pole of $x_1, z_2, \ldots, z_n$ and $Q_n$ is the common zero of $x_1, z_2, \ldots, z_n$.

Let $\alpha_1 \in F_{q^2}^*$, define

$$
M_{n\alpha_1} := \{(\alpha_2, \alpha_3, \ldots, \alpha_n) \mid \alpha_2^q + \alpha_2 = \alpha_1^{q+1}, \alpha_3^q + \alpha_3 = (\alpha_1^{-1}\alpha_2)^{q+1}, \ldots,
$$

$$
\alpha_n^q + \alpha_n = (\alpha_{n-2}^{-1}\alpha_{n-4}^{-1} \cdots \alpha_{n-3}^{-1})^{q+1}\}\},
$$

$$
M_n := \{M_{n\alpha_1} \mid \alpha_1 \in F_{q^2}^* \},
$$

$$
|M_n| = (q^2 - 1)q^{n-1}.
$$

Put

$$
M_{n0} := S_0^{(n)} \cup \{Q_n\} = \{P_0\ldots\delta \mid \delta^q + \delta = 0, \delta \in F_{q^2}\}.
$$

Then $|M_{n0}| = q$.

**Lemma 3.12.** Let $\epsilon$ denote a generator of $F_{q^2}$.

1) $\tau_{\epsilon,0} \in \text{Aut}(F_n/F_{q^2})$ and $\text{ord}(\tau_{\epsilon,0}) = q^2 - 1$.

2) $\tau_{\epsilon,0}(P_{\infty}^{(n)}) = P_{\infty}^{(n)}$ and $\tau_{\epsilon,0}(Q_n) = Q_n$.

3) The action of $\tau_{\epsilon,0}$ on all rational places in $M_n$ gives rise to $q^{n-1}$ orbits, and each of these orbits contains $q^2 - 1$ elements.

4) $S_0^{(n)} = (\tau_{\epsilon,0}(P_0\ldots\alpha))$, for some $\alpha \in F_{q^2}^*$, $\alpha^q + \alpha = 0$.

By Lemma 3.12 3), the automorphism group $\tau_{\epsilon,0}$ divides all rational places in $M_n$ into $q^{n-1}$ orbits and each of the orbits contains exactly $q^2 - 1$ elements. Let these $q^{n-1}$ orbits be

$$
\{\tau_{\epsilon,0}^j(R) \mid j = 0, 1, \ldots, q^2 - 2\}
$$

and

$$
\{\tau_{\epsilon,0}^j(P_i) \mid j = 0, 1, \ldots, q^2 - 2\}$$
for \( i = 1, 2, \ldots, q^{n-1} - 1 \). By the Riemann–Roch theorem, the dimension of \( \mathcal{L}((2g_n - 1)P_\infty^{(n)}) \) is \( g_n \) and the dimension of \( \mathcal{L}((2g_n - 1)P_\infty^{(n)} + R) \) is \( g_n + 1 \). So there exists a function \( f \in \mathcal{L}((2g_n - 1)P_\infty^{(n)} + R) \) such that \( (f)_{\infty} = K + rP_\infty^{(n)} \) for some \( r \leq 2g_n - 1 \). For each \( 1 \leq i \leq q^{n-1} - 1 \), put

\[
\epsilon_i(f) := \{ f\left( \tau_{i,0}^j(P_1) \right) \}_{j=0}^\infty.
\]

It is obviously that \( q^2 - 1 \) is a period of the above sequence. The multisequence \( C := \{ \epsilon_i(f) \}_{i=1}^{q^{n-1}-1} \) is a multisequence over \( \mathbb{F}_{q^2} \) of dimension \( q^{n-1} - 1 \), and \( q^2 - 1 \) is a period of \( C \).

**Theorem 3.13.** Let \( C' \subseteq C \). If

\[
|C'| \geq \left\lceil \frac{2g_n}{q^2 - 1} \right\rceil + 1
\]

then the linear complexity of \( C' \) is \( q^2 - 1 \). Especially, the linear complexity and the period of \( C \) are both equal to \( q^2 - 1 \).

**Proof.** The proof is similar to Theorem 3.6. We omit the details. \( \square \)

Let \( \alpha \in \mathbb{F}_{q^2}^* \) and \( \alpha^q + \alpha = 0 \). \( \tau_{1,\alpha} \in \text{Aut}(F_n/\mathbb{F}_{q^2}) \),

\[
\tau_{1,\alpha}(x_1) = x_1, \quad \tau_{1,\alpha}(z_i) = z_i \quad (\text{for } 2 \leq i \leq n - 1), \quad \tau_{1,\alpha}(z_n) = z_n + \alpha,
\]

and we have the following lemma.

**Lemma 3.14.**

1) \( \text{ord}(\tau_{1,\alpha}) = p \).
2) \( \tau_{1,\alpha}(P_\infty^{(n)}) = P_\infty^{(n)} \).
3) The action of \( \tau_{1,\alpha} \) on all rational places in \( M_{n0} \) gives rise to \( q/p \) orbits, and each of these orbits contains \( p \) elements.
4) The action of \( \tau_{1,\alpha} \) on all rational places in \( M_n \) gives rise to \( (q^2 - 1)q^{n-1}/p \) orbits, and every orbit contains \( p \) elements.

So we can obtain \( \frac{(q^2 - 1)q^{n-1} + q}{p} \) orbits, and every orbit contains \( p \) elements. Let us label these orbits

\[
\{\tau_{1,\alpha}^j(R): j = 0, \ldots, p - 1\}
\]

and

\[
\{\tau_{1,\alpha}^j(P_i): j = 0, \ldots, p - 1\}
\]

for \( i = 1, \ldots, (q^2 - 1)q^{n-1}/p + q/p - 1 \). By the Riemann–Roch theorem, the dimension of \( \mathcal{L}((2g_n - 1)P_\infty^{(n)}) \) is \( g_n \) and the dimension of \( \mathcal{L}((2g_n - 1)P_\infty^{(n)} + R) \) is \( g_n + 1 \). There exists a function \( f \in \mathcal{L}((2g_n - 1)P_\infty^{(n)} + R) \) such that \( (f)_{\infty} = R + rP_\infty^{(n)} \) for some \( r \leq 2g_n - 1 \). For each \( 1 \leq i \leq (q^2 - 1)q^{n-1}/p + q/p - 1 \), put

\[
d_i(f) := \{ f\left( \tau_{1,\alpha}^j(P_i) \right) \}_{j=0}^\infty.
\]

\( p \) is a period of \( d_i(f) \).
The multisequence

\[ D := \{ d_i(f) \}_{i=1}^{(q^2-1)q^{n+1}+1} / p - 1 \]

over \( \mathbb{F}_{q^2} \) is dimension \( \frac{(q^2-1)q^{n+1}+q}{p} - 1 \), and \( p \) is a period of \( D \).

**Theorem 3.15.** Let \( D' \subseteq D \), and

\[ |D'| \geq \left\lceil \frac{2g_n}{p} \right\rceil + 1. \]

Then the complexity of \( D' \) is \( p \). Especially, the linear complexity and the period of \( D \) are both equal to \( p \).

**4. Conclusion**

In this paper, we give a construction method of multisequences from a tower of Artin–Schreier extensions of function fields. Moreover we obtain some classes of multisequences over \( \mathbb{F}_{q^2} \) with both large linear complexity and large \( k \)-error linear complexity.

**References**


