Multi-sequences with Almost Perfect Linear Complexity Profile and Function Fields over Finite Fields

Chaoping Xing

Department of Mathematics, National University of Singapore,
2 Science Drive 2, Singapore 117543
E-mail: xingcp@math.nus.edu.sg
Received January 31, 2000

Sequences with almost perfect linear complexity profile defined by Niederreiter (1997, Lecture Notes in Computer Science, Vol. 304, pp. 37-51, Springer-Verlag, Berlin/New York) are quite important for stream ciphers. In this paper, we investigate multi-sequences with almost perfect linear complexity profile and obtain a construction of such multi-sequences by using function fields over finite fields. Some interesting examples from this construction are presented to illustrate our construction.

Key Words: multi-sequences; linear complexity profile; perfect sequences; function fields.

1. INTRODUCTION

For stream cipher, keystreams are pseudorandom sequences of elements of $\mathbb{F}_q$ that are used for encryption and decryption. The security of stream ciphers mainly depends on the quality of the keystream. A good keystream must possess satisfactory statistical randomness and complexity properties. One of the assessments of the quality of keystreams is the linear complexity that measures stages of linear recurring shift registers generating keystreams. We refer to [6] for background on stream ciphers.

Sequences with almost perfect linear complexity profile are of both theoretical interests and application importance. The existence results and constructions of sequences with almost perfect linear complexity profile have been discussed in [1–4, 8, 9]. On the other hand, no results on multi-sequences with almost perfect linear complexity profile are known, even no definitions of multi-sequences with almost perfect linear complexity profile are given. In this paper, we generalize Niederreiter's almost perfect sequences to almost perfect multi-sequences. Furthermore, based on function fields over finite fields, we present an interesting construction of perfect multi-sequences.

1 This research was supported by NUS Grant R-146-000-018-12.

0885-064X/00 $35.00
Copyright © 2000 by Academic Press
All rights of reproduction in any form reserved.
multi-sequences. This construction is a natural, but not obvious generalization of our construction for perfect sequences [8].

We first introduce some notations and definitions. Let $F_q$ be the finite field with $q$ elements, then a sequence $c = (c_1, c_2, ..., c_n)$ of elements of $F_q$ is called a $k$-th order linear feedback shift register sequence if there exist constants $\lambda_0, ..., \lambda_k \in F_q$ with $\lambda_k \neq 0$ such that

$$\lambda_k c_{i+k} + \cdots + \lambda_1 c_{i+1} + \lambda_0 c_i = 0 \quad (1)$$

for all $1 \leq i \leq n-k$. We also call the pair $(\sum_{i=0}^{k} \lambda_i T^i, k)$ a linear feedback shift register (LFSR) of order $k$ if $\lambda_k \neq 0$. We express Eq. (1) by saying that the LFSR $(\sum_{i=0}^{k} \lambda_i T^i, k)$ generates $c = (c_1, c_2, ..., c_n)$.

The zero sequence $0 = (0, ..., 0)$ is viewed as a shift register sequence of order 0.

**Definition 1.1.** The linear complexity of a sequence $c = (c_1, c_2, ..., c_n)$ of length $n$ is defined to be the least $k$ such that it is a $k$-th order shift register sequence.

It is trivial that the linear complexity of the zero sequence is equal to 0 and the linear complexity of a sequence of length $n$ is at most $n$.

We now consider multi-sequences $c_1, c_2, ..., c_m$ of dimension $m$ of length $n$. $C$ denotes the multi-sequences $\{c_i\}_{i=1}^{m}$ of length $n$.

**Definition 1.2.** The linear complexity of a multi-sequence set $C = \{c_i = (c_{i1}, c_{i2}, ..., c_{in})\}_{i=1}^{m}$ of length $n$ is defined to be the smallest order $k$ of LFSR $(f(T), k)$ generating all of sequences $c_i$ for $i = 1, 2, ..., m$.

For an LFSR $(f(T), k)$ and a multi-sequence set $C = \{c_i\}_{i=1}^{m}$ of length $n$, we simply say that $(f(T), k)$ generates $C$ if it generates each of the sequences $c_1, c_2, ..., c_m$.

All sequences we discussed above are of finite length. Now we turn to sequences of infinite length.

Consider multi-sequences of dimension $m \geq 1$,

$$a_1 = (a_{11}, a_{12}, a_{13}, ...) \in F_q^\infty$$

$$a_2 = (a_{21}, a_{22}, a_{23}, ...) \in F_q^\infty$$

$$\vdots$$

$$a_m = (a_{m1}, a_{m2}, a_{m3}, ...) \in F_q^\infty$$
and let $A$ be the multi-sequence set $\{a_i\}_{i=1}^m$. We also denote by $A_n$ the multi-sequences

$$\{(a_{i1}, a_{i2}, ..., a_{in})\}_{i=1}^m$$

of length $n$.

**Definition 1.3.** The linear complexity profile of a multi-sequence set $A = \{a_1, a_2, ..., a_m\}$ is defined by the sequence of integral numbers

$$\{\ell_n(A)\}_{n=1}^\infty,$$

where $\ell_n(A)$ denote the linear complexities of $A_n = \{(a_{i1}, a_{i2}, ..., a_{in})\}_{i=1}^m$ for all $n \geq 1$.

Analogous to a single sequence, we define almost perfect multi-sequences.

**Definition 1.4.** A multi-sequence set $A = \{a_1, a_2, ..., a_m\}$ is called almost perfect if

$$\ell_n(A) \geq \frac{m(n+1)}{m+1} + \mathcal{O}(1)$$

for all $n \geq 1$, where $\mathcal{O}(1)$ is a function independent of $n$.

Furthermore we can define $d$-perfect multi-sequences in a similar manner.

**Definition 1.5.** A multi-sequence set $A = \{a_1, a_2, ..., a_m\}$ is called $d$-perfect for a positive integer $d$ if

$$\ell_n(A) \geq \left\lceil \frac{m(n+1) - d}{m+1} \right\rceil$$

for all $n \geq 1$, where $\lceil v \rceil$ denotes the smallest integer bigger than or equal to the real number $v$. In particular, $A$ is called perfect if $A$ is an $m$-perfect sequence, i.e.,

$$\ell_n(A) \geq \left\lceil \frac{mn}{m+1} \right\rceil$$

for all $n \geq 1$.
Remark 1.6. (1) It can be seen in Sections 2 and 3 that our definitions of almost perfect and perfect multi-sequences are quite natural and consistent with Niederreiter and Rueppel’s definitions in case of $m = 1$.

(2) We will see in Remark 2.4 that if $A$ is a $d$-perfect multi-sequence set of dimension $m$, then $d$ is at least $m$.

This paper is organized as follows. In Section 2, we will prove an equivalent condition for perfect multi-sequences. Some background on function fields over finite fields will be introduced in Section 3 to meet the requirement for our construction of almost perfect multi-sequences. An interesting construction of almost perfect multi-sequences will be described in Section 4. In Section 5, we will present some examples of almost perfect binary and ternary multi-sequences to illustrate our construction in Section 4. Two open problems about multi-sequences are given in the last section.

2. PERFECT MULTI-SEQUENCES

For a multi-sequence set $A = \{a_i = (a_{i1}, a_{i2}, a_{i3}, \ldots)\}_{i=1}^m$, put

$$s_j = (a_{ij}, a_{ij}, \ldots, a_{ij})^T \in F_q^m$$

for all $j \geq 1$. Then we immediately have the following lemma from definitions.

**Lemma 2.1.** $(f(T) = \sum_{i=0}^k \lambda_i T^i, k)$ generates $A_n = \{(a_{i1}, a_{i2}, \ldots, a_{in})\}_{i=1}^m$ if and only if

$$\sum_{i=0}^k \lambda_i s_{i+u} = 0 \in F_q^m$$

for all $1 \leq u \leq n - k$, i.e.,

$$\begin{pmatrix}
    s_1 & s_2 & \cdots & s_{k+1} \\
    s_2 & s_3 & \cdots & s_{k+2} \\
    \vdots & \vdots & \cdots & \vdots \\
    s_{n-k} & s_{n-k+1} & \cdots & s_n
\end{pmatrix}
\begin{pmatrix}
    \lambda_0 \\
    \lambda_1 \\
    \vdots \\
    \lambda_k
\end{pmatrix}
= 0 \in F_q^{(n-k)m}.$$

In order to give an equivalent condition for perfect multi-sequences, we need another lemma.
Lemma 2.2. Let $A = \{ a_1, a_2, \ldots, a_m \}$ be a multi-sequence set. If

$$\ell_n(A) \geq \begin{bmatrix} nm \\ m+1 \end{bmatrix}$$

for all $n \geq 1$, then the rank of the matrix

$$S_{un} := \begin{pmatrix} s_1 & s_2 & \cdots & s_{um} \\ s_2 & s_3 & \cdots & s_{um+1} \\ \vdots & \vdots & \ddots & \vdots \\ s_u & s_{u+1} & \cdots & s_{um+u-1} \end{pmatrix} \in M_{um \times um}(F_q)$$

is equal to $u \cdot m$ for all $u \geq 1$, where $s_j$ is defined by (2).

Proof. Suppose that the rank of $S_{un}$ is less than $um$, i.e., there exists a non-zero solution $(\alpha_0, \alpha_1, \ldots, \alpha_{um-1}) \in F_q^{um}$ such that

$$\begin{pmatrix} s_1 & s_2 & \cdots & s_{um} \\ s_2 & s_3 & \cdots & s_{um+1} \\ \vdots & \vdots & \ddots & \vdots \\ s_u & s_{u+1} & \cdots & s_{um+u-1} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{um-1} \end{pmatrix} = 0 \in F_q^{um}.$$

Let $0 \leq r \leq um - 1$ be the integer satisfying $\alpha_r \neq 0$, $\alpha_{r+1} = \alpha_{r+2} = \cdots = \alpha_{um-1} = 0$. Then

$$\begin{pmatrix} s_1 & s_2 & \cdots & s_{um} \\ s_2 & s_3 & \cdots & s_{um+1} \\ \vdots & \vdots & \ddots & \vdots \\ s_u & s_{u+1} & \cdots & s_{um+u-1} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{um-1} \end{pmatrix} = 0 \in F_q^{um}.$$

Hence we obtain by Lemma 2.1 that

$$\ell_{r+1}(A) \leq r. \quad (3)$$

Write

$$r + u = w(m + 1) + 1$$
for some $w \geq 0$ and $0 \leq l \leq m$. Notice that $w \leq u - 1$ since $r + u \leq um - 1 + u = u(m + 1) - 1$. Therefore

$$\ell_{r + l}(A) \geq \left\lfloor \frac{(r + u) m}{m + 1} \right\rfloor = \left\lfloor \frac{(m + 1)nw + lm}{m + 1} \right\rfloor = mw + l + \left\lfloor \frac{-1}{m + 1} \right\rfloor = mw + l = r + w \geq r + 1.$$  

The above inequality contradicts to (3). This completes the proof.

We have the following result on perfect multi-sequences.

**Theorem 2.3.** A multi-sequence set $A = \{a_1, a_2, \ldots, a_m\}$ of dimension $m$ is perfect if and only if

$$\ell_n(A) = \left\lfloor \frac{mn}{m + 1} \right\rfloor$$

for all $n \geq 1$.

**Proof.** "$\Rightarrow"$ is trivial. We only need to prove "$\Leftarrow".$ It is obvious that $\ell_n(A) \leq n$ for all $n \geq 1$ since the LFSR $(T^n, n)$ generates every sequence of length $n$. On the other hand, we have

$$\ell_n(A) \geq \left\lfloor \frac{mn}{m + 1} \right\rfloor = n$$

for all $1 \leq n \leq m$. Therefore we obtain $\ell_n(A) = \left\lceil \frac{mn}{m + 1} \right\rceil$ for all $1 \leq n \leq m$.

We now assume that $n \geq m + 1$. Write

$$n = u(m + 1) + v, \quad u \geq 1, \quad 0 \leq v \leq m.$$  

Then we get

$$\ell_n(A) \geq \left\lfloor \frac{mn}{m + 1} \right\rfloor = \left\lfloor \frac{u(m + 1) + vm}{m + 1} \right\rfloor = mu + v.$$  

By Lemma 2.2, the vector

$$(s_{mu + v + 1}^T, s_{mu + v + 2}^T, \ldots, s_{mu + v + u}^T)^T \in F_q^{um}$$

for some $w \geq 0$ and $0 \leq l \leq m$. Notice that $w \leq u - 1$ since $r + u \leq um - 1 + u = u(m + 1) - 1$. Therefore

$$\ell_{r + l}(A) \geq \left\lfloor \frac{(r + u) m}{m + 1} \right\rfloor = \left\lfloor \frac{(m + 1)nw + lm}{m + 1} \right\rfloor = mw + l + \left\lfloor \frac{-1}{m + 1} \right\rfloor = mw + l = r + w \geq r + 1.$$  

The above inequality contradicts to (3). This completes the proof.

We have the following result on perfect multi-sequences.

**Theorem 2.3.** A multi-sequence set $A = \{a_1, a_2, \ldots, a_m\}$ of dimension $m$ is perfect if and only if

$$\ell_n(A) = \left\lfloor \frac{mn}{m + 1} \right\rfloor$$

for all $n \geq 1$.

**Proof.** "$\Rightarrow"$ is trivial. We only need to prove "$\Leftarrow".$ It is obvious that $\ell_n(A) \leq n$ for all $n \geq 1$ since the LFSR $(T^n, n)$ generates every sequence of length $n$. On the other hand, we have

$$\ell_n(A) \geq \left\lfloor \frac{mn}{m + 1} \right\rfloor = n$$

for all $1 \leq n \leq m$. Therefore we obtain $\ell_n(A) = \left\lceil \frac{mn}{m + 1} \right\rceil$ for all $1 \leq n \leq m$.

We now assume that $n \geq m + 1$. Write

$$n = u(m + 1) + v, \quad u \geq 1, \quad 0 \leq v \leq m.$$  

Then we get

$$\ell_n(A) \geq \left\lfloor \frac{mn}{m + 1} \right\rfloor = \left\lfloor \frac{u(m + 1) + vm}{m + 1} \right\rfloor = mu + v.$$  

By Lemma 2.2, the vector

$$(s_{mu + v + 1}^T, s_{mu + v + 2}^T, \ldots, s_{mu + v + u}^T)^T \in F_q^{um}$$
can be represented as an $\mathbb{F}_q$-linear combination of

$$
\begin{pmatrix}
  s_1 \\
  s_2 \\
  \vdots \\
  s_u \\
  s_{u+1} \\
  \vdots \\
  s_{um}
\end{pmatrix}
= 
\begin{pmatrix}
  b_{um+1} \\
  \vdots \\
  b_{um+u}
\end{pmatrix},
$$

i.e., there exist $\lambda_0, \lambda_1, \ldots, \lambda_{um-1} \in \mathbb{F}_q$ such that

$$
\begin{pmatrix}
  s_{um+v+1} \\
  s_{um+v+2} \\
  \vdots \\
  s_{um+v+u}
\end{pmatrix}
= 
\sum_{i=0}^{um-1} \lambda_i 
\begin{pmatrix}
  s_{i+1} \\
  \vdots \\
  s_{i+u}
\end{pmatrix}.
$$

Hence by Lemma 2.1, the LFSR

$$
(T_{um+v} - \sum_{i=0}^{um-1} \lambda_i T^i, mu + v)
$$
generates sequences $(a_{11}, a_{12}, \ldots, a_{1n}), (a_{21}, a_{22}, \ldots, a_{2n}), \ldots, (a_{m1}, a_{m2}, \ldots, a_{mn})$. This implies that

$$
\ell_d(A) = \ell_{um+1} + \ell(A) \leq mu + v. \quad (5)
$$

Combining (4) with (5) gives the desired result. The proof is complete.

**Remark 2.4.** We claim that $d$ is at least $m$ if there exists a $d$-perfect sequence $A$ of dimension $m$.

Suppose $d < m$, then

$$
\ell_d(A) \geq \frac{nm + m - d}{m + 1} > \frac{nm}{m + 1}
$$

for all $n \geq 1$. Hence according to Theorem 2.3,

$$
\ell_d(A) = \left\lfloor \frac{nm}{m + 1} \right\rfloor \quad (6)
$$
for all \( n \geq 1 \). On the other hand, we have

\[
/m+1(A) \geq \left\lfloor \frac{(m+1)m+m-d}{m+1} \right\rfloor = m+1. \tag{7}
\]

(6) contradicts (7).

3. BACKGROUND ON FUNCTION FIELDS

Let \( F \) be a global function field with the full constant field \( F_q \). For a place \( P \) of \( F \), \( v_P \) denotes the corresponding normal discrete valuation. The integral ring of \( P \) is

\[
\mathcal{O}_P = \{ z \in F | v_P(z) \geq 0 \}.
\]

This is a local ring with the maximal ideal

\[
\mathfrak{p}_P = \{ z \in \mathcal{O}_P | v_P(z) > 0 \}.
\]

The residue class field \( \mathcal{O}_P/\mathfrak{p}_P \), denoted by \( F_P \), is a finite extension of \( F_q \). Thus \( F_P \) is also a finite field. The degree \( [F_P : F_q] \) is called the degree of \( P \). It is denoted by \( \deg(P) \). For an element \( z \in \mathcal{O}_P \), we denote by \( z(P) \) the residue class \( \bar{z} \) of \( z \) in \( F_P = \mathcal{O}_P/\mathfrak{p}_P \).

For a divisor \( D = \sum P v_P P \), the degree of \( D \) is defined by \( \deg(D) = \sum m_P \deg(P) \). Let \( H = \sum n_P P \) be another divisor, we denote by \( D \lor H \) the divisor \( \sum \max\{m_P, n_P\} P \).

Let \( z \) be a non-zero element of \( F \), define the zero divisor of \( z \) by

\[
(z)_0 = \sum_{v_P(z) > 0} v_P(z) P
\]

and the pole divisor of \( z \) by

\[
(z)_\infty = -\sum_{v_P(z) < 0} v_P(z) P.
\]

Then \( (z)_0 \) and \( (z)_\infty \) are two effective divisors and \( \deg(z)_0 = \deg(z)_\infty \). The principal divisor of \( z \) is defined by

\[
\text{div}(z) = (z)_0 - (z)_\infty.
\]
Now assume that $Q$ is a place of $F$ of degree $m$, and $t$ is a local parameter of $Q$, i.e., $v_Q(t) = 1$ (such a local parameter always exists). Choose $m$ elements $x_1, x_2, \ldots, x_m \in \mathcal{O}_Q$ such that $x_1(Q), x_2(Q), \ldots, x_m(Q)$ form an $\mathbb{F}_q$-basis of $F_Q$. For an element $y \in \mathcal{O}_Q$, $y(Q)$ can be represented as an $\mathbb{F}_q$-linear combination of $x_1(Q), x_2(Q), \ldots, x_m(Q)$. Let $a_{10}, a_{20}, \ldots, a_{m0} \in \mathbb{F}_q$ satisfy

$$y(Q) = \sum_{i=1}^{m} a_{i0} x_i(Q).$$

The above equality is equivalent to

$$v_Q\left(y - \sum_{i=1}^{m} a_{i0} x_i\right) \geq 1.$$

Hence $(y - \sum_{i=1}^{m} a_{i0} x_i)/t \in \mathcal{O}_Q$. Let $a_{11}, a_{21}, \ldots, a_{m1} \in \mathbb{F}_q$ satisfy

$$\left(y - \sum_{i=1}^{m} a_{i0} x_i\right)(Q) = \sum_{i=1}^{m} a_{i1} x_i(Q),$$

i.e.,

$$v_Q\left(y - \sum_{i=1}^{m} a_{i0} x_i - \sum_{i=1}^{m} a_{i1} x_i\right) \geq 1.$$

This is equivalent to

$$v_Q\left(y - \sum_{i=1}^{m} a_{i0} x_i - \sum_{i=1}^{m} a_{i1} x_i\right) t \geq 2.$$

Hence $(y - \sum_{i=1}^{m} a_{i0} x_i - \sum_{i=1}^{m} a_{i1} x_i) t^2 \in \mathcal{O}_Q$.

By induction, we obtain a sequence of vectors $\{(a_{1j}, a_{2j}, \ldots, a_{mj})\}_{j=0}^{\infty}$ such that

$$v_Q\left(y - \sum_{j=0}^{\infty} \left(\sum_{i=1}^{m} a_{ij} x_i\right) t^j\right) \geq n + 1$$

for all $n \geq 0$. We express this fact by the formal series

$$y = \sum_{j=0}^{\infty} \left(\sum_{i=1}^{m} a_{ij} x_i\right) t^j. \tag{8}$$
The above series is called a local expansion of $y$ at $Q$. The coefficients of local expansion (8) will be used to construct our perfect multi-sequences in Section 4.

4. A CONSTRUCTION

Throughout this section, we have the following notations and assumptions.

- $F/F_q$: a global function field with the full constant field $F_q$.
- $Q$: a place of degree $m$ of $F$.
- $x_1, x_2, \ldots, x_m$: $m$ elements of $\mathcal{O}_Q$ satisfying that $x_i(Q), x_2(Q), \ldots, x_m(Q)$ form an $F_q$-basis of $F_Q$.
- $t$: a local parameter of $Q$ with $\deg(t) = m + 1$.
- $y$: an element of $\mathcal{O}_Q$ satisfying $y = \sum_{i=1}^{m} a_i x_i$.

Remark 4.1. The condition $\deg(t) = m + 1$ implies that $F$ is an $F_q(t)$-linear space of dimension $m + 1$ (see Theorem I.4.11 of [7]). Hence $x_1, x_2, \ldots, x_m$ generate a proper $F_q(t)$-linear subspace of $F$, i.e., $F - \bigoplus_{i=1}^{m} F_q(t)x_i$ is not empty.

Consider the local expansion of $y$ at $Q$ as in (8)

$$y = \sum_{j=0}^{\infty} \left( \sum_{i=1}^{m} a_i x_i \right) t^j.$$

Put

$$a_i(y) = (a_{i1}, a_{i2}, a_{i3}, \ldots) \in F_q^\infty$$

for any $1 \leq i \leq m$ and the multi-sequence set

$$A(y) = \{a_i(y)\}_{i=1}^{m}.$$  (9)

**Theorem 4.2.** Let $A(y) = \{a_i(y)\}_{i=1}^{m}$ be constructed as in (9). Then $A(y)$ is $d$-perfect, where $d = \deg((y)_x \cup (x_1)_x \cup (x_2)_x \cup \cdots \cup (x_m)_x)$. In particular, $\{a_i(y)\}_{i=1}^{m}$ are perfect multi-sequences if $d = m$. 
Proof. Denote by $x$ the vector $(x_1, x_2, ..., x_m) \in F^m$. For another vector $z = (z_1, z_2, ..., z_m)^T \in F^m$, we denote by $x \cdot z$ the inner product $\sum_{i=1}^m x_i z_i$. Then the local expansion of $y$ can be written into the form

$$y = \sum_{j=0}^{\infty} (x \cdot s_j) t^j,$$

where $s_j = (a_{ij}, a_{2j}, ..., a_{mj})^T$.

Suppose that an LFSR $(\sum_{i=0}^k \lambda_i t^i, k)$ with $\lambda_k \neq 0$ generates the multi-sequences of length $n$

$$A_n(y) = \{(a_{i1}, a_{i2}, ..., a_{im})\}_{i=1}^m,$$

i.e.,

$$\sum_{i=0}^k \lambda_i s_{i+u} = 0 \in F_q^m$$

for all $1 \leq u \leq n - k$ by Lemma 2.1.

Consider the function

$$L = (\lambda_0 t^k + \lambda_1 t^{k-1} + \cdots + \lambda_k) y - [\lambda_0(x \cdot s_0) + \lambda_1(x \cdot s_1) t + \cdots + (\lambda_0(x \cdot s_k) t^k)]$$

$$= \sum_{j=k+1}^{\infty} \lambda_0(x \cdot s_{j-k}) t^j + \sum_{j=k+1}^{\infty} \lambda_0(x \cdot s_{j-k+1}) t^j + \cdots + \sum_{j=k+1}^{\infty} \lambda_0(x \cdot s_{j-k}) t^j$$

$$= \sum_{j=k+1}^{\infty} \sum_{j=0}^{l} \lambda_i (x \cdot s_{j-k+l}) t^j = \sum_{j=0}^{\infty} x \cdot \left( \sum_{j=k+1}^{\infty} \lambda_{i+j-k-l} s_{j-k+l} \right) t^l$$

First of all, we can see $L \neq 0$ since $\lambda_k \neq 0$ and $y \notin \bigoplus_{i=1}^m F_q(t) x_i$. Considering the zero divisor of $L$ gives

$$\deg(L)_0 \geq v_q(L) \cdot \deg(Q) \geq (n+1) m.$$ (10)

Considering the pole divisor of $L$ gives

$$\deg(L)_\infty \leq \deg(t^k)_\infty + (y)_\infty \land (x_1)_\infty \land \cdots \land (x_m)_\infty \leq (m+1) k + d.$$ (11)
Combining (10) with (11) yields
\[(n + 1) m \leq \deg(L_0) = \deg(L_\omega) \leq (m + 1) k + d.\]
Hence
\[k \geq \frac{m(n + 1) - d}{m + 1}.\]
This implies
\[\ell_d(A(y)) \geq \frac{m(n + 1) - d}{m + 1}\]
for all \(n \geq 1\).

Since \(\ell_d(A(y))\) are integers, our result follows.

If \(d = m\), then \(\ell_d(A(y)) \geq (nm)/(m + 1)\) for all \(n \geq 1\). It follows from Theorem 2.3 and Remark 2.4 that \(\{a_i(y)\}_{i=1}^m\) are perfect multi-sequences.

**Remark 4.3.** Theorem 4.2 doesn’t mean that the multi-sequence set \(A(y)\) is not perfect for \(d > m\) (see examples of [1] for \(m = 1\)).

5. EXAMPLES

In this section, we explicitly compute several almost perfect multi-sequences over the binary and ternary fields. The function fields used to construct these examples are the rational and elliptic function fields.

**Example 5.1.** Binary multi-sequences of dimension \(m = 2\).

\(F = F_2(x)\) the rational function field over \(F_2\);
\(Q\) the unique zero of \(x^2 + x + 1\)
\(t = x(x^2 + x + 1)\) a local parameter of \(Q\).

Put \(y = x^2\) and \(x_1 = 1, x_2 = x\). Then \(x_1(Q), x_2(Q)\) are an \(F_2\)-basis of \(F_Q\)
and \(d = \deg ((y)_Q \vee (x_1)_Q \vee (x_2)_Q) = 2 = \deg (Q)\). The local expansion of \(y\) at \(Q\) is
\[y = (x_1 + x_2) + (x_1 + x_2) t + x_1 t^2 + (x_1 + x_2) t^3 + x_1 t^4 + x_1 t^6 + (x_1 + x_2) t^8 + \cdots.\]
Put
\[ a_1(y) = (1, 0, 1, 1, 0, 1, 0, 1, ...), \]
\[ a_2(y) = (1, 1, 1, 0, 0, 0, 1, ...). \]

By Theorem 4.2, \( a_1(y), a_2(y) \) are perfect multi-sequences of dimension 2.

**Example 5.2.** Binary multi-sequences of dimension \( m = 3 \).

\[ F = F_2(x) \] the rational function field over \( F_2 \);
\[ Q \] the unique zero of \( x^3 + x + 1 \);
\[ t = x(x^3 + x + 1) \] a local parameter of \( Q \).

Put, \( y = x^3 \) and \( x_1 = 1, x_2 = x, x_3 = x^3 \). Then \( x_1(Q), x_2(Q), x_3(Q) \) are an \( F_2 \)-basis of \( F_Q \) and \( d = \deg((y)_\infty) + \deg(x_1)_\infty + \deg(x_2)_\infty + \deg(x_3)_\infty = 3 = \deg(Q) \).

The local expansion of \( y \) at \( Q \) is
\[ y = x_1 + x_2 + x_3 t + x_1 x_2 + x_2 t^2 + x_3 t^3 \]
\[ + x_1 x_2 t^4 + x_1 t^5 + x_1 t^6 + \cdots. \]

Put
\[ a_1(y) = (1, 1, 1, 1, 1, 1, 0, 1, ...), \]
\[ a_2(y) = (0, 1, 0, 0, 0, 0, 0, 0, ...) \]
\[ a_3(y) = (1, 1, 0, 0, 0, 0, 1, ...). \]

By Theorem 4.2, \( a_1(y), a_2(y), a_3(y) \) are perfect multi-sequences of dimension 3.

**Example 5.3.** Ternary multi-sequences of dimension \( m = 2 \).

\[ F = F_3(x) \] the rational function field over \( F_3 \);
\[ Q \] the unique zero of \( x^2 + 1 \);
\[ t = x(x^2 + 1) \] a local parameter of \( Q \).

Put \( y = x^2 \) and \( x_1 = 1, x_2 = x \). Then \( x_1(Q), x_2(Q) \) are an \( F_3 \)-basis of \( F_Q \) and \( d = \deg((y)_\infty) + \deg(x_1)_\infty + \deg(x_2)_\infty = 2 = \deg(Q) \).

The local expansion of \( y \) at \( Q \) is
\[ y = 2x_1 + 2x_2 t + 2x_1 t^2 + x_2 t^3 + 2x_1 t^4 + 2x_1 t^6 + \cdots. \]
Put
\[ a_1(y) = (0, 2, 0, 2, 0, 2, 0, 0, ...), \]
\[ a_2(y) = (2, 0, 1, 0, 0, 0, 0, 0, ...). \]

By Theorem 4.2, \( a_1(y), a_2(y) \) are perfect multi-sequences of dimension 2.

**Example 5.4.** Binary 4-perfect multi-sequences of dimension \( m = 2 \).

\[ F = F_2(x, z) \quad \text{the elliptic function field over } F_2 \text{ defined by } z^2 + z = x^3 + 1; \]
\[ Q \quad \text{the unique common zero of } z \text{ and } x^3 + x + 1, \]
\[ t = z \quad \text{a local parameter of } Q. \]

Put \( y = x^2 \) and \( x_1 = 1, x_2 = x. \) Then \( x_1(Q), x_2(Q) \) are an \( F_2 \)-basis of \( F_Q \) and \( d = \deg((y)_Q \lor (x_1)_Q \lor (x_2)_Q) = 4. \) The local expansion of \( y \) at \( Q \) is
\[ y = x_1 + x_2 + x_1 t + x_1 t^2 + x_2 t^3 + 0 \cdot t^4 + \ldots. \]

Put
\[ a_1(y) = (0, 1, 0, 0, ...), \]
\[ a_2(y) = (1, 0, 1, 0, ...). \]

By Theorem 4.2, \( a_1(y), a_2(y) \) are 4-perfect multi-sequences of dimension 2.

6. TWO OPEN PROBLEMS

For sequences of dimension 1, it can be easily proven (see [3]) that a sequence \( a \) is \( d \)-perfect if and only if
\[ \left| \frac{n + 1 - d}{2} \right| \leq \ell_d(a) \leq \left| \frac{n + d}{2} \right| \]
for all \( n \geq 1. \)

A question is: do we have the similar result for \( d \)-perfect multi-sequences? Namely, for a \( d \)-perfect multi-sequence \( A \), do we have
\[ \left| \frac{mn + m - d}{m + 1} \right| \leq \ell_d(A) \leq \left| \frac{mn + d}{m + 1} \right| \]
for all \( n \geq 1? \)
Another natural question is what is the expected value of the linear complexity for a randomly and independently chosen multi-sequence set. The following result was conjectured by both H. Niederreiter and C. S. Ding.

**Conjecture.** For randomly and independently chosen sequences \( c_1, c_2, \ldots, c_m \) of length \( n \), the expected value of the linear complexity is around \( (mn)/(m+1) \).

**ACKNOWLEDGMENT**

The author gratefully acknowledges the helpful comments from one of the reviewers.

**REFERENCES**