# Multi-sequences with $d$-perfect property

Xiutao Feng, Quanlong Wang and Zongduo Dai

*State Key Laboratory of Information Security (Graduate School of Chinese Academy of Sciences), Beijing, 100039*

**Abstract**

Sequences with almost perfect linear complexity profile are defined by H. Niederreiter[4]. C.P. Xing and K.Y. Lam[5, 6] extended this concept from the case of single sequences to the case of multi-sequences and furthermore proposed the concept of $d$-perfect. In this paper, based on the technique of $m$-continued fractions due to Dai et al, we investigate the property of $d$-perfect multi-sequences and obtain the sufficient and necessary condition on $d$-perfect property. We show that multi-sequences with $d$-perfect property are not always strongly $d$-perfect. In particular, we give one example to disprove the conjecture on $d$-perfect property of multi-sequences proposed by C.P. Xing in [6].

*Key words:* multi-sequences, linear complexity profile, $d$-perfect, $m$-continued fraction

## 1 Introduction

Stream ciphers are based on pseudorandom key streams, i. e. specially on deterministically generated sequences of bits with acceptable of unpredictability[1, 2]. From the cryptographic viewpoint, a useful measure for unpredictability is the linear complexity profile (LCP) of pseudorandom sequences. Many researchers contrived to construct pseudorandom sequences whose LCP looks like the LCP of truly random sequences. H. Niederreiter[3, 4] introduced the concept of almost perfect linear complexity profile (PLCP). C.P. Xing and K.Y Lam[5, 6] extended the concept about almost PLCP from the case of single sequences to the case of multi-sequences and furthermore proposed

*Email address:* {fengxt, wangquanl}@mails.gscas.ac.cn, yangdai@public.bta.net.cn (Xiutao Feng, Quanlong Wang and Zongduo Dai).

[1] This work is partly supported by NSFC (Grant No. 60173016), and the National 973 Project (Grant No. 1999035804)

the concept of $d$-perfect. In this paper, based on the technique of $m$-continued fractions[7, 8], we investigate the property of $d$ perfect multi-sequences and obtain the sufficient and necessary condition on $d$-perfect property. We show that multi-sequences with $d$-perfect property are not always strongly $d$-perfect and illustrate this with one example.

This paper is organized as follows. In section 2, we list the preliminary knowledge including some known results about $d$-perfect multi-sequences and $m$-continued fractions. In section 3, we discuss $d$-perfect multi-sequences and get the main results. In section 4, further we disprove the conjecture on $d$-perfect property of multi-sequences proposed by C.P. Xing with one counter-example.

## 2 Preliminary

### *2.1 d-Perfect Multi-sequences*

We first introduce some notations and definitions. Let $\mathbf{F}_q$ be an finite field with $q$ elements and $\underline{s} = \{s_1, s_2, \ldots, s_n, \ldots\}$ be a sequence of elements of $\mathbf{F}_q$. Its linear complexity of the length $n$ prefix is denoted by $L(n)$. H. Nierderreiter gave the following definition about PLCP.

**Definition 1** *A sequence $\underline{s} = \{s_1, s_2, \ldots, s_n, \ldots\}$ has perfect linear complexity profile if for all $n(\geq 1)$, s.t.*

$$L(n) = \lfloor \frac{n+1}{2} \rfloor \tag{1}$$

Consider a multi-sequence of dimension $m > 1$:

$$S = \{\underline{s}_1, \underline{s}_2, \ldots, \underline{s}_m\}$$

where $\underline{s}_k \in \mathbf{F}_q^\infty, 1 \leq k \leq m$. We yet denote by $L(n)$ its linear complexity of the length $n$ prefix. C.P. Xing and K.Y. Lam[5, 6] investigated multi-sequences with almost PLCP and further proposed the concepts of d-perfect and perfect.

**Definition 2** *A multi-sequence $S = \{\underline{s}_1, \underline{s}_2, \ldots, \underline{s}_m\}$ is called d-perfect for a positive integer $d$ if*

$$L(n) \geq \frac{m(n+1) - d}{m+1} \tag{2}$$

*for all $n \geq 1$. In particular, $S$ is called perfect if $S$ is an $m$-perfect sequence.*

In [6], C.P. Xing got the following theorem and proposed two conjectures , one of which is about $d$-perfect property of multi-sequences.

**Theorem 1** *[6] A multi-sequence* $S = \{\underline{s}_1, \underline{s}_2, \ldots, \underline{s}_m\}$ *is perfect if and only if*

$$L(n) = \lceil \frac{mn}{m+1} \rceil \tag{3}$$

*for all* $n \geq 1$.

**Conjecture 1** *[6] If a multi-sequence* $S = \{\underline{s}_1, \underline{s}_2, \ldots, \underline{s}_m\}$ *is d-perfect, then*

$$\frac{m(n+1)-d}{m+1} \leq L(n) \leq \frac{mn+d}{m+1} \tag{4}$$

*for all* $n \geq 1$.

**Definition 3** *A multi-sequence* $S$ *is called strongly d-perfect if (4) holds.*

Obviously, if a multi-sequence $S$ is strongly $d$-perfect, it must be $d$-perfect.

### *2.2 m-Continued Fractions*

Denote by $C$ a sequence $[\underline{a}_0, h_1, \underline{a}_1, h_2, \underline{a}_2, \cdots, h_k, \underline{a}_k, \cdots]$, where $1 \leq k < w$, $w$ is a positive integer or $\infty$, $h_k$ is a positive integer and $1 \leq h_k \leq m$ , $\underline{a}_k = (a_{k,1}, a_{k,2}, \ldots, a_{k,m}) \in \mathbf{F}_q[x]^m$ and $\underline{a}_0 = \mathbf{0}$. We call $w$ the length of $C$. In the case when $w < \infty$, then $C = [\underline{a}_0, h_1, \underline{a}_1, h_2, \underline{a}_2, \cdots, h_{w-1}, \underline{a}_{w-1}]$. We always associate it with the following quantities(for each $1 \leq k < w$):

$$t_k = \deg(a_{k,h_k})$$

$$d_k = \textstyle\sum_{1\leq i\leq k} t_i,\ d_0 = 0$$

$$v_{k,j} = \textstyle\sum_{i\leq k, h_i=j} t_i,\ v_{0,j} = 0,\ v_k = v_{k,h_k}$$

$$n_k = d_{k-1} + v_k,\ n_0 = 0$$

**Definition 4** *[8] A sequence* $C$ *defined as above is called an m-continued fraction if it satisfies:*

*(1)* $t_k \geq 1, \quad 1 \leq k < w$;
*(2) if* $h_k < h_{k+1}$, *then* $v_{k-1,h_k} \leq v_{k+1}$; *if* $h_k > h_{k+1}$, *then* $v_{k-1,h_k} \leq v_{k+1} - 1$, *where* $1 \leq k < w-1$;
*(3) for* $k(1 \leq k < w)$ *and* $j(1 \leq j \leq m, j \neq h_k)$, *if* $h_k < j$, *then* $\deg(a_{k,j}) \leq v_{k,j} - v_{k-1,h_k}$; *if* $h_k > j$, *then* $\deg(a_{k,j}) \leq v_{k,j} - v_{k-1,h_k} - 1$.

**Remmark 1** *In fact, the conditions 1 and 2 are essential. This is because: Given $h_k$ and $t_k$, which satisfy conditions 1 and 2 for all $k \geq 1$, we can always construct an $m$-continued fraction $C$ such that $C$ also satisfies condition 3, e.g. $a_{k,j} = 0$ for $j(j \neq h_k)$, and $a_{k,h_k}$ is a polynomial with degree $t_k$ over $\mathbf{F}_q[x]$.*

For an $m$-continued fraction $C$, a map $\varphi$ from $m$-continued fractions to multi-sequences is defined in [8]. We denote by $\varphi(C)$ its image and call $C$ an $m$-continued fraction expansion of $\varphi(C)$. And given a multi-sequence $S = \{\underline{s}_1, \underline{s}_2, \ldots, \underline{s}_m\}$, we denote by $\mathcal{C}(S)$ the set of all $m$-continued fraction expansions of $S$. [8] indicates that $\mathcal{C}(S)$ is nonempty and can be got by an algorithm called *m-CF transform*(for details, refer to [8]).

**Lemma 1** *[8] For a multi-sequence $S$, let $C \in \mathcal{C}(S)$, then $L(n) = d_k$, where $n_k \leq n < n_{k+1}$ and $k \geq 1$.*

Therefore, we can immediately get the conclusion as below:

**Propisition 1** *For a multi-sequence $S$, let $C \in \mathcal{C}(S)$, we have*

*(1) $S$ is d-perfect if and only if for all $k \geq 0$, s.t.*

$$\frac{mn_{k+1} - d}{m+1} \leq d_k$$

*(2) $S$ is strongly d-perfect if and only if for all $k \geq 0$, s.t.*

$$\frac{mn_{k+1} - d}{m+1} \leq d_k \leq \frac{mn_k + d}{m+1}$$

<u>Proof</u> Here we only prove item 2) and item 1) can be got directly from the procedure proving item 2).
$\Rightarrow$. Considering a given multi-sequence $S$, we check easily that Lemma 1 is also correct when $k = 0$. For an integer $k \geq 0$, if $n_k < n_{k+1}$, then for an arbitrary integer $n$, s. t. $n_k \leq n < n_{k+1}$, by Lemma 1, we have $L(n) = d_k$. Hence we can get

$$d_k = L(n_{k+1} - 1) \geq \frac{m((n_{k+1} - 1) + 1) - d}{m+1} = \frac{mn_{k+1} - d}{m+1}$$

and

$$d_k = L(n_k) \leq \frac{mn_k + d}{m+1}$$

If $n_k = n_{k+1}$, let $K_0$ such that $n_k = n_{k+1} = \cdots = n_{K_0-1} < n_{K_0}$, similarly we have

$$d_k < d_{K_0-1} \leq \frac{mn_{K_0-1} + d}{m+1} = \frac{mn_k + d}{m+1}$$

and let $k_0$ such that $n_{k_0} < n_{k_0+1} = \cdots = n_k = n_{k+1}$, we have

$$d_k > d_{k_0} \geq \frac{mn_{k_0+1} - d}{m+1} = \frac{mn_{k+1} - d}{m+1}$$

$\Leftarrow$. For an arbitrary positive integer $n$, by Lemma 1, there exists an integer $k$, s. t. $n_k \leq n < n_{k+1}$ and $L(n) = d_k$. So

$$\frac{m(n+1) - d}{m+1} \leq \frac{m(n_{k+1}) - d}{m+1} \leq d_k \leq \frac{mn_k + d}{m+1} \leq \frac{mn + d}{m+1}$$

and we get the conclusion. $\square$

## 3 Multi-sequences with $d$-Perfect Property

We first introduce the following two useful notations before discussion:

- $l(k, j) = \max\{i | h_i = j,\ 1 \leq i \leq k\}$, if the $i$ doesn't exist, then $l(k, j) = 0$
- $L(k, j) = \min\{i | h_i = j, i \geq k\}$, if the $i$ doesn't exist, then $L(k, j) = 0$

**Definition 5** *Given an $m$-continued fraction $C$, let $J = \{j | L(k, j) > 0,$ for $\forall k \geq 1\}$ and $m' = |J|$. We call $m'$ the characteristic of $C$. $C$ is called non-degenerate if $m' = m$; otherwise, $C$ is called degenerate.*

**Definition 6** *An $m$-continued fraction $C$ is called bounded if there exists a constant $c$, such that: for all $k \geq 1$, $t_k \leq c$; otherwise, we say that it is boundless.*

Throughout this section, we denote by $c$ the bound of all $t_k (k \geq 1)$ if $C$ is bounded.

**Lemma 2** *For a multi-sequence $S$, let $C \in \mathcal{C}(S)$, then $S$ is $d$-perfect if and only if*

$$t_k + \sum_{1 \leq j \leq m} (v_k - v_{k,j}) \leq d \tag{5}$$

*for all $k \geq 1$.*

<u>Proof</u> Since $\sum_{1 \leq j \leq m} v_{k,j} = d_k$, we have

$$t_k + \sum_{1 \leq j \leq m} (v_k - v_{k,j}) = t_k + mv_k - d_k = t_k + m(n_k - d_{k-1}) - d_k = mn_k - (m+1)d_{k-1}$$

By Proposition 1, we can directly get the conclusion. $\square$

In order to evaluate $v_{k,j} - v_k$, we consider the sequence: $\{(j_i, k_i)\}_{0\le i\le\tau}$, which is defined iteratively as below: Initially set $j_0 = j$, and $k_0 = l(k, j_0)$. Assume $(j_i, k_i)$ is defined. If $j_i = h_k$, let $\tau = i$, the procedure stops; if $j_i \neq h_k$, let $j_{i+1} = h_{k_i+1}$, and $k_{i+1} = l(k, j_{i+1})$. It is clear that $j_i \neq j_s$ for $\forall s \neq i$, hence $\tau$ exists, and $\tau < m$.

**Lemma 3** *If the sequence $\{(j_i, k_i)\}_{0\le i\le\tau}$ is defined as above, then*

$$v_{k,j} - v_k \le t_{k_0} - t_k + \sum_{s=0}^{\tau-1} t_{k_s+1} \tag{6}$$

<u>Proof</u> By the condition 2 of $m$-continued fractions, we have $v_{k-1,h_k} \le v_{k+1}$. That is

$$v_k - v_{k,h_{k+1}} \le t_k + t_{k+1}$$

Notice that $h_{k_i+1} = j_{i+1} = h_{k_{i+1}}$, $v_{k,j_i} = v_{k_i}$ and $v_{k_{i+1}} = v_{k_{i+1}-1,j_{i+1}} + t_{k_{i+1}}$, we have

$$v_{k,j_i} - v_{k,j_{i+1}} = v_{k_i} - v_{k_{i+1}} = v_{k_i} - v_{k_{i+1}-1,j_{i+1}} - t_{k_{i+1}}.$$

By $k_i + 1 \le k_{i+1}$ and $v_k - v_{k,h_{k+1}} \le t_k + t_{k+1}$, we get

$$v_{k,j_i} - v_{k,j_{i+1}} = v_{k_i} - v_{k_{i+1}-1,h_{k_i+1}} - t_{k_{i+1}} \le v_{k_i} - v_{k_i,h_{k_i+1}} - t_{k_{i+1}} \le t_{k_i} + t_{k_i+1} - t_{k_{i+1}}$$

So

$$v_{k,j} - v_k = \sum_{s=0}^{\tau-1} (v_{k,j_s} - v_{k,j_{s+1}}) \le \sum_{s=0}^{\tau-1} (t_{k_s} + t_{k_s+1} - t_{k_{s+1}}) = t_{k_0} - t_k + \sum_{s=0}^{\tau-1} t_{k_s+1}$$

$\square$

**Lemma 4** *If an $m$-continued fraction $C$ is bounded and non-degenerate, then*

$$|v_k - v_{k,j}| \le mc \tag{7}$$

*for all $k \ge 1$ and $j(1 \le j \le m)$.*

<u>Proof</u> When $j = h_k$, it is obviously correct and we will consider the case of $j \neq h_k$. By lemma 3, for $k \ge 1$ and $j(1 \le j \le m, j \neq h_k)$, we have

$$v_{k,j} - v_k \le t_{k_0} - t_k + \sum_{s=0}^{\tau-1} t_{k_s+1} \le mc - t_k < mc$$

Similarly, set $K = L(k, j)$. Since $C$ is non-degenerate, $K > k$. Note that $v_{k,j} = v_{K-1,j} = v_K - t_K$, so

$$v_k - v_{k,j} = v_k - v_{K-1,j} \le v_{K,h_k} - v_K + t_K \le mc$$

Synthesize the above two aspects and we can get the desired result. $\square$

We can now establish the main result of this section which gives the sufficient and necessary condition on $d$-perfect property.

**Theorem 2** *For a multi-sequence $S$, let $C \in \mathcal{C}(S)$, then the following conditions are equivalent to each other:*

*(1) $S$ is $d$-perfect for some constant positive integer $d$;*
*(2) $C$ is bounded and non-degenerate;*
*(3) $S$ is strongly $d'$-perfect for some constant positive integer $d'$.*

Proof 1⇒2. We first prove that $C$ is bounded. For simplification, let $t_0 = 0$. In fact, we check easily that the inequality (5) is also correct when $k = 0$. For every $k(\geq 1)$ and $h(1 \leq h \leq m)$, note that $v_{l(k,h)} = v_{k,h}$ and $v_{l(k,h),j} \leq v_{k,j}(1 \leq j \leq m, j \neq h)$, by lemma 2, we have:

$$d \geq t_{l(k,h)} + \sum_{1\leq j\leq m} (v_{l(k,h)} - v_{l(k,h),j}) \geq t_{l(k,h)} + \sum_{1\leq j\leq m} (v_{k,h} - v_{k,j})$$

Add two sides of the above $m$ inequalities($h$ from 1 to $m$) together respectively and get:

$$md \geq \sum_{h=1}^{m} t_{l(k,h)} \geq t_k$$

so $t_k \leq md$ for every $k \geq 1$. Secondly, if $C$ is degenerate, let $m'$ and $J$ be defined as definition 5, then $m' < m$. Consider sufficient large $k$'s, i.e. $k \gg k_0 = \min\{n | L(n, j) = 0,\ j \notin J\}$, and we have

$$\begin{aligned} d &\geq t_k + \sum_{1\leq j\leq m} (v_k - v_{k,j}) = t_k + \sum_{j\in J} (v_k - v_{k,j}) + \sum_{j\notin J} (v_k - v_{k,j}) \\ &= t_k + \sum_{j\in J} (v_k - v_{k,j}) + (m - m')v_k - \sum_{j\notin J} v_{k_0,j} \end{aligned} \tag{8}$$

By Lemma 4, we have

$$|\sum_{j\in J} (v_k - v_{k,j})| \leq \sum_{j\in J} |v_{k,j} - v_k| \leq (m' - 1)mc$$

Therefore only one term $(m - m')v_k$ in the right side of (8) is infinite. A contradiction.

2⇒3. By Lemma 4, we have

$$|d_k - mv_k| = |\sum_{1\leq j\leq m, j\neq h_k} (v_{k,j} - v_k)| \leq \sum_{1\leq j\leq m, j\neq h_k} |v_{k,j} - v_k| \leq (m - 1)mc$$

set $d' = m^2c$, then

$$mn_{k+1} - (m + 1)d_k = m(d_k + v_{k+1}) - (m + 1)d_k$$

$$
\begin{aligned}
&= mv_{k+1} - d_k = t_{k+1} + (mv_{k+1} - d_{k+1}) \\
&\le c + m(m-1)c < d' \qquad (9)
\end{aligned}
$$

and

$$
\begin{aligned}
(m+1)d_k - mn_k &= (m+1)d_k - m(d_k + v_k - t_k) \\
&= mt_k + (d_k - mv_k) \\
&\le mc + m(m-1)c \le d' \qquad (10)
\end{aligned}
$$

Synthesize the above two inequalities and get that $S$ is strongly $d'$-perfect.
3⇒1. Let $d = d'$ and $S$ is obviously $d$-perfect. □

**Remmark 2** *Though the fact that a multi-sequence $S$ is $d$-perfect implies that there exists a constant $d'$ such that $S$ is strongly $d'$-perfect, $d'$ isn't usually equal to $d$.*

In particular, for perfect multi-sequences, we have:

**Theorem 3** *For a multi-sequence $S$, let $C \in \mathcal{C}(S)$, $S$ is perfect if and only if*

*(1) for all $k \ge 1$, $t_k = 1$, and*
*(2) for $\forall t \ge 0$, $h_{tm+1}, h_{tm+2}, \cdots, h_{tm+m}$ is pairwisely unequal.*

Proof ⇒. Firstly, we prove that it is correct for $1 \le k \le m$ and $t = 0$. When $k = 1$, $mt_1 \le d = m$, so $t_1 = 1$. Suppose that when $k \le k_0(k_0 < m)$, $t_k = 1$ and $l(k-1, h_k) = 0$. If $l(k, h_{k+1}) > 0$, then

$$
\begin{aligned}
m &\ge t_{k+1} + \sum_{1 \le j \le m, j \ne h_{k+1}} (v_{k+1} - v_{k+1,j}) \\
&= t_{k+1} + (k-1)t_{k+1} + (m-k)(t_{k+1}+1) \\
&> mt_{k+1} \ge m
\end{aligned}
$$

This leads to a contradiction. So $l(k, h_{k+1}) = 0$ and

$$
t_{k+1} + \sum_{1 \le j \le m, j \ne h_{k+1}} (v_{k+1} - v_{k+1,j}) = mt_{k+1} - k + 1 \le m
$$

Therefore $t_{k+1} \le \frac{m+k-1}{m} < 2$, it implies that $t_{k+1} = 1$.

Secondly, the process with $k_0 m + 1 \le k \le k_0 m + m$ and $t = k_0(k_0 \ge 1)$ is as same as the process with $k_0 = 0$. It is because: for every $j(1 \le j \le m)$, we have $v_{k_0 m, j} = k_0$. So the partial of each $v_{k_0 m + i, j}$ before $k_0 m$ is vanished when it subtracts from others by formula (5) and it comes back to the state of $k_0 = 0$. Therefore we get the conclusion.
⇐. we can check inequations directly and get easily that $m$-continued fraction is perfect. □

**Remmark 3** *By theorem 3, we can get the conclusion that multi-sequences with PLCP are weak and easily predicable. It is a natural generalization of* *theorem 2 in [4, sec 4] from the case of single sequences to the case of multi-sequences.*

**Remmark 4** *By theorem 3, if* $n = n_{tm+j}(t \geq 0$ *and* $1 \leq j \leq m)$*, we have* $n = d_{tm+j} + v_{tm+j-1,h_{tm+j}} = tm + j + t$ *and* $L(n) = d_{tm+j} = tm + j$*. It directly leads to theorem 1.*

## 4 Counterexample

In this section, we give one example and show that multi-sequences which are $d$-perfect are not always strongly $d$-perfect. That is, the conjecture on $d$-perfect property of multi-sequences proposed by C.P. Xing is not correct.

**Example**: Let

$$C = [\underline{0}, h_1, \underline{a}_1, h_2, \underline{a}_2, \cdots, h_k, \underline{a}_k, \cdots]$$

where $\underline{a}_k = (a_{k,1}, a_{k,2}, \ldots, a_{k,m}) \in \mathbf{F}_q[x]^m$, $m \geq 2$, $a_{k,j} = \begin{cases} x^{t_k}, \ j = h_k \\ 0, \quad j \neq h_k \end{cases}$, $t_k = \begin{cases} 1, \ k = (2t+1)m \\ 3, \ k = (2t+2)m \\ 2, \text{ others} \end{cases}$ and $h_{tm+j} = j$, $t \geq 0$, $1 \leq j \leq m$.

We claim that $C$ is an $m$-continued fraction and let $S = \varphi(C)$, then $S$ is $d$-perfect but not strongly $d$-perfect, where $d = 2m+1$. This is because: Firstly, we check easily that $C$ is an $m$-continued fraction. In fact, for $t \geq 0, \ 1 \leq i, j < m$, we have $v_{tm+i,j} = \begin{cases} 2t, & i < j \\ 2(t+1), & i \geq j \end{cases}$ and $v_{k,m} = \begin{cases} 4t+1, & k = (2t+1)m \\ 4(t+1), & k = (2t+2)m \end{cases}$.

Then

$$v_{k+1} - v_{k-1,h_k} = \begin{cases} 1, \ k = (2t+1)m - 1 \\ 4, \ k = (2t+1)m \\ 5, \ k = (2t+2)m \\ 2, \text{ others} \end{cases}$$

So $v_{k+1} - v_{k-1,h_k} \geq 1$ and $C$ is an $m$-continued fraction. Secondly, we have

$$t_k + \sum_{1 \leq j \leq m} (v_k - v_{k,j}) = \begin{cases} 2(m-i+1), & k = (2t+1)m+i,\ 1 \leq i \leq m-1 \\ 2(m-i+1)+1, & k = (2t+2)m+i,\ 1 \leq i \leq m-1 \\ 2-m, & k = (2t+1)m \\ 0, & k = (2t+2)m \end{cases}$$

Hence we immediately get

$$t_k + \sum_{1 \leq j \leq m} (v_k - v_{k,j}) \leq 2m+1 = d$$

and by lemma 2, $S$ is $(2m+1)$-perfect. But when $k = (2t+2)m$, we have:

$$(m+1)d_k - mn_k = mt_k + \sum_{1 \leq j \leq m} (v_{k,j} - v_k) = 3m > 2m+1 = d$$

Therefore $S$ is not strongly $(2m+1)$-perfect.

## References


[1] R.A. Rueppel, Analysis and Design of Stream Cipher, Springer-Verlag, Berlin, 1986

[2] R. Lidl and H.Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, Cambridge, 1986

[3] H. Niederreiter, Continued fractions for formal power series, pseudorandom numbers, and linear complexity of sequences, Contributions to General Algebra 5(Proc. Salzburg.Conf, 1986), pp.221-233, Teubner, Stuttgart, 1987

[4] H. Niederreiter, Sequences with almost perfect linear complexity profile, Advances in Cryptology-EUROCRYPT' 87, Lecture Notes in Computer Science, Vol.304, pp.37-51, Springer-Verlag, 1988

[5] Chaoping Xing, and K.Y. Lam, Sequences with almost perfect linear complexity profiles and curves over finite fields, IEEE Transaction of Information Theorem 45(1999),1267-1270

[6] Chaoping Xing, Multi-sequences with Almost Perfect Linear Complexity Profile and Function Fields over Finite Fields, Journal of Complexity 16, 661-675, 2000

[7] H. Stark, An Introduction to Number Theory, Cambridge, Mass.: M.I.T. Press, 1979

[8] Zongduo Dai, Kunpeng Wang and Dingfeng Ye, Multidimensional Continued Fraction and Rational Approximation, http://arxiv.org/abs/math.NT /0401141, 2003