Linear Complexity Profiles and Continued Fractions

Muzhong Wang
Department of Electrical Engineering
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1

Abstract

The linear complexity, $\mathcal{L}(s^n)$, of a sequence s^n is defined as the length of the shortest linear feedback shift-register (LFSR) that can generate the sequence. The linear complexity profile, $L_{s^n} = L_1 L_2 \ldots L_n$, of s^n (where $L_i = \mathcal{L}(s^i)$, $1 \leq i \leq n$, denotes the linear complexity of first i digits of s^n) provides better insight into the complexity of an individual sequence. By the increment sequence $\Delta_{s^n} = \Delta_1 \Delta_2 \cdots \Delta_m$ in a linear complexity profile, $L_1 L_2 \cdots L_n$, we mean the subsequence of positive numbers in the sequence $L_1 (L_2 - L_1) \ldots (L_n - L_{n-1})$. For example, if $L_1 \cdots L_5 = 0\,2\,2\,2\,3$, its increment sequence is $\Delta_{s^5} = \Delta_1 \Delta_2 = 2\,1$. If we associate a sequence s^n over F with an element $S(z)$ in the field of Laurent series over F in the following way

$$s^n = s_1 s_2 \cdots s_n \iff S(z) = s_1 z^{-1} + s_2 z^{-2} + \cdots + s_n z^{-n},$$

$S(z)$ can then be written as

$$S(z) = a_0(z) + \cfrac{1}{a_1(z) + \cfrac{1}{a_2(z) + \ddots + \cfrac{1}{a_k(z)}}},$$

where $a_i(z) \in F[z]$, the ring of polynomials in z over F, for all $i \geq 0$. It will be shown that, for a sequence s^n, the increment sequence Δ_{s^n} of the linear complexity profile of s^n is as follows. (1) If $2 \cdot \sum_{i=1}^{k} \deg(a_i(z)) - \deg(a_k(z)) \leq n$, then $\Delta_{s^n} = \deg(a_1(z)) \deg(a_2(z)) \cdots \deg(a_k(z))$. (2) If $2 \cdot \sum_{i=1}^{k} \deg(a_i(z)) - \deg(a_k(z)) > n$, then $\Delta_{s^n} = \deg(a_1(z)) \deg(a_2(z)) \cdots \deg(a_{k'}(z))$, where $k' = \max\{j : 2 \cdot \sum_{i=1}^{j} \deg(a_i(z) - \deg(a_j(z)) \leq n\}$.

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 571-585, 1990.
© Springer-Verlag Berlin Heidelberg 1990

1 Introduction

It has long been known that there is some sort of connection between linear complexity concepts and continued-fraction theory Recently, H. Niederreiter has done lots of works on the problem [NIED 87] [NIED 88] [NIED 89]. If sequences are associated with the elements in the field of Laurent series, the linear complexity profile of a sequence is totally specified by the degrees of partial quotients in the continued-fraction expansion of the corresponding Laurent series [NIED 87]. We will prove that the sequence of "jumps" in the linear complexity profile of a sequence is equal to the sequence of degrees of partial quotients in the continued-fraction expansion of the corresponding Laurent series. Therefore, sequences with desired linear complexity profiles can be constructed by choosing the degrees of partial quotients in the continued-fraction expansion.

We first give a short introduction to continued-fraction expansions in the field of Laurent series (Laurent series field). A *Laurent series* in the indeterminate z over the field $\boldsymbol{F}$ is an expression of the form

$$f_l(z) = \sum_{j=-\infty}^{+\infty} a_j z^j$$

for which $a_j \in \boldsymbol{F}$, all j, and where $a_j = 0 \quad$ for $j > d$, where d is some integer. The *degree* of $f_l(z)$, denoted by $\deg f_l(z)$, is the largest j (if any) such that $a_j \neq 0$ and is, by way of convention, $-\infty$ when $a_j = 0$ for all j. For instance, the Laurent series $z+1+z^{-1}+z^{-2}+\ldots$ has degree 1 whereas the Laurent series $z^{-1}+z^{-2}+z^{-3}+\ldots$ has degree -1. Addition and multiplication of Laurent series is defined in the same way as for power series. The set of all Laurent series in z over the field $\boldsymbol{F}$ forms a field that we denote by $\boldsymbol{F}(z^{-1})$. A *polynominal* is a Laurent series for which $a_j = 0$ for all $j < 0$. Note that the ring of polynomials in z over $\boldsymbol{F}$, denoted by $\boldsymbol{F}[z]$, is a subring of the field $\boldsymbol{F}(z^{-1})$.

For a Laurent series $f_l(z)$, one defines its *valuation*, $\|f_l(z)\|$, by

$$f_l(z) = \begin{cases} 2^{\deg f_l(z)} & \text{if} \quad f_l(z) \neq 0 \\ 0 & \text{if} \quad f_l(z) = 0. \end{cases}$$

This is a *nonarchimedean valuation* because

$$\|f_l(z) + g_l(z)\| \leq \max\{\|f_l(z)\|, \|g_l(z)\|\},$$

which is stronger than the more usual "norm inequality" in which the right side is the sum of the two valuations.

For convenience, we summarize without proof some obvious properties of $\|.\|$.

Lemma **1** $\|.\|$ *has the following properties:*

P1. $\|f_l(z)\, g_l(z)\| = \|f_l(z)\|\ \|g_l(z)\|$.

P2. $\|f_l(z)\| \geq 0$ *with equality if and only if* $f_l(z) = 0$.

P3. $\|f_l(z) + g_l(z)\| \leq \max\{\|f_l(z)\|, \|g_l(z)\|\}$, *with equality if* $\|f_l(z)\| \neq \|g_l(z)\|$.

P4. $\|1\| = 1$.

P5. $\|f_l(z)^{-1}\| = \|f_l(z)\|^{-1}$.

P6. $\| - f_l(z)\| = \|f_l(z)\|$.

P7. If $f_l(z) \in \boldsymbol{F}[z]$ *and* $f_l(z) \neq 0$, *then* $\|f_l(z)\| \geq 1$.

Euclid's division theorem for polynomials can be restated in terms of $\|.\|$ as follows.

Theorem **1** **(Euclid's Division Theorem for Polynomials)** *If* $f(z)$ *and* $g(z)$ *are in* $\boldsymbol{F}[z]$ *with* $g(z) \neq 0$, *then there exists unique* $q(z)$ *and* $r(z)$ *in* $\boldsymbol{F}[z]$ *such that*

$$f(z) = q(z)g(z) + r(z) \qquad \text{and } \|r(z)\| < \|g(z)\|.$$

A *continued-fraction* in the indeterminate z over the field of $\boldsymbol{F}$ is an expression of the form

$$a_0(z) + \cfrac{1}{a_1(z) + \cfrac{1}{a_2(z) + \ddots + \cfrac{1}{a_i(z) + \ddots}}},$$

where $a_i(z) \in \boldsymbol{F}[z]$ for all $i \geq 0$ and either (1) $\deg a_i(z) \geq 1$ ($\|a_i(z)\| \geq 2$) for all $i \geq 1$ (in which case the continued-fraction is called to be *infinite*) or (2), for some positive integer N,

$\deg a_i(z) \geq 1$ for $1 \leq i \leq N$ and $a_i(z) = 0$ for all $i > N$ (in which case the continued-fraction is said to be *finite*). The polynomials $a_i(z)$ are called the *partial quotients* of the continued-fraction. There is a unique way in which the indicated divisions in a continued-fraction can be carried out to give a Laurent series, and we thus regard hereafter a continued-fraction as an element of $\boldsymbol{F}(z^{-1})$.

Given any continued-fraction, let $[a_0(z); a_1(z), \ldots, a_n(z)]$ denote the finite continued-fraction obtained by setting $a_i(z) = 0$ for all $i \geq n$, i.e., the finite continued-fraction

$$a_0(z) + \cfrac{1}{a_1(z) + \cfrac{1}{a_2(z) + \ddots + \cfrac{1}{a_i(z)}}}.$$

Every finite continued-fraction can, after clearing of denominators, be written as the ratio of two polynomials, i.e., as an element of $\boldsymbol{F}(z)$, the field of rational functions over $\boldsymbol{F}$. Thus one can write

$$[a_0(z); a_1(z), \cdots, a_n(z)] = \frac{p_n(z)}{q_n(z)}, \qquad n \geq 0,$$

where $p_n(z)$ and $q_n(z)$ are polynomials, defined recursively by

$$p_0(z) = a_0(z), \quad p_k(z) = a_k(z)p_{k-1}(z) + p_{k-2}(z) \quad (k \geq 1), \tag{1}$$

$$q_0(z) = 1, \quad q_k(z) = a_k(z)q_{k-1}(z) + q_{k-2}(z) \quad (k \geq 1) \tag{2}$$

where, by way of convention, $p_{-1}(z) = 1$ and $q_{-1}(z) = 0$. The rational function $\frac{p_n(z)}{q_n(z)}$ is called the n-th *convergent* of the continued-fraction $[a_0(z); a_1(z), \cdots, a_i(z), \ldots]$.

The following lemma is proved in [LID-NIE 83, pp.235–239].

Lemma 2 *The convergents of* $[a_0(z); a_1(z), \ldots, a_i(z), \ldots]$ *have the following properties:*

$$p_k(z)q_{k-1}(z) - p_{k-1}(z)q_k(z) = (-1)^{k-1} \quad (k \geq 1) \tag{3}$$

or, equivalently,

$$\frac{p_k(z)}{q_k(z)} - \frac{p_{k-1}(z)}{q_{k-1}} = \frac{(-1)^{k-1}}{q_k(z)q_{k-1}(z)} \quad (k \geq 1).$$

Equation (3) implies that

$$\gcd(p_i(z), q_i(z)) = 1 \qquad \text{for } i \geq 1. \tag{4}$$

The following property of convergents, which appears to be new, will play an important role in the sequel.

Lemma **3** *The denominator $q_n(z)$ of the n-th convergent to $[a_0(z); a_1(z), \ldots, a_i(z), \ldots]$ satisfies*

$$\|q_0(z)\| = 1, \tag{5}$$

$$\|q_n(z)\| = \prod_{j=1}^{n} \|a_j(z)\|, \quad n \geq 1 \tag{6}$$

provided $a_n(z) \neq 0$.

Proof. Because $q_0(z) = 1$, we have $\|q_0(z)\| = 1$ as claimed. Because

$$q_1(z) = a_1(z),$$

(6) holds trivially for $n = 1$.

Suppose that (6) holds for $1 \leq n \leq N$. Because $\|a_j(z)\| > 1$ for $1 \leq j \leq N$, $\|q_{N-1}(z)\|$ is strictly smaller than $\|q_N(z)\|$. Thus

$$\begin{aligned} \|q_{N+1}(z)\| &= \|a_{N+1}(z)q_N(z) + q_{N-1}(z)\| \\ &= \|a_{N+1}(z)q_N(z)\| \qquad \text{(P3 in Lemma 1)} \\ &= \|a_{N+1}(z)\| \cdot \|q_N(z)\| \qquad \text{(P1 in Lemma 1)} \\ &= \prod_{j=1}^{N+1} \|a_j(z)\|. \end{aligned}$$

This completes the proof by induction.

The following theorem, which is proved in [WES-SCH 79, theorem 2], shows the sense in which the n-th convergent is the best approximation to

$$[a_0(z); a_1(z), \ldots, a_i(z), \ldots] = S(z).$$

Theorem **2** *The convergents to* $[a_0(z); a_1(z), \ldots, a_i(z), \ldots]$ *have the property that, for every* n $(n \geq 0)$, *if* $q(z)$ *is a polynomial with* $\|q(z)\| < \|q_{n+1}(z)\|$, *then, for any polynomial* $p(z)$ *such that*

$$\frac{p(z)}{q(z)} \neq \frac{p_n(z)}{q_n(z)},$$

it must hold that

$$\|\frac{p_n(z)}{q_n(z)} - S(z)\| < \|\frac{p(z)}{q(z)} - S(z)\|.$$

Let $g_l(z)$ be an element in $\boldsymbol{F}(z^{-1})$. If also $g_l(z) \in \boldsymbol{F}(z)$, then

$$g_l(z) = \frac{r_{-2}(z)}{r_{-1}(z)},$$

where $r_{-2}(z)$ and $r_{-1}(z)$ are polynomials with $\|r_{-1}(z)\| \geq 1$. There exist unique polynomials $a_0(z)$ and $r_0(z)$ such that $r_{-2}(z) = a_0(z)r_{-1}(z) + r_0(z)$ and $\|r_0(z)\| < \|r_{-1}(z)\|$. Equivalently,

$$g_l(z) \;\; = \;\; a_0(z) + \frac{r_0(z)}{r_{-1}(z)}.$$

If $\|r_0(z)\| \neq 0$, then by the same argument there exist unique polynomials $a_1(z)$ and $r_1(z)$ such that

$$\frac{r_{-1}(z)}{r_0(z)} = a_1(z) + \frac{r_1(z)}{r_0(z)}$$

and $\|r_1(z)\| < \|r_0(z)\| < \|r_{-1}(z)\|$. Continuing in this manner, we must eventually reach the case $r_N(z) = 0$ because the degrees of $r_{-1}(z), r_0(z), r_1(z), \cdots$ are strictly decreasing. Thus it follows that we can always write a rational function $\frac{r_{-2}(z)}{r_{-1}(z)}$ as a finite continued-fraction

$$\frac{r_{-2}(z)}{r_{-1}(z)} = [a_0(z); a_1(z), \cdots, a_N(z)].$$

The converse statement that every finite continued-fraction $[a_0(z); a_1(z), \ldots, a_N(z)]$ represents an element of $\boldsymbol{F}(z)$ was noted previously.

Example.

$$\begin{aligned} r_{-2}(z) &= z^3 + z^2 + 1, \quad r_{-1}(z) = z^4, \\ a_0(z) &= 0, \\ r_0(z) &= z^3 + z^2 + 1, \\ a_1(z) &= z + 1, \quad r_1(z) = z^2 + z + 1, \end{aligned}$$

$$
\begin{aligned}
a_2(z) &= z, \quad r_2(z) = z+1, \\
a_3(z) &= z, \qquad r_3(z) = 1, \\
a_4(z) &= z+1, \quad r_4(z) = 0, \\
\frac{r_{-2}(z)}{r_{-1}(z)} &= \frac{z^3+z^2+1}{z^4} \\
&= \cfrac{1}{z+1+\cfrac{1}{z+\cfrac{1}{z+\cfrac{1}{z+1}}}} \\
&= [0; z+1, z, z, z+1].
\end{aligned}
$$

2 Relation between Linear Complexity Profile and Continued Fractions

The *linear complexity* $\mathcal{L}(s^n)$ of a sequence, $s^n = s_1 s_2 \cdots s_n$ where $s_1, s_2, \ldots, s_n$ are from a field $\boldsymbol{F}$, can also be defined as the smallest nonnegative integer L such that there exist $c_0, c_1, \cdots, c_L$ in $\boldsymbol{F}$ satisfying

$$c_L s_{i+L} + c_{L-1} s_{i+L-1} + \cdots + c_0 s_i = 0, \ 1 \le i \le n-L, \tag{7}$$

where $c_L \neq 0$. The monic polynomial $c_L^{-1}(c_L D^L + \ldots + c_1 D + c_0)$ is called a *characteristic polynomial* of the sequence; we remark that the characteristic polynomial is unique if and only if $L \le n/2$.

The *linear complexity profile* L_{s^n} is defined as the sequence

$$L_{s^n} = L_1 L_2 \cdots L_n$$

where $L_i = \mathcal{L}(s^i)$. The definition of linear complexity implies

$$L_i \ge L_j \quad \text{for } i > j. \tag{8}$$

We associate a sequence s^n over $\boldsymbol{F}$ with an element $S(z)$ in the field of Laurent series over $\boldsymbol{F}$ in the following way

$$s^n = s_1 s_2 \cdots s_n \iff S(z) = s_1 z^{-1} + s_2 z^{-2} + \cdots + s_n z^{-n}. \tag{9}$$

We see immediately that the sequence s^n and the sequence $s^{n+m} = s^n 0^m$ (where $s^n 0^m$ denotes the concatenation of s^n and 0^m) are associated with the same element $\sum_{i=1}^{n} s_i z^{-i}$ in the field of Laurent series. Therefore, we can implicitly expand $s^n = s_1 s_2, \cdots s_n$ to a semi-infinite sequence s^∞ by concatenating s^n with infinitely many zeroes,

$$s^\infty = s_1 s_2 \cdots s_n 000 \cdots .$$

Suppose that $S(z) = s_1 z^{-1} + s_2 z^{-2} + \cdots$ is a Laurent series with $\|S(z)\| < 1$. Letting $q(z) = c_L z^L + \cdots + c_1 z + c_0$, $c_L \neq 0$, we see that the left side of (7) is the coefficient of z^{-i} in the product $S(z)q(z)$. Thus, if (7) holds, there is a unique polynomial $p(z)$ such that $\|p(z) - S(z)q(z))\| < 2^{n+L}$ and hence (by P1 and P5) such that

$$\|\frac{p(z)}{q(z)} - S(z)\| < 2^{-n}. \tag{10}$$

Moreover, $\|p(z)\| < \|q(z)\| = 2^L$.

Conversely, if (10) holds where $q(z) = c_L z^L + \cdots + c_1 z + c_0$ and $p(z)$ are polynomials with $\|q(z)\| = 2^L$, then (7) also holds and $\|p(z)\| < \|q(z)\|$. We have thus proved the following lemma.

Lemma 4 The linear complexity of a sequence $s^n = s_1 s_2 \ldots s_n$ is equal to the minimum degree of polynomials $q(z)$ such that there exists a polynomial $p(z)$ satisfying

$$\|\frac{p(z)}{q(z)} - S(z)\| < 2^{-n},$$

where $S(z) = s_1 z^{-1} + s_2 z^{-2} + \cdots + s_n z^{-n}$. Moreover, $c_L^{-1} q(z)$ is a characteristic polynomial of s^n, where c_L is the leading coefficient of $q(z)$.

Because $S(z)$ is in $\boldsymbol{F}(z)$, $S(z)$ can be expressed as a finite continued-fraction

$$\begin{aligned} S(z) &= a_0(z) + \cfrac{1}{a_1(z) + \cfrac{1}{a_2(z) + \ddots + \cfrac{1}{a_N(z)}}} \\ &= [0; a_1(z), \cdots, a_N(z)] \end{aligned}$$

for some N (where the polynomial part vanishes because $\|S(z)\| < 1$). Notice that $a_0(z)$ is always zero.

The following theorem is proved in [NIED 87]. For readers' convenience, we give an alternative proof here.

Theorem 3 The linear complexity profile, L_{s^∞}, of the sequence s^∞ is totally specified by the degrees of the partial quotients in the continued-fraction expansion of $S(z)$, in the following way:

L1 if $\deg a_1(z) > 1$, $L_i = 0$, $1 \le i < \deg a_1(z)$;

L2 $L_i = \deg a_1(z)$, $\deg a_1(z) \le i < \deg a_2(z) + \deg a_1(z)$;

$L_i = \deg a_2(z) + \deg a_1(z)$, $\deg a_2(z) + 2\deg a_1(z) \le i < \deg a_3(z) + 2\sum_{i=1}^{2} \deg a_i(z)$;

$\vdots$

$L_i = \sum_{i=1}^{N-1} \deg a_i(z)$, $\deg a_{N-1}(z) + 2\sum_{i=1}^{N-2} \deg a_i(z) \le i < \deg a_N(z) + 2\sum_{i=1}^{N-1} \deg a_i(z)$;

$\vdots$.

Proof. L1 is obvious because $\deg a_1(z) > 1$ implies $s_1 = \ldots = s_{(\deg a_1(z)-1)} = 0$.

Consider the convergents

$$\frac{p_n(z)}{q_n(z)} = [0; a_1(z), a_2(z), \cdots, a_n(z)], \qquad n \ge 1.$$

We know from Lemma 2 and Lemma 3 that

$$\frac{p_{n+1}(z)}{q_{n+1}(z)} - \frac{p_n(z)}{q_n(z)} = \frac{(-1)^n}{q_{n+1}(z)p_{n+1}(z)}$$

and that $\xi_n = \deg[q_n(z)q_{n+1}(z)] = \deg a_{n+1}(z) + 2\sum_{i=1}^{n} \deg a_i(z)$. This implies that the coefficients of z^{-i} for $1 \le i < \xi_n$ in the Laurent series for $\frac{p_{n+1}(z)}{q_{n+1}(z)}$ and $\frac{p_n(z)}{q_n(z)}$ are the same but that the coefficients of z^{ξ_n} are different. Thus

$$\frac{p_n(z)}{q_n(z)} = s'_1 z^{-1} + \cdots + s'_{\xi_n - 1} z^{-(\xi_n - 1)} + s'_{\xi_n} z^{-\xi_n} + \cdots$$

where

$$\begin{aligned} s'_i &= s_i \qquad \text{for } 1 \le i \le \xi_n - 1, \text{ and} \\ s'_{\xi_n} &\neq s_{\xi_n}. \end{aligned}$$

We have then

$$\|\frac{p_n(z)}{q_n(z)} - S(z)\| = 2^{-\xi_n}. \tag{11}$$

According to Lemma 4,

$$\mathcal{L}(s_1 s_2 \cdots s_{\xi_n}) \ge \deg q_n(z). \tag{12}$$

By the same argument that gives (11), we have

$$\|\frac{p_{n+1}(z)}{q_{n+1}(z)} - S(z)\| = 2^{-\xi_{(n+1)}}. \tag{13}$$

Theorem 4 shows that there exists no polynomials $p(z)$ and $q(z)$ with $\|q(z)\| < \|q_{n+1}(z)\|$ such that

$$\|\frac{p(z)}{q(z)} - S(z)\| < \|\frac{p_n(z)}{q_n(z)} - S(z)\|.$$

That is to say, $q_{n+1}(z)$ is the polynomial with minimum degree such that (13) holds.

It now follows from Theorem 2, (12) and (13) that

$$\mathcal{L}(s_1 s_2 \ldots s_i) = \deg q_{n+1}(z) \text{ for } \xi_n \le i < \xi_{n+1}.$$

This proves L2.

By the *increment sequence* $\Delta_1 \Delta_2 \cdots \Delta_m$ in a linear complexity profile, $L_1 L_2 \cdots L_n$, we mean the subsequence of positive numbers in the sequence $L_1\,(L_2 - L_1) \ldots (L_n - L_{n-1})$. For example, if $L_1 \cdots L_5 = 0\,2\,2\,2\,3$, its increment sequence is $\Delta_1 \Delta_2 = 2\,1$.

Lemma 5 The linear complexity profile $L_1 L_2 \ldots L_n$ is uniquely determined by its increment sequence, and conversely.

Proof. The linear complexity profile trivially determines the increment sequence. The increment sequence uniquely determines the linear complexity after the k-th jump as $\Delta_1 + \Delta_2 + \cdots + \Delta_k$. Suppose this jump occurs at position $i+1$, i.e., $L_{i+1} = \Delta_1 + \Delta_2 + \cdots + \Delta_k > L - i =$

$\Delta_1 + \Delta_2 + \cdots + \Delta_{k-1}$. By the "Length-Change Property of LFSR's" proved in [MASS 69, theorem 2], $L_{i+1} \neq L_i$ implies $L_{i+1} = i + 1 - L_i$ for all $i > 0$ ($L_0 = 0$ by way of convention). Thus

$$\begin{aligned} i+1 &= L_{i+1} + L_i & (14)\\ &= 2L_i + (L_{i+1} - L_i) & (15)\\ &= 2(\Delta_1 + \Delta_2 + \cdots + \Delta_{k-1}) + \Delta_k. & (16) \end{aligned}$$

Thus, the location $i + 1$ of the k-th jump $(L_{i+1} - L_i)$ is also uniquely determined by the increment sequence. This proves the lemma.

For instance, suppose that the increment sequence of a linear complexity profile is 1 3 2, the linear complexity profile can only be

$$L_{s^\infty} = 1^4 4^4 6^\infty . \tag{17}$$

With the aid of Lemma 5, we now have our main result.

Corollary 1 to Theorem 3. If a semi-infinite sequence $s^\infty = s_1 s_2 \cdots$ over a field $\boldsymbol{F}$ is associated with the element $S(z) = \sum_{i=1}^{\infty} s_i z^{-i}$ in the field of Laurent series over $\boldsymbol{F}$, then the increment sequence of the linear complexity profile of s^∞ is equal to the sequence of degrees of the partial quotients in the continued-fraction expansion of $S(z)$, i.e., $\Delta_k = \deg[a_k(z)]$.

Corollary 2 to Theorem 3. If a finite sequence $s^n = s_1 s_2 \cdots s_n$ over a field $\boldsymbol{F}$ is associated with the element $S(z) = \sum_{i=1}^{n} s_i z^{-i} = [0; a_1(z), a_2(z), \cdots, a_k(z)]$ in the field of Laurent series over $\boldsymbol{F}$, then the increment sequence Δ_{s^n} of the linear complexity profile of s^n is as follows.

1. *If $2 \cdot \sum_{i=1}^{k} \deg(a_i(z)) - \deg(a_k(z)) \leq n$, then $\Delta_{s^n} = \deg(a_1(z))\deg(a_2(z)) \cdots \deg(a_k(z))$.*
2. *If $2 \cdot \sum_{i=1}^{k} \deg(a_i(z)) - \deg(a_k(z)) > n$, then $\Delta_{s^n} = \deg(a_1(z))\deg(a_2(z)) \cdots \deg(a_{k'}(z))$, where $k' = max\{j : 2 \cdot \sum_{i=1}^{j} \deg(a_i(z) - \deg(a_j(z)) \leq n\}$.*

These corollaries tell us how to construct (finite and infinite) sequences with desired linear complexity profiles.

Example. Construct all sequences over $\boldsymbol{F}_2$ that have the linear complexity profile $1^4 4^4 6^\infty$ of (17). The increment sequence of this linear complexity profile is 1 3 2 . According

to the Corollary 1 to Theorem 3, a sequence with this increment sequence has the finite continued-fraction

$$S(z) = \cfrac{1}{a_1(z) + \cfrac{1}{a_2(z) + \cfrac{1}{a_3(z)}}},$$

where $\deg a_1(z) = 1$, $\deg a_2(z) = 3$, $\deg a_3(z) = 2$. There are 2^i ways to choose a polynomial over $\boldsymbol{F}_2$ with degree i. There are thus $2^1 2^3 2^2 = 64$ different choices for $S(z)$, i.e., there are 64 semi-infinite binary sequences having the linear complexity profile of (17). For a specific such sequence, we choose

$$\begin{aligned} a_1(z) &= z, \\ a_2(z) &= z^3, \\ a_3(z) &= z^2. \end{aligned}$$

We have then

$$\begin{aligned} S(z) &= \cfrac{1}{z + \cfrac{1}{z^3 + \cfrac{1}{z^2}}} \\ &= \frac{z^5 + 1}{z^6 + z^2 + z}. \end{aligned}$$

By long division, we find

$$S(z) = z^{-1} + z^{-5} + z^{-9} + z^{-10} + \cdots .$$

The desired sequence is

$$s^\infty = 1(00010001100101011111 0)^\infty.$$

If a semi-infinite sequence s^∞ corresponds to the element $S(z)$ of the Laurent field in the manner (9) such that the continued-fraction expansion is infinite, i.e.,

$$S(z) = [0; a_1(z), \ldots, a_k(z), \ldots],$$

then by using the k-th convergent of $S(z)$ to approximate $S(z)$, we can see that L1 and L2 in Theorem 3 still hold. If k goes to infinity, the k-th convergent then approaches $S(z)$. Therefore, L1 and L2 in Theorem 3 and the Corollary 1 to Theorem 3 are also valid for the case that the continued-fraction expansion of $S(z)$ is infinite.

3 Remarks

In [NIED 86], Niederreiter showed the following result. If the continued-fraction expansion of $S(z)$ is infinite, which is the same as saying that $S(z)$ is irrational, the linear complexity profile satisfies

$$\frac{1}{2}(i+1-K(S) \leq L_i \leq \frac{1}{2}(i+K(S)) \qquad \text{for all } i \geq 1, \tag{18}$$

where $L_i = \mathcal{L}(s_1 s_2 \cdots s_i)$ and $K(S) = \sup_{j \geq 1} \deg a_j(z)$. We now show that (18) is a simple consequence of L2 in Theorem 3 and the "length-change property of LFSR's" for the case that the continued-fraction expansion of $S(z)$ is infinite.

We restate (2) in Theorem 3 as follows.

For

$$\deg a_k(z) + 2\sum_{j+1}^{k-1} \deg a_j(z) \leq i \leq \deg a_{k+1}(z) + 2\sum_{j=1}^{k} \deg a_j(z) - 1, \tag{19}$$

where $k \geq 1$, we have

$$\begin{aligned} L_i &= \sum_{j=1}^{k} \deg a_j(z) && (20)\\ &= \frac{1}{2}(\deg a_k(z) + 2\sum_{j=1}^{k-1} \deg a_j(z) + \deg a_k(z)) && (21)\\ &\leq \frac{1}{2}(i + \deg a_k(z)) && (22) \end{aligned}$$

with equality when $i = \deg a_k(z) + 2\sum_{j=1}^{k-1}$, where the last step follows from the left inequality of (19).

Further,

$$L_i = \sum_{j=1}^{k} \deg a_j(z)$$

$$= \frac{1}{2}(a_{k+1}(z) + 2\sum_{j=1}^{k} \deg a_j(z) - a_{k+1}(z)).$$

It follows then from the right inequality of (19) that

$$L_i \geq \frac{1}{2}(i + 1 - \deg a_{k+1}(z)) \tag{23}$$

with equality when $i = \deg a_{k+1}(z) + 2\sum_{j=1}^{k} a_j(z) - 1$. Inequalities (22) and (23) immediately give (18).

Baum and Sweet [BAU-SWE 77] showed that all partial quotients of the continued-fraction expansion of $S(z)$ have degree one if and only if

$$S^2(z) + zS(z) + 1 = (1 + z)g^2(z) \tag{24}$$

for some polynomial $g(z)$. Their equation (24) is the same as

$$\begin{aligned} s_1 &= 1, \quad \text{and} \\ s_{2i+1} &= s_{2i} + s_i \qquad \text{for } i \geq 1. \end{aligned}$$

The Corollary 1 to Theorem 3 implies then that all sequences s^∞, for which $S(z)$ satisfies (24), have the linear complexity profile 1 1 2 2 3 3 ..., defined as the *perfect linear complexity profile* (PLCP). This is consistent with the result proved in [WAN-MAS 86], namely, that s^∞ has a perfect linear complexity profile if and only if

$$\begin{aligned} s_1 &= 1, \\ s_{2i+1} &= s_{2i} + s_i \qquad \text{for } i \geq 1. \end{aligned}$$

Acknowledgements

I wish to thank Prof. James L. Massey for his guidance of this work. I further wish to thank Prof. Ian F. Blake for his encouragement and help.

References

[BAU-SWE 77] L. E. Baum and M. M. Sweet, "Badly approximable power series in characteristic 2" , *Ann. of Math.* , 105 (1977), pp.573–580.

[LID-NIE 83] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley Publishing Company, Inc., 1983.

[MASS 69] J. L. Massey, "Shift-Register Synthesis and BCH Decoding", *IEEE Trans. on Info. Th.*, pp.122–127, IT-15, No.1, Jan. 1969.

[NIED 86] H. Niederreiter, "Continued Fractions for Formal Power Series, Pseudorandom Numbers, and Linear Complexity of Sequences", to appear in *Contributions to General Algebra 5* (Proc. Conf. Salzburg, 1986), Teubner, Stuttgart.

[NIED 87] H. Niederreiter, *"Sequences with almost perfect linear complexity profile"*, Proc. Eurocrypt'87, LNCS 304, 37-51 (1988).

[NIED 88] H. Niederreiter, *"The probabilistic theory of linear complexity"*, Proc. Eurocrypt'88, LNCS 330, 191-209, (1988).

[NIED 89] H. Niederreiter, *"Keystream sequence with good linear complexity profile for every starting point"*, paper presented at Eurocrypt'89, Hauthalen, Belgium.

[WAN-MAS 86] M. Z. Wang and J. L. Massey, "The Characterization of All Binary Sequences with Perfect Linear Complexity Profiles", paper presented at Eurocrypt'86, Linköping, Sweden.

[WES-SCH 79] L. R. Welch and R. A. Scholtz, "Continued Fractions and Berlekamp's Algorithm", *IEEE Trans. on Info. Th.*, pp.19–27, IT-25, No.1, January 1979.