AAECC (2006) 17: 29–39
DOI 10.1007/s00200-006-0195-2

Wilfried Meidl

Continued fraction for formal laurent series and the lattice structure of sequences

Received: 31 January 2004 / Published online: 2 March 2006

Abstract Besides equidistribution properties and statistical independence the lattice profile, a generalized version of Marsaglia's lattice test, provides another quality measure for pseudorandom sequences over a (finite) field. It turned out that the lattice profile is closely related with the linear complexity profile. In this article we give a survey of several features of the linear complexity profile and the lattice profile, and we utilize relationships to completely describe the lattice profile of a sequence over a finite field in terms of the continued fraction expansion of its generating function. Finally we describe and construct sequences with a certain lattice profile, and introduce a further complexity measure.

Keywords Sequences over finite fields · Continued fraction expansion · Marsaglia's lattice test · Linear complexity

1 Introduction

Besides good equidistribution properties and statistical independence of successive elements a fine lattice structure is a desirable feature for a sequence for applications in Monte Carlo methods (see the surveys in [4,12,13]). In the series of papers [1–3] the following generalization of Marsaglia's lattice test (see [6]) was introduced and analyzed. Let $S = s_1, s_2, \dots$ be a sequence with terms in the finite field $\mathbb{F}_q$ then we say that S passes the *Λ-dimensional n-lattice test* if the vectors $\{\mathbf{s_j} - \mathbf{s_1} \mid 2 \le j \le n - \Lambda + 1\}$ span $\mathbb{F}_q^{\Lambda}$, where

$$\mathbf{s_j} = (s_j, s_{j+1}, \dots, s_{j+\Lambda-1}) \quad 1 \le j \le n - \Lambda + 1.$$

Remark We follow the notation of [3]. In particular we start the sequences with s_1 and not with s_0 as in [1,2]. This is necessary in order to utilize the results of [9].

W. Meidl
Sabanci University, Orhanli, Tuzla, 34956 Istanbul, Turkey
E-mail: wmeidl@sabanciuniv.edu

If S passes the Λ-dimensional n-lattice test then it passes all Λ'-dimensional lattice tests for all $\Lambda' \leq \Lambda$, and if S fails the Λ-dimensional n-lattice test then it fails all Λ'-dimensional lattice tests for all $\Lambda' \geq \Lambda$. The greatest Λ such that S passes the Λ-dimensional n-lattice test denoted by $\Lambda_n(S)$ is called the *nth lattice level* of S. Additionally we define $\Lambda_0(S) = \Lambda_1(S) = 0$. The *lattice level* $\Lambda(S)$ of S is then defined to be

$$\Lambda(S) = \sup_{n \geq 0} \Lambda_n(S),$$

and we call the sequence $\langle \Lambda_n(S) \rangle_{n=0}^{\infty}$ the *lattice profile* of S (cf. [2,3]).

Recall that the *nth linear complexity* L_n of S, denoted by $L_n(S)$, is the length of the shortest recurrence relation

$$a_{L_n} s_{j+L_n} + a_{L_n-1} s_{j+L_n-1} + \cdots + a_0 s_j = 0 \quad \text{for } j = 1, 2, \ldots, n - L_n \tag{1}$$

satisfied by the first n terms of S. The corresponding polynomial

$$f_n = a_{L_n} x^{L_n} + a_{L_n-1} x^{L_n-1} + \cdots + a_0$$

is called the nth minimal polynomial of S. If S starts with n zeros and $s_{n+1} \neq 0$ then we define $L_i(S) = 0$ for $1 \leq i \leq n$, and $L_{n+1}(S) = n + 1$. Additionally we put $L_0(S) = 0$.

In general the recurrence relation (1) (and the corresponding nth minimal polynomial) is not unique, but apart from a multiplication with a constant we have uniqueness if and only if $L_n(S) \leq n/2$ (see [9, Theorem 1]). The *linear complexity* $L(S)$ of S is defined as

$$L(S) = \sup_{n \geq 0} L_n(S), \tag{2}$$

and the sequence $\langle L_n(S) \rangle_{n=0}^{\infty}$ is denoted as the *linear complexity profile* of S (cf. [8,9,15]).

Trivially the linear complexity (2) is finite, say $L(S) = L$, if and only if S is (ultimately) periodic. Then, if S satisfies the recurrence relation

$$a_L s_{j+L} + a_{L-1} s_{j+L-1} + \cdots + a_0 s_j = 0 \quad \text{for } j = 1, 2, \ldots, \tag{3}$$

the polynomial

$$f(x) = a_L x^L + a_{L-1} x^{L-1} + \cdots + a_0 \tag{4}$$

with $\deg(f) = L$ is called the *minimal polynomial* of S. Apart from a multiplication with a constant the recurrence relation (3) and the minimal polynomial f are uniquely determined.

In [9] formal Laurent series viewed as generating functions of sequences have been discussed. It has been shown that the linear complexity profile of a sequence can be described in terms of the continued fraction expansion of its generating function. The first connections between the linear complexity and the lattice level have been established in [14]. In [1,2,14] strong relationships between the linear complexity profile and the lattice profile have been elaborated. These strong relationships can be utilized to obtain a further understanding of the dynamic behavior of the nth lattice level.

In Section 2 we will describe the lattice profile of a sequence in terms of the continued fraction expansion of its generating function. In Section 3 we will use the results to describe and construct sequences with certain lattice profile. Finally in Section 4 we introduce a further related complexity measure for sequences over $\mathbb{F}_q$.

2 Lattice profile and continued fraction

We start the section with a collection of the significant relations between the linear complexity profile and the lattice profile.

Proposition 1 *[1, Theorem 1] We have either*

$$\Lambda_n(S) = \min(L_n(S), n+1-L_n(S)) \quad \textit{or}$$
$$\Lambda_n(S) = \min(L_n(S), n+1-L_n(S)) - 1.$$

Proposition 2 *[1, Corollary 13] If $L_n(S) = (n+1)/2$ then $\Lambda_n(S) = (n-1)/2$.*

If $L_n(S) \le n/2$ then we know from Proposition 1 that we either have $\Lambda_n(S) = L_n(S)$ or $\Lambda_n(S) = L_n(S) - 1$. The next proposition presents a necessary and sufficient condition for $\Lambda_n(S) < L_n(S)$ assuming that $L_n(S) \le n/2$. This proposition was originally shown in [1]. We present it in the notation of [3].

Proposition 3 *[3, Proposition 4] If $L_n(S) \le n/2$ and*

$$a_{L_n} s_{j+L_n} + a_{L_n-1} s_{j+L_n-1} + \cdots + a_0 s_j = 0, \quad 1 \le j \le n - L_n$$

is the shortest recurrence relation satisfied by the first n terms of S, then

$$\Lambda_n(S) = L_n(S) - 1$$

if and only if

$$a_0 + a_1 + \cdots + a_{L_n-1} + a_{L_n} = 0. \tag{5}$$

Otherwise $\Lambda_n(S) = L_n(S)$.

Proposition 4 *(cf.[2, Theorem 2]) Assume $L_{n_1}(S) = n_1/2$ and let n_2 be the smallest integer such that $n_1 < n_2$ and $L_{n_2}(S) = n_2/2$. (If such an integer n_2 does not exist, we can put $n_2 = \infty$.) If $\Lambda_{n_1}(S) = L_{n_1}(S) - 1$, i.e. the shortest recurrence relation satisfied by the first n_1 terms of S fulfills* (5)*, then for $n_1 \le n \le n_2 - 2$ we have*

$$\Lambda_n(S) = \min(L_n(S), n+1-L_n(S)) - 1.$$

Else we have

$$\Lambda_n(S) = \min(L_n(S), n+1-L_n(S)).$$

Notice that the condition (5) on the coefficients of the recurrence relation is equivalent to $f_n \equiv 0 \bmod (x-1)$, where f_n denotes the corresponding nth minimal polynomial.

Invoking the well known direct consequence of the Berlekamp-Massey algorithm ([7]) that the linear complexity can just increase if $L_n(S) \le n/2$, and that in the case of an increase we have $L_{n+1}(S) = n + 1 - L_n(S)$ (for a proof see [5, Theorem 6.7.4]), the above relations were utilized in [2] to describe the typical lattice profile. The fundamental feature of the lattice profile is that whenever the lattice profile starts to increase, it increases in each step by 1 until it meets the $n/2$-line. This also means that the lattice profile of a given sequence S is uniquely determined by the set of integers n for which we have $\Lambda_n(S) = n/2$.

In [8–10] the relations between the linear complexity profile and continued fraction have been investigated comprehensively. In the following we shortly summarize the basic concepts.

We can associate the sequence $S = s_1, s_2, \ldots$ with terms in the finite field $\mathbb{F}_q$ with its *generating function*

$$\mathcal{S} = \sum_{i=1}^{\infty} s_i x^{-i},$$

which can be viewed as an element of the field $\mathbb{F}_q((x^{-1}))$ of formal Laurent series over $\mathbb{F}_q$ in x^{-1}. The generating function of S is rational, i.e.

$$\sum_{i=1}^{\infty} s_i x^{-i} = \frac{g(x)}{f(x)}$$

with $f, g \in \mathbb{F}_q[x]$, $\deg(g) < \deg(f)$ and $\gcd(f, g) = 1$, if and only if S is (ultimately) periodic. Apart from a multiplication with a constant the polynomial $f(x)$ is uniquely determined and it is exactly the minimal polynomial (4) of the sequence S (see [9, Lemma 2]). Consequently we have $L(S) = \deg(f)$.

Every $\mathcal{S} \in \mathbb{F}_q((x^{-1}))$ has a unique continued fraction expansion

$$\mathcal{S} = \sum_{i=1}^{\infty} s_i x^{-i} = A_0 + 1/(A_1 + 1/(A_2 + \cdots)) =: [A_0, A_1, A_2, \ldots],$$

where the A_j, $j \ge 0$, are polynomials over $\mathbb{F}_q$ with $\deg(A_j) \ge 1$ for $j \ge 1$. If $\mathcal{S}$ is a generating function of a sequence S over $\mathbb{F}_q$ then the polynomial part $Pol(\mathcal{S})$ of $\mathcal{S}$ equals 0 and we have $A_0 = 0$. In general the polynomials A_j are obtained recursively by

$$A_{j+1} = Pol(B_j^{-1}), \quad B_{j+1} = B_j^{-1} - Pol(B_j^{-1}), \quad \text{for } j \ge 0, \tag{6}$$

with the initial polynomials $A_0 = Pol(\mathcal{S}(x))$ and $B_0 = \mathcal{S}(x) - Pol(\mathcal{S}(x))$. This can be continued as long as $B_j \ne 0$. If the continued fraction expansion is broken off after term A_j, $j \ge 0$, we get the rational convergent P_j/Q_j. The polynomials P_j and Q_j can be calculated recursively by

$$P_{-1} = 1,\ P_0 = A_0,\ P_j = A_j P_{j-1} + P_{j-2} \quad \text{for } j \ge 1,$$

$$Q_{-1} = 0,\ Q_0 = 1,\ Q_j = A_j Q_{j-1} + Q_{j-2} \quad \text{for } j \geq 1. \tag{7}$$

The following proposition is crucial for our considerations.

Proposition 5 *[9, Theorem 1] Let $S = s_1, s_2, \ldots$ be an arbitrary sequence with terms in $\mathbb{F}_q$ and let $\mathcal{S} = [0, A_1, A_2, \ldots]$ be its generating function. Then for any $n \geq 1$ the nth linear complexity of S is given by*

$$L_n(S) = \deg(Q_j),$$

where $j \geq 0$ is uniquely determined by the condition

$$\deg(Q_{j-1}) + \deg(Q_j) \leq n < \deg(Q_j) + \deg(Q_{j+1}). \tag{8}$$

Furthermore the nth minimal polynomials of S are exactly all polynomials f_n of the form

$$f_n = aQ_j + CQ_{j-1},$$

where $a \in \mathbb{F}_q$, $a \neq 0$, and $C \in \mathbb{F}_q[x]$ with $\deg(C) \leq 2\deg(Q_j) - n - 1$.

We remark that for $2\deg(Q_j) \leq n < \deg(Q_j) + \deg(Q_{j+1})$ the nth minimal polynomials are of the form $f_n = aQ_j$, and that $\deg(Q_j) = \sum_{i=1}^{j} \deg(A_i)$, for $j \geq 1$.

With Proposition 5 the linear complexity profile of a sequence S is explicitely described in terms of the continued fraction expansion of its generating function. In order to describe the lattice profile of a sequence S in terms of the continued fraction expansion of its generating function, for all $j \geq 1$ we will have to know whether the - apart from a multiplication with a constant - uniquely determined minimal polynomial Q_j is divisible by $x - 1$. Therefore we define the *residue sequence* $\bar{R} = \bar{r}_{-1}, \bar{r}_0, \bar{r}_1, \ldots$ over $\mathbb{F}_q$ by

$$\bar{R} = 0, 1, Q_1 \bmod (x-1), Q_2 \bmod (x-1), \ldots$$

which following (7) can easily be determined with the continued fraction expansion $[0, A_1, A_2, \ldots]$ of S by the recursion

$$\bar{r}_j = \bar{r}_{j-2} + \bar{r}_{j-1} A_j(1) \quad \text{for } j = 1, 2, \ldots. \tag{9}$$

We remark that the residue sequence $\bar{R}$ will never have two consecutive zeros.

Since we are only interested if $Q_j \equiv 0 \bmod (x-1)$ or $Q_j \not\equiv 0 \bmod (x-1)$, we transform $\bar{R}$ into the *binary residue sequence* $R = r_{-1}, r_0, r_1, \ldots$ defined by $r_j = 0$ iff $\bar{r}_j = 0$, $j = -1, 0, 1, \ldots$. We now can establish the connections between the lattice profile of a sequence S over the finite field $\mathbb{F}_q$ and the continued fraction expansion of its generating function.

Theorem 1 *Let S be an arbitrary sequence over $\mathbb{F}_q$, $[0, A_1, A_2, \ldots]$ the continued fraction expansion of its generating function, and $R = 0, 1, r_1, \ldots$ the corresponding binary residue sequence. Then for any $n \geq 0$ the nth lattice level $\Lambda_n(S)$ of S is given by*

$$\Lambda_n(S) = n - \deg(Q_j) + r_{j-1} \quad \textit{for}$$
$$\deg(Q_{j-1}) + \deg(Q_j) \leq n < 2\deg(Q_j) - 1, \tag{10}$$
$$\Lambda_n(S) = \deg(Q_j) - 1, \quad \textit{if } n = 2\deg(Q_j) - 1,$$
$$\Lambda_n(S) = \deg(Q_j) - 1 + r_j \quad \textit{for}$$
$$2\deg(Q_j) \leq n < \deg(Q_j) + \deg(Q_{j+1}). \tag{11}$$

Proof If $n = 2\deg(Q_j) - 1$ with Proposition 5 we get $L_n(S) = \deg(Q_j) = (n+1)/2$, and hence Proposition 2 yields $\Lambda_n(S) = (n-1)/2 = \deg(Q_j) - 1$.

If $\deg(Q_{j-1}) + \deg(Q_j) \le n < 2\deg(Q_j) - 1$ with Proposition 1 and Proposition 5 we immediately get that we either have $\Lambda_n(S) = n - \deg(Q_j)$ or $\Lambda_n(S) = n - \deg(Q_j) + 1$. Analogously for $2\deg(Q_j) \le n < \deg(Q_j) + \deg(Q_{j+1})$ Proposition 1 and Proposition 5 yield that we either have $\Lambda_n(S) = \deg(Q_j) - 1$ or $\Lambda_n(S) = \deg(Q_j)$. We apply Propositions 3–5 to obtain the exact value.

From Proposition 5 we know that the integers

$$n_1 = 2\deg(Q_{j-1}), n_2 = 2\deg(Q_j) \quad \text{and} \quad n_3 = 2\deg(Q_{j+1})$$

satisfy $L_{n_i}(S) = n_i/2, i = 1, 2, 3$. Furthermore there is no other integer $n_1 \le n \le n_3$ with that property. With Proposition 3 and the definition of r_{j-1} respectively r_j we get

$$\Lambda_{n_1}(S) = L_{n_1}(S) - 1 + r_{j-1} = \deg(Q_{j-1}) - 1 + r_{j-1} \quad \text{and}$$

$$\Lambda_{n_2}(S) = L_{n_2}(S) - 1 + r_j = \deg(Q_j) - 1 + r_j.$$

From Proposition 4 we know that then we have

$$\Lambda_n(S) = \min(L_n(S), n + 1 - L_n(S)) - 1 + r_{j-1}$$

for all n with $2\deg(Q_{j-1}) = n_1 \le n \le n_2 - 2 = 2\deg(Q_j) - 2$. In particular for $\deg(Q_{j-1}) + \deg(Q_j) \le n < 2\deg(Q_j) - 1$ we get

$$\Lambda_n(S) = n - \deg(Q_j) + r_{j-1}.$$

Similarly with Proposition 4 we get

$$\Lambda_n(S) = \deg(Q_j) - 1 + r_j$$

for $2\deg(Q_j) \le n < \deg(Q_j) + \deg(Q_{j+1})$, where we use that $\deg(Q_j) + \deg(Q_{j+1}) - 1 \le 2\deg(Q_{j+1}) - 2 = n_3 - 2$. □

3 Sequences with certain lattice profile

Theorem 1 provides the lattice profile given the continued fraction expansion of the generating function of a sequence over $\mathbb{F}_q$ (see (6)). In this section we conversely describe sequences possessing a certain predetermined lattice profile. In [3] the number of finite sequences over $\mathbb{F}_q$ with length n and given nth lattice level $\Lambda \le n/2$ has been determined. Given this counting function, the expected value [3, Theorem 2] and the variance [3, Theorem 3] of the nth lattice level of an arbitrary sequence over $\mathbb{F}_q$ have been calculated. The results show that the lattice profile of a random infinite sequence with terms in a finite field $\mathbb{F}_q$ follows closely the $n/2$-line (without exceeding $n/2$). Frequent large deviations from $n/2$ are not very likely. This motivates the following definition for sequences with maximal possible nth lattice level for all $n = 0, 1, 2, \ldots$ (see also [3, Section 6]).

Definition 1 *A sequence $S = s_1, s_2, \ldots$ with terms in a finite field $\mathbb{F}_q$ is said to have a perfect lattice profile if*

$$\Lambda_n = \left\lfloor \frac{n}{2} \right\rfloor, \quad \text{for } n \geq 0.$$

The following corollary gives an explicit characterization of sequences with a perfect lattice profile in terms of the continued fraction expansion of its generating function. A similar description of sequences with a perfect linear complexity profile (see [8,9]) has been given in [9, Theorem 2].

Corollary 1 *A sequence S with terms in $\mathbb{F}_q$ has a perfect lattice profile if and only if its generating function $\mathcal{S}$ is irrational and has a continued fraction expansion $\mathcal{S} = [0, A_1, A_2, \ldots]$ with $\deg(A_j) \leq 2$ for all $j \geq 1$, and binary residue sequence $R = 0, 1, 1, 1, \ldots$.*

Proof Suppose $r_j = 0$ for any $j \geq 1$. Then with Theorem 1 for $n = 2\deg(Q_j)$ we have $\Lambda_n(S) = \deg(Q_j) - 1 < \lfloor n/2 \rfloor$. If $\deg(A_{j+1}) \geq 3$ for an index $j \geq 0$, then $\Lambda_n(S) \leq \deg(Q_j) < \lfloor n/2 \rfloor$ for $n = 2\deg(Q_j) + 2 < \deg(Q_j) + \deg(Q_{j+1})$.

Conversely let $\deg(A_j) \leq 2$, for $j \geq 1$ and $R = 0, 1, 1, 1, \ldots$. Then we have the inequalities

$$2\deg(Q_j) - 2 \leq \deg(Q_{j-1}) + \deg(Q_j) \quad \text{and}$$

$$\deg(Q_{j-1}) + \deg(Q_j) \leq 2\deg(Q_j) + 2.$$

Consequently for (10) only the value $n = 2\deg(Q_j) - 2$ is possible and for (11) only the cases $n = 2\deg(Q_j)$ and $n = 2\deg(Q_j) + 1$ are possible. Since for $j \geq 1$ we have $r_j = 1$ for all of those possible cases we get $\Lambda_n(S) = \lfloor n/2 \rfloor$. Note that for $n = 2\deg(Q_j) - 1$ we always have $\Lambda_n(S) = \lfloor n/2 \rfloor$. □

We note that the binary residue sequence equals $R = 0, 1, 1, 1, \ldots$ if and only if for $j \geq 1$ we have $\bar{r}_{j-2} + \bar{r}_{j-1} A_j(1) \neq 0$, i.e.

$$A_j(1) \neq -\frac{\bar{r}_{j-2}}{\bar{r}_{j-1}}, \quad j \geq 1. \tag{12}$$

For instance the choice $A_1(1) = 1$ and $A_j(1) = 0$ for $j \geq 2$ guarantees that (12) is satisfied.

Remark For the important binary case recursion (9) and Corollary 1 yield that a sequence S has a perfect lattice profile if and only if its generating function $\mathcal{S}$ is irrational and has a continued fraction expansion $\mathcal{S} = [0, A_1, A_2, \ldots]$ with $\deg(A_j) \leq 2$, for all $j \geq 1$, $A_1(1) = 1$ and $A_j(1) = 0$ for $j \geq 2$.

This fact has been implicitely used in [3] to show that in the binary case a sequence $S = s_1, s_2, \ldots$ has a perfect lattice profile if and only if it satisfies

$$s_i + s_{2i} = 1 \quad \text{for } i = 1, 2, \ldots.$$

Similarly one can define a k-almost perfect lattice profile, i.e. sequences for which the deviation of the nth lattice level from the $n/2$-line does not exceed a given value k for each $n \geq 0$. With Theorem 1 we easily see that a sequence S has a k-almost perfect lattice profile if and only if the continued fraction expansion of its generating function $\mathcal{S} = [0, A_1, A_2, \dots]$ satisfies

$$\frac{\deg(A_{j+1}) + 1}{2} - r_j \leq k, \quad j = 0, 1, \dots .$$

Theorem 1 also supports a procedure for constructing a sequence S over $\mathbb{F}_q$ with a desired lattice profile. We describe our desired lattice profile in terms of the gaps $(g_1, g_2, \dots)$ between the integers for which the lattice profile meets the $n/2$-line, i.e. lattice profile $(2, 4, 2, 6, 4, \dots)$ means that the first 6 integers with lattice level $\Lambda_n(S) = n/2$ are $n = 0$ (by definition) and $n = 2, 6, 8, 14, 18$. The idea behind is to construct an appropriate continued fraction expansion $[0, A_1, A_2, \dots]$ given a lattice profile with gaps $(g_1, g_2, \dots)$. Suppose we already used $g_1, g_2, \dots, g_{t-1}$ to calculate appropriate polynomials $A_0 = 0, A_1, A_2, \dots A_{j-1}$, and suppose that $r_{j-1} = 1$. Then for $\mu = 2\sum_{r=1}^{j-1} \deg(A_r)$ Theorem 1 yields $\Lambda_\mu(S) = \mu/2$. We refer to this situation as an initial state. Note that the first initial state will be the starting position, where $n = 0$, $j = 1$.

Case 1: $g_t = 2$.

Choose a polynomial A_j of degree 1 such that $r_j = 1$, which is always possible. With $\mu = 2\sum_{r=1}^{j} \deg(A_r)$ we arrive at an initial state.

Case 2: $g_t > 2$, $g_{t+1} = 2$.

Choose a polynomial A_j of degree $g_t/2 + 1$ such that $r_j = 1$. With $\mu = 2\sum_{r=1}^{j} \deg(A_r)$ we again arrive at an initial state.

Case 3: $g_t > 2$, $g_{t+1} > 2$.

Choose a polynomial A_j of degree $g_t/2 + 1$ such that $r_j = 0$, and a polynomial A_{j+1} of degree $g_{t+1}/2 - 1$. Independently from the choice of A_{j+1} we will have $r_{j+1} = 1$, and with $\mu = 2\sum_{r=1}^{j+1} \deg(A_r)$ we again arrive at an initial state.

To show the correctness of the procedure it suffices to prove that whenever we move from one to the next initial state, the calculated polynomials guarantee that the gaps between the next integers where the lattice profile meets the $n/2$ line are in fact the g_i we used for the calculation. For a given j we note the following observations.

(I) There exists an n satisfying (10) and $\Lambda_n(S) = n/2$ if and only if $\deg A_j > 1$ and $r_{j-1} = 1$, namely $n = 2\deg(Q_j) - 2$.

(II) There exists an n satisfying (11) and $\Lambda_n(S) = n/2$ if and only if $r_j = 1$, namely $n = 2\deg(Q_j)$.

At the formulation of the algorithm we started at an initial state $\mu = 2\sum_{r=1}^{j-1} \deg(A_r)$ and $r_{j-1} = 1$ such that we have $\Lambda_\mu(S) = \mu/2$. For the Case 1 we have to show that $\mu + g_t$ is the next integer that satisfies $\Lambda_n(S) = n/2$. For the Case 2 and the Case 3 we have to show that the next two integers that satisfy $\Lambda_n(S) = n/2$ are $\mu + g_t$ and $\mu + g_t + g_{t+1}$.

Case 1: With the choice $\deg(A_j) = 1$ and $r_j = 1$ we observe that the conditions in (II) are satisfied. As required, the integer satisfying (11) and $\Lambda_n(S) = n/2$ is exactly $n = 2\deg(Q_j) = \mu + 2$. We emphasize that we are then at an initial state.

Case 2: With the choice $\deg(A_j) = g_t/2 + 1$ and $r_j = 1$ the conditions in (I) and (II) are satisfied. As required, the corresponding integers satisfying $\Lambda_n(S) = n/2$ are

$$n_1 = 2\deg(Q_j) - 2 = \mu + 2\deg(A_j) - 2 = \mu + g_t$$

for (I) and

$$n_2 = 2\deg(Q_j) = \mu + g_t + g_{t+1}$$

for (II).

Case 3: With the choice $\deg(A_j) = g_t/2+1, r_j = 0$ and $\deg(A_{j+1}) = g_{t+1}/2-1$ the conditions in (I) are satisfied for j while the conditions in (II) are satisfied for $j+1$. As required, the corresponding integers where the lattice profile meets the $n/2$-line are $n_1 = \mu + g_t$ and

$$n_2 = 2\deg(Q_{j+1}) = \mu + 2\deg(A_j) + 2\deg(A_{j+1}) = \mu + g_t + g_{t+1}.$$

We again emphasize that in all cases we arrive at an initial state.

Example over $\mathbb{F}_3$. $(g_1, g_2, \dots) = (2, 4, 2, 6, 4, \dots)$:

We have $g_1 = 2$, thus Case 1. We choose $A_1 = x$ in order to obtain $\bar{r}_1 = \bar{r}_{-1} + \bar{r}_0 A_1(1) = 1$ (see (9)) and thus $r_1 = 1$.

For the next step we have $g_2 = 4$, $g_3 = 2$ and consequently Case 2. With the choice $A_2 = x^3 + x + 2$ we obtain $\deg(A_2) = g_2/2 + 1$ and $\bar{r}_2 = \bar{r}_0 + \bar{r}_1 A_2(1) = 2$ and consequently $r_2 = 1$, as required.

Finally $g_4 = 6$ and $g_5 = 4$ yields Case 3. We choose $A_3 = x^4 + x + 2$ and $A_4 = x + 1$ in order to obtain $\deg(A_3) = g_4/2 + 1, \bar{r}_3 = \bar{r}_1 + \bar{r}_2 A_3(1) = 1 + 2 \cdot 1 = 0 = r_3$, and $\deg(A_4) = g_5/2 - 1$.

Applying Theorem 1 it is easy to check that the continued fraction expansion $[0, x, x^3 + x + 2, x^4 + x + 2, x + 1, \dots]$ yields the desired lattice profile.

Simultaneously to an appropriate continued fraction expansion we can calculate the terms of the corresponding sequence. Here we use the fact that the polynomials Q_j determined by the recursion (7) are nth minimal polynomials for n satisfying (8). For a more detailed description see [10, Section 7].

4 The increase frequency

In [16], Wang introduced a new way of looking at the linear complexity profile. The *nth jump complexity* $P_n(S)$ of a sequence S is defined as the number of positive integers among $L_1(S), L_2(S) - L_1(S), \dots, L_n(S) - L_{n-1}(S)$. Thus $P_n(S)$ is the number of "jumps" in the first n terms of the linear complexity profile. For a detailed study of the jump complexity we refer to [11]. The following complexity measure can be seen as the lattice profile equivalent to the jump complexity. The *nth increase frequency* $F_n(S)$ of a sequence S is defined as the number of integers j with $1 \le j \le n$ for which we have $\Lambda_j(S) = j/2$. The nth jump complexity and the nth increase frequency can differ much more than the nth linear complexity and the nth lattice level. Hence we can see the increase frequency as a more independent complexity measure. Anyway we can show that the increase frequency is lower and upper bounded by the jump complexity.

Theorem 2 *The nth increase frequency $F_n(S)$ of a sequence S over $\mathbb{F}_q$ is bounded by*

$$\frac{P_n(S)}{2} - 1 \leq F_n(S) \leq 2P_n(S).$$

Proof We utilize the continued fraction expansion of the generating function of S and note that the nth jump complexity of S is the maximal number j' for which we have $2\deg(Q_{j'}) = \sum_{j=1}^{j'} \deg(A_j) \leq n$. By Theorem 1 for each $1 \leq j \leq j'$ the interval given by (10) contains an integer $\hat{n}$ with $\Lambda_{\hat{n}}(S) = \hat{n}/2$ if and only if $r_{j-1} = 1$ and $\deg(A_j) \geq 2$, and the interval given by (11) contains such an integer $\hat{n}$ if and only if $r_j = 1$. Thus the upper bound is given by $F_n(S) \leq 2P_n(S)$ which for $2\deg(Q_{j'}) \leq n < deg(Q_{j'}) + \deg(Q_{j'+1})$ is attained if $r_0 = r_1 = \ldots = r_{j'} = 1$ and $\deg(A_j) \geq 2$, $1 \leq j \leq j'$. Conversely we see that we get the minimal possible value for $F_n(S)$ relative to $P_n(S)$, i.e. $F_n(S) = P_n(S)/2 - 1$, if we put $\deg(A_j) = 1$, $1 \leq j \leq j'$, the first terms of the binary residue sequence $r_{-1} = 0, 1, 0, 1, \ldots, 0, 1 = r_{j'}$, and $\deg(Q_{j'-1}) + \deg(Q_{j'}) \leq n < 2\deg(Q_{j'})$. □

Acknowledgements The research was supported by DSTA research grant R-394-000-011-422.

References

1. Dorfer, G., Winterhof, A.: Lattice Structure and linear complexity profile of nonlinear pseudorandom number generators. AAECC **13**(6), 499–508 (2003)
2. Dorfer, G.: Lattice profile and linear complexity profile of pseudorandom number sequences. In: Mullen, G.L., Poli, A., Stichtenoth, H. (eds.) Proceedings of the 7th international conference on finite fields and applications. Lecture Notes in Computer Science, Vol. 2948, 69–78. Berlin: Springer, 2004
3. Dorfer, G., Meidl, W., Winterhof, A.: Counting functions and expected values for the lattice profile at n. Finite Fields Appl. **10**, 636–652 (2004)
4. Eichenauer-Herrmann, J., Herrmann, E., Wegenkittl, S.: A survey of quadratic and inversive congruential pseudorandom numbers. In: Niederreiter, H., Shiue, P.J.S. (eds.) Monte Carlo and Quasi-Monte Carlo Methods 1996. Lecture Notes in Statistics, Vol. 127, 66–97. New York: Springer, 1998
5. Jungnickel, D.: Finite fields. Structure and Arithmetics. Bibliographisches Institut. Mannheim 1993
6. Marsaglia, G.: The structure of linear congruential sequences. In: Zaremba, S.K. (ed.): Applications of number theory to numerical analysis, pp 249–285. New York: Academic Press, 1972
7. Massey, J.L.: Shift-register synthesis and BCH decoding. IEEE Trans. Inform. Theory **15**, 122–127 (1969)
8. Niederreiter, H.: Continued fractions for formal power series, pseudorandom numbers, and linear complexity of sequences. Contributions to General Algebra 5, (Proc. Salzburg Conf., 1986), 221–233. Stuttgart: Teubner, 1987
9. Niederreiter, H.: Sequences with almost perfect linear complexity profile. In: Chaum, D., Price, W.L. (eds.) Advances in Cryptology - EUROCRYPT '87. Lecture Notes in Computer Science 304, 37–51. Berlin: Springer, 1988
10. Niederreiter, H.: The probabilistic theory of linear complexity. In: Günther, C.G. (ed.) Advances in Cryptology - EUROCRYPT '88. Lecture Notes in Computer Science 330, 191–209. Berlin: Springer, 1988
11. Niederreiter, H.: The linear complexity profile and the jump complexity of keystream sequences. In: Damgard, I. (ed.) Advances in Cryptology - EUROCRYPT '90. Lecture Notes in Computer Science 473, 174–188. Berlin: Springer, 1991

12. Niederreiter, H.: Design and analysis of nonlinear pseudorandom number generators. Monte Carlo Simulation, 3–9. Rotterdam: A. A. Balkema Publishers 2001
13. Niederreiter, H., Shparlinski, I.E.: Recent advances in the theory of nonlinear pseudorandom number generators. In: Fang, K.-T., Hickernell, F.J., Niederreiter, H. (eds.) Monte Carlo and Quasi-Monte Carlo Methods 2000, 86–102. Berlin: Springer, 2002
14. Niederreiter H., Winterhof, A.: Lattice structure and linear complexity of nonlinear pseudorandom numbers. AAECC **13** (4), 319–326 (2002)
15. Rueppel, R.A.: Analysis and design of stream ciphers. Berlin: Springer, 1986
16. Wang, M.Z.: Cryptographic aspects of sequence complexity measures. Ph.D. dissertation, ETH. Zürich 1988