Available online at www.sciencedirect.com

ScienceDirect

Journal of Complexity 24 (2008) 144–153

Journal of COMPLEXITY

www.elsevier.com/locate/jco

Successive minima profile, lattice profile, and joint linear complexity profile of pseudorandom multisequences

Li-Ping Wang[a], Harald Niederreiter[b,*]

[a] *Center for Advanced Study, Tsinghua University, Beijing 100084, People's Republic of China*

[b] *Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, Republic of Singapore*

Received 26 October 2006; accepted 2 July 2007

Available online 27 July 2007

Abstract

In this paper we use the successive minima profile to measure structural properties of pseudorandom multisequences. We show that both the lattice profile and the joint linear complexity profile of a multisequence can be expressed in terms of the successive minima profile.

Keywords: Multisequences; Marsaglia's lattice test; Joint linear complexity profile; Successive minima

1. Introduction

Complexity theory is of great relevance to cryptology, in particular, to the area of stream ciphers (see [18]). Recent developments in stream ciphers point towards an interest in word-based or vectorized keystreams; see e.g. Dawson and Simpson [2], Hawkes and Rose [9], and the proposals DRAGON, NLS, and SSS to the ECRYPT stream cipher project [7]. The theory of such stream ciphers requires the study of multisequences, i.e., of parallel streams of finitely many sequences, and of their complexity properties.

For a positive integer m, consider m sequences $S^{(h)} = s_1^{(h)}, s_2^{(h)}, \ldots$, where $1 \leqslant h \leqslant m$, with terms $s_j^{(h)}$ in an arbitrary field $\mathbb{F}$, i.e., an *m-fold multisequence* (or *m-dimensional vector sequence*)

$$\mathbf{S} = (S^{(1)}, \ldots, S^{(m)}).$$

* Corresponding author. Fax: +65 6779 5452.

E-mail addresses: wanglp@mail.tsinghua.edu.cn (L.-P. Wang), nied@math.nus.edu.sg (H. Niederreiter).

0885-064X/$ - see front matter
doi:10.1016/j.jco.2007.07.001

For a positive integer n, let $\mathbf{S}_n$ denote the finite-length multisequence consisting of the first n terms of $\mathbf{S}$. A monic polynomial $C(x) = x^d + \sum_{i=0}^{d-1} c_i x^i \in \mathbb{F}[x]$ is called a *characteristic polynomial* of $\mathbf{S}_n$ if

$$s_j^{(h)} + c_{d-1}s_{j-1}^{(h)} + \cdots + c_0 s_{j-d}^{(h)} = 0 \quad \text{for } j = d+1, d+2, \ldots, n \quad \text{and} \quad h = 1, 2, \ldots, m. \tag{1}$$

A *minimal polynomial* of $\mathbf{S}_n$ is a characteristic polynomial of $\mathbf{S}_n$ with the least degree. The *nth joint linear complexity* $\mathrm{LC}(\mathbf{S}_n)$ of $\mathbf{S}$ is the degree of a minimal polynomial of $\mathbf{S}_n$. The *joint linear complexity profile* of $\mathbf{S}$ is the sequence $\{\mathrm{LC}(\mathbf{S}_n)\}_{n \geqslant 1}$. We refer to [16] for a recent survey of work on the joint linear complexity and the joint linear complexity profile of multisequences.

Another quality measure appraising the intrinsic structure of multisequences is given by the extension of Marsaglia's lattice test in [12] from single sequences to multisequences: for $n \geqslant 2$, $\mathbf{S}$ passes the R-dimensional n-lattice test if the vectors $\{\underline{s}_j^{(h)} - \underline{s}_1^{(h)} : 2 \leqslant j \leqslant n - R + 1, 1 \leqslant h \leqslant m\}$ span $\mathbb{F}^R$, where

$$\underline{s}_j^{(h)} = (s_j^{(h)}, s_{j+1}^{(h)}, \ldots, s_{j+R-1}^{(h)}), \quad 1 \leqslant j \leqslant n - R + 1, \quad 1 \leqslant h \leqslant m.$$

If $\mathbf{S}$ passes the R-dimensional n-lattice test, then it passes all R'-dimensional n-lattice tests for $R' \leqslant R$, and if $\mathbf{S}$ fails the R-dimensional n-lattice test, then it fails all R'-dimensional n-lattice tests for $R' \geqslant R$. We call the greatest R such that $\mathbf{S}$ passes the R-dimensional n-lattice test, denoted by $\mathrm{LA}(\mathbf{S}_n)$, the *nth lattice level* of $\mathbf{S}$. The *lattice profile* of $\mathbf{S}$ is the sequence $\{\mathrm{LA}(\mathbf{S}_n)\}_{n \geqslant 2}$. The lattice profile was originally introduced in the context of pseudorandom number generation (see [5]). There are many results about the lattice test for a single sequence, i.e., for $m = 1$ (see [3–6,8,13,14,17]). Recently, multisequences were also studied with regard to the lattice test by Meidl [15] who discussed the relationship between the lattice level and the joint linear complexity for multisequences.

In [1] the authors utilized successive minima to study certain pseudorandom number generators. In Section 2 of the present paper we use the successive minima profile to measure the structural properties of pseudorandom multisequences. We show that the joint linear complexity profile and the lattice profile of a multisequence can be expressed in terms of the successive minima profile in Section 3 and Section 4, respectively.

2. Successive minima profile

For each $h = 1, 2, \ldots, m$, we identify the sequence $S^{(h)}$ having terms $s_1^{(h)}, s_2^{(h)}, \ldots \in \mathbb{F}$ with the formal power series $S^{(h)}(x) = \sum_{j=1}^{\infty} s_j^{(h)} x^{-j}$ which we view as an element of the Laurent series field

$$K = \mathbb{F}((x^{-1})) = \left\{ \sum_{j=j_0}^{\infty} a_j x^{-j} : \ j_0 \in \mathbb{Z}, \ a_j \in \mathbb{F} \right\}.$$

There is a standard (exponential) valuation υ on K whereby for $\alpha = \sum_{j=j_0}^{\infty} a_j x^{-j} \in K$ we put $\upsilon(\alpha) = \max\{-j \in \mathbb{Z} : a_j \neq 0\}$ if $\alpha \neq 0$ and $\upsilon(\alpha) = -\infty$ if $\alpha = 0$. The *valuation* $v(\gamma)$ of an $(m+1)$-dimensional vector $\gamma = (\alpha_1, \ldots, \alpha_{m+1}) \in K^{m+1}$ is defined as $\max\{\upsilon(\alpha_i) : 1 \leqslant i \leqslant m+1\}$. In the sequel we often use the *projection* $\theta : K^{m+1} \to \mathbb{F}^{m+1}$ such that $\gamma = (\alpha_i)_{1 \leqslant i \leqslant m+1} \mapsto (a_{1,-v(\gamma)}, \ldots, a_{m+1,-v(\gamma)})^T$, where $\alpha_i = \sum_{j=j_0}^{\infty} a_{i,j} x^{-j}$, $1 \leqslant i \leqslant m+1$, and T denotes the transpose of a vector.

A subset Λ of K^{m+1} is called an $\mathbb{F}[x]$-*lattice* if there exists a basis $\omega_1, \ldots, \omega_{m+1}$ of K^{m+1} such that

$$\Lambda = \sum_{i=1}^{m+1} \mathbb{F}[x]\,\omega_i = \left\{ \sum_{i=1}^{m+1} f_i\,\omega_i : f_i \in \mathbb{F}[x],\ i = 1, \ldots, m+1 \right\}.$$

In this situation we say that $\omega_1, \ldots, \omega_{m+1}$ form a *basis* for Λ and we often denote the lattice by $\Lambda(\omega_1, \ldots, \omega_{m+1})$. We call $m+1$ the *rank* of Λ. A basis $\omega_1, \ldots, \omega_{m+1}$ is *reduced* if $\theta(\omega_1), \ldots, \theta(\omega_{m+1})$ are linearly independent over $\mathbb{F}$. A reduced basis is *normal* if $v(\omega_1) \leqslant \cdots \leqslant v(\omega_{m+1})$ and the $(m+1)$th component of $\theta(\omega_i)$ is either 0 or 1 for $i = 1, \ldots, m+1$. The *determinant* of the lattice is defined by $\det(\Lambda(\omega_1, \ldots, \omega_{m+1})) := v(\det(\omega_1, \ldots, \omega_{m+1}))$. In [10] it was proved that

$$\sum_{i=1}^{m+1} v(\omega_i) = \det(\Lambda), \tag{2}$$

if $\omega_1, \ldots, \omega_{m+1}$ are a reduced basis for a lattice Λ.

There is an important notion of *successive minima* (see [11]). The ith successive minimum $M_i(\Lambda)$ is defined by $M_i(\Lambda) := \min\{k \in \mathbb{Z} :$ there are i $\mathbb{F}[x]$-linearly independent vectors $\gamma_1, \ldots, \gamma_i$ in Λ such that $v(\gamma_j) \leqslant k,\ 1 \leqslant j \leqslant i\}$ for $1 \leqslant i \leqslant m+1$. If the reduced basis $\omega_1, \ldots, \omega_{m+1}$ satisfies $v(\omega_1) \leqslant \cdots \leqslant v(\omega_{m+1})$, then $M_i(\Lambda) = v(\omega_i)$ for $1 \leqslant i \leqslant m+1$ (see [10]), and so it is clear that ω_1 is a shortest nonzero element in the lattice.

For any integer $n \geqslant 1$, we construct a special lattice $\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n)$ in K^{m+1} spanned by the vectors $\varepsilon_1 = (1, 0, \ldots, 0), \ldots, \varepsilon_m = (0, \ldots, 0, 1, 0)$, $\alpha_n = (S^{(1)}(x), \ldots, S^{(m)}(x), x^{-n-1})$. Clearly

$$\det(\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n)) = -n - 1. \tag{3}$$

By means of a lattice basis reduction algorithm [10,19], we can transform the initial basis $\varepsilon_1, \ldots, \varepsilon_m, \alpha_n$ into a reduced one and then it is easy to transform a reduced basis into a normal one only by rearranging its elements and multiplying them by scalars. We denote a normal basis for the lattice by $\omega_{1,n}, \ldots, \omega_{m+1,n}$. So we obtain $M_i(\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n)) = v(\omega_{i,n})$ for $1 \leqslant i \leqslant m+1$. It is clear that the successive minima of the lattice $\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n)$ are completely determined by the m-fold multisequence $\mathbf{S}$ and the length n, and so these successive minima can be viewed as intrinsic parameters of multisequences. Therefore we also denote $M_i(\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n))$ by $M_i(\mathbf{S}_n)$. Now we can introduce the following definition.

Definition 1. The multiset $\{M_1(\mathbf{S}_n), \ldots, M_{m+1}(\mathbf{S}_n)\}$, denoted by $\mathrm{SM}(\mathbf{S}_n)$, is called the *successive minima* of the multisequence $\mathbf{S}$ at n, and the *successive minima profile* is the sequence $\{\mathrm{SM}(\mathbf{S}_n)\}_{n \geqslant 1}$.

3. Relationship between successive minima and joint linear complexity profile

In [21,22] the lattice $\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n)$ constructed above was used to obtain a minimal polynomial of $\mathbf{S}_n$ by means of the so-called LBRMS algorithm. Using this algorithm, we first establish an important relationship between the joint linear complexity and the successive minima.

Let $\pi_i(\rho)$, $i = 1, \ldots, m+1$, denote the ith component of a vector $\rho \in \mathbb{F}^{m+1}$, let $\Gamma(\mathbf{S}_n)$ be the set of all characteristic polynomials of $\mathbf{S}_n$, and put

$$S(\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n)) := \{\gamma \in \Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n) : \pi_{m+1}(\theta(\gamma)) = 1\}.$$

The mapping $\eta : \Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n) \to \mathbb{F}[x]$ is given by

$$\eta(D_1(x)\varepsilon_1 + \cdots + D_m(x)\varepsilon_m + C(x)\alpha_n) = C(x),$$

where $D_1(x), \ldots, D_m(x), C(x) \in \mathbb{F}[x]$. Conversely, $C(x)$ completely determines an associated element in $\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n)$ given by

$$\sigma(C(x))|_{\Lambda(\varepsilon_1,\ldots,\varepsilon_m,\alpha_n)} := C(x)\alpha_n - \sum_{h=1}^{m} \mathrm{Pol}(C(x)S^{(h)}(x))\varepsilon_h,$$

where $\mathrm{Pol}(C(x)S^{(h)}(x))$ is the polynomial part of $C(x)S^{(h)}(x)$. The following result is obtained from [22, Theorem 2].

Theorem 1. *The mapping η is a valuation-preserving one-to-one correspondence between $S(\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n))$ and $\Gamma(\mathbf{S}_n)$.*

Therefore the problem of determining a minimal polynomial of $\mathbf{S}_n$ is reduced to asking for a shortest element γ in $S(\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n))$. The following theorem (see [21, Theorem 1] and [22, Theorem 3]) shows that such an element must appear in a normal basis of $\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n)$.

Theorem 2. *Let $\omega_1, \ldots, \omega_l$ be a normal basis of a lattice Λ of rank l and let*

$$S(\Lambda) = \{\gamma \in \Lambda : \pi_l(\theta(\gamma)) = 1\}.$$

Let k be the least integer such that $\omega_k \in S(\Lambda)$. Then ω_k is a shortest element of $S(\Lambda)$.

Let k_n denote the least integer such that $\omega_{k_n,n} \in S(\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n))$. Then $\eta(\omega_{k_n,n})$ is a minimal polynomial of $\mathbf{S}_n$ by Theorems 1 and 2, and

$$v(\omega_{k_n,n}) = \mathrm{LC}(\mathbf{S}_n) - n - 1. \tag{4}$$

This is the basic idea of the LBRMS algorithm (see [21,22] and Appendix A for details).

Proposition 1. *For any m-fold multisequence $\mathbf{S}$ and any integer $n \geqslant 1$, there exists some integer k_n, $1 \leqslant k_n \leqslant m+1$, such that $M_{k_n}(\mathbf{S}_n) = \mathrm{LC}(\mathbf{S}_n) - n - 1$ and*

$$\sum_{\substack{i=1 \\ i \neq k_n}}^{m+1} M_i(\mathbf{S}_n) = -\mathrm{LC}(\mathbf{S}_n). \tag{5}$$

Proof. The result easily follows from (2), (3), and (4). □

In the following, we describe the dynamics of the successive minima profile and the joint linear complexity profile.

Let

$$\omega_i' = \sigma(\eta(\omega_{i,n}))|_{\Lambda(\varepsilon_1,\ldots,\varepsilon_m,\alpha_{n+1})}, \quad 1 \leqslant i \leqslant m+1.$$

Then $\omega_1', \ldots, \omega_{m+1}'$ form a basis for the lattice $\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_{n+1})$ and now we transform it into a reduced one. It is clear that $v(\omega_i') = v(\omega_{i,n})$ for $i \neq k_n$. As to the value of $v(\omega_{k_n}')$, there are two cases.

If $\pi_{m+1}(\theta(\omega_{k_n}')) \neq 0$, it means that $\eta(\omega_{k_n}')$ also generates the first $n+1$ terms of $\mathbf{S}$ and hence $\omega_1', \ldots, \omega_{m+1}'$ form a reduced basis for the lattice $\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_{n+1})$. So $v(\omega_{k_n}') = v(\omega_{k_n,n}) - 1$ and $\mathrm{LC}(\mathbf{S}_{n+1}) = \mathrm{LC}(\mathbf{S}_n) = n + 1 + v(\omega_{k_n,n})$.

Otherwise, we have $\pi_{m+1}(\theta(\omega_{k_n}')) = 0$ and $v(\omega_{k_n}') = v(\omega_{k_n,n}) = \mathrm{LC}(\mathbf{S}_n) - n - 1$. Therefore $\theta(\omega_{k_n}')$ is a linear combination of $\{\theta(\omega_i') : 1 \leqslant i \leqslant m+1,\ i \neq k_n\}$, and so there exist scalars $a_i \in \mathbb{F}$ with $a_{k_n} = 1$ such that

$$\sum_{i=1}^{m+1} a_i \theta(\omega_i') = 0.$$

Let h_n be an integer such that $v(\omega_{h_n}') = \max\{v(\omega_i') : 1 \leqslant i \leqslant m+1,\ a_i \neq 0\}$. We let

$$\xi = \sum_{i=1}^{m+1} a_i x^{-v(\omega_i')+v(\omega_{h_n}')} \omega_i'.$$

The reduced basis for $\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_{n+1})$ is $\omega_1', \ldots, \omega_{h_n-1}', \xi, \omega_{h_n+1}', \ldots, \omega_{m+1}'$, and

$$\mathrm{LC}(\mathbf{S}_{n+1}) = n + 1 + v(\omega_{h_n}'),$$

$$v(\xi) = \mathrm{LC}(\mathbf{S}_{n+1}) - n - 2 = v(\omega_{h_n}') - 1.$$

Suppose $v(\omega_{1,n}) \leqslant v(\omega_{2,n}) \leqslant v(\omega_{t_n,n}) < v(\omega_{t_n+1,n}) = \cdots = v(\omega_{h_n,n}) \leqslant v(\omega_{h_n+1,n}) \leqslant \cdots \leqslant v(\omega_{m+1,n})$. Then $\omega_1', \ldots, \omega_{t_n}', \xi, \omega_{t_n+1}', \ldots, \omega_{h_n-1}', \omega_{h_n+1}', \ldots, \omega_{m+1}'$ is a normal basis for the lattice.

These results are summarized in the following proposition.

Proposition 2. *We have*:

(i) $\mathrm{LC}(\mathbf{S}_{n+1}) = n + 1 + M_{h_n}(\mathbf{S}_n)$, $\mathrm{SM}(\mathbf{S}_{n+1}) = (\mathrm{SM}(\mathbf{S}_n) \cup \{M_{h_n}(\mathbf{S}_n) - 1\}) \setminus \{M_{h_n}(\mathbf{S}_n)\}$, *for some integer* h_n, $1 \leqslant h_n \leqslant m+1$.
(ii) $M_i(\mathbf{S}_{n+1}) = M_i(\mathbf{S}_n)$ *or* $M_i(\mathbf{S}_n) - 1$ *for all* $1 \leqslant i \leqslant m+1$.

4. Relationship between successive minima profile and lattice profile

In this section we investigate the relationship between the successive minima profile and the lattice profile.

Lemma 1. *For any integer* N *with* $1 \leqslant N \leqslant n$, *we have* $\mathrm{LC}(\mathbf{S}_N) - N - 1 \geqslant M_1(\mathbf{S}_n)$.

Proof. We prove the lemma by contradiction. So suppose that there exists an integer N_0 with $1 \leqslant N_0 \leqslant n$ such that $\mathrm{LC}(\mathbf{S}_{N_0}) - N_0 - 1 < M_1(\mathbf{S}_n)$. Then Proposition 1 yields $M_1(\mathbf{S}_{N_0}) < M_1(\mathbf{S}_n)$, which is a contradiction to Proposition 2(ii). □

Lemma 2. *Let $\omega_{1,n}, \ldots, \omega_{m+1,n}$ be a normal basis for the lattice $\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n)$. Then $\eta(\omega_{1,n})$ is a minimal polynomial of $\mathbf{S}_N$, where $N = -M_1(\mathbf{S}_n) + \deg(\eta(\omega_{1,n})) - 1$.*

Proof. Put $\omega = \sigma(\eta(\omega_{1,n}))|_{\Lambda(\varepsilon_1,\ldots,\varepsilon_m,\alpha_N)}$. Then ω is an element of a basis for $\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_N)$. Since $\pi_{m+1}(\theta(\omega)) = 1$, by Theorem 1 we have $\eta(\omega) = \eta(\omega_{1,n})$ is a characteristic polynomial of $\mathbf{S}_N$. By Proposition 2(ii) we have $v(\omega) \leqslant M_i(\mathbf{S}_N)$ for all $1 \leqslant i \leqslant m+1$, and so ω is a shortest element of $S(\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_N))$ by Theorem 2. □

Theorem 3. *For any m-fold multisequence* $\mathbf{S}$ *and any integer* $n \geqslant 1$, *we have*

$$\mathrm{LA}(\mathbf{S}_n) = n + 1 + M_1(\mathbf{S}_n) \quad \text{or} \quad \mathrm{LA}(\mathbf{S}_n) = n + M_1(\mathbf{S}_n).$$

Proof. First we show that $\mathrm{LA}(\mathbf{S}_n) \leqslant n + 1 + M_1(\mathbf{S}_n)$, and so we need to prove that $\mathbf{S}$ fails to pass the R-dimensional n-lattice test with $R = n + 2 + M_1(\mathbf{S}_n)$, that is, the vectors $\{\underline{s}_j^{(h)} - \underline{s}_1^{(h)} : 2 \leqslant j \leqslant n - R + 1, 1 \leqslant h \leqslant m\}$ do not span $\mathbb{F}^R$, i.e., the row vectors of the matrix

$$A = \begin{pmatrix} s_2^{(1)} - s_1^{(1)} & \cdots & s_{n-R+1}^{(1)} - s_1^{(1)} & \cdots & s_2^{(m)} - s_1^{(m)} & \cdots & s_{n-R+1}^{(m)} - s_1^{(m)} \\ s_3^{(1)} - s_2^{(1)} & \cdots & s_{n-R+2}^{(1)} - s_2^{(1)} & \cdots & s_3^{(m)} - s_2^{(m)} & \cdots & s_{n-R+2}^{(m)} - s_2^{(m)} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ s_{R+1}^{(1)} - s_R^{(1)} & \cdots & s_n^{(1)} - s_R^{(1)} & \cdots & s_{R+1}^{(m)} - s_R^{(m)} & \cdots & s_n^{(m)} - s_R^{(m)} \end{pmatrix}_{R \times m(n-R)}$$

are linearly dependent over $\mathbb{F}$.

Let $\omega_{1,n}, \ldots, \omega_{m+1,n}$ be a normal basis for the lattice $\Lambda(\varepsilon_1, \ldots, \varepsilon_m, \alpha_n)$. Then $M_1(\mathbf{S}_n) = v(\omega_{1,n})$. Put $N = -M_1(\mathbf{S}_n) + \deg(\eta(\omega_{1,n})) - 1$. Then $\eta(\omega_{1,n})$ is a minimal polynomial of $\mathbf{S}_N$ by Lemma 2. Let $\eta(\omega_{1,n}) = x^{\mathrm{LC}(\mathbf{S}_N)} + c_{\mathrm{LC}(\mathbf{S}_N)-1}x^{\mathrm{LC}(\mathbf{S}_N)-1} + \cdots + c_0$. Then for $1 \leqslant j \leqslant N - \mathrm{LC}(\mathbf{S}_N)$, $1 \leqslant h \leqslant m$, we have

$$s_{j+\mathrm{LC}(\mathbf{S}_N)}^{(h)} + c_{\mathrm{LC}(\mathbf{S}_N)-1}s_{j+\mathrm{LC}(\mathbf{S}_N)-1}^{(h)} + \cdots + c_0 s_j^{(h)} = 0. \tag{6}$$

Since $R - \mathrm{LC}(\mathbf{S}_N) - 1 = n + 2 - (N + 1 - \mathrm{LC}(\mathbf{S}_N)) - \mathrm{LC}(\mathbf{S}_N) - 1 = n - N \geqslant 0$, we get $R \geqslant \mathrm{LC}(\mathbf{S}_N) + 1$. On the other hand, we have $n - R + \mathrm{LC}(\mathbf{S}_N) \leqslant N - 1$ because of $n - R + \mathrm{LC}(\mathbf{S}_N) - N = -M_1(\mathbf{S}_n) - 2 + \mathrm{LC}(\mathbf{S}_N) - N \leqslant -1$. Using elementary row operations and (6), the $(\mathrm{LC}(\mathbf{S}_N) + 1)$th row is transformed to the zero row and $\mathrm{LA}(\mathbf{S}_n) \leqslant n + 1 + M_1(\mathbf{S}_n)$ is shown.

It remains to prove that $\mathrm{LA}(\mathbf{S}_n) \geqslant n + M_1(\mathbf{S}_n)$, i.e., that $\mathbf{S}$ passes the R-dimensional n-lattice test with $R = n + M_1(\mathbf{S}_n)$, i.e., the row vectors of the corresponding matrix A are linearly independent over $\mathbb{F}$. Suppose that the row vectors of A were linearly dependent over $\mathbb{F}$, so that there are scalars $a_1, a_2, \ldots, a_t = 1$ such that

$$a_1\beta_1 + a_2\beta_2 + \cdots + a_t\beta_t = \mathbf{0},$$

where β_i denotes the ith row vector of A for $1 \leqslant i \leqslant R$. Let $N = n - R + t$. Then $1 \leqslant N \leqslant n$ because of $t \leqslant R$. Furthermore, $f(x) = (a_t x^{t-1} + a_{t-1}x^{t-2} + \cdots + a_1)(x - 1)$ is a characteristic polynomial of $\mathbf{S}_N$. So $t \geqslant \mathrm{LC}(\mathbf{S}_N)$ and

$$M_1(\mathbf{S}_n) = -n + R = -N + t \geqslant -N + \mathrm{LC}(\mathbf{S}_N) > -N - 1 + \mathrm{LC}(\mathbf{S}_N),$$

which is impossible by Lemma 1. □

Using Theorem 3, it is easy to deduce some properties of the lattice profile, some of which were already shown in [15] by a different argument.

Corollary 1. *For any m-fold multisequence* $\mathbf{S}$ *and any integer* $n \geqslant 1$, *we have*

$$\mathrm{LA}(\mathbf{S}_n) \leqslant \frac{m}{m+1}(n+1).$$

Proof. By (2) and (3), we get

$$-n-1 = \sum_{a \in \mathrm{SM}(\mathbf{S}_n)} a \geqslant (m+1) M_1(\mathbf{S}_n).$$

Thus, $M_1(\mathbf{S}_n) \leqslant -\frac{1}{m+1}(n+1)$ and $\mathrm{LA}(\mathbf{S}_n) \leqslant n+1+M_1(\mathbf{S}_n) \leqslant \frac{m}{m+1}(n+1)$ by Theorem 3. □

Corollary 2. *We have* $\mathrm{LA}(\mathbf{S}_n) \leqslant \mathrm{LC}(\mathbf{S}_n)$.

Proof. By Theorem 3 and Proposition 1 we get $\mathrm{LA}(\mathbf{S}_n) \leqslant n+1+M_1(\mathbf{S}_n) \leqslant n+1+\mathrm{LC}(\mathbf{S}_n) - n-1 = \mathrm{LC}(\mathbf{S}_n)$. □

Corollary 3. *If* $M_1(\mathbf{S}_n) = \mathrm{LC}(\mathbf{S}_n) - n - 1$, *then*

$$\mathrm{LA}(\mathbf{S}_n) = \mathrm{LC}(\mathbf{S}_n) \quad \textit{or} \quad \mathrm{LA}(\mathbf{S}_n) = \mathrm{LC}(\mathbf{S}_n) - 1.$$

Proof. The result follows directly from Theorem 3. □

Corollary 4. *If* $M_1(\mathbf{S}_n) = \mathrm{LC}(\mathbf{S}_n) - n - 1$ *and* $M_1(\mathbf{S}_n) < M_2(\mathbf{S}_n)$, *then* $\mathrm{LA}(\mathbf{S}_{n-1}) \geqslant \mathrm{LC}(\mathbf{S}_n) - 1$.

Proof. Since $M_1(\mathbf{S}_n) = \mathrm{LC}(\mathbf{S}_n) - n - 1$ and $M_1(\mathbf{S}_n) < M_2(\mathbf{S}_n)$, we have $M_1(\mathbf{S}_{n-1}) > M_1(\mathbf{S}_n) = \mathrm{LC}(\mathbf{S}_n) - n - 1$ by Proposition 2, hence $M_1(\mathbf{S}_{n-1}) \geqslant \mathrm{LC}(\mathbf{S}_n) - n$, and the desired result follows from Theorem 3. □

The following result for single sequences in [5, Theorem 1] is also obtained as a consequence of Theorem 3.

Corollary 5. *If* $m = 1$, *then*

$$\mathrm{LA}(\mathbf{S}_n) = \min(\mathrm{LC}(\mathbf{S}_n), n+1-\mathrm{LC}(\mathbf{S}_n))$$

or

$$\mathrm{LA}(\mathbf{S}_n) = \min(\mathrm{LC}(\mathbf{S}_n), n+1-\mathrm{LC}(\mathbf{S}_n)) - 1.$$

Proof. Since $m = 1$, by Propositions 1 and 2 we obtain

$$M_1(\mathbf{S}_n) = \min(-\mathrm{LC}(\mathbf{S}_n), \mathrm{LC}(\mathbf{S}_n) - n - 1).$$

The result follows from Theorem 3. □

We now return to the general case of m-fold multisequences $\mathbf{S}$ with arbitrary $m \geqslant 1$. We recall the following result which provides a necessary and sufficient condition for the uniqueness of minimal polynomials (see [20, Theorem 4]).

Proposition 3. *The minimal polynomial of* $\mathbf{S}_n$ *is unique if and only if* $M_1(\mathbf{S}_n) = \mathrm{LC}(\mathbf{S}_n) - n - 1$ *and* $M_1(\mathbf{S}_n) < M_2(\mathbf{S}_n)$.

We can now give a condition under which the alternative $\mathrm{LA}(\mathbf{S}_n) = \mathrm{LC}(\mathbf{S}_n) - 1$ holds in Corollary 3.

Theorem 4. *If the minimal polynomial* $C(x)$ *of* $\mathbf{S}_n$ *is unique, then* $\mathrm{LA}(\mathbf{S}_n) = \mathrm{LC}(\mathbf{S}_n) - 1$ *if and only if* $C(1) = 0$.

Proof. The sufficiency of the condition $C(1) = 0$ for multisequences is shown in a similar way as in [5, Proposition 6] for single sequences. Now we prove the converse. Suppose $C(x) = x^d - c_{d-1}x^{d-1} - \cdots - c_0$, where $d := \mathrm{LC}(\mathbf{S}_n)$. Applying elementary column operations to the matrix A defined in the proof of Theorem 3 with $R = d$, we get a matrix

$$A' = \begin{pmatrix} s_2^{(1)} - s_1^{(1)} & s_3^{(1)} - s_2^{(1)} & \cdots & s_{n-d+1}^{(1)} - s_{n-d}^{(1)} & \cdots & s_2^{(m)} - s_1^{(m)} & \cdots & s_{n-d+1}^{(m)} - s_{n-d}^{(m)} \\ s_3^{(1)} - s_2^{(1)} & s_4^{(1)} - s_3^{(1)} & \cdots & s_{n-d+2}^{(1)} - s_{n-d+1}^{(1)} & \cdots & s_3^{(m)} - s_2^{(m)} & \cdots & s_{n-d+2}^{(m)} - s_{n-d+1}^{(m)} \\ \vdots & \vdots & & \vdots & & \vdots & & \vdots \\ s_{d+1}^{(1)} - s_d^{(1)} & s_{d+2}^{(1)} - s_{d+1}^{(1)} & \cdots & s_n^{(1)} - s_{n-1}^{(1)} & \cdots & s_{d+1}^{(m)} - s_d^{(m)} & \cdots & s_n^{(m)} - s_{n-1}^{(m)} \end{pmatrix}_{d \times m(n-d)}.$$

Since $\mathrm{LA}(\mathbf{S}_n) < d$, there exists a d-dimensional vector $(b_0, b_1, \ldots, b_{d-1}) \neq \mathbf{0}$ such that

$$b_{d-1}\beta_{d-1} + b_{d-2}\beta_{d-2} + \cdots + b_0\beta_0 = \mathbf{0},$$

where β_i denotes the $(i+1)$th row vector of A' for $0 \leqslant i \leqslant d-1$.

First we assume $b_{d-1} \neq 0$. From the above linear dependence relation we infer a recurrence relation, i.e.,

$$s_{j+d}^{(h)} = b_{d-1}^{-1}((b_{d-1} - b_{d-2})s_{j+d-1}^{(h)} + \cdots + (b_1 - b_0)s_{j+1}^{(h)} + b_0 s_j^{(h)})$$

for $1 \leqslant j \leqslant n-d$, $1 \leqslant h \leqslant m$. Since the minimal polynomial is unique by assumption, we get

$$c_0 + c_1 + \cdots + c_{d-1} = b_{d-1}^{-1}(b_{d-1} - b_{d-2} + \cdots + b_1 - b_0 + b_0) = 1,$$

that is, $C(1) = 0$. Finally we prove that $b_{d-1} = 0$ is impossible. Suppose we had $t := \max\{i : b_i \neq 0\} < d-1$. Put $N = n - d + t + 2$. Then

$$f(x) = b_t^{-1}(b_t x^{t+1} + (b_{t-1} - b_t)x^t + \cdots + (b_0 - b_1)x - b_0)$$

is a characteristic polynomial of $\mathbf{S}_N$. Hence $t + 1 \geqslant \mathrm{LC}(\mathbf{S}_N)$, and so

$$n + 1 - d = N - t - 1 \leqslant N - \mathrm{LC}(\mathbf{S}_N) < N + 1 - \mathrm{LC}(\mathbf{S}_N),$$

which is impossible by Lemma 1 and the fact that $M_1(\mathbf{S}_n) = d - n - 1$ (see Proposition 3). □

Example. We consider the following two sequences over the binary field $\mathbb{F}_2$:

$$S^{(1)} = 1\ 1\ 1\ 1\ 1\ 0\ 0\ 1,$$

$$S^{(2)} = 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1.$$

For this two-fold multisequence, we give a table of the three profiles we have studied in this paper.

n	2	3	4	5	6	7	8
LA($\mathbf{S}_n$)	1	1	1	1	2	3	4
SM($\mathbf{S}_n$)	(-1-1,-1)	(-2,-1,-1)	(-3,-1,-1)	(-4,-1,-1)	(-4,-2,-1)	(-4,-2,-2)	(-4,-3,-2)
LC($\mathbf{S}_n$)	2	2	2	2	5	6	6

5. Conclusions

In this paper we have seen that the joint linear complexity and Marsaglia's lattice level are closely related to some special value and the first value of the successive minima of the multisequence, respectively. Therefore the successive minima profile provides a powerful quality measure for the intrinsic structure of multisequences. For a single sequence, these three profiles yield essentially equivalent quality measures for pseudorandomness.

Acknowledgments

The authors would like to thank Gerhard Dorfer and Wilfried Meidl for helpful discussions. The research of the authors was supported by the DSTA Grant R-394-000-025-422 with Temasek Laboratories in Singapore. The research of the first author is also supported by 973 project (No. 2007CB807902) in China. Useful comments by two anonymous referees are gratefully acknowledged.

Appendix A. The LBRMS Algorithm

We summarize the LBRMS algorithm from [21,22] in the following pseudocode.
Input: m-fold multisequence $\mathbf{S}_n$.
Output: a minimal polynomial of $\mathbf{S}_n$.

---

1. Initialize: $\omega_1 \leftarrow \varepsilon_1, \ldots, \omega_m \leftarrow \varepsilon_m, \omega_{m+1} \leftarrow \alpha_n, r \leftarrow 0$.
2. While $\theta(\omega_1), \ldots, \theta(\omega_{m+1})$ are linearly dependent over $\mathbb{F}$ do
   Set $r \leftarrow r + 1$.
   (reduction step) Find a vector $(a_1, \ldots, a_m)$ such that $\theta(\omega_{m+1}) = \sum_{i=1}^{m} a_i\, \theta(\omega_i)$.
   Find an integer k such that $v(\omega_k) = \max\{v(\omega_i) : 1 \leqslant i \leqslant m, a_i \neq 0\}$.
      If $v(\omega_{m+1}) \geqslant v(\omega_k)$ then
         Set $\xi \leftarrow \omega_{m+1} - \sum_{i=1}^{m} a_i x^{-v(\omega_i)+v(\omega_{m+1})}\omega_i$.
      else
         Set $\xi \leftarrow x^{-v(\omega_{m+1})+v(\omega_k)}\omega_{m+1} - \sum_{i=1}^{m} a_i x^{-v(\omega_i)+v(\omega_k)}\omega_i$, $\omega_k \leftarrow \omega_{m+1}$.
      end if
      Set $\omega_{m+1} \leftarrow \xi$.
   end while
3. Set $t \leftarrow r$, $C(x) \leftarrow \eta(\omega_{m+1})$, output $C(x)$ and terminate the algorithm.

References

[1] R. Couture, P. L'Ecuyer, S. Tezuka, On the distribution of k-dimensional vectors for simple and combined Tausworthe sequences, Math. Comp. 60 (1993) 749–761 S11–S16.

[2] E. Dawson, L. Simpson, Analysis and design issues for synchronous stream ciphers, in: H. Niederreiter (Ed.), Coding Theory and Cryptology, World Scientific, Singapore, 2002, pp. 49–90.

[3] G. Dorfer, Lattice profile and linear complexity profile of pseudorandom number sequences, in: G.L. Mullen, A. Poli, H. Stichtenoth (Eds.), Finite Fields and Applications, Lecture Notes in Computer Science, vol. 2948, Springer, Berlin, 2004, pp. 69–78.

[4] G. Dorfer, W. Meidl, A. Winterhof, Counting functions and expected values for the lattice profile at n, Finite Fields Appl. 10 (2004) 636–652.

[5] G. Dorfer, A. Winterhof, Lattice structure and linear complexity profile of nonlinear pseudorandom number generators, Appl. Algebra Engrg. Comm. Comput. 13 (2003) 499–508.

[6] G. Dorfer, A. Winterhof, Lattice structure of nonlinear pseudorandom number generators in parts of the period, in: H. Niederreiter (Ed.), Monte Carlo and Quasi-Monte Carlo Methods 2002, Springer, Berlin, 2004, pp. 199–211.

[7] ECRYPT stream cipher project; available at: ⟨http://www.ecrypt.eu.org/stream⟩.

[8] F.-W. Fu, H. Niederreiter, On the counting function of the lattice profile of periodic sequences, J. Complexity, to appear.

[9] P. Hawkes, G.G. Rose, Exploiting multiples of the connection polynomial in word-oriented stream ciphers, in: T. Okamoto (Ed.), Advances in Cryptology—ASIACRYPT 2000, Lecture Notes in Computer Science, vol. 1976, Springer, Berlin, 2000, pp. 303–316.

[10] A.K. Lenstra, Factoring multivariate polynomials over finite fields, J. Comput. System Sci. 30 (1985) 235–248.

[11] K. Mahler, An analogue to Minkowski's geometry of numbers in a field of series, Ann. of Math. 42 (1941) 488–522.

[12] G. Marsaglia, The structure of linear congruential sequences, in: S.K. Zaremba (Ed.), Applications of Number Theory to Numerical Analysis, Academic Press, New York, 1972, pp. 249–285.

[13] W. Meidl, Continued fraction for formal Laurent series and the lattice structure of sequences, Appl. Algebra Engrg. Comm. Comput. 17 (2006) 29–39.

[14] W. Meidl, Enumeration results on linear complexity profiles and lattice profiles, J. Complexity 22 (2006) 275–286.

[15] W. Meidl, personal communication.

[16] H. Niederreiter, The probabilistic theory of the joint linear complexity of multisequences, in: G. Gong et al. (Ed.), Sequences and Their Applications—SETA 2006, Lecture Notes in Computer Science, vol. 4086, Springer, Berlin, 2006, pp. 5–16.

[17] H. Niederreiter, A. Winterhof, Lattice structure and linear complexity of nonlinear pseudorandom numbers, Appl. Algebra Engrg. Comm. Comput. 13 (2002) 319–326.

[18] R.A. Rueppel, Stream ciphers, in: G.J. Simmons (Ed.), Contemporary Cryptology: The Science of Information Integrity, IEEE Press, New York, 1992, pp. 65–134.

[19] W.M. Schmidt, Construction and estimation of bases in function fields, J. Number Theory 39 (1991) 181–224.

[20] L.-P. Wang, The vector key equation and multisequence shift register synthesis, in: M. Fossorier et al. (Ed.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science, vol. 3857, Springer, Berlin, 2006, pp. 68–75.

[21] L.-P. Wang, Y.-F. Zhu, $F[x]$-lattice basis reduction algorithm and multisequence synthesis, Sci. China Ser. F 44 (2001) 321–328.

[22] L.-P. Wang, Y.-F. Zhu, D.-Y. Pei, On the lattice basis reduction multisequence synthesis algorithm, IEEE Trans. Inform. Theory 50 (2004) 2905–2910.