On the joint linear complexity profile of explicit inversive multisequences

Wilfried Meidl\textsuperscript{a}, Arne Winterhof\textsuperscript{b,}\textsuperscript{*}

\textsuperscript{a}Temasek Laboratories, National University of Singapore, 5 Sports Drive 2, 117508 Singapore
\textsuperscript{b}Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstraße 69, A-4040 Linz, Austria

Received 27 April 2004; accepted 22 September 2004
Available online 23 December 2004

Abstract

We prove lower bounds on the joint linear complexity profile of multisequences obtained by explicit inversive methods and show that for some suitable choices of parameters these joint linear complexity profiles are close to be perfect.

© 2004 Elsevier Inc. All rights reserved.

Keywords: Linear complexity profile; Multisequences; Nonlinear pseudorandom numbers; Inversive method; Parallelization

1. Introduction

Let \( N \) be a positive integer and \( S = (\sigma_n)_{n=0}^{\infty} \) be a sequence with terms in a finite field \( \mathbb{F}_q \) of \( q \) elements. Then the \( N \)th linear complexity \( L_N(S) \) is the least order of a linear recurrence relation over \( \mathbb{F}_q \) that generates the first \( N \) terms of \( S \), i.e., \( L_N(S) \) is the smallest positive integer such that there exist coefficients \( \lambda_0, \ldots, \lambda_{L-1} \in \mathbb{F}_q \) with

\[
\sigma_{n+L} = \lambda_{L-1} \sigma_{n+L-1} + \cdots + \lambda_0 \sigma_n, \quad 0 \leq n \leq N - L - 1.
\]

\textsuperscript{*}Corresponding author.

E-mail addresses: wilfried.meidl@oeaw.ac.at (W. Meidl), arne.winterhof@oeaw.ac.at (A. Winterhof).

0885-064X/S - see front matter © 2004 Elsevier Inc. All rights reserved.
If $S$ starts with $N - 1$ zeros then we define $L_N(S) = 0$ if $\sigma_{N-1} = 0$ and $L_N(S) = N$ if $\sigma_{N-1} \neq 0$. The linear complexity $L(S)$ of $S$ is defined by

$$L(S) = \sup_{N \geq 1} L_N(S)$$

and the function $L(N) = L_N(S)$, $N \geq 1$, is called the linear complexity profile of $S$. For a periodic sequence $S$ of period $T$ we have

$$L_N(S) \leq T, \quad N \geq 1.$$ 

Linear complexity and linear complexity profile are important characteristics of a sequence for applications in cryptography and Monte Carlo methods (see [2,4,6,13,15–17]). Both, linear complexity and linear complexity profile of a given sequence can be determined with the well-known Berlekamp–Massey algorithm (see [1,7]). In [12,20] it has been shown that the expected value of the $N$th linear complexity of a random sequence is approximately $N/2$ and the linear complexity profile of a random sequence follows closely the $N/2$-line, where the increases of the linear complexity are performed symmetrical with respect to the $N/2$-line. This observation leads to the definition of the perfect linear complexity profile (cf. [11]). A sequence $S$ with terms in a finite field $\mathbb{F}_q$ is said to have a perfect linear complexity profile if $L_N(S) = \lfloor (N + 1)/2 \rfloor$, $N \geq 1$. Because of the symmetric increase behavior of the linear complexity it is sufficient to demand that $L_N(S) \geq N/2$, $N \geq 1$.

The concept of the linear complexity has been generalized to vector sequences or multisequences, i.e., $m$ parallel sequences $S_1, \ldots, S_m$ with terms in a finite field. Let $S = (S_1, \ldots, S_m)$ be $m$ sequences with terms in the finite field $\mathbb{F}_q$. Then the $N$th joint linear complexity $L_N(S) = L_N(S_1, \ldots, S_m)$ is the least order of a linear recurrence relation over $\mathbb{F}_q$ that simultaneously generates the first $N$ terms of each sequence $S_j$, $1 \leq j \leq m$. If no linear recurrence relation over $\mathbb{F}_q$ generates the first $N$ terms of each sequence simultaneously, then the $N$th joint linear complexity is defined to be $N$. The joint linear complexity $L(S) = L(S_1, \ldots, S_m)$ is defined by

$$L(S) = \sup_{N \geq 1} L_N(S)$$

and the function $L(N) = L_N(S)$, $N \geq 1$, is called the joint linear complexity profile of $S = (S_1, \ldots, S_m)$. An extension of the Berlekamp–Massey algorithm for multisequences is described in [5]. Recently, multisequences and their linear complexity became a wide research area (see [8,21,22,24], and for a recent comprehensive overview see [16]). In [24] the definition of the perfect linear complexity profile has been generalized to multisequences. A multisequence $S = (S_1, \ldots, S_m)$ with terms in a finite field $\mathbb{F}_q$ is said to have a perfect linear complexity profile if

$$L_N(S) \geq mN/(m + 1) \quad (1)$$

for all $N \geq 1$.

Let $q = p^r$ with a prime $p$ and a positive integer $r$. For a fixed basis $\{\gamma_1, \ldots, \gamma_r\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$ and $0 \leq n < q$ define

$$\zeta_n = n_1\gamma_1 + n_2\gamma_2 + \cdots + n_r\gamma_r.$$
respectively. The linear complexity profile of a single sequence defined as in (3) satisfies

\[ L_N(S_1) \geq \begin{cases} (N - 1)/3, & 1 \leq N \leq (3p - 7)/2, \\ N - p + 2, & (3p - 5)/2 \leq N \leq 2p - 3, \\ p - 1, & N \geq 2p - 2 \end{cases} \] (4)

and for \( r \geq 2, \)

\[ L_N(S_r) \geq \begin{cases} \lfloor \sqrt{N}/4 \rfloor + 1, & 2 \leq N \leq q - 2 + \sqrt{q - 2}/4, \\ N - q + 2, & q - 2 + \sqrt{q - 2}/4 < N \leq 2q - q/p - 2, \\ q - q/p, & N \geq 2q - q/p - 1, \end{cases} \] (5)

respectively. The linear complexity profile of a single sequence defined as in (3) satisfies

\[ L_N(Z) \geq \min \left( \frac{N - 1}{3}, \frac{t - 1}{2} \right). \] (6)

If \( \gamma \) is a primitive element we also know the improvement

\[ L_N(Z) \geq \min \left( q - \frac{q}{p}, N - q + \frac{q}{p} + 1 \right) \quad \text{if} \quad t = q - 1. \] (7)
Trivially the bounds (4)–(7) are lower bounds for the multisequence case.

For the multisequence $S_1$ we will improve bound (4) in Section 2. Section 3 deals with the multisequence $S_r$ for $r \geq 2$. Section 4 contains analogs for multisequence (3). For a suitable choice of the parameters $\alpha_i, \beta_i$ the lower bounds for $S_1$ and $Z$ are close to (1). Moreover, constructions of sequences and multisequences of the form $S_1$ and (3) are presented for which we can show that (1) is true as long as $N$ is not too large.

The results of this paper and the results of [14,19,23] on the statistical independence of parallel streams of explicit inversive generators suggest them as attractive candidates for parallelization if the parameters are carefully chosen.

2. The joint linear complexity profile of $S_1$

To present the results of this section we will use the following notation. Given a multisequence $S_1$ of form (2) we put

$$\beta_i' := \alpha_i^{-1} \beta_i, \quad 1 \leq i \leq m.$$  

We define $d_1$ and $D_1$ to be the minimal, respectively, maximal (Lee)-distance modulo $p$ between two $\beta_i'$'s, or more accurately for $m \geq 2$,

$$d_1 := \min_{1 \leq i < j \leq m} \min_{z \in \mathbb{Z}} |\beta_i' - \beta_j' + z|,$$

$$D_1 := \max_{1 \leq i < j \leq m} \min_{z \in \mathbb{Z}} |\beta_i' - \beta_j' + z|.$$  

For $m = 1$ we define $d_1 := D_1 := p$.

**Proposition 1.** Let $S_1$ be a multisequence of form (2). The $N$th linear complexity $L_N(S_1)$ of $S_1$ satisfies

$$L_N(S_1) \geq \min \left( \frac{mN - 1}{m + 2}, \frac{d_1m - 1}{2} \right), \quad N \geq 1.$$  

**Proof.** Suppose that $L_N(S_1) < N$ and

$$\sigma_{n+L}^{(i)} = \lambda_{L-1} \sigma_{n+L-1}^{(i)} + \cdots + \lambda_0 \sigma_n^{(i)}, \quad 0 \leq n \leq N - L - 1, \quad 1 \leq i \leq m,$$  

is a recurrence relation that jointly generates the first $N$ terms of the $m$ parallel sequences $(S_1, \ldots, S_m) = S_1$. With our definition of $\beta_i'$ this is equivalent to

$$-(n + \beta_i' + L)p^{-2} + \lambda_{L-1}(n + \beta_i' + L - 1)p^{-2} + \cdots + \lambda_0(n + \beta_i')p^{-2} = 0,$$  

$0 \leq n \leq N - L - 1, \quad 1 \leq i \leq m$. For pairs $(n, i)$ satisfying the condition

$$n + \beta_i' + j \not\equiv 0 \mod p \quad \text{for} \quad 0 \leq j \leq L$$

we can write (9) as

$$-(n + \beta_i' + L)^{-1} + \lambda_{L-1}(n + \beta_i' + L - 1)^{-1} + \cdots + \lambda_0(n + \beta_i')^{-1} = 0.$$
Thus all elements of the form

\[ u = n + \beta_i', \quad 0 \leq n \leq N - L - 1, \quad 1 \leq i \leq m \quad \text{and} \]
\[ u + j \not\equiv 0 \mod p \quad \text{for } 0 \leq j \leq L \]  \tag{10}

are roots of the polynomial

\[ f(x) = - (L - 1) \prod_{l=0}^{L-1} (x + l) + \lambda_{L-1} \prod_{l=0}^{L} (x + l) + \cdots + \lambda_0 \prod_{l=1}^{L} (x + l) \]  \tag{11}

of degree at most \( L \). For \( mN = 1 \) the result is trivial and for \( mN \geq 2 \) we obviously have \( L \geq 1 \). We may also assume \( L < p \). Hence,

\[ f(-L) = - \prod_{l=1}^{L} (-l) \neq 0 \]

and \( f(x) \) is not the zero polynomial over \( \mathbb{F}_p \). Consequently, \( L \) is at least the number \( K \) of different elements of form (10).

If \( N \leq d_1 + L \) then \( n_1 + \beta_{i_1}' \equiv n_2 + \beta_{i_2}' \mod p \) yields \( n_1 = n_2 \) and \( i_1 = i_2 \). Thus \( m(N - L) \) different elements are of the form \( u = n + \beta_i', \quad 0 \leq n \leq N - L - 1, \quad 1 \leq i \leq m \). At most \( L + 1 \) of those elements do not satisfy the condition \( u + j \not\equiv 0 \mod p \) for \( 0 \leq j \leq L \). Hence \( L \geq m(N - L) - (L + 1) \) which yields the desired formula.

If \( N > d_1 + L \) then

\[ L \geq L_N(S_1) \geq L_{d_1 + L}(S_1) \geq \frac{m(d_1 + L) - 1}{m + 2} \]

and the result follows. \( \square \)

If \( 1 \leq \beta_i' < p \) and \( N \leq p - \beta_j' \) for all \( 1 \leq i \leq m \), then no term \( n + l + \beta_i' \), \( 0 \leq n \leq N - L - 1 \), \( 0 \leq l \leq L \), is zero and slight modifications of the proof yield

\[ L_N(S_1) \geq \min \left( \frac{mN}{m + 1}, md_1 \right), \quad 1 \leq N \leq p - \max_{1 \leq i \leq m} \beta_i'. \]

Since

\[ \sigma_n^{(j)} = x_j^{-1} x_i \sigma_{n+\beta_j'-\beta_i'} \]

the sequence \( S_j \) is up to a multiplicative constant, which is not important for the linear complexity, a shift of \( S_j \) by \( \beta_j' - \beta_i' \) positions. Hence, the dependence of the lower bound on the Lee-distance of the \( \beta_i' \) is natural.

For larger \( N \) we can establish a better bound expressed in terms of \( D_1 \).

**Proposition 2.** Let \( S_1 \) be a multisequence of form (2). The \( N \)th linear complexity \( L_N(S_1) \) of \( S_1 \) satisfies

\[ L_N(S_1) \geq \min \left( N - D_1 + 1, \frac{p - 1}{2} \right), \quad N \geq 1. \]
Then the $N$th linear complexity $L_N(S_1)$ of $S_1$ is at least

$$
\begin{array}{l}
(mN - 1)/(m + 2), & 1 \leq N \leq \lfloor(m + 1)/2\rfloor, \\
(m - 1)/2, & \lceil(m + 3)/2\rceil \leq N \leq p - m + \lfloor(m - 1)/2\rfloor, \\
N - p + m, & p - m + \lfloor(m + 1)/2\rfloor \leq N \leq p - m + (p - 1)/2, \\
(p - 1)/2, & p - m + (p + 1)/2 \leq N \leq (3p - 5)/2, \\
N - p + 2, & (3p - 3)/2 \leq N \leq 2p - 3, \\
p - 1, & N \geq 2p - 2.
\end{array}
$$

In practice we may choose the parameters $\alpha_i$, $\beta_i$ in a best possible way. The next corollary describes this best case. However, Corollary 1 is still of theoretical interest.

**Corollary 2.** Let $S_1$ be a multisequence of form (2) such that

$$
\beta'_i = \beta'_1 + \left\lfloor \frac{(i - 1)p}{m} \right\rfloor, \quad i = 1, \ldots, m.
$$

Then the $N$th linear complexity $L_N(S_1)$ of $S_1$ is at least

$$
\begin{array}{l}
\frac{mN - 1}{m + 2}, & 1 \leq N \leq \lfloor((m + 2)[p/m] - m - 3)/2\rfloor, \\
N - \left\lfloor \frac{p}{m} \right\rfloor + 1, & \lfloor((m + 2)[p/m] - m - 1)/2\rfloor \leq N \leq (p - 3)/2 + \lceil p/m \rceil, \\
(p - 1)/2, & (p - 1)/2 + \lceil p/m \rceil \leq N \leq (3p - 5)/2, \\
N - p + 2, & (3p - 3)/2 \leq N \leq 2p - 3, \\
p - 1, & N \geq 2p - 2.
\end{array}
$$

3. The joint linear complexity profile of $S_r$, $r \geq 2$

With similar methods we can establish a nontrivial but somewhat weaker bound on the joint linear complexity profile of the multisequence $S_r$, $r \geq 2$, defined by (2). Again we put $\beta'_i = \alpha_i^{-1}\beta_i$, define $0 \leq n_i < q$ by $\beta'_i = \xi_{n_i}$, and let the minimal or maximal distance $d_r$ or
$D_r$, respectively, between two $\beta'_i$’s be

$$d_r := \min_{1 \leq i < j \leq m} \min_{z \in \mathbb{Z}} |n_i - n_j + zq|, \quad m \geq 2,$$

$$D_r := \max_{1 \leq i < j \leq m} \min_{z \in \mathbb{Z}} |n_i - n_j + zq|, \quad m \geq 2$$

and $D_r := d_r := q$ if $m = 1$.

First we prove an extension of Proposition 1.

**Proposition 3.** Let $S_r$, $r \geq 2$, be a multisequence of form (2). The $N$th linear complexity $L_N(S_r)$ of $S_r$ satisfies

$$L_N(S_r) \geq \min \left( \frac{N}{2} \sqrt{\frac{mN}{12}}, d_r, \sqrt{\frac{md_r}{12}} \right), \quad N \geq 1.$$  

**Proof.** We proceed as in the proof of Proposition 1. Again we can reduce the case $N \geq L + d_r + 1$ to the case $N \leq L + d_r$ and restrict ourselves to the latter case. In the considered case the recurrence relation (8) yields

$$(\xi_{n+L} + \beta'_i)^{q-2} = \lambda_{n+L-1}(\xi_{n+L-1} + \beta'_i)^{q-2} + \cdots + \lambda_0(\xi_n + \beta'_i)^{q-2}$$

for $0 \leq n \leq N - L - 1, 1 \leq i \leq m$. For those $n$ which additionally satisfy $\xi_{n+l} + \beta'_i \neq 0$ for $0 \leq l \leq L$ and any $1 \leq i \leq m$, this gives

$$-(\xi_{n+L} + \beta'_i)^{-1} + \lambda_{n+L-1}(\xi_{n+L-1} + \beta'_i)^{-1} + \cdots + \lambda_0(\xi_n + \beta'_i)^{-1} = 0$$

which yields

$$- \prod_{l=0}^{L-1} (\xi_{n+l} + \beta'_i) + \lambda_{n-L-1} \prod_{l=0}^{L} (\xi_{n+l} + \beta'_i) + \cdots + \lambda_0 \prod_{l=0}^{L} (\xi_{n+l} + \beta'_i) = 0.$$  

(12)

We exclusively consider those $n$, $0 \leq n \leq N - L - 1$, for which we additionally have $\xi_{n+l} = \xi_n + \xi_l$ for $0 \leq l \leq L$. Then (12) is equivalent to

$$- \prod_{l=0}^{L-1} (\xi_n + \beta'_i + \xi_l) + \lambda_{n-L-1} \prod_{l=0}^{L} (\xi_n + \beta'_i + \xi_l)$$

$$+ \cdots + \lambda_0 \prod_{l=1}^{L} (\xi_n + \beta'_i + \xi_l) = 0.$$  

Hence all elements of the form

$$u = \xi_n + \beta'_i$$

for any $0 \leq n \leq N - L - 1, 1 \leq i \leq m$, with

$$\xi_{n+l} = \xi_n + \xi_l$$

and $u + \xi_l \neq 0$ for $0 \leq l \leq L$. 


are roots of the polynomial
\[ f(x) = -\prod_{l=0}^{L-1} (x + \zeta_l) + \lambda_{n-L-1} \prod_{l \neq L-1}^{L} (x + \zeta_l) + \cdots + \lambda_0 \prod_{l=1}^{L} (x + \zeta_l) \]
of degree at most \( L \). Since \( f(-\xi_L) \neq 0 \) we see that \( f(x) \) is not the zero polynomial.

Let \( v, w \) and \( 1 \leq N_v, L_w < p \) be the integers defined by
\[ N_v p^v \leq N < (N_v + 1) p^v \quad \text{and} \quad L_w p^w \leq L < (L_w + 1) p^w. \]

Since \( L \leq N \) we have \( w \leq v \).

If \( w < v \) then we have \( \xi_{n+l} = \xi_n + \xi_l \) for all \( l = 0, \ldots, L \) for at least
\[ N_v (p - L_w) p^{v-w-1} > \frac{N_v}{N_v + 1} \frac{(p - L_w) L_w}{p} \frac{N}{L} \geq \frac{N}{4L} \]
distinct elements, namely, \( \xi_n \) with
\[ n = n_w p^w + \cdots + n_v p^v, \]
where
\[ 0 \leq n_{w+1}, \ldots, n_{v-1} < p, \ 0 \leq n_w < p - L_w, \ \text{and} \ 0 \leq n_v < N_v. \]

Hence, \( f(x) \) has at least
\[ \frac{mN}{4L} - L - 1 \]
zeros and we get \( 3L \geq 2L + 1 \geq mN/(4L) \). Thus
\[ L \geq \sqrt{\frac{mN}{12}} \quad \text{if} \quad w < v. \]

If \( w = v \) and \( L_v = N_v \) then we have
\[ L \geq N_v p^v > \frac{N_v}{N_v + 1} N > \frac{N}{2}. \]

If \( w = v, N_v \geq L_v + 1 \geq 2, \) and
\[ m > \left( \frac{3L_v}{N_v + 1} \right)^2 N \]
then we have \( \xi_{n+l} = \xi_n + \xi_l \) for all \( l = 0, \ldots, L \) for at least \( (N_v - L_v) \) distinct elements, namely \( \xi_n \) with \( n = n_v p^v, L_v \leq n_v < N_v \) and get
\[ L \geq \frac{m(N_v - L_v)}{3} > \sqrt{mN} \frac{(N_v - L_v) L_v}{N_v + 1} \geq \frac{\sqrt{mN}}{3}. \]
Otherwise we have

\[ L \geq L_v p^w > \frac{L_v}{N_v + 1} N \geq \sqrt{\frac{mN}{3}}. \]

Altogether we have

\[ L \geq \min \left( \frac{N}{2}, \frac{\sqrt{mN}}{3} \right) \text{ if } w = v. \]

So

\[ L \geq \min \left( \frac{N}{2}, \sqrt{\frac{mN}{12}} \right) \text{ if } N \leq L + d_r \]

and if \( N \geq L + d_r + 1 \) then \( L \geq L_N(S_r) \geq L_{d_r + L}(S_r) \) yields

\[ L \geq \min \left( d_r, \left( \frac{md_r}{12} + \left( \frac{m}{24} \right)^2 \right)^{1/2} + \frac{m}{24} \right) \]

and the result follows. \( \square \)

Now we extend Proposition 2.

**Proposition 4.** Let \( S_r, r \geq 2 \), be a multisequence of form (2). The \( N \)th linear complexity \( L_N(S_r) \) of \( S_r \) satisfies

\[ L_N(S_r) \geq \min \left( N - D_r + 1, \sqrt{\frac{q}{6}} \right), \quad N \geq 1. \]

**Proof.** We may assume \( L \leq \min(N - D_r, q - 1) \). We use the notation of the proof of Proposition 3. As in the proof of Proposition 2 the polynomial \( f(x) \) has at least

\[ (p - L_w)p^{r-w-1} - L - 1 \geq \frac{q}{2L} - 2L \]

zeros and the result follows. \( \square \)

Now we combine Propositions 3 and 4 and (5). We restrict ourselves to the case that \( d_r \) is not too small.

**Corollary 3.** Let \( S_r, r \geq 2 \), be a multisequence of form (2). The \( N \)th linear complexity \( L_N(S_1) \) of \( S_1 \) is at least

\[
\begin{cases}
[N/2], & 1 \leq N \leq \lfloor m/3 \rfloor, \\
\lfloor \sqrt{mN/12} \rfloor, & \lfloor m/3 \rfloor + 1 \leq N \leq d_r, \\
\lfloor \sqrt{md_r/12} \rfloor, & d_r + 1 \leq N \leq q - m + \lfloor \sqrt{md_r/12} \rfloor, \\
N - q + m, & q - m + 1 + \lfloor \sqrt{md_r/12} \rfloor \leq N \leq 2q - q/p - m, \\
q - q/p, & N \geq 2q - q/p - m + 1,
\end{cases}
\]

if \( d_r \geq m/12 \).
4. The joint linear complexity profile of $\mathbf{Z}$

Given a multisequence of form (3) we put $\mathbf{x}'_i := \mathbf{x}_i \beta_i^{-1}$, $i = 1, \ldots, r$. We define

$$\|\mathbf{z}\|_t = |n| \quad \text{if} \quad \mathbf{z} = \gamma^n \quad \text{with} \quad -\frac{t}{2} \leq n < \frac{t}{2}$$

and $|\mathbf{z}|_t = t$ if $\mathbf{z} \in \mathbb{F}_q^n$ is not of the form $\gamma^n$. Then we put for $m \geq 2$,

$$d_t := \min_{1 \leq i < j \leq m} \|\mathbf{x}_i \mathbf{x}_j^{-1}\|_t,$$

$$D_t := \max_{1 \leq i < j \leq m} \|\mathbf{x}_i \mathbf{x}_j^{-1}\|_t,$$

with the convention $d_t := D_t := t$ if $t = 1$. Propositions 5 and 6 are the analogs of Propositions 1 and 2 for multisequence (3).

**Proposition 5.** Let $\gamma \in \mathbb{F}_q^\ast$ be an element of order $t$ and $\mathbf{Z}$ a multisequence of form (3). The $N$th linear complexity $L_N(\mathbf{Z})$ of $\mathbf{Z}$ satisfies

$$L_N(\mathbf{Z}) \geq \min \left( \frac{Nm - 1}{m + 2}, \frac{d_t m - 1}{2}, t \right), \quad N \geq 1.$$

**Proof.** Suppose that $L_N(\mathbf{Z}) < N$ and

$$\sigma_{n+L}^{(i)} = \lambda_{L-1} \sigma_{n+L-1}^{(i)} + \cdots + \lambda_0 \sigma_n^{(i)}, \quad 0 \leq n \leq N - L - 1, \quad 1 \leq i \leq m$$

is a recurrence relation that jointly generates the first $N$ terms of the $m$ parallel sequences $(Z_1, \ldots, Z_m) = \mathbf{Z}$. With our definition of $\mathbf{x}'_i$ this yields

$$-(\mathbf{x}'_i \gamma^n L + 1)q^{-2} + \lambda_{L-1}(\mathbf{x}'_i \gamma^{n-1} L - 1)q^{-2} + \cdots + \lambda_0 (\mathbf{x}'_i \gamma^n + 1)q^{-2} = 0,$$

(13)

$0 \leq n \leq N - L - 1, 1 \leq i \leq m$. For those integers $n$ and indices $i$ that also satisfy $\mathbf{x}'_i \gamma^{n+l} \neq -1$ for $0 \leq l \leq L$, Eq. (13) can be written in the form

$$-(\mathbf{x}'_i \gamma^n L + 1)^{-1} + \lambda_{L-1}(\mathbf{x}'_i \gamma^{n-1} L - 1)^{-1} + \cdots + \lambda_0 (\mathbf{x}'_i \gamma^n + 1)^{-1} = 0.$$

Hence all elements of the form

$$u = \mathbf{x}'_i \gamma^n, \quad 0 \leq n \leq N - L - 1, \quad 1 \leq i \leq m$$

and

$$\mathbf{x}'_i \gamma^{n+l} \neq -1 \quad \text{for} \quad 0 \leq l \leq L$$

are roots of the polynomial

$$g(x) = -\prod_{l=0}^{L-1} (x \gamma^l + 1) + \lambda_{L-1} \prod_{l=0}^{L-1} (x \gamma^l + 1) + \cdots + \lambda_0 \prod_{l=0}^{L-1} (x \gamma^l + 1)$$

of degree at most $L$. Since $g(\gamma^{-L}) = -\prod_{l=0}^{L-1} (-\gamma^{-l} + 1) \neq 0$ if $1 \leq L < t$ the polynomial $g(x)$ is not the zero polynomial over $\mathbb{F}_q$. As in the proof of Proposition 1 we get
\( L_N(S) \geq (mN - 1)/(m + 2) \) if we assume \( N \leq d_t + L \) and \( L_N \geq (d_tm - 1)/2 \) if we assume \( N > d_t + L \). □

**Proposition 6.** Let \( \gamma \in \mathbb{F}_q^* \) be an element of order \( t \) and \( Z \) be a multisequence of form (3). The \( N \)th linear complexity \( L_N(Z) \) of \( Z \) satisfies

\[
L_N(Z) \geq \min \left( N - D_t + 1, \frac{t - 1}{2} \right), \quad N \geq 1.
\]

**Proof.** Substituting \( t \) for \( p \) and exchanging the additive group \( \mathbb{F}_p \) with the group generated by \( \gamma \) in the proof of Proposition 2 we get the requested bound. □

**Corollary 4** is the analog of Corollary 1.

**Corollary 4.** Let \( Z \) be a multisequence of form (3). The \( N \)th linear complexity \( L_N(Z) \) of \( Z \) is at least

\[
\begin{cases}
(mN - 1)/(m + 2), & 1 \leq N \leq [(m + 1)/2], \\
(m - 1)/2, & [(m + 3)/2] \leq N \leq t - m + [(m - 1)/2], \\
N - t + m, & t - m + [(m + 1)/2] \leq N \leq t - m + (t - 1)/2, \\
(t - 1)/2, & N \geq t - m + (p + 1)/2.
\end{cases}
\]

Now we consider the case when \( t < q - 1 \) only. If we assume that the coset which contains the element \(-1\) does not contain any \( \alpha_i' \), then we can improve the bound on \( L_N(Z) \). In this case \( \alpha_i' \gamma^{n+1} \) will never be \(-1\). Thus we do not have to exclude \( L + 1 \) values at the calculation of our bound and we will get \( L \geq m(N - L) \). We summarize this observation in the subsequent corollary.

**Corollary 5.** Let \( \gamma \) be an element of \( \mathbb{F}_q \) of order \( t < q - 1 \), let \( G = \langle \gamma \rangle \) be the multiplicative subgroup generated by \( \gamma \), and let \( Z \) be a multisequence of form (3). Suppose that for all \( 1 \leq i \leq m \), \( \alpha_i' \) is not an element of the coset of \( G \) which contains \(-1\). Then the \( N \)th linear complexity \( L_N(Z) \) of \( Z \) satisfies

\[
L_N(Z) \geq \min \left( \frac{mN}{m + 1}, md_t, t \right), \quad N \geq 1.
\]

Corollary 5 shows that in the considered case the sequence \( Z \) satisfies (1) for small values of \( N \).

If \( q - 1 = ht \) then we can choose \( m < h \) cosets of \( G = \langle \gamma \rangle \) which do not contain the element \(-1\). If each of those cosets contains exactly one \( \alpha_i' \) then for the resulting \( m \)-dimensional multisequence the minimal distance \( d_t \) equals \( t \). This leads to the following corollary.

**Corollary 6.** Let \( q - 1 = ht \), \( h > 1 \), let \( \gamma \in \mathbb{F}_q \) be an element of order \( t \), and let \( C_1, \ldots, C_m \), \( m < h \), be different cosets of the group \( G = \langle \gamma \rangle \) which do not contain the element \(-1\).
For $1 \leq i \leq m$ we choose exactly one $\gamma_i'$ in each of the cosets $C_i$. Then the resulting $m$-dimensional $t$-periodic multisequence $Z$ of form (3) satisfies

$$L_N(Z) \geq \min\left(\frac{mN}{m+1}, t\right), \quad N \geq 1.$$  

The multisequence constructed in Corollary 6 exhibits a perfect joint linear complexity profile until we reach $N = \lceil (m+1)t/m \rceil + 1$.

Finally, we mention an interesting property of some single inversive sequences of period $t < q - 1$.

**Corollary 7.** Let $\gamma \in \mathbb{F}_q$ be an element of order $t < q - 1$ and $x, \beta \in \mathbb{F}_q^*$ such that $x\beta^{-1}$ is not in the coset of $\langle \gamma \rangle$ containing $-1$. Then the linear complexity profile of any shifted sequence $Z_k$ of a sequence $Z$ defined by

$$y_n = (x\gamma^n + \beta y^{q-2}), \quad n \geq 0,$$

satisfies

$$L_N(Z_k) = \min\left(\left\lfloor \frac{N+1}{2} \right\rfloor, t\right), \quad N \geq 1.$$  

**Acknowledgments**

The paper was partially written during a visit of the second author to NUS. He wishes to thank the Department of Mathematics for the hospitality. The first author was supported by DSTA research grant R-394-000-011-422. The second author was supported by the Austrian Academy of Sciences and by the FWF research Grant S8313.

**References**


