Generalized Joint Linear Complexity of Linear Recurring Multisequences

Wilfried Meidl[1] and Ferruh Özbudak[2]

[1] Faculty of Engineering and Natural Sciences,
Sabancı University, Tuzla, 34956, İstanbul, Turkey
wmeidl@sabanciuniv.edu
[2] Department of Mathematics and Institute of Applied Mathematics,
Middle East Technical University, İnönü Bulvarı, 06531, Ankara, Turkey
ozbudak@metu.edu.tr

Abstract. The joint linear complexity of multisequences is an important security measure for vectorized stream cipher systems. Extensive research has been carried out on the joint linear complexity of N-periodic multisequences using tools from Discrete Fourier transform. Each N-periodic multisequence can be identified with a single N-periodic sequence over an appropriate extension field. It has been demonstrated that the linear complexity of this sequence, the so called generalized joint linear complexity of the multisequence, may be considerably smaller than the joint linear complexity, which is not desirable for vectorized stream ciphers. Recently new methods have been developed and results of greater generality on the joint linear complexity of multisequences consisting of linear recurring sequences have been obtained. In this paper, using these new methods, we investigate the relations between the generalized joint linear complexity and the joint linear complexity of multisequences consisting of linear recurring sequences.

1 Introduction

A sequence $S = s_0, s_1, \dots$ with terms in a finite field $\mathbb{F}_q$ with q elements (or over the finite field $\mathbb{F}_q$) is called a *linear recurring sequence* over $\mathbb{F}_q$ with *characteristic polynomial*

$$f(x) = \sum_{i=0}^{d} c_i x^i \in \mathbb{F}_q[x]$$

of degree d, if

$$\sum_{i=0}^{d} c_i s_{n+i} = 0 \quad \text{for } n = 0, 1, \dots .$$

Without loss of generality we can always assume that f is monic, i.e. $c_d = 1$. In accordance with the notation in [4] we denote the set of sequences over $\mathbb{F}_q$ with characteristic polynomial f by $\mathcal{M}_q^{(1)}(f)$. Let S be a linear recurring sequence over

S.W. Golomb et al. (Eds.): SETA 2008, LNCS 5203, pp. 266–277, 2008.

$\mathbb{F}_q$, i.e. $S \in \mathcal{M}_q^{(1)}(f)$ for some $f \in \mathbb{F}_q[x]$, then the *minimal polynomial* of S is defined to be the (uniquely determined) monic polynomial $d \in \mathbb{F}_q[x]$ of smallest degree such that $S \in \mathcal{M}_q^{(1)}(d)$. We remark that then d is a divisor of f. The degree of d is called the *linear complexity* $L(S)$ of the sequence S. Alternatively the linear complexity of a recurring sequence over $\mathbb{F}_q$ can be described as the length L of the shortest linear recurring relation with coefficients in $\mathbb{F}_q$ the sequence satisfies.

The concept of linear complexity is crucial in the study of the security of stream ciphers [13,14,15]. A keystream used in a stream cipher must have a high linear complexity to resist an attack by the Berlekamp-Massey algorithm [7].

Motivated by the study of vectorized stream cipher systems (see [2,5]) we consider the set $\mathcal{M}_q^{(m)}(f)$ of *m-fold multisequences* over $\mathbb{F}_q$ with joint characteristic polynomial f, i.e. m parallel sequences over $\mathbb{F}_q$ each of them being in $\mathcal{M}_q^{(1)}(f)$. The *joint minimal polynomial* of an m-fold multisequence $\mathbf{S} = (\sigma_1, \sigma_2, \ldots, \sigma_m)$ is then defined to be the (uniquely determined) monic polynomial d of least degree which is a characteristic polynomial for all sequences σ_r, $1 \leq r \leq m$. The *joint linear complexity* $L_q^{(m)}(\boldsymbol{S})$ of $\boldsymbol{S}$ is then the degree of d.

Extensive research has been carried out on the average behaviour of the linear complexity of a random sequence S and a random m-fold multisequence $\boldsymbol{S}$ in $\mathcal{M}_q^{(1)}(f)$ and $\mathcal{M}_q^{(m)}(f)$, respectively, for the special case that $f = x^N - 1$. Then $\mathcal{M}_q^{(1)}(f)$ and $\mathcal{M}_q^{(m)}(f)$ are precisely the sets of N-periodic sequences and N-periodic m-fold multisequences over $\mathbb{F}_q$. For the case of single N-periodic sequences we can refer to [1,9,10], for the case of N-periodic multisequences we refer to [3,11]. For the N-periodic case discrete Fourier transform turned out to be a convenient research tool.

Recently Fu, Niederreiter and Özbudak [4] developed new methods which made it possible to obtain results of greater generality. In fact in [4] expected value and variance for a random multisequence $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ are presented for an arbitrary characteristic polynomial f.

Let $\boldsymbol{S} = (\sigma_1, \sigma_2, \ldots, \sigma_m) \in \mathcal{M}_q^{(m)}(f)$ be an m-fold multisequence over $\mathbb{F}_q$, and for $r = 1, \ldots, m$ let $s_{r,i} \in \mathbb{F}_q$ denote the ith term of the rth sequence of $\boldsymbol{S}$, i.e. $\sigma_r = s_{r,0}s_{r,1}s_{r,2} \ldots$.

Since the $\mathbb{F}_q$-linear spaces $\mathbb{F}_q^m$ and $\mathbb{F}_{q^m}$ are isomorphic, the multisequence $\boldsymbol{S}$ can be identified with a single sequence $\mathcal{S}$ having its terms in the extension field $\mathbb{F}_{q^m}$, namely $\mathcal{S} = s_0, s_1, \ldots$ with

$$s_n = \xi_1 s_{1,n} + \cdots + \xi_m s_{m,n} \in \mathbb{F}_{q^m}, \quad n \geq 0, \tag{1}$$

where $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_m)$ is an ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. It is clear that $\mathcal{S}$ depends on the m-fold multisequence $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ and the ordered basis $\boldsymbol{\xi}$. Therefore we also denote $\mathcal{S}$ as $\mathcal{S}(\boldsymbol{S}, \boldsymbol{\xi})$.

Let $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})$ be the linear complexity of the sequence $\mathcal{S} = \mathcal{S}(\boldsymbol{S}, \boldsymbol{\xi}) \in \mathcal{M}_{q^m}^{(1)}(f)$. In accordance with [8] we call $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})$ the *generalized joint linear complexity of* $\boldsymbol{S}$ *(depending on* $\boldsymbol{\xi}$*)*. The generalized joint linear complexity $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})$ may be considerably smaller than $L_q^{(m)}(\boldsymbol{S})$ which is clearly not desirable for vectorized stream ciphers.

In [8] joint linear complexity and generalized joint linear complexity have been compared for the case of N-periodic multisequences. In particular conditions on the period have been presented for which generalized joint linear complexity always equals joint linear complexity, and a tight lower bound for the generalized joint linear complexity of an N-periodic multisequence with a given joint linear complexity has been established. As investigation tool a generalized discrete Fourier transform has been utilized. However this method is only applicable for the case of periodic sequences. In this article we will use the new approach and the methods of [4] to obtain similar results as in [8] for the much more general case of multisequences in $\mathcal{M}_q^{(m)}(f)$ with arbitrary characteristic polynomial f.

2 Preliminaries

Let $\boldsymbol{S} = (\sigma_1, \sigma_2, \ldots, \sigma_m) \in \mathcal{M}_q^{(m)}(f)$ be an m-fold multisequence with characteristic polynomial f, and suppose that $\sigma_r = s_{r,0}s_{r,1}s_{r,2}\ldots$, $1 \le r \le m$. Then there exist unique polynomials $g_r \in \mathbb{F}_q[x]$ with $\deg(g_r) < \deg(f)$ and $g_r/f = s_{r,0} + s_{r,1}x + s_{r,2}x^2 \ldots$, $1 \le r \le m$. By [12, Lemma 1] this describes a one-to-one correspondence between the set $\mathcal{M}_q^{(m)}(f)$ and the set of m-tuples of the form $\left(\frac{g_1}{f}, \frac{g_2}{f}, \ldots, \frac{g_m}{f}\right)$, $g_r \in \mathbb{F}_q[x]$ and $\deg(g_r) < \deg(f)$ for $1 \le r \le m$.

If $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ corresponds to $(g_1/f, g_2/f, \ldots, g_m/f)$ then the joint minimal polynomial d of $\boldsymbol{S}$ is the unique polynomial in $\mathbb{F}_q[x]$ for which there exist $h_1, \ldots, h_m \in \mathbb{F}_q[x]$ with $g_r/f = h_r/d$ for $1 \le r \le m$ and $\gcd(h_1, \ldots, h_m, d) = 1$. The joint linear complexity of $\boldsymbol{S}$ is then given by $L_q^{(m)}(\boldsymbol{S}) = \deg(f) - \deg(\gcd(g_1, g_2, \ldots, g_m, f))$.

Let again $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ correspond to $(g_1/f, g_2/f, \ldots, g_m/f)$, then it is easily seen that the single sequence $\mathcal{S} \in \mathcal{M}_{q^m}^{(1)}(f)$ defined as in (1) corresponds to the 1-tuple (G/f) with

$$G = g_1\xi_1 + g_2\xi_2 + \cdots + g_m\xi_m.$$

The minimal polynomial of $\mathcal{S}$ is then $D = f/\gcd(G, f) \in \mathbb{F}_{q^m}[x]$ and $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S}) = \deg(f) - \deg(\gcd(G, f))$, where the greatest common divisor is now calculated in $\mathbb{F}_{q^m}[x]$.

It is clear that divisibility of polynomials in $\mathbb{F}_q[x]$ and $\mathbb{F}_{q^m}[x]$ plays a crucial role. We will use the following two propositions on divisibility.

Proposition 1. *Let m be a positive integer and $r \in \mathbb{F}_q[x]$ be an irreducible polynomial. Let $u = \gcd(m, \deg(r))$. Then the canonical factorization of r into irreducibles over $\mathbb{F}_{q^m}$ is of the form*

$$r = r_1 r_2 \ldots r_u,$$

where $r_1, \ldots, r_u \in \mathbb{F}_{q^m}[x]$ are distinct irreducible polynomials with

$$\deg(r_1) = \cdots = \deg(r_u) = \frac{\deg(r)}{u}.$$

Proof. This is just a restatement of [6, Theorem 3.46]. We refer to [6] for a proof. □

Proposition 2. *Let m be a positive integer, let $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_m)$ be an ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and let $h_1, \ldots, h_m \in \mathbb{F}_q[x]$ be arbitrary polynomials. For $h \in \mathbb{F}_q[x]$, there exists $s \in \mathbb{F}_{q^m}[x]$ such that*

$$sh = \xi_1 h_1 + \cdots + \xi_m h_m$$

if and only if there exist $s_1, \ldots, s_m \in \mathbb{F}_q[x]$ such that

$$s_i h = h_i \text{ for } 1 \leq i \leq m.$$

Proof. For a polynomial $s \in \mathbb{F}_{q^m}[x]$ let $s_1, \ldots, s_m \in \mathbb{F}_q[x]$ be the uniquely determined polynomials in $\mathbb{F}_q[x]$ such that

$$s = \xi_1 s_1 + \cdots + x_m s_m.$$

Then

$$sh = \xi_1 s_1 h + \cdots + x_m s_m h$$

is the unique representation in the basis $\boldsymbol{\xi}$ of the polynomial sh and the claim immediately follows. □

Finally we recall an important definition from [4]. For a monic polynomial $f \in \mathbb{F}_q[x]$ and a positive integer m we let $\Phi_q^{(m)}(f)$ denote the number of m-fold multisequences over $\mathbb{F}_q$ with minimal joint polynomial f. Note that $\Phi_q^{(m)}(f)$ can be considered as a function on the set of monic polynomials in $\mathbb{F}_q[x]$. In [4, Section 2] several important properties of $\Phi_q^{(m)}(f)$ have been derived, which we will use in this paper. We refer to [4] for further details.

3 Generalized Joint Linear Complexity

In this section we obtain our main results and we give illustrative examples. The following three lemmas will be used in the proof of the next theorem.

Lemma 1. *For an integer $n \geq 2$, let $H_n(x)$ be the real valued function on $\mathbb{R}$ defined by*

$$H_n(x) = x^n - 1 - (x-1)^n.$$

For a real number $x > 1$, we have $H_n(x) > 0$.

Proof. We prove by induction on n. The case $n = 2$ is trivial and hence we assume that $n \geq 3$ and the lemma holds for $n-1$. For the derivative we have

$$\frac{dH_n}{dx} = nx^{n-1} - n(x-1)^{n-1} = n\left(H_{n-1}(x) + 1\right). \tag{2}$$

By the induction hypothesis we have that $H_{n-1}(x) > 0$, for $x > 1$. Therefore using (2) we complete the proof. □

Lemma 2. *Let $q \geq 2$ be a prime power. Let a and $n \geq 2$ be positive integers. Then*

$$1 - \frac{1}{q^{na}} > \left(1 - \frac{1}{q^a}\right)^n.$$

Proof. Let $H_n(x)$ be the real valued function on $\mathbb{R}$ defined in Lemma 1. Note that $q^a > 1$ and

$$H_n\left(q^a\right) = q^{na} - 1 - \left(q^a - 1\right)^n.$$

Therefore using Lemma 1 we obtain that

$$q^{na} - 1 > \left(q^a - 1\right)^n. \tag{3}$$

Dividing both sides of (3) by q^{na} we complete the proof. □

Lemma 3. *Let $r \in \mathbb{F}_q[x]$ be an irreducible polynomial. For positive integers m and e we have*

$$\Phi_q^{(m)}(r^e) = \Phi_{q^m}^{(1)}(r^e) \textit{ if } \gcd(\deg(r), m) = 1, \quad \textit{and}$$

$$\Phi_q^{(m)}(r^e) > \Phi_{q^m}^{(1)}(r^e) \textit{ if } \gcd(\deg(r), m) > 1.$$

Proof. It follows from [4, Lemma 2.2, (iii)] that

$$\Phi_q^{(m)}(r^e) = q^{me\deg(r)}\left(1 - \frac{1}{q^{m\deg(r)}}\right). \tag{4}$$

If $\gcd(\deg(r), m) = 1$, then, by Proposition 1, r is irreducible over $\mathbb{F}_{q^m}$ as well and hence using [4, Lemma 2.2, (iii)] again we obtain that $\Phi_{q^m}^{(1)}(r^e) = \Phi_q^{(m)}(r^e)$.

Assume that $u := \gcd(\deg(r), m) > 1$. It follows from Proposition 1 that the canonical factorization of r into irreducibles over $\mathbb{F}_{q^m}$ is of the form

$$r = t_1 t_2 \dots t_u,$$

and $\deg(t_1) = \cdots = \deg(t_u) = \deg(r)/u$. Using [4, Lemma 2.2, (iii)] we have

$$\Phi_{q^m}^{(1)}(r^e) = q^{me\deg(r)}\left(1 - \frac{1}{q^{m\deg(r)/u}}\right)^u. \tag{5}$$

Therefore using Lemma 2, (4) and (5) we complete the proof. □

The following theorem determines the exact conditions on m and $f \in \mathbb{F}_q[x]$ for which the joint linear complexity and the generalized joint linear complexity on $\mathcal{M}_q^{(m)}(f)$ are the same.

Theorem 1. *Let m be a positive integer, let $f \in \mathbb{F}_q[x]$ be a monic polynomial with $\deg(f) \geq 1$, let*

$$f = r_1^{e_1} r_2^{e_2} \dots r_k^{e_k}$$

be the canonical factorization of f into irreducibles, and let $\boldsymbol{\xi} = (\xi_1, \dots, \xi_m)$ be an ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then we have

$$L_q^{(m)}(\boldsymbol{S}) = L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S}) \quad \textit{for each } \boldsymbol{S} \in \mathcal{M}_q^{(m)}(f),$$

if and only if

$$\gcd(m, \deg(r_i)) = 1, \quad \textit{for } i = 1, 2, \dots, k. \tag{6}$$

Proof. We first assume that $\gcd(m, \deg(r_i)) = 1$ for $i = 1, 2, \dots, k$. Let $\boldsymbol{S} = (\sigma_1, \sigma_2, \dots, \sigma_m)$ be an arbitrary multisequence in $\mathcal{M}_q^{(m)}(f)$, and let $g_1, g_2, \dots, g_m$ be the polynomials in $\mathbb{F}_q[x]$ such that $\boldsymbol{S}$ corresponds to the m-tuple $(g_1/f, g_2/f, \dots, g_m/f)$ as described in Section 2. The joint minimal polynomial of $\boldsymbol{S}$ is then the (uniquely determined) monic polynomial $d \in \mathbb{F}_q[x]$ dividing f such that

$$h_i/d = g_i/f, \quad \text{for } i = 1, 2, \dots, m, \quad \text{and} \quad \gcd(h_1, h_2, \dots, h_m, d) = 1, \tag{7}$$

for certain polynomials $h_1, h_2, \dots, h_m$ in $\mathbb{F}_q[x]$. The sequence $\mathcal{S} = \mathcal{S}(\boldsymbol{S}, \boldsymbol{\xi})$ defined as in Section 1 depending on $\boldsymbol{S}$ and $\boldsymbol{\xi}$ then corresponds to

$$\frac{G}{f} = \frac{\xi_1 g_1 + \xi_2 g_2 + \dots + \xi_m h_m}{f} = \frac{\xi_1 h_1 + \xi_2 h_2 + \dots + \xi_m h_m}{d}.$$

We have to show that d is also the minimal polynomial of $\mathcal{S} \in \mathcal{M}_{q^m}^{(1)}(f)$, or equivalently that d and $\xi_1 h_1 + \xi_2 h_2 + \dots + \xi_m h_m$ are relatively prime in $\mathbb{F}_{q^m}[x]$. From (6) and Proposition 1 the canonical factorizations of f are the same over both fields, $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$. Consequently this also applies to the divisor d of f. If d and $\xi_1 h_1 + \xi_2 h_2 + \dots + \xi_m h_m$ are not relatively prime in $\mathbb{F}_{q^m}[x]$ then there exists a common factor in $\mathbb{F}_q[x]$ which contradicts (7) by Proposition 2.

We show the converse with a simple counting argument. Let $\boldsymbol{S_1}$ and $\boldsymbol{S_2}$ be distinct multisequences in $\mathcal{M}_q^{(m)}(f)$ both having minimal polynomial f. If $L_q^{(m)}(\boldsymbol{S}) = L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})$ for all elements $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$, then the distinct sequences $\mathcal{S}_1, \mathcal{S}_2 \in \mathcal{M}_{q^m}^{(1)}(f)$ corresponding to $\boldsymbol{S_1}$ and $\boldsymbol{S_2}$, respectively, will also have f as their minimal polynomial. By [4, Theorem 4.1] the numbers $\Phi_q^{(m)}(f)$ and $\Phi_{q^m}^{(1)}(f)$ of elements in $\mathcal{M}_q^{(m)}(f)$ and $\mathcal{M}_{q^m}^{(1)}(f)$, respectively, with minimal polynomial f are given by

$$\Phi_q^{(m)}(f) = \prod_{i=1}^{k} \Phi_q^{(m)}(r_i^{e_i}) \quad \text{and} \quad \Phi_{q^m}^{(1)}(f) = \prod_{i=1}^{k} \Phi_{q^m}^{(1)}(r_i^{e_i}).$$

With Lemma 3 we see that $\Phi_{q^m}^{(1)}(f) < \Phi_q^{(m)}(f)$ if condition (6) does not hold, which completes the proof. □

Remark 1. For each $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$, we always have

$$L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S}) \le L_q^{(m)}(\boldsymbol{S}).$$

In Theorem 2 below we also derive tight lower bounds on $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})$ (see also Proposition 3 below).

Remark 2. Theorem 1 implies that the choice of f as a product of powers of irreducible polynomials $r_1, r_2, \ldots, r_k$ such that $\deg(r_1) = \cdots = \deg(r_k)$ is a (large) prime guarantees that generalized joint linear complexity is not smaller than joint linear complexity for any multisequence $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ if $m < \deg(r_i)$.

The following theorem gives a lower bound for the generalized joint linear complexity of a multisequence $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ with given minimal polynomial d.

Theorem 2. *Let f be a monic polynomial in $\mathbb{F}_q[x]$ with canonical factorization into irreducible monic polynomials over $\mathbb{F}_q$ given by*

$$f = r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k},$$

and let $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ be an m-fold multisequence over $\mathbb{F}_q$ with joint minimal polynomial

$$d = r_1^{a_1} r_2^{a_2} \cdots r_k^{a_k}, \quad 0 \le a_i \le e_i \text{ for } 1 \le i \le k.$$

The generalized joint linear complexity $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})$ of $\boldsymbol{S}$ is then lower bounded by

$$L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S}) \ge \sum_{i=1}^{k} a_i \frac{deg(r_i)}{\gcd(\deg(r_i), m)}.$$

Proof. As the multisequence $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ has joint minimal polynomial d, we can uniquely associate $\boldsymbol{S}$ with an m-tuple $\left(\frac{h_1}{d}, \frac{h_2}{d}, \ldots, \frac{h_m}{d}\right)$ with $h_t \in \mathbb{F}_q[x]$, $\deg(h_t) < \deg(d)$ for $1 \le t \le m$, and $\gcd(h_1, \ldots, h_m, d) = 1$. If $a_i > 0$ then r_i does not divide all of the polynomials $h_1, \ldots, h_m$. Hence by Proposition 2 the polynomial r_i does not divide the polynomial $H = h_1\xi_1 + h_2\xi_2 + \cdots + h_m\xi_m$ over the extension field $\mathbb{F}_{q^m}$. Therefore if $r_i = t_{i,1}t_{i,2}\cdots t_{i,u_i}$ is the canonical factorization of r_i over $\mathbb{F}_{q^m}$, where $u_i = \gcd(\deg(r_i), m)$ and $\deg(t_{i,j}) = \deg(r_i)/u_i$ by Proposition 1, at least for one j, $1 \le j \le u_i$, we have $t_{i,j} \nmid H$. Consequently $t_{i,j}^{a_i}$ and H are relatively prime in $\mathbb{F}_{q^m}[x]$ which yields the lower bound for $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})$. □

The following proposition shows that the lower bound of Theorem 2 is tight.

Proposition 3. *Let f be a monic polynomial in $\mathbb{F}_q[x]$ with canonical factorization into irreducible monic polynomials over $\mathbb{F}_q$ given by*

$$f = r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k}.$$

Let $a_1, a_2, \ldots, a_k$ be integers with $0 \le a_i \le e_i$ for $1 \le i \le k$. Let $m \ge 2$ be an integer and $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_m)$ be an ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. There exists an m-fold multisequence $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ over $\mathbb{F}_q$ such that its joint minimal polynomial d is

$$d = r_1^{a_1} r_2^{a_2} \ldots r_k^{a_k},$$

and its generalized joint linear complexity $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})$ is

$$L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S}) = \sum_{i=1}^{k} a_i \frac{\deg(r_i)}{\gcd(\deg(r_i), m)}.$$

Proof. By reordering $r_1, \ldots, r_k$ suitably, we can assume without loss of generality that there exists an integer l, $1 \le l \le k$, with $\gcd(m, \deg(r_i)) = u_i \ge 2$ for $1 \le i \le l$ and $\gcd(m, \deg(r_i)) = 1$ for $l+1 \le i \le k$. Indeed otherwise $\gcd(m, \deg(r_i)) = 1$ for $1 \le i \le k$ and hence the result is trivial by Theorem 1. Using Proposition 1 we obtain that the canonical factorizations of r_i, $1 \le i \le l$, into irreducibles over $\mathbb{F}_{q^m}$ are of the form

$$r_i = t_{i,1} t_{i,2} \ldots t_{i,u_i}.$$

Let $\mathcal{S}$ be the sequence in $\mathcal{M}_{q^m}^{(1)}(f)$ corresponding to the polynomial

$$G = \frac{f}{d} \prod_{i=1}^{l} (t_{i,2} \ldots, t_{i,u_i})^{a_i} \in \mathbb{F}_{q^m}[x]$$

and let $h_1, h_2, \ldots, h_m \in \mathbb{F}_q[x]$ be the uniquely determined polynomials in $\mathbb{F}_q[x]$ such that

$$\prod_{i=1}^{l} (t_{i,2} \ldots, t_{i,u_i})^{a_i} = \xi_1 h_1 + \xi_2 h_2 + \cdots + \xi_m h_m. \tag{8}$$

Let $\boldsymbol{S} = (\sigma_1, \ldots, \sigma_m) \in \mathcal{M}_q^{(m)}(f)$ be the m-fold multisequence such that the sequence σ_i corresponds to $g_i = h_i f/d \in \mathbb{F}_q[x]$ for $1 \le i \le m$. We observe that we have $\mathcal{S} = \mathcal{S}(\boldsymbol{S}, \boldsymbol{\xi})$ and

$$L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S}) = \sum_{i=1}^{l} a_i \deg(t_{i,1}) + \sum_{i=l+1}^{k} a_i \deg(r_i).$$

Moreover d is the joint minimal polynomial of $\boldsymbol{S}$. Indeed, otherwise using (8) we obtain that there exists $1 \le i \le k$ with

$$r_i \mid \prod_{i=1}^{l} (t_{i,2} \ldots, t_{i,u_i})^{a_i} \text{ in } \mathbb{F}_{q^m}[x].$$

This is a contradiction, which completes the proof. □

In the following corollary we consider $\frac{L_q^{(m)}(\boldsymbol{S}) - L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})}{L_q^{(m)}(\boldsymbol{S})}$, the difference of joint linear complexity and generalized joint linear complexity in relation to the value for the joint linear complexity. We give a uniform and tight upper bound which applies to arbitrary nonzero multisequences in $\mathcal{M}_q^{(m)}(f)$.

Corollary 1. *Let $m \geq 2$ be an integer and f be a monic polynomial in $\mathbb{F}_q[x]$ with canonical factorization into irreducible monic polynomials over $\mathbb{F}_q$ given by*

$$f = r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k}$$

with

$$u_{\max} = \max\{\gcd(\deg(r_i), m) : 1 \leq i \leq k\}.$$

Then for an arbitrary nonzero multisequence $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ and an ordered basis $\boldsymbol{\xi}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ we have

$$\frac{L_q^{(m)}(\boldsymbol{S}) - L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})}{L_q^{(m)}(\boldsymbol{S})} \leq 1 - \frac{1}{u_{\max}}. \tag{9}$$

Moreover the bound in (9) is tight.

Proof. For any nonzero m-fold multisequence $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$, its joint minimal polynomial d is of the form

$$d = r_1^{a_1} r_2^{a_2} \ldots r_k^{a_k},$$

where $0 \leq a_i \leq e_i$ are integers and $(a_1, \ldots, a_k) \neq (0, \ldots, 0)$. Therefore, using Theorem 2, for its joint linear complexity $L_q^{(m)}(\boldsymbol{S})$ and its generalized joint linear complexity $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})$ we obtain that

$$L_q^{(m)}(\boldsymbol{S}) = \sum_{i=1}^{k} a_i \deg(r_i), \quad \text{and} \quad L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S}) \geq \sum_{i=1}^{k} a_i \frac{\deg(r_i)}{\gcd(\deg(r_i), m)}. \tag{10}$$

It follows from the definition of $u_{\max}$ that

$$\frac{1}{u_{\max}} a_i \deg(r_i) \leq a_i \frac{\deg(r_i)}{\gcd(\deg(r_i), m)} \tag{11}$$

for $1 \leq i \leq k$. Combining (10) and (11) we obtain (9). Moreover let $a_1, \ldots, a_k$ be integers such that

$$a_i = \begin{cases} 0 & \text{if } \gcd(\deg(r_i), m) \neq u_{\max}, \\ \neq 0 & \text{if } \gcd(\deg(r_i), m) = u_{\max}. \end{cases} \tag{12}$$

For integers $a_1, \ldots, a_k$ as in (12) we have equality in (11). Using Proposition 3 we obtain an m-fold multisequence $\boldsymbol{S}_{u_{\max}} \in \mathcal{M}_q^{(m)}(f)$ such that we have equality for $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})$ in (10), where the integers $a_1, \ldots, a_k$ are as in (12). Hence we conclude that the bound in (9) is attained by $\boldsymbol{S}_{u_{\max}}$, which completes the proof. □

Remark 3. If condition (6) is satisfied then (9) will be zero for all multisequences $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$. As $\gcd(\deg(r_i), m)$ can at most be m the largest possible relative distance between joint linear complexity and generalized joint linear complexity of an m-fold multisequence is given by $(m-1)/m$.

We give two examples illustrating our results.

Example 1. Let N, m be positive integers and consider the N-periodic m-fold multisequences over $\mathbb{F}_q$. Equivalently, let $f = x^N - 1 \in \mathbb{F}_q[x]$ and we can consider the multisequences in $\mathcal{M}_q^{(m)}(f)$. Let p be the characteristic of the finite field $\mathbb{F}_q$ and $N = p^v n$ with $\gcd(n, p) = 1$. Then we have $x^N - 1 = (x^n - 1)^{p^v}$, and the canonical factorization of $x^n - 1$ in $\mathbb{F}_q[x]$ is given by

$$x^n - 1 = \prod_{i=1}^{k} r_i(x) \quad \text{with} \quad r_i(x) = \prod_{j \in C_i} (x - \alpha^j),$$

where $C_1, \ldots, C_k$ are the different cyclotomic cosets modulo n relative to powers of q and α is a primitive nth root of unity in some extension field of $\mathbb{F}_q$. Let $\boldsymbol{S}$ be an N-periodic m-fold multisequence over $\mathbb{F}_q$ with minimal polynomial $d = r_1^{\rho_1} r_2^{\rho_2} \cdots r_k^{\rho_k}$, where $0 \le \rho_i \le p^v$. Then using Theorem 2 we have

$$L(\boldsymbol{S}) \ge \sum_{i=1}^{k} \rho_i \frac{l_i}{\gcd(l_i, m)}, \tag{13}$$

where l_i denotes the cardinality of the cyclotomic coset C_i. Equation (13) coincides with the corresponding result in [8, Theorem 2].

Example 2. Let $r_1, \ldots, r_k \in \mathbb{F}_q[x]$ be distinct irreducible polynomials and let $e_1, \ldots, e_k$ be positive integers. For a positive integer m, let

$$f = r_1^{e_1} r_2^{e_2} \ldots r_k^{e_k},$$

and consider the multisequences in $\mathcal{M}_q^{(m)}(f)$. It is not difficult to observe that there exists a multisequence $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ with joint linear complexity $L_q^{(m)}(\boldsymbol{S}) = t$ if and only if t can be written as

$$t = i_1 \deg(r_1) + i_2 \deg(r_2) + \cdots + i_k \deg(r_k), \tag{14}$$

where $0 \le i_1 \le e_1, \ldots, 0 \le i_k \le e_k$ are integers. Let $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_m)$ be an ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let $0 \le i_1 \le e_1, \ldots, 0 \le i_k \le e_k$ be chosen integers. Consider the nonempty subset $\mathcal{T}(i_1, \ldots, i_k)$ of $\mathcal{M}_q^{(m)}(f)$ consisting of $\boldsymbol{S}$ such that $L_q^{(m)}(\boldsymbol{S}) = t$, where t is as in (14). Using the methods of this paper we obtain that, among the multisequences in $\mathcal{T}(i_1, \ldots, i_k)$, there exists a multisequence $\boldsymbol{S}$ with generalized joint linear complexity $L_{q^m, \boldsymbol{\xi}}(\boldsymbol{S}) = \tilde{t}$ if and only if $\tilde{t}$ can be written as

$$\tilde{t} = i_1 j_1 \frac{\deg(r_1)}{\gcd(\deg(r_1), m)} + i_2 j_2 \frac{\deg(r_2)}{\gcd(\deg(r_2), m)} + \cdots + i_k j_k \frac{\deg(r_k)}{\gcd(\deg(r_k), m)},$$

where $1 \le j_1 \le \gcd(\deg(r_1), m), \ldots, 1 \le j_k \le \gcd(\deg(r_k), m)$ are integers.

Remark 4. The results above do not depend on the choice of the basis. However the generalized joint linear complexity actually depends on the basis. The following simple example illustrates this fact.

Example 3. Let $\boldsymbol{S} = (\sigma_1, \sigma_2, \sigma_3)$ be the 7-periodic 3-fold multisequence over $\mathbb{F}_2$ given by

$$\begin{aligned} \sigma_1 &= 1\ 0\ 0\ 1\ 0\ 1\ 1 \cdots \\ \sigma_2 &= 0\ 1\ 0\ 1\ 1\ 1\ 0 \cdots \\ \sigma_3 &= 0\ 0\ 1\ 0\ 1\ 1\ 1 \cdots . \end{aligned}$$

Let $\alpha \in \mathbb{F}_8$ with $\alpha^3 + \alpha + 1 = 0$. Consider the ordered bases $\boldsymbol{\xi}_1 = (1, \alpha, \alpha^2)$ and $\boldsymbol{\xi}_2 = (\alpha, 1, \alpha^2 + 1)$ of $\mathbb{F}_8$ over $\mathbb{F}_2$. The 7-periodic sequences over $\mathbb{F}_8$ obtained from $\boldsymbol{S}$ using the bases $\boldsymbol{\xi}_1$ and $\boldsymbol{\xi}_2$ are

$$\begin{aligned} \mathcal{S}_1 &:= \mathcal{S}\left(\boldsymbol{S}, \boldsymbol{\xi}_1\right) = 1, \alpha, \alpha^2, \alpha+1, \alpha^2+\alpha, \alpha^2+\alpha+1, \alpha^2+1, \cdots \quad \text{and} \\ \mathcal{S}_2 &:= \mathcal{S}\left(\boldsymbol{S}, \boldsymbol{\xi}_2\right) = \alpha, 1, \alpha^2+1, \alpha+1, \alpha^2, \alpha^2+\alpha, \alpha^2+\alpha+1, \cdots . \end{aligned}$$

For the terms of $\mathcal{S}_1$ we have $s_{n+1} = \alpha s_n$, where $n \geq 0$, and hence $L_{8,\boldsymbol{\xi}_1}(\boldsymbol{S}) = 1$.

The first three terms of $\mathcal{S}_2$ are $s_0 = \alpha$, $s_1 = (\alpha^2+1)s_0$ and $s_2 = (\alpha^2+1)s_1$. However for the third term of $\mathcal{S}_2$ we have $s_3 \neq (\alpha^2+1)s_2$ and hence $L_{8,\boldsymbol{\xi}_2}(\boldsymbol{S}) > 1$.

Acknowledgments

We would like to thank Arne Winterhof for very useful suggestions. The second author was partially supported by TÜBİTAK under Grant No. TBAG-107T826.

References

1. Davies, D.W. (ed.): EUROCRYPT 1991. LNCS, vol. 547, pp. 168–175. Springer, Heidelberg (1991)
2. Dawson, E., Simpson, L.: Analysis and design issues for synchronous stream ciphers. In: Niederreiter, H. (ed.) Coding Theory and Cryptology, pp. 49–90. World Scientific, Singapore (2002)
3. Fu, F.W., Niederreiter, H., Su, M.: The expectation and variance of the joint linear complexity of random periodic multisequences. J. Complexity 21, 804–822 (2005)
4. Fu, F.W., Niederreiter, H., Özbudak, F.: Joint Linear Complexity of Multisequences Consisting of Linear Recurring Sequences, Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences (to appear)
5. Hawkes, P., Rose, G.G.: Exploiting multiples of the connection polynomial in word-oriented stream ciphers. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 303–316. Springer, Heidelberg (2000)
6. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press, Cambridge (1997)
7. Massey, J.L.: Shift-register synthesis and BCH decoding. IEEE Trans. Inform. Theory 15, 122–127 (1969)

8. Meidl, W.: Discrete Fourier transform, joint linear comoplexity and generalized joint linear complexity of multisequences. In: Helleseth, T., Sarwate, D., Song, H.-Y., Yang, K. (eds.) SETA 2004. LNCS, vol. 3486, pp. 101–112. Springer, Heidelberg (2005)
9. Meidl, W., Niederreiter, H.: Linear complexity, k-error linear complexity, and the discrete Fourier transform. J. Complexity 18, 87–103 (2002)
10. Meidl, W., Niederreiter, H.: On the expected value of the linear complexity and the k-error linear complexity of periodic sequences. IEEE Trans. Inform. Theory 48, 2817–2825 (2002)
11. Meidl, W., Niederreiter, H.: The expected value of the joint linear complexity of periodic multisequences. J. Complexity 19, 61–72 (2003)
12. Niederreiter, H.: Sequences with almost perfect linear complexity profile. In: Chaum, D., Price, W.L. (eds.) Advances in Cryptology-EUROCRYPT 1987. LNCS, vol. 304, pp. 37–51. Springer, Berlin (1988)
13. Niederreiter, H., Johansson, T., Maitra, S. (eds.): INDOCRYPT 2003. LNCS, vol. 2904, pp. 1–17. Springer, Berlin (2003)
14. Rueppel, R.A.: Analysis and Design of Stream Ciphers. Springer, Berlin (1986)
15. Rueppel, R.A.: Stream ciphers. In: Simmons, G.J. (ed.) Contemporary Cryptology: The Science of Information Integrity, pp. 65–134. IEEE Press, New York (1992)