Error Linear Complexity Measures for Multisequences

Wilfried Meidl[a] Harald Niederreiter[b,*]
Ayineedi Venkateswarlu[b]

[a] Sabanci University, Orhanli, Tuzla, 34956 Istanbul, Turkey
e-mail: wmeidl@sabanciuniv.edu
[b] Department of Mathematics, National University of Singapore,
2 Science Drive 2, Singapore 117543, Republic of Singapore
e-mail: nied@math.nus.edu.sg (H. Niederreiter),
g0403231@nus.edu.sg (A. Venkateswarlu)

To the memory of Hans Dobbertin

Abstract

Complexity measures for sequences over finite fields, such as the linear complexity and the k-error linear complexity, play an important role in cryptology. Recent developments in stream ciphers point towards an interest in word-based stream ciphers, which require the study of the complexity of multisequences. We introduce various options for error linear complexity measures for multisequences. For finite multisequences as well as for periodic multisequences with prime period, we present formulas for the number of multisequences with given error linear complexity for several cases, and we present lower bounds for the expected error linear complexity.

Keywords: Multisequences; Joint linear complexity; Error linear complexity; Stream ciphers.

1 Introduction

Complexity measures for keystream sequences over finite fields, such as the linear complexity and the k-error linear complexity, play a crucial role in designing good stream cipher systems. A lot of research has been done on the linear complexity and related complexity measures for keystream sequences. For a recent survey the reader is referred to [15]. Most of this research so far has been concentrated on

[*] Corresponding author.

studying single keystream sequences. Some recent works focused on word-based or vectorized stream cipher systems [3, 8, 9, 10], which require the study of parallel streams of finitely many sequences. In this direction the joint linear complexity of multisequences has been investigated in [2, 5, 6, 7, 14, 15, 16, 18, 19, 21, 24, 25]. Let $\mathbb{F}_q$ be the finite field with q elements, where q is an arbitrary prime power. We denote a multisequence (of finite or infinite length) consisting of m parallel streams of sequences $S_1, \ldots, S_m$ over $\mathbb{F}_q$ by $\mathbf{S} = (S_1, \ldots, S_m)$.

Definition 1.1 *For an ultimately periodic multisequence* $\mathbf{S} = (S_1, \ldots, S_m)$ *over* $\mathbb{F}_q$*, we denote the terms of the* j*th sequence* S_j *by* $s_{j,1}, s_{j,2}, \ldots$*. Then the* joint linear complexity $L(\mathbf{S}) = L(S_1, \ldots, S_m)$ *of* $\mathbf{S}$ *is the least nonnegative integer* L *for which there exist coefficients* $d_1, d_2, \ldots, d_L \in \mathbb{F}_q$ *such that*

$$s_{j,i} + d_1 s_{j,i-1} + \cdots + d_L s_{j,i-L} = 0 \quad \textit{for all } 1 \le j \le m \textit{ and } i \ge L+1.$$

In other words, $L(\mathbf{S})$ *is the least order of a linear recurrence relation over* $\mathbb{F}_q$ *that simultaneously generates each sequence* S_j*,* $1 \le j \le m$*. For an arbitrary multisequence* $\mathbf{S} = (S_1, \ldots, S_m)$ *and any integer* $n \ge 1$ *not exceeding the length of* $\mathbf{S}$*, the* (nth) joint linear complexity $L_n(\mathbf{S}) = L_n(S_1, \ldots, S_m)$ *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*,* $1 \le j \le m$*.*

We always have $0 \le L_n(\mathbf{S}) \le n$ and $L_n(\mathbf{S}) \le L_{n+1}(\mathbf{S})$, and for an ultimately periodic multisequence $\mathbf{S}$ with preperiod t and period N we will always have $L(\mathbf{S}) \le N + t$. Note that in the latter case, $L(\mathbf{S})$ is also the degree of the polynomial

$$J(x) = x^L + d_1 x^{L-1} + \cdots + d_{L-1} x + d_L \in \mathbb{F}_q[x].$$

The polynomial $J(x)$ is called the *joint minimal polynomial* of the ultimately periodic multisequence $\mathbf{S}$.

Since the $\mathbb{F}_q$-linear spaces $\mathbb{F}_q^m$ and $\mathbb{F}_{q^m}$ are isomorphic, the given m-fold multisequence $\mathbf{S}$ over $\mathbb{F}_q$ can also be identified with a single sequence $\mathcal{S} = [S_1, \ldots, S_m]$ having its terms in the extension field $\mathbb{F}_{q^m}$. The (nth) joint linear complexity $L_n(\mathbf{S})$ of $\mathbf{S}$ can also be interpreted as the (nth) $\mathbb{F}_q$-*linear complexity* $L_n^q(\mathcal{S})$ of $\mathcal{S}$, which is the least order of a linear recurrence relation *over* $\mathbb{F}_q$ that the (first n) terms of $\mathcal{S}$ satisfy (see [5, pp. 83–85]). This viewpoint is often convenient in proofs [15]. In [24] enumeration results on the (nth) joint linear complexity of multisequences were presented. Expected values for the joint linear complexity of periodic multisequences were determined in [14].

The stability theory of stream ciphers suggests that good keystream sequences must not only have a large linear complexity, but also a change of a few terms must not cause a significant drop of the linear complexity. This requirement leads to the theory of the *k-error linear complexity* of keystream sequences for integers $k \ge 0$. In [23] Stamp and Martin defined the k-error linear complexity $L_{N,k}(S)$ of an N-periodic single sequence S with period $(s_1, \ldots, s_N)$ to be the smallest linear complexity that can be obtained by altering k or fewer of the terms s_i, $1 \le i \le N$, and then continuing the changes periodically with period N. The concept of the

k-error linear complexity was built on the earlier concept of the *sphere complexity* $SC_k(S)$ introduced in [4] (see also the monograph [5]).

A lot of research on the k-error linear complexity of single keystream sequences has been carried out (see again [15] for a survey). In this article we develop a theory of the k-error linear complexity for multisequences.

In Section 2 we introduce various options for error linear complexity measures for multisequences, analogous to the framework of the k-error linear complexity of single sequences over finite fields. In Section 3 we establish formulas for counting functions for the error linear complexity measures for finite multisequences, and in Section 4 we provide bounds for the expected values for the error linear complexity measures for finite multisequences. Sections 5 and 6 consider the case of periodic multisequences with prime period. Section 7 concludes the paper.

2 Definition of Error Linear Complexity Measures for Multisequences

We shall first fix the notation. An m-fold multisequence $\mathbf{S}$ over $\mathbb{F}_q$ of length n can also be interpreted as a matrix of size $m \times n$ over $\mathbb{F}_q$, i.e., $\mathbf{S} \in \mathbb{F}_q^{m\times n}$. For a periodic multisequence $\mathbf{S}$, it suffices to consider the terms within the given period length N, and so it can also be interpreted as an $m \times N$ matrix over $\mathbb{F}_q$; we will write $\mathbf{S} \in (\mathbb{F}_q^{m\times N})^\infty$ to signify that the first period of $\mathbf{S}$ (which is identified with an element of $\mathbb{F}_q^{m\times N}$) is repeated infinitely often to get the full periodic multisequence $\mathbf{S}$. The following definitions of term, column, term distance, and column distance also suit this interpretation. Let $\mathbf{S} = (S_1, \ldots, S_m)$ be an m-fold multisequence over $\mathbb{F}_q$. A *term* in $\mathbf{S}$ is defined to be a term of S_j for some j, $1 \le j \le m$. A *column* in $\mathbf{S}$ is meant to be the column vector in $\mathbb{F}_q^m$ formed by the ith terms of $S_1, \ldots, S_m$, for some integer $i \ge 1$.

Definition 2.1 *Let* $\mathbf{S} = (S_1, \ldots, S_m)$ *and* $\mathbf{T} = (T_1, \ldots, T_m)$ *be two* m*-fold multisequences over* $\mathbb{F}_q$ *of the same finite length. We define the* term distance $d_T(\mathbf{S}, \mathbf{T})$ *between* $\mathbf{S}$ *and* $\mathbf{T}$ *as the number of terms in* $\mathbf{S}$ *that are different from the corresponding terms in* $\mathbf{T}$*, and the* column distance $d_C(\mathbf{S}, \mathbf{T})$ *as the number of columns in* $\mathbf{S}$ *that are different from the corresponding columns in* $\mathbf{T}$*. We define the* individual distances vector *by* $d_V(\mathbf{S}, \mathbf{T}) = (d_H(S_1, T_1), \ldots, d_H(S_m, T_m))$*, where* $d_H(S_j, T_j)$ *is the Hamming distance between* S_j *and* T_j *for* $1 \le j \le m$*.*

Example 2.1 For $m = 2$, $n = 5$, and

$$\mathbf{S} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}, \qquad \mathbf{T} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix},$$

we have $d_T(\mathbf{S}, \mathbf{T}) = 3$, $d_C(\mathbf{S}, \mathbf{T}) = 2$, and $d_V(\mathbf{S}, \mathbf{T}) = (2, 1)$.

As mentioned in Section 1, an m-fold multisequence $\mathbf{S} = (S_1, \ldots, S_m)$ over $\mathbb{F}_q$ can be identified with a single sequence $\mathcal{S} = [S_1, \ldots, S_m]$ having its terms in the extension field $\mathbb{F}_{q^m}$. Consequently, the columns of $\mathbf{S} = (S_1, \ldots, S_m)$ can also be treated as the terms of $\mathcal{S} = [S_1, \ldots, S_m]$. Then the column distance $d_C(\mathbf{S}, \mathbf{T})$ between $\mathbf{S}$ and $\mathbf{T}$ is the same as the Hamming distance $d_H(\mathcal{S}, \mathcal{T})$ between $\mathcal{S}$ and $\mathcal{T}$, the corresponding sequences with terms in $\mathbb{F}_{q^m}$.

We will distinguish three options of defining error linear complexity for a finite multisequence $\mathbf{S} \in \mathbb{F}_q^{m\times n}$ and an N-periodic multisequence $\mathbf{S} \in (\mathbb{F}_q^{m\times N})^\infty$, respectively. In the following, the definitions for the case of finite multisequences are given.

Definition 2.2 *Let* $\mathbf{S} \in \mathbb{F}_q^{m\times n}$ *be an* m*-fold multisequence of length* $n \geq 1$ *and let* k *be an integer with* $0 \leq k \leq mn$*. Then the* (nth) k-error joint linear complexity $L_{n,k}(\mathbf{S})$ *of* $\mathbf{S}$ *is defined by*

$$L_{n,k}(\mathbf{S}) = \min_{\mathbf{T}} L_n(\mathbf{T}),$$

where the minimum is taken over all $\mathbf{T} \in \mathbb{F}_q^{m\times n}$ *with term distance* $d_T(\mathbf{S}, \mathbf{T}) \leq k$*.*

Similar to the definition of the $\mathbb{F}_q$-linear complexity (see Section 1), we define the *k-error $\mathbb{F}_q$-linear complexity* by allowing k or fewer column changes.

Definition 2.3 *Let* $\mathbf{S} \in \mathbb{F}_q^{m\times n}$ *be an* m*-fold multisequence of length* $n \geq 1$ *and let* k *be an integer with* $0 \leq k \leq n$*. Then the* (nth) k-error $\mathbb{F}_q$-linear complexity $L^q_{n,k}(\mathbf{S})$ *of* $\mathbf{S}$ *is defined by*

$$L^q_{n,k}(\mathbf{S}) = \min_{\mathbf{T}} L_n(\mathbf{T}),$$

where the minimum is taken over all $\mathbf{T} \in \mathbb{F}_q^{m\times n}$ *with column distance* $d_C(\mathbf{S}, \mathbf{T}) \leq k$*. Alternatively, if* $\mathcal{S}$ *is the corresponding sequence of length* n *with terms in* $\mathbb{F}_{q^m}$*, then* $L^q_{n,k}(\mathbf{S})$ *is the* (nth) k-error $\mathbb{F}_q$-linear complexity $L^q_{n,k}(\mathcal{S})$ *of* $\mathcal{S}$*, defined by*

$$L^q_{n,k}(\mathcal{S}) = \min_{\mathcal{T}} L^q_n(\mathcal{T}),$$

where the minimum is taken over all $\mathcal{T} \in \mathbb{F}^n_{q^m}$ *with Hamming distance* $d_H(\mathcal{S}, \mathcal{T}) \leq k$*.*

For $\vec{\mathbf{k}} = (k_1, \ldots, k_m)$ and $\vec{\mathbf{k}}' = (k'_1, \ldots, k'_m)$ in $\mathbb{Z}^m$, we say that $\vec{\mathbf{k}} \leq \vec{\mathbf{k}}'$ if $k_j \leq k'_j$ for $1 \leq j \leq m$, which induces a partial order on $\mathbb{Z}^m$.

Definition 2.4 *Let* $\mathbf{S} = (S_1, \ldots, S_m) \in \mathbb{F}_q^{m\times n}$ *be an* m*-fold multisequence of length* $n \geq 1$ *and let* $\vec{\mathbf{k}} = (k_1, \ldots, k_m) \in \mathbb{Z}^m$ *be such that* $0 \leq k_j \leq n$ *for* $1 \leq j \leq m$*. Then the* (nth) $\vec{\mathbf{k}}$-error joint linear complexity $L_{n,\vec{\mathbf{k}}}(\mathbf{S})$ *of* $\mathbf{S}$ *is defined by*

$$L_{n,\vec{\mathbf{k}}}(\mathbf{S}) = \min_{\mathbf{T}} L_n(\mathbf{T}),$$

where the minimum is taken over all m*-fold multisequences* $\mathbf{T} = (T_1, \ldots, T_m)$ *over* $\mathbb{F}_q$ *of length* n *with* $d_V(\mathbf{S}, \mathbf{T}) \leq \vec{\mathbf{k}}$*, i.e., with Hamming distances* $d_H(S_j, T_j) \leq k_j$ *for* $1 \leq j \leq m$*.*

For N-periodic multisequences $\mathbf{S} \in (\mathbb{F}_q^{m\times N})^\infty$, we analogously define the k-error joint linear complexity $L_{N,k}(\mathbf{S})$, the k-error $\mathbb{F}_q$-linear complexity $L^q_{N,k}(\mathbf{S})$, and the $\vec{\mathbf{k}}$-error joint linear complexity $L_{N,\vec{\mathbf{k}}}(\mathbf{S})$ via the term distance, the column distance, and the individual distances vector, respectively, of the corresponding $m \times N$ matrices over $\mathbb{F}_q$ (compare with Section 1 for the case $m = 1$).

3 Enumeration Results for the Error Linear Complexity of Finite Multisequences

We start this section with the definition of some counting functions corresponding to the three options for the error linear complexity.

Definition 3.1 *Let m, n, k, and L be integers with $m \geq 1,\ n \geq 1,\ 0 \leq k \leq mn$, and $0 \leq L \leq n$. Then we define $\mathcal{N}^m_{n,k}(L)$, respectively $\mathcal{M}^m_{n,k}(L)$, to be the number of m-fold multisequences $\mathbf{S} \in \mathbb{F}_q^{m\times n}$ with $L_{n,k}(\mathbf{S}) = L$, respectively $L_{n,k}(\mathbf{S}) \leq L$.*

Definition 3.2 *For integers m, n, k, and L with $m \geq 1,\ n \geq 1,\ 0 \leq k \leq n$, and $0 \leq L \leq n$, we define $\mathcal{N}^{m,q}_{n,k}(L)$, respectively $\mathcal{M}^{m,q}_{n,k}(L)$, to be the number of m-fold multisequences $\mathcal{S} \in \mathbb{F}^n_{q^m}$ with $L^q_{n,k}(\mathcal{S}) = L$, respectively $L^q_{n,k}(\mathcal{S}) \leq L$.*

Definition 3.3 *For integers n and L and an integer vector $\vec{\mathbf{k}} = (k_1, \ldots, k_m)$ with $n \geq 1$, $0 \leq L \leq n$, and $0 \leq k_j \leq n$ for $1 \leq j \leq m$, we define $\mathcal{N}^m_{n,\vec{\mathbf{k}}}(L)$, respectively $\mathcal{M}^m_{n,\vec{\mathbf{k}}}(L)$, to be the number of m-fold multisequences $\mathbf{S} \in \mathbb{F}_q^{m\times n}$ with $L_{n,\vec{\mathbf{k}}}(\mathbf{S}) = L$, respectively $L_{n,\vec{\mathbf{k}}}(\mathbf{S}) \leq L$.*

For any $m \geq 1$ and $0 \leq L \leq n/2$, the counting function $\mathcal{N}^m_{n,0}(L)$ was determined in [15]. With $\mathcal{N}^m_{n,0}(L) = \mathcal{N}^{m,q}_{n,0}(L) = \mathcal{N}^m_{n,\vec{\mathbf{0}}}(L)$ we obtain the following proposition from [15].

Proposition 3.1 *We have $\mathcal{N}^m_{n,0}(0) = \mathcal{N}^{m,q}_{n,0}(0) = \mathcal{N}^m_{n,\vec{\mathbf{0}}}(0) = 1$ and*

$$\mathcal{N}^m_{n,0}(L) = \mathcal{N}^{m,q}_{n,0}(L) = \mathcal{N}^m_{n,\vec{\mathbf{0}}}(L) = (q^m - 1)q^{(m+1)L-m} \quad \text{for } 1 \leq L \leq \frac{n}{2}. \qquad (1)$$

It turned out that it is not easy to calculate $\mathcal{N}^m_{n,0}(L)$ for $L > n/2$. In [24] a method to determine $\mathcal{N}^m_{n,0}(L)$ for any $m \geq 1$ and $n/2 < L \leq n$ was introduced and a convenient closed-form expression for $\mathcal{N}^m_{n,0}(L)$ was given when $m = 2$. A similar expression for $m = 3$ can be found in [19]. For larger values of m it becomes more cumbersome to get convenient closed-form expressions for $\mathcal{N}^m_{n,0}(L)$.

We now present formulas for $\mathcal{N}^m_{n,k}(L), \mathcal{N}^{m,q}_{n,k}(L)$, and $\mathcal{N}^m_{n,\vec{\mathbf{k}}}(L)$ in specific cases. Throughout this paper we use the function notation $\mathrm{Wt}(\cdot)$ to denote the number of nonzero entries in a vector or a matrix.

Theorem 3.1 *The following formulas are valid for any $m \geq 1$:*
(i) *For $1 \leq k \leq mn$,*

$$\mathcal{N}^m_{n,k}(0) = \sum_{t=0}^{k} \binom{mn}{t} (q-1)^t.$$

(ii) *For $1 \leq k < (n-1)/4$,*

$$\mathcal{N}^m_{n,k}(1) = (q^m - 1) \sum_{t=0}^{k} \binom{mn}{t} (q-1)^{t+1} + \sum_{j=1}^{m} \binom{m}{j} \sum_{t=\max(0,k-j+1)}^{k} \binom{m(n-1)}{t} (q-1)^{t+j}.$$

(iii) *$\mathcal{N}^m_{n,k}(n) = 0$ for $m \leq k \leq mn$.*

Proof : (i) The result immediately follows from the size of the set of all multisequences in the ball $B_{d_T}(\mathbf{Z}, k)$ of radius k in the term distance metric around the zero multisequence $\mathbf{Z} = (0)_{m\times n} \in \mathbb{F}_q^{m\times n}$.

(ii) The multisequences with joint minimal polynomial x are of the form $(s_{j,i})_{m\times n}$ such that the first column $\mathbf{s}_1 = (s_{1,1}, \ldots, s_{m,1})^{\mathrm{T}}$ is nonzero and all other columns are zero. For any such multisequence $\mathbf{S}$ over $\mathbb{F}_q$, consider all multisequences $\mathbf{T} \in \mathbb{F}_q^{m\times n}$ with the same first column vector $\mathbf{s}_1$ and $k - \mathrm{Wt}(\mathbf{s}_1) + 1 \leq d_T(\mathbf{S}, \mathbf{T}) \leq k$. These multisequences $\mathbf{T}$ can be reduced to $\mathbf{S}$ but not to the zero multisequence by allowing at most k term changes. The second term in the formula for $\mathcal{N}_{n,k}^{m}(1)$ counts all these multisequences which can be reduced to a multisequence with joint minimal polynomial x.

For fixed $d \in \mathbb{F}_q^*$, the $q^m - 1$ multisequences over $\mathbb{F}_q$ with joint minimal polynomial $x+d$ have ith column vector $\mathbf{s}_i = (-d)^{i-1}(s_{1,1}, \ldots, s_{m,1})^{\mathrm{T}}$ for all $i \geq 1$. Clearly, two different multisequences with the same joint minimal polynomial $x+d$, $d \in \mathbb{F}_q^*$, must have at least one pair of corresponding nonidentical rows and different terms at corresponding positions in this row. Multisequences with different joint minimal polynomials $x + d_1$ and $x + d_2$, where $d_1, d_2 \in \mathbb{F}_q^*$, differ in at least one pair of corresponding rows in at least $(n-1)/2$ positions. Consequently, the term distance between two different multisequences in $\mathbb{F}_q^{m\times n}$ with joint minimal polynomial of the form $x + d$, $d \in \mathbb{F}_q^*$, is at least $(n-1)/2$, and so the balls of radius k, $1 \leq k < (n-1)/4$, around these multisequences do not intersect. Furthermore, a multisequence with joint minimal polynomial x and a multisequence with joint minimal polynomial of the form $x + d$, $d \in \mathbb{F}_q^*$, differ in at least one pair of corresponding rows in at least $n - 1$ positions. Therefore, the balls of radius k, $1 \leq k < (n-1)/4$, around these two multisequences are again disjoint. This leads to the claimed formula for $\mathcal{N}_{n,k}^{m}(1)$.

(iii) We can manipulate the last column to be the sum of the first $n-1$ column vectors by at most m term changes, and hence the result follows. □

With similar arguments as above we obtain the following results for $\mathcal{N}_{n,k}^{m,q}(L)$.

Theorem 3.2 *The following formulas are valid for any $m \geq 1$:*
(i) *For $1 \leq k \leq n$,*

$$\mathcal{N}_{n,k}^{m,q}(0) = \sum_{t=0}^{k} \binom{n}{t} (q^m - 1)^t.$$

(ii) *For $1 \leq k < (n-1)/4$,*

$$\mathcal{N}_{n,k}^{m,q}(1) = (q-1) \sum_{t=0}^{k} \binom{n}{t} (q^m - 1)^{t+1} + \binom{n-1}{k} (q^m - 1)^{k+1}.$$

(iii) $\mathcal{N}_{n,k}^{m,q}(n) = 0$ *for $1 \leq k \leq n$.*

For the $\vec{\mathbf{k}}$-error joint linear complexity the formulas are as follows.

Theorem 3.3 *Let* $m \geq 1$, $M = \{1, 2, \ldots, m\}$, *and* $\vec{\mathbf{k}} = (k_1, \ldots, k_m)$.
(i) *If* $0 \leq k_j \leq n$ *for* $1 \leq j \leq m$, *then*

$$\mathcal{N}^m_{n,\vec{\mathbf{k}}}(0) = \prod_{j=1}^{m} (\sum_{t=0}^{k_j} \binom{n}{t} (q-1)^t).$$

(ii) *If* $1 \leq k_j < (n-1)/4$ *for* $1 \leq j \leq m$, *then*

$$\begin{aligned}\mathcal{N}^m_{n,\vec{\mathbf{k}}}(1) &= (q^m - 1)(q-1) \prod_{j=1}^{m} (\sum_{t=0}^{k_j} \binom{n}{t} (q-1)^t) + \sum_{j=1}^{m} (q-1)^j \\ &\quad \sum_{E \subseteq M, |E| = j} (\prod_{i \in E} \binom{n-1}{k_i} (q-1)^{k_i}) \cdot \prod_{i \in M \setminus E} (\sum_{r=0}^{k_i} \binom{n}{r} (q-1)^r).\end{aligned}$$

(iii) $\mathcal{N}^m_{n,\vec{\mathbf{k}}}(n) = 0$ *if* $\mathrm{Wt}(\vec{\mathbf{k}}) = m$.

Proof : The formulas (i) and (iii) can easily be derived in analogy with the corresponding formulas in Theorem 3.1. We show (ii) by counting all multisequences in $\mathbb{F}_q^{m \times n}$ that can be reduced to an m-fold multisequence of length n with nth joint linear complexity 1 but not to $\mathbf{Z} = (0)_{m \times n} \in \mathbb{F}_q^{m \times n}$, by making at most k_j changes in the jth row for $1 \leq j \leq m$.

The first term in the formula for $\mathcal{N}^m_{n,\vec{\mathbf{k}}}(1)$ counts all multisequences $\mathbf{T} \in \mathbb{F}_q^{m \times n}$ that can be reduced to an m-fold multisequence of length n with a joint minimal polynomial of the form $x + d$, $d \in \mathbb{F}_q^*$. Note that since we suppose that $k_j < (n-1)/4$, $1 \leq j \leq m$, the balls of radius $\vec{\mathbf{k}}$ around different m-fold multisequences with length n and joint minimal polynomial of the form $x + d$, $d \in \mathbb{F}_q^*$, do not intersect (compare with the proof of part (ii) of Theorem 3.1).

A multisequence $\mathbf{T} \in \mathbb{F}_q^{m \times n}$ can be reduced to an m-fold multisequence of length n with joint minimal polynomial x if each row of $\mathbf{T}$ can be reduced to the form $(a, 0, \ldots, 0)$ with some $a \in \mathbb{F}_q$, but a nonempty subset of rows cannot be reduced to the zero row by applying at most the term changes allowed per row. Let $E \subseteq \{1, \ldots, m\} = M$ be the nonempty set of row indices such that for $i \in E$ the ith row is nonzero after reduction and for $i \in M \setminus E$ the ith row is zero after reduction. To avoid multiple counting, we assume that, for each $i \in E$, exactly k_i terms of the last $n-1$ terms of the ith row of $\mathbf{T}$ are nonzero. Let $|E| = j$. Then $(q-1)^j \prod_{i \in E} \binom{n-1}{k_i} (q-1)^{k_i}$ is the number of possible choices for the corresponding rows such that each row with row index in E can be reduced to a row of the form $(a, 0, \ldots, 0)$ with $a \in \mathbb{F}_q^*$. The term $\prod_{i \in M \setminus E} \left(\sum_{r=0}^{k_i} \binom{n}{r} (q-1)^r \right)$ counts all possible choices for the remaining rows such that these can be reduced to the zero row with the allowed number of term changes per row. Adding over all nonempty subsets $E \subseteq M$ yields the desired formula. □

For the determination of $\mathcal{N}^m_{n,k}(L)$, $\mathcal{N}^{m,q}_{n,k}(L)$, and $\mathcal{N}^m_{n,\vec{\mathbf{k}}}(L)$ for more values of k and $\vec{\mathbf{k}}$, we need the number of purely periodic multisequences with fixed joint linear complexity L.

Theorem 3.4 *For any $m \geq 1$, the number $P^{(m)}(L)$ of purely periodic m-fold multisequences over $\mathbb{F}_q$ with fixed joint linear complexity L is given by $P^{(m)}(0) = 1$ and*

$$P^{(m)}(L) = \frac{(q^m - 1)(q - 1)}{q^{m+1} - 1}(q^{(m+1)L} - 1) \quad \textit{for } L \geq 1.$$

Proof : The case $L = 0$ is trivial. For $L \geq 1$ we proceed by induction on L. If $\mathbf{S}$ is purely periodic with linear complexity 1, then the joint minimal polynomial of $\mathbf{S}$ is of the form $x + d$, $d \in \mathbb{F}_q^*$. For each of these $q - 1$ different joint minimal polynomials we can choose $q^m - 1$ different initial column vectors in $\mathbb{F}_q^m$ in order to obtain different purely periodic m-fold multisequences with joint linear complexity 1. Thus, we have $P^{(m)}(1) = (q^m - 1)(q - 1)$ and the formula of the theorem is true for $L = 1$.

Let $U^{(m)}(L)$ be the number of ultimately but not purely periodic m-fold multisequences $\mathbf{S}$ over $\mathbb{F}_q$ with fixed joint linear complexity L. Let t be the length of the preperiod of the sequence $\mathbf{S}$. Then the purely periodic part of $\mathbf{S}$ has joint linear complexity $L - t$. Thus, there are $P^{(m)}(L - t)$ possibilities for the purely periodic part of $\mathbf{S}$. For the preperiod of $\mathbf{S}$ we have $q^{m(t-1)}(q^m - 1)$ possibilities, since we have to guarantee that the choice of the tth column of $\mathbf{S}$ does not decrease the length of the preperiod. Taking into account that $1 \leq t \leq L$, we get

$$U^{(m)}(L) = (q^m - 1)\sum_{t=1}^{L} q^{m(t-1)}P^{(m)}(L - t) = (q^m - 1)\sum_{t=0}^{L-1} q^{m(L-t-1)}P^{(m)}(t).$$

The formula (1) yields

$$P^{(m)}(L) = (q^m - 1)q^{(m+1)L-m} - (q^m - 1)\sum_{t=0}^{L-1} q^{m(L-t-1)}P^{(m)}(t).$$

Using the induction hypothesis, we get the desired formula after simple algebraic manipulations. □

From Theorem 3.4 and the identity $P^{(m)}(L) + U^{(m)}(L) = (q^m - 1)q^{(m+1)L-m}$ for $L \geq 1$ (see (1)) we obtain the following corollary.

Corollary 3.1 *For any $m \geq 1$, the number $U^{(m)}(L)$ of ultimately but not purely periodic m-fold multisequences over $\mathbb{F}_q$ with fixed joint linear complexity L is given by $U^{(m)}(0) = 0$ and*

$$U^{(m)}(L) = \frac{(q^m - 1)(q - 1)}{q^{m+1} - 1}\left(\frac{q^m - 1}{q - 1}q^{(m+1)L-m} + 1\right) \quad \textit{for } L \geq 1.$$

Let $Q^{(m)}(L)$ and $V^{(m)}(L)$ denote the number of purely periodic m-fold multisequences $\mathbf{S}$ over $\mathbb{F}_q$ with $L(\mathbf{S}) \leq L$ and the number of ultimately but not purely periodic m-fold multisequences $\mathbf{S}$ over $\mathbb{F}_q$ with $L(\mathbf{S}) \leq L$, respectively. Hence $Q^{(m)}(L) = \sum_{t=0}^{L} P^{(m)}(t)$ and $V^{(m)}(L) = \sum_{t=0}^{L} U^{(m)}(t)$, and the following corollaries can easily be deduced.

Corollary 3.2 *For any $m \geq 1$, the number $Q^{(m)}(L)$ of purely periodic m-fold multisequences $\mathbf{S}$ over $\mathbb{F}_q$ with $L(\mathbf{S}) \leq L$ is given by*

$$Q^{(m)}(L) = \frac{(q^m-1)(q-1)}{(q^{m+1}-1)^2}\left(q^{(m+1)(L+1)} - (q^{m+1}-1)L - q^{m+1}\right) + 1 \quad \textit{for } L \geq 0.$$

Corollary 3.3 *For any $m \geq 1$, the number $V^{(m)}(L)$ of ultimately but not purely periodic m-fold multisequences $\mathbf{S}$ over $\mathbb{F}_q$ with $L(\mathbf{S}) \leq L$ is given by*

$$V^{(m)}(L) = \frac{(q^m-1)^2}{(q^{m+1}-1)^2}\left(q^{(m+1)L+1} + \frac{(q^{m+1}-1)(q-1)}{q^m-1}L - q\right) \quad \textit{for } L \geq 0.$$

We remark that the formulas in Theorem 3.4 and Corollaries 3.1–3.3 coincide with the formulas for $m = 1$ in [17] for the binary case and in [12] for arbitrary q.

Let $\mathcal{S}$ and $\mathcal{S}'$ be two purely periodic sequences with terms in $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$-linear complexity at most L. We remark that the conventional linear complexity of $\mathcal{S}$ and $\mathcal{S}'$ is also at most L, and may be even smaller than the $\mathbb{F}_q$-linear complexity. If $\mathcal{S}$ and $\mathcal{S}'$ have the same minimal polynomial (over $\mathbb{F}_{q^m}$), then $\mathcal{S}$ and $\mathcal{S}'$ are either identical or they differ at least once at any L consecutive terms. If they have different minimal polynomials, then $\mathcal{S}$ and $\mathcal{S}'$ differ at least once at any $2L$ consecutive terms. If $\mathcal{S}$ is an ultimately periodic sequence with $\mathbb{F}_q$-linear complexity at most L, then its preperiod is at most L. Hence from position $L+1$ to position $(4k+3)L$, any two ultimately periodic sequences $\mathcal{S}$ and $\mathcal{S}'$ with terms in $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$-linear complexity at most L are either the same or differ at least at $2k+1$ positions. Similarly, two different purely periodic m-fold multisequences $\mathbf{S}$ and $\mathbf{S}'$ with column vectors in $\mathbb{F}_q^m$ and with joint linear complexity at most L differ at least once at any L consecutive columns if they have the same joint minimal polynomial, and at least once at any $2L$ consecutive columns if they have different joint minimal polynomials. With the same argument as before, from position $L+1$ to position $(4k+3)L$, two ultimately periodic sequences of column vectors in $\mathbb{F}_q^m$ with joint linear complexity at most L are either the same or they differ at least at $2k+1$ column positions. With these facts we can prove two generalizations of [12, Theorem 3], where a formula for the number of single sequences with terms in $\mathbb{F}_q$, length n, and given k-error linear complexity L has been presented, under the condition that $n \geq (4k+3)L$. The first generalization is a formula for $\mathcal{N}_{n,k}^{m,q}(L)$ without proof. The proof is analogous to that of [12, Theorem 3].

Theorem 3.5 *For any integers $m \geq 1$, $L \geq 1$, $k \geq 0$, and $n \geq (4k+3)L$, we have*

$$\mathcal{N}_{n,k}^{m,q}(L) = P^{(m)}(L)\sum_{r=0}^{k}\binom{n}{r}(q^m-1)^r + (q^m-1)^{k+1}\sum_{t=1}^{L}\binom{n-t}{k}q^{m(t-1)}P^{(m)}(L-t),$$

where $P^{(m)}$ is the counting function in Theorem 3.4.

The following theorem generalizes [12, Theorem 3] to the case of the k-error joint linear complexity of m-fold multisequences.

Theorem 3.6 *For any integers $m \geq 1$, $L \geq 1$, $k \geq 0$, and $n \geq (4k+3)L$, we have*

$$\begin{aligned}\mathcal{N}^m_{n,k}(L) &= P^{(m)}(L)\sum_{r=0}^{k}\binom{mn}{r}(q-1)^r \\ &\quad + \sum_{j=1}^{m}\binom{m}{j}(q-1)^j \sum_{r=\max(0,k-j+1)}^{k}\sum_{t=1}^{L}\binom{m(n-t)}{r}q^{m(t-1)}(q-1)^r P^{(m)}(L-t),\end{aligned}$$

where $P^{(m)}$ is the counting function in Theorem 3.4.

Proof : We suppose that all considered m-fold multisequences have fixed length $n \geq (4k+3)L$. Then from the previous considerations we know that the ball $B_{d_T}(\mathbf{S}, k)$ around a finite m-fold multisequence $\mathbf{S}$ of length n which corresponds to a purely periodic multisequence with joint linear complexity L does not intersect the ball of radius k around any multisequence $\mathbf{T} \neq \mathbf{S}$ of length n with $L_n(\mathbf{T}) \leq L$. Thus $L_{n,k}(\mathbf{R}) = L$ for all $\mathbf{R} \in B_{d_T}(\mathbf{S}, k)$. Consequently, the contribution of the balls of radius k around all finite m-fold multisequences of length n corresponding to purely periodic multisequences with joint linear complexity L to the counting function $\mathcal{N}^m_{n,k}(L)$ is given by

$$P^{(m)}(L)\sum_{r=0}^{k}\binom{mn}{r}(q-1)^r.$$

Let $\mathbf{S}$ be a finite m-fold multisequence of length n corresponding to an ultimately periodic multisequence with preperiod $t > 0$ and joint linear complexity L. We want to count all multisequences of length n which can be transformed into $\mathbf{S}$ but not into a multisequence with joint linear complexity less than L by changing at most k terms. The candidates are the multisequences of length n which equal $\mathbf{S}$ at the first t columns and satisfy $d_T(\mathbf{S}, \mathbf{T}) \leq k$. Additionally it must not be possible to shorten the preperiod by suitably changing the tth column. Suppose that the tth column of $\mathbf{S}$ differs at j, $1 \leq j \leq m$, positions from the unique column vector that would yield a reduction of the preperiod. Then we must have $k - j + 1 \leq d_T(\mathbf{S}, \mathbf{T}) \leq k$. Else we would be able to transform $\mathbf{T}$ into $\mathbf{S}$ and then additionally to shorten the preperiod. Thus, the number of m-fold multisequences of length n that by changing at most k terms can be transformed into a multisequence with preperiod t, $1 \leq t \leq L$, and joint linear complexity L but not into a multisequence with smaller joint linear complexity is given by

$$q^{m(t-1)}\sum_{j=1}^{m}\binom{m}{j}(q-1)^j \sum_{r=\max(0,k-j+1)}^{k}\binom{m(n-t)}{r}(q-1)^r P^{(m)}(L-t).$$

Combining all possible choices for t yields the desired formula. □

In the third case the formula is given as follows.

Theorem 3.7 *Let $m \geq 1$ be an integer and let $M = \{1, 2, \ldots, m\}$, $\vec{\mathbf{k}} = (k_1, \ldots, k_m)$, and $k = \max(k_1, \ldots, k_m)$ with $k_j > 0$ for $1 \leq j \leq m$. Then for any integers $L \geq 1$ and $n \geq (4k+3)L$, we have*

$$\begin{aligned}\mathcal{N}^m_{n,\vec{\mathbf{k}}}(L) &= P^{(m)}(L) \prod_{j=1}^{m} (\sum_{r=0}^{k_j} \binom{n}{r} (q-1)^r) + \sum_{t=1}^{L} q^{m(t-1)} P^{(m)}(L-t) \sum_{j=1}^{m} (q-1)^j \\ & \sum_{E \subseteq M, |E|=j} (\prod_{i \in E} \binom{n-t}{k_i} (q-1)^{k_i}) \cdot \prod_{i \in M \setminus E} (\sum_{r=0}^{k_i} \binom{n-t+1}{r} (q-1)^r),\end{aligned}$$

where $P^{(m)}$ is the counting function in Theorem 3.4. In particular, if $k_j = k$ for $1 \leq j \leq m$, then we have

$$\begin{aligned}\mathcal{N}^m_{n,\vec{\mathbf{k}}}(L) &= P^{(m)}(L) \left(\sum_{r=0}^{k} \binom{n}{r} (q-1)^r\right)^m + \sum_{t=1}^{L} q^{m(t-1)} P^{(m)}(L-t) \sum_{j=1}^{m} (q-1)^j \\ & \sum_{E \subseteq M, |E|=j} (\binom{n-t}{k} (q-1)^k)^j \cdot (\sum_{r=0}^{k} \binom{n-t+1}{r} (q-1)^r)^{m-j}.\end{aligned}$$

Proof : We have to count all multisequences in $\mathbb{F}_q^{m \times n}$ that can be reduced to an m-fold multisequence of length n with joint linear complexity L, but not to an m-fold multisequence of length n with a lower joint linear complexity.

The first summand in the formula for $\mathcal{N}^m_{n,\vec{\mathbf{k}}}(L)$ counts all multisequences $\mathbf{T} \in \mathbb{F}_q^{m \times n}$ that can be reduced to an m-fold multisequence of length n and joint linear complexity L which corresponds to a purely periodic m-fold multisequence. Note that since we suppose that $n \geq (4k+3)L$, the balls of radius $\vec{\mathbf{k}}$ around different m-fold multisequences with length n and joint linear complexity L which correspond to purely periodic multisequences are disjoint and they do not intersect with the ball of radius $\vec{\mathbf{k}}$ around an m-fold multisequence with length n and smaller joint linear complexity.

Now consider an ultimately periodic but not purely periodic m-fold multisequence $\mathbf{S} = (S_1, \ldots, S_m)$ of length n with joint linear complexity L and preperiod t $(1 \leq t \leq L)$. Then the joint linear complexity of the periodic part of $\mathbf{S}$ is $L-t$. We associate each such multisequence $\mathbf{S}$ with a set of multisequences $\mathbf{T} = (T_1, \ldots, T_m)$ (like the ball of radius $\vec{\mathbf{k}}$ in the purely periodic case) having the first $t-1$ column vectors identical with the first $t-1$ column vectors of $\mathbf{S}$ and with the allowed number of term changes per row: (i) the periodic part of $\mathbf{T}$ can be transformed into the periodic part of $\mathbf{S}$; (ii) $\mathbf{T}$ cannot be transformed into an m-fold multisequence of length n having joint linear complexity smaller than L. This means that the periodic part of $\mathbf{T}$ must be in the ball of radius $\vec{\mathbf{k}}$ around the periodic part of $\mathbf{S}$. We have $n-t \geq (4k+3)(L-t)$, and by the latter condition we get the disjointness property of the balls as in the purely periodic case above, and we need only to ensure that the preperiod of $\mathbf{T}$ cannot be shortened. This is possible only if the Hamming distance between the periodic parts of T_i and S_i is exactly k_i and the tth term of T_i is different from the unique term which can reduce the preperiod of S_i, for at least a nonempty subset of rows. Let $E \subseteq \{1,\ldots,m\} = M$ be a nonempty set of row indices with $|E| = j$. Then $(q-1)^j \prod_{i\in E} \binom{n-t}{k_i}(q-1)^{k_i}$ is the number of possible choices for the corresponding rows such that the periodic part of each row with row index in E can be reduced to the periodic part of the corresponding row in $\mathbf{S}$, but the preperiod cannot be shortened for this rows with the allowed number of term changes per row. The term $\prod_{i\in M\setminus E}\big(\sum_{r=0}^{k_i}\binom{n-t+1}{r}(q-1)^r\big)$ counts all possible choices for the remaining rows such that the periodic part of these rows can be reduced to the periodic part of the corresponding rows in $\mathbf{S}$ and additionally the terms at position t can be chosen in such a way that they match the linear recurrence for the periodic part of $\mathbf{S}$. Adding over all nonempty subsets $E \subseteq M$ and over all possible lengths for the preperiod yields the desired formula. □

The following two propositions give obvious upper bounds on $\mathcal{N}^m_{n,k}(L)$, $\mathcal{M}^m_{n,k}(L)$, $\mathcal{N}^{m,q}_{n,k}(L)$, $\mathcal{M}^{m,q}_{n,k}(L)$, $\mathcal{N}^m_{n,\vec{\mathbf{k}}}(L)$, and $\mathcal{M}^m_{n,\vec{\mathbf{k}}}(L)$.

Proposition 3.2 *For any integers $m \geq 1$, $n \geq 1$, and $0 \leq L \leq n$, we have*

$$\begin{aligned}
\mathcal{N}^m_{n,k}(L) &\leq \min\left(q^{mn}, \mathcal{N}^m_{n,0}(L)\sum_{t=0}^{k}\binom{mn}{t}(q-1)^t\right),\ 0 \leq k \leq mn,\\
\mathcal{N}^{m,q}_{n,k}(L) &\leq \min\left(q^{mn}, \mathcal{N}^{m,q}_{n,0}(L)\sum_{t=0}^{k}\binom{n}{t}(q^m-1)^t\right),\ 0 \leq k \leq n,\\
\mathcal{N}^m_{n,\vec{\mathbf{k}}}(L) &\leq \min\left(q^{mn}, \mathcal{N}^m_{n,\vec{\mathbf{0}}}(L)\prod_{j=1}^{m}\Big(\sum_{t=0}^{k_j}\binom{n}{t}(q-1)^t\Big)\right),\ 0 \leq k_j \leq n,\ 1 \leq j \leq m.
\end{aligned}$$

Proposition 3.3 *For any integers $m \geq 1$, $n \geq 1$, and $0 \leq L \leq n$, we have*

$$\begin{aligned}
\mathcal{M}^m_{n,k}(L) &\leq \min\left(q^{mn}, \mathcal{M}^m_{n,0}(L)\sum_{t=0}^{k}\binom{mn}{t}(q-1)^t\right),\ 0 \leq k \leq mn,\\
\mathcal{M}^{m,q}_{n,k}(L) &\leq \min\left(q^{mn}, \mathcal{M}^{m,q}_{n,0}(L)\sum_{t=0}^{k}\binom{n}{t}(q^m-1)^t\right),\ 0 \leq k \leq n,\\
\mathcal{M}^m_{n,\vec{\mathbf{k}}}(L) &\leq \min\left(q^{mn}, \mathcal{M}^m_{n,\vec{\mathbf{0}}}(L)\prod_{j=1}^{m}\Big(\sum_{t=0}^{k_j}\binom{n}{t}(q-1)^t\Big)\right),\ 0 \leq k_j \leq n,\ 1 \leq j \leq m.
\end{aligned}$$

Remark 3.1 The bounds of Proposition 3.3 can be written explicitly using formulas for $\mathcal{M}^m_{n,0}(L) = \mathcal{M}^{m,q}_{n,0}(L) = \mathcal{M}^m_{n,\vec{\mathbf{0}}}(L)$. For $0 \leq L \leq n/2$ with formula (1) and $\mathcal{M}^m_{n,0}(L) = \sum_{r=0}^{L}\mathcal{N}^m_{n,0}(r)$, we obtain the compact expression

$$\mathcal{M}^m_{n,0}(L) = \mathcal{M}^{m,q}_{n,0}(L) = \mathcal{M}^m_{n,\vec{\mathbf{0}}}(L) = \frac{q^m-1}{q^{m+1}-1}\left(q^{(m+1)L+1} + \frac{q-1}{q^m-1}\right). \qquad (2)$$

Since any sequence of column vectors in $\mathbb{F}_q^m$ of length n and joint linear complexity $L > n/2$ can be seen as the first n terms of a (not necessarily uniquely determined) multisequence of length $2L$ and joint linear complexity L, the expression in (1) is also an upper bound on $\mathcal{N}_{n,0}^m(L)$, $\mathcal{N}_{n,0}^{m,q}(L)$, and $\mathcal{N}_{n,\vec{\mathbf{0}}}^m(L)$ for arbitrary L. Consequently, with (1) and (2) and the Propositions 3.2 and 3.3 we can always explicitly determine upper bounds on $\mathcal{N}_{n,k}^m(L)$, $\mathcal{M}_{n,k}^m(L)$, $\mathcal{N}_{n,k}^{m,q}(L)$, $\mathcal{M}_{n,k}^{m,q}(L)$, $\mathcal{N}_{n,\vec{\mathbf{k}}}^m(L)$, and $\mathcal{M}_{n,\vec{\mathbf{k}}}^m(L)$.

4 Expected Values for the Error Linear Complexity of Finite Multisequences

For integers $m \geq 1$ and $n \geq 1$, let $E_{n,0}^m$ be the expected value of the joint linear complexity of finite m-fold multisequences over $\mathbb{F}_q$ of length n, where the underlying probability distribution is the uniform distribution on $\mathbb{F}_q^{m\times n}$, i.e., each element of $\mathbb{F}_q^{m\times n}$ has probability q^{-mn}. For $m = 1$ the exact formula for $E_{n,0}^m$ is known for a long time (see [20, 22]). In [24] an exact formula for $E_{n,0}^2$ was presented (for the case $q = 2$ see also [6]). Finally, in [18] it was shown that for any $m \geq 1$ we have $E_{n,0}^m = mn/(m+1) + o(n)$ as $n \to \infty$. Moreover, the lower bound

$$E_{n,0}^m \geq \left\lfloor \frac{mn}{m+1} \right\rfloor - \frac{q^{mn}-1}{q^{mn}(q^{m+1}-1)}$$

was obtained in [19].

In this section we establish a lower bound on the expected k-error joint linear complexity $E_{n,k}^m$ of finite m-fold multisequences over $\mathbb{F}_q$ of length n, a lower bound on the expected k-error $\mathbb{F}_q$-linear complexity $E_{n,k}^{m,q}$ of finite sequences over $\mathbb{F}_{q^m}$ of length n, and a lower bound on the expected $\vec{\mathbf{k}}$-error joint linear complexity $E_{n,\vec{\mathbf{k}}}^m$ of finite m-fold multisequences over $\mathbb{F}_q$ of length n. The following lemma is a straightforward generalization of [17, Lemma 3].

Lemma 4.1 *For any integers $m \geq 1$ and $n \geq 1$, we have*

$$\begin{aligned}
E_{n,k}^m &= n - \frac{1}{q^{mn}} \sum_{L=0}^{n-1} \mathcal{M}_{n,k}^m(L), \ 0 \leq k \leq mn, \\
E_{n,k}^{m,q} &= n - \frac{1}{q^{mn}} \sum_{L=0}^{n-1} \mathcal{M}_{n,k}^{m,q}(L), \ 0 \leq k \leq n, \\
E_{n,\vec{\mathbf{k}}}^m &= n - \frac{1}{q^{mn}} \sum_{L=0}^{n-1} \mathcal{M}_{n,\vec{\mathbf{k}}}^m(L), \ \vec{\mathbf{k}} = (k_1, \ldots, k_m), \, 0 \leq k_j \leq n, \, 1 \leq j \leq m.
\end{aligned}$$

For establishing a lower bound on $E_{n,k}^m$, we will use the following lemma.

Lemma 4.2 *With*

$$\alpha = \left\lfloor \frac{1}{m+1} \log_q \frac{q^{mn-1}(q^{m+1}-1)}{(q^m-1)\sum_{t=0}^{k} \binom{mn}{t}(q-1)^t} \right\rfloor$$

we have the inequality

$$\frac{q-1}{q^{mn}(q^{m+1}-1)}\left(\sum_{t=0}^{k}\binom{mn}{t}(q-1)^t\right)(\alpha+1)<\frac{2}{3}.$$

Proof : First we note that

$$\beta:=\frac{q-1}{q^{mn}(q^{m+1}-1)}\left(\sum_{t=0}^{k}\binom{mn}{t}(q-1)^t\right)\le\frac{1}{q^m+q^{m-1}+\cdots+1}. \tag{3}$$

For the second factor $\alpha+1$ we obtain

$$\begin{aligned}\alpha+1 &\le \frac{1}{m+1}\log_q\frac{q^{mn-1}(q^{m+1}-1)}{(q^m-1)\sum_{t=0}^{k}\binom{mn}{t}(q-1)^t}+\log_q q\\ &= \log_q\left(\left(\frac{q^{mn-1}(q^{m+1}-1)}{(q^m-1)\sum_{t=0}^{k}\binom{mn}{t}(q-1)^t}\right)^{\frac{1}{m+1}}q\right)\\ &= \log_q\left(\frac{q^{mn}(q^{m+1}-1)}{(q-1)\sum_{t=0}^{k}\binom{mn}{t}(q-1)^t}\right)^{\frac{1}{m+1}}+\log_q\left(\left(\frac{q-1}{q^m-1}\right)^{\frac{1}{m+1}}q^{\frac{m}{m+1}}\right)\\ &< \log_q\left(\frac{q^{mn}(q^{m+1}-1)}{(q-1)\sum_{t=0}^{k}\binom{mn}{t}(q-1)^t}\right)^{\frac{1}{m+1}}+1.\end{aligned}$$

Consequently, with (3) we get

$$\beta(\alpha+1)\le\frac{\beta\log_q\frac{1}{\beta}}{m+1}+\beta<\frac{2}{3(m+1)}+\frac{1}{q^m+q^{m-1}+\cdots+1}\le\frac{2}{3},$$

where we used the fact that $0<x\log_q\frac{1}{x}<\frac{2}{3}$ for $0<x<1$ and $q\ge 2$. □

Theorem 4.1 *For any integers $m\ge 1$, $n\ge 1$, and $0\le k\le mn$, we have*

$$\begin{aligned}E_{n,k}^m &\ge \frac{m}{m+1}n-\frac{1}{m+1}\log_q\big(\sum_{t=0}^{k}\binom{mn}{t}(q-1)^t\big)-\frac{(m+2)q^{m+1}-1}{(m+1)(q^{m+1}-1)}\\ &\quad+\frac{1}{m+1}\log_q\left(\frac{q^{m+1}-1}{q^m-1}\right)-\frac{2}{3}.\end{aligned}$$

Proof : The term

$$\alpha=\left\lfloor\frac{1}{m+1}\log_q\frac{q^{mn-1}(q^{m+1}-1)}{(q^m-1)\sum_{t=0}^{k}\binom{mn}{t}(q-1)^t}\right\rfloor$$

is chosen in such a way that, due to Proposition 3.3, Remark 3.1, and the subsequent considerations, we can use the bound

$$\mathcal{M}_{n,k}^m(L)\le\frac{q^m-1}{q^{m+1}-1}\left(q^{(m+1)L+1}+\frac{q-1}{q^m-1}\right)\sum_{t=0}^{k}\binom{mn}{t}(q-1)^t$$

for $0 \leq L \leq \alpha$ and the trivial bound

$$\mathcal{M}_{n,k}^{m}(L) \leq q^{mn}$$

for $\alpha < L \leq n-1$. This yields

$$\begin{aligned}
\frac{1}{q^{mn}} \sum_{L=0}^{n-1} \mathcal{M}_{n,k}^{m}(L) &\leq \frac{q^m-1}{q^{mn}(q^{m+1}-1)} \left(\sum_{t=0}^{k} \binom{mn}{t} (q-1)^t \right) \cdot \\
&\quad \sum_{L=0}^{\alpha} \left(q^{(m+1)L+1} + \frac{q-1}{q^m-1} \right) + n - 1 - \alpha \\
&= \frac{q^m-1}{q^{mn-1}(q^{m+1}-1)} \left(\sum_{t=0}^{k} \binom{mn}{t} (q-1)^t \right) \frac{q^{(m+1)(\alpha+1)}-1}{q^{m+1}-1} \\
&\quad + \frac{q-1}{q^{mn}(q^{m+1}-1)} \left(\sum_{t=0}^{k} \binom{mn}{t} (q-1)^t \right) (\alpha+1) \\
&\quad + n - 1 - \alpha \\
&\leq \frac{q^m-1}{q^{mn-1}(q^{m+1}-1)} \left(\sum_{t=0}^{k} \binom{mn}{t} (q-1)^t \right) \frac{q^{(m+1)(\alpha+1)}}{q^{m+1}-1} \\
&\quad + \frac{q-1}{q^{mn}(q^{m+1}-1)} \left(\sum_{t=0}^{k} \binom{mn}{t} (q-1)^t \right) (\alpha+1) \\
&\quad + n - \frac{1}{m+1} \Bigg(mn - 1 + \log_q \left(\frac{q^{m+1}-1}{q^m-1} \right) \\
&\quad - \log_q \left(\sum_{t=0}^{k} \binom{mn}{t} (q-1)^t \right) \Bigg) \\
&\leq \frac{q^{m+1}}{q^{m+1}-1} + n - \frac{mn}{m+1} + \frac{1}{m+1} - \frac{1}{m+1} \log_q \left(\frac{q^{m+1}-1}{q^m-1} \right) \\
&\quad + \frac{1}{m+1} \log_q \left(\sum_{t=0}^{k} \binom{mn}{t} (q-1)^t \right) + \frac{2}{3},
\end{aligned}$$

where in the last step we used Lemma 4.2. With Lemma 4.1 we obtain the desired bound. □

Let $\mathcal{H}_q$ denote the q-ary entropy function defined by (cf. [11, p. 55])

$$\mathcal{H}_q(\gamma) = \gamma \log_q(q-1) - \gamma \log_q \gamma - (1-\gamma) \log_q(1-\gamma), \quad 0 < \gamma < 1.$$

Note that $\mathcal{H}_q(\gamma) \to 0$ as $\gamma \to 0+$ and $\mathcal{H}_q(\frac{q-1}{q}) = 1$. Furthermore, $\mathcal{H}_q$ is an increasing function on the interval $(0, (q-1)/q]$.

Corollary 4.1 *For any integers $m \geq 1$, $n \geq 1$, and $0 < k < \frac{mn(q-1)}{q}$, we have*

$$E_{n,k}^{m} > \frac{mn}{m+1} \Big(1 - \mathcal{H}_q(\frac{k}{mn}) \Big) - 2.$$

Proof : By [1, p. 301] we have

$$\sum_{t=0}^{k} \binom{mn}{t} (q-1)^t \leq q^{mn\mathcal{H}_q(\frac{k}{mn})}.$$

With the additional observations that

$$\frac{(m+2)q^{m+1}-1}{(m+1)(q^{m+1}-1)} = \frac{1}{m+1} + \frac{q^{m+1}}{q^{m+1}-1} \leq \frac{1}{m+1} + \frac{4}{3}$$

and that

$$\frac{1}{m+1}\log_q\left(\frac{q^{m+1}-1}{q^m-1}\right) > \frac{1}{m+1}$$

we obtain the desired result. □

With similar arguments we get the following lower bounds for $E_{n,k}^{m,q}$ and $E_{n,\vec{\mathbf{k}}}^{m}$.

Theorem 4.2 *For any integers $m \geq 1$, $n \geq 1$, and $0 \leq k \leq n$, we have*

$$\begin{aligned} E_{n,k}^{m,q} \geq & \frac{m}{m+1}n - \frac{1}{m+1}\log_q\left(\sum_{t=0}^{k}\binom{n}{t}(q^m-1)^t\right) - \frac{(m+2)q^{m+1}-1}{(m+1)(q^{m+1}-1)} \\ & + \frac{1}{m+1}\log_q\left(\frac{q^{m+1}-1}{q^m-1}\right) - \frac{2}{3}. \end{aligned}$$

For any integers $m \geq 1$, $n \geq 1$, and $0 < k < n(q-1)/q$, we have

$$E_{n,k}^{m,q} > \frac{mn}{m+1}\Big(1 - \mathcal{H}_{q^m}(\frac{k}{n})\Big) - 2.$$

Theorem 4.3 *For any integers $m \geq 1$, $n \geq 1$, and $\vec{\mathbf{k}} = (k_1, \ldots, k_m)$, $0 \leq k_j \leq n$ for $1 \leq j \leq m$, we have*

$$\begin{aligned} E_{n,\vec{\mathbf{k}}}^{m} \geq & \frac{m}{m+1}n - \frac{1}{m+1}\log_q\left(\prod_{j=1}^{m}(\sum_{t=0}^{k_j}\binom{n}{t}(q-1)^t)\right) - \frac{(m+2)q^{m+1}-1}{(m+1)(q^{m+1}-1)} \\ & + \frac{1}{m+1}\log_q\left(\frac{q^{m+1}-1}{q^m-1}\right) - \frac{2}{3}. \end{aligned}$$

For any integers $m \geq 1$, $n \geq 1$, and $0 < k_j < n(q-1)/q$, $1 \leq j \leq m$, we have

$$E_{n,\vec{\mathbf{k}}}^{m} > \frac{n}{m+1}\Big(m - \sum_{j=1}^{m}\mathcal{H}_q(\frac{k_j}{n})\Big) - 2.$$

5 Multisequences with Prime Period

An important class of periodic multisequences is the class of multisequences with prime period. In this section we present several results for this class of periodic multisequences, such as counting functions and lower bounds on the expected error linear complexity. We denote the number of m-fold N-periodic multisequences over $\mathbb{F}_q$ with k-error joint linear complexity L, with k-error $\mathbb{F}_q$-linear complexity L, and with $\vec{\mathbf{k}}$-error joint linear complexity L by $\mathcal{P}^m_{N,k}(L)$, $\mathcal{P}^{m,q}_{N,k}(L)$, and $\mathcal{P}^m_{N,\vec{\mathbf{k}}}(L)$, respectively. In the following propositions we present formulas for $\mathcal{P}^m_{N,k}(L)$, $\mathcal{P}^{m,q}_{N,k}(L)$, and $\mathcal{P}^m_{N,\vec{\mathbf{k}}}(L)$ for m-fold multisequences with prime period N for specific values of L. These results can be seen as generalizations of [13, Theorem 4.1].

Proposition 5.1 *Let $m \geq 1$ and let N be a prime with* $\gcd(N,q)=1$. *Then the following formulas for $\mathcal{P}^m_{N,k}(L)$ are valid:*
(i) *For $1 \leq k \leq mN$,*

$$\mathcal{P}^m_{N,k}(0) = \sum_{t=0}^{k} \binom{mN}{t} (q-1)^t.$$

(ii) *If N does not divide $q-1$, then for $1 \leq k \leq (N-1)/2$,*

$$\mathcal{P}^m_{N,k}(1) = (q^m-1) \sum_{t=0}^{k} \binom{mN}{t} (q-1)^t.$$

(iii) $\mathcal{P}^m_{N,k}(N) = 0$ *for $m \leq k \leq mN$.*

Proof : (i) The result immediately follows from the fact that $\mathcal{P}^m_{N,k}(0) = |B_{d_T}(\mathbf{Z},k)|$, where $B_{d_T}(\mathbf{Z},k)$ denotes the ball of radius k around the zero matrix $\mathbf{Z}=(0)_{m\times N} \in \mathbb{F}_q^{m\times N}$ with term distance metric.

(ii) If N does not divide $q-1$, then there are q^m-1 m-fold N-periodic multisequences over $\mathbb{F}_q$ with joint linear complexity $L=1$. They correspond to the $m\times N$ matrices $\mathbf{R}$ over $\mathbb{F}_q$ with each row being a constant string and at least one of the rows being nonzero. For the zero matrix $\mathbf{Z} \in \mathbb{F}_q^{m\times N}$ we have $d_T(\mathbf{Z},\mathbf{R}) \geq N$. Additionally, the term distance per period between any two different multisequences (with joint linear complexity equal to 1) is at least N. Hence for $1 \leq k \leq \frac{N-1}{2}$, the number $\mathcal{P}^m_{N,k}(1)$ is the cardinality of the union of balls $B_{d_T}(\mathbf{R},k)$ of radius k around the center $\mathbf{R}$, where $\mathbf{R}$ runs through all elements of $\mathbb{F}_q^{m\times N}$ different from $\mathbf{Z}$ with constant rows. This yields the desired result.

(iii) Consider a multisequence $\mathbf{S} \in \mathbb{F}_q^{m\times N}$ with columns $\mathbf{s}_i$, $1 \leq i \leq N$. If $\sum_{i=1}^{N} \mathbf{s}_i = \mathbf{0}$, then the joint linear complexity of $\mathbf{S}$ is less than N. Evidently, at most m term changes are necessary in order to satisfy the above condition. □

With similar arguments as above we obtain the corresponding formulas for the other error linear complexity measures.

Proposition 5.2 *Let $m \geq 1$ and let N be a prime with* $\gcd(N,q)=1$. *Then the following formulas for $\mathcal{P}^{m,q}_{N,k}(L)$ are valid:*

(i) *For* $1 \leq k \leq N$,

$$\mathcal{P}_{N,k}^{m,q}(0) = \sum_{t=0}^{k} \binom{N}{t} (q^m - 1)^t.$$

(ii) *If* N *does not divide* $q-1$*, then for* $1 \leq k \leq (N-1)/2$,

$$\mathcal{P}_{N,k}^{m,q}(1) = (q^m - 1) \sum_{t=0}^{k} \binom{N}{t} (q^m - 1)^t.$$

(iii) $\mathcal{P}_{N,k}^{m,q}(N) = 0$ *for* $1 \leq k \leq N$.

Proposition 5.3 *Let* $m \geq 1$*, let* N *be a prime with* $\gcd(N, q) = 1$*, and let* $\vec{\mathbf{k}} = (k_1, \ldots, k_m)$*. Then the following formulas for* $\mathcal{P}_{N,\vec{\mathbf{k}}}^{m}(L)$ *are valid:*
(i) *If* $0 \leq k_j \leq N$ *for* $1 \leq j \leq m$*, then*

$$\mathcal{P}_{N,\vec{\mathbf{k}}}^{m}(0) = \prod_{j=1}^{m} \Big(\sum_{t=0}^{k_j} \binom{N}{t} (q-1)^t \Big).$$

(ii) *If* N *does not divide* $q-1$*, then for* $0 \leq k_j \leq \frac{N-1}{2}$*,* $1 \leq j \leq m$*, we have*

$$\mathcal{P}_{N,\vec{\mathbf{k}}}^{m}(1) = (q^m - 1) \prod_{j=1}^{m} \Big(\sum_{t=0}^{k_j} \binom{N}{t} (q-1)^t \Big).$$

(iii) $\mathcal{P}_{N,\vec{\mathbf{k}}}^{m}(N) = 0$ *if* $1 \leq k_j \leq N$ *for* $1 \leq j \leq m$.

Suppose that q is a primitive element modulo the prime $N \geq 3$. Then the joint linear complexity of any m-fold N-periodic multisequence over $\mathbb{F}_q$ is either $0, 1, N-1$, or N (see [14, Corollary 3]). By the above propositions, for suitable values of k and $\vec{\mathbf{k}}$ we obtain the following formulas for the number of m-fold N-periodic multisequences over $\mathbb{F}_q$ with error linear complexity $N-1$ (see [13, Corollary 4.1] for the case $m = 1$).

Corollary 5.1 *Let* $m \geq 1$*, let* $N \geq 3$ *be a prime with* $\gcd(N, q) = 1$*, and let* q *be a primitive element modulo* N*. Then we have:*
(i) *For* $m \leq k \leq (N-1)/2$,

$$\mathcal{P}_{N,k}^{m}(N-1) = q^{mN} - q^m \sum_{t=0}^{k} \binom{mN}{t} (q-1)^t.$$

(ii) *For* $1 \leq k \leq (N-1)/2$,

$$\mathcal{P}_{N,k}^{m,q}(N-1) = q^{mN} - q^m \sum_{t=0}^{k} \binom{N}{t} (q^m - 1)^t.$$

(iii) *If* $1 \leq k_j \leq (N-1)/2$ *for* $1 \leq j \leq m$,

$$\mathcal{P}_{N,\vec{\mathbf{k}}}^{m}(N-1) = q^{mN} - q^m \prod_{j=1}^{m} \Big(\sum_{t=0}^{k_j} \binom{N}{t} (q-1)^t \Big).$$

Consequently, for the case where q is a primitive element modulo the prime $N \geq 3$, we know the formulas for the counting function for all possible values of the error linear complexity with suitable k and $\vec{\mathbf{k}}$. Hence we can calculate $G^m_{N,k}$, $G^{m,q}_{N,k}$, and $G^m_{N,\vec{\mathbf{k}}}$, i.e., the expected values of the k-error joint linear complexity, the k-error $\mathbb{F}_q$-linear complexity, and the $\vec{\mathbf{k}}$-error joint linear complexity of a random m-fold N-periodic multisequence over $\mathbb{F}_q$, respectively. The result is a generalization of the formula for the case $m = 1$ presented in [13, Corollary 4.2].

Corollary 5.2 *Let $m \geq 1$, let $N \geq 3$ be a prime with $\gcd(N, q) = 1$, and let q be a primitive element modulo N. Then the expected values for the error linear complexities of m-fold N-periodic multisequences over $\mathbb{F}_q$ are given by:*
(i) *For $m \leq k \leq (N-1)/2$,*

$$G^m_{N,k} = N - 1 - \frac{q^m(N-2)+1}{q^{mN}} \sum_{t=0}^{k} \binom{mN}{t} (q-1)^t.$$

(ii) *For $1 \leq k \leq (N-1)/2$,*

$$G^{m,q}_{N,k} = N - 1 - \frac{q^m(N-2)+1}{q^{mN}} \sum_{t=0}^{k} \binom{N}{t} (q^m-1)^t.$$

(iii) *For $\vec{\mathbf{k}} = (k_1, \dots, k_m)$ with $1 \leq k_j \leq (N-1)/2$ for $1 \leq j \leq m$,*

$$G^m_{N,\vec{\mathbf{k}}} = N - 1 - \frac{q^m(N-2)+1}{q^{mN}} \prod_{j=1}^{m} (\sum_{t=0}^{k_j} \binom{N}{t} (q-1)^t).$$

6 Expected Values for the Error Linear Complexity of Periodic Multisequences

In this section we establish lower bounds on the expected values $G^m_{N,k}$, $G^{m,q}_{N,k}$, and $G^m_{N,\vec{\mathbf{k}}}$ for a more general class of multisequences with prime period. For exact formulas for $G^m_{N,0} = G^{m,q}_{N,0} = G^m_{N,\vec{\mathbf{0}}}$ for arbitrary periods we refer to [14, Theorem 1] and [7, Remark 2].

Let $\mathcal{R}^m_{N,k}(L)$, $\mathcal{R}^{m,q}_{N,k}(L)$, and $\mathcal{R}^m_{N,\vec{\mathbf{k}}}(L)$ denote the number of m-fold N-periodic multisequences $\mathbf{S}$ over $\mathbb{F}_q$ with $L_{N,k}(\mathbf{S}) \leq L$, $L^q_{N,k}(\mathbf{S}) \leq L$, and $L_{N,\vec{\mathbf{k}}}(\mathbf{S}) \leq L$, respectively, that is,

$$\mathcal{R}^m_{N,k}(L) = \sum_{t=0}^{L} \mathcal{P}^m_{N,k}(t), \ \mathcal{R}^{m,q}_{N,k}(L) = \sum_{t=0}^{L} \mathcal{P}^{m,q}_{N,k}(t), \ \mathcal{R}^m_{N,\vec{\mathbf{k}}}(L) = \sum_{t=0}^{L} \mathcal{P}^m_{N,\vec{\mathbf{k}}}(t).$$

If N is a prime with $\gcd(N, q) = 1$ and l is the multiplicative order of q modulo N, then any N-periodic multisequence with terms in $\mathbb{F}_q$ has linear complexity L of the form $L = rl$ or $L = rl + 1$ with $0 \leq r \leq (N-1)/l$ (see [14, Corollary 3]).

Thus, if $l \geq 2$, then for $L = rl + s$ with $0 \leq r < (N-1)/l$ and $1 < s < l$ we have $\mathcal{P}^m_{N,0}(L) = 0$ and $\mathcal{R}^m_{N,0}(L) = \mathcal{R}^m_{N,0}(rl+1)$. For this case, with [14, Corollary 3] we obtain for $1 \leq r \leq \frac{N-1}{l}$ that

$$\mathcal{R}^m_{N,0}(rl) = \mathcal{R}^{m,q}_{N,0}(rl) = \mathcal{R}^m_{N,\vec{\mathbf{0}}}(rl) = q^m \sum_{i=0}^{r-1} \binom{\frac{N-1}{l}}{i} (q^{lm}-1)^i + \binom{\frac{N-1}{l}}{r} (q^{lm}-1)^r$$

and

$$\mathcal{R}^m_{N,0}(rl+1) = \mathcal{R}^{m,q}_{N,0}(rl+1) = \mathcal{R}^m_{N,\vec{\mathbf{0}}}(rl+1) = q^m \sum_{i=0}^{r} \binom{\frac{N-1}{l}}{i} (q^{lm}-1)^i.$$

If N is a prime dividing $q-1$ (that is, if $l = 1$), then

$$\mathcal{R}^m_{N,0}(L) = \mathcal{R}^{m,q}_{N,0}(L) = \mathcal{R}^m_{N,\vec{\mathbf{0}}}(L) = \sum_{t=0}^{L} \binom{N}{t} (q^m-1)^t, \ 0 \leq L \leq N.$$

The fact that $\mathcal{R}^m_{N,k}(L)$ is the cardinality of the union of the balls of radius k with term distance metric around all matrices $\mathbf{S} \in \mathbb{F}_q^{m \times N}$ for which the corresponding multisequence has joint linear complexity at most L yields the following obvious upper bound which is similar to that in Proposition 3.3. The other parts of the following proposition use the same argument with the appropriate metric.

Proposition 6.1 *For all integers $m \geq 1$, $N \geq 1$, and $0 \leq L \leq N$, we have*

$$\mathcal{R}^m_{N,k}(L) \leq \min\left(q^{mN}, \mathcal{R}^m_{N,0}(L) \sum_{t=0}^{k} \binom{mN}{t} (q-1)^t\right), \ 0 \leq k \leq mN,$$

$$\mathcal{R}^{m,q}_{N,k}(L) \leq \min\left(q^{mN}, \mathcal{R}^{m,q}_{N,0}(L) \sum_{t=0}^{k} \binom{N}{t} (q^m-1)^t\right), \ 0 \leq k \leq N,$$

$$\mathcal{R}^m_{N,\vec{\mathbf{k}}}(L) \leq \min\left(q^{mN}, \mathcal{R}^m_{N,\vec{\mathbf{0}}}(L) \prod_{j=1}^{m} \Big(\sum_{t=0}^{k_j} \binom{N}{t} (q-1)^t\Big)\right), \ \vec{\mathbf{k}} = (k_1, \ldots, k_m)$$

with $0 \leq k_j \leq N, \ 1 \leq j \leq m.$

The next lemma, which is an analog of Lemma 4.1, enables us to express the expected values by means of the respective counting functions.

Lemma 6.1 *For all integers $m \geq 1$ and $N \geq 1$, the expected values $G^m_{N,k}$, $G^{m,q}_{N,k}$, and $G^m_{N,\vec{\mathbf{k}}}$ for the error linear complexity measures of a random m-fold N-periodic multisequence over $\mathbb{F}_q$ are given by*

$$G^m_{N,k} = N - \frac{1}{q^{mN}} \sum_{L=0}^{N-1} \mathcal{R}^m_{N,k}(L), \ 0 \leq k \leq mN,$$

$$G^{m,q}_{N,k} = N - \frac{1}{q^{mN}} \sum_{L=0}^{N-1} \mathcal{R}^{m,q}_{N,k}(L), \ 0 \leq k \leq N,$$

$$G^m_{N,\vec{\mathbf{k}}} = N - \frac{1}{q^{mN}} \sum_{L=0}^{N-1} \mathcal{R}^m_{N,\vec{\mathbf{k}}}(L), \ \vec{\mathbf{k}} = (k_1, \ldots, k_m) \text{ with } 0 \leq k_j \leq N, \ 1 \leq j \leq m.$$

Let us now return to the case where N is a prime with $\gcd(N,q)=1$. Using the fact that $\mathcal{R}^m_{N,k}(L)=\mathcal{R}^m_{N,k}(rl+1)$ for $L=rl+s$ and $1<s<l$, where l again denotes the multiplicative order of q modulo N, we get the following corollary.

Corollary 6.1 *Let $m\geq 1$, let N be a prime with $\gcd(N,q)=1$, and let l be the multiplicative order of q modulo N. Then we have*

$$G^m_{N,k}=N-\frac{1}{q^{mN}}\left((l-1)\sum_{r=0}^{\frac{N-1}{l}-1}\mathcal{R}^m_{N,k}(rl+1)+\sum_{r=0}^{\frac{N-1}{l}}\mathcal{R}^m_{N,k}(rl)\right),\ 0\leq k\leq mN,$$

$$G^{m,q}_{N,k}=N-\frac{1}{q^{mN}}\left((l-1)\sum_{r=0}^{\frac{N-1}{l}-1}\mathcal{R}^{m,q}_{N,k}(rl+1)+\sum_{r=0}^{\frac{N-1}{l}}\mathcal{R}^{m,q}_{N,k}(rl)\right),\ 0\leq k\leq N,$$

$$G^m_{N,\vec{\mathbf{k}}}=N-\frac{1}{q^{mN}}\left((l-1)\sum_{r=0}^{\frac{N-1}{l}-1}\mathcal{R}^m_{N,\vec{\mathbf{k}}}(rl+1)+\sum_{r=0}^{\frac{N-1}{l}}\mathcal{R}^m_{N,\vec{\mathbf{k}}}(rl)\right),\ \vec{\mathbf{k}}=(k_1,\ldots,k_m)$$

with $0\leq k_j\leq N,\ 1\leq j\leq m$.

Now we establish lower bounds on $G^m_{N,k}$, $G^{m,q}_{N,k}$, and $G^m_{N,\vec{\mathbf{k}}}$ using the above corollary.

Theorem 6.1 *Let $m\geq 1$, let N be a prime with $\gcd(N,q)=1$, and let $l\geq 2$ be the multiplicative order of q modulo N. For a given k with $0\leq k\leq mN$, let β be the largest nonnegative integer such that*

$$\mathcal{R}^m_{N,0}(\beta l+1)\sum_{t=0}^{k}\binom{mN}{t}(q-1)^t\leq q^{mN},$$

where we put $\beta=-1$ if there is no such nonnegative integer. Then for the expected value $G^m_{N,k}$ of the k-error joint linear complexity of a random m-fold N-periodic multisequence over $\mathbb{F}_q$ we have

$$\begin{aligned}G^m_{N,k}\ \geq\ & l(\beta+1)-\frac{1}{q^{mN}}\left(\sum_{t=0}^{k}\binom{mN}{t}(q-1)^t\right)\\ &\cdot\sum_{i=0}^{\beta}\binom{\frac{N-1}{l}}{i}(q^ml(\beta-i+1)-q^m+1)(q^{lm}-1)^i.\end{aligned}$$

Proof : We establish the lower bound on $G^m_{N,k}$ by determining an upper bound for

$$\Omega:=(l-1)\sum_{r=0}^{\frac{N-1}{l}-1}\mathcal{R}^m_{N,k}(rl+1)+\sum_{r=0}^{\frac{N-1}{l}}\mathcal{R}^m_{N,k}(rl).$$

Proposition 6.1 yields

$$\Omega \le (l-1)\sum_{r=0}^{\frac{N-1}{l}-1} \min\left(q^{mN}, \mathcal{R}^m_{N,0}(rl+1)\sum_{t=0}^{k}\binom{mN}{t}(q-1)^t \right)$$

$$+\sum_{r=0}^{\frac{N-1}{l}} \min\left(q^{mN}, \mathcal{R}^m_{N,0}(rl)\sum_{t=0}^{k}\binom{mN}{t}(q-1)^t \right).$$

From the inequality

$$\mathcal{R}^m_{N,0}(\beta l+1)\sum_{t=0}^{k}\binom{mN}{t}(q-1)^t \le q^{mN},$$

where we put $\beta = -1$ if there is no such nonnegative integer and with empty sums being 0 as usual, we obtain

$$\begin{aligned}\Omega \quad &\le \quad (l-1)\Big(\sum_{r=0}^{\beta}\mathcal{R}^m_{N,0}(rl+1)\sum_{t=0}^{k}\binom{mN}{t}(q-1)^t + \sum_{r=\beta+1}^{\frac{N-1}{l}-1} q^{mN}\Big) \\ &\quad +\sum_{r=0}^{\beta}\mathcal{R}^m_{N,0}(rl)\sum_{t=0}^{k}\binom{mN}{t}(q-1)^t + \sum_{r=\beta+1}^{\frac{N-1}{l}} q^{mN}. \qquad (4)\end{aligned}$$

Using the formulas for $\mathcal{R}^m_{N,0}(rl)$ and $\mathcal{R}^m_{N,0}(rl+1)$ for $l \ge 2$, we get

$$\begin{aligned}\Omega \quad &\le \quad (N-l(\beta+1))q^{mN} + \left(\sum_{t=0}^{k}\binom{mN}{t}(q-1)^t\right) \\ &\quad \cdot\Bigg\{(l-1)q^m\sum_{r=0}^{\beta}\sum_{i=0}^{r}\binom{\frac{N-1}{l}}{i}(q^{lm}-1)^i \\ &\quad +\sum_{r=0}^{\beta}\left(q^m\sum_{i=0}^{r-1}\binom{\frac{N-1}{l}}{i}(q^{lm}-1)^i + \binom{\frac{N-1}{l}}{r}(q^{lm}-1)^r\right)\Bigg\} \\ &= \quad (N-l(\beta+1))q^{mN} + \left(\sum_{t=0}^{k}\binom{mN}{t}(q-1)^t\right) \\ &\quad \cdot\left\{lq^m\sum_{r=0}^{\beta}\sum_{i=0}^{r}\binom{\frac{N-1}{l}}{i}(q^{lm}-1)^i - (q^m-1)\sum_{r=0}^{\beta}\binom{\frac{N-1}{l}}{r}(q^{lm}-1)^r\right\} \\ &= \quad (N-l(\beta+1))q^{mN} + \left(\sum_{t=0}^{k}\binom{mN}{t}(q-1)^t\right) \\ &\quad \cdot\sum_{i=0}^{\beta}\binom{\frac{N-1}{l}}{i}(q^m l(\beta-i+1)-q^m+1)(q^{lm}-1)^i.\end{aligned}$$

With the formula in Corollary 6.1 we obtain the desired lower bound on $G^m_{N,k}$. □

A similar calculation yields the following lower bounds on the expected value of the k-error $\mathbb{F}_q$-linear complexity and the expected value of the $\vec{\mathbf{k}}$-error joint linear complexity of a random m-fold N-periodic multisequence, N prime.

Theorem 6.2 *Let $m \geq 1$, let N be a prime with $\gcd(N, q) = 1$, and let $l \geq 2$ be the multiplicative order of q modulo N. For a given k with $0 \leq k \leq N$, let β be the largest nonnegative integer such that*

$$\mathcal{R}^m_{N,0}(\beta l + 1) \sum_{t=0}^{k} \binom{N}{t} (q^m - 1)^t \leq q^{mN},$$

where we put $\beta = -1$ if there is no such nonnegative integer. Then for the expected value $G^{m,q}_{N,k}$ of the k-error $\mathbb{F}_q$-linear complexity of a random m-fold N-periodic multisequence over $\mathbb{F}_q$ we have

$$\begin{aligned} G^{m,q}_{N,k} &\geq l(\beta+1) - \frac{1}{q^{mN}} \left(\sum_{t=0}^{k} \binom{N}{t} (q^m - 1)^t \right) \\ &\quad \cdot \sum_{i=0}^{\beta} \binom{\frac{N-1}{l}}{i} (q^m l(\beta - i + 1) - q^m + 1)(q^{lm} - 1)^i. \end{aligned}$$

Theorem 6.3 *Let $m \geq 1$, let N be a prime with $\gcd(N, q) = 1$, and let $l \geq 2$ be the multiplicative order of q modulo N. For a given $\vec{\mathbf{k}} = (k_1, \ldots, k_m)$ with $0 \leq k_j \leq N$ for $1 \leq j \leq m$, let β be the largest nonnegative integer such that*

$$\mathcal{R}^m_{N,\vec{\mathbf{0}}}(\beta l + 1) \prod_{j=1}^{m} \left(\sum_{t=0}^{k_j} \binom{N}{t} (q - 1)^t \right) \leq q^{mN},$$

where we put $\beta = -1$ if there is no such nonnegative integer. Then for the expected value $G^m_{N,\vec{\mathbf{k}}}$ of the $\vec{\mathbf{k}}$-error joint linear complexity of a random m-fold N-periodic multisequence over $\mathbb{F}_q$ we have

$$\begin{aligned} G^m_{N,\vec{\mathbf{k}}} &\geq l(\beta+1) - \frac{1}{q^{mN}} \left(\prod_{j=1}^{m} (\sum_{t=0}^{k_j} \binom{N}{t} (q - 1)^t) \right) \\ &\quad \cdot \sum_{i=0}^{\beta} \binom{\frac{N-1}{l}}{i} (q^m l(\beta - i + 1) - q^m + 1)(q^{lm} - 1)^i. \end{aligned}$$

Remark 6.1 If $\beta = -1$, then the expression on the right-hand side of (4) reduces to Nq^{mN} and the lower bound in Theorem 6.1 vanishes. For $\beta \geq 0$ the expression in (4) is less than Nq^{mN}. Hence the lower bound in Theorem 6.1 is nontrivial if and only if $\beta \geq 0$. The same argument is valid for the other two cases considered in Theorem 6.2 and Theorem 6.3.

Remark 6.2 If $k = 0$ and consequently $\beta = (N-1)/l$, then we have equalities in the proof of Theorem 6.1 and the bound reduces to the exact value (see [14, Corollary 6])

$$G_{N,0}^{m} = G_{N,0}^{m,q} = G_{N,\vec{\mathbf{0}}}^{m} = (N-1)(1-\frac{1}{q^{lm}}) + 1 - \frac{1}{q^{m}}.$$

7 Conclusions

The goal of this paper has been the extension of the stability theory of stream ciphers and the theory of error linear complexity measures from single sequences to multisequences. The case of multisequences is relevant for the design and the analysis of word-based stream ciphers. For multisequences there are various possibilities of defining analogs of the k-error linear complexity of single sequences. We considered the k-error joint linear complexity, the k-error $\mathbb{F}_q$-linear complexity, and the $\vec{\mathbf{k}}$-error joint linear complexity for finite as well as for periodic multisequences. Various enumeration results and lower bounds on the expected values of these error linear complexity measures were established.

This is only the beginning of the theory of error linear complexity measures for multisequences and a lot remains to be done. The general aim should be to find analogs of all major results on the k-error linear complexity of single sequences (see the survey [15]) for the case of multisequences.

Acknowledgment

The research of the second author is supported in part by the DSTA research grant R-394-000-025-422 with Temasek Laboratories in Singapore.

References

[1] E.R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.

[2] Z. Dai, K. Imamura, J. Yang, Asymptotic behavior of normalized linear complexity of multi-sequences, in: T. Helleseth, D. Sarwate, H.-Y. Song, K. Yang (Eds.), Sequences and Their Applications – SETA 2004, Lecture Notes in Computer Science, vol. 3486, Springer, Berlin, 2005, pp. 129–142.

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

[4] C. Ding, Lower bounds on the weight complexities of cascaded binary sequences, in: J. Seberry, J. Pieprzyk (Eds.), Advances in Cryptology – AUSCRYPT '90, Lecture Notes in Computer Science, vol. 453, Springer, Berlin, 1990, pp. 39–43.

[5] C. Ding, G. Xiao, W. Shan, The Stability Theory of Stream Ciphers, Lecture Notes in Computer Science, vol. 561, Springer, Berlin, 1991.

[6] X. Feng, Z. Dai, Expected value of the linear complexity of two-dimensional binary sequences, in: T. Helleseth, D. Sarwate, H.-Y. Song, K. Yang (Eds.), Sequences and Their Applications – SETA 2004, Lecture Notes in Computer Science, vol. 3486, Springer, Berlin, 2005, pp. 113–128.

[7] F.-W. Fu, H. Niederreiter, M. Su, The expectation and variance of the joint linear complexity of random periodic multisequences, J. Complexity 21 (2005) 804–822.

[8] 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.

[9] P. Hawkes, M. Paddon, G.G. Rose, M. Wiggers de Vries, SSS, ECRYPT candidate, http://www.ecrypt.eu.org/stream/ciphers/sss/sss.pdf.

[10] P. Hawkes, M. Paddon, G.G. Rose, M. Wiggers de Vries, NLS, ECRYPT candidate, http://www.ecrypt.eu.org/stream/ciphers/nls/nls.pdf.

[11] J.H. van Lint, Introduction to Coding Theory, Springer, New York, 1982.

[12] W. Meidl, H. Niederreiter, Counting functions and expected values for the k-error linear complexity, Finite Fields Appl. 8 (2002) 142–154.

[13] W. Meidl, H. Niederreiter, Linear complexity, k-error linear complexity, and the discrete Fourier transform, J. Complexity 18 (2002) 87–103.

[14] W. Meidl, H. Niederreiter, The expected value of the joint linear complexity of periodic multisequences, J. Complexity 19 (2003) 61–72.

[15] H. Niederreiter, Linear complexity and related complexity measures for sequences, in: T. Johansson, S. Maitra (Eds.), Progress in Cryptology – INDOCRYPT 2003, Lecture Notes in Computer Science, vol. 2904, Springer, Berlin, 2003, pp. 1–17.

[16] H. Niederreiter, The probabilistic theory of the joint linear complexity of multisequences, in: G. Gong, T. Helleseth, H.-Y. Song, K. Yang (Eds.), Sequences and Their Applications – SETA 2006, Lecture Notes in Computer Science, vol. 4086, Springer, Berlin, 2006, pp. 5–16.

[17] H. Niederreiter, H. Paschinger, Counting functions and expected values in the stability theory of stream ciphers, in: C. Ding, T. Helleseth, H. Niederreiter (Eds.), Sequences and Their Applications, Springer, London, 1999, pp. 318–329.

[18] H. Niederreiter, L.-P. Wang, Proof of a conjecture on the joint linear complexity profile of multisequences, in: S. Maitra, C.E. Veni Madhavan, R. Venkatesan (Eds.), Progress in Cryptology – INDOCRYPT 2005, Lecture Notes in Computer Science, vol. 3797, Springer, Berlin, 2005, pp. 13–22.

[19] H. Niederreiter, L.-P. Wang, The asymptotic behavior of the joint linear complexity profile of multisequences, Monatsh. Math., to appear.

[20] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer, Berlin, 1986.

[21] S. Sakata, Extension of the Berlekamp-Massey algorithm to N dimensions, Inform. and Comput. 84 (1990) 207–239.

[22] B. Smeets, The linear complexity profile and experimental results on a randomness test of sequences over the field $\mathbf{F}_q$, Technical Report, University of Lund, 1988.

[23] M. Stamp, C.F. Martin, An algorithm for the k-error linear complexity of binary sequences with period 2^n, IEEE Trans. Inform. Theory 39 (1993) 1398–1401.

[24] L.-P. Wang, H. Niederreiter, Enumeration results on the joint linear complexity of multisequences, Finite Fields Appl. 12 (2006) 613–637.

[25] 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.