Improved results on periodic multisequences with large error linear complexity

Ayineedi Venkateswarlu\textsuperscript{a,}\textsuperscript{*}, Harald Niederreiter\textsuperscript{b}

\textsuperscript{a} C. R. Rao AIMSCS, University of Hyderabad Campus, Prof. C. R. Rao Road, Gachibowli, Hyderabad-500046, India
\textsuperscript{b} Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstraße 69, A-4040 Linz, Austria

\textbf{ARTICLE INFO}

Article history:
Received 30 June 2010
Revised 28 August 2010
Accepted 7 September 2010
Available online 21 September 2010
Communicated by Arne Winterhof

MSC:
94A55
94A60
11B50

Keywords:
Multisequences
Joint linear complexity
Error linear complexity
Word-based stream ciphers

\textbf{ABSTRACT}

For multisequences there are various possibilities of defining analogs of the $k$-error linear complexity of single sequences. We consider the $k$-error joint linear complexity, the $k$-error $\mathbb{F}_q$-linear complexity, and the $\vec{k}$-error joint linear complexity. Improving the existing results, several results on the existence of, and lower bounds on the number of, multisequences with large error linear complexity are obtained. Improved lower bounds are shown for the case of prime-power periodic multisequences. An asymptotic analysis for the prime-power period case is carried out.

\textcopyright{} 2010 Elsevier Inc. All rights reserved.


1. Introduction

The theory of word-based stream ciphers [1–3] requires the study of complexity measures for multisequences, i.e., for parallel streams of finitely many sequences. In this direction, joint linear complexity, joint linear complexity profile, and error linear complexity of multisequences have been investigated (see [4–8]). We consider the $k$-error joint linear complexity, the $k$-error $\mathbb{F}_q$-linear complexity, and the $\vec{k}$-error joint linear complexity, and in the present paper we find analogs and im-
provements of some of the results on the $k$-error linear complexity of single sequences for the case of multisequences.

A good keystream sequence must not only possess a large linear complexity, but also a large $k$-error linear complexity for relatively high values of $k$. Therefore it is interesting to find suitable parameters for which we can make the linear complexity and the error linear complexity simultaneously large. In the book of Ding, Xiao, and Shan [9, Section 7.1], a belief has been expressed that there may be a trade-off between the linear complexity $L(S)$ and the $k$-error linear complexity $L_{N,k}(S)$ (or rather the closely related $k$-error sphere complexity) of a periodic sequence $S$. In particular, it has been conjectured that for any $N$-periodic binary sequence $S$ and for any positive integer $k \leq N$ we have

$$SC_{N,k}(S) + L(S) \leq \left(1 + \frac{1}{k}\right)N - 1,$$

where $SC_{N,k}(S)$ is the $k$-error sphere complexity of the sequence $S$. One can see that $L_{N,k}(S) = \min(SC_{N,k}(S), L(S))$, and so the above conjecture (1) would also be valid with the replacement of $SC_{N,k}(S)$ by $L_{N,k}(S)$. In [10] the conjecture has been disproved by providing several examples for which the inequality (1) is not valid for many values of $k$. In fact, one of the results in that paper shows that for almost all primes $N$ there exist $N$-periodic single sequences over $\mathbb{F}_2$ with maximal linear complexity $N$ and $k$-error linear complexity equal to $N - 1$, for relatively large values of $k \geq 1$.

Extending this result, in [11, Theorem 1] it has been proved that there are infinitely many primes $N$ such that there exist $N$-periodic single sequences over an arbitrary but fixed finite field $\mathbb{F}_q$ with maximal linear complexity $N$ and $k$-error linear complexity at least $N - 1$ for all positive integers $k \leq N^{0.677}/(2 \log N)$. In a more general case, the problem of what proportion of single sequences have large $k$-error linear complexity relative to the period length $N$, among all $N$-periodic single sequences with maximal linear complexity $N$, was considered in [12]. In a different direction, the $k$-error linear complexity over $\mathbb{F}_p$ of Legendre and Sidelnikov (binary) sequences, where $p$ is an odd prime, was considered in [13], and it was shown that the inequality (1) is violated for many values of $k$. Recently, Hu et al. [14] established improved lower bounds and asymptotic results for the case of single sequences. In the present paper, we will show that analogous results are also valid in the case of multisequences. In fact, we will present refined results in Sections 3 and 4 by combining ideas from [6] and [14].

2. Preliminaries

Throughout this paper, let $\mathbb{F}_q$ denote the finite field containing $q$ elements and let $p$ be the characteristic of $\mathbb{F}_q$.

2.1. Joint linear complexity

Let $m$ and $N$ be two positive integers. We denote an $m$-fold $N$-periodic multisequence consisting of $m$ parallel streams of $N$-periodic sequences $S_1, \ldots, S_m$ over $\mathbb{F}_q$ by $\vec{S} = (S_1, \ldots, S_m)$. The joint linear complexity $L(\vec{S}) = L(S_1, \ldots, S_m)$ of $\vec{S}$ is the least order of a linear recurrence relation over $\mathbb{F}_q$ that simultaneously generates each sequence $S_u$, $1 \leq u \leq m$. We have the following result on the joint linear complexity of periodic multisequences [15, p. 65].

**Theorem 2.1.** Let $\vec{S} = (S_1, \ldots, S_m)$ be an $m$-fold $N$-periodic multisequence over $\mathbb{F}_q$ and let $S_u = (s_{u1}, s_{u2}, \ldots, s_{uN})^\infty$ for $1 \leq u \leq m$. Then the joint linear complexity of the multisequence $\vec{S}$ is given by

$$L(\vec{S}) = N - \deg(\gcd(s_1^{(N)}(x), \ldots, s_m^{(N)}(x), x^N - 1)),$$

where $s_u^{(N)}(x) = s_{u1} + s_{u2}x + \cdots + s_{uN}x^{N - 1}$ is the generating function of $S_u$. 

From the identity (2) above, one can observe that the possible values of $L(\vec{S})$, for a given period length $N$, depend on the factorization of $x^N - 1$. In this and the next section we let: $N = p^n v$ be a positive integer with integers $v \geq 0$ and $n \geq 1$ such that gcd($n, q$) = 1; $n_1, n_2, \ldots, n_r$ be the distinct positive divisors of $n$; $d_i$ be the multiplicative order of $q$ modulo $n_i$ for $1 \leq i \leq r$. Then we have the canonical factorization

$$x^N - 1 = \prod_{i=1}^r \prod_{j=1}^{h_i} f_{ij}(x)^{p^v}$$

over $\mathbb{F}_q$, where $h_i = \frac{\phi(n_i)}{d_i}$ and each $f_{ij}(x)$ is a monic irreducible polynomial of degree $d_i$ over $\mathbb{F}_q$ (see [16, Section 2.4]).

We use the ideas presented in [4,6] on the polynomial vector interpretation of periodic multisequences. The corresponding system of congruences of polynomial vectors modulo the irreducible polynomials $f_{ij}$, $1 \leq j \leq h_i$ and $1 \leq i \leq r$, in the proofs below. For convenience let us recall some basic identities on the polynomial vector interpretation of multisequences. With the notation for the canonical factorization of $x^N - 1$ above, for each $u = 1, \ldots, m$, we consider the system of polynomial congruences

$$S_u^{(N)}(x) \equiv s_{ij}^{(u)}(x) \mod f_{ij}(x)^{p^v} \quad \text{for } 1 \leq i \leq r \text{ and } 1 \leq j \leq h_i, \quad (3)$$

where the $s_{ij}^{(u)}(x)$ are given polynomials over $\mathbb{F}_q$ of degree less than $d_i p^v$. Let $\vec{S}^{(N)}(x) = (s_1^{(N)}(x), \ldots, s_m^{(N)}(x))$ and $\vec{s}_{ij}(x) = (s_{ij}^{(1)}(x), \ldots, s_{ij}^{(m)}(x))$, and then by (3) we have

$$\vec{S}^{(N)}(x) \equiv \vec{s}_{ij}(x) \mod f_{ij}(x)^{p^v} \quad \text{for } 1 \leq i \leq r \text{ and } 1 \leq j \leq h_i, \quad (4)$$

where the congruence is meant to hold componentwise. Then one can check that, by the identities (2) and (4), the joint linear complexity of $\vec{S}$ is given by

$$L(\vec{S}) = \sum_{i=1}^r \sum_{j=1}^{h_i} (p^v - w_{ij})d_i, \quad (5)$$

where $w_{ij}$ is the largest integer $\leq p^v$ such that $f_{ij}(x)^{w_{ij}}$ divides $s_{ij}^{(u)}(x)$ for all $u = 1, \ldots, m$.

### 2.2. Error linear complexity measures for periodic multisequences

An $m$-fold $N$-periodic multisequence $\vec{S}$ can be interpreted as an $m \times N$ matrix over $\mathbb{F}_q$. The following definitions of term, column, term distance, and column distance also suit this interpretation (see also [6, Section 2.3]).

Let $\vec{S} = (S_1, \ldots, S_m)$ be an $m$-fold multisequence over $\mathbb{F}_q$. A term in $\vec{S}$ is defined to be a term of $S_u$ for some $u$, $1 \leq u \leq m$. A column in $\vec{S}$ is meant to be the column vector $(s_{11}, \ldots, s_{mi})$ in $\mathbb{F}_q^m$ formed by the $i$th terms of $S_1, \ldots, S_m$, for some integer $i \geq 1$.

**Definition 2.1.** Let $\vec{S} = (S_1, \ldots, S_m)$ and $\vec{T} = (T_1, \ldots, T_m)$ be two $m$-fold $N$-periodic multisequences over $\mathbb{F}_q$ and denote the $m \times N$ matrix of the first period of $\vec{S}$ and $\vec{T}$ by $S$ and $T$, respectively. We define the term distance $\delta_T(\vec{S}, \vec{T})$ between $\vec{S}$ and $\vec{T}$ as the number of entries in $S$ that are different from the corresponding entries in $T$, and the column distance $\delta_C(\vec{S}, \vec{T})$ as the number of columns in $S$ that are different from the corresponding columns in $T$. We define the individual distances vector by $\delta_{ij}(\vec{S}, \vec{T}) = (\delta_{11}, \ldots, \delta_{mi})$, where $\delta_u$ is the Hamming distance between the $u$th rows of $S$ and $T$ for $1 \leq u \leq m$. 
Definition 2.2. Let \( \vec{S} \) be an \( m \)-fold \( N \)-periodic multisequence over \( \mathbb{F}_q \). For an integer \( k \) with \( 0 \leq k \leq mN \), the \( k \)-error joint linear complexity \( L_k(\vec{S}) \) of \( \vec{S} \) is given by

\[
L_k(\vec{S}) = \min_{\vec{T}} L(\vec{T}),
\]

where the minimum is taken over all \( m \)-fold \( N \)-periodic multisequences \( \vec{T} \) over \( \mathbb{F}_q \) with term distance \( \delta_T(\vec{S}, \vec{T}) \leq k \).

Definition 2.3. Let \( \vec{S} \) be an \( m \)-fold \( N \)-periodic multisequence over \( \mathbb{F}_q \). For an integer \( k \) with \( 0 \leq k \leq N \), the \( k \)-error \( \mathbb{F}_q \)-linear complexity \( L^q_k(\vec{S}) \) of \( \vec{S} \) is given by

\[
L^q_k(\vec{S}) = \min_{\vec{T}} L(\vec{T}),
\]

where the minimum is taken over all \( m \)-fold \( N \)-periodic multisequences \( \vec{T} \) over \( \mathbb{F}_q \) with column distance \( \delta_C(\vec{S}, \vec{T}) \leq k \).

For \( \vec{k} = (k_1, \ldots, k_m) \) and \( \vec{k}' = (k_1', \ldots, k_m') \) in \( \mathbb{Z}^m \), we say that \( \vec{k} \leq \vec{k}' \) if \( k_u \leq k_u' \) for \( 1 \leq u \leq m \), which induces a partial order on \( \mathbb{Z}^m \).

Definition 2.4. Let \( \vec{S} = (S_1, \ldots, S_m) \) be an \( m \)-fold \( N \)-periodic multisequence over \( \mathbb{F}_q \). For \( \vec{k} = (k_1, \ldots, k_m) \in \mathbb{Z}^m \) with \( 0 \leq k_u \leq N \) for \( 1 \leq u \leq m \), the \( \vec{k} \)-error joint linear complexity \( L_k(\vec{S}) \) of \( \vec{S} \) is given by

\[
L_k(\vec{S}) = \min_{\vec{T}} L(\vec{T}),
\]

where the minimum is taken over all \( m \)-fold \( N \)-periodic multisequences \( \vec{T} \) over \( \mathbb{F}_q \) with \( \delta_V(\vec{S}, \vec{T}) \leq \vec{k} \).

Suppose the term distance \( \delta_T(\vec{S}, \vec{T}) \) between two \( m \)-fold \( N \)-periodic multisequences \( \vec{S} \) and \( \vec{T} \) over \( \mathbb{F}_q \) is equal to \( k \). Then the error positions in \( \vec{S} \) can be identified with a multisequence \( \vec{E} \), which is the termwise difference between \( \vec{S} \) and \( \vec{T} \), having \( k \) nonzero terms in each period of length \( N \). Furthermore, we have the relation

\[
\vec{S}^{(N)}(x) - \vec{T}^{(N)}(x) = \vec{E}^{(N)}(x)
\]

between the corresponding polynomial vectors. Similar identities can be obtained for the other two cases, the column distance and the individual distances vector.

3. Lower bounds

For cryptographic purposes one is interested in (multi)sequences with a guaranteed large error (joint) linear complexity. We now prove an improved lower bound on the \( k \)-error joint linear complexity of multisequences that have maximum joint linear complexity \( N \). We also present a lower bound on the number of such multisequences.

First we present a lemma which is used in the proof of Theorem 3.1. For this purpose we define a set \( \mathcal{E}_1(N, k) \) of admissible errors with respect to the term distance. Let \( k \) be an integer such that \( 1 \leq k \leq mN \). Let \( \mathcal{E}_1(N, k) \) be the set of all polynomial vectors corresponding to \( m \)-fold \( N \)-periodic nonzero multisequences over \( \mathbb{F}_q \) with \( k \) or fewer nonzero elements and let \( \mathcal{E}_1(N, k, f(x)^l) \) denote the set

\[
\{ \vec{E}^{(N)}(x) \mod f(x)^l : \vec{E}^{(N)}(x) \in \mathcal{E}_1(N, k) \}
\]
for any irreducible factor $f(x)$ of $x^N - 1$ and any integer $l$ with $1 \leq l \leq p^v$.

**Lemma 3.1.** Let $E_1(N, k)$ be as defined above. Let $f(x)$ be an irreducible factor of $x^N - 1$ of order $n_i$ and let $l$ be an integer such that $1 \leq l + 1 \leq p^v$. Let $w$ be the least integer with $p^w \geq l + 1$. Then the number of distinct residue classes in $E_1(N, k)$ modulo $f(x)^{l+1}$ satisfies

$$|E_1(N, k, f(x)^{l+1})| \leq \sum_{\tau=1}^{k} \left( \frac{m p^{w n_i}}{\tau} \right) (q - 1)^{\tau}.$$ 

**Proof.** First note that the order of $f(x)^{l+1}$ is $p^w n_i$ by [16, Theorem 3.8]. For any $\vec{E}^{(N)}(x) \in E_1(N, k)$, a component $E_{u}^{(N)}(x)$, $1 \leq u \leq m$, of the polynomial vector $\vec{E}^{(N)}(x)$ is of the form

$$E_{u}^{(N)}(x) = \sum_{j=1}^{k_u} e_{uj} x^{b_{uj}},$$

where $0 \leq t_{u1} < \cdots < t_{uk_u} < N$, $1 \leq k_1 + \cdots + k_m \leq k$, and $e_{uj} \in \mathbb{F}_q^*$. Let $t_{uj} \equiv b_{uj} \mod p^w n_i$, where $0 \leq b_{uj} < p^w n_i$. Then we have

$$E_{u}^{(N)}(x) \equiv \sum_{j=1}^{k_u} e_{uj} x^{b_{uj}} \mod (x^{p^w n_i} - 1).$$

Since $f(x)^{l+1}(x^{p^w n_i} - 1)$, we obtain

$$E_{u}^{(N)}(x) \equiv \sum_{j=1}^{k_u} e_{uj} x^{b_{uj}} \mod f(x)^{l+1},$$

and hence the result. □

**Theorem 3.1.** Let $k$ be an integer such that $1 \leq k \leq mN$. For each $i = 1, \ldots, r$, we choose $l_i$ as follows: either we have an integer $l_i$ with $p^{w_i - 1} < l_i + 1 \leq p^{w_i}$ for some integer $w_i$, $0 \leq w_i \leq v$, such that

$$M_i := \sum_{\tau=1}^{k} \left( \frac{m p^{w_i n_i}}{\tau} \right) (q - 1)^{\tau} \leq q^{m d_i} (q^{m d_i} - 1),$$

or otherwise we set $l_i = p^v$. Then the number $\Omega_1$ of $m$-fold $N$-periodic multisequences $\vec{S}$ over $\mathbb{F}_q$ with $L(\vec{S}) = N$ and $L_k(\vec{S}) \geq N - \sum_{i=1}^{r} l_i \phi(n_i)$ satisfies

$$\Omega_1 \geq \prod_{\substack{i=1 \atop l_i \neq p^v}}^{r} q^{m h_i d_i (p^v - l_i - 1)} (q^{m d_i} (q^{m d_i} - 1) - M_i) \sum_{\substack{i=1 \atop l_i = p^v}}^{r} q^{m h_i d_i (p^v - 1)} (q^{m d_i} - 1)^{h_i}.$$ 

**Proof.** The proof follows the method of the proof of Theorem 1 in [6]. We first prove the existence of an $m$-fold $N$-periodic multisequence $\vec{S}$ over $\mathbb{F}_q$ with $L(\vec{S}) = N$ and $L_k(\vec{S}) \geq N - \sum_{i=1}^{r} l_i \phi(n_i)$. To show this, we choose a special set of polynomial vectors $\vec{s}_{ij}(x)$ for $1 \leq i \leq r$ and $1 \leq j \leq h_i$ and construct a multisequence $\vec{S}$ from the system of congruences in (4). Let $V_{ij}^{(m)} = (\mathbb{F}_q[x]/(f_{ij}^{l+1}(x)))^m$ be the set of polynomial vectors of dimension $m$ whose components are polynomials of degree less than $d_i(l + 1)$. 


The number of nonzero polynomial vectors modulo \( f_{ij}(x) \) in \( V_{ij}^{l_i} \) is \( q^{md_i}(q^{md_i} - 1) \). Suppose we have an integer \( l_i \), \( p^{w_i - 1} < l_i + 1 \leq p^{w_i} \), for some \( 0 \leq w_i \leq v \) such that

\[
\sum_{\tau=1}^{k} \left( m_{\tau}^{w_i} n_i \right) (q - 1)^{\tau} < q^{md_i}(q^{md_i} - 1).
\]

By Lemma 3.1 we have at most \( \sum_{\tau=1}^{k} \left( m_{\tau}^{w_i} n_i \right) (q - 1)^{\tau} \) distinct residue classes in \( E_1(N, k, f_{ij}(x)^{l_i+1}) \). This implies that there exists a polynomial vector \( \bar{g}_{ij}(x) \) in \( V_{ij}^{l_i} \) satisfying

\[
\bar{g}_{ij}(x) \not\equiv \bar{0} \mod f_{ij}(x) \quad \text{and} \quad \bar{g}_{ij}(x) \not\equiv \bar{E}^{(N)}(x) \mod f_{ij}^{l_i+1}(x) \quad \text{for all} \quad \bar{E}^{(N)}(x) \in E_1(N, k), \quad (6)
\]

for all \( 1 \leq j \leq h_i \). If \( l_i = p^v \), then we choose a polynomial vector \( \bar{g}_{ij}(x) \not\equiv \bar{0} \mod f_{ij}(x) \) whose components are polynomials of degree less than \( d_i \). Set \( \bar{s}_{ij}(x) = \bar{g}_{ij}(x) \). Let \( \bar{S} \) be the multisequence obtained by solving the following system of congruences using the Chinese Remainder Theorem:

\[
\bar{S}^{(N)}(x) \equiv \bar{s}_{ij}(x) \mod f_{ij}^{p^v}(x) \quad \text{for} \quad 1 \leq i \leq r \quad \text{and} \quad 1 \leq j \leq h_i.
\]

Since we have \( \bar{S}^{(N)}(x) \not\equiv \bar{0} \mod f_{ij}(x) \) for all \( 1 \leq i \leq r \) and \( 1 \leq j \leq h_i \), the joint linear complexity of the multisequence \( \bar{S} \) is \( L(\bar{S}) = N \) by (5).

Let \( \bar{T} \neq \bar{S} \) be an \( m \)-fold \( N \)-periodic multisequence over \( \mathbb{F}_q \) which differs from \( \bar{S} \) in \( k \) or fewer positions per period. Then \( \bar{T}^{(N)}(x) = \bar{S}^{(N)}(x) - \bar{E}^{(N)}(x) \) for some \( \bar{E}^{(N)}(x) \in E_1(N, k) \). Note that \( E_1(N, k) \) represents the set of all allowed errors in \( \bar{S} \). If \( l_i \neq p^v \), then \( \bar{T}^{(N)}(x) = \bar{S}^{(N)}(x) - \bar{E}^{(N)}(x) \not\equiv \bar{0} \mod f_{ij}^{l_i+1}(x) \). For otherwise \( \bar{s}_{ij}(x) \equiv \bar{E}^{(N)}(x) \mod f_{ij}^{l_i+1}(x) \) for some \( \bar{E}^{(N)}(x) \in E_1(N, k) \), which is a contradiction to our choice of \( \bar{s}_{ij}(x) \). Therefore \( \text{gcd}(T_1^{(N)}(x), \ldots, T_m^{(N)}(x), x^N - 1) \) must be a factor of \( \prod_{i=1}^{h_i} \prod_{j=1}^{l_i} f_{ij}(x) \). This implies \( L(\bar{T}) \geq N - \sum_{i=1}^{r} h_i l_i d_i \). We recall that \( h_i d_i = \phi(n_i) \), and hence the \( k \)-error joint linear complexity of \( \bar{S} \) satisfies \( L_k(\bar{S}) \geq N - \sum_{i=1}^{r} l_i \phi(n_i) \).

Now we enumerate all possible choices for the \( \bar{s}_{ij}(x) \), \( 1 \leq i \leq r \) and \( 1 \leq j \leq h_i \). For any polynomial vector \( \bar{S}^{(N)}(x) \) corresponding to an \( m \)-fold \( N \)-periodic multisequence \( \bar{S} \) over \( \mathbb{F}_q \), we have the system of congruences

\[
\bar{S}^{(N)}(x) \equiv \bar{s}_{ij}(x) \mod f_{ij}^{p^v}(x) \quad \text{for} \quad 1 \leq i \leq r \quad \text{and} \quad 1 \leq j \leq h_i, \quad (7)
\]

where the components of \( \bar{s}_{ij}(x) \) are polynomials of degree less than \( d_i p^v \). If \( l_i = p^v \), then we set \( \bar{s}_{ij}(x) = \bar{g}_{ij}(x) + f_{ij}(x) \bar{p}_{ij}(x) \), where \( \bar{p}_{ij}(x) \) is a polynomial vector whose components are polynomials of degree less than \( d_i (p^v - l_i - 1) \). Thus, we have \( q^{md_i(l_i+1)}(q^{md_i} - 1) \) choices for \( \bar{s}_{ij}(x) \) in this case. Otherwise, i.e., if \( l_i \neq p^v \), we set \( \bar{s}_{ij}(x) = \bar{g}_{ij}(x) + f_{ij}^{l_i+1}(x) \bar{p}_{ij}(x) \), where \( \bar{p}_{ij}(x) \) is a polynomial vector whose components are polynomials of degree less than \( d_i (p^v - l_i - 1) \). Therefore, in this case, the number of choices for \( \bar{s}_{ij}(x) \) is at least \( q^{md_i(l_i+1)}(q^{md_i} - 1) - \sum_{\tau=1}^{k} \left( m_{\tau}^{w_i} n_i \right) (q - 1)^{\tau} \). Thus, the total number of choices for all \( \bar{s}_{ij}(x) \), \( 1 \leq i \leq r \) and \( 1 \leq j \leq h_i \), is at least

\[
\prod_{i=1}^{r} q^{md_i h_i (p^v - l_i - 1)}(q^{md_i} - 1)^{h_i} - \prod_{i=1}^{r} q^{md_i h_i (p^v - l_i - 1)}(q^{md_i} - 1)^{h_i}.
\]
From the first part of the proof and by applying the Chinese Remainder Theorem, for any such choice of the $\bar{s}_{ij}(x)$, $1 \leq i \leq r$ and $1 \leq j \leq h_1$, the system of congruences in (7) yields an $m$-fold $N$-periodic multisequence $\bar{S}$ over $\mathbb{F}_q$ satisfying $L(\bar{S}) = N$ and $L_k(\bar{S}) \geq N - \sum_{i=1}^r l_i \phi(n_i)$. Hence the result. □

The above lower bound is an improvement on the existing results for both the single sequence and the multisequence cases. The improvement is obtained by combining ideas from [6] and [14]. The following is an important special case of Theorem 3.1, where the period $N$ is relatively prime to $q$.

**Corollary 3.1.** Let $\gcd(N, q) = 1$ and $k$ be an integer with $1 \leq k \leq mn$. For each $i = 1, \ldots, r$, set $l_i = 0$ if

$$\sum_{\tau=0}^{k} \left( \frac{mn_i}{\tau} \right) (q - 1)^\tau < q^{md_i},$$

otherwise $l_i = 1$. Then the number $\Omega_1$ of $m$-fold $N$-periodic multisequences $\bar{S}$ over $\mathbb{F}_q$ with $L(\bar{S}) = N$ and $L_k(\bar{S}) \geq N - \sum_{i=1}^r l_i \phi(n_i)$ satisfies

$$\Omega_1 \geq \prod_{i=1}^{r} \left( q^{md_i} - \left( \sum_{\tau=0}^{k} \left( \frac{mn_i}{\tau} \right) (q - 1)^\tau \right) 1^{l_i} \frac{\phi(n_i)}{\phi(\eta_i)} \right)^{-1}.$$

**Proof.** First note that $\phi(n_i) = h_i d_i$. The result can be obtained by suitably substituting the values in Theorem 3.1 and algebraic simplifications. □

Next we define analogs of the set $E_1(N, k)$ of admissible errors for the remaining two cases of error linear complexity and present the corresponding results without proof.

Let $k$ be an integer such that $1 \leq k \leq N$. Let $E_2(N, k)$ be the set of all polynomial vectors corresponding to $m$-fold $N$-periodic nonzero multisequences over $\mathbb{F}_q$ with $k$ or fewer nonzero columns and let $E_3(N, k, f(x)^l)$ denote the set

$$\left\{ \tilde{E}^{(N)}(x) \mod f(x)^l : \tilde{E}^{(N)}(x) \in E_2(N, k) \right\}$$

for any irreducible factor $f(x)$ of $x^N - 1$ and any integer $l$ with $1 \leq l \leq p^v$.

Let $\tilde{k} = (k_1, \ldots, k_m)$ be a nonzero integer vector such that $0 \leq k_{uv} \leq N$ for $1 \leq u \leq m$. Let $E_3(N, \tilde{k})$ be the set of all polynomial vectors corresponding to $m$-fold $N$-periodic nonzero multisequences $\tilde{E}$ over $\mathbb{F}_q$ with $k_{uv}$ or fewer nonzero elements in the $u$th component sequence $E_{uv}$ and let $E_3(N, \tilde{k}, f(x)^l)$ denote the set

$$\left\{ \tilde{E}^{(N)}(x) \mod f(x)^l : \tilde{E}^{(N)}(x) \in E_3(N, \tilde{k}) \right\}$$

for any irreducible factor $f(x)$ of $x^N - 1$ and any integer $l$ with $1 \leq l \leq p^v$.

We have the following results similar to Lemma 3.1.

**Lemma 3.2.** Let $E_2(N, k)$ be as defined above. Let $f(x)$ be an irreducible factor of $x^N - 1$ of order $n_i$ and let $l$ be an integer such that $1 \leq l + 1 \leq p^v$. Let $w$ be the least integer with $p^w \geq l + 1$. Then the number of distinct residue classes in $E_2(N, k)$ modulo $f(x)^{l+1}$ satisfies

$$|E_2(N, k, f(x)^{l+1})| \leq \sum_{\tau=1}^{k} \left( \frac{p^w n_i}{\tau} \right) (q^m - 1)^\tau.$$
Lemma 3.3. Let $E_3(N, \tilde{k})$ be as defined above. Let $f(x)$ be an irreducible factor of $x^N - 1$ of order $n_i$ and let $l$ be an integer such that $1 \leq l + 1 \leq p^y$. Let $w$ be the least integer with $p^w \geq l + 1$. Then the number of distinct residue classes in $E_3(N, \tilde{k})$ modulo $f(x)^{l+1}$ satisfies

$$|E_3(N, \tilde{k}, f(x)^{l+1})| \leq -1 + \prod_{u=1}^{m} \sum_{\tau=0}^{k_u} \left( \frac{p^w n_i}{\tau} \right) (q - 1)^\tau.$$ 

The main step in the proof of Theorem 3.1 is the condition (6). Observe that the enumeration depends on the number of choices for the $f_{ij}$ where $l_i \neq p^y$, which in turn depends on the cardinality of the allowed errors modulo $f_{ij}(x)^{l_i+1}$ represented by $E_1(N, k, f_{ij}(x)^{l_i+1})$. Therefore a similar result for the cases of $k$-error $\mathbb{F}_q$-linear complexity and $\tilde{k}$-error joint linear complexity can be obtained using Lemmas 3.2 and 3.3 and with a similar argument.

Theorem 3.2. Let $k$ be an integer such that $1 \leq k \leq N$. For each $i = 1, \ldots, r$, we choose $l_i$ as follows: either we have an integer $l_i$ with $p^{w_i-1} < l_i + 1 \leq p^{w_i}$ for some integer $w_i$, $0 \leq w_i \leq v$, such that

$$M_i^2 := \sum_{\tau=1}^{k} \left( \frac{p^{w_i} n_i}{\tau} \right) (q^m - 1)^\tau < q^{md_i} (q^{md_i} - 1),$$

or otherwise we set $l_i = p^y$. Then the number $\Omega_2$ of $m$-fold $N$-periodic multisequences $\vec{S}$ over $\mathbb{F}_q$ with $L(\vec{S}) = N$ and $L_k^q(\vec{S}) \geq N - \sum_{i=1}^{r} l_i \phi(n_i)$ satisfies

$$\Omega_2 \geq \prod_{i=1}^{r} q^{m h_i d_i (p^y - l_i - 1)} (q^{md_i} (q^{md_i} - 1) - M_i^2) {h_i} \prod_{i=1}^{r} q^{m h_i d_i (p^y - 1)} (q^{md_i} - 1)^{h_i}.$$

Corollary 3.2. Let $\gcd(N, q) = 1$ and $k$ be an integer with $1 \leq k \leq N$. For each $i = 1, \ldots, r$, set $l_i = 0$ if

$$\sum_{\tau=0}^{k} \left( \frac{n_i}{\tau} \right) (q^m - 1)^\tau < q^{md_i},$$

otherwise $l_i = 1$. Then the number $\Omega_2$ of $m$-fold $N$-periodic multisequences $\vec{S}$ over $\mathbb{F}_q$ with $L(\vec{S}) = N$ and $L_k^q(\vec{S}) \geq N - \sum_{i=1}^{r} l_i \phi(n_i)$ satisfies

$$\Omega_2 \geq \prod_{i=1}^{r} \left( q^{md_i} - \left( \sum_{\tau=0}^{k} \left( \frac{n_i}{\tau} \right) (q^m - 1)^\tau \right)^{1-l_i} \frac{\phi(n_i)}{d_i} \right)^{\phi(n_i)/d_i}.$$ 

Theorem 3.3. Let $\tilde{k} = (k_1, \ldots, k_m)$ be a nonzero integer vector with $0 \leq k_u \leq N$ for $1 \leq u \leq m$. For each $i = 1, \ldots, r$, we choose $l_i$ as follows: either we have an integer $l_i$ with $p^{w_i-1} < l_i + 1 \leq p^{w_i}$ for some integer $w_i$, $0 \leq w_i \leq v$, such that

$$M_i^3 := -1 + \prod_{u=1}^{m} \sum_{\tau=0}^{k_u} \left( \frac{p^{w_i} n_i}{\tau} \right) (q - 1)^\tau < q^{md_i} (q^{md_i} - 1),$$

or otherwise we set $l_i = p^y$. Then the number $\Omega_3$ of $m$-fold $N$-periodic multisequences $\vec{S}$ over $\mathbb{F}_q$ with $L(\vec{S}) = N$ and $L_k^q(\vec{S}) \geq N - \sum_{i=1}^{r} l_i \phi(n_i)$ satisfies

$$\Omega_3 \geq \prod_{i=1}^{r} \left( q^{md_i} - \left( \sum_{\tau=0}^{k} \left( \frac{n_i}{\tau} \right) (q^m - 1)^\tau \right)^{1-l_i} \frac{\phi(n_i)}{d_i} \right)^{\phi(n_i)/d_i}.$$
\[ \Omega_3 \geq \prod_{i=1}^{r} q^{mh_d_i(p^r-l_i-1) - M_i} \prod_{i=1}^{r} q^{m_{d_i}d_i(p^r-1) - M_i} \phi(n_i). \]

In the above theorem, the \( k_u \)'s can be different for \( 1 \leq u \leq m \), whereas in [6, Theorem 3] \( k_u = k \) for all \( 1 \leq u \leq m \) and \( 1 \leq k \leq N \).

**Corollary 3.3.** Let \( \gcd(N, q) = 1 \) and \( \vec{k} = (k_1, \ldots, k_m) \) be a nonzero integer vector with \( 0 \leq k_u \leq N \) for \( 1 \leq u \leq m \). For each \( i = 1, \ldots, r \), set \( l_i = 0 \) if

\[
\prod_{u=1}^{m} \sum_{\tau=0}^{k_u} \binom{n_i}{\tau} (q - 1)^\tau < q^{md_i},
\]

otherwise \( l_i = 1 \). Then the number \( \Omega_3 \) of \( m \)-fold \( N \)-periodic multisequences \( \vec{S} \) over \( \mathbb{F}_q \) with \( L(\vec{S}) = N \) and \( L_k(\vec{S}) = N - \sum_{i=1}^{r} l_i \phi(n_i) \) satisfies

\[ \Omega_3 \geq \prod_{i=1}^{r} \left( q^{md_i} - \left( \prod_{u=1}^{m} \sum_{\tau=0}^{k_u} \binom{n_i}{\tau} (q - 1)^\tau \right) \right). \]

In the case of single sequences, i.e., if \( m = 1 \), the above Theorems 3.1, 3.2, and 3.3 reduce to the following result.

**Theorem 3.4.** Let \( k \) be an integer such that \( 1 \leq k \leq N \). For each \( i = 1, \ldots, r \), choose \( l_i \) as follows: either we have an integer \( l_i \) with \( p^{w_i} - l_i + 1 \leq p^{w_i} \) for some integer \( w_i \), \( 0 \leq w_i \leq v \), such that

\[
M_i := \sum_{\tau=1}^{k} \left( p^{w_i n_i} \right)(q - 1)^\tau < q^{d_i l_i} (q^{d_i} - 1),
\]

or otherwise we set \( l_i = p^r \). Then the number \( \Omega \) of \( N \)-periodic sequences \( S \) over \( \mathbb{F}_q \) with \( L(S) = N \) and \( L_k(S) \geq N - \sum_{i=1}^{r} l_i \phi(n_i) \) satisfies

\[ \Omega \geq \prod_{i=1}^{r} q^{h_d d_i (p^r - l_i - 1)} (q^{d_i l_i} (q^{d_i} - 1) - M_i) h_i. \]

We view the above result as the currently most general form, by which we mean that all the existing results in the single sequence case [10–12,14] are improved upon or restricted derivations of it.

**Corollary 3.4.** Let \( \gcd(N, q) = 1 \) and \( k \) be an integer with \( 1 \leq k \leq N \). For each \( i = 1, \ldots, r \), set \( l_i = 0 \) if

\[
\sum_{\tau=0}^{k} \binom{n_i}{\tau} (q - 1)^\tau < q^{d_i},
\]
otherwise $l_i = 1$. Then the number $\Omega$ of $N$-periodic sequences $S$ over $\mathbb{F}_q$ with $L(S) = N$ and $L_k(S) \geq N - \sum_{i=1}^r l_i \phi(n_i)$ satisfies

$$\Omega \geq \prod_{i=1}^r \left( q^{d_i} - \left( \sum_{\tau=0}^{k} \left(\frac{n_i}{\tau}\right)(q-1)^\tau \right)^{1-l_i} \right).$$

4. Asymptotic results

In this section we first consider the asymptotic case for prime-power period length. We present the results only for the $k$-error joint linear complexity of multisequences. Similar results can be given for the remaining two cases also. For an integer $t \geq 2$, the entropy function $H_t$ is defined by (cf. [17, p. 389])

$$H_t(\gamma) = \gamma \log_t (t-1) - \gamma \log_t t - (1-\gamma) \log_t (1-\gamma), \quad 0 < \gamma < 1,$$

where $\log_t$ denotes the logarithm to the base $t$. Note that $H_t(\gamma) \to 0$ as $\gamma \to 0^+$ and $H_t(\frac{t-1}{t}) = 1$. Furthermore, $H_t$ is an increasing function on the interval $(0, \frac{t-1}{t}]$. By [17, p. 389] we have the following result.

**Lemma 4.1.** Let $k$ and $\ell$ be positive integers such that $0 < \frac{k}{\ell} < \frac{q-1}{q}$. Then we have

$$\sum_{\tau=0}^{k} \left(\frac{\ell}{\tau}\right)(q-1)^\tau \leq q^{H_t(\frac{\ell}{t})}.$$ 

The following lemma is an immediate consequence of Lemma 4.1. We write $H_q^{-1}$ for the inverse function of the restriction of $H_q$ to $(0, \frac{q-1}{q}]$.

**Lemma 4.2.** Let $n \geq 2$ be an integer and put $\gamma = H_q^{-1}(\frac{n-1}{n})$. Then we have

$$\sum_{\tau=0}^{[\gamma^{mn^a}]} \left(\frac{mn^a}{\tau}\right)(q-1)^\tau \leq q^{mn^a(\frac{n-1}{n})} \quad \text{for } i \geq a \geq 1.$$ 

Let $n$ be an odd prime number such that $q$ is a primitive root modulo $n^2$. Then by [18, Theorem 10.6] it is true that $q$ is a primitive root modulo $n^k$ for all $\lambda \geq 1$. Thereby, using Corollary 3.1 and Lemma 4.2, we have the following result.

**Theorem 4.1.** Let $N = n^\lambda$ with $n$ an odd prime and an integer $\lambda \geq 1$. Let $q$ be a primitive root modulo $n^2$. Put $\gamma = H_q^{-1}(\frac{n-1}{n})$. Then for $1 \leq k < [\gamma^{mn^a}]$ with $1 \leq a \leq \lambda$, the number of $m$-fold $N$-periodic multisequences $\mathbf{S}$ over $\mathbb{F}_q$ such that $L(\mathbf{S}) = N$ and $L_k(\mathbf{S}) \geq N - n^{a-1}$ is at least

$$(q^n - 1) \prod_{i=1}^{a-1} \left( q^{mn^i(n-1)-1} - \sum_{\tau=0}^{k} \left(\frac{mn^i}{\tau}\right)(q-1)^\tau \right).$$

Now we consider a slightly different case where the period length $N$ is an odd prime power, but without the condition that $q$ is a primitive root modulo $n^2$. We use the following auxiliary result from [19, p. 2820].
Lemma 4.3. Suppose that $n$ is an odd prime number different from $p$ and $d$ is the multiplicative order of $q$ modulo $n$. If $q^d = 1 + cn^j$ with $\gcd(n, c) = 1$, $\rho \geq 1$, then for any $1 \leq j \leq \rho$, the multiplicative order of $q$ modulo $n^j$ is $d$, and for any $i \geq 1$, the multiplicative order of $q$ modulo $n\rho + i$ is $dn^i$.

The following lemma is another immediate consequence of Lemma 4.1.

Lemma 4.4. Suppose that $n$ is an odd prime number different from $p$ and $d$ is the multiplicative order of $q$ modulo $n$. Let $q^d = 1 + cn^\rho$ with $\gcd(n, c) = 1$, $\rho \geq 1$. Put $\gamma = \mathcal{H}_q^{-1}(d/n^\rho)$. Then for any $0 < \alpha < 1$, there exists an $m$-fold $N$-periodic multisequence $\vec{S}$ over $\mathbb{F}_q$ satisfying

$$L(\vec{S}) = N \quad \text{and} \quad L_k(\vec{S}) = N + o(N)$$

for any $1 \leq k < \lfloor \gamma mn^\rho N \alpha \rfloor$.

By Corollary 3.1, Lemmas 4.3 and 4.4, and some algebraic simplifications we obtain the following result.

Theorem 4.2. Suppose that $n$ is an odd prime number different from $p$ and $d$ is the multiplicative order of $q$ modulo $n$. Let $q^d = 1 + cn^\rho$ with $\gcd(n, c) = 1$, $\rho \geq 1$. Let $N = n^\lambda$ with an integer $\lambda > \rho$ and put $\gamma = \mathcal{H}_q^{-1}(d/n^\rho)$. Then for any $0 < \alpha < 1$, there exists an $m$-fold $N$-periodic multisequence $\vec{S}$ over $\mathbb{F}_q$ satisfying

$$L(\vec{S}) = N \quad \text{and} \quad L_k(\vec{S}) = N + o(N)$$

for any $1 \leq k < \lfloor \gamma mn^\rho N \alpha \rfloor$.

Now we consider the case of the period length $N = p^v$, where $p$ is the characteristic of $\mathbb{F}_q$. In this case we use the following consequence of Lemma 4.1.

Lemma 4.5. Let $N = p^v$ with an integer $v \geq 1$ and put $\gamma = \mathcal{H}_q^{-1}(1/p)$. Then for any $0 < \alpha < 1$, we have

$$\sum_{\tau = 0}^{\lfloor \gamma mn^w \rfloor} \binom{mn^\tau}{\tau} (q - 1)^\tau \leq q^{mn^w}$$

where $w = \lceil \alpha v \rceil$.

By Theorem 3.1, Lemma 4.5, and some algebraic simplifications we obtain the following result.

Theorem 4.3. Let $N = p^v$ with an integer $v \geq 1$ and put $\gamma = \mathcal{H}_q^{-1}(1/p)$. Then for any $0 < \alpha < 1$, there is an $m$-fold $N$-periodic multisequence $\vec{S}$ over $\mathbb{F}_q$ satisfying

$$L(\vec{S}) = N \quad \text{and} \quad L_k(\vec{S}) = N + o(N)$$

for any $1 \leq k < \lfloor \gamma mn^\alpha \rfloor$.

Now we consider a combination of the earlier two cases, i.e., the period length $N = p^v n^\lambda$ with integers $v, \lambda \geq 1$, where $p$ is the characteristic of $\mathbb{F}_q$ and $n$ is an odd prime different from $p$.

Theorem 4.4. Suppose that $n$ is an odd prime number different from $p$ and $d$ is the multiplicative order of $q$ modulo $n$. Let $q^d = 1 + cn^\rho$ with $\gcd(n, c) = 1$, $\rho \geq 1$. Let $N = p^vn^\lambda$ with integers $v, \lambda \geq 1$ and put $\gamma = \mathcal{H}_q^{-1}(d/m^\rho)$. Then for any $0 < \alpha < 1$, there exists an $m$-fold $N$-periodic multisequence $\vec{S}$ over $\mathbb{F}_q$ satisfying
for any $1 \leq k < \lfloor \gamma mn^p N^\alpha \rfloor$.

**Proof.** We have $\nu, \lambda$ are positive integers and $N = p^\nu n^\lambda$. Therefore $N \to \infty$ is possible in three ways: (i) $\nu$ is fixed and $\lambda \to \infty$; (ii) $\nu \to \infty$ and $\lambda$ is fixed; (iii) $\nu \to \infty$ and $\lambda \to \infty$. Let $w = [\alpha \nu]$ and $a = [\alpha \lambda]$.

(i) We have $\nu$ is fixed and so $w$ is fixed for any given $0 < \alpha < 1$. Let $s$ be the least positive integer such that $n^s \geq p^w$. Then we can see from Lemma 4.1 that

$$\sum_{\tau = 0}^{\lfloor \gamma mn^p N^\alpha \rfloor} \binom{mn^{l+s+\rho}}{\tau} (q - 1)^\tau \leq q^{mn^{l+s}}$$

for $i \geq a \geq 0$.

Therefore, by Theorem 3.1, for $1 \leq k < \lfloor \gamma mn^p N^\alpha \rfloor$ there exists an $m$-fold $N$-periodic multisequence $\boldsymbol{S}$ over $\mathbb{F}_q$ such that $L(\boldsymbol{S}) = N$ and

$$L_k(\boldsymbol{S}) \geq p^\nu n^\lambda - p^\nu - p^\nu \sum_{i=1}^{a+s+\rho-1} \phi(n^i)$$

$$= p^\nu (n^\lambda - n^{a+s+\rho-1}).$$

We have

$$\lim_{\lambda \to \infty} \frac{p^\nu (n^\lambda - n^{a+s+\rho-1})}{p^\nu n^\lambda} = 1,$$

and hence the result.

(ii) We have $\lambda$ is fixed and so $a$ is fixed for any given $0 < \alpha < 1$. Let $b$ be the least positive integer such that $p^b \geq n^{a+\rho}$. Then we can see from Lemma 4.1 that

$$\sum_{\tau = 0}^{\lfloor \gamma mn^p N^\alpha \rfloor} \binom{mp^{w+b} n^i}{\tau} (q - 1)^\tau \leq q^{mp^{w+b-1} n^{i-\rho}}$$

for $0 \leq i \leq \lambda$.

Therefore, by Theorem 3.1, for $1 \leq k < \lfloor \gamma mn^p N^\alpha \rfloor$ there exists an $m$-fold $N$-periodic multisequence $\boldsymbol{S}$ over $\mathbb{F}_q$ such that $L(\boldsymbol{S}) = N$ and

$$L_k(\boldsymbol{S}) \geq p^\nu n^\lambda - p^w - p^w \sum_{i=1}^{\lambda} \phi(n^i)$$

$$= (p^\nu - p^{w+b}) n^\lambda.$$

We have

$$\lim_{\nu \to \infty} \frac{(p^\nu - p^{w+b}) n^\lambda}{p^\nu n^\lambda} = 1,$$

and hence the result.
(iii) In this case, by Lemma 4.1, we have
\[ \sum_{\tau=0}^{[\gamma mn^\rho N^\alpha]} \left( \frac{mp^\omega n^{i+\rho}}{\tau} \right) (q-1)^\tau \leq q^{mdn^\rho \omega^{-1}} \quad \text{for } i \geq a \geq 0. \]

Therefore, by Theorem 3.1, for \( 1 \leq k < [\gamma mn^\rho N^\alpha] \) there exists an \( m \)-fold \( N \)-periodic multisequence \( \vec{S} \) over \( \mathbb{F}_q \) such that \( L(\vec{S}) = N \) and
\[
L_k(\vec{S}) \geq p^v n^\lambda - p^v - p^v \sum_{i=1}^{a-1} \phi(n^i) - p^w \sum_{i=0}^\lambda \phi(n^i)
= p^v n^\lambda - p^v - p^v (n^{a-1} - 1) - p^w (n^\lambda - n^{a-1})
= (p^v - p^w)(n^\lambda - n^{a-1}).
\]

We have
\[
\lim_{v \to \infty, \lambda \to \infty} \frac{(p^v - p^w)(n^\lambda - n^{a-1})}{p^v n^\lambda} = 1,
\]
and hence the result. \( \square \)

We now consider the most general case where \( N \) can be any positive integer. Let \( N = p^v n \) be a positive integer with integers \( v \geq 0 \) and \( n \geq 1 \) such that \( \gcd(n, q) = 1 \). Let \( n_1, n_2, \ldots, n_r \) be the distinct positive divisors of \( n \) and \( d_i \) be the multiplicative order of \( q \) modulo \( n_i \) for \( 1 \leq i \leq r \).

**Theorem 4.5.** Let \( k \) be an integer such that \( 1 \leq k \leq mN \). For each \( i = 1, \ldots, r \), we choose \( l_i \) as follows: either we have a positive integer \( l_i \) with \( p^{w_i-1} < l_i + 1 \leq p^{w_i} \) for some integer \( w_i \), \( 0 < w_i \leq v \), such that
\[
\frac{k}{mp^{w_i}n_i} < \frac{q-1}{q} \quad \text{and} \quad \mathcal{H}_q\left( \frac{k}{mp^{w_i}n_i} \right) < \frac{l_i d_i}{p^{w_i}n_i}
\]
or we set \( l_i = 0 \) if
\[
\frac{k}{mn_i} < \frac{q-1}{q} \quad \text{and} \quad \mathcal{H}_q\left( \frac{k}{mn_i} \right) < \frac{d_i}{n_i}
\]
or otherwise we set \( l_i = p^v \). Then there exists an \( m \)-fold \( N \)-periodic multisequence \( \vec{S} \) over \( \mathbb{F}_q \) with \( L(\vec{S}) = N \) and \( L_k(\vec{S}) \geq N - \sum_{i=1}^{r} l_i \phi(n_i) \).

The proof follows from Theorem 3.1 and Lemma 4.1. The advantage of the above theorem is that one can easily check the inequalities in Theorem 4.5 for any \( 1 \leq k \leq mN \). By the argument in the proof of Theorem 3.1, one can construct an \( m \)-fold \( N \)-periodic multisequence \( \vec{S} \) over \( \mathbb{F}_q \) satisfying \( L(\vec{S}) = N \) and \( L_k(\vec{S}) \geq N - \sum_{i=1}^{r} l_i \phi(n_i) \). Moreover, one can observe that for all large divisors \( n_i \) of \( n \), if the corresponding orders \( d_i \) of \( q \) are close to \( n_i \) (thus we can have \( l_i \) to be smaller), then there exists an \( m \)-fold \( N \)-periodic multisequence over \( \mathbb{F}_q \) with large error linear complexity.

Similar results for the \( k \)-error \( \mathbb{F}_q \)-linear complexity and the \( k \)-error joint linear complexity of multisequences can be given as well.
Acknowledgments

The authors would like to thank the anonymous reviewers for their helpful comments in improving the clarity of exposition in this paper.

References