Lower Bounds On Error Complexity Measures For Periodic LFSR and FCSR Sequences*

Ramakanth Kavuluru Andrew Klapper

Department of Computer Science, University of Kentucky
Lexington, KY 40506, USA.

Abstract

Non-trivial lower bounds on the linear complexity are derived for a sequence obtained by performing a combination of up to k substitutions, insertions, and deletions. The bounds derived are similar to those previously established for either k substitutions, k insertions or k deletions within a single period. The bounds are useful when $T/2k < \lambda < T/k$, where λ is the linear complexity of the original sequence and T is its period. It is shown that similar bounds hold for the joint linear complexity of periodic multisequences. Similar results are obtained for the N-adic complexity of periodic sequences over $\{0, \cdots, N-1\}$. New non-trivial lower bounds on the minimum number of operations needed to decrease the complexity are also given. The derivations are simpler compared to those in previous work on these problems.

1 Introduction

The linear complexity of a sequence is the length of the shortest linear feedback shift register (LFSR) that can generate the sequence. Alternatively, the linear complexity of a sequence is also the least order of a homogeneous linear recurrence relation satisfied by the sequence. The N-adic complexity of an N-ary sequence is an estimate of the size of the shortest feedback with carry shift register (FCSR) that can generate the sequence (we define this precisely later). Both are important measures of randomness of a sequence. The LFSR that generates a given sequence can be determined by using the Berlekamp-Massey algorithm using only the first 2λ elements of the sequence, where λ is the linear complexity of the sequence. Also, the FCSR that generates a given sequence can be determined by using the rational approximation algorithm by using only the first $2\lambda_N + O(\log_N(\lambda_N))$ elements of

*This paper has been accepted to appear in the journal Cryptography and Communications. A portion of this paper has appeared in the proceedings of INDOCRYPT 2007. This material is based upon work supported by the National Science Foundation under Grant No. CCF-0514660. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

the sequence, where λ_N is the N-adic complexity of the sequence. Hence for cryptographic purposes sequences with high linear and N-adic complexities are essential as an adversary would then need large initial segments of the sequences to recover, respectively, the LFSRs and the FCSRs that generate them using these attacks.

It is well known that the linear complexity and the N-adic complexity of a sequence might decrease drastically by altering a few symbols in the sequence. This instability can be measured using k-error complexity which, for a periodic sequence, is the smallest complexity value that can be obtained by changing k or fewer elements in a single period of the sequence. Counting functions and expected values for linear complexity and k-error linear complexity were extensively explored by Meidl and Niederreiter [9, 10]. Linear complexities of periodic sequences obtained by substituting, inserting, and deleting few symbols were also determined [1, 14, 15, 16]. However, similar results for the N-adic complexity do not exist in the literature. It is well accepted that a cryptographically strong sequence should have high linear complexity and N-adic complexity and that these measures should not decrease considerably with substitution, insertion and deletion of a few symbols.

For a T-periodic sequence A, by $\hat{A}$ denote any periodic sequence obtained by performing up to k modifications in one period of A and periodically repeating the modified period. Let $\lambda(A)$ denote the linear complexity of sequence A over $\mathbb{F}_q$. For an integer $N > 1$, let $\lambda_N(A)$ denote the N-adic complexity of sequence A over $\{0, \cdots, N-1\}$.

Jiang, Dai, and Imamura [6] gave a proof that $\lambda(\hat{A}) \geq T/k - \lambda(A)$ in each of the following three separate cases:

1. at most k substitutions are performed;
2. at most k insertions are performed; or
3. at most k deletions are performed.

Their analysis did not allow any combination of these operations.

Definition 1. The k-operation linear complexity of a periodic sequence A is the smallest linear complexity obtained by performing any combination of up to k substitutions, insertions, and deletions in a single period of A and then repeating the period.

The k-operation N-adic complexity is similarly defined for N-ary sequences. In this paper

1. We show Jiang, Dai, and Imamura's bound should be
$$\lambda(\hat{A}) \geq \min\left(\lambda(A), \frac{T}{k} - \lambda(A)\right).$$
2. We prove that this bound holds for *any combination* of up to k substitutions, insertions, and deletions. That is, we do not restrict all the operations to be of the same type. Thus we derive a lower bound on the k-operation linear complexity of a periodic sequence.
3. We derive similar bounds for the joint linear complexity of periodic multisequences.
4. Using a similar approach we derive a lower bound on k-operation N-adic complexity of N-ary sequences,
$$\lambda_N(\hat{A}) > \min\left(\lambda_N(A), \frac{T}{k} - \lambda_N(A) - 2 - \log_N\left(\frac{2}{N-1}\right)\right).$$

2 Linear Complexity Preliminaries

Let $\mathbb{F}_q$ denote the finite field with q elements, where $q = p^r, r \geq 1$, and p is prime. Let $A = (a_0, a_1, \cdots, a_{T-1})^\infty$ be a T-periodic sequence over $\mathbb{F}_q$ with period $(a_0, \cdots, a_{T-1})$. Let $a(x) = a_0 + a_1 x + ... + a_{T-1}x^{T-1}$ be the polynomial corresponding to sequence A. The sequence A can be represented as the power series

$$\sum_{i\geq 0} a_i x^i = \frac{a(x)}{1-x^T} = \frac{g(x)}{f(x)}, \quad \gcd(g(x), f(x)) = 1, \quad \deg(g(x)) < \deg(f(x)). \tag{1}$$

Then the linear complexity of A is

$$\lambda(A) = \deg\left(\frac{1-x^T}{gcd(a(x), 1-x^T)}\right) = \deg(f(x)). \tag{2}$$

We can see that

$$\lambda(A) \leq T.$$

In later sections we use the following lemma to derive bounds for the linear complexity after k operation modification of a single period. The proof is due to Jiang et al. [6].

Lemma 1. *Let $C(x), D(x) \in \mathbb{F}_q[x]$ with $\deg(D(x)) < \deg(C(x))$ and $C(x) \neq 0$. Define a periodic sequence $S = (s_0, s_1, \cdots)$ over $\mathbb{F}_q$ by*

$$\sum_{i\geq 0} s_i x^i = \frac{D(x)}{C(x)}.$$

Define another sequence $\tilde{S} = (\tilde{s}_0, \tilde{s}_1, \cdots)$ by

$$\sum_{i\geq 0} \tilde{s}_i x^i = \frac{[H(x)D(x)] \mod C(x)}{C(x)},$$

where $H(x) \in \mathbb{F}_q[x]$. Then

$$\lambda(\tilde{S}) \leq \lambda(S). \tag{3}$$

If $\gcd(C(x), H(x)) = 1$, then equality holds in equation (3).

Let $A_{-r} = (a_{T-r}, \cdots, a_{T-1}, a_0, \cdots, a_{T-r-1})^\infty$ denote the sequence obtained by shifting one period of A to the right cyclically by r symbols and repeating this modified period. It is straightforward to see that

$$\lambda(A) = \lambda(A_{-r}), \quad 1 \leq r \leq T-1. \tag{4}$$

3 Notation for k operation modification

In this section we describe k operation modification of a sequence and establish the notation we use to prove the main results of the paper.

Let A be the original sequence of period T and $\hat{A}$ be the sequence obtained after k operations are performed on a single period of A. Say there are k_S substitutions, k_D deletions, and k_I insertions.

We do not allow the combination when $k_D = T$, $k_I = 0$, and $k_S = 0$ as this would amount to deleting all symbols resulting in an empty sequence. Let $S, D, I \subset \{0, \cdots, T-1\}$ be sets that denote the positions of substitutions, deletions, and insertions respectively. Substitutions and deletions are performed on the elements with indices in sets S and D respectively. Insertions occur before the elements with indices in the set I. More than one element can be inserted before the elements with indices in the set I and there are $|I| = k_L$ insertion positions. Thus we have $|S| = k_S, |D| = k_D$, $|I| = k_L$,

$$k = k_S + k_D + k_I, \quad \text{and} \quad k_L \leq k_I. \tag{5}$$

If there are a deletion and a substitution at the same place we can remove the substitution and obtain the same modified sequence. Thus we can replace our list of k modifications by a list of $l \leq k$ modifications with no deletions and substitutions at the same place. Similarly we can replace an insertion and a deletion at the same position by a substitution of the element at that position with the element to be inserted. That is, we may assume that

$$D \cap S = D \cap I = \emptyset. \tag{6}$$

However, an insertion and a substitution can occur at the same position. Hence if k' is the cardinality of $S \cup D \cup I$, from equations (5) and (6) we have

$$k' = |S \cup D \cup I| \leq k_S + k_D + k_L \leq k.$$

Let $t_1, \cdots, t_{k'}$ be the list of the distinct elements of $S \cup D \cup I$ so that

$$t_1 < t_2 < \cdots < t_{k'}, \quad k' = |S \cup D \cup I|.$$

From equation (4), by replacing A by a cyclic shift A_{-r}, $0 \leq r \leq T-1$, we can make $t_1 = 0$ and

$$T - t_{k'} = \max(t_2, t_3 - t_2, \cdots, T - t_{k'}) \geq \frac{T}{k'}. \tag{7}$$

So from equation (7) we have

$$t_{k'} \leq \frac{(k'-1)T}{k'} \leq \frac{(k-1)T}{k}. \tag{8}$$

4 Error Linear Complexity Bounds

With the notation established in the previous section, we obtain a lower bound on the linear complexity of the modified sequence. We ultimately want a bound that applies when up to k modifications are made. We first prove a lower bound assuming exactly k modifications.

Theorem 1. *Let A be a sequence over $\mathbb{F}_q$ of period T. Let $\hat{A}$ be a sequence obtained after any combination of k substitutions, insertions, and deletions is performed on a single period of A and repeated periodically. Then*

1. $\lambda(\hat{A}) \geq \min(\lambda(A), T/k - \lambda(A))$ *if the number of deletions is greater than or equal to the number of insertions.*

2. $\lambda(\hat{A}) \geq \min(\lambda(A), (T+1)/k - \lambda(A))$ *if the number of deletions is less than the number of insertions.*

Proof. Let $\hat{a}(x) = \hat{a}_0 + \hat{a}_1 x + \cdots + \hat{a}_{T+k_I-k_D-1} x^{T+k_I-k_D-1}$ be the polynomial corresponding to the new sequence $\hat{A} = (\hat{a}_0, \cdots, \hat{a}_{T+k_I-k_D-1})^\infty$ as in equation (1). The generating function of the new sequence is

$$\sum_{i \geq 0} \hat{a}_i x^i = \frac{\hat{a}(x)}{1 - x^{T+k_I-k_D}}. \tag{9}$$

We consider two cases based on whether the number of insertions is greater than the number of deletions.

Case 1: $k_I \leq k_D$
Let

$$B(x) = x^{k_D-k_I}\hat{a}(x) - a(x). \tag{10}$$

Since $t_{k'}$ is the position where the last operation is made, the last $T - 1 - t_{k'}$ coefficients are the same in $x^{k_D-k_I}\hat{a}(x)$ and $a(x)$. Thus

$$\deg B(x) \leq (T-1) - (T-1-t_{k'}) = t_{k'}. \tag{11}$$

From equations (1), (9), and (10) we have

$$\begin{aligned}
\sum_{i \geq 0} \hat{a}_i x^i &= \frac{\hat{a}(x)}{1 - x^{T+k_I-k_D}} \\
&= \frac{x^{k_I-k_D}(a(x) + B(x))}{1 - x^{T+k_I-k_D}} \\
&= \frac{(g(x)(1-x^T))/f(x) + B(x)}{x^{k_D-k_I} - x^T} \\
&= \frac{g(x)(1-x^T) + f(x)B(x)}{f(x)(x^{k_D-k_I} - x^T)}.
\end{aligned}$$

Next we can apply Lemma 1 with $S = \hat{A}$ and $H(x) = f(x)$. Hence $\tilde{S}$ is the sequence represented by

$$\begin{aligned}
\sum_{i \geq 0} \tilde{s}_i x^i &= \frac{[f(x)(g(x)(1-x^T) + f(x)B(x))] \mod (f(x)(x^{k_D-k_I} - x^T))}{f(x)(x^{k_D-k_I} - x^T)} \\
&= \frac{[g(x)(1-x^{k_D-k_I}) + f(x)B(x)] \mod (x^{k_D-k_I} - x^T)}{x^{k_D-k_I} - x^T}.
\end{aligned} \tag{12}$$

Since $k_D \leq t_{k'} + 1$ and from equations (1), (2), and (11), we have

$$\deg(g(x)(1-x^{k_D-k_I}) + f(x)B(x)) \leq \lambda(A) + t_{k'}. \tag{13}$$

We have the following two subcases based on the numerator in equation (12).
Case 1a: $[g(x)(1-x^{k_D-k_I})+f(x)B(x)] \not\equiv 0 \mod (x^{k_D-k_I}-x^T)$
From Lemma 1 and equations (8), (12), and (13), we have

$$\begin{aligned}\lambda(\hat{A}) &\geq \lambda(\hat{S}) \\ &\geq T - \deg(g(x)(1-x^{k_D-k_I})+f(x)B(x)) \\ &\geq T - (\lambda(A)+t_{k'}) \\ &\geq T - \lambda(A) - \frac{(k-1)T}{k}.\end{aligned}$$

Thus we have

$$\lambda(\hat{A}) \geq \frac{T}{k} - \lambda(A). \tag{14}$$

Case 1b: $[g(x)(1-x^{k_D-k_I})+f(x)B(x)] \equiv 0 \mod (x^{k_D-k_I}-x^T)$
If $\lambda(A) \geq T/k$, then the right hand side of equation (14) is at most 0 and so the result is trivial. Hence we may assume that

$$\lambda(A) < T/k. \tag{15}$$

Let

$$g(x)(1-x^{k_D-k_I})+f(x)B(x) = l(x)(x^{k_D-k_I}-x^T) \tag{16}$$

for some $l(x) \in \mathbb{F}_q[x]$. From equations (13) and (8) we have

$$\deg(l(x)(x^{k_D-k_I}-x^T)) \leq \lambda(A) + \frac{(k-1)T}{k}.$$

So from equation (15) $\deg(l(x)) \leq \lambda(A) - T/k < 0$. From equation (16) this implies that $g(x)(1-x^{k_D-k_I})+f(x)B(x) = 0$. Hence we have

$$B(x) = \frac{g(x)(x^{k_D-k_I}-1)}{f(x)}. \tag{17}$$

From equations (1), (9), (10), and (17) we have

$$\begin{aligned}\sum_{i\geq 0} \hat{a}_i x^i &= \frac{\hat{a}(x)}{1-x^{T+k_I-k_D}} \\ &= \frac{B(x)+a(x)}{x^{k_D-k_I}-x^T} \\ &= \frac{1}{x^{k_D-k_I}-x^T}\left(\frac{g(x)(x^{k_D-k_I}-1)}{f(x)} + \frac{g(x)(1-x^T)}{f(x)}\right) \\ &= \frac{g(x)}{f(x)} \\ &= \sum_{i\geq 0} a_i x^i.\end{aligned} \tag{18}$$

From equations (14) and (18) Case 1 of the theorem is proved.

Case 2: $k_I > k_D$
We use the result of Case 1 by switching the roles of A and $\hat{A}$. Let the original sequence be $R = \hat{A}$. Then the new sequence $\hat{R} = A$ is formed by inserting $k'_I = k_D$ symbols, deleting $k'_D = k_I$, and substituting $k'_S = k_S$ symbols. So $k'_D > k'_I$. The periods of R and $\hat{R}$ are $T+k_I-k_D$ and T respectively. Because $\hat{R}$ is formed by modifying R by deleting more symbols than those inserted, from equation (14) we have $\lambda(\hat{R}) \geq \min(\lambda(R), (T+k_I-k_D)/k - \lambda(R))$.

If $\min(\lambda(R), (T+k_I-k_D)/k - \lambda(R)) = \lambda(R)$ and $\lambda(R) \neq (T+k_I-k_D)/k - \lambda(R)$ we must have been in Case 1b for R. We also have

$$\frac{T+k_I-k_D}{k} - \lambda(R) > \lambda(R) \geq 0. \tag{19}$$

From equation (19) and the hypothesis of Case 1b we have $R = \hat{R}$.

If $\min(\lambda(R), (T+k_I-k_D)/k - \lambda(R)) = (T+k_I-k_D)/k - \lambda(R)$ we have

$$\begin{aligned}\lambda(\hat{R}) &\geq \frac{T+k_I-k_D}{k} - \lambda(R) \\ &\geq \frac{T+1}{k} - \lambda(R).\end{aligned}$$

This implies $\lambda(R) \geq (T+1)/k - \lambda(\hat{R})$. That is,

$$\lambda(\hat{A}) \geq \frac{T+1}{k} - \lambda(A).$$

Thus Case 2 is proved. □

Example 1. For a simple example of Case 1b, let $T = 10$, the sequence $A = (0101010101)^\infty$ and $k = 2$. Hence $T/k - \lambda(A) = 3$ which is not a lower bound for the linear complexity of the modified sequence because we can delete any two consecutive symbols to have a sequence with linear complexity 2. Similarly we can insert two symbols and use a combination of an insertion and a deletion to obtain the same linear complexity as that of the original sequence. This shows that we must include $\lambda(A)$ in our lower bound. It is this term that was missing from Jiang et al.'s lower bound [6]. Their analysis does not consider the possibility of Case 1b and hence the missing term.

Remark 1. We note that we can shift the sequence by one position with an insertion and a deletion by deleting the last symbol and inserting it at the beginning of the period. Hence we can leave any sequence as is up to a shift using k operation modification if k is even. Even when $k \geq 3$ is odd, we can shift the sequence by $(k-3)/2$ positions using $(k-3)/2$ pairs of insertion, deletion operations. For the remaining 3 operations we look for an ab in a single period where a, $b \in \mathbb{F}_q$ such that $a \neq b$. We insert an a before a, substitute the original a by b and delete the b to leave the sequence as is up to a shift. The inclusion of $\lambda(A)$ in the bound in Theorem 1 is also needed in view of this remark.

Corollary 1. *Let A be a sequence over $\mathbb{F}_q$ of period T. Let $\hat{A}$ be a sequence obtained after any combination of up to k substitutions, insertions, and deletions is performed on a single period of A and repeated periodically. Then*

(i) $\lambda(\hat{A}) \geq \min(\lambda(A), T/k - \lambda(A))$ *if the number of deletions is greater than or equal to the number of insertions.*

(ii) $\lambda(\hat{A}) \geq \min(\lambda(A), (T+1)/k - \lambda(A))$ *if the number of deletions is less than the number of insertions.*

Proof. We note that the lower bound established in Theorem 1 is monotonically nonincreasing in k. Thus if we make $l \leq k$ modifications, the bound for exactly k modifications still applies. □

Corollary 2. *Let A be a sequence over $\mathbb{F}_q$ of period T. Suppose there is an $r \in \mathbb{F}_q$ that occurs $t > T/2$ times in a single period of A.*

(i) If $r = 0$, then $\lambda(A) \leq T/(2(T-t))$ or $\lambda(A) \geq T/(T-t)$.

(ii) If $r \neq 0$, then $\lambda(A) \leq T/(2(T-1))$ or $\lambda(A) \geq T/(T-t) - 1$.

Proof. Assume $\lambda(A) > T/(2(T-t))$. This implies that

$$\lambda(A) > \frac{T}{T-t} - \lambda(A). \tag{20}$$

Let $\hat{A}$ be a sequence obtained by performing $T-t$ operations on A and assume that the number of deletions is greater than or equal to the number of insertions. From equation (20) and Corollary 1(i) we have

$$\lambda(\hat{A}) \geq \frac{T}{T-t} - \lambda(A). \tag{21}$$

If $r = 0$, by deleting or substituting a 0 for each nonzero symbol we obtain the all 0 sequence which has linear complexity 0. So by equation (21) we have $\lambda(A) \geq T/(T-t)$. So we have $\lambda(A) \leq T/(2(T-t))$ or $\lambda(A) \geq T/(T-t)$. If $r \neq 0$, by deleting or substituting an r for each symbol that is not an r we obtain the all r sequence which has linear complexity 1. So by equation (21) we have $\lambda(A) \geq T/(T-t) - 1$. So we have $\lambda(A) \leq T/(2(T-t))$ or $\lambda(A) \geq T/(T-t) - 1$. □

Remark 2. The results of Corollary 2 hold for any $r \in \mathbb{F}_q$ and the corresponding t as defined in Corollary 2 even if $t \leq T/2$. But the results are useful only when $t > T/2$ and there can only be one element, if any, that satisfies this condition.

Kurosawa et al. [8] derived the exact formula for the minimum number of substitutions required to obtain a modified sequence with linear complexity less than the original sequence when the period is a power of the characteristic of the finite field.

Definition 2. For a periodic sequence A, define $minsub(A)$ as the minimum number of substitutions required to modify a period of A so that the modified sequence has linear complexity less than the linear complexity of A.

Let p be the characteristic of $\mathbb{F}_q$ from now on.

Definition 3. For a nonnegative integer $i = \sum_{j=0}^{d-1} i_j p^j$ with $i_j \in \{0, \cdots, p-1\}$, define

$$Prod(i) = \prod_{j=0}^{d-1} (i_j + 1).$$

Lemma 2 ([8]). *Let $T = p^n$ for some $n \in \mathbb{Z}^+$. Let t_0 denote the number of occurrences of 0 in a single period of a sequence A over $\mathbb{F}_q$. Then*

(i) $minsub(A) = Prod(T - \lambda(A))$.

(ii) $minsub(A) = T - t_0$ *if and only if the minimum linear complexity achievable by performing up to $minsub(A)$ substitutions on A is 0.*

(iii) If $q = 2$, $minsub(A) < T - minsub(A) = T - t_0$ if and only if the minimum linear complexity achievable by performing up to $minsub(A)$ substitutions on A is 1.

Here we obtain a lower bound on the minimum number of operations required to obtain a sequence with linear complexity less than the original sequence without any restrictions on the period. From here on let A and $\hat{A}$ be sequences of period T as in Corollary 1.

Definition 4. For a periodic sequence A, define $minerror(A)$ as the minimum number of operations required to modify a period of A so that the modified sequence has linear complexity less than the linear complexity of A.

We note that in Definition 4 the minimum number operations includes any combination of substitutions, insertions, and deletions. That is, we do not restrict the operations to be of the same type.

Corollary 3. *Let A be a not all zero sequence. Then,*

(i) $minerror(A) > T/(2\lambda(A))$.

(ii) If $minerror(A) = T - t_0$, where t_0 is the number of occurrences of 0 in a single period of A, then

$$minerror(A) \geq \frac{T}{\lambda(A)}.$$

(iii) If $T = p^n$ for some $n \in \mathbb{Z}^+$, then

$$\frac{T}{2\lambda(A)} < minerror(A) \leq Prod(T - \lambda(A)).$$

Proof. After performing the necessary $k = minerror(A)$ operations we have $\lambda(A) > \lambda(\hat{A})$. So from Corollary 1(i, ii) we have

$$\begin{aligned} \lambda(A) &> \lambda(\hat{A}) \\ &\geq \min(\lambda(A), T/k - \lambda(A)). \end{aligned} \tag{22}$$

From equation (22) we have $\min(\lambda(A), T/k - \lambda(A)) = T/k - \lambda(A)$. Hence we have $\lambda(A) > T/k - \lambda(A)$. That is, $\lambda(A) > T/2k$ which implies the bound in (i). Using Remark 2 and Corollary 2(i), (ii) follows from (i). Since $minerror(A) \leq minsub(A)$, (iii) follows from (i) and Lemma 2(i). □

5 Examples

In this section we discuss the tightness of the bounds established in Theorem 1. Because the derivation in Theorem 1 does not use information about the positions and relative orders of operations, it is reasonable to investigate the tightness of those bounds.

We give non-trivial examples where the lower bounds are achieved when the least period is used in calculating them. Let V_2 denote the set of odd primes v such that 2 is a primitive root modulo v^2. We need the following results due to Meidl [12] and Han et al. [4].

Lemma 3 ([12]). *Let $v \in V_2$ and λ be a nonnegative integer of the form*

$$\lambda = \epsilon + (v-1)\sum_{r\in R} v^{r-1}, \quad R \subseteq \{1, \cdots, n\}, \ \epsilon \in \{0, 1\}.$$

If $\lambda \geq (v-1)v^{n-1}$, then there exists a binary sequence with least period v^n such that the linear complexity is λ and the 1-error linear complexity is $v^n - \lambda$.

Lemma 4 ([4]). *For any $v \in V_2$ and $0 \leq k \leq T$, the linear complexity and hence the k-error linear complexity of a v^n-periodic binary sequence belongs to*

$$\{v^n - 1, v^n\} \cup \bigcup_{r=0}^{n-1} I_r,$$

where $I_r = \{l \in \mathbb{Z} : v^n - v^{r+1} \leq l \leq v^n - (v-1)v^r\}$.

We count the number of values greater than or equal to $(v-1)v^{n-1}$ that fall in the range specified in Lemma 4. From Lemma 3 this count gives the following result on the number of values of linear complexities for which the lower bound is achieved for v^n-periodic binary sequences.

Lemma 5. *For any $v \in V_2$, the number of nonnegative integers λ such that there is a binary sequence with least period v^n and linear complexity λ that achieves the lower bound in Theorem 1 for $k = 1$ is*

$$\frac{v^{n-1} - 1}{v - 1} + n + 1.$$

Next we give an infinite family of binary sequences where the lower bound is met for a single deletion and a single insertion.

Example 2. For a prime n, consider a 2^n-periodic binary sequence A with linear complexity

$$\lambda = 2 + tn, \text{ where } \frac{2^n - 2}{2n} \leq t < \frac{2^n - 2}{n}. \tag{23}$$

Also, pick A so that a period (or a shift of a period) corresponds to the polynomial $a(x) = x(1-x)^{2^n-\lambda} r_1(x) r_2(x) \cdots r_t(x)$, where $r_i(x)$, $1 \leq i \leq t$, are distinct irreducible polynomials of degree n. We note that $\lambda > 2^{n-1}$ and hence A has least period 2^n. Since $x^{2^n} - x$ is the product of all monic irreducible polynomials whose degrees divide n, the number of irreducible polynomials of prime degree n in $\mathbb{F}_2[x]$ is $(2^n - 2)/n$. Now deleting the 0 at the

beginning of each period results in $\hat{A}$ with period $2^n - 1$ corresponding to the polynomial $\hat{a}(x) = (1-x)^{2^n-\lambda} r_1(x) \cdots r_t(x)$. From equation (23) we have $\lambda < 2^n$. Hence

$$\lambda(\hat{A}) = \deg\left(\frac{1-x^{2^n-1}}{\gcd(1-x^{2^n-1}, \hat{a}(x))}\right) = 2^n - 1 - (nt+1) = 2^n - \lambda,$$

which achieves the lower bound in Theorem 1. We can also find examples for one symbol insertion by choosing $\lambda < 2^{n-1}$ in equation (23) and switching the roles of A and $\hat{A}$.

Remark 3. For a 2^n-periodic binary sequence A, $minsub(A) = 1$ if and only if $\lambda(A) = 2^n$. From Example 2 we note that there exist sequences with $minerror(A) = 1$ even when $2^{n-1} < \lambda(A) < 2^n$. Hence these sequences serve as examples where $minerror(A) < minsub(A)$ and also achieve the lower bound in Corollary 3(i).

Next we use a different approach to give examples where the least period of the sequence over $\mathbb{F}_q$ is used and where a set of k substitutions yields the lower bound. With this approach we can find examples where the lower bound is achieved for nonbinary periodic sequences where the period is not necessarily a power of the characteristic. The following result is needed for the next example. If S and R are two periodic sequences with the same period, let $d(S, R)$ denote the Hamming distance between a period of S and a period of R.

Lemma 6. *Let S be a sequence with least period T and minimal polynomial $f(x) \in \mathbb{F}_q[x]$ of degree m. Let $s(x)$ be the polynomial corresponding to a single period as in equation (1). Then the sequence S' represented by $s(x^l), l \in \mathbb{Z}^+$, has linear complexity ml and least period Tl. Also, if R is a different sequence of period T and R' is the sequence represented by $r(x^l)$, then $d(S, R) = d(S', R')$.*

Proof. Let $\gcd(1-x^T, s(x)) = g(x)$ and $s(x) = g(x)m(x)$. From equation (2), $1 - x^T = g(x)f(x)$ and $\gcd(f(x), m(x)) = 1$. So $\gcd(f(x^l), m(x^l)) = 1$ which implies that $\gcd(1 - x^{Tl}, s(x^l)) = g(x^l)$. So

$$\lambda(S') = \deg\left(\frac{1-x^{Tl}}{\gcd(1-x^{Tl}, s(x^l))}\right) = \deg\left(\frac{f(x^l).g(x^l)}{g(x^l)}\right) = ml.$$

We note that a single period of sequence S' corresponding to $s(x^l)$ can be obtained by placing $l-1$ zeroes after each element in one period of S. Hence the least period of S' is Tl if T is the least period of S. For the same reason, the single period Hamming distance $d(S, R) = d(S', R')$ where R is a sequence with period T (which may not be its least period) and R' is the sequence corresponding to $r(x^l)$. □

Example 3. Let $k = 2, q = 5$, and $T = 6$. We have $1 - x^6 = 4(4+x)(1+x)(1+x+x^2)(1+4x+x^2)$, the factorization of $1 - x^6$ into irreducible factors in $\mathbb{F}_5[x]$. Consider the sequences S and R of least periods 6 and 2 respectively, corresponding to

$$s(x) = \frac{(1-x^6)(2+x)}{1+4x+x^2} = 2 + 3x + x^2 + 3x^3 + 2x^4 + 4x^5,$$

$$r(x) = \frac{2(1-x^6)}{1+x} = 2 + 3x + 2x^2 + 3x^3 + 2x^4 + 3x^5.$$

We have $S = (231324)^\infty$ and $R = (232323)^\infty$. Here the Hamming distance of one period is $d(S, R) = 2$. It is straightforward to check that $\lambda(S) = 2$ and $\lambda(R) = 1$. From Lemma 6, considering S', R' corresponding to $s(x^l)$, $r(x^l)$, $l = 1, 2, ...$, we have $\lambda(S') = 2l$ and $\lambda(R') = l$. Also, the least period of S' is $6l$ and the single period Hamming distance is $d(S', R') = 2$. The lower bound from Theorem 1 is $(6l)/2 - \lambda(S') = 3l - 2l = l$. This can be achieved by considering R' which can be obtained by two modifications in a single period of S'. Also, note that S' achieves the lower bound in Corollary 3(i) since $T/(2\lambda(S')) = 6l/(4l) = 3/2$ and $d(S', R') = 2$.

6 Error Joint Linear Complexity Bounds

In this section we show that the bounds established in Corollary 1 also apply for periodic multisequences over $\mathbb{F}_q$. Let $\mathbf{A} = (A^1, \cdots, A^m)$ denote the periodic multisequence of period T consisting of m parallel streams of sequences $A^j = (a_0^j, \cdots, a_{T-1}^j)$, $1 \leq j \leq m$, each of period T. The joint linear complexity $\lambda(\mathbf{A})$ of a periodic multisequence $\mathbf{A}$ is defined as the length of the shortest LFSR that can generate each of the component sequences A^j, $1 \leq j \leq m$, of the multisequence possibly with different initial states. The expected value and variance of joint linear complexity of random periodic multisequences are determined in [3, 11]. The counting functions of error complexity measures for finite multisequences are studied in [13].

A given multisequence $\mathbf{A}$ consisting of m parallel streams over $\mathbb{F}_q$ can also be identified with a single sequence $\mathcal{A}$ over $\mathbb{F}_{q^m}$ (see page 84, [2]). The $\mathbb{F}_q$-linear complexity of a sequence $\mathcal{A}$ over $\mathbb{F}_{q^m}$ is defined as the length of the shortest LFSR over $\mathbb{F}_{q^m}$ with feedback coefficients in $\mathbb{F}_q$ that can generate the sequence. Hence the joint linear complexity of a multisequence over $\mathbb{F}_q$ is equal to the $\mathbb{F}_q$-linear complexity of its corresponding single sequence over $\mathbb{F}_{q^m}$. We can also see that the $\mathbb{F}_q$-linear complexity of a sequence is greater than or equal to the $\mathbb{F}_{q^m}$-linear complexity of the sequence. Hence we have

$$\lambda(\mathbf{A}) \geq \lambda(\mathcal{A}), \tag{24}$$

where $\lambda(\mathbf{A})$ is the joint linear complexity of the multisequence $\mathbf{A}$ and $\lambda(\mathcal{A})$ is the linear complexity of the corresponding single sequence $\mathcal{A}$ over $\mathbb{F}_{q^m}$.

Meidl et al. [13] introduced error complexity measures for finite and periodic multisequences. If each component sequence of $\mathbf{A}$ is arranged in a row of a matrix, each column can be identified with an element in $\mathbb{F}_{q^m}$. For any m-fold multisequence $\mathbf{A}$ over $\mathbb{F}_q$, by $\mathcal{A}$ denote the corresponding single sequence over $\mathbb{F}_{q^m}$.

Definition 5. The joint k-operation $\mathbb{F}_q$-linear complexity, $\lambda^{(q,k)}(\mathbf{A})$, of a periodic multisequence $\mathbf{A}$ is defined as the minimum value of the joint linear complexities achievable by performing at most k column-operations on the multisequence. A column-operation is a substitution, an insertion, or a deletion of an entire column and hence can affect up to m symbols in the multisequence.

Definition 6. The joint k-error linear complexity, $\lambda^{(k)}(\mathbf{A})$, of a periodic multisequence $\mathbf{A}$ is defined as the minimum value of the joint linear complexities achievable by substituting at most k symbols among all the mT elements in a single period of $\mathbf{A}$.

Since allowing insertions and deletions in each component sequence may result in component sequences of different periods we restrict the operations to substitutions in Definition 6. We can also see that $\lambda^{(k)}(\mathbf{A}) \geq \lambda^{(q,k)}(\mathbf{A})$.

Corollary 4. *Let* $\mathbf{A}$ *be an* m*-fold multisequence over* $\mathbb{F}_q$ *of period* T*. Then we have*

(i) $\lambda^{(k)}(\mathbf{A}) \geq \lambda^{(q,k)}(\mathbf{A}) \geq \min(\lambda(\mathbf{A}), T/k - \lambda(\mathbf{A}))$ *if the number of column deletions is greater than or equal to the number of column insertions.*

(ii) $\lambda^{(k)}(\mathbf{A}) \geq \lambda^{(q,k)}(\mathbf{A}) \geq \min(\lambda(\mathbf{A}), (T+1)/k - \lambda(\mathbf{A}))$ *if the number of column deletions is less than the number of column insertions.*

Proof. Let $\mathcal{A}$ be the sequence over $\mathbb{F}_{q^m}$ corresponding to the multisequence $\mathbf{A}$ over $\mathbb{F}_q$. Let $\hat{\mathcal{A}}$ be any m-fold multisequence obtained by performing any combination of up to k substitutions, insertions, and deletions in each period of $\mathcal{A}$ and repeating the modified period. From Corollary 1(i) we have

$$\lambda(\hat{\mathcal{A}}) \geq \min\left(\lambda(\mathcal{A}), \frac{T}{k} - \lambda(\mathcal{A})\right),$$

if the number of deletions is greater than or equal to the number of insertions. In case $\min(\lambda(\mathcal{A}), T/k - \lambda(\mathcal{A})) = T/k - \lambda(\mathcal{A})$, from equation (24) we have

$$\begin{aligned}\lambda^{(q,k)}(\mathbf{A}) &\geq \lambda(\hat{\mathcal{A}}) \\ &\geq \frac{T}{k} - \lambda(\mathcal{A}) \\ &\geq \frac{T}{k} - \lambda(\mathbf{A}).\end{aligned}$$

If $\min(\lambda(\mathcal{A}), T/k - \lambda(\mathcal{A})) = \lambda(\mathcal{A})$, from Case 2 of Theorem 1 we know that the modified sequence must be the same as the original sequence. Thus the first statement of this corollary is proved. The second statement follows using a similar argument as above. □

Corollary 5. *Let* $\mathbf{A}$ *be an* m*-fold multisequence over* $\mathbb{F}_q$ *of period* T *and* $\hat{\mathbf{A}}$ *be an* m*-fold multisequence obtained by performing exactly* k *substitutions among all* mT *elements in a single period of* $\mathbf{A}$*. If* l *is the number of component sequences with at least one substitution, then we have*

$$\lambda(\hat{\mathbf{A}}) \geq \min\left(\lambda(\mathbf{A}), \frac{T}{k-l+1} - \lambda(\mathbf{A})\right).$$

Proof. Consider the arrangement of $\mathbf{A}$ in a matrix of order $m \times T$, where each row is a period of a component sequence and each column can be identified with an element in $\mathbb{F}_{q^m}$. We can see that the joint linear complexity will not change if each of the component sequences is cyclically shifted. Thus each of the l component sequences can be shifted so that there is at least one column with l substitutions. As a result the single sequence $\mathcal{A}$ over $\mathbb{F}_{q^m}$ and the corresponding single sequence obtained by performing up to k substitutions in the multisequence $\mathbf{A}$ differ in at most $k - l + 1$ positions. So the result follows from Corollary 4. □

From equation (24) and Corollary 4 using a similar argument as in Corollary 2 we obtain the following result.

Corollary 6. *Let* $\mathbf{A}$ *be an* m*-fold multisequence over* $\mathbb{F}_q$ *of period* T *and let* $\mathcal{A}$ *be its corresponding single sequence over* $\mathbb{F}_{q^m}$*. Suppose there is an* $r \in \mathbb{F}_{q^m}$ *that occurs* $t > T/2$ *times in a single period of* $\mathcal{A}$*.*

(i) If $r = 0$*, then* $\lambda(\mathbf{A}) \leq T/2(T-t)$ *or* $\lambda(\mathbf{A}) \geq T/(T-t)$*.*

(ii) If $r \neq 0$*, then* $\lambda(\mathbf{A}) \leq T/2(T-t)$ *or* $\lambda(\mathbf{A}) \geq T/(T-t) - 1$*.*

Next we extend the bounds obtained for $minerror(A)$ for single sequences to multisequences. Let $minerror^{(q)}(\mathbf{A})$ denote the minimum value of k so that $\lambda^{(q,k)}(\mathbf{A}) < \lambda(\mathbf{A})$ and let $minsub(\mathbf{A})$ denote the minimum value of k so that $\lambda^{(k)}(\mathbf{A}) < \lambda(\mathbf{A})$.

Lemma 7. *Let* $\mathbf{A}$ *be an* m*-fold multisequence over* $\mathbb{F}_q$ *of period* $T = p^n$*. Set the integer* $c = \max\{\lambda(\{a_i^j\}) : 1 \leq j \leq m\}$ *and* $l = |\{j : \lambda(\{a_i^j\}) = c, 1 \leq j \leq m\}|$*. Then*

(i) $minsub(\mathbf{A}) = l \cdot Prod(T - \lambda(\mathbf{A}))$*.*

(ii) $minerror^{(q)}(\mathbf{A}) \leq l \cdot Prod(T - \lambda(\mathbf{A}))$ *with equality holding when* $l = 1$*.*

Proof. If $T = p^n$, the minimal connection polynomial of a sequence with linear complexity λ is $(1-x)^\lambda$. Since the joint minimal connection polynomial is the LCM of the minimal connection polynomials of all the component sequences, the joint linear complexity is c. If there are l sequences with linear complexity c, to lower the joint linear complexity, the linear complexity of all of the l sequences must be lowered due to the special form of connection polynomials and hence (i) follows. By shifting the l component sequences, k symbol substitutions among mT elements can be affected using $k - l + 1$ column substitutions when $\mathbf{A}$ is arranged in the form of a matrix of order $m \times T$. Using this observation and the inequality $minerror^{(q)}(\mathbf{A}) \leq minsub(\mathbf{A})$, (ii) follows from (i). □

From Corollary 4 and Lemma 7, using a similar argument as in Corollary 3 we have the following result.

Corollary 7. *Let* $\mathbf{A}$ *be an* m*-fold multisequence over* $\mathbb{F}_q$ *of period* T*. We have*

(i) $minsub(\mathbf{A}) \geq minerror^{(q)}(\mathbf{A}) > T/(2\lambda(\mathbf{A}))$*.*

(ii) If $T = p^n$ *for some* $n \in \mathbb{Z}^+$*, then*

$$\frac{T}{2\lambda(\mathbf{A})} < minerror^{(q)}(\mathbf{A}) \leq l \cdot Prod(T - \lambda(\mathbf{A})),$$

where l *is as in Lemma 7.*

7 N-adic Complexity Preliminaries

Klapper and Goresky [7] introduced FCSRs as a class of sequence generators with analogs of several properties of LFSRs. FCSRs are similar to LFSRs but with an additional memory register and generate sequences over $\{0, \cdots, N-1\}$, $N \geq 2$. An FCSR is characterized by a connection number q, $\gcd(q, N) = 1$, which determines the number of cells in the main register and the coefficients of taps on the main register for the feedback function. Any sequence generated by such an FCSR is the coefficient sequence of an N-adic integer p/q for some $p \in \mathbb{Z}^+$. The following lemma is due to Xu [17].

Lemma 8. *Let $A = (a_0, a_1, \cdots)$ be a sequence over $\{0, \cdots, N-1\}$ and let $-p/q$ be the rational representation of the N-adic integer $\sum_{i=0}^{\infty} a_i N^i$ associated with A. Then*

(i) $\gcd(N, q) = 1$.

(ii) *A is eventually periodic.*

(iii) *$p/q = 1$ if and only if $A = (N-1, N-1, \cdots)$.*

(iv) *A is strictly periodic if and only if $0 \leq p \leq q$.*

Next we define the N-adic complexity of a periodic sequence.

Definition 7. Let A be a periodic N-ary sequence, $N \geq 2$, with reduced rational representation $-p/q$. Then the N-adic complexity of A is the real number

$$\lambda_N(A) = \max(\log_N(|p|), \log_N(|q|)).$$

The N-adic complexity is not exactly the size of an FCSR because N-adic complexity does not include the size of the memory register. The N-adic span is defined as the number of N-ary cells used over an infinite execution of an FCSR. However, it has been shown that the N-adic span and N-adic complexity differ at most by $O(\log_N(\lambda_N(A)))$ (Theorem 3.4.3, [17]). Hence for practical purposes the N-adic complexity is a reasonable estimate for the size of an FCSR.

Let $A = (a_0, \cdots, a_{T-1})^{\infty}$ be a T-periodic sequence over $\{0, \cdots, N-1\}$, $N \geq 2$. Let $a(N) = a_0 + a_1 N + ... + a_{T-1} N^{T-1}$ be the integer corresponding to sequence A. Thus $a(N)$ is an ordinary integer and $a_0, \cdots, a_{T-1}$ are the coefficients in its N-ary expansion. The sequence A can be represented as the N-adic number

$$\sum_{i \geq 0} a_i N^i = -\frac{a(N)}{N^T - 1} = -\frac{p}{q}, \quad \gcd(p, q) = 1, \quad 0 \leq p \leq q. \tag{25}$$

The N-adic complexity of A is

$$\lambda_N(A) = \log_N \left(\frac{N^T - 1}{gcd(a(N), N^T - 1)} \right) = \log_N(q).$$

We have that

$$\lambda_N(A) \leq \log_N(N^T - 1).$$

We need the following lemma to derive bounds for N-adic complexity. The proof is due to Hu and Feng [5].

Lemma 9. *Let u and v be integers with $0 \le u \le v$ and $v \neq 0$. Let h be a nonzero integer and $((uh) \mod v)/v = u'/v'$ where $(uh) \mod v$ means the reduced residue of uh modulo v, and $0 \le u' \le v'$, $v' \neq 0$. Then*

$$\frac{v'}{\gcd(u', v')} \le \frac{v}{\gcd(u, v)}. \tag{26}$$

The equality in equation (26) holds if and only if

$$\gcd\left(h, v/\gcd(u, v)\right) = 1.$$

From Lemma 1 it is straightforward to show that

$$\lambda_N(A) = \lambda_N(A_{-s}), \quad 1 \le s \le T-1.$$

8 Error N-adic Complexity Bounds

We use the notation established for Theorem 1 in Section 3. We also retain the notation in Section 7.

Theorem 2. *Let A be a sequence over $\{0, \cdots, N\}$ of period T and let $\hat{A}$ be a sequence obtained after any combination of k substitutions, insertions, and deletions is performed on a single period of A and repeated periodically. Then*

(1) $\lambda_N(\hat{A}) > \min(\lambda_N(A), T/k - \lambda_N(A) - 2 - \log_N(2/(N-1)))$ if the number of deletions is greater than or equal to the number of insertions.

(2) $\lambda_N(\hat{A}) > \min(\lambda_N(A), (T+1)/k - \lambda_N(A) - 2 - \log_N(2/(N-1)))$ if the number of deletions is less than the number of insertions.

Proof. Let

$$\hat{a}(N) = \hat{a}_0 + \hat{a}_1 N + \cdots + \hat{a}_{T+k_I-k_D-1} N^{T+k_I-k_D}$$

be the integer corresponding to the new sequence as in equation (25). Now the modified sequence $\hat{A}$ corresponds to the N-adic number

$$\sum_{i \ge 0} \hat{a}_i N^i = -\frac{\hat{a}(N)}{N^{T+k_I-k_D} - 1}. \tag{27}$$

We consider two cases based on whether the number of insertions is greater than the number of deletions.

Case 1: $k_I \le k_D$
Let

$$B(N) = N^{k_D-k_I}\hat{a}(N) - a(N), \tag{28}$$

and

$$S(N) = a_{t_{k'}+1} N^{t_{k'}+1} + \cdots + a_{T-1} N^{T-1}$$

be the sum of the leading $T - t_{k'} - 1$ terms in the N-adic expansion of $a(N)$. Set

$$f(N) = N^{k_D - k_I}\hat{a}(N) - S(N)$$

and $e(N) = a(N) - S(N)$. The T coefficients in the N-ary expansion of $N^{k_D-k_I}\hat{a}(N)$ are

$$0, \cdots, 0, \hat{a}_0, \hat{a}_1, \cdots, \hat{a}_{T+k_I-k_D-1},$$

where there are $k_D - k_I$ zeroes before $\hat{a}_0$. The last $T - 1 - t_{k'}$ coefficients are unchanged from A, so equal the last $T - 1 - t_{k'}$ coefficients in the N-ary expansion of $a(N)$, so also of $S(N)$. Since these are all the coefficients of $S(N)$, we have

$$0 \le f(N) \le N^{t_{k'}+1} - N^{k_D-k_I}.$$

Also, each nonzero coefficient in the N-ary expansion of $S(N)$ is the coefficient of the same degree term of $a(N)$, so that

$$0 \le e(N) \le N^{t_{k'}+1} - 1.$$

Thus we have

$$|B(N)| = |f(N) - e(N)| \le \max(f(N), e(N)) \le N^{t_{k'}+1} - 1. \tag{29}$$

From equations (25), (27) and (28) we have

$$\begin{aligned}\sum_{i\ge 0}\hat{a}_i N^i &= -\frac{\hat{a}(N)}{N^{T+k_I-k_D}-1}\\ &= -\frac{N^{k_I-k_D}(a(N)+B(N))}{N^{T+k_I-k_D}-1}\\ &= -\frac{(p(N^T-1))/q + B(N)}{N^T - N^{k_D-k_I}}.\end{aligned}$$

Let

$$-\frac{u}{v} = -\frac{p(N^T-1)/q + B(N)}{N^T - N^{k_D-k_I}},$$

where $0 \le u \le v$, $v \ne 0$, and $\gcd(u, v) = 1$. We consider the following two cases.

Case 1a: $(p(N^{k_D-k_I} - 1) + qB(N)) \not\equiv 0 \mod (N^T - N^{k_D-k_I})$
By Lemma 9, with $h = q$ we have

$$\begin{aligned}v &\ge \frac{N^T - N^{k_D-k_I}}{\gcd(N^T - N^{k_D-k_I}, |p(N^{k_D-k_I} - 1) + qB(N)|)}\\ &\ge \frac{N^T - N^{k_D-k_I}}{|p(N^{k_D-k_I} - 1) + qB(N)|}.\end{aligned} \tag{30}$$

Since $k_D \le t_{k'} + 1$, from equation (29) we have

$$|p(N^{k_D-k_I} - 1) + qB(N)| < 2qN^{t_{k'}+1}. \tag{31}$$

From equations (8), (30), and (31) we have

$$\begin{aligned}\log_N(v) &> \log_N(N^T - N^{k_D-k_I}) - \log_N 2 - \lambda_N(A) - t_{k'} - 1 \\ &\geq \log_N(N^T - N^{T-1}) - \log_N 2 - \lambda_N(A) - \frac{(k-1)T}{k} - 1 \\ &\geq \frac{T}{k} + \log_N\left(\frac{N-1}{N}\right) - \log_N 2 - \lambda_N(A) - 1.\end{aligned} \tag{32}$$

Since $\lambda_N(\hat{A}) = \max(\log_N(|u|), \log_N(|v|))$, we have

$$\lambda_N(\hat{A}) > \frac{T}{k} - \lambda_N(A) - 2 - \log_N\left(\frac{2}{N-1}\right). \tag{33}$$

Case 1b: $(p(N^{k_D-k_I}-1) + qB(N)) \equiv 0 \mod (N^T - N^{k_D-k_I})$
If $\lambda_N(A) + 2 + \log_N(2/(N-1)) \geq T/k$, then the right hand side of equation (33) is at most 0 and so the result is trivial. Hence we may assume that

$$\lambda_N(A) + 2 + \frac{2}{N-1} < \frac{T}{k}. \tag{34}$$

We have

$$p(N^{k_D-k_I}-1) + qB(N) = l(N^T - N^{k_D-k_I}), \tag{35}$$

for some $l \in \mathbb{N}$. From equations (8), (31), (34), and (35) we have

$$\begin{aligned}\log_N l &\leq \log_N(2qN^{t_{k'}+1}) - \log_N(N^T - N^{k_D-k_I}) \\ &\leq \lambda_N(A) + \log_N(2) + \frac{(k-1)T}{k} + 1 - \log_N(N^T - N^{T-1}) \\ &= \lambda_N(A) + 2 + \log_N\left(\frac{2}{N-1}\right) - \frac{T}{k} \\ &< 0.\end{aligned}$$

Thus $l = 0$. From equation (35) this implies that

$$p(N^{k_D-k_I}-1) + qB(N) = 0. \tag{36}$$

From equation (36) using a similar derivation as in case 1b of Theorem 1 we can show that $\hat{A} = A$. Thus Case 1 of the theorem is proved.

Case 2: $k_I > k_D$
By switching the roles of $\hat{A}$ and A, using a similar derivation as in Case 2 of Theorem 1 we have

$$\lambda_N(\hat{A}) > \frac{T+1}{k} - \lambda_N(A) - 2 - \log_N\left(\frac{2}{N-1}\right).$$

□

Corollary 8. *Let A be a sequence over $\{0, \cdots, N\}$ of period T and let $\hat{A}$ be a sequence obtained after any combination of up to k substitutions, insertions, and deletions is performed on a single period of A and repeated periodically. Then*

(i) $\lambda_N(\hat{A}) > \min(\lambda_N(A), T/k - \lambda_N(A) - 2 - \log_N(2/(N-1)))$ *if the number of deletions is greater than the number of insertions.*

(ii) $\lambda_N(\hat{A}) > \min(\lambda_N(A), \log_N(N^T - 1) - (k-1)T/k - \lambda_N(A) - 1)$ *if the number of deletions is equal to the number of insertions. (With* $N = 2$*, compare with Theorem 3 in [5])*

(iii) $\lambda_N(\hat{A}) > \min(\lambda_N(A), (T+1)/k - \lambda_N(A) - 2 - \log_N(2/(N-1)))$ *if the number of deletions is less than the number of insertions.*

Proof. Parts (i) and (iii) of the corollary follow from the same observation as in Corollary 1. For part (ii), considering equation (31) with $k_D = k_I$, we have $|p(N^{k_D - k_I} - 1) + qB(N)| \leq qN^{t_{k'}+1}$. So from equation (32) with $k_D = k_I$ we have

$$\lambda_N(\hat{A}) > \min\left(\lambda_N(A), \log_N(N^T - 1) - \frac{(k-1)T}{k} - \lambda_N(A) - 1\right).$$

□

In Corollary 8 we note that for $N = 2$, the term $\log_N(2/(N-1)) = 1$ and for $N > 2$, $-1 < \log_N(2/(N-1)) \leq 0$ and can be ignored in stating the bound.

Corollary 9. *Let* A *be a sequence over* $\{0, \cdots, N-1\}$ *of period* T*. Suppose there is an* $r \in \{0, \cdots, N-1\}$ *that occurs* $t > T/2$ *times in a single period of* A*.*

(i) If $r = 0$ *or* $r = N - 1$ *then*

$$\lambda_N(A) \leq \frac{1}{2} \cdot \left(\log_N(N^T - 1) - \frac{(T-t-1)T}{T-t} - 1\right)$$

or

$$\lambda_N(A) > \left(\log_N(N^T - 1) - \frac{(T-t-1)T}{T-t} - 1\right).$$

(ii) If $r \neq 0$ *and* $r \neq N - 1$ *then*

$$\lambda_N(A) \leq \frac{1}{2} \cdot \left(\log_N(N^T - 1) - \frac{(T-t-1)T}{T-t} - 1\right)$$

or

$$\lambda_N(A) > \left(\log_N(N^T - 1) - \frac{(T-t-1)T}{T-t} - 1\right) - 1.$$

Proof. From Corollary 8(ii) using an argument similar to the one in Corollary 2 we obtain the result when $r = 0$. Unlike the linear complexity case, the bound does not change when $r = N - 1$ since the all $N - 1$ sequence has N-adic complexity 0. But when $r \notin \{0, N-1\}$ the maximum value for the N-adic complexity of an all r sequence, $r \in \{1, \cdots, N-2\}$, is $\log_N(N-1) < 1$. From this the bound follows using an argument similar to the one in Corollary 2(ii). □

Considering $\log_N(N^T - 1) - (T-t-1)T/(T-t) \approx T/(T-t)$ we note that the bounds in Corollary 9 are similar to the linear complexity bounds in Corollary 2.

Corollary 10. *By $minerror_N(A)$ denote the minimum number of operations required to decrease the N-adic complexity of A. Then,*

(i) $minerror_N(A)$ satisfies

$$minerror_N(A) > \frac{T}{2\lambda_N(A) + 3}.$$

(ii) If $minerror_N(A) = T - t_0$ or $minerror_N(A) = T - t_{N-1}$ where t_i is the number of occurrences of i in A, we have

$$minerror_N(A) > \frac{T}{\lambda_N(A) + 2}.$$

Proof. We note that for each of the three cases in Corollary 8 the second term in the minimum is greater than or equal to $T/k - \lambda_N(A) - 3$. Using this we obtain the bound in part (i) by an argument similar to the one in Corollary 3. Using part (i), Corollary 9(i) and an argument similar to the one in Corollary 3 we obtain the bound in part (ii). □

9 Conclusion

A derivation of non-trivial lower bounds for the linear complexity of a sequence over $\mathbb{F}_q$ obtained by performing k or fewer operations on a single period of a periodic sequence is presented, where an operation is a substitution, insertion or a deletion of a symbol. The bounds are useful when the linear complexity of the original sequence is less then T/k and greater than $T/2k$ where T is the period. Several infinite families where the bounds are tight are given for small k. Since the information about the positions and the corresponding values of the new elements to be inserted, deleted or substituted is not used, the bounds are not always tight. However, it is interesting to see that the bounds using any combination of the three operations are similar to those proved by Jiang et al. when only one type of operation at a time is allowed [6]. In fact the three bounds they derived for k symbol substitution, insertion and deletion are corollaries of Theorem 1 of this paper.

Non-trivial lower bounds for the N-adic complexity of sequences over $\{0, \cdots, N-1\}$ are also derived. It is interesting to note that the bounds derived in the N-adic case and the bounds derived in the linear complexity case differ by a small constant even though the derivation in the former case involves additions with carry. Finding bounds for the joint N-adic complexity is an interesting future problem.

Acknowledgements

The first author thanks Dr. James Griffioen and Dr. Kenneth Calvert for providing office space and resources while researching for this paper.

References

[1] S. Dai and K. Imamura, "Linear complexity for one-symbol substitution of a periodic sequence over GF(q)", *IEEE Trans. Inf. Theory*, vol. 44, pp. 1328-1331, May 1998.

[2] C. Ding, G. Xiao, and W. Shan, "The stability theory of stream ciphers", LNCS 561, Springer Verlag, 1991.

[3] F. Fu, H. Niederreiter, and M. Su "The expectation and variance of the joint linear complexity of random periodic multisequences", *Journal of Complexity*, vol. 21, pp. 804-822, 2005.

[4] Y. Han, J. Chung, and K. Yang, "On the k-error linear complexity of p^m-periodic binary sequences", *IEEE Trans. Inf. Theory*, vol. 53(6), pp. 2297-2304, 2007.

[5] H. Hu and D. Feng, "On the 2-adic complexity and the k-Error 2-adic complexity of periodic binary sequences", *Proc. SETA 2004*, LNCS vol. 3486, pp. 185-196, Springer Berlin, May 2005.

[6] S. Jiang, Z. Dai, and K. Imamura, "Linear complexity of a sequence obtained from a periodic sequence by either substituting, inserting or deleting k symbols within one period", *IEEE Trans. Inf. Theory*, vol. 44(3), pp. 1328-1331, May 2000.

[7] A. Klapper and M. Goresky, "Feedback shift registers, combiners with memory, and 2-adic span", *Journal of Cryptology*, vol. 10, pp. 111-147, 1997.

[8] K. Kurosawa, F. Sato, T. Sakata, and W. Kishimoto, "A relationship between linear complexity and k-error linear complexity", *IEEE Trans. Inf. Theory*, vol. 46 (2), pp. 694-698, March 2000.

[9] W. Meidl and H. Niederreiter, "Counting functions and expected values for the k-error linear complexity", *Finite Fields Appl.*, vol. 8, pp. 142-154, 2002.

[10] W. Meidl and H. Niederreiter, "On the expected value of linear complexity and the k-error linear complexity of periodic sequences", *IEEE Trans. Inf. Theory*, vol. 48(11), pp. 2817-2825, 2002.

[11] W. Meidl and H. Niederreiter, "The expected value of joint linear complexity of periodic multisequences", *Journal of Complexity*, vol. 19, pp.61-72, 2003.

[12] W. Meidl, "How many bits have to be changed to decrease the linear complexity?", *Des. Codes. Cryptography*, vol. 33, pp. 109-122, 2004.

[13] W. Meidl, H. Niederreiter, and A. Venkateswarlu "Error linear complexity measures for multisequences", *Journal of Complexity*, vol. 23, pp.169-192, 2007.

[14] S. Uehara and K. Imamura, "Linear complexity of periodic sequences obtained from $GF(q)$ sequences with period $q^n - 1$ by one-symbol insertion", *IEICE Trans. Fundamentals*, vol. E79-A, pp. 1739-1740, Oct. 1996.

[15] S. Uehara and K. Imamura, "Linear complexities of periodic sequences obtained from an m-sequence by two-symbol substitution", *Proc. 1998 Int. Symp. Inf. Theory and Its Appl.*, Mexico City, Mexico, Oct. 1998, pp. 690-692.

[16] S. Uehara and K. Imamura, "Linear complexity of periodic sequences obtained from a sequence over $GF(p)$ with period $p^n - 1$ by one-symbol deletion", *IEICE Trans. Fundamentals*, vol. E80-A, pp. 1164-1166, June 1997.

[17] J. Xu, "Stream cipher analysis based on FCSRs", PhD Dissertation, University of Kentucky, May 2000.