Periodic sequences with maximal $N$-adic complexity and large $k$-error $N$-adic complexity over $\mathbb{Z}/(N)$

Shixin Zhu\textsuperscript{a,b}, Fulin Li\textsuperscript{a,}\textsuperscript{\ast}

\textsuperscript{a} Department of Applied Mathematics, Hefei University of Technology, Hefei 230009, Anhui, PR China
\textsuperscript{b} National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, PR China

Abstract

Complexity measures for keystream sequences over $\mathbb{Z}/(N)$ play a crucial role in designing good stream cipher systems. This correspondence shows a general upper bound on $k$-error $N$-adic complexity of periodic sequences over $\mathbb{Z}/(N)$, and establishes the existence of periodic sequences over $\mathbb{Z}/(N)$ which simultaneously possess maximal $N$-adic complexity and large $k$-error $N$-adic complexity. Under some conditions the overwhelming majority of all $T$-periodic sequences over $\mathbb{Z}/(N)$ with maximal $N$-adic complexity $\log_{N}(N^T - 1)$ have a $k$-error $N$-adic complexity close to $\log_{N}(N^T - 1)$. The existence of many such sequences thwarts attacks against the keystreams by exhaustive search.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

The notion of feedback with carry shift registers (FCSRs), introduced by Klapper and Goresky [10], has received a great amount of attention in cryptography (see [11,12,3,1,2]). A lot of work has been focused on FCSRs that generate sequences over $\mathbb{Z}/(p)$, where $p$ is a prime number, especially for the case of $p = 2$. Some basic properties, such as periods, rational expressions, exponential representations, rational approximation algorithms and randomness of FCSR sequences, based on the algebraic structure of $N$-adic numbers which is much weaker than that of $p$-adic numbers in [14], have been discussed (see [13,19,7,17,9]).

It is well known that the linear complexity and the $k$-error linear complexity of LFSR sequences are important concepts for the theory of stream ciphers in cryptography [5,16,15,8]. Recently refinements...
and generalizations of the results in [8] were shown in [18]. This is also true for the FCSR sequences over $Z/(N)$. Efficient algorithms have been developed and proved for solving the register synthesis problem for $N$-FCSRs (see [13,7]). Consequently any sequence over $Z/(N)$ used as a keystream in a stream cipher must have large $N$-adic complexity. It is an interesting open problem to find efficient devices that can generate sequences with large $N$-adic complexity in [13]. But the $N$-adic complexity of FCSR sequences shows the same instability under small perturbations as the linear complexity of LFSR sequences. For example, let $S = (1, 0, ..., 0)^\infty$ or $(0, 1, ..., 1)^\infty$ with period $T$. Then the $N$-adic complexity $\lambda_N(S)$ of the sequence $S$ is $\log_N(N^T - 1)$. However, after changing one bit within every period, the $N$-adic complexity becomes 0. Hence it is interesting to study FCSR sequences which simultaneously possess a large value of the $N$-adic complexity and $k$-error $N$-adic complexity.

This work is organized as follows. In Section 2, we first recall some basic facts and previous results on FCSR sequences. In Section 3, we establish a general upper bound on $k$-error $N$-adic complexity. In Section 4, we construct some periodic FCSR sequences with maximal $N$-adic complexity and large $k$-error $N$-adic complexity; and the number of such sequences is large. In Section 5, we show conditions under which the overwhelming majority of all $T$-periodic sequences over $Z/(N)$ with maximal $N$-adic complexity $\log_N(N^T - 1)$ have a $k$-error $N$-adic complexity close to $\log_N(N^T - 1)$.

2. Preliminary

An FCSR is determined by coefficients $q_1, q_2, \ldots, q_c$, and an initial memory $m_{c-1}$, with $q_i \in \{0, 1, \ldots, N - 1\}$ for $i = 1, 2, \ldots, c$ and $m_{c-1} \in Z$, which can iteratively generate an FCSR sequence $S$ with initial state $\{s_0, s_1, \ldots, s_{c-1}\}$ in the following way, for $n = c, c+1, \ldots$ and $s_i \in \{0, 1, \ldots, N - 1\}$ for $i = 0, 1, 2, \ldots$:

- Form the integer sum $\sigma_n = \sum_{k=1}^{c} q_k s_{n-k} + m_{n-1}$.
- Shift the contents one step to the right, outputting the rightmost digit $s_{n-c}$.
- Put $s_n = \sigma_n \mod N$.
- Replace the memory integer $m_{n-1}$ with $m_n = (\sigma_n - s_n)/N = \lfloor \sigma_n/N \rfloor$.

The integer $q = q_c N^c + q_{c-1} N^{c-1} + \cdots + q_1 N - 1$ is called the connection integer of the FCSR. Feedbacks with carry shift registers are similar to LFSRs, but with the addition of an “extra memory” that retains a carry from one stage to the next. It is not immediately clear, but this is a finite state device. The first algebraic structure associated with an FCSR is the connection number $q = q_c N^c + q_{c-1} N^{c-1} + \cdots + q_1 N - 1$. This is the arithmetic analog of the connection polynomial of an LFSR. The second algebraic mechanism for analyzing FCSR sequences is the ring of $N$-adic numbers, denoted by $Z/(N)$. The ring structure on $Z/(N)$ obtained by defining addition and multiplication of $N$-adic numbers is shown in [9].

Lemma 1 ([13]). Let $S$ be an $N$-adic sequence, and let $S(N)$ denote the $N$-adic number corresponding to the $N$-adic sequence $S$. Then:

1. $S(N) = -1$ if and only if $S = (N - 1, N - 1, \ldots, N - 1)$.
2. $S(N) = -u/q$, $\gcd(u, q) = 1$ with $q > 1$ and $\gcd(q, N) = 1$ if and only if $S$ is eventually periodic.
3. $0 \leq u \leq q$ if and only if $S$ is strictly periodic.

From now on we only consider strictly periodic sequences, and we just call them periodic sequences for simplicity.

Let us write $\alpha = -u/q$ as a fraction reduced to lowest terms with $q$ minimal positive integer and $0 \leq u \leq q$. Then the period $T = \ord_q(N)$ is the minimal positive integer $t$ such that $N^t \equiv 1 \mod q$. According to [7], $q$ is the connection integer of the smallest FCSR with minimal positive number $c$ of coefficients $q_i$ which can generate the $N$-ary sequence $S$ over $Z/(N)$.

There is a useful polynomial $f(x) = \sum_{i=0}^{T-1} s_i x^i$ that associates a $T$-periodic sequence $S$ with its $N$-adic interpretation. The degree of the $N$-adic number $f(N)$ can be defined as $\deg(f(x))$, i.e., $\deg(f(N)) = \deg(f(x))$. In this case the corresponding $N$-adic number is given as

$$\alpha = f(N) N^0 + f(N) N^T + f(N) N^{2T} + \cdots = \frac{-f(N)}{N^T - 1}. $$
Remark 1. If \( S \) is the 0 sequence or the all-\( N \) − 1 sequence, then \( \lambda_N(S) = 0 \).

Definition 2 ([6]). Let \( S \) be a sequence with period \( T \); then the \( k \)-error \( N \)-adic complexity is defined as

\[
\lambda_{k,N}(S) = \min_{\text{per}(S')=T, d(S,S') \leq k} \lambda_N(S'),
\]

where the minimum is extended over all \( T \)-periodic sequences \( S' = s'_0, s'_1, \ldots, s'_{T-1} \), for which the Hamming distance, denoted as \( d(S,S') \), of the vectors \((s_0, s_1, \ldots, s_{T-1})\) and \((s'_0, s'_1, \ldots, s'_{T-1})\) is at most \( k \). In other words, \( \lambda_{k,N}(S) \) is the least \( N \)-adic complexity \( \lambda_N(S) \) among all \( T \)-periodic sequences \( S \) that are obtained by changing up to \( k \) terms among the first \( T \) bits of \( S \) and continuing these changes periodically with period \( T \).

3. A general upper bound

Let \( S = (s_0, s_1, \ldots, s_{T-1})^\infty \) be a \( T \)-periodic sequence over \( Z/(N) \) corresponding to an \( N \)-adic number \( S(N) \); then

\[
S(N) = -\frac{S^T(N)}{N^T - 1} = -\frac{S^T(N)}{\gcd(S^T(N), N^T - 1) / (N^T - 1) / \gcd(S^T(N), N^T - 1)},
\]

where \( S^T(N) = s_0 + s_1N + \cdots + s_{N-1}N^{T-1} \).

By Definition 1, the \( N \)-adic complexity of \( S \) is

\[
\lambda_N(S) = \log_N(N^T - 1) - \log_N[\gcd(S^T(N), N^T - 1)].
\]

If the canonical factorization of \( N^T - 1 \) is given by \( N^T - 1 = p_1^{e_1}p_2^{e_2} \cdots p_h^{e_h} \), then we can establish the following general upper bound on \( \lambda_{k,N}(S) \).

Theorem 1. Let \( S \) be a \( T \)-periodic sequence over \( Z/(N) \) corresponding to the \( N \)-adic number \( S(N), N \geq 2 \). Let \( m_i \) and \( k \) be integers with \( 1 \leq m_i \leq e_i \) and \( \lceil \log_N \omega \rceil + r \leq k \leq T \) for some \( i \) with \( 1 \leq i \leq h \), where \( \omega < p_i^{m_i} \), \( r \) is the least length of the bit string \((s_1^T \log_N \omega), s_2^T \log_N \omega, \ldots, s_i^T \log_N \omega, \ldots, s_T^T \log_N \omega) \), with \( 0 \leq s_i^T \log_N \omega \leq i \leq N - 1, 1 \leq i \leq r - 1, \) and \( s_i^T \log_N \omega \neq 0 \). Then

\[
\lambda_{k,N}(S) \leq \log_N(N^T - 1) - m_i \log_N p_i.
\]

Proof. Consider now an arbitrary \( T \)-periodic \( N \)-adic sequence \( S \). For some \( \omega < p_i^{m_i}, 1 \leq m_i \leq e_i \), we have

\[
S^T(N) \equiv \omega \pmod{p_i^{m_i}},
\]

where \( S^T(N) \) is the \( N \)-adic number corresponding to the first periodic term, denoted by \( S^T \), of the \( T \)-periodic sequence \( S \).

The \( N \)-adic number

\[
S^T(N) := S^T(N) - \omega
\]

is obtained from \( S^T(N) \) by changing terms, at most \( \lceil \log_N \omega \rceil + r \leq k \), where \( \omega < p_i^{m_i}, r \) is the least length of the bit string \((s_1^T \log_N \omega), s_2^T \log_N \omega, \ldots, s_i^T \log_N \omega, s_{i+1}^T \log_N \omega, \ldots, s_T^T \log_N \omega) \), with \( 0 \leq s_i^T \log_N \omega \leq i \leq N - 1, 1 \leq i \leq r - 1, \) and \( s_i^T \log_N \omega \neq 0 \). Furthermore, \( S^T(N) \) is divisible by \( p_i^{m_i} \), and so \( \log_N(\gcd(S^T(N), N^T - 1)) \geq \log_N p_i^{m_i} \). Consequently, the \( T \)-periodic \( N \)-adic sequence \( S' \) corresponding to \( S^T(N) \) satisfies \( \lambda_N(S') \leq \log_N \left[ \frac{N^T - 1}{\gcd(S^T(N), N^T - 1)} \right] \leq \log_N(N^T - 1) - m_i \log_N p_i \) in view of (1). Since \( d(S, S') \leq k \), it follows that \( \lambda_{k,N}(S) \leq \log_N(N^T - 1) - m_i \log_N p_i \). \( \square \)
Remark 2. Let \( p = \min\{p_1, p_2, \ldots, p_h\} \); then \( \lambda_{k,N}(S) \leq \log_N(N^T - 1) - \log_N p \leq \log_N(N^T - 1) - \log_N 2 \), since prime number \( p \geq 2 \).

4. Sequences with large \( k \)-error \( N \)-adic complexity

In this section, we will show some interesting results for FCSR sequences analogous to the results for LFSR sequences in [16,15,8].

We know that the largest possible value of the \( N \)-adic complexity among all \( T \)-periodic \( N \)-adic sequences is \( \log_N(N^T - 1) \) from Section 2. Let the canonical factorization of \( N^T - 1 \) be \( N^T - 1 = p_1^{e_1}p_2^{e_2} \cdots p_h^{e_h} \) with \( p_1 < p_2 < \cdots < p_h, p_i, 1 \leq i \leq h \), being the distinct prime factors. Now we show the existence of a \( T \)-periodic sequence \( S \) over \( Z/(N) \) such that \( \lambda_{N}(S) = \log_N(N^T - 1) \) and the value of \( \lambda_{k,N}(S) \) is large, and the number of such sequences is large.

**Theorem 2.** Let \( l \) and \( k \) be integers such that \( \sum_{j=0}^{k} \binom{T}{j} (N - 1)^j < l \), where \( 1 \leq l \leq p_h, 1 \leq k \leq T \). Then there exists a \( T \)-periodic sequence with \( \lambda_{k,N}(S) \geq \log_N(N^T - 1) - \log_N(\prod_{p_i < l} p_i^{\lambda_i}) \) and \( \lambda_{N}(S) = \log_N(N^T - 1) \). Further, the number of such sequences is at least \( \prod_{p_i \leq l} (p_i - \sum_{j=0}^{k} \binom{T}{j} (N - 1)^j) \prod_{p_i < l} (p_i - 1) \).

**Proof.** Let \( E \) be another \( T \)-periodic sequence corresponding to the \( N \)-adic number with \( E^T(N) = e_0 + e_1N + \cdots + e_{T-1}N^{T-1} \), and \( P(T, k) = |E^T(N) \in Z/(N) : T' \leq T, W_H(E) \leq k \) \), where \( W_H(N) \) is the number of the \( N \)-adic number \( |E(N)| = \sum_{j=0}^{k} \binom{T}{j} (N - 1)^j \). Let \( p_i \), \( 1 \leq i \leq h \), be the distinct prime factors of \( N^T - 1 \).

If \( l \leq p_i \), then the residue class ring \( Z/(p_i) \) consists of \( p_i \geq l \) residue classes modulo \( p_i \). Since \( |P(T, k)| < l \), we can choose at least \( p_i - |P(T, k)| \) residue classes \( g_i \) modulo \( p_i \) such that

\[
g_i \neq E^T(N) \pmod{p_i} \quad \text{for all } E(N) \in P(T, k) \quad (2).
\]

If \( l > p_i \), then the existence of a residue class \( g_i \) modulo \( p_i \) satisfying (2) is not guaranteed. But we have \( p_i - 1 \) possibilities for choosing a nonzero residue class modulo \( p_i \).

Therefore, by the Chinese remainder theorem, we can find an \( N \)-adic number \( S^T(N) \) with \( \deg(S^T(N)) < T \) and

\[
S^T(N) \equiv g_i \pmod{p_i} \quad \text{for all } i \text{ with } p_i \geq l,
\]

\[
S^T(N) \not\equiv 0 \pmod{p_i} \quad \text{for all } i \text{ with } p_i < l.
\]

Let \( S' \) be an arbitrary \( T \)-periodic sequence with \( d(S, S') \leq k \) and let \( S'^T(N) \) be the \( N \)-adic number corresponding to \( S' \). Suppose that for some \( j \) with \( p_j \geq l \) we have \( \gcd(S'^T(N), p_j) \neq 1 \). Then \( S'^T(N) \equiv 0 \pmod{p_j} \) since \( p_j \) is a prime. The \( N \)-adic numbers \( S^T(N) \) and \( S'^T(N) \) differ in at most \( k \) terms. Hence for some \( E(N) \in P(N, k) \) we have

\[
S^T(N) \equiv E(N) \pmod{p_j},
\]

which is a contradiction to the construction of \( S^T(N) \). Thus, we have shown that

\[
\gcd(S^T(N), p_j) = 1 \quad \text{for } p_j \geq l,
\]

and consequently

\[
\log_N(\gcd(S^T(N), N^T - 1)) \leq \log_N \left( \prod_{p_i < l} p_i^{\lambda_i} \right).
\]

Together with (1) this yields \( \lambda_{N}(S') \geq \log_N(N^T - 1) - \log_N(\prod_{p_i < l} p_i^{\lambda_i}) \), and so we obtain

\[
\lambda_{k,N}(S) \geq \log_N(N^T - 1) - \log_N \left( \prod_{p_i < l} p_i^{\lambda_i} \right).
\]
The above argument holds also for $S' = S$, and so
\[ \gcd(S^T(N), p_i) = 1, \quad \text{for } p_i \geq l. \]
By the construction of $S^T(N)$ we also have
\[ \gcd(S^T(N), p_i) = 1, \quad \text{for } p_i < l. \]
Consequently $\gcd(S^T(N), N^T - 1) = 1$, and so $\lambda_N(S) = \log_N(N^T - 1)$.

Furthermore, the number of such sequences is at least
\[ \prod_{p_i \geq 1} (p_i - \sum_{j=0}^{k} \binom{i}{j} (N - 1)^j) \prod_{p_i < 1} (p_i - 1), \]
by choosing differently for $S^T(N)$. \(\square\)

**Corollary 1.** Let $N^T - 1 = p_1p_2 \cdots p_h$ with $p_1 < p_2 < \cdots < p_h$, where $p_i$, $1 \leq i \leq h$, are distinct prime numbers. Let $l$ and $k$ be integers such that $\sum_{j=0}^{k} \binom{i}{j} (N - 1)^j < p_2$, where $1 \leq k \leq T$. Then there exists a $T$-periodic sequence with $\lambda_{k,N}(S) = \log_N(N^T - 1) - \log_N p_1$ and $\lambda_N(S) = \log_N(N^T - 1)$. Further, the number of such sequences is at least $(p_1 - 1) \prod_{j=2}^{h} (p_2 - \sum_{j=0}^{k} \binom{i}{j} (N - 1)^j)$.

**Proof.** By Theorem 2, there exists a $T$-periodic sequence with $\lambda_{k,N}(S) \geq \log_N(N^T - 1) - \log_N p_1$ and $\lambda_N(S) = \log_N(N^T - 1)$. But, on the other hand, we have $\lambda_{k,N}(S) \leq \log_N(N^T - 1) - \log_N p_1$ by Theorem 1. \(\square\)

### 5. Asymptotic results

In this section, we show conditions under which the overwhelming majority of all $T$-periodic sequences over $\mathbb{Z}/(N)$ with maximal $N$-adic complexity $\log_N(N^T - 1)$ have a $k$-error $N$-adic complexity close to $\log_N(N^T - 1)$.

First of all, we show that the number of $T$-periodic sequences over $\mathbb{Z}/(N)$ with $N$-adic complexity $\log_N(N^T - 1)$ can be easily determined.

**Proposition 1.** Let $S$ be a $T$-periodic sequence, and $S^T(N)$ be the $N$-adic number corresponding to $S$. Then the number $\mathcal{N}_T(\log_N(N^T - 1))$ of $T$-periodic sequences with $N$-adic complexity $\log_N(N^T - 1)$ is given by
\[ \mathcal{N}_T(\log_N(N^T - 1)) = (N^T - 1) \prod_{i=1}^{h} \left(1 - \frac{1}{p_i}\right). \]

**Proof.** Note that a $T$-periodic sequence $S$ satisfies $\lambda_N(S) = \log_N(N^T - 1)$ if and only if $\gcd(S^T(N), N^T - 1) = 1$. Therefore, by Lemma 1, we have
\[ \mathcal{N}_T(\log_N(N^T - 1)) = \phi(N^T - 1), \]
where $\phi(.)$ denotes the Euler function. Note the canonical factorization $N^T - 1 = p_1^{e_1}p_2^{e_2} \cdots p_h^{e_h}$, where $p_i$ are prime numbers with $p_1 < p_2 < \cdots < p_h$, $e_i \geq 1$, $i = 1, 1, \ldots, h$. Since $N \geq 2$, the general formula for $\phi(.)$ yields
\[ \mathcal{N}_T(\log_N(N^T - 1)) = (N^T - 1) \prod_{i=1}^{h} \left(1 - \frac{1}{p_i}\right). \quad \square \]

Put $0 < \gamma < 1$, and let $\alpha_T(\gamma)$ denote the proportion of the sequences that have large $\gamma N$-error $N$-adic complexity among all $T$-periodic sequences $S$ over $\mathbb{Z}/(N)$ with $\lambda(S) = \log_N(N^T - 1)$. Note that here $\gamma$ is the percentage of terms that can be changed in the period of a given $T$-periodic sequence.

The entropy function $H_N(x)$ on $[0, (N - 1)/N]$ is defined by [4, p.301] $H_N(x) = 0$, if $x = 0$;
\[ H_N(x) = x \log_N(N - 1) - x \log_N x - (1 - x) \log_N(1 - x), \quad 0 < x < (N - 1)/N. \]

Note that $H_N(x)$ increases from 0 to $(N - 1)/N$.

It is interesting to establish a counterpart of an analogous result for LFSR sequences in [15] as follows.
Theorem 3. Let $N_T - 1 = p_1 p_2 \cdots p_h$, where $p_i$, $1 \leq i \leq h$, are distinct prime numbers, and $p_1 < p_2 < \cdots < p_h$. Fix real numbers $\gamma$ and $\delta$ with $0 < \gamma < \frac{1}{2}$ and $\mathcal{H}_N(\gamma) < \delta < 1$. For some $1 \leq m \leq h < \frac{r}{p_{h-m+1}}, p_{h-m+1} \geq N^{\delta T}$. Then

$$Q_T(\gamma) > (1 - N^{-\delta - \mathcal{H}_N(\gamma) T})^{1/\delta}.$$  

In particular, if there exists an infinite set $P_{N, \delta}$ of $T$ with $N_T - 1 = p_1 p_2 \cdots p_h$ and for some $1 \leq m \leq h < \frac{r}{p_{h-m+1}}, p_{h-m+1} \geq N^{\delta T}$, then

$$\lim_{T \to \infty, T \notin P_{N, \delta}} Q_T(\gamma) = 1.$$  

Proof. Note that

$$p_{h-m+1} \geq N^{\delta T} > N^{\mathcal{H}_N(\gamma) T},$$  

and

$$1 = [\gamma + (1 - \gamma)]^T \geq \sum_{j=0}^{\lfloor \gamma T \rfloor} \binom{T}{j} \gamma^j (1 - \gamma)^{T-j} \geq \sum_{j=0}^{\lfloor \gamma T \rfloor} \binom{T}{j} (1 - \gamma)^T \left( \frac{\gamma}{1 - \gamma} \right)^{\gamma T} (N - 1)^j \gamma^j = N^{-\mathcal{H}_N(\gamma) T} \sum_{j=0}^{\lfloor \gamma T \rfloor} \binom{T}{j} (N - 1)^j,$$

and then we have

$$\sum_{j=0}^{\lfloor \gamma T \rfloor} \binom{T}{j} (N - 1)^j \leq N^{\mathcal{H}_N(\gamma) T} < p_{h-m+1}.$$  

Thus by Theorem 2 the number of $T$-periodic sequences $S$ satisfying $\lambda(S) = \log_N (N_T - 1)$ and $\lambda_{\lfloor \gamma T \rfloor, T}(S) \geq \log_N (N_T - 1) - \log_N (\prod_{i=h-m+1}^h p_i)$ is at least

$$\prod_{i=h-m+1}^h p_i - \sum_{j=0}^{\lfloor \gamma T \rfloor} \binom{T}{j} (N - 1)^j \prod_{i=1}^h (p_i - 1).$$  

Since $\mathcal{N}_T (\log_N (N_T - 1)) = \prod_{i=1}^h (p_i - 1)$ by Proposition 1, we get

$$Q_T(\gamma) \geq \prod_{i=h-m+1}^h \frac{p_i - \sum_{j=0}^{\lfloor \gamma T \rfloor} \binom{T}{j} (N - 1)^j}{p_i - 1} \geq \prod_{i=h-m+1}^h \left( 1 - \frac{\sum_{j=0}^{\lfloor \gamma T \rfloor} \binom{T}{j} (N - 1)^j}{p_i} \right) \geq \left( 1 - \frac{\sum_{j=0}^{\lfloor \gamma T \rfloor} \binom{T}{j} (N - 1)^j}{p_{h-m+1}} \right)^m \geq (1 - N^{-\mathcal{H}_N(\gamma) T - \delta T})^m.$$
Furthermore, 
\[ Q_T(\gamma) > (1 - N^{-(\delta - H_N(\gamma)T)})^{1/\delta}, \]
since \( m < T/p_{h-m+1} \leq T/N^{\delta T} < 1/\delta. \)

6. Conclusions

Cryptosystems are used to provide security in communications and data transmissions. Based on different schemes for generating sequences and different ways of representing them, there are a variety of stream cipher analyses. In order to have security, complexity measures for keystream sequences over \( Z/(N) \) will play a crucial role in designing good stream cipher systems. This paper focuses on stream cipher analysis based on feedback with carry shift registers. A general upper bound on the \( k \)-error \( N \)-adic complexity of periodic sequences over \( Z/(N) \) has been shown. We establish the existence of periodic sequences over \( Z/(N) \) which simultaneously possess maximal \( N \)-adic complexity and large \( k \)-error \( N \)-adic complexity. Under certain conditions, the overwhelming majority of all \( T \)-periodic sequences over \( Z/(N) \) with maximal \( N \)-adic complexity \( \log_N(N^T - 1) \) have a \( k \)-error \( N \)-adic complexity close to \( \log_N(N^T - 1) \). The existence of many such sequences thwarts attacks against the keystreams by exhaustive search.

Acknowledgments

The authors wish to express their deep gratitude to the anonymous reviewers for many helpful comments and suggestions.

References