2-Adic Complexity of a Sequence Obtained from a Periodic Binary Sequence by Either Inserting or Deleting k Symbols within One Period

ZHAO Lu, WEN Qiao-yan

(State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract. In this paper, we propose a method to get the lower bounds of the 2-adic complexity of a sequence obtained from a periodic sequence over $GF(2)$ by either inserting or deleting k symbols within one period. The results show the variation of the distribution of the 2-adic complexity becomes as k increases. Particularly, we discuss the lower bounds when $k=1$ respectively.

Key words: Periodic Binary Sequence; 2-Adic Complexity; *k*-symbol deletion; *k*-symbol insertion

1 Introduction

Many modern stream ciphers are designed by combining the output of several LFSRs in various nonlinear ways. Since 1955, large amount of efforts have been devoted into the study of other ("nonlinear") feedback architectures. In **[**1**],** Klapper and Goresky introduced a new feedback architecture for shift register generation of pseudorandom binary sequences called feedback with carry shift register (FCSR) and discussed some basic properties of FCSR sequences, such as the periods, the exponential representations and so on. Based on FCSR they presented the concept of the 2-adic complexity (denoted $\phi(\bullet)$) as an important index of the security of pseudorandom sequences and summarized the rational approximation algorithm. For every periodic sequence S, only knowledge of $\lceil 2\phi(s) \rceil + 2$ bits is sufficient to reproduce it using the algorithm. In another word, the higher 2-adic complexity a sequence has, the more secure it is. In recent years, more and more researchers show their interest in the 2-adic complexity of sequences. It is well known that the linear complexity of a periodic sequence is unstable under small perturbations, so k-error linear complexity is proposed to study of the stability of stream ciphers. Similar to k-error linear complexity, Honggang proposed the concept of k-error 2-adic complexity and gave the expected value and variance of a periodic binary sequence's 2-adic complexity [2]. In [3], Chen Lanfang provided an analog of the extended Games-Chan algorithm which can yield upper and lower bounds for the 2-adic complexity of periodic binary sequences with period $2^m p^n$.

Jiang Shaoquan and Dai Zongduo discussed linear complexity of a sequence by substituting, inserting or deleting k symbols in a periodic sequence [4]. Motivated by their work, we study the lower bounds of the 2-adic complexity of a sequence obtained from a periodic sequence over $GF(2)$ by either inserting or deleting k symbols within one period. The method of this paper is simple, can deal both the two different cases with the same manner and the results show the variation of the distribution of the 2-adic complexity becomes as k increases. Finally, we also give out the lower bounds when $k = 1$.

2 Definitions and Lemmas

An FCSR is determined by r coefficients $q_1, q_2, \cdots, q_r$, where $q_i \in \{0,1\}, i = 1, 2, \cdots, r$, and an initial memory m_{r-1} . The contents of the register at any given time consist of r bits, denoted $(a_{n-1}, a_{n-2}, \cdots, a_{n-r+1}, a_{n-r})$ and the memory is m_{n-1} . The operation of the shift register is defined as following:

1. Form the integer sum $\sigma_n = \sum_{k=1}^{r} q_k a_{n-k} + m_{n-1}$;
2. Shift the contents one step to the right, while outputting the rightmost bit a_{n-r} ;
3. Put $a_n \equiv \sigma_n \bmod 2$ into the leftmost cell of the shift register;
4. Replace the memory integer m_{n-1} with $m_n = (\sigma_n - a_n)/2$.

The integer $q = -1 + q_1 2 + q_2 2^2 + \cdots + q_r 2^r$ is called the connection integer of the FCSR.

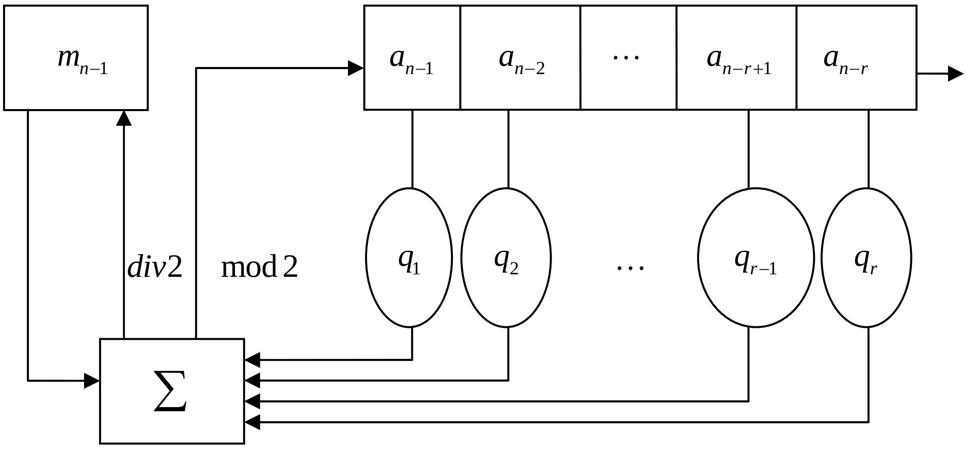

Fig 1. Feedback with carry shift register

Any infinite binary sequence $S=\{s_i\}_{i=0}^{\infty}$ can be presented by a formal power series $\alpha=\sum_{i=0}^{\infty}s_i 2^i$ called 2-adic number. Such power series forms the ring of 2-adic number, denoted Z_2. Sis eventually periodic if and only if the 2-adic number α is rational, i.e. there exist integer p,q such that $\alpha=-\frac{p}{q}\in Z_2$. If S is strictly periodic with minimal period T, then

$$\alpha=\sum_{i=0}^{\infty}s_i 2^i=-\frac{\sum_{i=0}^{T-1}s_i 2^i}{2^T-1}=-\frac{p}{q}$$

where $0\le p\le q$. $p=q$ if and only if S is the all-1 sequence. If $\gcd(p,q)=1$, $-{}^{p}\!/_{q}$ is called the reduced rational expression of S.

Definition 1. Let S be a periodic binary sequence with reduced rational expression $-{}^{p}\!/_{q}$, then the 2-adic complexity $\phi(S)$ is the real number $\log_2 q$.

Obviously, if S is the all-0 sequence or the all-1 sequence, then $\phi(S)=0$.

Lemma 1.[2] Let p,q be two positive integers, where $0<p<q$. Let h be a nonzero integer and $(ph)_{\bmod q}/q=p'/q'$, where the notation $(ph)_{\bmod q}$ means the reduced residue of ph modulo q, and $0<p'<q'$. Then

$$\frac{q'}{\gcd(p',q')}\le\frac{q}{\gcd(p,q)}$$

The equality holds if and only if

$$\gcd(h,\frac{q}{\gcd(p,q)})=1$$

Proof. Put $d=\gcd(p,q)$. Then $p=dp_1,q=dq_1$, and $\gcd(p_1,q_1)=1$. We have

$$\frac{(ph)_{\bmod q}}{q}=\frac{(dp_1h)_{\bmod(dq_1)}}{dq_1}=\frac{(p_1h)_{\bmod(q_1)}}{q_1}$$

Thus

$$\frac{q'}{\gcd(p',q')} \le q_1 = \frac{q}{\gcd(p,q)}$$

The equality holds if and only if

$$\gcd(h, \frac{q}{\gcd(p,q)}) = \gcd(h, q_1) = 1 \qquad ■$$

Definition 2. Let $S = (s_0, s_1, \cdots s_{T-1}, s_0, \cdots)$ be a periodic binary sequence, then $\tilde{S} = (\tilde{s}_0, \tilde{s}_1, \cdots, \tilde{s}_{T-1}, \tilde{s}_0,)$ is the complementary sequence of S , if $s_i + \tilde{s}_i = 1, 0 \le i < T$.

Lemma 2. Let $S = (s_0, s_1, \cdots s_{T-1}, s_0, \cdots)$ be a periodic binary sequence, 2-adic complexity of S is $\phi(S)$, if $\tilde{S}$ is the complementary sequence of S , and 2-adic complexity of $\tilde{S}$ is $\phi(\tilde{S})$, then $\phi(S) = \phi(\tilde{S})$.

Proof. Let the reduced rational expression of S and $\tilde{S}$ be $-\frac{p}{q}$ and $-\frac{\tilde{p}}{\tilde{q}}$ respectively, that is,

$$-\frac{p}{q} = -\frac{\sum_{i=0}^{T-1} s_i 2^i}{2^T - 1} \text{ and } -\frac{\tilde{p}}{\tilde{q}} = -\frac{\sum_{i=0}^{T-1} \tilde{s}_i 2^i}{2^T - 1}.$$

Thus $\phi(S) = \log_2 q$ and $\phi(\tilde{S}) = \log_2 \tilde{q}$.

Hence

$$-\frac{\tilde{p}}{\tilde{q}} = -\frac{\sum_{i=0}^{T-1} \tilde{s}_i 2^i}{2^T - 1} = -\frac{(2^T - 1) - \sum_{i=0}^{T-1} s_i 2^i}{2^T - 1}$$

$$\tilde{q} = \frac{2^T - 1}{\gcd(2^T - 1 - \sum_{i=0}^{T-1} s_i 2^T, 2^T - 1)} = \frac{2^T - 1}{\gcd(\sum_{i=0}^{T-1} s_i 2^T, 2^T - 1)} = q$$

Then we can get

$$\phi(S) = \phi(\tilde{S}) \qquad ■$$

3 k -Symbol Insertion

Theorem 1. Let $S = (s_0, s_1, \cdots, s_{T-1}, s_0, \cdots)$ be a periodic binary sequence with period T . Suppose that the rational expression of S is $\alpha = -\frac{p}{q}$, where $0 < p < q$, $\gcd(p,q) = 1$. Let $S' = (s'_0, s'_1, \cdots, s'_{T+k-1}, s'_0, \cdots)$ be a sequence obtained from S by k -symbol $a_i (i = 1, 2, \cdots, k)$

insertion within one period, where $0 \le t_1 < t_2 < \cdots < t_k < T, a_i \in \{0,1\}, i = 1, 2, \cdots, k$, then we have

$$\log_2(2^{T+k} - 1) - \phi(S) - (t_k + 1) < \phi(\tilde{S}) \le \log_2(2^{T+k} - 1)$$

Proof. Let $m = \max_{s_i = 1, 0 \le i < t_k - k} i$, $n = \max_{a_1 = 1, 1 \le i \le k} i$

Let $-\dfrac{S'^{T+k}(2)}{2^{T+k} - 1} = -\dfrac{p'}{q'}$ be the rational expression of S', where $\gcd(p', q') = 1$, $0 < p' < q'$, and

$$S'^{T+k}(2) = \sum_{i=0}^{T+k-1} s_i' 2^i$$

$$= \sum_{i=0}^{t_1 - 1} s_i 2^i + 2\sum_{i=t_1}^{t_2 - 2} s_i 2^i + \cdots + 2^{j-1} \sum_{i=t_{j-1}-j+2}^{t_j - j} s_i 2^i + \cdots + 2^{k-1} \sum_{i=t_{k-1}-k+2}^{t_k - k} s_i 2^i + 2^k \sum_{i=t_k - k+1}^{T-1} s_i 2^i + \sum_{i=1}^{k} a_i 2^{t_i}$$

If $n < m + k$, let

$$A(2) = S'^{T+k}(2) - 2^k S^T(2)$$

$$= (2^{k-1} - 2^k) \sum_{i=t_{k-1}-(k-2)}^{t_k - k} s_i 2^i + \cdots + (2^{j-1} - 2^k) \sum_{i=t_{j-1}-j+2}^{t_j - j} s_i 2^i + \cdots + (2 - 2^k)\sum_{i=t_1}^{t_2 - 2} s_i 2^i + (1 - 2^k)\sum_{i=0}^{t_1 - 1} s_i 2^i + \sum_{i=1}^{k} a_i 2^{t_i}$$

Then we have $\dfrac{p'}{q'} = \dfrac{S'^{T+k}(2)}{2^{T+k} - 1} = \dfrac{2^k S^T(2) + A(2)}{2^{T+k} - 1} = \dfrac{2^k p(2^T - 1) + qA(2)}{q(2^{T+k} - 1)}$

So

$$\frac{\{q[2^k p(2^T - 1) + qA(2)]\} \bmod [q(2^{T+k} - 1)]}{q(2^{T+k} - 1)} = \frac{q[2^k p(2^T - 1) + qA(2)] \bmod (2^{T+k} - 1)}{q(2^{T+k} - 1)}$$

$$= \frac{qA(2) + (1 - 2^k)p}{2^{T+k} - 1}$$

From lemma 1 we have: $q' \ge \dfrac{2^{T+k} - 1}{\gcd(2^{T+k} - 1, \left|qA(2) + (1 - 2^k)p\right|)} \ge \dfrac{2^{T+k} - 1}{\left|qA(2) + (1 - 2^k)p\right|}$ (1)

In the following, we discuss the value of $\left|qA(2) + (1 - 2^k)p\right|$.

For each $j = 2, \cdots, k$, we have

$$(2^{j-1} - 2^k) \sum_{i=t_{j-1}-j+2}^{t_j - j} s_i 2^i \ge (2^{j-1} - 2^k) \sum_{i=t_{j-1}-j+2}^{t_j - j} 2^i = 2^{t_j} - 2^{t_j - j + k + 1} - 2^{t_{j-1} + 1} + 2^{t_{j-1} - j + k + 2},$$

Then

$$\sum_{j=2}^{k}[(2^{j-1}-2^{k})\sum_{i=t_{j-1}-j+2}^{t_j-j} s_i 2^i] \ge \sum_{j=2}^{k}(2^{t_j}-2^{t_j-j+k+1}-2^{t_{j-1}+1}+2^{t_{j-1}-j+k+2}) = -\sum_{j=2}^{k-1}2^{t_j}-2^{t_k}-2^{t_1+1}+2^{t_1+k}$$

While $(1-2^k)\sum_{i=0}^{t_1-1}s_i 2^i \ge (1-2^k)\sum_{i=0}^{t_1-1}2^i = 2^{t_1}-2^{t_1+k}-1+2^k$

So $A(2) \ge -\sum_{j=1}^{k}2^{t_j}+(2^k-1)+\sum_{i=1}^{k}a_i 2^{t_i} \ge -\sum_{j=1}^{k}2^{t_j}+(2^k-1)$

If $n < m+k$, then $A(2) < 0$

So

$$\left|qA(2)+(1-2^k)p\right| = -qA(2)+(2^k-1)p \le q\sum_{j=1}^{k}2^{t_j}-(2^k-1)(q-p) < q\sum_{j=1}^{k}2^{t_j} < q2^{t_k+1}$$

From (1), $q' \ge \dfrac{2^{T+k}-1}{\left|qA(2)+(1-2^k)p\right|} > \dfrac{2^{T+k}-1}{q2^{t_k+1}}$

So $\phi(S') > \log_2(2^{T+k}-1)-\phi(S)-(t_k+1)$

If $n > m+k$, let S and S' be complementary sequence of $\tilde{S}$ and $\tilde{S}'$ respectively.

By lemma 2, we have $\phi(S)=\phi(\tilde{S})$ and $\phi(S')=\phi(\tilde{S}')$.

Let $-\dfrac{p}{q}$ and $-\dfrac{\tilde{p}'}{\tilde{q}}$ be the reduced rational expression of S and $\tilde{S}'$ respectively, that is,

$-\dfrac{\tilde{p}}{q} = -\dfrac{\tilde{S}^T(2)}{2^T-1}$ and $-\dfrac{\tilde{p}'}{q'} = -\dfrac{\tilde{S}'^{T+k}(2)}{2^{T+k}-1}$, where $\gcd(p',q')=1$, $0 < p' < q'$ and

$$\tilde{S}'^{T+k}(2) = \sum_{i=0}^{T+k-1}\tilde{s}'_i 2^i$$

$$= \sum_{i=0}^{t_1-1}\tilde{s}_i 2^i + 2\sum_{i=t_1}^{t_2-2}\tilde{s}_i 2^i + \cdots + 2^{j-1}\sum_{i=t_{j-1}-j+2}^{t_j-j}\tilde{s}_i 2^i + \cdots + 2^{k-1}\sum_{i=t_{k-1}-k+2}^{t_k-k}\tilde{s}_i 2^i + 2^k\sum_{i=t_k-k+1}^{T-1}\tilde{s}_i 2^i + \sum_{i=1}^{k}\tilde{a}_i 2^{t_i}$$

where $a_i + \tilde{a}_i = 1$

Let

$$\tilde{A}(2) = \tilde{S}'^{T+k}(2) - 2^k\tilde{S}^T(2)$$

$$= (2^{k-1} - 2^k) \sum_{i=t_{k-1}-(k-2)}^{t_k - k} \tilde{s}_i 2^i + \cdots + (2^{j-1} - 2^k) \sum_{i=t_{j-1}-j+2}^{t_j - j} \tilde{s}_i 2^i + \cdots + (2 - 2^k) \sum_{i=t_1}^{t_2 - 2} \tilde{s}_i 2^i + (1 - 2^k) \sum_{i=0}^{t_1 - 1} \tilde{s}_i 2^i + \sum_{i=1}^{k} \tilde{a}_i 2^{t_i}$$

Hence $\dfrac{\tilde{p}'}{q'} = \dfrac{\tilde{S}'^{T+k}(2)}{2^{T+k} - 1} = \dfrac{2^k \tilde{S}^T(2) + \tilde{A}(2)}{2^{T+k} - 1} = \dfrac{2^k \tilde{p}(2^T - 1) + q\tilde{A}(2)}{q(2^{T+k} - 1)}$

$$\frac{\{q[2^k \tilde{p}(2^T - 1) + q\tilde{A}(2)]\} \operatorname{mod}[q(2^{T+k} - 1)]}{q(2^{T+k} - 1)} = \frac{q[2^k \tilde{p}(2^T - 1) + q\tilde{A}(2)] \operatorname{mod}(2^{T+k} - 1)}{q(2^{T+k} - 1)}$$

$$= \frac{q\tilde{A}(2) + (1 - 2^k)\tilde{p}}{2^{T+k} - 1}$$

By lemma 1, we have

$$q' \geq \frac{2^{T+k} - 1}{\gcd(2^{T+k} - 1, \left| q\tilde{A}(2) + (1 - 2^k)\tilde{p} \right|)} \geq \frac{2^{T+k} - 1}{\left| q\tilde{A}(2) + (1 - 2^k)\tilde{p} \right|} \qquad (1')$$

In the following, we discuss the value of $\left| q\tilde{A}(2) + (1 - 2^k)\tilde{p} \right|$.

For each $j = 2, \cdots, k$, we have

$$(2^{j-1} - 2^k) \sum_{i=t_{j-1}-j+2}^{t_j - j} \tilde{s}_i 2^i \geq (2^{j-1} - 2^k) \sum_{i=t_{j-1}-j+2}^{t_j - j} 2^i = 2^{t_j} - 2^{t_j - j + k + 1} - 2^{t_{j-1}+1} + 2^{t_{j-1} - j + k + 2}$$

Then

$$\sum_{j=2}^{k} [(2^{j-1} - 2^k) \sum_{i=t_{j-1}-j+2}^{t_j - j} \tilde{s}_i 2^i] \geq \sum_{j=2}^{k} (2^{t_j} - 2^{t_j - j + k + 1} - 2^{t_{j-1}+1} + 2^{t_{j-1} - j + k + 2}) = -\sum_{j=2}^{k-1} 2^{t_j} - 2^{t_k} - 2^{t_1 + 1} + 2^{t_1 + k}$$

While $(1 - 2^k) \sum_{i=0}^{t_1 - 1} \tilde{s}_i 2^i \geq (1 - 2^k) \sum_{i=0}^{t_1 - 1} 2^i = 2^{t_1} - 2^{t_1 + k} - 1 + 2^k$

So $\tilde{A}(2) \geq -\sum_{j=1}^{k} 2^{t_j} + (2^k - 1) + \sum_{i=1}^{k} \tilde{a}_i 2^{t_i} \geq -\sum_{j=1}^{k} 2^{t_j} + (2^k - 1)$

If $n > m + k$, then $\tilde{A}(2) < 0$

So

$$\left| q\tilde{A}(2) + (1 - 2^k)\tilde{p} \right| = -q\tilde{A}(2) + (2^k - 1)\tilde{p} \leq q \sum_{j=1}^{k} 2^{t_j} - (2^k - 1)(q - \tilde{p}) < q \sum_{j=1}^{k} 2^{t_j} < q 2^{t_k + 1}$$

From $(1')$, $q' \geq \dfrac{2^{T+k} - 1}{\left| q\tilde{A}(2) + (1 - 2^k)\tilde{p} \right|} > \dfrac{2^{T+k} - 1}{q 2^{t_k + 1}}$

So $\phi(\tilde{S}') > \log_2(2^{T+k}-1)-\phi(\tilde{S})-(t_k+1)$, that is $\phi(S') > \log_2(2^{T+k}-1)-\phi(S)-(t_k+1)$.

If $n=m+k$, we can get the conclusion with the same method above. ■

4 k-Symbol Deletion

Theorem 2. Let $S=(s_0,s_1,\cdots,s_{T-1},s_0,\cdots)$ be a periodic binary sequence with period T. Suppose that the rational expression of S is $\alpha=-\dfrac{p}{q}$, where $0<p<q$, $\gcd(p,q)=1$. Let $S'=(s_0',s_1',\cdots,s_{T-k-1}',s_0',\cdots)$ be a sequence obtained from S by k-symbol $s_{t_i}\ (i=1,2,\cdots,k)$ deletion within one period, where $0\le t_1<t_2<\cdots<t_k<T, a_i\in\{0,1\}, i=1,2,\cdots,k$, then we have

$$\log_2(2^{T-k}-1)+k-\phi(S)-(t_k+1)<\phi(S')\le\log_2(2^{T-k}-1)$$

Proof. Let $m=\max\limits_{s_i=1,1\le i<t_k, i\ne t_j, j\in\{1,2,\cdots,k\}} i$, $n=\max\limits_{s_{t_i}=1,1\le i\le k} i$

Let $-\dfrac{S'^{T-k}(2)}{2^{T-k}-1}=-\dfrac{p'}{q'}$ be the rational expression of S', where $\gcd(p',q')=1$, $0<p'<q'$, and

$$S'^{T-k}(2)=\sum_{i=0}^{T-k-1}s_i'2^i$$

$$=\sum_{i=0}^{t_1-1}s_i2^i+2^{-1}\sum_{i=t_1+1}^{t_2-1}s_i2^i+\cdots+2^{-j}\sum_{i=t_j+1}^{t_{j+1}-1}s_i2^i+\cdots+2^{-(k-1)}\sum_{i=t_{k-1}+1}^{t_k+1}s_i2^i+2^{-k}\sum_{i=t_k+1}^{T-1}s_i2^i$$

Hence $\phi(S')=\log_2 q'\le\log_2(2^{T-k}-1)$

If $n<m+k$, let

$$S'^{T-k}(2)-2^{-k}S^T(2)=2^{-k}B(2)$$

$$=2^{-k}[(2^k-1)\sum_{i=0}^{t_1-1}s_i2^i+(2^{k-1}-1)\sum_{i=t_1+1}^{t_2-1}s_i2^i+\cdots+(2^{k-j}-1)\sum_{i=t_j+1}^{t_{j+1}-1}s_i2^i+\cdots+(2-1)\sum_{i=t_{k-1}+1}^{t_k-1}s_i2^i-\sum_{i=1}^{k}s_{t_i}2^{t_i}]$$

Then $\dfrac{p'}{q'}=\dfrac{S'^{T-k}(2)}{2^{T-k}-1}=\dfrac{2^{-k}[S^T(2)+B(2)]}{2^{T-k}-1}=\dfrac{\dfrac{p(2^T-1)}{q}+B(2)}{2^T-2^k}=\dfrac{p(2^T-1)+qB(2)}{q(2^T-2^k)}$

So

$$\frac{\{q[p(2^T-1)+qB(2)]\}\bmod[q(2^T-2^k)]}{q(2^T-2^k)}=\frac{q[p(2^T-1)+qB(2)]\bmod(2^T-2^k)}{q(2^T-2^k)}=\frac{p(2^k-1)+qB(2)}{2^T-2^k}$$

From lemma 1 we have: $q'\geq\frac{2^{T-k}-1}{\gcd(2^{T-k}-1,p(2^k-1)+qB(2))}\geq\frac{2^{T-k}-1}{p(2^k-1)+qB(2)}$ (2)

For each $j=1,\cdots,k-1$, we have

$$(2^{k-j}-1)\sum_{i=t_j+1}^{t_{j+1}-1}s_i2^i\leq(2^{k-j}-1)\sum_{i=t_j+1}^{t_{j+1}-1}2^i=2^{t_{j+1}+k-j}-2^{t_j+k-j+1}-2^{t_{j+1}}+2^{t_j+1}$$

Then

$$\sum_{j=1}^{k-1}[(2^{k-j}-1)\sum_{i=t_j+1}^{t_{j+1}-1}s_i2^i]\leq\sum_{j=1}^{k-1}(2^{t_{j+1}+k-j}-2^{t_j+k-j+1}-2^{t_{j+1}}+2^{t_j+1})=2^{t_k}-2^{t_1+k}+\sum_{j=2}^{k-1}2^{t_j}+2^{t_1+1}$$

While $(2^k-1)\sum_{i=0}^{t_1-1}s_i2^i\leq(2^k-1)\sum_{i=0}^{t_1-1}2^i=2^{t_1+k}-2^{t_1}-2^k+1$

So $B(2)\leq(1-2^k)+\sum_{j=1}^{k}(1-s_{t_j})2^{t_j}\leq(1-2^k)+\sum_{j=1}^{k}2^{t_j}$

If $n<m+k$, then $B(2)>0$

So $p(2^k-1)+qB(2)\leq q\sum_{j=1}^{k}2^{t_j}-(q-p)(2^k-1)<q\sum_{j=1}^{k}2^{t_j}<q2^{t_k+1}$

From (2) $q'\geq\frac{2^{T-k}-1}{\gcd(2^{T-k}-1,p(2^k-1)+qB(2))}\geq\frac{2^{T-k}-1}{p(2^k-1)+qB(2)}>\frac{2^{T-k}-1}{q2^{t_k+1}}$

So $\log_2(2^{T-k}-1)+k-\phi(S)-(t_k+1)<\phi(S')\leq\log_2(2^{T-k}-1)$

If $n>m+k$, let S and S' be complementary sequence of $\tilde{S}$ and $\tilde{S}'$ respectively.

By lemma 2, we have $\phi(S)=\phi(\tilde{S})$ and $\phi(S')=\phi(\tilde{S}')$.

Let $-\frac{p}{q}$ and $-\frac{\tilde{p}'}{\tilde{q}}$ be the reduced rational expression of S and $\tilde{S}'$ respectively, that is,

$-\frac{\tilde{p}}{q}=-\frac{\tilde{S}'^{T}(2)}{2^T-1}$ and $-\frac{\tilde{p}'}{q'}=-\frac{\tilde{S}'^{T-k}(2)}{2^{T-k}-1}$, where $\gcd(p',q')=1$, $0<p'<q'$ and

$$\tilde{S}'^{T-k}(2) = \sum_{i=0}^{T-k-1} \tilde{s}'_i 2^i$$

$$= \sum_{i=0}^{t_1-1} \tilde{s}_i 2^i + 2^{-1} \sum_{i=t_1+1}^{t_2-1} \tilde{s}_i 2^i + \cdots + 2^{-j} \sum_{i=t_j+1}^{t_{j+1}-1} \tilde{s}_i 2^i + \cdots + 2^{-(k-1)} \sum_{i=t_{k-1}+1}^{t_k+1} \tilde{s}_i 2^i + 2^{-k} \sum_{i=t_k+1}^{T-1} \tilde{s}_i 2^i$$

So $\phi(\tilde{S}') = \log_2 q' \le \log_2 (2^{T-k} - 1)$

Let

$$\tilde{S}'^{T-k}(2) - 2^{-k} \tilde{S}^T(2) = 2^{-k} \tilde{B}(2)$$

$$= 2^{-k}[(2^k - 1)\sum_{i=0}^{t_1-1} \tilde{s}_i 2^i + (2^{k-1} - 1) \sum_{i=t_1+1}^{t_2-1} \tilde{s}_i 2^i + \cdots + (2^{k-j} - 1) \sum_{i=t_j+1}^{t_{j+1}-1} \tilde{s}_i 2^i + \cdots + (2 - 1) \sum_{i=t_{k-1}+1}^{t_k-1} \tilde{s}_i 2^i - \sum_{i=1}^{k} \tilde{s}_{t_i} 2^{t_i}]$$

So we have $\dfrac{p'}{q'} = \dfrac{\tilde{S}'^{T-k}(2)}{2^{T-k} - 1} = \dfrac{2^{-k}[\tilde{S}^T(2) + \tilde{B}(2)]}{2^{T-k} - 1} = \dfrac{\dfrac{\tilde{p}(2^T - 1)}{q} + \tilde{B}(2)}{2^T - 2^k} = \dfrac{\tilde{p}(2^T - 1) + q\tilde{B}(2)}{q(2^T - 2^k)}$

Therefore,

$$\frac{\{q[\tilde{p}(2^T - 1) + q\tilde{B}(2)]\} \bmod [q(2^T - 2^k)]}{q(2^T - 2^k)} = \frac{q[\tilde{p}(2^T - 1) + q\tilde{B}(2)] \bmod (2^T - 2^k)}{q(2^T - 2^k)} = \frac{\tilde{p}(2^k - 1) + q\tilde{B}(2)}{2^T - 2^k}$$

By lemma 1, we have $q' \ge \dfrac{2^T - 2^k}{\gcd(2^T - 2^k, \tilde{p}(2^k - 1) + q\tilde{B}(2))} \ge \dfrac{2^T - 2^k}{\tilde{p}(2^k - 1) + q\tilde{B}(2)}$ $\qquad (2')$

For each $j = 1, \cdots, k-1$, we have

$$(2^{k-j} - 1) \sum_{i=t_j+1}^{t_{j+1}-1} \tilde{s}_i 2^i \le (2^{k-j} - 1) \sum_{i=t_j+1}^{t_{j+1}-1} 2^i = 2^{t_{j+1}+k-j} - 2^{t_j+k-j+1} - 2^{t_{j+1}} + 2^{t_j+1}$$

Then

$$\sum_{j=1}^{k-1} [(2^{k-j} - 1) \sum_{i=t_j+1}^{t_{j+1}-1} \tilde{s}_i 2^i] \le \sum_{j=1}^{k-1} (2^{t_{j+1}+k-j} - 2^{t_j+k-j+1} - 2^{t_{j+1}} + 2^{t_j+1}) = 2^{t_k} - 2^{t_1+k} + \sum_{j=2}^{k-1} 2^{t_j} + 2^{t_1+1}$$

While $(2^k - 1)\sum_{i=0}^{t_1-1} \tilde{s}_i 2^i \le (2^k - 1)\sum_{i=0}^{t_1-1} 2^i = 2^{t_1+k} - 2^{t_1} - 2^k + 1$

So $\tilde{B}(2) \le (1 - 2^k) + \sum_{j=1}^{k} (1 - \tilde{s}_{t_j}) 2^{t_j} \le (1 - 2^k) + \sum_{j=1}^{k} 2^{t_j}$

If $n > m + k$, then $\tilde{B}(2) > 0$

So $\tilde{p}(2^k-1)+q\tilde{B}(2)\le q\sum_{j=1}^{k}2^{t_j}-(q-\tilde{p})(2^k-1)<q\sum_{j=1}^{k}2^{t_j}<q2^{t_k+1}$

From (2) $q'\ge\dfrac{2^T-2^k}{\gcd(2^T-2^k,\tilde{p}(2^k-1)+q\tilde{B}(2))}\ge\dfrac{2^T-2^k}{\tilde{p}(2^k-1)+q\tilde{B}(2)}>\dfrac{2^T-2^k}{q2^{t_k+1}}$

So $\log_2(2^{T-k}-1)+k-\phi(\tilde{S})-(t_k+1)<\phi(\tilde{S}')\le\log_2(2^{T-k}-1)$

That is $\log_2(2^{T-k}-1)+k-\phi(S)-(t_k+1)<\phi(S')\le\log_2(2^{T-k}-1)$.

If $n=m+k$, we can get the conclusion with the same method above. ■

5 One Symbol Insertion or Deletion

In this section, we look into a special case. We get the lower bounds of the 2-adic complexity for a sequence obtained from a periodic binary sequence by either inserting or deleting 1 bit.

Theorem 3. Let $S=(s_0,s_1,\cdots,s_{T-1},s_0,\cdots)$ be a periodic binary sequence with period T . Suppose that the rational expression of S is $\alpha=-\dfrac{p}{q}$, where $0<p<q$, $\gcd(p,q)=1$. Let $S'=(s'_0,s'_1,\cdots,s'_T,s'_0,\cdots)$ be a sequence obtained from S by 1 symbol a insertion within one period, then we have

$$\log_2(2^{T+1}-1)-\phi(S)<\phi(S')\le\log_2(2^{T+1}-1)$$

Proof. It is well known that 2-adic complexity of a sequence obtained from a sequence by shifting is not changed, without losing generality we insert 1 symbol behind the last bit within one period.

If $a=0$, let $-\dfrac{S'^{T+1}(2)}{2^{T+1}-1}=-\dfrac{p'}{q'}$ is the rational expression of S' , where

$$S'^{T+1}(2)=s_0+s_1 2+\cdots+s_{T-1}2^{T-1}+a2^T=\sum_{i=0}^{T-1}s_i2^i+a2^T=\sum_{i=0}^{T-1}s_i2^i=S^T(2)$$

So $\dfrac{p'}{q'}=\dfrac{S^T(2)}{2^{T+1}-1}=\dfrac{p\dfrac{2^T-1}{q}}{2^{T+1}-1}$

Since $\gcd(2^T-1,2^{T+1}-1)=1$, so $q'=\dfrac{2^{T+1}-1}{\gcd(2^{T+1}-1,p)}\ge\dfrac{2^{T+1}-1}{p}>\dfrac{2^{T+1}-1}{q}$

Therefore $\phi(S') = \log_2 q' > \log_2(2^{T+1} - 1) - \phi(S)$

If $a = 1$, let S and S' be complementary sequence of $\tilde{S}$ and $\tilde{S}'$ respectively.

By lemma 2, we have $\phi(S) = \phi(\tilde{S})$ and $\phi(S') = \phi(\tilde{S}')$.

Because $\tilde{a} = 0$, we have $\phi(\tilde{S}') > \log_2(2^{T+1} - 1) - \phi(\tilde{S})$

That is $\phi(S') > \log_2(2^{T+1} - 1) - \phi(S)$ ■

Theorem 4. Let $S = (s_0, s_1, \cdots, s_{T-1}, s_0, \cdots)$ be a periodic binary sequence with period T. Suppose that the rational expression of S is $\alpha = -\frac{p}{q}$, where $0 < p < q$, $\gcd(p,q) = 1$. Let $S' = (s'_0, s'_1, \cdots, s'_{T-2}, s'_0, \cdots)$ be a sequence obtained from S by 1 symbol a deletion within one period, then we have

$$\log_2(2^{T-1} - 1) - \phi(S) < \phi(S') \le \log_2(2^{T-1} - 1)$$

Proof. The method is similar to theorem 3.

6 Conclusion

In communications, noise can easily cause modification to the original key stream, even compromise the security. In this paper, we discuss the lower bounds of the 2-adic complexity of a sequence obtained from a periodic sequence over $GF(2)$ by either inserting or deleting k symbols within one period. Interestingly, two types of changes can be treated with the same method. The results show the stability of the stream ciphers which generated by FCSR. Particularly, we give out the lower bounds of 2-adic complexity when $k = 1$ respectively.

References

1. A. klapper, M. Goresky. Feedback shift registers, 2-adic span, and combiners with memory, J. Cryptogoly, Vol.10, pp.111-147, 1997.
2. Honggang Hu, Dengguo Feng. On the 2-Adic Complexity and the *k*-Error 2-Adic Complexity of Periodic Binary Sequences. IEEE Trans. Inform. Theory, Vol.54, No.2, pp.874-883, 2008.
3. Lanfang Chen, Wenfeng Qi. 2-Adic Complexity of Binary Sequences with Period $2^m p^n$.

Journal on Communications, Vol.26, No.6, 2005.

4. Shaoquan Jiang, Zongduo Dai et al. Linear Complexity of a Sequence Obtained from a Periodic Sequence by Either Substituting, Inserting, or Deleting *k* Symbols Wihtin One Period. IEEE Trans. Inform. Theory, Vol.46, No.3, pp.1174-1177, 2000.
5. Lei Wang, Mian Cai et al. On Stability of 2-Adic Complexity of Periodic Sequence. Journal of Xidian University, Vol.27, No.3, pp.348-350, 2000.
6. Lihua Dong, Yupu Hu et al. *k*-Error 2-Adic Complexity Algorithm for the Binary Sequences with Period 2^n . Chinese Journal of Computers, Vol.29, No.9, pp.1590-1595, 2006.
7. Yaodong Zhao, Wenfeng Qi. The Linear Complexity of the Period Sequences Obtained from the Binary Sequences by One-Symbol Delete or Insert. Journal of Information Engineering University, Vol.5, No.2, pp.1-3, 2004.