On the linear complexity of feedforward clock-controlled sequence

Yangpan Zhang[1] and Maozhi Xu[1]

School of Mathematical Sciences, Peking University, Beijing 100871, China
zyp94@pku.edu.cn

Abstract. As a research field of stream ciphers, the pursuit of a balance of security and practicality is the focus. The conditions for security usually have to satisfy at least high period and high linear complexity. Because the feedforward clock-controlled structure can provide quite a high period and utility, many sequence ciphers are constructed based on this structure. However, the past study of its linear complexity only works when the controlled sequence is an m-sequence. Using the theory of matrix over the ring and block matrix in this paper, we construct a more helpful method. It can estimate the lower bound of the linear complexity of the feedforward clock-controlled sequence. Even the controlled sequence has great linear complexity.

Keywords: stream cipher · clock-controlled · linear complexity · block matrix.

1 Introduction

A clock-controlled structure is a structure that uses one sequence generator as a clock to control another sequence generator (or control itself) to generate a new sequence. The sequences generated by this structure have a large linear complexity and are widely used in stream cipher design.

The first proposal of the clock-controlled structure dates back to 1980 when Jennings[12] and Kjeldsen[14] proposed a similar structure, respectively. In 1984, T. Beth and F. C. Piper[1] first introduced the concept of "clock-controlled."

The subsequent studies[11] divided the clock-controlled structure into two categories, i.e., feedforward and feedback clock-controlled. The basic feedforward clock-controlled structure refers to using a regular sequence generator to control the clock of another sequence generator. For the feedback clock-controlled structure, it uses the output of the pseudo-random sequence generator to clock-control itself. In practice, the feedback structure makes it challenging to analyze the security from the theory, so most of the clock-controlled sequences are of feedforward structure.

The feedforward clock-controlled structure has a mathematically more apparent structure and better theoretical analysis results for its periodic and statistical properties[13]. However, the study of linear complexity is not as clear.

The upper bound on the linear complexity is nq[20], where the order n is the linear complexity of the controlled sequence, and q is the period of the control sequence. However, the conditions for the linear complexity to reach the upper bound are pretty demanding.

By analyzing irreducible polynomials over a finite field, assuming that the controlled sequence is an m-sequence, Li finds a sufficient condition for the linear complexity to reach an upper bound[20]. In contrast, Golic J.D analyzes it from a probabilistic point of view in 1988[10]. The probability of the linear complexity reaching the upper bound tends to 1 as n grows. When the controlled sequence is an m-sequence of order n, the step sum M is less than 2^n.

The above studies were published around 1990. However, in the last years of the 20th century, stream cryptanalysis tools such as linear analysis [16][5], correlation analysis [9][17], and algebraic attacks [6] were widely researched and developed. The discovery of these analysis tools has made the traditional sequence cryptosystem based on LFSR design less secure. People gradually abandoned the design approach using LFSRs as linear drivers and shifted to nonlinear design schemes. In this way, the above-mentioned linear complexity study of clock-controlled sequences based on m-sequences was rendered useless.

Furthermore, when the controlled sequence is nonlinear, its minimal polynomials are often reducible and irregular. Even the linear complexity is unknown. Therefore, in practical analysis, people tend to use less rigorous experimental analysis methods. That is, analyze the actual linear complexity in the degenerate case with shortened register. Then the nondegenerate case is reasonably guessed by the relationship between register length and linear complexity. Such as the LILI-128 algorithm [7].

In this paper, we make a new method to estimate the lower bound of linear complexity of a feedforward clock-controlled sequence. This new method can estimate better when the clock-controlled sequence is under a nonlinear driver. Unlike the current result, this paper does not analyze the polynomial reducibility. However, it estimates the lower bound of the matrix rank of the sequence-generating circulant matrix after a proper transformation. Our approach method gives a better bound on the linear complexity of the feedforward clock-controlled sequence. Unlike the current results in the papers [20][10][19], this method does not require the controlled sequence to be an m-sequence. It is, therefore, suitable for feedforward clock-controlled sequences in a general sense.

The article is structured as follows. Section 2 will give the basic concepts in the study and some mathematical tools for the study of block matrices. With the help of these tools, we give in Section 3 an estimation method for the lower bound of the linear complexity of the feedforward clock-controlled sequence. Section 4 proposes its improved algorithm LIFI-128 based on the LILI-128 algorithm and estimates its linear complexity very well. A summary of the whole paper is given in Section 5.

2 Pre-requisite knowledge

2.1 feedforward clock-controlled sequence

The paper [11] is a good review of clock-controlled shift registers, after which the definition of a basic feedforward clock-controlled sequence generator can be given as follows.

Definition 1 (Basic clock-controlled sequence generator).

Input: *a Control Sequence Generator A with period T_1; a Controlled Sequence Generator B with period T_2; a step map $f_L : output_A \to Z_{T_2}$. where $output_A$ represents the set of possible states of the output of generator A at any moment.*

Key: *the initial states of the two sequence generators A and B.*

Process: *Denote the initial state moment as $t = 0$. For $t = 1, 2, \cdots$, complete the following actions step by step.*
– 1 Run sequence generator A for one time, after which the current output state of sequence generator A is recorded as a_t, and $f_L(a_t)$ is calculated.
– 2 Run the sequence generator B for a total of $f_L(a_t)$ times, after which the state b_{σ_t} of the output of B is set to the output state $c_t = b_{\sigma_t}$ of the clock-controlled sequence generator at moment t. where b_i is the output state of generator B after continuous running i times since the initial state, $\sigma_t = \sum_{i=1}^{t} (f_L(a_i))$.

Output: *clock-controlled sequence $\{c_t\}_{t=1}^{\infty}$.*

In the above definition, we call the sequence generated by A under the action of f_L a Control Sequence and the sequence generated by B under the control of a regular clock a Controlled Sequence.

This definition can also be reduced to a binary pseudo-random sampling sequence as follows.

Definition 2 (Binary pseudo-random sampling sequence).

Input: *given a binary periodic sequence $\{b_t\} = (b_0, b_1, \cdots,)$, where $b_i \in F_2$; given a pseudo-random sampling subscript sequence $\{\sigma_t\} = (\sigma_1, \sigma_2, \cdots)$, where $\sigma_i \in N$.*

Output: *a new set of binary sequences $\{c_t\} = (b_{\sigma_1}, b_{\sigma_2}, \cdots)$. Call it a pseudo-random sampling sequence.*

For the period of the clock-controlled sequence, the following result is obtained.

Theorem 1. *[2] Denote $S = \sum_{i=1}^{T_1} (f_L(a_i))$, i.e., $S = \sigma_{T_1}$. When $gcd(S, T_2) = 1$, i.e., when the integer S is coprime with the period T_2. The minimum positive period of the clock-controlled sequence $\{c_t\}_{t=1}^{\infty}$ is $T_3 = T_1 T_2$, which reaches a maximum period.*

For clock-controlled sequence algorithms, the maximum period is always preferred in practical applications. Therefore, all the sequence models for clock control that appear below in this paper are chosen to reach the maximum period.

2.2 Linear complexity and circulant matrix

In recent years, the LFSR structure is no longer directly used to construct stream cipher regimes. However, the linear complexity also measures the resistance of a sequence to many linear-based attacks. Therefore, linear complexity is still a very important metric in measuring stream cipher security.

An equivalent definition of linear complexity is given below after the definition of circulant matrix.

Definition 3. *On a field $\mathbb{K}$, a matrix of the following shape is called a $n \times n$ r-circulant matrix. where $r \in K$.*

$$\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ ra_n & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \\ ra_{n-1} & ra_n & a_1 & \cdots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ ra_2 & ra_3 & ra_4 & \cdots & ra_n & a_1 \end{pmatrix}_{n\times n} \tag{1}$$

For convenience, it can be generally shortened to $Cir_n^r(a_1, a_2, \cdots, a_n)$. Specially, if $r = 1$, we call it circulant matrix.

For a purely periodic sequence $A = (a_1, a_2, \cdots)$ of period n over a field $\mathbb{K}$. Denote $Cir_n^1(a_1, a_2, \cdots, a_n)$ by $M_{cir}(A)$.

Theorem 2. *[18] A is a purely periodic sequence on a field $\mathbb{K}$ with period n. Then, for $M_{cir}(A)$, there is such a property. That is, the rank of $M_{cir}(A)$ is equal to the linear complexity $L(A)$ of the sequence A over the field $\mathbb{K}$.*

When the sequence $B = (b_1, b_2, \cdots)$, is regular sampled from the sequence $A = (a_1, a_2, \cdots)$, with a period of l. That is, for any $i \geq 1$, we have $b_i = a_{s+l\cdot(i-1)}$, where $b_1 = a_s$ is called the starting sampling point. It can be denoted briefly as $B = A(s, l)$. If A is a sequence of period n and satisfies $gcd(l, n) = 1$, then the following corollary can be obtained using Theorem 2.

Corollary 1. *Assume A is a purely periodic sequence over a field $\mathbb{K}$ with period n. And the sequence $B = A(s, l)$ is a sequence of regular samples of the sequence A. If $gcd(l, n) = 1$, then: (1) the period of sequence B is n; (2) $L(A) = L(B)$.*

The proof of the corollary is simple; it only requires a proper primary rows and columns swap for $M_{cir}(A)$ to become $M_{cir}(B)$. Therefore, the two sequences have the same linear complexity.

For any r-circulant matrix over a number field $\mathbb{K}$, there is a very important theorem.

Theorem 3. *[4] Let $M = Cir_n^r(w_1, w_2, \cdots, w_n)$ be an r-circulant matrix over field $\mathbb{K}$.Denote the function $w(x) = \sum_{i=0}^{n-1} w_{i+1}x^i$. If the set of all roots of the equation $x^n - r = 0$ over field $\mathbb{K}$ can be written as $\{\theta\xi^i \mid i = 0, 1, \cdots, n-1\}$, where $\theta^n = r$. Then the set of all characteristic roots of the matrix M is $\{w(\theta\xi^i) \mid i = 0, 1, \cdots, n-1\}$.*

2.3 Block matrix and matrix over ring

Let $\mathbb{K}$ be a field, denote the ring of all $mn \times mn$ matrices over field $\mathbb{K}$ by $M_{mn\times mn}(\mathbb{K})$. Mark matrix ring R as subring of $M_{n\times n}(\mathbb{K})$. Suppose a matrix A belongs to $M_{m\times m}(R)$, then A also belongs to $M_{mn\times mn}(\mathbb{K})$. Let $[A]^R_{i,j}$ denote the i,jth block of A, $a_{i,j}$ denote the i,jth entry of A when over $M_{mn\times mn}(\mathbb{K})$. It's easy to see that

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,mn} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,mn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{mn,1} & a_{mn,2} & \cdots & a_{mn,mn} \end{pmatrix} = \begin{pmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,m} \\ A_{2,1} & A_{2,2} & \cdots & A_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m,1} & A_{m,2} & \cdots & A_{m,m} \end{pmatrix} = A^R$$

The above sliced matrix A is called the block matrix, In particular, when we discuss A as a element of $M_{m\times m}(R)$, we use A^R to denote A, and the corner marks are used only for distinction.

For a general commutative ring R, Brown W C [3] studied relevant properties about matrices over the ring R. Including the determinant $det_R(A^R)$, rank $rank_R(A^R)$, modulus, diagonalization. Based on the definitions and results given in the book, we got the following remarkable theorems.

Theorem 4. *Let $A \in M_{m\times m}(R)$, where R is the subalgebra of $M_{n\times n}(\mathbb{K})$ and $R =< S >$ is a subalgebra generated by S only, i.e., the smallest subalgebra of $M_{n\times n}(\mathbb{K})$ that contains S. Where the minimal polynomial $f(x) = p^r(x)$ of $S \in M_{n\times n}(\mathbb{K})$ is an power of an irreducible polynomial $p(x)$ over the field $\mathbb{K}$. Thus,*

$$rank_R\left(A^R\right) = k \Rightarrow rank_{\mathbb{K}}(A) \geq kn, 0 \leq k \leq m$$

Clearly, when the commutative ring R satisfies the conditions in the above theorem, R is isomorphic to the residue class ring $H = \mathbb{K}[x]/(p^r(x))$. This means that the equation $rank_R(A^R) = rank_H(A^H)$ will hold automatically under isomorphism.

Denote another ring of residue classes $\overline{H} = \mathbb{K}[x]/(p(x))$, it's easy to see $\overline{H}$ is a field. At the same time, there exists a surjective homomorphism mapping π from H to $\overline{H}$. The image of A^H under the action of π is written as $\overline{A} \in M_{m\times m}(\overline{H})$. We have the following theorem.

Theorem 5.

$$rank_H\left(A^H\right) = rank_{\overline{H}}\left(\overline{A}\right)$$

These two theorems provide theoretical support for our estimate of the lower bound on linear complexity. The proof procedure is complex and unproductive for this paper. For logical reasons, the exact process of their proof is omitted.

3 Linear complexity estimation model for feedforward clock-controlled sequences

This section we will show you how to use the basic model of pseudo-random sampling. And transform sequences' circulant matrix. Finally estimate the rank of block matrix.

Denote two period sequence $\{a_i\}_\infty$ and $\{b_i\}_\infty$, where $a_i \in \mathbb{N}$ and $b_i \in \mathbb{F}_2$. Denote $\sum_{i=1}^{k} a_i$ by s_k. By sampling $\{b_i\}_\infty$ with index sequence $\{s_i\}_\infty$, we get a new sequence $C = \{c_i\}_\infty$, where $c_i = b_{s_i}$. We call $\{c_i\}_\infty$ a clock-controlled sequence generated by $\{a_i\}_\infty$ controlling $\{b_i\}_\infty$.

In general case, people prefer to use maximal period sequences as them have good statistical properties. So we always assume s_m is coprime with the period n in follow discussion.

3.1 Primary transformation of the circulant matrix $M_{cir}(C)$

It's hard to direct calculate rank of $M_{cir}(C)$, so we do some row operations and column operations on $M_{cir}(C)$ and denote the matrix after operations by $\overline{C}$:

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ \vdots \\ mn \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & \cdots & mn \end{array} \\ \begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_{mn} \\ c_{mn} & c_1 & c_2 & & c_{mn-1} \\ c_{mn-1} & c_{mn} & c_1 & & c_{mn-2} \\ \vdots & & & \ddots & \vdots \\ c_2 & c_3 & c_4 & \cdots & c_1 \end{pmatrix} \end{array} \Rightarrow \begin{array}{c} \\ I_1 \\ I_2 \\ I_3 \\ \vdots \\ I_m \end{array} \begin{array}{c} \begin{array}{ccccc} I_1 & I_2 & I_3 & \cdots & I_m \end{array} \\ \begin{pmatrix} C_{1,1} & C_{1,2} & C_{1,3} & & C_{1,m} \\ C_{2,1} & C_{2,2} & C_{2,3} & \cdots & C_{2,m} \\ C_{3,1} & C_{3,2} & C_{3,3} & & C_{3,m} \\ & \vdots & & \ddots & \vdots \\ C_{m,1} & C_{m,2} & C_{m,3} & \cdots & C_{m,m} \end{pmatrix} \end{array}$$

Where the index set $I_i = \{i, m+i, 2m+i, \cdots, (n-1)m+i\}$, and the submatrix $C_{i,j}$ was construct by entries from I_i's rows and I_j's columns of $M_{cir}(C)$. Assume $t = (j - i + 1) \mod mn$, then:

$$C_{i,j} = \begin{array}{c} \\ i \\ m+i \\ 2m+i \\ \vdots \\ (n-1)m+i \end{array} \begin{array}{c} \begin{array}{ccccc} j & m+j & 2m+j & \cdots & (n-1)m+j \end{array} \\ \begin{pmatrix} c_t & c_{t+m} & c_{t+2m} & & c_{t+(n-1)m} \\ c_{t+(n-1)m} & c_t & c_{t+m} & \cdots & c_{t+(n-2)m} \\ c_{t+(n-2)m} & c_{t+(n-1)m} & c_t & & c_{t+(n-3)m} \\ & \vdots & & \ddots & \vdots \\ c_{t+m} & c_{t+2m} & c_{t+3m} & \cdots & c_t \end{pmatrix} \end{array}$$

It's easy to show that $C_{i,j}$ was a circulant matrix, and for two submatrices $C_{i,j}$ and $C_{i',j'}$, $C_{i,j} = C_{i',j'}$ if and only if $j - i = j' - i'$.

Consider subsequence $C^t = \{c_{t+m\cdot i}\}_\infty$, this sequence has a period of n. In fact, C^t equals to $\{b_{s_t+s_m\cdot i}\}_\infty$, it's a sampling sequence of $\{b_i\}_\infty$ with s_m step length. Further, assume $v = (s_m)^{-1} \mod n$ and $l_t = v(s_t - s_1)$, C^t equals to C^1 start from l_tth position.

Using the fact that $C_{i,j}$ is a circulant matrix, $C_{i,j}$ equals to $M_{cir}(C^t)$. Thus, there is a formula:

$$C_{i,j} = M_{cir}(C^t) = M_{cir}(C^1) \cdot D^{l_t} \tag{2}$$

D is a primitive circulant matrix with dimension n, as shown in follow:

Turn back to $C_{i,j}$, if $j \geq i$, then $t = j - i + 1$, if $j < i$, then $t = j - i + 1 + mn$. So

$$C_{i,j} = M_{cir}(C^1) \cdot D^{l_t} = M_{cir}(C^1) \cdot D^{v(s_t - s_1)}.$$

Denote D^v by T, denote $M_{cir}(C^1) \cdot T^{-s_1}$ by $\hat{C}$. Notice that $T^n = I$, we denote $s_{-i} = s_{m-i} - s_m$. When $j \geq i$, $C_{i,j} = \hat{C} \cdot T^{s_{j-i+1}}$; when $j < i$, $C_{i,j} = \hat{C} \cdot T^{s_{j-i+1}+s_m n} = \hat{C} \cdot T^{s_{j-i+1}} = \hat{C} \cdot T^{s_{m+j-i+1}-s_m} = \hat{C} \cdot T^{s_{m+j-i+1}} \cdot D^{-1}$. Different premise get same result.

Thus,

$$\overline{C} = \begin{pmatrix} \hat{C}T^{s_1} & \hat{C}T^{s_2} & \hat{C}T^{s_3} & & \hat{C}T^{s_m} \\ \hat{C}T^{s_m}D^{-1} & \hat{C}T^{s_1} & \hat{C}T^{s_2} & \cdots & \hat{C}T^{s_{m-1}} \\ \hat{C}T^{s_{m-1}}D^{-1} & \hat{C}T^{s_m}D^{-1} & \hat{C}T^{s_1} & & \hat{C}T^{s_{m-2}} \\ & \vdots & & \ddots & \vdots \\ \hat{C}T^{s_2}D^{-1} & \hat{C}T^{s_3}D^{-1} & \hat{C}T^{s_4}D^{-1} & \cdots & \hat{C}T^{s_1} \end{pmatrix}.$$

3.2 Decomposition of the matrix over the ring

In this part, some Lemmas are needed to decompose the matrix over the ring $R =< S >= \left\{\sum_{i=0}^{\infty} k_i S^i \middle| k_i \in \mathbb{K}, i = 0, 1, \cdots\right\}$.

Let $R =< S >= \{\sum_{i=0}^{\infty} k_i S^i | k_i \in \mathbb{K}, i = 0, 1, \cdots\}$, where S is an element of $M_{n\times n}(\mathbb{K})$. It's obvious that R is a commutative(multiplication) subalgebra of $M_{n\times n}(\mathbb{K})$

Denote S's minimal polynomial over $\mathbb{K}$ by $f(x) = \sum_{i=0}^{l} f_i x^i$, where $l \leq n$ and $f_i \in \mathbb{K}(f_l = 1)$. Thus,

$$< S >= \{\sum_{i=0}^{l-1} k_i S^i | k_i \in \mathbb{K}, i = 0, 1, \cdots, l-1\}.$$

Given $U, V \in< S >$, where $U = \sum_{i=0}^{l-1} u_i S^i, V = \sum_{i=0}^{l-1} v_i S^i$. It's obvious that $U = V$ if and only if $u_i = v_i, \forall i = 0, 1, \cdots, l-1$.

Lemma 1. *Suppose that $S \in M_{n\times n}(\mathbb{K})$ is a matrix over the field $\mathbb{K}$, where the minimal polynomial of S is $f(x)$. And the unique factorization of $f(x)$ over field K is $f(x) = \prod_{i=1}^{d} p_i^{r_i}(x)$, $p_i(x)$ is irreducible and $p_i(x) \neq p_j(x)$ when $i \neq j$.*

Thus, there exists a non-singular matrix $P \in M_{n\times n}(\mathbb{K})$, and matrices S_i for $1 \leq i \leq d$. Where the minimal polynomial of S_i is $p_i^{r_i}(x)$. Such that:

$$S = P^{-1} \cdot \begin{pmatrix} S_1 & & & \\ & S_2 & & \\ & & \ddots & \\ & & & S_d \end{pmatrix} \cdot P$$

In the classical theory of linear algebra, this lemma can be easily proved by analyzing the invariant subspace of the linear transformation.

Corollary 2. *For any* $U = \sum_{i=0}^{l-1} u_i S^i \in R =< S >$, *exist mapping* $g(U) = P \cdot U \cdot P^{-1}$, *from* $R =< S >$ *to* $\overline{R} =< PSP^{-1} >$. *And,*

$$g\left(U\right) = \begin{pmatrix} \sum_{i=0}^{l-1} u_i S_1^i & & \\ & \ddots & \\ & & \sum_{i=0}^{l-1} u_i S_d^i \end{pmatrix}$$

Extend the mapping g from $M_{n\times n}\left(\mathbb{K}\right)$ to $M_{m\times m}\left(M_{n\times n}\left(\mathbb{K}\right)\right)$. Define a mapping G on $M_{m\times m}\left(M_{n\times n}\left(\mathbb{K}\right)\right)$. for any element $T \in M_{m\times m}\left(M_{n\times n}\left(\mathbb{K}\right)\right)$, T can be written as block matrix $T^{M_{n\times n}(\mathbb{K})} = \left(T_{ij}\right)_{m\times m}$, where $T_{ij} \in M_{n\times n}\left(\mathbb{K}\right)$. The mapping G is defined as:

$$G((T_{ij})_{m\times m}) = (g(T_{ij}))_{m\times m}.$$

Obviously, G is a self-isomorphism on $M_{m\times m}\left(M_{n\times n}\left(\mathbb{K}\right)\right)$. And $M_{m\times m}\left(R\right)$ is isomorphic to $M_{m\times m}\left(\overline{R}\right)$ under the action of G, and for $\forall A \in M_{m\times m}\left(R\right)$, $rank_{\mathbb{K}}\left(A\right) = rank_{\mathbb{K}}\left(G\left(A\right)\right)$.

Return to $M_{m\times m}(R)$. According to corollary 2, suppose $A \in M_{m\times m}(R)$, $G(A) \in M_{m\times m}(\overline{R})$. Thus, every entry of $G(A)$ must have a diagonal shape like:

$$[G(A)]_{i,j}^{\overline{R}} = \begin{pmatrix} S_1^{i,j} & & & \\ & S_2^{i,j} & & \\ & & \ddots & \\ & & & S_d^{ij} \end{pmatrix}.$$

Further, if

$$[A]_{i,j}^{R} = f_{i,j}(S) = \sum_{t=0}^{l-1} a_t S^t,$$

then

$$[G(A)]_{i,j}^{\overline{R}} = g([A]_{i,j}^{R}) = P \cdot f_{i,j}(S) \cdot P^{-1} = \sum_{t=0}^{l-1} a_t (PSP^{-1})^t.$$

It's trivial that $S_k^{i,j} = f_{i,j}(S_k)$ for all $i, j = 1, 2, \cdots, m$; $k = 1, 2, \cdots, d$.

Thus, by some row operations and column operations, we can transform $G(A)$ into a quasi-diagonal matrix over $M_{mn\times mn}(\mathbb{K})$:

$$\Gamma_0 \cdot G(A) \cdot \Gamma_1 = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_d \end{pmatrix}.$$

Γ_0 and Γ_1 are products of some elementary matrix over $M_{mn\times mn}(\mathbb{K})$. $A_t \in M_{mn_t\times mn_t}(\mathbb{K})$ was constructed by $S_t^{i,j}$ as follow:

$$A_t = \begin{pmatrix} S_t^{1,1} & S_t^{1,2} & \cdots & S_t^{1,m} \\ S_t^{2,1} & S_t^{2,2} & & \vdots \\ \vdots & & \ddots & \\ S_t^{m,1} & \cdots & & S_t^{mm} \end{pmatrix}.$$

So $A_t \in M_{m\times m}(< S_t >)$, and we arrive at the conclusion that:

$$rank_{\mathbb{K}}(A) = rank_{\mathbb{K}}(G(A)) = \sum_{t=1}^{d} rank_{\mathbb{K}}(A_t).$$

3.3 Linear complexity estimation model

Let $R =< D >\in M_{n\times n}$, D is a primitive circulant matrix with dimension n.

Obviously, the minimal polynomials of D is $f(x) = x^n + 1$. Assume $f(x)$ have unique factorization $f(x) = \prod_{i=1}^{d} p_i^{2^\sigma}(x)$, where $n/2^\sigma$ is exactly an odd integer.

From the conclusion of subsection 3.1, the linear complexity of the clock-controlled sequence $L(C) = rank_{\mathbb{K}}(\overline{C})$. At the same time, $\overline{C} \in M_{m\times m}(R)$. Combining the matrix decomposition conclusions of subsection 3.2, we know that

$$rank_{\mathbb{K}}(\overline{C}) = rank_{\mathbb{K}}(G(\overline{C})) = \sum_{t=1}^{d} rank_{\mathbb{K}}(\overline{C}_t)$$

At the same time, $\overline{C}_t$ is very similar to $\overline{C}$ and has the following form:

$$\overline{C}_t = \begin{pmatrix} \hat{C}_t & O & \cdots & O \\ O & \hat{C}_t & & O \\ \vdots & & \ddots & \\ O & O & \cdots & \hat{C}_t \end{pmatrix} \cdot \begin{pmatrix} T_t^{s_1} & T_t^{s_2} & T_t^{s_3} & & T_t^{s_m} \\ T_t^{s_m} D_t^{-1} & T_t^{s_1} & T_t^{s_2} & \cdots & T_t^{s_{m-1}} \\ T_t^{s_{m-1}} D_t^{-1} & T_t^{s_m} D_t^{-1} & T_t^{s_1} & & T_t^{s_{m-2}} \\ & \vdots & & \ddots & \vdots \\ T_t^{s_2} D_t^{-1} & T_t^{s_3} D_t^{-1} & T_t^{s_4} D_t^{-1} & \cdots & T_t^{s_1} \end{pmatrix}$$

Where

$$P \cdot D \cdot P^{-1} = \begin{pmatrix} D_1 & & & \\ & D_2 & & \\ & & \ddots & \\ & & & D_d \end{pmatrix}.$$

and $T_t = D_t^v$, where $v \times s_m \equiv 1 \mod n$.

D_t's minimal polynomial is $p_t^{2^\sigma}(x)$, D_t generate a commutative subalgebra, denote it by $R_t =< D_t >$. Recall the theory of block-matrix, we know $R_t \cong \mathbb{F}_2[x]/(p_t^{2^\sigma}(x)) \triangleq H_t$. Set up ϕ_t to be the isomorphism function from R_t to $\mathbb{F}_t[x]/(p_t^{2^\sigma}(x))$, denote $\phi_t(D_t)$ by α_t, denote $\phi_t(T_t)$ by β_t. Thus, $\beta_t = \alpha^v$

mod $p_t^{2^\sigma}(x)$. Furthermore, consider the projection δ_t from $\mathbb{F}_2[x]/(p_t^{2^\sigma}(x))$ to field $\mathbb{F}_2[x]/(p_t(x)) \triangleq \overline{H_t}$:

$$\delta_t(\overline{h(x)}) = \overline{(h(x) \mod p_t(x))}$$

Let $\delta_t(\alpha_t) = \overline{\alpha_t}$, $\delta_t(\beta_t) = \overline{\beta_t}$.

Denoted matrix $M_t \in M_{m\times m}(R_t)$ and $\overline{M_t} \in M_{m\times m}(\overline{H_t})$:

$$M_t^{R_t} = \begin{pmatrix} T_t^{s_1} & T_t^{s_2} & T_t^{s_3} & & T_t^{s_m} \\ T_t^{s_m} D_t^{-1} & T_t^{s_1} & T_t^{s_2} & \cdots & T_t^{s_{m-1}} \\ T_t^{s_{m-1}} D_t^{-1} & T_t^{s_m} D_t^{-1} & T_t^{s_1} & & T_t^{s_{m-2}} \\ & \vdots & & \ddots & \vdots \\ T_t^{s_2} D_t^{-1} & T_t^{s_3} D_t^{-1} & T_t^{s_4} D_t^{-1} & \cdots & T_t^{s_1} \end{pmatrix}$$

$$\overline{M_t} = \begin{pmatrix} \overline{\beta_t}^{s_1} & \overline{\beta_t}^{s_2} & \overline{\beta_t}^{s_3} & & \overline{\beta_t}^{s_m} \\ \overline{\beta_t}^{s_m} \overline{\alpha_t}^{-1} & \overline{\beta_t}^{s_1} & \overline{\beta_t}^{s_2} & \cdots & \overline{\beta_t}^{s_{m-1}} \\ \overline{\beta_t}^{s_{m-1}} \overline{\alpha_t}^{-1} & \overline{\beta_t}^{s_m} \overline{\alpha_t}^{-1} & \overline{\beta_t}^{s_1} & & \overline{\beta_t}^{s_{m-2}} \\ & \vdots & & \ddots & \vdots \\ \overline{\beta_t}^{s_2} \overline{\alpha_t}^{-1} & \overline{\beta_t}^{s_3} \overline{\alpha_t}^{-1} & \overline{\beta_t}^{s_4} \overline{\alpha_t}^{-1} & \cdots & \overline{\beta_t}^{s_1} \end{pmatrix}$$

Since Theorem 4,

$$rank_{\mathbb{K}}(\overline{C}_t) \geq rank_{\mathbb{K}}(\hat{C}_t) \times rank_{R_t}(M_t^{R_t}).$$

Since Theorem 5,

$$rank_{\mathbb{K}}(\overline{C}_t) \geq rank_{\mathbb{K}}(\hat{C}_t) \times rank_{R_t}(M_t^{R_t}) = rank_{\mathbb{K}}(\hat{C}_t) \times rank_{\overline{H_t}}(\overline{M_t}).$$

Finally, we get a Linear complexity lower bound estimation inequality.

Theorem 6.

$$L(C) = \sum_{t=1}^{d} rank_{\mathbb{K}}(\overline{C}_t) \geq \sum_{t=1}^{d} rank_{\mathbb{K}}(\hat{C}_t) \times rank_{\overline{H_t}}(\overline{M_t})$$

The last problem turns into how to estimate $rank_{\mathbb{K}}(\hat{C}_t)$ and $rank_{\overline{H_t}}(\overline{M_t})$.

Estimate $\boldsymbol{rank(\hat{C}_t)}$ over $\boldsymbol{F_2}$: Since $C^1 = \{c_{1+m\cdot i}\}_{i=0}^{\infty}$, so $\hat{C} = M_{cir}\left(C^1\right) \cdot T^{-s_1} = \left(\sum_{i=0}^{n-1} c_{1+m\cdot i} D^i\right) \cdot D^{-s_1 v}$. Thus:

$$\hat{C}_t = \left(\sum_{i=0}^{n-1} c_{1+m\cdot i} D_t^i\right) \cdot D_t^{-s_1 v}$$

That means, $rank_{F_2}(\hat{C}_t)$ equals to rank of matrix $\sum_{i=0}^{n-1} c_{1+m\cdot i} D_t^i$.

Let the formal power series $F^1(x) = \sum_{i=0}^{\infty} c_{1+m\cdot i} x^i$, be the generating function of the sequence C^1, and let $H(x) \in F_2[x]$, be the minimum generator

Polynomial of C^1. The order of $H(x)$ is equal to the linear complexity of C^1. There exists polynomial $P(x) \in F_2[x]$ with number less than l such that the following constant equation holds, $H(x)$ and $P(x)$ are coprime.[8]

$$F^1(x) = \frac{P(x)}{H(x)}$$

Let $\overline{F^1}(x) = \sum_{i=0}^{n-1} c_{1+m\cdot i} x^i$, then the power series of the form

$$F^1(x) = \frac{\overline{F^1}(x)}{1+x^n}$$

and $H(x)|1+x^n$. This is a conclusion that comes from the minimal property of $H(x)$.

Thus,

$$\overline{F^1}(x) \cdot H(x) = P(x) \cdot (1+x^n)$$

The equation no longer needs to be discussed under the formal power series sense and goes back to the polynomial ring $F_2[x]$.

As we know, $x^n + 1 = \prod_{i=1}^{d} p_i^{2^\delta}(x)$ and $H(x)|(1+x^n)$. Assume $H(x) = \prod_{i=1}^{d} p_i^{h_i}(x)$, where $0 \le h_i \le 2^\sigma$. Then:

$$\overline{F^1}(x) = P(x) \cdot \prod_{i=1}^{d} p_i^{2^\delta - h_i}(x)$$

- When $h_t = 0$, Since the characteristic(minimal) polynomial of the matrix D_t is $p_t^{2^\delta}(x)$, $p_t^{2^\delta}(D_t)$ is a zero square matrix. Led to

$$\overline{F^1}(D_t) = P(D_t) \cdot \prod_{i \ne t} p_i^{2^\delta - h_i}(D_i) \cdot p_t^{2^\delta}(D_t) = O$$

$$rank\left(\hat{C}_t\right) = rank(\overline{F^1}(D_t)) = 0$$

- When $h_t > 0$, Since $H(x)$ is coprime to $P(x)$, $p_t(x)$ is coprime to $P(x)$. Therefore, $P(D_t)$ is still a full-rank square (because the root sets of $P(x) = 0$ does not include any characteristic root of D_t). Thus,

$$rank\left(\hat{C}_t\right) = rank\left(\overline{F^1}(D_t)\right) = rank\left(p_t^{2^\delta - h_t}(D_t)\right) \ge h_t \times deg\left(p_t(x)\right)$$

Combining these two cases, the following inequalities can be derived.

$$rank\left(\hat{C}\right) = \sum_{t=1}^{d} rank\left(\hat{C}_t\right) \ge \sum_{t=1}^{d} \left(h_t \times deg\left(p_t(x)\right)\right) = deg\left(H(x)\right)$$

Notice that both left and right of the inequality are equal to the $L\left(C^1\right)$, so the inequality equal sign holds constant. That is, for $\forall 1 \le t \le d$, we have

$$rank\left(\hat{C}_t\right) = h_t \times deg\left(p_t(x)\right).$$

Estimate $\boldsymbol{rank_{\overline{H_t}}(\overline{M_t})}$: It's easy to see that $\overline{M_t}$ is an $\overline{\alpha_t}^{-1}$-circulant matrix over field $\overline{H_t}$. Let $E_t(x) = \sum_{i=0}^{m-1} \overline{\beta_t}^{s_{i+1}} x^i \in \overline{H_t}[x]$, $J_t(x) = x^m + \overline{\alpha_t}^{-1} \in \overline{H_t}[x]$. Use theorem 3, denote The degree of the greatest common factor of $E_t(x)$ and $J_t(x)$ by g_t, then

$$rank_{\overline{H_t}}(\overline{M_t}) = m - g_t.$$

In summary, we get a final inequality of rank:

$$rank\left(M_t\right) \geq rank\left(\hat{C}_t\right) \cdot rank_{R_t}\left(\overline{M_t}^{R_t}\right) = h_t \times deg\left(p_t\left(x\right)\right) \times (m - g_t)$$

After accumulation:

Theorem 7.

$$L(C) \geq \sum_{t=1}^{d} h_t \times deg\left(p_t\left(x\right)\right) \times (m - g_t)$$

3.4 Section summary

This section analyzed the lower bound on the linear complexity of the basic feedforward clock-controlled sequence.

The first step is to correspond the linear complexity to the rank of the cyclic matrix. After that, the matrix is organized according to a particular sampling law. In this way, the matrix becomes a matrix on a circulant matrix ring.

However, the matrix on a normal commutative ring is not easy to count the rank. So further quasi-diagonalization is performed for each matric block at the same time. Then the goal becomes to compute the sum of the ranks of all matrices M_t on the diagonal.

Using Theorem 4 and Theorem 5, we can successfully estimate the rank of the matrix M_t.

Through such a series of transformations, we decompose the problem to each subfield. In this way, the enormous problem of overall linear complexity becomes a collection of several minor problems. Finally, we obtained a valuable conclusion.

The following section gives a new stream cipher LIFI-128 using a nonlinear drive module reference to the LILI-128 algorithm. This kind of stream cipher's complexity is impossible to be estimated by traditional results. However, our new method can solve its linear complexity problem.

4 LIFI-128, and it's linear complexity

4.1 Description of LIFI-128

We give an example that was set up to follow the LILI-128 algorithm. The clock-control subsystem uses a pseudorandom binary sequence produced by a regularly clocked LFSR, $LFSR_a$, of length 39, and a function, f_a, operating on some contents of $LFSR_a$ to produce a pseudorandom integer sequence, $A = \{a_i\}_\infty$, and $a_i \in \{1, 2, 3, 4\}$. The feedback polynomial of $LFSR_a$ is chosen to be a

primitive polynomial. Moreover, the initial state of $LFSR_a$ must not be all zero. It follows that $LFSR_a$ produces a maximum-length sequence of period $m = 2^{39}-1$. Set f_a to be boolean balance function every bit, so $s_m = 2^{39-1}(2^2+1)-1$.

The data-generation subsystem uses the integer sequence A to control the clocking of a binary FCSR[15], $FCSR_b$, of length 89. The lowest content bit of $FCSR_b$ will generate a binary sequence $B = \{b_i\}_\infty$. The feedback integer of $FCSR_b$ is chosen to be a safe prime integer $q = 2p+1$, where p is a prime, $\lfloor \log_2(q) \rfloor = 89$. And the initial state of $FCSR_b$ is not zero, 2 is a primitive elements of $\mathbb{F}_q^*$. It follows that $FCSR_b$ produces a nonlinear binary sequence with period $n = 2p$, linear complexity $L(B) = p+1$. Specially, in this example, we assume 2 also is a primitive elements of $\mathbb{F}_p^*$, and $gcd(p-1, 39) = 1$.

Notice that $n = 2p$ is coprime with $s_m = 2^{39-1}(2^2+1)-1$. Define the clock-controlled sequence $C = \{c_i = b_{s_i}\}_\infty$ as the keystream, thus C get a maximum-length of period $mn = (2^{39}-1) \times (2p) \approx 2^{128}$.

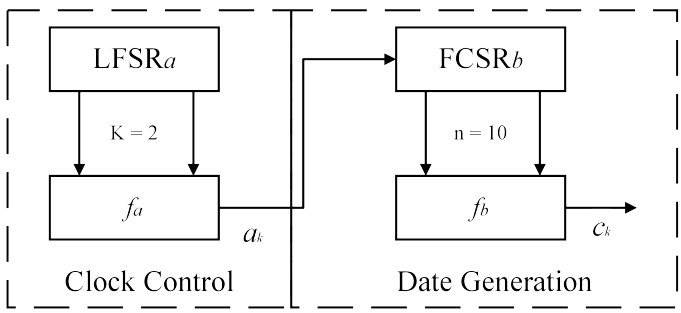

Fig. 1. The Structure of LIFI-128

4.2 Linear Complexity

We are going to prove that the linear complexity of C has a lower bound $(L(B)-2)m+2 = (p-1)(2^{39}-1)+2$.

Consider the $n \times n$ circulant matrices ring R which was generated by D. It's easy to show that R is a commutative algebra over $\mathbb{F}_2$, thus, for any period n sequence S, $M_{cir}(S) \in R$. As this result, the clock-matrix is a $m \times m$ matrix over R.

It is obvious that the minimal polynomial of D equals to $f(x) = x^n+1$. $f(x)$ has a decomposition over $\mathbb{F}_2$:

$$f(x) = x^{2p}+1 = (x^p+1)^2 = (x+1)^2(\sum_{i=0}^{p-1} x^i)^2.$$

As 2 is a primitive elements of $\mathbb{F}_p^*$, $\sum_{i=0}^{p-1} x^i$ is reduced in $\mathbb{F}_2[x]$. Assume $f(x) = p_1^2(x)p_2^2(x)$, where $p_1(x) = x+1$, $p_2(x) = \sum_{i=0}^{p-1} x^i$. Thus, we can find a $n \times n$ nonsingular matrix P over $\mathbb{F}_2$ such that $P \cdot S \cdot P^{-1}$ is a quasi-diagonalization on $S \in R$.

$$P \cdot S \cdot P^{-1} = \begin{pmatrix} Q_1 & O \\ O & Q_2 \end{pmatrix}$$

In above formula Q_1 is the factor relates to $p_1^2(x)$, Q_2 is factor relates to $p_2^2(x)$. As $degree(p_1) = 1, degree(p_2) = p-1$, $Q_1 \in M_{2\times 2}(\mathbb{F}_2)$, $Q_2 \in M_{2(p-1)\times 2(p-1)}(\mathbb{F}_2)$.

Notice that $\hat{C}, T, D \in R$, we denote:

$$P\hat{C}P^{-1} = \begin{pmatrix} \hat{C}_1 & O \\ O & \hat{C}_2 \end{pmatrix}, \quad PTP^{-1} = \begin{pmatrix} T_1 & O \\ O & T_2 \end{pmatrix}, \quad PDP^{-1} = \begin{pmatrix} D_1 & O \\ O & D_2 \end{pmatrix}$$

By theory of FCSR[15], the minimial generator Polynomial of sequence $B' = \{b_{s_m i+1}\}_{i=0}^{\infty}$ is $H(x) = (x+1)(x^p+1) = p_1^2(x)p_2(x)$. Thus $rank(\hat{C}_1) = 2$, $rank(\hat{C}_2) = p-1$.

In field $F_2[x]/(x+1) = F_2$, $\overline{\alpha_1} = \overline{\beta_1} = \overline{1}$. Then:

$$\overline{M_1} = \begin{pmatrix} \overline{\beta_1}^{s_1} & \overline{\beta_1}^{s_2} & \overline{\beta_1}^{s_3} & & \overline{\beta_1}^{s_m} \\ \overline{\beta_1}^{s_m}\overline{\alpha_1}^{-1} & \overline{\beta_1}^{s_1} & \overline{\beta_1}^{s_2} & \cdots & \overline{\beta_1}^{s_{m-1}} \\ \overline{\beta_1}^{s_{m-1}}\overline{\alpha_1}^{-1} & \overline{\beta_1}^{s_m}\overline{\alpha_1}^{-1} & \overline{\beta_1}^{s_1} & & \overline{\beta_1}^{s_{m-2}} \\ & \vdots & & \ddots & \vdots \\ \overline{\beta_1}^{s_2}\overline{\alpha_1}^{-1} & \overline{\beta_1}^{s_3}\overline{\alpha_1}^{-1} & \overline{\beta_1}^{s_4}\overline{\alpha_1}^{-1} & \cdots & \overline{\beta_1}^{s_1} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{1} & \cdots & \overline{1} \\ \overline{1} & \overline{1} & \cdots & \overline{1} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{1} & \overline{1} & \cdots & \overline{1} \end{pmatrix}.$$

It's easy to see $rank(\overline{M_1}) = 1$.

Next, we are going to count follow matrix $\overline{M_2}$.

$$\overline{M_2} = \begin{pmatrix} \overline{\beta_2}^{s_1} & \overline{\beta_2}^{s_2} & \overline{\beta_2}^{s_3} & & \overline{\beta_2}^{s_m} \\ \overline{\beta_2}^{s_m}\overline{\alpha_2}^{-1} & \overline{\beta_2}^{s_1} & \overline{\beta_2}^{s_2} & \cdots & \overline{\beta_2}^{s_{m-1}} \\ \overline{\beta_2}^{s_{m-1}}\overline{\alpha_2}^{-1} & \overline{\beta_2}^{s_m}\overline{\alpha_2}^{-1} & \overline{\beta_2}^{s_1} & & \overline{\beta_2}^{s_{m-2}} \\ & \vdots & & \ddots & \vdots \\ \overline{\beta_2}^{s_2}\overline{\alpha_2}^{-1} & \overline{\beta_2}^{s_3}\overline{\alpha_2}^{-1} & \overline{\beta_2}^{s_4}\overline{\alpha_2}^{-1} & \cdots & \overline{\beta_2}^{s_1} \end{pmatrix}$$

$\overline{\beta_2} = \overline{\alpha_2}^{v}$, where $v \times s_m \equiv 1 \mod n$.

Notice that $\overline{M_2}$ is a $m \times m$ matrix over field $\mathbb{F}_2[x]/(p_2(x))$, in particular, $\overline{M_2}$ is a $\overline{\alpha_2}^{-1}$-circulant matrix.

With the help of Theorem 3, we know $\overline{M_2}$ is non-singular if and only if $w(x) = \sum_{i=1}^{m} \overline{\beta_2}^{s_i} x^{i-1}$ doesn't have common root with $x^m - \overline{\alpha_2}^{-1} = 0$, or $\overline{M_2}$ has a zero eigenvalue.

As m is coprime with the order p of $\overline{\alpha_2}^{-1}$, there is a integer k such that $(\overline{\alpha_2}^{k})^m = \overline{\alpha_2}^{-1}$. Assume $\{\xi^i | i = 0, 1, \cdots, m-1\}$ is all roots of equation $x^m - 1 = 0$, then roots set of $x^m - \overline{\alpha_2}^{-1} = 0$ is $\{\xi^i \overline{\alpha_2}^{k} | i = 0, 1, \cdots, m-1\}$. If $\xi^j \overline{\alpha_2}^{k}$ is a

root of $w(x)$, which means:

$$\begin{aligned} w(\xi^j\overline{\alpha_2}^k) =& \sum_{i=1}^{m} \overline{\beta_2}^{s_i}(\xi^j\overline{\alpha_2}^k)^{i-1} \\ =& \sum_{i=1}^{m} \overline{\alpha_2}^{s_i v+(i-1)k}(\xi^j)^{i-1} \end{aligned}$$

Define another function $g(x) = \sum_{i=1}^{m} \overline{\alpha_2}^{s_i v+(i-1)k} x^{i-1}$, it's easy to see that $gcd(w(x), x^m - \overline{\alpha_2}^{-1}) \neq 1$ equals to $gcd(g(x), x^m - 1) \neq 1$.

The proof is by contradiction, suppose that there is $0 \leq i' \leq m-1$, $\xi' = \xi^{i'}$ is a common root of $g(x)$ and $x^m - 1$. Notice that $\xi'^{m+1} = \xi'^{2^{39}} = \xi'$, we calculate the 2^{39}th power of $g(\xi')$. It shows:

$$\begin{aligned} 0 =& (g(\xi'))^{2^{39}} \\ =& \sum_{i=1}^{m} \overline{\alpha_2}^{(s_i v+(i-1)k)\times 2^{39}}(\xi'^{2^{39}})^{i-1} \\ =& \sum_{i=1}^{m} (\overline{\alpha_2}^{2^{39}})^{s_i v+(i-1)k}\xi'^{i-1} \end{aligned}$$

Define function

$$\begin{aligned} h(\overline{\alpha_2}) =& \sum_{i=1}^{m} \xi'^{i-1}(\overline{\alpha_2})^{(s_i v+(i-1)k \mod p)} \\ =& \sum_{i=0}^{p-1}[\sum_{s_j v+(j-1)k\equiv i} \xi'^j]\overline{\alpha_2}^i \end{aligned}$$

Above formula shows that if $\overline{\alpha_2}$ is a root of $h(\overline{\alpha_2}) = 0$, then $\overline{\alpha_2}^{2^{39}}$ will also be a root of $h(\overline{\alpha_2}) = 0$. Now we get a set $\Omega = \{\overline{\alpha_2}^{2^{39i}} | i = 0, 1, \cdots\}$, any elements of this set would be a root of $h(\overline{\alpha_2}) = 0$. Recall that $\overline{\alpha_2}$'s order is p, and 2 is a primitive element of $\mathbb{F}_p^*$, so $\overline{\alpha_2}^{2^{39a}} = \overline{\alpha_2}^{2^{39b}}$ if and only if $39a \equiv 39b \mod (p-1)$. Thus $\#|\Omega| = p-1$. As degree of $h(\overline{\alpha_2})$ less than or equal to $p-1$, Ω must be all roots set of $h(\overline{\alpha_2}) = 0$. Thus, $h(\overline{\alpha_2}) = \xi^* \prod_{i=0}^{p-1}(\overline{\alpha_2} - \overline{\alpha_2}^{2^{39i}})$, ξ^* is a constant.

Denote $\sum_{s_j v+(j-1)k\equiv i} \xi'^j$ by ε_i, $h(\overline{\alpha_2}) = \sum_{i=0}^{p-1} \varepsilon_i \overline{\alpha_2}^i$ and $\xi^* = \varepsilon_{p-1} \neq 0$. Notice $\Omega \subseteq \mathbb{F}_2[x]/p_2(x)$, suppose that $\varepsilon_{i_0} \neq 0$, then ε_{i_0}/ξ^* must be an element in field $\mathbb{F}_2[x]/p_2(x)$, as it is represented as an element generated by Ω over field $\mathbb{F}_2[x]/p_2(x)$. Denote this field by $\mathbb{F}_{2^{p-1}}$.

In the same way,

$$\varepsilon_{i_0}/\xi^* = [\sum_{s_j v+(j-1)k\equiv i_0} \xi'^j]/[\sum_{s_j v+(j-1)k\equiv p-1} \xi'^j].$$

In fact, we can show that $\#\{1 \leq j \leq m | s_j v + (j-1)k \equiv i_0 \mod p\} \leq 1$ for any i_0. Suppose there are $1 \leq j < j' \leq m$ such that $s_j v + (j-1)k \equiv$

$s_{j'}v+(j'-1)k \mod p$. Thus, $s_m m(s_{j'}-s_j)v+s_m m(j'-j)k \equiv 0 \mod p$, equals to $(s_{j'}-s_j)m - s_m(j'-j) \equiv 0 \mod p$. Notice that

$$\begin{aligned}|(s_{j'}-s_j)m - s_m(j'-j)| \leq & |(s_{j'}-s_j)m| + |s_m(j'-j)| \\ \leq & 4(j'-j)m + s_m(j'-j) \\ = & (5\times 2^{38}+3)(j'-j) \\ \leq & 2^{41}\times 2^{39} \\ = & 2^{80} < p.\end{aligned}$$

Thus $(s_{j'}-s_j)m = s_m(j'-j)$. Because $gcd(m, s_m) = gcd(2^{39}-1, 5\times 2^{38}-1) = 1$, we get $m|(j'-j)$, conflicts with $1 \leq j'-j \leq m-1$ and implies $\#\{1 \leq j \leq m | s_j v + (j-1)k \equiv i_0 \mod p\} \leq 1$.

This fact shows that $\varepsilon_{i_0}/\xi^* = 0$, or $\varepsilon_{i_0}/\xi^* = \xi'^s$ for an integer s. As $\varepsilon_{i_0}/\xi^* \in \mathbb{F}_{2^{p-1}}$, $\xi'^m = 1$ and $gcd(m, 2^{p-1}-1) = 1$, those facts led to $\xi'^s = 1$. But it's easy to confirm that $g(\xi') = g(1) \neq 0$.This result conflicts with $g(\xi') = 0$. Based on these facts, $g(x)$ doesn't have common root with $x^m - 1$, $\overline{M_2}$ is non-singular, $rank(\overline{M_2}) = m$

Thus, recall theorem 7,

$$\begin{aligned}L(C) &\geq \sum_{t=1}^{2} h_t \times deg(p_t(x)) \times (m-g_t) \\ &= 2\times 1\times 1 + 1\times (p-1)\times m \\ &= m(p-1)+2.\end{aligned}$$

C's rank greater then $(p-1)m+2 = (p-1)(2^{39}-1)+2$, we get a linear complexity lower bound of clock-controlled sequence $\{c_i\}_\infty$.

4.3 Section summary

This section modifies the LILI-128 algorithm so that its controlled sequence becomes nonlinearly driven with extremely high linear complexity. We call the new algorithm LIFI-128.

None of the published linear complexity analysis methods give a good result for LIFI-128. However, our new model can solve this type of problem very well. The practical value of the linear complexity lower bound estimation method proposed in this paper is fully illustrated.

5 Conclusion

The feedforward clock control structure is a hardware-friendly and widely used structure for designing sequence encryption algorithms. Its basic structure is that two sequence generators connect in series. The first generator is regular output and the second generator clock-controlled by the output of the first generator.

In this paper, we research the feedforward clock-controlled sequence structure by new methods such as circulant matrix and matrix over the ring. Finally, the resulting complexity estimation inequalities can widely apply to the analysis of cryptographic properties of the clock-controlled structure. The traditional result base on cyclotomic polynomials over finite fields is not practical when the controlled sequence is nonlinear. The results presented in this paper can be exactly effective for the analysis of clock-controlled cryptographic systems whether the drive module is linear or nonlinear.

Acknowledgements.

We thank the anonymous reviewers for their helpful comments. This work was supported by the National Natural Science Foundation of China(Grant No.6207211, No.61672059) and the National Key R&D Program of China 2017YFB0802000.

References

1. Beth, T., Piper, F.: The stop-and-go generator. In: Eurocrypt. vol. 84, pp. 88–92. Springer (1984)
2. Blakley, G., Purdy, G.B.: A necessary and sufficient condition for fundamental periods of cascade machines to be products of the fundamental periods of their constituent finite state machines. Information Sciences **24**(1), 71–91 (1981)
3. Brown, W.C.: Matrices over commutative rings. Marcel Dekker, Inc. (1993)
4. Cline, R., Plemmons, R., Worm, G.: Generalized inverses of certain toeplitz matrices. Linear Algebra and Its Applications **8**(1), 25–33 (1974)
5. Coppersmith, D., Halevi, S., Jutla, C.: Cryptanalysis of stream ciphers with linear masking. In: Annual International Cryptology Conference. pp. 515–532. Springer (2002)
6. Courtois, N.T., Meier, W.: Algebraic attacks on stream ciphers with linear feedback. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 345–359. Springer (2003)
7. Dawson, E., Clark, A., Golic, J., Millan, W., Penna, L., Simpson, L.: The lili-128 keystream generator. In: Proceedings of first NESSIE Workshop. Citeseer (2000)
8. Denguo, F., Dingyi, P.: Cryptography Guide. Science Press (1999)
9. Golić, J.D.: Correlation properties of a general binary combiner with memory. Journal of Cryptology **9**(2), 111–126 (1996)
10. Golic, J.D., Zivkovic, M.V.: On the linear complexity of nonuniformity decimated pn-sequences. IEEE Transactions on Information Theory **34**(5), 1077–1079 (1988)
11. Gollmann, D., Chambers, W.G.: Clock-controlled shift registers: a review. IEEE Journal on Selected Areas in communications **7**(4), 525–533 (1989)
12. Jennings, S., M.: A special case of binary sequences. Ph.D. thesis, University of London (1980)
13. Kholosha, A.: Investigations in the design and analysis of key-stream generators. (2004)
14. KjeldsenK, AndresenE: Some randomness properties of cascaded sequences (corresp.). IEEE Transactions on Information Theory (1980)
15. Klapper, A., Goresky, M.: 2-adic shift registers. In: International Workshop on Fast Software Encryption. pp. 174–178. Springer (1993)

16. Matsui, M.: Linear cryptanalysis method for des cipher. In: Workshop on the Theory and Application of of Cryptographic Techniques. pp. 386–397. Springer (1993)
17. Meier, W., Staffelbach, O.: Correlation properties of combiners with memory in stream ciphers. In: Workshop on the Theory and Application of of Cryptographic Techniques. pp. 204–213. Springer (1990)
18. Schaub, T.: A linear complexity approach to cyclic codes. (1990)
19. Xiangang, L.: Analysis of clock-controlled sequences. Information security and communications privacy **2** (1991)
20. Xiangang, L., Zengfa, W., Guozhen, X.: The complexity of some pseudo-random decimated sequences. Journal of china institute of communications **11**(2), 1–6 (1990)