Periods on Two Kinds of Nonlinear Feedback Shift Registers with Time Varying Feedback Functions

Honggang Hu
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
Email. h7hu@ecemail.uwaterloo.ca

Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
Email. ggong@calliope.uwaterloo.ca

Abstract

Grain and Trivium are the hardware-oriented finalists of the eSTREAM. They are both based on nonlinear feedback shift registers. In this paper, we study their generalized classes of nonlinear feedback shift registers with time varying feedback functions, namely, Grain-like and Trivium-like structures. Some interesting results regarding their periods are obtained.

Keywords. eSTREAM, Grain, LFSR, NFSR, period, Trivium.

1 Introduction

Although block ciphers can be implemented as stream ciphers using OFB and CTR mode, stream ciphers are in favor of many applications for two reasons. First, stream ciphers may be implemented much faster than block ciphers. Second, stream ciphers may be much smaller in hardware implementation than block ciphers. Many widely employed stream ciphers have been analyzed successfully, e.g., RC4 in Internet [14], E_0 in Bluetooth [10], [11], [12], [13], $A5/1$ and $A5/2$ in GSM [8], [9].

Linear feedback shift register (LFSR) sequences are widely used as basic functional blocks in key stream generators in stream cipher models due to their fast implementation in hardware as well as in software in some cases, e.g., filtering sequence generators, combinatorial sequence generators, clock-controlled sequence generators, and shrinking generators. Nonlinear feedback shift register (NFSR) sequences are known to be more resistant to cryptanalytic attacks than LFSR sequences. However,

the construction of NFSR sequences with guaranteed long periods is an open problem [3]. Grain and Trivium are the hardware-oriented finalists of the eSTREAM contest [5], [6]. They are both based on NFSRs. In Grain, one LFSR is used to control one NFSR. In Trivium, three NFSRs with simple feedback functions are employed. The first one controls the second one, the second one controls the third one, and the third one controls the first one.

In this paper, we prove some interesting results regarding the periods of two kinds of NFSRs with time varying feedback functions, namely, Grain-like and Trivium-like structures. For the Grain-like structure, if the initial state of the LFSR is nonzero, then the sequence generated by the NFSR is periodic, and the least period is a multiple of that of the sequence generated by the LFSR. The experimental results about those results were first reported in [4]. For the Trivium-like structure, with high probability, the sequences generated by three NFSRs are periodic, and possess the same least period. Such results have been verified using smaller version of Grain and Trivium.

This paper is organized as follows. In Section 2, some necessary background on sequences will be provided. In Section 3, we present the formal definitions of Grain-like and Trivium-like structures. Section 4 contains the main results. Some specific results regarding Grain and Trivium will be given in Section 5. Finally, Section 6 concludes this paper.

2 Preliminaries

Let $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + 1$ be a polynomial over $\mathbb{F}_2$. A sequence $\mathbf{s} = \{s_i\}$ is called an LFSR sequence generated by $f(x)$ if it satisfies the following recursive relation

$$s_{n+k} = \sum_{i=0}^{n-1} c_i s_{k+i}, k = 0, 1, \cdots .$$

$(s_0, s_1, \cdots, s_{n-1})$ is the initial state of the LFSR which generates $\mathbf{s}$. The sequence $\mathbf{s}$ is an m-sequence if $f(x)$ is primitive [2].

The minimal polynomial of $\mathbf{s}$ is a polynomial with smallest degree which generates $\mathbf{s}$. Let $m(x)$ be the minimal polynomial of $\mathbf{s}$, then $m(x) \,|\, f(x)$. The linear complexity (or linear span) of $\mathbf{s}$ is the degree of $m(x)$, denoted by $l(\mathbf{s})$. In general, $m(x)$ can be found using the Berlekamp-Massey algorithm [16] from any $2l(\mathbf{s})$ consecutive bits of $\mathbf{s}$. The (left cyclically) shift operator L is defined by $L\mathbf{s} = s_1, s_2, \cdots$, and $L^r\mathbf{s} = s_r, s_{r+1}, \cdots, r \geq 1$. If $\mathbf{t} = L^r\mathbf{s}$, then we say that they are shift equivalent, and $\mathbf{t}$ is a shift of $\mathbf{s}$; otherwise, they are shift distinct. A sequence $\mathbf{s} = \{s_i\}$ is generated by $f(x)$ if and only if $f(L)\mathbf{s} = \mathbf{0}$, where $\mathbf{0}$ is the zero sequence.

For any $f(x) \in \mathbb{F}_2[x]$ with $f(0) \neq 0$, the order of $f(x)$ is defined to be the minimal integer $l \geq 1$ such that $f(x) \mid x^l + 1$. The period of the sequence $\mathbf{s}$ is equal to the order of its minimal polynomial $m(x)$.

3 Two Structures for Nonlinear Feedback Shift Registers

3.1 The Grain-Like Structure

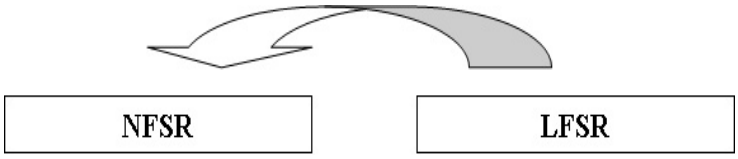

Figure 1: The Grain-Like Structure

In the Grain-like structure, one LFSR is used to control one NFSR (see Figure 1).

Suppose that the content of the LFSR contains n bits denoted by $s_i, s_{i+1}, ..., s_{i+n-1}$, and the content of the NFSR contains m bits denoted by $b_i, b_{i+1}, ..., b_{i+m-1}$. The feedback polynomial of the LFSR is $f(x)$ which is primitive of degree n, and the feedback function of the NFSR is $x_0 + g(x_1, x_2, ..., x_{m-1})$. Then the sequence $\{b_i\}_{i=0}^{\infty}$ generated by the Grain-like structure is defined by

$$b_{i+m} = s_i + b_i + g(b_{i+1}, b_{i+2}, ..., b_{i+m-1}), \text{ for any } i \geq 0.$$

3.2 The Trivium-Like Structure

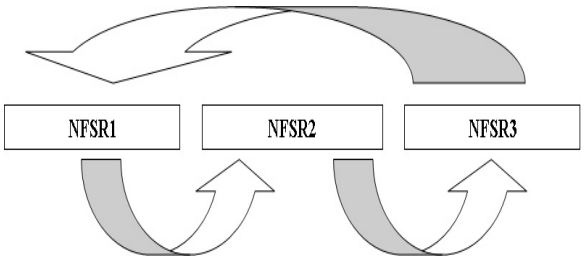

Figure 2: The Trivium-Like Structure

In the Trivium-like structure, there are three NFSRs. The first one controls the second one, the second one controls the third one, and the third one controls the first one (see Figure 2).

Suppose that the content of the first NFSR contains m bits denoted by $a_i, a_{i+1}, ..., a_{i+m-1}$, the content of the second NFSR contains n bits denoted by $b_i, b_{i+1}, ..., b_{i+n-1}$, and the content of the third NFSR contains l bits denoted by $c_i, c_{i+1}, ..., c_{i+l-1}$. Let d_1, d_2, and d_3 be three integers satisfying $1 \leq d_1 < m$, $1 \leq d_2 < n$, and $1 \leq d_3 < l$. The feedback function of the first NFSR is $x_{d_1} + y_0 + f_1(y_1, y_2, ..., y_{l-1})$, the feedback function of the second NFSR is $x_{d_2} + y_0 + f_2(y_1, y_2, ..., y_{m-1})$, and the feedback function of the third NFSR is $x_{d_3} + y_0 + f_3(y_1, y_2, ..., y_{n-1})$. Then the sequences $\{a_i\}_{i=0}^{\infty}$,

$\{b_i\}_{i=0}^{\infty}$, and $\{c_i\}_{i=0}^{\infty}$ generated by the three NFSRs are defined by

$$a_{i+m} = a_{i+d_1} + c_i + f_1(c_{i+1}, c_{i+2}, ..., c_{i+l-1}),$$

$$b_{i+n} = b_{i+d_2} + a_i + f_2(a_{i+1}, a_{i+2}, ..., a_{i+m-1}),$$

$$c_{i+l} = c_{i+d_3} + b_i + f_3(b_{i+1}, b_{i+2}, ..., b_{i+n-1}),$$

for any $i \geq 0$.

4 Main Results

In this section, we keep all notations in Section 3.

4.1 The Grain-Like Structure

It is known that $\{s_i\}$ is periodic, and $\{b_i\}$ is ultimately periodic. Let T_0 denote the pre-period of $\{b_i\}$, and T denote the minimal period of $\{b_i\}$, i.e., $b_i = b_{i+T}$ for any $i \geq T_0$.

Theorem 1 *If $\{s_i\}$ is not the all-0 sequence, then $(2^n - 1)|T$.*

Proof. Because $b_{i+n} = b_{i+T+n}$ for any $i \geq T_0$, we have

$$\begin{aligned} s_i + b_i + g(b_{i+1}, b_{i+2}, ..., b_{i+m-1}) &= s_{i+T} + b_{i+T} + g(b_{i+T+1}, b_{i+T+2}, ..., b_{i+T+m-1}) \\ &= s_{i+T} + b_i + g(b_{i+1}, b_{i+2}, ..., b_{i+m-1}) \end{aligned}$$

holds for any $i \geq T_0$. Hence $s_i = s_{i+T}$ for any $i \geq T_0$ which means that $s_i = s_{i+T}$ for any $i \geq 0$. If $\{s_i\}$ is not the all-0 sequence, then the minimal period of $\{s_i\}$ is $2^n - 1$. Thus, $(2^n - 1)|T$. □

Theorem 2 *If $\{s_i\}$ is not the all-0 sequence, then $\{b_i\}$ is periodic.*

Proof. Suppose that $T_0 > 0$. Because $b_{T_0+n-1} = b_{T_0+n-1+T}$, we have

$$\begin{aligned} & s_{T_0-1} + b_{T_0-1} + g(b_{T_0}, b_{T_0+1}, ..., b_{T_0+m-2}) \\ &= s_{T_0-1+T} + b_{T_0-1+T} + g(b_{T_0+T}, b_{T_0+1+T}, ..., b_{T_0+m-2+T}) \\ &= s_{T_0-1+T} + b_{T_0-1+T} + g(b_{T_0}, b_{T_0+1}, ..., b_{T_0+m-2}) \end{aligned}$$

Thus, $s_{T_0-1} + b_{T_0-1} = s_{T_0-1+T} + b_{T_0-1+T}$. Since $(2^n - 1)|T$ by Theorem 1, we have $s_{T_0-1} = s_{T_0-1+T}$. It follows that $b_{T_0-1} = b_{T_0-1+T}$ which means that $b_i = b_{i+T}$ for any $i \geq T_0 - 1$. It is a contradiction. Hence $T_0 = 0$. □

Let $\mathbf{B}_t = (b_t, b_{t+1}, ..., b_{t+m-1})$ be the state of the NFSR at time t, and $\mathbf{S}_t = (s_t, s_{t+1}, ..., s_{t+n-1})$ be the state of the LFSR at time t, $t = 0, 1, \cdots$. Then $\mathbf{B}_0$ and $\mathbf{S}_0$ are the initial states of the NFSR and LFSR, respectively.

Theorem 3 *Let the initial state* $\mathbf{S}_0$ *of the LFSR be nonzero. If there exists an initial state* $\mathbf{B}_0 = (b_0, b_1, ..., b_{n-1})$ *of the NFSR such that the period of* $\{b_i\}$ *is* $(2^n - 1)d$*, then there exist* $d - 1$ *initial states* $\mathbf{B}_{2^n-1}, \mathbf{B}_{2(2^n-1)}, ..., \mathbf{B}_{(d-1)(2^n-1)}$ *other than* $\mathbf{B}_0$ *of the NFSR such that the period of the sequence generated by* $\mathbf{B}_{j(2^n-1)}$ *and* $\mathbf{S}_0$ *is also* $(2^n - 1)d$*, where* $0 < j < d$*.*

Proof. Because the period of $\{s_i\}$ is $2^n - 1$, we have $\mathbf{S}_{j(2^n-1)} = \mathbf{S}_0$ for any $0 < j < d$. The sequence generated by $\mathbf{B}_{j(2^n-1)}$ and $\mathbf{S}_{j(2^n-1)}$ is $\{b_{i+j(2^n-1)}\}$, the shift of $\{b_i\}$. Hence, there exist $d - 1$ initial states $\mathbf{B}_{2^n-1}, \mathbf{B}_{2(2^n-1)}, ..., \mathbf{B}_{(d-1)(2^n-1)}$ other than $\mathbf{B}_0$ of the NFSR such that the period of the sequence generated by $\mathbf{B}_{j(2^n-1)}$ and $\mathbf{S}_0$ is also $(2^n - 1)d$, where $0 < j < d$. □

For the distributions of periods of $\{b_i\}$, we provide two examples below.

Example 1. Both the contents of the LFSR and the NFSR contain 8 bits. The linear feedback is defined by $s_{i+8} = s_i + s_{i+2} + s_{i+3} + s_{i+4}, i \geq 8$. The nonlinear feedback $g(x_0, x_1, ..., x_7)$ is defined as $g(x_0, x_1, ..., x_7) = x_0 + x_1 + x_3 + x_5x_7 + x_5x_6 + x_4x_6x_7$, and the recursive relation is given by $b_{i+8} = s_i + g(b_i, ..., b_{i+7}), i \geq 8$. The distributions of periods of $\{b_i\}$ are listed in Table 1 in the case that the initial state of the LFSR is nonzero.

Table 1:

Period	Frequency
255×190	48450
255×26	6630
255×10	2550
255×9	2295
255×7	1785
255×5	1275
255×4	1020
255×2	1020
255×1	255

Example 2. Both the contents of the LFSR and the NFSR contain 8 bits. The linear feedback is defined by $s_{i+8} = s_i + s_{i+2} + s_{i+3} + s_{i+4}, i \geq 8$. The nonlinear feedback $g(x_0, x_1, ..., x_7)$ is defined as $g(x_0, x_1, ..., x_7) = x_0 + x_2 + x_6 + x_5x_7 + x_5x_6 + x_4x_6x_7$, and the recursive relation is given by $b_{i+8} = s_i + g(b_i, ..., b_{i+7}), i \geq 8$. The distributions of periods of $\{b_i\}$ are listed in Table 2 in the case that the initial state of the LFSR is nonzero.

Based on such examples, we propose the following open problem.

Table 2:

Period	Frequency
255×140	35700
255×40	10200
255×35	8925
255×33	8415
255×6	1530
255×2	510

Open Problem. For fixed feedback of the LFSR and the NFSR, determine the minimal period $2^n - 1$ of $\{b_i\}$ is achieveable or not. If achieveable, provide at least one pair of initial states $\mathbf{B}_0$ and $\mathbf{S}_0$ explicitly.

4.2 The Trivium-Like Structure

Lemma 1 *Let $\mathbf{s} = \{s_i\}$ be a sequence with least period N. For any integer $0 < d < N$, if $\gcd(d, N) = 1$, then the least period of $\{s_i + s_{i+d}\}$ is N.*

Proof. Let $f(x)$ be the minimal polynomial of $\mathbf{s}$, and T be the least period of $\{s_i + s_{i+d}\}$. Then $T|N$. For any $i \geq 0$, we have

$$s_i + s_{i+N} + s_{i+d} + s_{i+N+d} = 0$$

which means that $f(x)|(x^T+1)(x^d+1)$. The order of $(x^T+1)(x^d+1)$ is $\mathrm{lcm}(T, d)$. Hence $N|\mathrm{lcm}(T, d)$. Because $\gcd(d, N) = 1$, we get $N|T$. So $T = N$. □

Theorem 4 ([15]) *Let $N = 2^v n$ with $v \geq 0$ and $\gcd(n, 2) = 1$. Let $l_1, l_2, ..., l_s$ be the cardinalities of cyclotomic cosets modulo n. Then the expected value E_N of the linear complexity of random binary sequences of period N is given by*

$$E_N = N - \sum_{i=1}^{s} \frac{l_i(1 - 2^{-2^v l_i})}{2^{l_i} - 1}.$$

Lemma 2 *Let E_N be the expected value of the linear complexity of random binary sequences with period N. Then we have $E_N > 5N/6 - 1$ if N is even, and $E_N > 2N/3 - 1$ if N is odd.*

Proof. Let $N = 2^v n$ with $v \geq 0$ and $\gcd(n, 2) = 1$. Let $l_1, l_2, ..., l_s$ be the cardinalities of cyclotomic cosets modulo n. Assume that $l_1 \leq l_2 \leq ... \leq l_s$. Then $l_1 = 1$, and $l_2 > 1$. Thus, by Theorem 4, we

have

$$\begin{aligned} E_N &= N - \sum_{i=1}^{s} \frac{l_i(1-2^{-2^v l_i})}{2^{l_i}-1} > N - \sum_{i=1}^{s} \frac{l_i}{2^{l_i}-1} = N - 1 - \sum_{i=2}^{s} \frac{l_i}{2^{l_i}-1} \\ &> N - 1 - \frac{n-1}{3} > N - 1 - \frac{n}{3}. \end{aligned}$$

Thus, $E_N > 5N/6 - 1$ if N is even, and $E_N > 2N/3 - 1$ if N is odd. □

Lemma 3 ([1]) *Let $N = 2^v n$ with $v \geq 0$ and $\gcd(n, 2) = 1$. Let V_N be the variance of the linear complexity of random binary sequences with period N. Then we have $V_N < 2 + (d(n) - 1)\log_2(n + 1)$, where $d(n)$ is the number of positive divisors of n.*

Remark 1 *Because $d(n) < \log_2 n$, by Lemma 3, we have $V_N < 2 + (\log_2 n - 1)\log_2(n + 1) < 2 + (\log_2(n + 1))^2$.*

We will need the following Chebyshev's inequality later.

Lemma 4 *Let X be a random variable with expected value μ and finite variance σ^2. Then for any real number $k > 0$,*

$$Pr(|X - \mu| \geq k\sigma) \leq 1/k^2.$$

Lemma 5 *Let $N = 2^v n$ with $v \geq 0$ and $\gcd(n, 2) = 1$. Let $\mathbf{s} = \{s_i\}$ be a sequence with least period N. For any integer $0 < d < N$ satisfying $\gcd(d, N) > 1$, if $d < N/6$, then the least period of $\{s_i + s_{i+d}\}$ is N with probability $1 - \left(\frac{2+(\log_2(n+1))^2}{N/6-1}\right)^2$.*

Proof. Let $f(x)$ be the minimal polynomial of $\mathbf{s}$, and T be the least period of $\{s_i + s_{i+d}\}$. Similar to the proof of Lemma 1, we have $f(x)|(x^T + 1)(x^d + 1)$. Hence, $l(\mathbf{s}) = \deg(f) \leq T + d$. Suppose that $T < N$. Then $T \leq N/2$ for N even, and $T \leq N/3$ for N odd. It follows that $l(\mathbf{s}) \leq 2N/3$ for N even, and $l(\mathbf{s}) \leq N/2$ for N odd.

Let E_N be the expected value of the linear complexity of random binary sequences with period N. For the case of N even, by Lemmas 4, 3, and 4, the probability that $l(\mathbf{s}) \leq 2N/3$ satisfies

$$Pr(l(\mathbf{s}) \leq 2N/3) \leq Pr(|l(\mathbf{s}) - E_N| > N/6 - 1) < \left(\frac{2 + (\log_2(n + 1))^2}{N/6 - 1}\right)^2.$$

For the case of N odd, by Lemmas 4, 3, and 4, the probability that $l(\mathbf{s}) \leq N/2$ satisfies

$$Pr(l(\mathbf{s}) \leq N/2) \leq Pr(|l(\mathbf{s}) - E_N| > N/6 - 1) < \left(\frac{2 + (\log_2(n + 1))^2}{N/6 - 1}\right)^2.$$

□

Remark 2 *If N is large, then $1-\left(\frac{2+(\log_2(n+1))^2}{N/6-1}\right)^2$ is close to 1.*

It is known that $\{a_i\}$, $\{b_i\}$, and $\{c_i\}$ are ultimately periodic. Let T_1 be the least period of $\{a_i\}$, T_2 be the least period of $\{b_i\}$, and T_3 be the least period of $\{c_i\}$. Let T_0^1 be the pre-period of $\{a_i\}$, T_0^2 be the pre-period of $\{b_i\}$, and T_0^3 be the pre-period of $\{c_i\}$.

Assumption 1. $\{a_i\}$, $\{b_i\}$, and $\{c_i\}$ are distributed uniformly in the set of binary sequences with period T_1, T_2, and T_3 respectively.

Theorem 5 *With the notations as above, if $\min(T_1,T_2,T_3) > 6\max(m,n,l)$, then $T_1 = T_2 = T_3$ with high probability under Assumption 1.*

Proof. For any $i \geq T_0^3$, we have

$$\begin{aligned} a_{i+m}+a_{i+T_3+m} &= a_{i+d_1}+c_i+f_1(c_{i+1},c_{i+2},...,c_{i+l-1}) \\ &\quad +a_{i+T_3+d_1}+c_{i+T_3}+f_1(c_{i+T_3+1},c_{i+T_3+2},...,c_{i+T_3+l-1}) \\ &= a_{i+d_1}+a_{i+T_3+d_1}. \end{aligned}$$

Hence, if the least period of $\{a_{i+m}+a_{i+d_1}\}$ is equal to the least period of $\{a_i\}$, then $T_1|T_3$. Similarly, if the least period of $\{b_{i+n}+b_{i+d_2}\}$ is T_2, then $T_2|T_1$, and if the least period of $\{c_{i+l}+c_{i+d_3}\}$ is T_3, then $T_3|T_2$. Hence, under these assumptions, $T_1 = T_2 = T_3$.

By Lemmas 1, 5 and Assumption 1, with high probability, the least period of $\{a_{i+m}+a_{i+d_1}\}$ is T_1, the least period of $\{b_{i+n}+b_{i+d_2}\}$ is T_2, and the least period of $\{c_{i+l}+c_{i+d_3}\}$ is T_3. Hence, with high probability, we have $T_1 = T_2 = T_3$. □

Theorem 6 *With the notation as above, if $T_1 = T_2 = T_3$, then $T_0^1 = T_0^2 = T_0^3 = 0$.*

Proof. Let $T = T_1 = T_2 = T_3$. Without loss of generality, we may assume that $T_0^3 = \max(T_0^1, T_0^2, T_0^3)$. Suppose that $T_0^3 > 0$. Because $a_{T_0^3-1+m} = a_{T+T_0^3-1+m}$ and $d_1 \geq 1$, we have

$$\begin{aligned} & a_{T_0^3-1+d_1}+c_{T_0^3-1}+f_1(c_{T_0^3},c_{T_0^3+1},...,c_{T_0^3+l-2}) \\ &= a_{T+T_0^3-1+d_1}+c_{T+T_0^3-1}+f_1(c_{T+T_0^3},c_{T+T_0^3+1},...,c_{T+T_0^3+l-2}) \\ &= a_{T_0^3-1+d_1}+c_{T+T_0^3-1}+f_1(c_{T_0^3},c_{T_0^3+1},...,c_{T_0^3+l-2}). \end{aligned}$$

Hence $c_{T_0^3-1} = c_{T+T_0^3-1}$ which means that $c_i = c_{i+T}$ for any $i \geq T_0^3 - 1$. It is a contradiction. Hence $T_0^1 = T_0^2 = T_0^3 = 0$. □

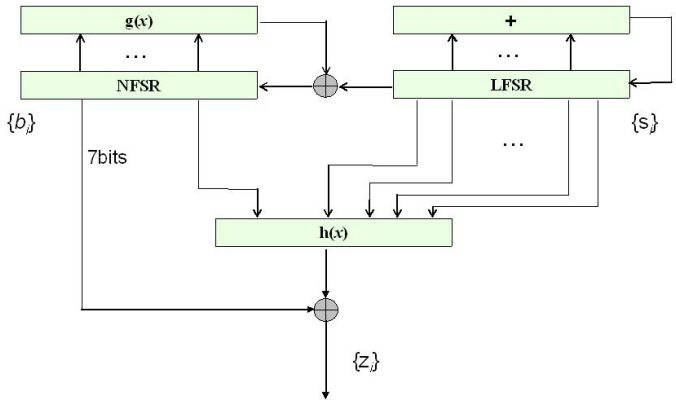

Figure 3: Grain

5 Periods of Grain and Trivium

5.1 Grain

Both of the contents of the registers deployed in Grain contain 80 bits. The content of the LFSR is denoted by $s_i, s_{i+1}, ..., s_{i+79}$, and the content of the NFSR is denoted by $b_i, b_{i+1}, ..., b_{i+79}$. The feedback polynomial for the LFSR is defined by

$$f(x) = 1 + x^{18} + x^{29} + x^{42} + x^{57} + x^{67} + x^{80}$$

which means that $s_{i+80} = s_{i+62} + s_{i+51} + s_{i+38} + s_{i+23} + s_{i+13} + s_i$ for any $i \geq 0$. The feedback polynomial for the NFSR is given by

$$\begin{aligned} g(x) \quad = \quad & 1 + x^{18} + x^{20} + x^{28} + x^{35} + x^{43} + x^{47} + x^{52} + x^{59} + x^{66} + x^{71} + x^{80} + \\ & + x^{17}x^{20} + x^{43}x^{47} + x^{65}x^{71} + x^{20}x^{28}x^{35} + x^{47}x^{52}x^{59} + x^{17}x^{35}x^{52}x^{71} + \\ & + x^{20}x^{28}x^{43}x^{47} + x^{17}x^{20}x^{59}x^{65} + x^{17}x^{20}x^{28}x^{35}x^{43} + x^{47}x^{52}x^{59}x^{65}x^{71} + \\ & + x^{28}x^{35}x^{43}x^{47}x^{52}x^{59}. \end{aligned}$$

For any $i \geq 0$, b_{i+80} is given by

$$\begin{aligned} b_{i+80} \quad = \quad & s_i + b_i + b_{i+62} + b_{i+60} + b_{i+52} + b_{i+45} + b_{i+37} + b_{i+33} + b_{i+28} + \\ & + b_{i+21} + b_{i+14} + b_{i+9} + b_{i+63}b_{i+60} + b_{i+33}b_{i+37} + b_{i+9}b_{i+15} + \\ & + b_{i+45}b_{i+52}b_{i+60} + b_{i+21}b_{i+28}b_{i+33} + b_{i+9}b_{i+28}b_{i+45}b_{i+63} + \\ & + b_{i+33}b_{i+37}b_{i+52}b_{i+60} + b_{i+15}b_{i+21}b_{i+60}b_{i+63} + \\ & + b_{i+37}b_{i+45}b_{i+52}b_{i+60}b_{i+63} + b_{i+9}b_{i+15}b_{i+21}b_{i+28}b_{i+33} + \\ & + b_{i+21}b_{i+28}b_{i+33}b_{i+37}b_{i+45}b_{i+52}. \end{aligned}$$

The filtering function is defined by

$$h(x_0, x_1, x_2, x_3, x_4) = x_1 + x_4 + x_0x_3 + x_2x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4.$$

Among the input of the filtering function, four bits are from the LFSR, and one bit is from the NFSR. Finally, the keystream is given by

$$z_i = b_{i+1} + b_{i+2} + b_{i+4} + b_{i+10} + b_{i+31} + b_{i+43} + b_{i+56} + h(s_{i+3}, s_{i+25}, s_{i+46}, s_{i+64}, b_{i+63}).$$

By Theorems 1 and 2, we have the following results.

Corollary 1 *If the initial state of the LFSR is nonzero, then the sequence $\{b_i\}$ generated by the NFSR is periodic, and the period is a multiple of $2^{80} - 1$.*

Corollary 2 *The key stream generated by Grain is periodic.*

The following conjecture seems not easy to prove because we only know the information about the least period of $\{b_i\}$.

Conjecture 1 *The least period of the key stream generated by Grain is equal to the least period of $\{b_i\}$.*

5.2 Trivium

The contents of registers deployed in Trivium contain 93 bits, 84 bits, and 111 bits, respectively. We denote the content of the first register by $a_i, a_{i+1}, ..., a_{i+92}$, the content of the second register by $b_i, b_{i+1}, ..., b_{i+83}$, and the content of the third register by $c_i, c_{i+1}, ..., b_{i+110}$. Let $\{z_i\}$ denote the key stream generated by Trivium.

In each step of the key stream generation, 15 specific state bits are used to update 3 bits of the state and to compute 1 bit of key stream z_i. The output of Trivium is given by

$$z_i = a_i + a_{i+27} + b_i + b_{i+15} + c_i + c_{i+45}, i = 0, 1, \cdots .$$

The updating functions of three NFSRs are given as follows.

$$\begin{aligned} a_{i+93} &= a_{i+24} + c_i + c_{i+45} + c_{i+1}c_{i+2}, i \geq 0 \\ b_{i+84} &= b_{i+6} + a_i + a_{i+27} + a_{i+1}a_{i+2}, i \geq 0 \\ c_{i+111} &= c_{i+24} + b_i + b_{i+15} + b_{i+1}b_{i+2}, i \geq 0 \end{aligned} \tag{1}$$

Using the notation in Section 3.2, the parameters of Trivium are given in the following table.

$m = 93$	$n = 84$	$l = 111$
$d_1 = 24$	$d_2 = 6$	$d_3 = 24$
$f_1(x_1, \cdots, x_{92}) = x_{45} + x_1x_2$	$f_2(x_1, \cdots, x_{83}) = x_{27} + x_1x_2$	$f_3(x_1, \cdots, x_{110}) = x_{15} + x_1x_2$

Let T_1 be the minimal period of $\{a_i\}$, T_2 be the minimal period of $\{b_i\}$, and T_3 be the minimal period of $\{c_i\}$. By Theorems 5 and 6, we have the following results.

Corollary 3 *With the notations as above,*

$$T_1 = T_2 = T_3$$

holds with high probability under Assumption 1.

Corollary 4 *With the notations as above, the key stream generated by Trivium is periodic with high probability.*

6 Conclusion

NFSR sequences are more resistant to cryptanalytic attacks than LFSR sequences, but the construction of NFSR sequences with guaranteed long periods is an open problem. We study two kinds of NFSRs with time varying feedback functions, namely, Grain-like and Trivium-like structures. Some interesting results regarding their periods are obtained. Hopefully, the study of general NFSRs may benefit from such results.

Acknowledgement

The authors would like to thank all who did the course project in [4]. This research is supported by NSERC Discovery and DAS Grant.

References

[1] F. Fu, H. Niederreiter, and M. Su, The expectation and variance of the joint linear complexity of random periodic multisequences, J. Com- plex., vol. 21, no. 6, pp. 804-822, Dec. 2005.

[2] S. Golomb, *Shift Register Sequences*, Oakland, CA: Holden-Day, 1967. Revised edition: Laguna Hills, CA: Aegean Park Press, 1982.

[3] S. W. Golomb and G. Gong, *Signal Designs With Good Correlation: For Wireless Communications, Cryptography and Radar Applications*. Cambridge, U.K.: Cambridge University Press, 2005.

[4] G. Gong, Course Project in ECE 710 Topic 4: Sequence Design and Cryptography, Class 2008 and 2009, University of Waterloo, 2008.

[5] M. Hell, T. Johansson, and W. Meier, Grain-a stream cipher for constrained environments, eSTREAM portfolio at http://www.ecrypt.eu.org/stream/grainp3.html.

[6] C. De Cannière and B. Preneel, Trivium specifications, eSTREAM portfolio at http://www.ecrypt.eu.org/stream/triviump3.html

[7] X. Lai, Condition for the nonsingularity of a feedback shift-register over a general finite field, IEEE Transactions on Information Theory, vol. 33, pp. 747-749, Sep. 1987.

[8] E. Barkan, E. Biham, and N. Keller, Instant ciphertext-only cryptanalysis of GSM encrypted communication, J. Cryptology, vol. 21, no. 3, pp. 392-429, 2008.

[9] P. Ekdahl and T. Johansson, Another attack on A5/1, IEEE Transactions on Information Theory, vol. 49, pp. 1-7, 2003.

[10] Y. Lu and S. Vaudenay, Cryptanalysis of an E0-like combiner with memory, *J. Cryptol.*, vol. 21(3), pp. 430-457, 2008.

[11] Y. Lu, W. Meier, and S. Vaudenay, The conditional correlation attack: a practical attack on Bluetooth encryption, in Advances in Cryptology-CRYPTO 2005, Lecture Notes in Computer Science, vol. 3621, pp. 97-117, Springer, Berlin, 2005.

[12] Y. Lu and S. Vaudenay, Cryptanalysis of Bluetooth keystream generator two-level E0, in Advances in Cryptology-ASIACRYPT 2004, Lecture Notes in Computer Science, vol. 3329, pp. 483-499, Springer, Berlin, 2004.

[13] Y. Lu and S. Vaudenay, Faster correlation attack on Bluetooth keystream generator E0, in Advances in Cryptology-CRYPTO 2004, Lecture Notes in Computer Science, vol. 3152, pp. 407-425, Springer, Berlin, 2004.

[14] I. Mantin and A. Shamir, A practical attack on broadcast RC4, in Proceedings of Fast Software Encryption-FSE01 (M. Matsui, ed.), no. 2355 in Lecture Notes in Computer Science, pp. 152-164, Springer-Verlag, 2001.

[15] W. Meidl and H. Niederreiter, On the expected value of the linear complexity and the k-error linear complexity of periodic sequences, *IEEE Trans. Inform. Theory*, vol. 48, pp. 2817-2825, 2002.

[16] J. L. Massey, Shift-register synthesis and BCH decoding, *IEEE Trans. Information Theory*, Vol. 15, No. 1, pp. 122-127, January 1969.