Chaos, Solitons and Fractals 109 (2018) 36–40

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

journal homepage: www.elsevier.com/locate/chaos

A novel method for reconstructing period with single input in NFSR

Bo Gao[a,*], Xuan Liu[a], Zhongzhou Lan[a], Rongrong Fu[b]

[a] *School of Computer Information management, Inner Mongolia University of Finance and Economics, China*
[b] *China Academy of Information and Communication Technology, China*

ARTICLE INFO

Article history:
Received 24 November 2017
Revised 5 January 2018
Accepted 8 January 2018

Keywords:
Non-Linear Feedback Shift Registers (NFSR)
Single input
Semi-tensor product (STP)
Period
Reconstruction
Boolean network (BN)

ABSTRACT

Non-Linear Feedback Shift Registers (NFSRs) are a generalization of Liner Feedback Shift Registers (LFSRs). The study of NFSR sequence helps to analyze the cryptographical security of NFSR-based stream cipher. Due to lack of efficient algebraic tools, the period of NFSR still remains an open crucial theoretical problem. In this paper, we view the NFSR as a Boolean network (BN), so that the study about the period of NFSR can be viewed as the study about period of BN. Furthermore, based on the mathematical tool of semi-tensor product (STP), a Boolean network can be mapped into an algebraic form. For these, we put forward a method for reconstructing the period of NFSR with single input. Especially, we propose a procedure to choose the controlled states and steer the controlled states from initial state to desirable one. At last, the general derivation is exemplified by numerical simulations for a kind of NFSR.

1. Introduction

Non-Linear Feedback Shift Registers (NFSRs) are a generalization of Liner Feedback Shift Registers (LFSRs) [1]. There exist lots of well-developed theories on LFSRs, while many fundamental problems related to NFSRs still remain to be further explored [2–6]. Since lack of efficient analysis tools, the theory of NFSRs has yet to be well-understood. At present, NFSRs not only have been applied in coder and decoder, but also have been widely used in stream ciphers. With the increas ng resistance to cryptanalysis attacks, cascaded connection of NFSRs, those controlling NFSRs cascade with their controlled NFSRs by means of their outputs, are more adopted in recently developed ciphers, for instance, Grain [7], Trivium [8] and Mickey [9]. This implies the outputs of controlling NFSRs are the inputs of their controlled NFSRs. In order to analyze the cryptographical security of NFSR-based stream cipher, the periods of controlled NFSR must be considered [10].

There are two major kinds of NFSRs are generally classified as autonomous NFSRs (without input) and non-autonomous NFSRs(with inputs). In recent years, autonomous NFSR and non-autonomous NFSR are especially regarded as a Boolean network [11–14]. A Boolean network which consists of Boolean functions is an autonomous system that evolves as a finite set of states. The Boolean network in order to describe a network whose variables only includes two kinds of values, “1” and “0” [15]. The behaviors of Boolean network rely on its internal structure. But when a Boolean network includes some external force, called input (control), then the concept is naturally extended to a Boolean control network. Recently, a large amount of attention has been paid in Boolean (control) network, such as physics [16–18] to system science [19–26]. In this research area, Cheng and his team put forward an algebraic framework for the Boolean (control) network, by mean of semi-tensor product (STP) [27]. Base on their contributions, the NFSR is transformed into a Boolean network, which is very useful to analyze the NFSRs.

On the basis of clear and strict evidence, we design a method to reconstruct the period of NFSR with single input. To do so, we need three steps. Firstly, with the purpose of adjusting the trajectory in period of NFSR, we provide a way to choose the controlled nodes. Secondly, we will provide a method to choose two pairs of special states, which can be reachable to each other. Finally, an algorithm is provided to design the controlled path between the dual states and the new period can be constructed.

The paper is organized as follows. Some theoretical backgrounds are reviewed in Section 2. Section 3 introduces the main results of this paper. In this section, a method is design to reconstruct the period with single input in NFSR, and the formula deduction is also presented. In Section 4, we conduct some simulations to illustrate the efficiency of the results. Section 5 is a short conclusion.

2. Preliminaries

Some background theories are reviewed in this section.

[*] Corresponding author.
E-mail address: gaobo@imufe.edu.cn (B. Gao).

https://doi.org/10.1016/j.chaos.2018.01.012
0960-0779/© 2018 Elsevier Ltd. All rights reserved.

Definition 2.1. Assume that M and N are matrices of dimensions $a \times b$ and $c \times d$. Let k be the least common multiple of b and c. The STP of M and N is defined as:

$$M \ltimes N := (M \otimes I_{k/b})(N \otimes I_{k/c}) \tag{2.1}$$

where $\otimes$ is the Kronecker product.

Since STP is a general form of the classical matrix product, we will omit the symbol "$\ltimes$" in the sequel unless there exist special needs . Though the mathematical tool STP, we can transfer a logical function to an algebraic form.

Lemma 2.2. *Given a logical function $g(x_1, x_2, \dots, x_n)$, there will exist a unique structure matrix M of the logical function, such that:*

$$g(x_1, x_2, \dots, x_n) = Mx_1x_2 \dots x_n \tag{2.2}$$

Definition 2.3. The feedback function of n-stag Fibonacci NFSR can be expressed as follows:

$$\begin{cases} x_1(t+1) = x_2(t) \\ x_2(t+1) = x_3(t) \\ \dots \\ x_{n-1}(t+1) = x_n(t) \\ x_n(t+1) = g(x_1(t), x_2(t), \dots, x_n(t)) \end{cases} \tag{2.3}$$

where $x_i(t)$ is the state of the ith register of NFSR, for $i = 1, 2, \dots, n$. And g is the Boolean function.

3. Main results

3.1. Reachable set of state

NFSR is viewed as a Boolean network. According the properties of STP, a Boolean function f with n variables can be mapped to an algebraic form. We will use the equations to describe the state of the NFSR as follows.

An n-stage feedback function of NFSR can be expressed as a BN with n nodes:

$$x_i(t+1) = g_i(x_1(t), x_2(t), \dots, x_n(t)), \text{for } \ i = 1, 2, \dots, n \tag{3.1}$$

where $x_i \in \mathcal{D}$ are logical variables of NFSR states in the time t, and f_i: $\mathcal{D}^n \to \mathcal{D}$ are logical functions. Additionally, $\mathcal{D}$ is the set of elements of δ_2^1 and δ_2^2. δ_n^i is the ith column of the identity matrix of dimension n. And $\mathcal{D}^n$ is the set of all n-dimensional vectors over $\mathcal{D}$.

Then denote by the structure matrix M_i, a 2×2^n matrix, which corresponds to the node x_i. By using Lemma 2.2, Eq. (3.1) can be represented as

$$x_i(t+1) = M_i x_1(t) \dots x_n(t) = M_i x(t) \tag{3.2}$$

Define $x(t) = \ltimes_{i=1}^n x_i(t)$, then Eq. (3.2) can be further represented as

$$x(t+1) = M_1 x(t) M_2 x(t) \dots M_n x(t) := Lx(t) \tag{3.3}$$

where L is the transition matrix of Eq. (3.1), which is a $2^n \times 2^n$ matrix composed by $\delta_{2^n}^{i_k}$, $1 \le i_k \le 2^n$, the matrix $L = [\delta_{2^n}^{i_1}, \delta_{2^n}^{i_2}, \dots, \delta_{2^n}^{i_{2^n}}]$. To simply, we rewrite L in a form as $L = \delta_{2^n}[i_1, i_2, \dots, i_{2^n}]$. We can calculate the transition matrix L by $Col_i(L) = \ltimes_{j=1}^n Col_i(M_j)$. The transition matrix is used to reflect the transition of the state of the NFSR. If the ith column of the transition matrix L is $\delta_{2^n}^j$, which means the subsequent state of ith state is jth state.

Suppose that Eq. (3.1) with single input will represent as

$$x_i(t+1) = G_i(u(t), x(t), \dots, x_n(t)), fori = 1, 2, \dots n \tag{3.4}$$

where G_i are logical functions, $i = i_1, i_2, \dots, i_j$. The $u(t) \in \Delta_2$ is the single input free Boolean sequence control, Δ_a is the set of all δ_b^a, $a = 1, 2, \dots b$. The i is the node to be controlled, $i = i_1, i_2, \dots, i_j$.

Denote by M_i' the structure matrix of g_i with single input, then the Eq. (3.4) is performed as

$$x_i(t+1) = M_i' u(t) x_1(t) \dots x_n(t) = M_i' u(t) x(t) \tag{3.5}$$

where $M_i' = [M_i | 1 - M_i]$ (with control) or $M_i' = [M_i | M_i]$ (without control).

Similar to the form of Eq. (3.3), Define $x(t) = \ltimes_{i=1}^n x_i(t)$, Eq. (3.5) can be further performed as

$$x(t+1) = M_1' x(t) \dots M_i' u(t) x(t) \dots M_n' x(t) := L' u(t) x(t) \tag{3.6}$$

where L' is the transition matrix of Eq. (3.2) with single input. And L' is a $2^n \times 2^{n+1}$ matrix composed by $\delta_{2^n}^{i_k}$, $1 \le i_k \le 2^n$. We can calculate the transition matrix L' by $Col_i(L') = \ltimes_{k=1}^n Col_i(M_i')$.

Then consider the state of NFSR. Given an initial state s_0 and a desirable state s_0' in the period of Eq. (3.1), where $(s_0, s_0') \in L$ are stable states. Next, we will discuss the reachable set of state in NFSR, which is very useful to steer the initial state to the desirable one.

Definition 3.1.1. Define R_{s_0} as the reachable state set from s_0 at the kth step under control u, if and only if

$$R_{s_0} = Col\{(L')^k s_0\} \tag{3.7}$$

And let $R_{s_0}^*$ is the largest reachable state set of $s_{0,}$ if and only if

$$R_{s_0}^* = Col\left\{\bigcup\nolimits_{i=1}^{\infty} (L')^i s_0\right\} \tag{3.8}$$

Furthermore, if the $k* > 0$ is the smallest number such that $Col\{(L')^{k+1} s_0\} \subset Col\{(L')^r s_0 | r = 1, 2, \dots, k\}$. Then the largest reachable set is

$$R_{s_0}^* = Col\left\{\bigcup\nolimits_{i=1}^{k^*} (L')^i s_0\right\}. \tag{3.9}$$

Next, we will discuss the reachability from one state to another one.

Definition 3.1.2. The transition from s_0 to s_0' is reachable at the kth step, if and only if

$$(L')^k s_0 \cap s_0' \neq \phi \tag{3.10}$$

where ϕ is the null set. Otherwise, the transition from s_0 to s_0' is not reachable at the kth step, if and only if

$$(L')^k s_0 \cap s_0' {=} \phi \tag{3.11}$$

Assume that $Col_r(L) \neq s_0'$, and calculate $R(s_0)$. If $s_0' \in R(s_0)$, then we can choose the node x_i as the pining node to steer trajectory from the state s_0 to the state s_0'. The results are summarized in Algorithm 3.1.3.

Algorithm 3.1.3: Step 1: Assume that $i \in \{i_1, i_2, \dots, i_j\}$ is the node to be controlled, take

$$M_i' := [M_i | 1 - M_i] \tag{3.12}$$

And

$$M_l' := [M_l | M_l], forl \neq i \tag{3.13}$$

Step 2: Calculate L', where $Col_i(L') = \ltimes_{k=1}^n Col_i(M_i')$.

Step 3: Calculate $R(s_0)$, $R(s_0) = Col\{(L')^k s_0\}$. If $s_0' \in R(s_0)$, then we choose the node x_i as the pining node.

By using Algorithm 3.1.3, s_0' is reachable from s_0.

3.2. Single-input controller design

As is shown in the Definition 2.3, only the last register of Fibonacci NFSR can accept the feedback of other registers. Through the Algorithm 3.1.3, we can illustrate whether the last node x_n can be choose as the pining node in the feedback function of NFSR.