SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •
Special Focus on Analysis and Control of Finite-Valued Network Systems

January 2018, Vol. 61 010204:1–010204:12
https://doi.org/10.1007/s11432-017-9269-6

Nonsingularity of Grain-like cascade FSRs via semi-tensor product

Jianquan LU[1,2*], Meilin LI[1], Yang LIU[2], Daniel W.C. HO[3] & Jürgen KURTHS[4]

[1] *School of Mathematics, Southeast University, Nanjing* 210096*, China;*
[2] *College of Mathematics, Physics and Information Engineering, Zhejiang Normal University, Jinhua* 321004*, China;*
[3] *Department of Mathematics, City University of Hong Kong, Hong Kong, China;*
[4] *Potsdam Institute for Climate Impact Research, Potsdam* 14415*, Germany*

Received 7 September 2017/Accepted 17 October 2017/Published online 12 December 2017

Abstract In this paper, Grain-like cascade feedback shift registers (FSRs) are regarded as two Boolean networks (BNs), and the semi-tensor product (STP) of the matrices is used to convert the Grain-like cascade FSRs into an equivalent linear equation. Based on the STP, a novel method is proposed herein to investigate the nonsingularity of Grain-like cascade FSRs. First, we investigate the property of the state transition matrix of Grain-like cascade FSRs. We then propose their sufficient and necessary nonsingularity condition. Next, we regard the Grain-like cascade FSRs as Boolean control networks (BCNs) and further provide a sufficient condition of their nonsingularity. Finally, two examples are provided to illustrate the results obtained in this paper.

Keywords Grain-like cascade FSRs, Boolean control networks, Boolean networks, semi-tensor product, nonsingularity

Citation Lu J Q, Li M L, Liu Y, et al. Nonsingularity of Grain-like cascade FSRs via semi-tensor product. Sci China Inf Sci, 2018, 61(1): 010204, https://doi.org/10.1007/s11432-017-9269-6

1 Introduction

Pseudo-random sequences as a signal form with good correlation properties have been widely used for many applications, such as secure communication, delay measurements and spread spectrum communication generators. A linear feedback shift register (LFSR) is one of the most popular configurations for generating pseudo-random sequences [1–3], where its current state is determined through a linear function with respect to its previous states. The output sequences of LFSR possess good cryptographic properties, and hence many stream cipher algorithms are composed of an LFSR or nonlinear feedback shift register (NLFSR). In an NLFSR, its feedback function is nonlinear. Li et al. [4] investigated certain properties about LFSR. The advantages of an LFSR are its fast speed, easy and simple implementation in hardware and software, and it's ability to generate random sequences with the same statistical distribution of 0's and 1's [2]. Nevertheless, An LFSR is not safe to apply in a stream cipher. Inspecting $2n$ consecutive bits of the output sequence can allow the structure of a n-bit LFSR to be determined [5].

To solve this problem, NLFSR was proposed in [2], the feedback functions of which are nonlinear Boolean functions. Owing to the complicated structures of NLFSR, its output sequences are extremely difficult to deduce through a cryptanalytic method, such as a correlation attack [6]. Many different methods have been proposed for the design of an NLFSR-based stream ciphers [7–10].

[*] Corresponding author (email: jqluma@seu.edu.cn)

Owing to the linearity between the output signal of an LFSR, many attack methods based on the structure of an LFSR have been developed, including fast correlation attacks [6] or an algebraic attack [11]. These attack methods have encouraged the discovery of a new stream cipher structure. The Trivium algorithm [12], Grain algorithm [13], and Mickey algorithm [14] are the final hardware-oriented stream ciphers of the eSTREAM project. These three algorithms are all based on NLFSR. At present, the NLFSR-based algorithm design has gradually developed into an important method of stream cipher design.

The Grain-like algorithm [15] and Trivium-like algorithm are typical algorithms of a stream cipher based on NLFSR. Grain-like cascade FSRs contain an LFSR and an NLFSR, where the output of the LFSR is regarded as the input of the NLFSR which proposed a typically method to design the structure of stream cipher. Berbain et al. [16] studied algebraic and correlation attacks against Grain-like cascade FSRs. Hu et al. [17] investigated the period of Grain-like and Trivium-like cascade FSRs.

Recently, a new mathematical tool for a matrix calculation called semi-tensor product (STP) of matrices was proposed by Cheng and his colleagues [18]. This STP method has been widely used to study Boolean networks (BNs) [19, 20]. Lu et al. [21] studied the controllability of delayed Boolean control networks (BCNs) based on STP method. The STP method was used to analyze the controllability of a BCN with impulsive effects and forbidden states [22]. Using STP, the pinning controllability problem, synchronization problem, stabilization problem, observability problem, and feedback control and output tracking control problems of BCNs have been investigated [23–31]. Based on STP method, the stability of a BN was studied [32]. The controllability problem of a BN was investigated [33,34]. Li and Wang [33] developed a novel constrained controllability matrix approach, which is very interesting and efficient, to study the controllability of Boolean networks with constraints. In [35], the STP method was used to study problems of game theory. In [36], the STP method was applied to the robust control of BCNs. The STP tool has also been successfully applied to the Fibonacci NLFSR [37–39]. The STP method was applied to global robust stability and stabilization of BN in [40]. Up to now, some interesting results about Fibonacci NLFSR have been obtained by using STP. In [41], the STP method was used on the sampled-data state feedback stabilization of BCNs. Zhong et al. [34] investigated the controllability and synchronization of identical-hierarchy mixed-valued logical control networks. Motivated by the above discussions, the STP method was applied in the present study with regard to the nonsingularity of Grain-like cascade FSRs.

The nonsingularity of an NLFSR is the basic requirement for the design of a stream cipher. If an NLFSR is singular, then there must exist two different states producing the same subsequence state, and hence, equivalent secret keys probably exist. If the NFSR is singular, it might encounter a differential attack [42]. Hence, when we design a stream cipher algorithm, to avoid potential security problems, we should ensure the nonsingularity of an NLFSR. The FSRs are said to be nonsingular if its state transition graph contains only cycles [43]. In [43, 44], the nonsingularity of Grain-like cascade FSRs is investigated by an algebraic method, but the author only gave some certain conditions to determine whether FSR are nonsingular. It is necessary to investigate how to find a control input such that an NLFSR with input is nonsingular. In this paper, we regard Grain-like cascade FSRs as BNs. We then investigate the properties of the state transition matrix of Grain-like cascade FSRs by using the STP of matrices. We found that the nonsingularity of Grain-like cascade FSRs is equivalent with the nonsingularity of the state transition matrix. We thus regard Grain-like cascade FSRs as an NLFSR with an input. We thus propose an algorithm to find an input sequence which can make the NLFSR with an input be nonsingular. Finally, the sufficient and necessary condition to judge the nonsingularity of Grain-like cascade FSRs is provided. The contributions of this paper is listed in the following.

(1) A sufficient and neccessary condition is given to judge the nonsingularity of Grain-like cascade FSRs.

(2) The Grain-like cascade FSRs is generalized into BCN, then propose an algorithm to find an input sequence such that the BCN is nonsingular.

(3) Some useful properties of state transition matrix of Grain-like cascade FSRs are given.

The remainder of this paper is organized as follows. Section 2 provides some preliminaries on STP and Grain-like cascade FSRs. In Section 3, Grain-like cascade FSRs are firstly turned into a linear equation.

The properties of the state transition matrix of the linear equation are investigated. Finally, a sufficient and necessary condition is proposed for the nonsingularity. In Section 4, two examples are given to illustrate our theoretical results. Finally, our conclusion is given.

2 Preliminaries

In this section, some knowledge regarding an STP is first reviewed for reference. We then describe obtained the algebraic expressions of Grain-like cascade FSRs. Using STP, multi-linear form of Grain-like cascade FSRs are yield. We provide some of the notations used in this paper.

- $\mathcal{D} = \{0, 1\}$.
- I_n : identity matrix of dimension n.
- $\delta_{2^n}^i$: i-th column of identity matrix I_n.
- $\Delta_{2^n} = \{\delta_{2^n}^i | i = 1, 2, 3, \dots, 2^n\}$.
- $\mathcal{L}_{n\times m}$: set of $n \times m$ matrices, whose columns belong to Δ_n. For the matrix $L \in (L)_{n\times m}$, where $L = [\delta_n^{i_1}\ \delta_n^{i_2}\ \cdots\ \delta_n^{i_m}]$, we write $L = \delta_{2^n}[i_1\ i_2\ \cdots\ i_m]$ for simplicity.
- $\mathrm{col}_i(L)$: i-th column of matrix L.
- $\mathrm{col}(L)$: set of all columns of matrix L.
- $\mathbb{R}$: set of all real number.
- $|S|$: base of set S.
- $\mathbb{N}$: the set of all integers.
- $\oplus$: modulo 2 addition.
- $\mathrm{GF}(q)$: Galois field of q elements.
- mod : modulo 2 division.
- $A\backslash B$: the set of $\{x | x \in A, x \notin B\}$.

2.1 Semi-tensor product of matrices

In this subsection, we provide the definition of the STP of the matrices and some STP properties.

Definition 1 ([18]). Let $A \in \mathbb{R}^{n\times m}$, $B \in \mathbb{R}^{p\times q}$. The semi-tensor product of A and B is defined as

$$A \ltimes B = (A \otimes I_{\frac{l}{m}})(B \otimes I_{\frac{l}{p}}), \tag{1}$$

where l is the least common multiple of m and p.

Clearly, if $m = p$ in Definition 1, then the STP of A and B is reduced to the conventional matrix product AB.

We identify $\Delta_2 \sim \mathcal{D}$, i.e. $(\delta_2^1 \sim 1, \delta_2^2 \sim 0)$, and $\delta_2^1(\delta_2^2)$ is called the vector form of the logical value 1(0).

Lemma 1 ([18]). Any Boolean function $f(x_1, x_2, \dots, x_n)$ with variables $x_1, x_2, \dots, x_n \in \Delta_2$ can be expressed as a multi-linear form:

$$f(x_1, x_2, \dots, x_n) = Fx_1 \ltimes x_2 \ltimes \cdots \ltimes x_n, \tag{2}$$

where $F \in \mathcal{L}_{2\times 2^n}$ is called the structure matrix of f, and F can be uniquely expressed as

$$F = \begin{bmatrix} s_1 & s_2 & \cdots & s_{2^n} \\ 1 - s_1 & 1 - s_2 & \cdots & 1 - s_{2^n} \end{bmatrix} \tag{3}$$

with $[s_1, s_2, \dots, s_{2^n}]$ being the truth table of f, arranged in reverse alphabetical order.

In the following, we omit the $\ltimes$ symbol for simplicity.

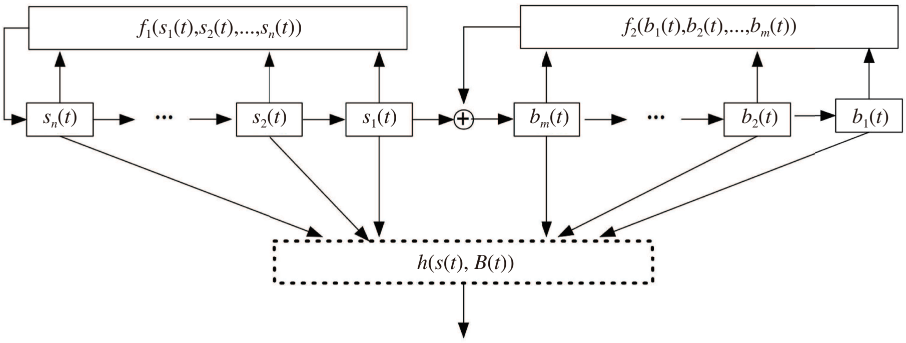
$f_1(s_1(t),s_2(t),\ldots,s_n(t))$
$f_2(b_1(t),b_2(t),\ldots,b_m(t))$
$s_n(t)$
$s_2(t)$
$s_1(t)$
$b_m(t)$
$b_2(t)$
$b_1(t)$
$h(s(t), B(t))$

Figure 1 Grain-like cascade FSRs.

2.2 Grain-like cascade feedback shift register

In Grain-like cascade FSRs, one LFSR is used to control another NLFSR (see Figure 1). In this paper, we only investigate the Grain-like cascade FSRs on GF(2). The results can be generalized to the case for GF(q).

Suppose that the content of the LFSR in Figure 1 contains n bits denoted by $s_1(t), s_2(t), \ldots, s_n(t)$ at time t, and that the content of the NLFSR in Figure 1 contains m bits denoted by $b_1(t), b_2(t), \ldots, b_m(t)$ at time t. The feedback function of the LFSR is $f_1(s_1(t), s_2(t), \ldots, s_n(t))$, and the feedback function of NLFSR is $f_2(b_1(t), b_2(t), \ldots, b_m(t))$. The state of the LFSR at time t is denoted by $s(t) = (s_1(t), s_2(t), \ldots, s_n(t))$, and the state of the NLFSR at time t is denoted by $b(t) = (b_1(t), b_2(t), \ldots, b_m(t))$. Then $(s(t), b(t))$ is the state of Grain-like cascade FSRs at time t. The update process from $(s(t), b(t))$ to $(s(t+1), b(t+1))$ is called state transition.

Here are two types of status transition modes. If the box bordered by dashed line in Figure 1 were to be removed, then the status transition mode would be as follows:

$$\begin{cases} s_1(t+1) = s_2(t), \\ s_2(t+1) = s_3(t), \\ \qquad \vdots \\ s_n(t+1) = f_1(s_1(t), s_2(t), \ldots, s_n(t)), \\ b_1(t+1) = b_2(t), \\ b_2(t+1) = b_3(t), \\ \qquad \vdots \\ b_m(t+1) = f_2(b_1(t), b_2(t), \ldots, b_m(t)) \oplus s_1(t), \end{cases} \tag{4}$$

where $s_i(t), b_i(t) \in \mathcal{D}$, and $f_1(s_1(t), s_2(t), \ldots, s_n(t))$ is a linear logic function, and $f_2(b_1(t), b_2(t), \ldots, b_m(t))$ is a nonlinear logic function.

Remark 1. The linear logic function is the function only contains operations $(\oplus, \&)$. The nonlinear function is not linear function [45].

Using Lemma 1, we obtain the multi-linear form of (4) as follows:

$$\begin{cases} s(t+1) = L_1 s(t), \\ b(t+1) = L_2 s_1(t) b(t), \end{cases} \tag{5}$$

where $s(t) = \ltimes_{i=1}^{n} s_i(t)$, and $b(t) = \ltimes_{j=1}^{m} b_j(t)$, $L_1 \in \mathcal{L}_{2\times 2^n}$, and $L_2 \in \mathcal{L}_{2\times 2^{m+1}}$. We call L_1 and L_2 state transition matrices.

If the box bordered by dashed line in Figure 1 exists, then the status update mode is different from (4). Here, the states of the last registers are updated through different feedback functions which are shown as follows:

$$s_n(t+1) = f_1(s_1(t), s_2(t), \dots, s_n(t)) \oplus H(s(t), b(t)),$$
$$b_m(t+1) = f_2(b_1(t), b_2(t), \dots, b_m(t)) \oplus s_1(t) \oplus H(s(t), b(t)),$$

where $H(s(t), b(t))$ are logical functions with respect to $s(t)$ and $b(t)$. Then, using STP, we obtain the following algebraic form:

$$\begin{cases} s(t+1) = \tilde{L}_1 s(t) b(t), \\ b(t+1) = \tilde{L}_2 s(t) b(t), \end{cases} \tag{6}$$

where $\tilde{L}_1 \in \mathcal{L}_{2^n \times 2^n}$, $\tilde{L}_2 \in \mathcal{L}_{2^m \times 2^{m+1}}$.

Next, we give the definition of nonsingularity of Grain-like cascade connection FSRs.

Definition 2 ([43])**.** A NLFSR is said to be nonsingular if its state transition diagram contains only cycles.

From Definition 2, we have following definition for FSRs.

Definition 3. FSRs are called nonsingular if their state transition is a bijection. In the contrast, if the state transition of FSRs is not a bijection, then they are singular.

3 Main results

In this section, some interesting properties of Grain-like cascade FSRs are investigated. We also provide some sufficient and necessary conditions about nonsingularity.

Lemma 2 ([44])**.** Supposing that an LFSR is nonsingular in the Grain-like cascade FSRs (4), then the following conditions are equivalent:

- The Gain-like cascade FSRs (4) are nonsingular;
- The NLFSR is nonsingular in Grain-like cascade FSRs (4);
- For any $(b_2(t), b_3(t), \dots, b_m(t))$, the function $f_2(b_1(t), b_2(t), \dots, b_m(t))$ is a bijection concerning the variable $b_1(t)$.

From Lemma 2, if LFSR in Grain-like cascade FSRs (4) is nonsingular, the nonsingular problem of Grain-like cascade FSRs (4) can be regarded as the NLFSR in Grain-like cascade FSRs (4) with the input $s_1(t)$. In the following analysis, we use $u(t)$ to replace $s_1(t)$. Hence, the nonsingular problem of Grain-like cascade FSRs (4) is reduced to a nonsingular problem of the following system:

$$s(t+1) = Fu(t)s(t), \tag{7}$$

where $F = L_2$ in (5), and $u(t) \in \mathcal{D}$. We then have following result.

Remark 2. For general investigation, we reduce the Grain-like cascade FSRs to be (7). The reason why we use matrix F instead of matrix L_2 is that $u(t)$ is not decided by equation $L_1 s(t)$ in (6).

Definition 4 ([43])**.** An NLFSR is said to be nonsingular if its state transition diagram contains only cycles.

From Definition 4, we have the definition of nonsingularity for system (7).

Definition 5. System (7) is said nonsingular if the state transition graph of system (7) has a sub-graph that contains all states, and for this sub-graph the in-degree and out-degree of every point are both 1, and the subgraph only contains cycle.

From Definition 5, we get Theorem 1.

Theorem 1. System (7) is said to be nonsingular if $F = [F_1, F_2]$, with $F_1 \in \mathcal{L}_{2^m \times 2^m}$ and matrices F_1 and F_2 are both nonsingular.

Proof. We want to prove that system (7) is nonsingular. This means that we need to prove that there exists a sub-graph in the state transition graph of system (7), and the sub-graph contains all states of system (7), but the in-degree and the out-degree of every point in the sub-graph are 1, and this sub-graph contains only cycle.

Hence, we need to find a control sequence $u(0),\ u(1),\dots$ such that the state transition graph based on this control sequence only contains the cycle.

Apparently, if the control is always be 0, and hence system (7) becomes $F_2x(t)$, then the state transition graph only contains cycle due to the nonsingularity of matrix F_2. If the control is always 1, and hence system (7) becomes $F_1x(t)$, then the state transition graph only contains cycle due to nonsingularity of matrix F_1. Hence, we prove that if $F_1,\ F_2$ are nonsingular, then system (7) is nonsingular.

Through Theorem 1, we know that if the matrices $F_1,\ F_2$ are nonsingular, we can always find a control sequence $u(0),\ u(1),\dots$ such that there is no cycle in the state transition graph of system (7). This means the system is nonsingular based on Definition 5.

Remark 3. From above analysis, we can know that the nonsingularity of NLFSR is equivalent to the nonsingularity of the matrix.

Next, we provide a property about the structure matrix of the function $g(b_1(t),b_2(t),\dots,b_m(t),s_1(t)) = f_2(b_1(t),b_2(t),\dots,b_m(t))\oplus s_1(t)$. Suppose that the structure matrix of the function $g(b_1(t),b_2(t),\dots,b_m(t), s_1(t)) = M_gs_1(t)b(t)$ is $M_g\in\mathcal{L}_{2\times 2^{m+1}}$, and the structure matrix of the function $f_2(b_1(t),b_2(t),\dots,b_m(t)) = M_fb(t)$ is $M_f\in\mathcal{L}_{2\times 2^m}$ with $b(t)=\ltimes_{i=1}^m b_i(t)\in\Delta_{2^m}$.

Property 1. The structure matrix M_g has the following property:

$$M_g=[M_f,\delta_2[2\ 1]M_f].$$

Proof. Using the vector form of states, i.e. $1\sim\delta_2^1$ and $0\sim\delta_2^2$, by Lemma 1, we have

$$g(b_1(t),b_2(t),\dots,b_m(t),s_1(t))=M_gs_1(t)b(t),$$

where $b_i(t)\in\Delta$. Hence, M_g can be expressed as

$$\begin{aligned}M_g &= M_\oplus(I_2\otimes M_f)\\ &= \delta_2[2\ 1\ 1\ 2]\begin{pmatrix}M_f & 0\\ 0 & M_f\end{pmatrix}\\ &= [\delta_2[2\ 1]M_f\ \delta_2[1\ 2]M_f],\end{aligned}$$

where $M_\oplus$ is the structural matrix of mod 2 addition. Hence, $M_g=[M_f,\delta_2[2\ 1]M_f]$.

Lemma 3 ([2])**.** A binary FSR is nonsingular if and only if its function $f(x_1,x_2,\dots,x_n)$ can be represented as $f(x_1,x_2,\dots,x_n)=x_1\oplus f_0(x_2,\dots,x_n)$ where $x_i\in\mathcal{D}$.

From Theorem 1, Property 1 and Lemma 3, we can easily obtain the following corollary.

Corollary 1. NLFSR in Grain-like cascade FSRs (7) is nonsingular, if system (7) has following property:

$$\begin{aligned}F_{11} &= \delta_2[2\ 1]F_{12},\\ F_{21} &= \delta_2[2\ 1]F_{22},\end{aligned}$$

where $F_{11},F_{12},F_{21},F_{22}\in\mathcal{L}_{2^{m-1}\times 2^{m-1}}$ are four blocks of matrix $F=[F_{11}\ F_{12}\ F_{21}\ F_{22}]$.

After the analysis of the matrix F in (7), we now provide a sufficient condition to the singularity of system (7).

Theorem 2. If in system (7) $\mathrm{col}(F)\neq\Delta_{2^m}$, then system (7) is singular.

Proof. By Definition 5, suppose that system (7) is nonsingular, we can then find a subgraph containing all states, where the in-degree and out-degree of every point are 1, and the subgraph only contains the cycle. Hence, we can conclude that every point can be reached, which means that $\mathrm{col}(F)=\Delta_{2^m}$. Thus if $\mathrm{col}(F)\neq\Delta_{2^m}$, then system (7) is singular.

Theorem 3. In Grain-like cascade FSRs (5), supposing that $\mathrm{col}_i(L_{21}) = \delta_{2^m}^{j}$, the matrix of L_2 has following properties:

- If $j\%2 = 0$, then $\mathrm{col}_i(L_{22}) = \delta_{2^m}^{j-1}$;
- If $j\%2 = 1$, then $\mathrm{col}_i(L_{22}) = \delta_{2^m}^{j+1}$,

where $L_2 = [L_{21}\ L_{22}]$, and $L_{21}, L_{22} \in \mathcal{L}_{2^m\times 2^m}$.

Proof. From the definition of the state transition matrix, for a given state $(b_1, b_2, \ldots, b_m)$ $\delta_{2^m}^i$, assume that

$$L_2u\delta_{2^m}^i = \delta_{2^m}^j = \delta_{2^{m-1}}^{k_1}\delta_2^{k_2}. \tag{8}$$

Because the state of the Grain-like cascade FSRs is shifted over time, we can deduce the next state through shifting. The next state of $(b_1, b_2, \ldots, b_m)$ is $(b_2, \ldots, b_m, f_2(b_1, b_2, \ldots, b_m) + u)$.

$$2^{m-1}b_1 + 2^{m-2}b_2 + \cdots + b_m = 2^m - i.$$

Suppose that the structure matrix of the function f_2 is

$$F = \begin{pmatrix} s_1 & s_2 & \cdots & s_{2^m} \\ 1-s_1 & 1-s_2 & \cdots & 1-s_{2^m} \end{pmatrix}, \tag{9}$$

then the next state can be expressed as

$$(f_2(b_1, b_2, \ldots, b_m) + u) + \cdots + 2^{m-2}b_3 + 2^{m-1}b_2 = (2^m - i - b_1)2 + (s_i \oplus u).$$

If $u = 0$, then $L_2u\delta_{2^m}^i = L_{22}\delta_{2^m}^i = \delta_{2^m}^{j_1}$, and thus $(2^m-i-b_1)2+(s_i\oplus u) = (2^m-i-b_1)2+s_i = 2^m-j_1$.

If $u = 1$, then $L_2u\delta_{2^m}^i = L_{21}\delta_{2^m}^i = \delta_{2^m}^{j_2}$, and thus $(2^m - i - b_1)2 + (s_i \oplus u) = (2^m - i - b_1)2 + (s_i \oplus 1) = 2^m - j_2$.

Hence, there are two possible situations:

- $s_i = 0$, $j_1 = j_2 + 1$;
- $s_i = 1$, $j_1 = j_2 - 1$.

$s_i = 0$ indicates that $\delta_{2^m}^j = \delta_{2^m}^k\delta_{2^n}^2$, which is equivalent to $j\%2 = 0$, and $s_i = 0$ is equivalent to $j\%2 = 1$. Hence, we can conclude if $j\%2 = 0$, then $\mathrm{col}_i(L_{22}) = \delta_{2^m}^{j-1}$, whereas if $j\%2 = 1$, then $\mathrm{col}_i(L_{22}) = \delta_{2^m}^{j+1}$.

Hence, the proof is ended.

From Theorem 3, we obtain that $|\mathrm{col}(L_{21})| = |\mathrm{col}(L_{22})|$, and thus the following corollary can be obtained.

Corollary 2. In Grain-like cascade FSRs (5), the matrix L_{21} is nonsingular if and only if L_{22} is nonsingular.

Proof. Because L_{22} is nonsingular, then $\mathrm{col}(L_{22}) = \Delta_{2^n}$. From Theorem 3, we know that $\mathrm{col}(L_{22}) = \Delta_{2^n}$. Hence, we have the result.

Lemma 4 ([44])**.** If the LFSR and NLFSR in Grain-like cascade FSRs (6) are nonsingular, and $s_1(t)$ and $b_1(t)$ are irrelevant to the function $H(s(t), b(t))$, then Grain-like cascade FSRs (6) are nonsingular.

By using STP, the function $H(s(t), b(t))$ can be expressed as follows:

$$\begin{aligned} H(s(t), b(t)) &= M_Hs(t)b(t) \\ &= M_Hs_1(t)s_2(t)\cdots s_n(t)b_1(t)\cdots b_m(t) \\ &= M_Hs_1(t)W_{[2^{n-1},2]}b_1(t)s_2(t)\cdots s_n(t)b_2(t)\cdots b_m(t) \\ &= M_H(I_2 \otimes W_{[2^{n-1},2]})s_1(t)b_1(t)s_2(t)\cdots s_n(t)b_2(t)\cdots b_m(t) \\ &= \tilde{M}_Hs_1(t)b_1(t)s_2(t)\cdots s_n(t)b_2(t)\cdots b_m(t) \\ &= \tilde{M}_Hs_1(t)b_1(t)s_{2,\ldots,n}(t)b_{2,\ldots,m}(t), \end{aligned}$$

where $M_H, \tilde{M}_H \in \mathcal{L}_{2\times 2^{m+n}}$. Matrix $\tilde{M}_H$ can be divided into four parts, $\tilde{M}_H = [M_{H1}\ M_{H2}\ M_{H3}\ M_{H4}]$, where $M_{Hi}, i = 1, 2, 3, 4 \in \mathcal{L}_{2\times 2^{m+n-4}}$.

Form Lemma 4, we obtain the following corollary.

Corollary 3. If the LFSR and NLFSR in the Grain-like cascade FSRs (6) are nonsingular, and futher if $M_{H1} = M_{H2} = M_{H3} = M_{H4}$, then the Grain-like cascade FSRs (6) are nonsingular.

Proof. Considering the fact that $H(s(t), b(t)) = \tilde{M}_H s_1(t) b_1(t) s_2(t) \cdots s_n(t) b_2(t) \cdots b_m(t)$, and the variables $s_1(t)$ and $b_1(t)$ are irrelevant to the function $H(s(t), b(t))$, then for arbitrary $s_1(t)$ and $b_1(t)$, if $s_{2,\ldots,n}(t)$ and $b_{2,\ldots,m}(t)$ are given, $s_1(t)b_1(t) = \delta_4^i$,

$$\begin{aligned} H(s(t), b(t)) &= \tilde{M}_H \delta_4^i s_{2,\ldots,n}(t) b_{2,\ldots,m}(t) \\ &= M_{Hi} s_{2,\ldots,n}(t) b_{2,\ldots,m}(t). \end{aligned}$$

Because the variables $s_1(t)$ and $b_1(t)$ are irrelevant to the function $H(s(t), b(t))$, $M_{H1} = M_{H2} = M_{H3} = M_{H4}$.

For a binary FSR with m registers, assume that the structure matrix of the feedback function is $M_f = [M_1 \ M_2] \in \mathcal{L}_{2\times 2^m}$. If the binary FSR is nonsingular, then the matrix M_f has the following property.

Lemma 5 ([46])**.** A binary FSR is nonsingular if and only if

$$M_1 = \delta_2[2 \ 1] M_2,$$

where M_1 and $M_2 \in \mathcal{L}_{2\times 2^{m-1}}$.

In the following theorem, we investigate the state transition matrix of system (5). By using STP, we can turn system (5) into the following linear equation:

$$s(t+1)b(t+1) = \tilde{L} s(t) b(t), \tag{10}$$

where $\tilde{L} \in \mathcal{L}_{2^{m+n}\times 2^{m+n}}$.

Next, we want to investigate the relationship between the truth tables of f_1, f_2 in system (5) and matrix $\tilde{L}$ in system (10). Suppose that the truth table of f_1 is $[\zeta_1 \ \zeta_2 \ \cdots \ \zeta_{2^m}]$, and the truth table of f_2 is $[\xi_1 \ \xi_2 \ \cdots \ \xi_{2^n}]$. We then have the following result.

Theorem 4. In (10), we have $\mathrm{col}_i(\tilde{L}) = s_1 2^{m+n} + b_1 2^n + i - (s_1 \oplus \xi_i) - \zeta_i 2^n - 2^{m+n} = \delta_{2^{m+n}}^j$, where $s_1 = k_1 \bmod 2$, $b_1 = k_2 \bmod 2$, $\delta_{2^{m+n}}^i = \delta_2^{k_1} \delta_{2^{m-1}}^i \delta_2^{k_2} \delta_{2^{n-1}}^j$.

Proof. Suppose the state at time t is $(s_1, \ldots, s_m, b_1, b_2, \ldots, b_n) \sim \delta_{2^{m+n}}^i$, then we know that the next state is $(s_2, \ldots, s_n, f_1(s_1, \ldots, s_m), b_2, \ldots, b_n, s_1 \oplus f_2(b_1, \ldots, b_n)) \sim \delta_{2^{m+n}}^j$. Hence, we have

$$\begin{aligned} &s_1 2^{m+n-1} + s_2 2^{m+n-2} + \cdots + s_m 2^n + b_1 2^{n-1} + \cdots + b_n = 2^{m+n} - i, \\ &s_2 2^{m+n-1} + \cdots + \zeta_i 2^n + b_2 2^{n-1} + \cdots + (s_1 \oplus \xi_i) = 2^{m+n} - j. \end{aligned}$$

Then we have $s_2 2^{m+n-1} + \cdots + s_m 2^{n+1} + b_2 2^{n-1} + \cdots + b_n 2 = (2^{m+n} - i - s_1 2^{m+n-1} - b_1 2^{n-1})2$. Hence, we have

$$(2^{m+n} - i - s_1 2^{m+n-1} - b_1 2^{n-1})2 + (s_1 \oplus \xi_i) + \zeta_i 2^n = 2^{m+n} - j,$$

where $b_1 = k_1 \bmod 2$, $s_1 = k_2 \bmod 2$, $\delta_{2^{m+n}}^i = \delta_2^{k_1} \delta_{2^{m-1}}^i \delta_2^{k_2} \delta_{2^{n-1}}^j$. Therefore, we have $\mathrm{col}_i(\tilde{L}) = s_1 2^{m+n} + b_1 2^n + i - (s_1 \oplus \xi_i) - \zeta_i 2^n - 2^{m+n} = \delta_{2^{m+n}}^j$.

In the above theorem, we obtain the property of the state matrix $\tilde{L}$ of Grain-like cascade FSRs. Next, we will provide a sufficient and necessary condition for its nonsingularity.

Theorem 5. System (10) is nonsingular if and only if state transition matrix $\tilde{L}$ is nonsingular.

Proof. (necessity). If $\tilde{L}$ is nonsingular, for the given states x_1, x_2, if $\tilde{L}x_1 = \tilde{L}x_2$, then $x_1 = x_2$. Hence, system (10) is nonsingular.

(sufficiency). For given states x_1, x_2, their next states are assumed to be y_1 and y_2. Suppose that $y_1 \neq y_2$, by the definition of nonsingular, we know that $x_1 \neq x_2$. Hence, matrix $\tilde{L}$ is nonsingular.

However if F_1, F_2 are not singular in Theorem 1, is there any probability such that there exists a subgraph described in Definition 5 which contains only the cycle? In the next theorem, we give the answer.

Theorem 6. If the feedback function of system (7) is given as $x_n(t+1) = u(t) + f(x_1(t), \ldots, x_n(t))$, where $u(t) \in \mathcal{D}$, then system (7) is nonsingular.

Proof. Because the feedback function is $x_n(t+1) = u(t) + f(x_1(t), \ldots, x_n(t))$, we can conclude that matrix F has the following properties:

- F has the property in Theorem 3,
- $F = [F_1,\ F_2]$, where $F_1, F_2 \in \mathcal{L}_{2^m \times 2^m}$, $|\mathrm{col}(F_1)| = |\mathrm{col}(F_2)| > 2^{m-1} - 1$.

An arbitrary state in system (7) has at most two previous status, and thus we have $|\mathrm{col}(F_1)| = |\mathrm{col}(F_2)| > 2^{m-1} - 1$.

Consider the worst situation such that $|\mathrm{col}(F_1)| = |\mathrm{col}(F_2)| = 2^{m-1}$, then it must be true that in the matrix $F_i, i = 1, 2$ for arbitrary $\delta_{2^m}^j \in \mathrm{col}(F_i)$, there exist $j_1 \neq j_2$, such that $\mathrm{col}_{j_1}(F_i) = \mathrm{col}_{j_2}(F_i) = \delta_{2^m}^i$. Because F has the property of Theorem 3, then $\Delta_{2^m} \setminus \mathrm{col}(F_1) \subseteq \mathrm{col}(F_2)$, and $\mathrm{col}(F_1) \cup \mathrm{col}(F_2) = \Delta_{2^m}$. Hence, we obtain that $|\mathrm{col}(F)| = 2^m$, and we can find a subgraph with 2^m points containing only cycles, and the in-degree and out-degree of every point are 1. Hence, system (7) is nonsingular.

Based on Theorem 6, we develope an algorithm to find the subgraph mentioned in Theorem 6.

Algorithm 1

```
Require: Set $\mathrm{Index}_1 = \varnothing$, set $\mathrm{Index}_2 = \varnothing$, $S = \{1, 2, \ldots, 2^m\}$.
for $x \in \mathrm{col}(F_1)$
    If $\mathrm{col}_i(F_1) = x$ then
        $\mathrm{Index}_1 \Leftarrow \mathrm{Index}_1 \cup i$;
    else
        $\mathrm{Index}_2 \Leftarrow \mathrm{Index}_2 \cup i$.
    end if
end for
```

Remark: For $\delta_{2^m}^i$, if $i \in \mathrm{Index}_1$, then the next state of $\delta_{2^m}^i$ is $F\delta_2^1\delta_{2^m}^i = F_1\delta_{2^m}^i$, which means that the control input is δ_2^1 for $\delta_{2^m}^i$. If $i \in \mathrm{Index}_2$, then the next state of $\delta_{2^m}^i$ is $F\delta_2^2\delta_{2^m}^i = F_2\delta_{2^m}^i$, which means that the control input is δ_2^2 for $\delta_{2^m}^i$.

Hence, through the above four steps, we find a control input for every state in Δ_{2^m}, such that the subgraph in Theorem 6 can be found.

4 Examples

In this section, we provide two examples to illustrate the effectiveness of the algorithm and our theoretical results obtained through this paper.

Example 1. Consider the following Grain-like cascade FSRs:

$$\begin{aligned} b_1(t+1) &= b_2(t), \\ b_2(t+1) &= b_1(t) \oplus b_2(t), \\ s_1(t+1) &= s_2(t), \\ s_2(t+1) &= \neg s_1(t) \oplus b_1(t), \end{aligned}$$

where $s_i(t), b_i(t) \in \mathcal{D},\ i = 1, 2$.

By using STP, we can turn system (11) into the following:

$$b(t+1) = L_1 b(t), \tag{11}$$

$$s(t+1) = L_2 b_1(t) s(t), \tag{12}$$

where $L_1 = \delta_4[2\ 3\ 1\ 4]$, $L_2 = \delta_4[1\ 3\ 2\ 4\ 2\ 4\ 1\ 3]$. The state transition graph of LFSR and NLFSR are shown in Figures 2 and 3 respectively.

We know that L_1 is nonsingular, and thus the LFSR is nonsingular. From Theorem 1, $L_2 = [L_{21}\ L_{22}]$, and matrices L_{21}, L_{22} are nonsingular. In addition, L_{21} and L_{22} satisfy Theorem 3.

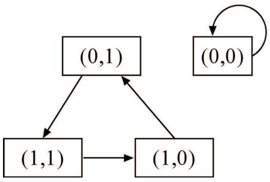

Figure 2 Transition graph of LFSR in Example 1.

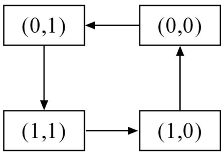

Figure 3 Transition graph of NLFSR in Example 1.

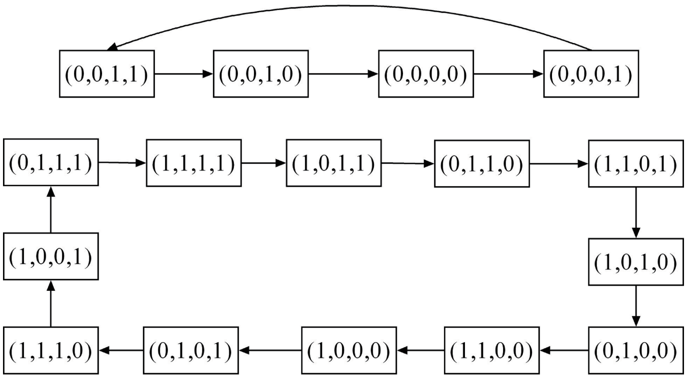

Figure 4 Transition graph of cascade NLFSR in Example 1.

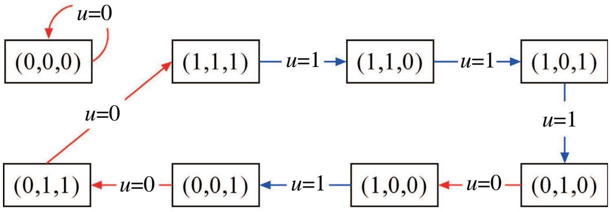

Figure 5 (Color online) Subgraph of NLFSR in Example 2.

Multiplying equations in (11), we obtain the following:

$$b(t+1)s(t+1) = \tilde{L}b(t)s(t), \tag{13}$$

where $\tilde{L} = [5\ 7\ 6\ 8\ 10\ 12\ 9\ 11\ 1\ 3\ 2\ 4\ 14\ 16\ 13\ 15]$, it is clear that matrix $\tilde{L}$ is nonsingular, which is consistent with Theorem 4. The state transition graph of system (11) is shown in Figure 4.

Example 2. Consider NLFSR with an input

$$x_1(t+1) = x_2(t), \tag{14}$$
$$x_2(t+1) = x_3(t), \tag{15}$$
$$x_3(t+1) = \neg x_3(t) \oplus u(t), \tag{16}$$

where $x_i(t) \in \mathcal{D},\ i = 1,2,3,\ u(t) \in \mathcal{D}$.

By using STP, we obtain the following equation:

$$x(t+1) = Lu(t)x(t), \tag{17}$$

where $L = [1\ 4\ 5\ 8\ 1\ 4\ 5\ 8\ 2\ 3\ 6\ 7\ 2\ 3\ 6\ 7]$. By using Algorithm 1, let $\text{Index}_1 = \{1,\ 2,\ 3,\ 4\}$, $\text{Index}_2 = \{5,\ 6,\ 7,\ 8\}$, we yield the input of states $\delta_8^1,\ \delta_8^2,\ \delta_8^3,\ \delta_8^4$ is δ_2^1, the input of states $\delta_8^5,\ \delta_8^6,\ \delta_8^7,\ \delta_8^8$ is δ_2^2. We find a subgraph satisfying the conditions in Theorem 6 as shown in Figure 5.

5 Conclusion

In this paper, We investigated the nonsingularity of Grain-like cascade FSRs using STP method and the nonsingularity of BCN. First, we treated Grain-like cascade FSRs as BN. Then, Grain-like cascade FSRs were converted into a linear form. Based on the linear form of Grain-like cascade FSRs, we investigated the properties of the state transition graph of Grain-like cascade FSRs. We then provided a sufficient and necessary condition for the nonsingularity of Grain-like cascade FSRs. At last, if the first LFSR is nonsingular, we treated Grain-like cascade FSRs as BCNs, and generalize the Grain-like cascade FSRs into a general form. An algorithm was provided to find a subgraph satisfying the conditions in Definition 5. Finally, two examples were given to illustrate our theoretical results.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61573102, 11671361), Natural Science Foundation of Jiangsu Province of China (Grant No. BK20170019), Jiangsu Provincial Key Laboratory of Networked Collective Intelligence (Grant No. BM2017002), China Postdoctoral Science Foundation (Grant Nos. 2014M560377, 2015T80483), Jiangsu Province Six Talent Peaks Project (Grant No. 2015-ZNDW-002), and Fundamental Research Funds for the Central Universities.

References

1 Goresky M, Klapper A. Algebraic Shift Register Sequences. Cambridge: Cambridge University Press, 2012

2 Golomb S W. Shift Register Sequences. Walnut Creek: Aegean Park Press, 1982

3 Goresky M, Klapper A. Pseudonoise sequences based on algebraic feedback shift registers. IEEE Trans Inf Theory, 2006, 52: 1649–1662

4 Li C Y, Zeng X Y, Helleseth T, et al. The properties of a class of linear FSRs and their applications to the construction of nonlinear FSRs. IEEE Trans Inf Theory, 2014, 60: 3052–3061

5 Massey J. Shift-register synthesis and BCH decoding. IEEE Trans Inf Theory, 1969, 15: 122–127

6 Meier W, Staffelbach O. Fast correlation attacks on certain stream ciphers. J Cryptology, 1989, 1: 159–176

7 Hell M, Johansson T, Meier M. Grain: a stream cipher for constrained environments. Int J Wirel Mobile Comput, 2007, 2: 86–93

8 Gammel B M, Gottfert R, Kniffler O. An NLFSR-based stream cipher. In: Proceedings of IEEE International Symposium on Circuits and Systems, Island of Kos, 2006

9 Chen K, Henricksen M, Millan W, et al. Dragon: a fast word based stream cipher. In: Proceedings of International Conference on Information Security and Cryptology. Berlin: Springer, 2004. 33–50

10 Gammel B, Göttfert R, Kniffler O. Achterbahn-128/80: design and analysis. ECRYPT Network of Excellence – SASC Workshop Record, 2007. https://www.cosic.esat.kuleuven.be/ecrypt/stream/papersdir/2007/020.pdf

11 Courtois N T, Meier W. Algebraic attacks on stream ciphers with linear feedback. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2003. 345–359

12 Robshaw M, Matsumoto M, Saito M, et al. New Stream Cipher Designs: the eSTREAM Finalists. Berlin: Springer, 2008

13 Hell M, Johansson T, Maximov A. The grain family of stream ciphers. Lect Notes Comput Sci, 2008, 4986: 179–190

14 Babbage S, Dodd M. The MICKEY Stream Ciphers. Berlin: Springer, 2008

15 Maximov A. Cryptanalysis of the "Grain" family of stream ciphers. In: Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, Taipei, 2006. 283–288

16 Berbain C, Gilbert H, Joux A. Algebraic and correlation attacks against linearly filtered non linear feedback shift registers. In: Proceedings of the 15th International Workshop on Selected Areas in Cryptography, Sackville, 2008. 184–198

17 Hu H G, Gong G. Periods on two kinds of nonlinear feedback shift registers with time varying feedback functions. Int J Found Comput Sci, 2011, 22: 1317–1329

18 Cheng D Z, Qi H S, Li Z Q. Analysis and Control of Boolean Networks. Berlin: Springer, 2011

19 Li H T, Zhao G D, Meng M, et al. A survey on applications of semi-tensor product method in engineering. Sci China Inf Sci, 2018, 61: 010202

20 Lu J Q, Li H T, Liu Y, et al. Survey on semi-tensor product method with its applications in logical networks and other finite-valued systems. IET Control Theory Appl, 2017, 11: 2040–2047

21 Lu J Q, Zhong J, Ho D W C, et al. On controllability of delayed Boolean control networks. SIAM J Control Optim, 2016, 54: 475–494

22 Liu Y, Chen H W, Wu B. Controllability of Boolean control networks with impulsive effects and forbidden states. Math Method Appl Sci, 2014, 37: 1–9

23 Zhu Q X, Liu Y, Lu J Q, et al. Observability of Boolean control networks. Sci China Inf Sci, 2018, 61: 092201. doi: 10.1007/s11432-017-9135-4

24 Lu J Q, Zhong J, Huang C, et al. On pinning controllability of Boolean control networks. IEEE Trans Autom Control,

2016, 61: 1658–1663

25 Zhong J, Lu J Q, Liu Y, et al. Synchronization in an array of output-coupled Boolean networks with time delay. IEEE Trans Neural Netw Learn Syst, 2014, 25: 2288–2294

26 Liu Y, Li B W, Lu J Q, et al. Pinning control for the disturbance decoupling problem of Boolean networks. IEEE Trans Autom Control, 2017. doi:10.1109/TAC.2017.2715181

27 Liu Y, Sun L J, Lu J Q, et al. Feedback controller design for the synchronization of Boolean control networks. IEEE Trans Neural Netw Learn Syst, 2016, 27: 1991–1996

28 Li F F, Sun J T. Controllability of Boolean control networks with time delays in states. Automatica, 2011, 47: 603–607

29 Cheng D Z, Qi H S. Controllability and observability of Boolean control networks. Automatica, 2009, 45: 1659–1667

30 Laschov D, Margaliot M. Controllability of Boolean control networks via the perron-frobenius theory. Automatica, 2012, 48: 1218–1223

31 Li H T, Wang Y Z, Xie L H. Output tracking control of Boolean control networks via state feedback: constant reference signal case. Automatica, 2015, 59: 54–59

32 Cheng D Z, Qi H S, Li Z Q, et al. Stability and stabilization of Boolean networks. Int J Robust Nonlinear Control, 2011, 21: 134–156

33 Li H T, Wang Y Z. Controllability analysis and control design for switched Boolean networks with state and input constraints. SIAM J Control Optim, 2015, 53: 2955–2979

34 Zhong J, Lu J Q, Huang T W, et al. Controllability and synchronization analysis of identical-hierarchy mixed-valued logical control networks. IEEE Trans Cybern, 2017, 47: 3482–3493

35 Guo P L, Wang Y Z, Li H T. A semi-tensor product approach to finding Nash equilibria for static games. In: Proceedings of the 32nd Chinese Control Conference (CCC), Xi'an, 2013. 107–112

36 Li H T, Xie L H, Wang Y Z. On robust control invariance of Boolean control networks. Automatica, 2016, 68: 392–396

37 Zhong J H, Lin D D. A new linearization method for nonlinear feedback shift registers. J Comput Syst Sci, 2014, 81: 783–796

38 Zhong J H, Lin D D. Stability of nonlinear feedback shift registers. Sci China Inf Sci, 2016, 59: 012204

39 Zhong J H, Lin D D. Driven stability of nonlinear feedback shift registers with inputs. IEEE Trans Commun, 2016, 64: 2274–2284

40 Zhong J, Ho D W C, Lu J Q, et al. Global robust stability and stabilization of Boolean network with disturbances. Automatica, 2017, 84: 142–148

41 Liu Y, Cao J D, Sun L J, et al. Sampled-data state feedback stabilization of Boolean control networks. Neural Comput, 2016, 28: 778–799

42 Wu H J, Huang T, Nguyen P H, et al. Differential attacks against stream cipher ZUC. In: Proceedings of the 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, 2012. 262–277

43 Lai X J. Condition for the nonsingularity of a feedback shift-register over a general finite field (corresp.). IEEE Trans Inf Theory, 1987, 33: 747–749

44 Wang Q Y, Jin C H. Criteria for nonsingularity of Grain-like cascade feedback shift register (in Chinese). Comput Eng, 2014, 40: 519–523

45 Girard J Y. Linear logic. Theor Comput Sci, 1987, 50: 1–101

46 Liu Z B, Wang Y Z, Cheng D Z. Nonsingularity of feedback shift registers. Automatica, 2015, 55: 247–253