Automatica 55 (2015) 247–253

Contents lists available at ScienceDirect

Automatica

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

Brief paper

Nonsingularity of feedback shift registers☆

Zhenbin Liu [a,b], Yuzhen Wang [b,1], Daizhan Cheng [b]

[a] School of Science and Information Science, Qingdao Agricultural University, Qingdao 266109, PR China
[b] School of Control Science and Engineering, Shandong University, Jinan 250061, PR China

ARTICLE INFO

Article history:
Received 17 January 2014
Received in revised form
25 November 2014
Accepted 3 March 2015
Available online 31 March 2015

Keywords:
Feedback shift register
Nonsingularity
Cycle
Decomposition and synthesis
Semi-tensor product

ABSTRACT

In this paper, the multi-valued feedback shift register (FSR) is studied and a new approach is present to analyze its nonsingularity, number of cycles, and cycle synthesis. Firstly, the FSR is expressed in an algebraical form, based on which several necessary and sufficient conditions are given for the nonsingularity. Secondly, the structural matrix of FSR is defined, and a new method is introduced to determine the number of cycles with different lengths for arbitrarily given FSR. Thirdly, the problem on cycle decomposition and synthesis of an FSR is investigated, and some new results are obtained. Finally, an illustrative example is studied to support our new results.

1. Introduction

The feedback shift register (FSR) is used to create pseudo-random sequences in many fields, such as error detecting and correcting codes (Rajpal, Kumar, Dudhani, & Jindal, 2004), and cryptographic systems (Bruen & Mollin, 2009). The major research fields on FSRs usually have the following three aspects (Jansen, 1986): (1) Analysis for a given FSR, including the nonsingularity, the number of fixed points and cycles with different lengths of the sequence generated by FSR, decomposition and synthesis of cycles, etc.; (2) Construction of the shortest FSR which can generate a given sequence; (3) Construction of all full length FSRs.

An FSR is called a nonsingular FSR if it only has cycles without branches in its transition diagram. For the nonsingularity of FSRs, there are several results until now. It is well known that a given n-stage FSR is completely decided by a feedback function $f(x_1, x_2, \ldots, x_n)$. In Golomb (1967), a necessary and sufficient condition was given for nonsingularity of binary FSRs (i.e., $x_i \in \{0, 1\}, i = 1, 2, \ldots, n$). That is, a binary FSR is nonsingular iff its feedback function $f(x_1, x_2, \ldots, x_n)$ can be expressed as $x_1 + f_0(x_2, \ldots, x_n) \pmod 2$, where f_0 is independent of the variable x_1. But it is not generalized to FSRs over the general field. Hence, it is necessary to establish some new methods to judge the nonsingularity of multi-valued FSRs. In Lai (1987), Lai gave a necessary and sufficient condition for nonsingularity of nonlinear FSRs over the q-valued field. Since there are $q-1$ n-ary functions to be constructed, it is difficult to use this method in practice. Thus, it is still an interesting and challenging topic to study the nonsingularity of FSRs.

It is worth noting that the semi-tensor product of matrices (Cheng, Qi, & Li, 2011) has been successfully used in the study of Boolean (control) networks (Cheng & Qi, 2009, 2010; Cheng, Li, & Qi, 2010), multi-valued and mix-valued logical networks (Li & Cheng, 2010; Liu & Wang, 2012), and some other related fields (Laschov & Margaliot, 2012; Li, Sun, & Wu, 2011; Li & Wang, 2012; Qi & Cheng, 2010; Wang, Zhang, & Liu, 2012; Yang, Li, & Chu, 2013; Zhang & Zhang, 2013). In Cheng and Qi (2010), authors investigated a matrix expression of a Boolean network, and presented some results about the number of cycles, transient period and basin of each attractor. Multi-valued logical networks were studied in Li and Cheng (2010), and the controllability of multi-valued logical control networks was revealed.

This paper investigates the multi-valued FSR and presents a new method to analyze its nonsingularity, number of cycles, and cycle synthesis. First, the FSR is expressed as an algebraical form, based on which several necessary and sufficient conditions are

☆ This work is supported by the National Natural Science Foundation of China (G61174036, G61374065, G61403223), the Research Fund for the Taishan Scholar Project of Shandong Province of China, and the Research Fund of high-level personnel of Qingdao Agricultural University (631114329). The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Oswaldo Luiz V. Costa under the direction of Editor Berç Rüstem.

E-mail addresses: lzbzj@163.com (Z. Liu), yzwang@sdu.edu.cn (Y. Wang), dcheng@iss.ac.cn (D. Cheng).

[1] Tel.: +86 531 88392515; fax: +86 531 88392205.

http://dx.doi.org/10.1016/j.automatica.2015.03.014
0005-1098/

given for the nonsingularity. Second, we define the structural matrix of FSRs, and introduce a new method to determine the number of cycles with different lengths for arbitrary given FSR. Third, we consider the problem on cycle decomposition and synthesis, and obtain some new results. Finally, we give an illustrative example to support our new results. The study of example shows that the results obtained in this paper are very effective.

Compared with the existing results (Golomb, 1967; Lai, 1987; Li & Xie, 1995), the results of this paper have the following advantages: (1) The method of this paper only needs a little knowledge on the matrix product, which is easy to understand. However, the methods of existing results generally need a large amount of knowledge over the finite field in using, and it is difficult to grasp for the scholars not engaging in research of mathematics. (2) Our results can be applied to all FSRs, and also be used to deal with certain problems which have not been solved by the existing methods. In fact, the existing results can only solve the nonsingularity of some special classes of FSRs. The method of Golomb (1967), for example, can only judge the nonsingularity of binary FSRs. Although Lai (1987) generalized Golomb (1967) to the multi-valued form, its result is only a theoretical method, where in order to verify the nonsingularity of an FSR over the field $GF(q)$, one needs to construct $q-1$ multi-ary functions. Thus, it is difficult to use this method in practice. Moreover, although Li and Xie (1995) gave the necessary and sufficient conditions for the nonsingularity of FSRs over the field $GF(q)$, the method of Li and Xie (1995) can only deal with FSRs of degree at most three over finite field $GF(q)$. (3) The conditions of our results can be easily verified. In fact, one only needs to compute a kind of matrix, called the structural matrix of the FSR. Based on the matrix, the nonsingularity can be judged from the singularity of block matrices of the structural matrix. In a word, the main contributions of this paper are as follows. (i) A criteria for the nonsingularity of FSRs is obtained in this paper. The criteria can be applied to all FSRs and its conditions can be easily verified. Moreover, it can solve FSRs with the degree more than three, which could not be solved in Li and Xie (1995). (ii) The structural matrix of the FSR is first defined via the semi-tensor product in this paper. Based on the structural matrix, a necessary and sufficient condition is given on the synthesis and decomposition of FSRs.

The rest of this paper is organized as follows. Section 2 gives some necessary preliminaries on the semi-tensor product of matrices. In Section 3, we present the main results of this paper, and in Section 4, we give an illustrative example to support our new results, which is followed by the conclusion in Section 5.

2. Preliminaries

In this section, we recall some necessary preliminaries on the semi-tensor product and the matrix expression of logical networks, which will be used in the sequel. In this paper, the used matrix product is the semi-tensor product (STP) "$\ltimes$", which is a generalization of the conventional matrix product and retains all the fundamental properties of the latter. Because of this, we can omit the sign "$\ltimes$" without confusion. To see the definition and properties of the STP, please refer to Cheng et al. (2011).

First, we give some notations.

- $\mathcal{D}_k = \{0, 1, \ldots, k-1\}$, especially, $\mathcal{D} := \mathcal{D}_2 = \{0, 1\}$.
- δ_n^i: the ith column of the identity matrix I_n.
- Denote by $Col_b(B)$ the b-th column of matrix B, and by $\mathrm{Col}(B)$ the set of all columns of matrix B.
- $\mathbb{R}^{n\times r}$: the set of $n \times r$ real matrices, where $\mathbb{R}$ denotes the set of real numbers.
- $\Delta_n := \{\delta_n^i \mid i = 1, 2, \ldots, n\}$, and for simplicity, let $\Delta := \Delta_2$. Identify $k - i \sim \delta_k^i$, $i = 1, 2, \ldots, k$, which implies $\mathcal{D}_k \sim \Delta_k$, where $p \sim q$ means they are equivalent.

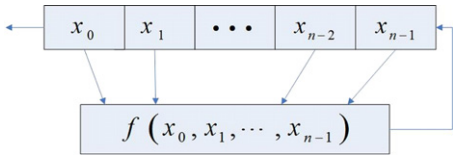

Fig. 1. A feedback shift register.

- A matrix $L \in \mathbb{R}^{n\times r}$ is called a logical matrix, if columns of L are of the form of δ_n^i. Denote by $\mathcal{L}_{n\times r}$ the set of $n \times r$ logical matrices.
- If $L \in \mathcal{L}_{n\times r}$, it can be expressed as $L = \left[\delta_n^{i_1}\ \delta_n^{i_2}\ \cdots\ \delta_n^{i_r}\right]$. For the sake of compactness, it is briefly denoted by $L = \delta_n[i_1\ i_2\ \cdots\ i_r]$.

Now, we list some basic properties of the semi-tensor product (Cheng et al., 2011).

1. Let $X \in \mathbb{R}^m$ and $Y \in \mathbb{R}^n$ be column vectors. Then
$$W_{[m,n]}XY = YX, \tag{1}$$
where $W_{[m,n]}$ is called a swap matrix and can be written as
$$\left[\delta_n^1 \ltimes \delta_m^1\ \cdots\ \delta_n^n \ltimes \delta_m^1 \vdots \cdots \vdots \delta_n^1 \ltimes \delta_m^m\ \cdots\ \delta_n^n \ltimes \delta_m^m\right].$$
2. Let $X \in \mathbb{R}^t$ be a column vector. Then
$$XA = (I_t \otimes A)X.$$
3. Let $X = \delta_t^i \in \mathbb{R}^t$ be a logical vector. Then
$$X^2 = M_{r,t}X, \tag{2}$$
where $M_{r,t} = \left[\delta_t^1 \ltimes \delta_t^1\ \cdots\ \delta_t^t \ltimes \delta_t^t\right] \in \mathcal{L}_{t^2\times t}$.
4. Let $X = \delta_t^i \in \mathbb{R}^t$ be a logical vector and $A \in \mathbb{R}^{m\times nt}$. Then
$$AX = A_i,$$
where $A_i \in \mathbb{R}^{m\times n}$ is the ith block of $A = [A_1\ A_2\ \cdots\ A_t]$.

Lemma 1 (*Cheng et al., 2011*). *Any logical function $y = f(x_1, x_2, \ldots, x_n)$ with logical variables $x_i \in \mathcal{D}_k$, $i = 1, \ldots, n$, can be expressed in a multi-linear form as*
$$y = f(x_1, x_2, \ldots, x_n) = M_f x_1 x_2 \cdots x_n, \tag{3}$$
where $y \in \Delta_k$, and $M_f \in \mathcal{L}_{k\times k^n}$ is unique, called the structural matrix of f.

3. Main results

This section studies FSRs and presents the main results. First, we analyze the nonsingularity of FSRs.

3.1. Nonsingularity of FSRs

Fig. 1 denotes an n-stage k-valued FSR with a logical function $f(x_0, \ldots, x_{n-1})$, where $x_i \in \mathcal{D}_k$. Now, starting from the state $\alpha^0 = (x_0, x_1, \ldots, x_{n-1})$, a state sequence $\alpha^0, \alpha^1, \alpha^2, \ldots$ is generated by the FSR, where $\alpha^1 = (x_1, x_2, \ldots, x_n)$ is decided by the state α^0, $x_n = f(x_0, x_1, \ldots, x_{n-1})$, α^2 is decided by state α^1, and so on. Thus, the algebraic form of FSR can be as
$$\alpha^{t+1} = (x_{t+1}, \ldots, x_{t+n}) = T_f(\alpha^t),\ t = 0, 1, \ldots \tag{4}$$
where $x_{t+n} = f(x_t, x_{t+1}, \ldots, x_{t+n-1})$, and $T_f : \mathcal{D}_k^n \to \mathcal{D}_k^n$ is called the transition function of FSR.

Definition 1 (*Lai, 1987*). An FSR is said to be nonsingular if its states transition diagram contains only cycles.