Zhe GAO, Jun'e FENG, Yongyuan YU, Yanjun CUI, 2022. On observability of Galois nonlinear feedback shift registers over finite fields. *Frontiers of Information Technology & Electronic Engineering*, 23(10):1533-1545.
https://doi.org/10.1631/FITEE.2200228

On observability of Galois nonlinear feedback shift registers over finite fields

Keywords: Observability; Nonlinear feedback shift registers (NFSRs); Galois NFSRs; Semi-tensor product; Finite fields; Logical networks

Corresponding author: Jun'e FENG
E-mail: fengjune@sdu.edu.cn
ORCID: https://orcid.org/0000-0003-3881-3042

Motivation

1. As a pseudo-random sequence generator, nonlinear feedback shift registers (NFSRs) are widely used in many scenarios, such as classical stream ciphers, cryptographic systems, secure communication, delay measurement, and spread spectrum communication generators.

2. According to the definition of observability, NFSR-based stream ciphers should avoid unobservable Galois NFSRs from the security viewpoint and select observable ones.

3. The semi-tensor product of matrices has great potential as a new mathematical tool in NFSR research.

Main idea

1. NFSRs are treated as logical networks using the semi-tensor product of matrices.

2. The observability of general Galois NFSRs is researched using two methods that are based on the state pair trajectory table and a new observability matrix, separately.

3. Two special types of Galois NFSRs, i.e., the full-length Galois NFSRs and the nonsingular Galois NFSRs, are investigated.

Method

1. For general Galois NFSRs, a vector form as well as an algorithm based on the vector form is proposed to draw the state pair trajectory table, by which a necessary and sufficient condition for the observability of this type of NFSR is obtained.

2. For general Galois NFSRs, a new observability matrix is defined, by which a necessary and sufficient condition with a lower computation complexity is derived.

3. For full-length Galois NFSRs and nonsingular Galois NFSRs, two simpler methods are proposed according to the state transition diagram (ST-diagram) and state pair transition diagram (SPT-diagram), respectively.

Method (Cont'd)

Algorithm 1 Observability judgment of an n-stage Galois NFSR over $\mathbb{F}_p$

Require: the vector form of the state transition matrix of the Galois NFSR and its indistinguishable initial state set Ω

Ensure: a state pair trajectory table

1: $k = 1$
2: **for** all $(\delta_{p^n}^i, \delta_{p^n}^j) \in \Omega$ **do**
3: **while** $k \neq 0$ **do**
4: **if** $(\varphi(i), \varphi(j)) = (i, j)$ **then**
5: $R_k = *$, $k = 0$
6: **else if** $(\varphi(i), \varphi(j)) \in \Phi \backslash \Omega$ **then**
7: $R_k = \surd$, $k = 0$
8: **else**
9: $k = k + 1$, $(i, j) = (\varphi(i), \varphi(j))$
10: **end if**
11: **end while**
12: **end for**

Major results

Table 2 State pair trajectory table of Galois NFSR in Example 1

Step	Indistinguishable initial state pair								
	(1,2)	(1,3)	(2,3)	(4,5)	(4,6)	(5,6)	(7,8)	(7,9)	(8,9)
R_1	(2,3)	√	√	√	√	(7,9)	(1,2)	(1,3)	(2,3)
R_2	√					(1,3)	(2,3)	√	√
R_3						√	√		

Table 3 State pair trajectory table in Example 3

Step	Indistinguishable initial state pair							
	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)	(1,7)	(1,8)	(1,9)
R_1	(2,3)	(2,4)	(2,5)	(2,6)	(2,7)	(2,8)	(2,9)	√
R_2	(3,4)	(3,5)	(3,6)	(3,7)	(3,8)	(3,9)	√	
R_3	(4,5)	(4,6)	(4,7)	(4,8)	(4,9)	√		
R_4	(5,6)	(5,7)	(5,8)	(5,9)	√			
R_5	(6,7)	(6,8)	(6,9)	√				
R_6	(7,8)	(7,9)	√					
R_6	(8,9)	√						
R_7	√							

Major results (Cont'd)

Theorem 2 An n-stage Galois NFSR is observable if and only if there exists an integer $l \in \mathbb{N}$ such that the corresponding new observability matrix $\boldsymbol{Q}_l$ has p^n distinct rows. Moreover, if such an l exists, and the smallest l is denoted as l^*, then $l^* \leq \min\{p^n - p, \frac{p^{2n-1}-p^n}{2}\}$ must hold.

Theorem 3 For an n-stage full-length Galois NFSR over $\mathbb{F}_p$, $\boldsymbol{L}$ is the state transition matrix of this Galois NFSR. Then the Galois NFSR is observable if and only if there exists $i \in \{1, 2, \cdots, p^n\}$, such that the state pairs in $P_i \cap \Omega$ can be distinguished.

Theorem 4 An n-stage nonsingular Galois NFSR over $\mathbb{F}_p$ is observable if and only if each cycle of the SPT-diagram contains a state pair in set $\Phi \backslash \Omega$.

Major results (Cont'd)

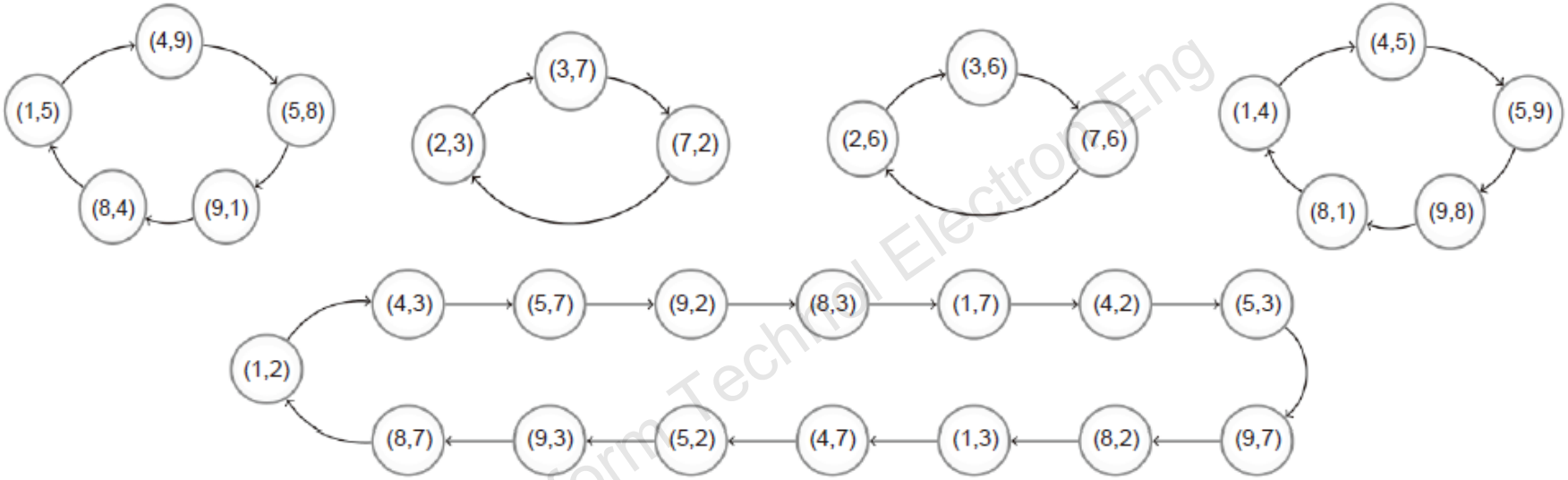

Fig. 3 SPT-diagram of the Galois NFSR in Example 4

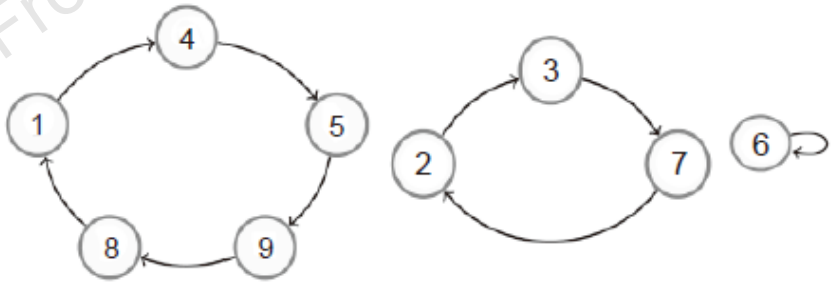

Fig. 4 ST-diagram of the Galois NFSR in Example 4

Conclusions

1. In this paper, the observability of Galois NFSRs over finite fields was investigated.

2. We researched the observability of general Galois NFSRs and gave the observability criteria by two methods.

3. We studied two special types of Galois NFSRs, i.e., full-length Galois NFSRs and nonsingular Galois NFSRs, and proposed simpler observability criteria.

4. In the future, the observability of Galois NFSRs with inputs will be studied, and reducing computation complexity will be explored.

Zhe GAO received her BS degree in the School of Mathematics from Shandong University, Jinan, China, in 2017, and her MS degree from Shandong University, in 2020. She is currently pursuing her PhD degree at the School of Mathematics at Shandong University. Her research interests include Boolean networks and feedback shift registers.

Jun’e FENG received her PhD degree from Shandong University, in 2003. She is currently a professor with the School of Mathematics at Shandong University, Jinan, China. She was a visiting scholar at the MIT, USA, from 2006 to 2007, and a visiting scholar at the University of Hong Kong, Hong Kong, China, in 2008, 2009, and 2013. Her research interests include singular systems, Boolean networks, robust control, and feedback shift registers.

Yongyuan YU received his PhD degree from the School of Mathematics, Shandong University, Jinan, China, in 2019. From January to April 2019, he was a research assistant in the Department of Applied Mathematics, the Hong Kong Polytechnic University, China. From June 2019 to July 2021, he was a postdoctor in the Institute of System Science, Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He is currently an associate professor of Shandong University. His research interest covers Boolean control networks, quantum computation, and game-based control systems.