ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.1, January 2007, pp.40−49
DOI: 10.1360/jos180040

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

关于二元延迟 3 步前馈逆有限自动机的结构*

王鸿吉[1,2+], 姚 刚[3]

[1](中国科学院 软件研究所,北京 100080)
[2](中国科学院 研究生院,北京 100049)
[3](信息安全国家重点实验室(中国科学院 软件研究所),北京 100080)

On the Structure of Binary Feedforward Inverse Finite Automata with Delay 3

WANG Hong-Ji[1,2+], YAO Gang[3]

[1](Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China)
[2](Graduate School, The Chinese Academy of Sciences, Beijing 100049, China)
[3](The State Key Laboratory of Information Security (Institute of Software, The Chinese Academy of Sciences), Beijing 100080, China)
+ Corresponding author: Phn: +86-10-82625471, E-mail: whj@gcl.iscas.ac.cn, http://lcs.ios.ac.cn

Wang HJ, Yao G. On the structure of binary feedforward inverse finite automata with delay 3. *Journal of Software*, 2007,18(1):40−49. http://www.jos.org.cn/1000-9825/18/40.htm

Abstract: The structure of feedforward inverses is a fundamental problem in the invertibility theory of finite automata. The characterization of the structure of feedforward inverses with delay steps ≥3 is a long-term unsolved problem. This paper deals with this topic. For a binary weakly invertible semi-input memory finite automaton $C(M_a,f)$ with delay 3, where the state graph of M_a is cyclic, the characterizations of the structures are given when its minimal 3-output weight is 1, 2, and 8, respectively. Because $C(M_a,f)$ is weakly invertible with delay 3 iff it is weakly inverse with delay 3, a partial characterization of the structure of binary feedforward inverses with delay 3 is obtained.

Key words: finite automata; semi-input memory; feedforward inverses; invertibility

摘 要: 前馈逆有限自动机的结构是有限自动机可逆性理论中的基本问题.对延迟步数≥3 的前馈逆结构的刻划,则是一个长期的未解决问题.研究了二元延迟 3 步前馈逆有限自动机的结构.对于自治有限自动机 M_a 的状态图为圈的二元延迟 3 步弱可逆半输入存储有限自动机 $C(M_a,f)$,给出了其长 3 极小输出权分别为 1,2,8 三种情形下结构的一种刻画.由于 $C(M_a,f)$延迟 3 步弱可逆当且仅当它是延迟 3 步弱逆,因此,得到了二元延迟 3 步前馈逆有限自动机结构的一种部分刻画.

关键词: 有限自动机;半输入存储;前馈逆;可逆性
中图法分类号: TP301 文献标识码: A

* Supported by the National Natural Science Foundation of China for Grand International Joint Project under Grant No.60310213 (国家自然科学基金重大国际(地区)合作研究项目); the National Natural Science Foundation for Distinguished Young Scholars of China under Grant No.60325206 (国家杰出青年科学基金)

Received 2005-01-26; Accepted 2005-04-18

1 Introduction

A semi-input memory (SIM) finite automaton (FA) is called feedforward inverse if it is weakly inverse[1]. A fundamental problem of feedforward inverses is to characterize their structures[2]. However, this is not trivial. The previous systematic results on this topic are in the case of delay steps ≤ 2[3−7], while keeping unsolved for the case of delay steps ≥ 3 for a long-term. This paper studies the structure of binary feedforward inverses with delay 3.

Reference [6] shows that the binary weakly invertible(WI) SIM finite automata $C(M_a,f)$ with delay 3, where the state graph of M_a is cyclic, can be divided into four classes by the minimal 3-output weight $w_{3,M}$, i.e., $w_{3,M}$=1, 2, 4, 8. Because the binary WI finite automata with delay 3 and the weak inverse finite automata with delay 3 are the same in some sense[8], we investigate the structure of binary feedforward inverses with delay 3 via WI finite automata in case of $w_{3,M}$=1, 2, and 8, respectively, and give their corresponding characterizations.

We briefly recall some definitions and notations. Let $M=\langle X,Y,S,\delta,\lambda\rangle$ be an FA, $s\in S$. If for any $\alpha=x_0x_1\ldots x_l$ in X^* of length $l+1$, x_0 can be uniquely determined by s and $\lambda(s,\alpha)$, then s is called a $\le l$-step state, $l\ge 0$. If s is a $\le l$-step state and not a $\le (l-1)$-step state, then s is called an l-step state. Especially, if s is a ≤ 0-step state, then s is called a 0-step state. Denote $S_0=\{s|s\in S, |W_{3,s}^M|=w_{3,M}\}$. Throughout this paper, an FA M is referred to $M=\langle X,Y,S,\delta,\lambda\rangle$, which has the property of $|X|=|Y|=2$. $C(M_a,f)=\langle X,Y,X^c\times S_a,\delta,\lambda\rangle$ is called a c-order SIM FA, if $\delta(\langle x_{-c},\ldots,x_{-1},s_a\rangle,x_0)=\langle x_{-c+1},\ldots,x_0,\delta_a(s_a)\rangle$, $\lambda(\langle x_{-c},\ldots,x_{-1},s_a\rangle,x_0)=f(x_{-c},\ldots,x_0,\lambda_a(s_a))$, where $M_a=\langle S_a,Y_a,\delta_a,\lambda_a\rangle$ is an autonomous FA, f is a mapping from $X^{c+1}\times\lambda_a(S_a)$ to Y. M_a is called cyclic, if $S_a=\{s_{a,1},\ldots,s_{a,na}\}$, $\delta_a(s_{a,i})=s_{a,i+1}$ for $i=1,\ldots,n_a-1$, $\delta_a(s_{a,na})=s_{a,1}$, and $\lambda_a(s_a)=s_a$ for any $s_a\in S_a$. For those terminologies not explained here, readers are referred to Refs.[1,8].

2 Binary WI SIM Finite Automata with Delay 3 of Which $w_{3,M}$=2

Let Ω stand for the condition: Let M be an WIFA, $w_{3,M}=2$, s_i and s_{ij} be the successor states of $s\in S_0$ and s_i $(i,j=1,2)$, respectively, $s_1\ne s_2$.

Lemma 1. Assume that Ω holds. If s is a 0-step state, then $|\lambda(s_i,X)|=|\lambda(s_{ij},X)|=1$, $\lambda(s_{i1},X)=\lambda(s_{i2},X)$.

Proof: Since s is a 0-step state, $|\lambda(s,X)|=2$. Since $s\in S_0$, $|\lambda(s_i,X)|=|\lambda(s_{ij},X)|=1$, $\lambda(s_{i1},X)=\lambda(s_{i2},X)$ $(i,j=1,2)$.

Lemma 2. Assume that Ω holds, then s is a 1-step state iff $|\lambda(s,X)|=|\lambda(s_i,X)|=1$ $(i=1,2)$, $\lambda(s_1,X)\ne\lambda(s_2,X)$. Furthermore, $|\lambda(s_{ij},X)|=1$, $\lambda(s_{i1},X)=\lambda(s_{i2},X)$ $(i,j=1,2)$.

Proof: "⇐" It is obvious. "⇒" Since s is a 1-step state, $|\lambda(s,X)|=1$. First, $|\lambda(s_i,X)|=1$ $(i=1,2)$ (Otherwise, there exist x_0x_1 and $x_0'x_1'$ such that $\lambda(s,x_0x_1)=\lambda(s,x_0'x_1')$, $x_0\ne x_0'$, a contradiction). By the definition of 1-step state, $\lambda(s_1,X)\ne\lambda(s_2,X)$. Since $s\in S_0$, $|\lambda(s_{ij},X)|=1$, $\lambda(s_{i1},X)=\lambda(s_{i2},X)$ $(i,j=1,2)$.

Lemma 3. Assume that Ω holds, then s_1 is a 0-step state iff s_2 is a 0-step state.

Proof: Since $s\in S_0$, using Proposition 2 in Ref.[6], $s_i\in S_0$ $(i=1,2)$. By symmetry we need only to prove "⇒". Suppose that s_1 is a 0-step state while s_2 isn't. By Lemma 1, s isn't a 0-step state. Thus $\lambda(s_1,X)=Y$, $|\lambda(s_2,X)|=|\lambda(s,X)|=1$. Since $s\in S_0$, $|\lambda(s_{2i},X)|=1$ $(i=1,2)$, $\lambda(s_{21},X)=\lambda(s_{22},X)$. Note $s_2\in S_0$, $\cup_{i,j=1,2}\lambda(s_{2ij},X)=Y$. Since $\lambda(s_2,X)\subset\lambda(s_1,X)$, there exists $x_1\in X$ such that $\lambda(s_1,x_1)=\lambda(s_2,x_1')$ for any $x_1'\in X$. Denote $s_{11}=\delta(s_1,x_1)$. Since $s\in S_0$, $\lambda(s_{21},X)=\lambda(s_{22},X)=\{\lambda(s_{11},x_2)\}$. Let $s_{111}=\delta(s_{11},x_2)$, then $\lambda(s_{111},X)\subseteq\cup_{i,j=1,2}\lambda(s_{2ij},X)$. There exist x_3 and x_3' such that $\lambda(s_{111},x_3)=\lambda(s_{2ij},x_3')$. Let $s_1=\delta(s,x_0)$, $s_2=\delta(s,x_0')$, $s_{2ij}=\delta(s_{2i},x_2')$, $x_0\ne x_0'$. Then $\lambda(s,x_0x_1x_2x_3)=\lambda(s,x_0'x_1'x_2'x_3')$, $x_0\ne x_0'$, which contradicts that M is weakly invertible with delay 3. Hence "⇒" follows.

Lemma 4. Assume that Ω holds, then s is a 2-step state iff (a), (b) and (c) hold, where (a) $|\lambda(s,X)|=1$; (b) $|\lambda(s_i,X)|=1$ $(i=1,2)$, $\lambda(s_1,X)=\lambda(s_2,X)$; (c) $|\lambda(s_{ij},X)|=1$ $(i,j=1,2)$, $\lambda(s_{i1},X)=\lambda(s_{i2},X)$ $(i=1,2)$, $\lambda(s_{11},X)\ne\lambda(s_{22},X)$.

Proof: "⇐" It is obvious."⇒" Since s is a 2-step state, $|\lambda(s,X)|=1$. (a) Follows; (b) Suppose that $|\lambda(s_i,X)|\ne 1$ for some $i\in\{1,2\}$, then s_i is a 0-step state. By Lemma 3, s_1 and s_2 are 0-step states. Thus $\lambda(s_1,X)=\lambda(s_2,X)=Y$. Then there exist $x_1, x_1' \in X$ such that $\lambda(s_1,x_1)=\lambda(s_2,x_1')$. Let $s_{11}=\delta(s_1,x_1)$, $s_{21}=\delta(s_2,x_1')$. Since $s\in S_0$, by Lemma 1, there exist $x_2, x_2' \in X$ such that $\lambda(s_{11},x_2)=\lambda(s_{21},x_2')$. Let $s_1=\delta(s,x_0)$, $s_2=\delta(s,x_0')$, $x_0\neq x_0'$. Then $\lambda(s,x_0x_1x_2)=\lambda(s,x_0'x_1'x_2')$, $x_0\neq x_0'$, a contradiction. Thus $|\lambda(s_i,X)|=1$ (i=1,2). Since s is a 2-step state, by Lemma 2, $\lambda(s_1,X)=\lambda(s_2,X)$; (c) Since s is a 2-step state, using (a) and (b) $|\lambda(s_{ij},X)|=1$ and $\lambda(s_{i1},X)=\lambda(s_{i2},X)$ (i,j=1,2). Note $s\in S_0$, $\lambda(s_{11},X)\neq\lambda(s_{22},X)$. Thus (c) follows.

Lemma 5. Assume that Ω holds. If s is a 3-step state, then s_1 is not a 2-step state.

Proof: Suppose that s_1 is a 2-step state. By Lemma 3 s_2 is not a 0-step state, then $|\lambda(s_2,X)|=1$. Since s is not a 1-step state, by Lemma 2, $|\lambda(s,X)|=|\lambda(s_i,X)|=1$ (i=1,2) and $\lambda(s_1,X)=\lambda(s_2,X)$. Since s_1 is a 2-step state, by Lemma 4, $|\lambda(s_{1j},X)|=1$ (j=1,2), $\lambda(s_{11},X)=\lambda(s_{12},X)$ and $\cup_{i,j=1,2}\lambda(s_{1ij},X)=Y$. It is easy to see whether s_{11} is a 0-step state or not, $\lambda(s_{11},X)=\lambda(s_{12},X)\subset\lambda(s_{21},X)\cup\lambda(s_{22},X)=Y$. Thus there exist x_2 and x_2' such that $\{\lambda(s_{2k},x_2')\}=\lambda(s_{11},X)=\lambda(s_{12},X)$ for some $k\in\{1,2\}$. Let $s_{2k1}=\delta(s_{2k},x_2')$, since $\lambda(s_{2k1},x_3')\in Y=\cup_{i,j=1,2}\lambda(s_{1ij},X)$, there exists $x_3\in X$ such that $\lambda(s_{2k1},x_3')=\lambda(s_{1ij},x_3)$ for some $i,j\in\{1,2\}$. Let $s_1=\delta(s,x_0)$, $s_2=\delta(s,x_0')$, $s_{1i}=\delta(s_1,x_1)$, $s_{2k}=\delta(s_2,x_1')$, $s_{1ij}=\delta(s_{1i},x_2)$, $x_0\neq x_0'$. Then $\lambda(s,x_0x_1x_2x_3)=\lambda(s,x_0'x_1'x_2'x_3')$, $x_0\neq x_0'$, which contradicts that s is a 3-step state.

Lemma 6. Assume that Ω holds. If s_1 is a 0-step state, then s is a 3-step state, $|\lambda(s_{ij},X)|=|\lambda(s_{ijk},X)|=1$ and $\lambda(s_{ij1},X)=\lambda(s_{ij2},X)$ (i,j,k=1,2). Denote $\{e_1\}=\lambda(s_{11},X)$, $\{e_2\}=\lambda(s_{12},X)$, $\{e_3\}=\lambda(s_{21},X)$, $\{e_4\}=\lambda(s_{22},X)$, $\{e_5\}=\lambda(s_{111},X)$, $\{e_6\}=\lambda(s_{121},X)$, $\{e_7\}=\lambda(s_{211},X)$, $\{e_8\}=\lambda(s_{221},X)$, then the following statements hold. (1) If $\lambda(s_1,x)=\lambda(s_2,x')$, then $e_1=e_3$, $e_5\neq e_7$; (2) $e_1=e_2$ iff $e_3=e_4$, and if $e_1=e_2$, then $e_1=e_2=e_3=e_4$; if $e_1\neq e_2$, then $\lambda(s_1,x)=\lambda(s_2,x')$ iff $e_1=e_3$; (3) $e_5=e_6$ iff $e_7=e_8$. And if $e_5=e_6$, then $e_5\neq e_7$; if $e_5\neq e_6$, then $e_5\neq e_7$ iff $\lambda(s_1,x)=\lambda(s_2,x')$ and $e_1=e_3$, where $s_{11}=\delta(s_1,x)$, $s_{21}=\delta(s_2,x')$.

Proof: Since s_1 is a 0-step state, by Lemma 3, s_2 is a 0-step state. By Lemma 1, $|\lambda(s_{ij},X)|=|\lambda(s_{ijk},X)|=1$, $\lambda(s_{ij1},X)=\lambda(s_{ij2},X)$ (i,j,k=1,2). Since M is WI with delay 3, s is an l-step state ($0\leq l\leq 3$). By Lemmas 1, 2 and 4, s is a 3- step state. Assume $\lambda(s_1,x)=\lambda(s_2,x')$, and let $s_{11}=\delta(s_1,x)$, $s_{21}=\delta(s_2,x')$. Since $s\in S_0$, $e_1=e_2$. Since s is a 3-step state, $e_5\neq e_7$. Thus (1) follows.

(2) By symmetry we need only to prove "⇒". Suppose $e_1=e_2$ and $e_3\neq e_4$, then $|W_{3,s}^M|=3$. This contradicts $s\in S_0$. Thus "⇔"follows. Clearly, by (1) if $e_1=e_2$ then $e_1=e_2=e_3=e_4$. Let $e_1\neq e_2$, $e_1=e_3$, then $e_3\neq e_4$. Now suppose $\lambda(s_1,x)\neq\lambda(s_2,x')$, where $s_{11}=\delta(s_1,x)$, $s_{21}=\delta(s_2,x')$. Then $\lambda(s_1,x)=\lambda(s_2,x'')$, $x'\neq x''$. Using (1), $e_1=e_4$. Thus $e_3=e_4$, a contradiction. Combining with (1), $\lambda(s_1,x)=\lambda(s_2,x')$ iff $e_1=e_3$.

(3) By symmetry we need only to prove "⇒". Suppose $e_5=e_6$ and $e_7\neq e_8$. Since $e_5=e_6\in\{e_7,e_8\}$, $e_5=e_6=e_7$ or e_8. Without loss of generality, let $e_5=e_6=e_7$. Let $s_{11}=\delta(s_1,x)$, $s_{12}=\delta(s_1,x_1)$, $s_{21}=\delta(s_2,x')$, $x\neq x_1$. By (1), $\lambda(s_1,x)\neq\lambda(s_2,x')$, $\lambda(s_1,x_1)\neq\lambda(s_2,x')$. Thus $\lambda(s_2,x')\notin\{\lambda(s_1,x), \lambda(s_1,x_1)\}=Y$, a contradiction. Thus "⇔"follows. Since s is a 3-step state, clearly, if $e_5=e_6$ then $e_5\neq e_7$. Now assume $e_5\neq e_6$. To prove "⇐", it is immediate from (1). To prove "⇒", suppose $e_5\neq e_7$, $\lambda(s_1,x)\neq\lambda(s_2,x')$, where $s_{11}=\delta(s_1,x)$, $s_{21}=\delta(s_2,x')$. Then $e_6=e_7$. Let $s_{12}=\delta(s_1,x_1)$, $x_1\neq x$. By (1), $\lambda(s_1,x_1)\neq\lambda(s_2,x')$. Thus $\lambda(s_1,x_1)\notin\{\lambda(s_1,x),\lambda(s_1,x_1)\}=Y$, a contradiction. Combining with (1) "⇒"follows.

Lemma 7. Assume that Ω holds. If s_1 is a 1-step state, then s is a 3-step state, s_2 is not a 0-step state, $|\lambda(s_1,X)|=|\lambda(s_{1j},X)|=|\lambda(s_{1jk},X)|=1$ and $\lambda(s_{1j1},X)=\lambda(s_{1j2},X)$ (j,k=1,2). Furthermore, (1) and (2) hold. (1) If some s_{2k} is not a 0-step state, then s_2 is a 1-step state, $|\lambda(s_2,X)|=|\lambda(s_{2j},X)|=|\lambda(s_{2jk},X)|=1$ and $\lambda(s_{2j1},X)=\lambda(s_{2j2},X)$ (j,k=1,2). Denote $\{e_1\}=\lambda(s_{11},X)$, $\{e_2\}=\lambda(s_{12},X)$, $\{e_3\}=\lambda(s_{21},X)$, $\{e_4\}=\lambda(s_{22},X)$, $\{e_5\}=\lambda(s_{111},X)$, $\{e_6\}=\lambda(s_{121},X)$, $\{e_7\}=\lambda(s_{211},X)$, $\{e_8\}=\lambda(s_{221},X)$, then (a) If $e_1=e_3$ then $e_5\neq e_7$; (b) $e_5=e_6$ iff $e_7=e_8$. And if $e_5=e_6$ then $e_5\neq e_7$; if $e_5\neq e_6$, then $e_1=e_3$ iff $e_5\neq e_7$; (2) If some s_{2k} is a 0-step state, then s_2 is a 3-step state, s_{2j} is a 0-step state (j=1,2), $|\lambda(s_{2jk},X)|=1$ (j,k=1,2). Denote $\{e_9\}=\lambda(s_{211},X)$, $\{e_{10}\}=\lambda(s_{221},X)$, $\{e_{11}\}=\lambda(s_{212},X)$, $\{e_{12}\}=\lambda(s_{222},X)$, let $e_1=\lambda(s_{21},x)=\lambda(s_{22},x')$, then (a) $e_5\neq e_9$, $e_9=e_{10}$, $e_{11}=e_{12}$, where $s_{211}=\delta(s_{21},x)$, $s_{221}=\delta(s_{22},x')$; (b) $e_5=e_6$ iff $e_9=e_{10}=e_{11}=e_{12}$. And if $e_5=e_6$, then $e_5\neq e_9$; if $e_5\neq e_6$, then $e_1=\lambda(s_{21},x)=\lambda(s_{22},x')$ iff $e_5\neq e_9$.

Proof: Since s_1 is a 1-step state, by Lemma 3 s_2 is not a 0-step state, then $|\lambda(s_2,X)|=1$, by Lemma 2, $|\lambda(s_1,X)|=|\lambda(s_{1j},\ )|=|\lambda(s_{1jk},X)|=1$ and $\lambda(s_{1j1},X)=\lambda(s_{1j2},X)$ (j,k=1,2). Since M is weakly invertible with delay 3, s is a

l-step state ($0\le l\le 3$). By Lemmas 1, 2, and 4, s is a 3-step state. Then $|\lambda(s,X)|=1$. By Lemma 2, $\lambda(s_1,X)=\lambda(s_2,X)$. Since $s\in S_0$, by Proposition 2 in Ref.[6], $s_2\in S_0$.

(1). Assume some s_{2k} is not a 0-step state, by Lemma 3, s_{2j} is not a 0-step state (j=1,2), then $|\lambda(s_{2j},X)|=1$ (j=1,2). Suppose s_2 is not a 1-step state. Note $s_2\in S_0$, $\cup_{i,j=1,2}\lambda(s_{2ij},X)=Y$, then $\{e_5,e_6\}\subseteq\cup_{i,j=1,2}\lambda(s_{2ij},X)$. On the other hand, $\lambda(s_1,X)=\lambda(s_2,X)\subset Y=\{e_1,e_2\}$. Then there exist $x_0x_1x_2x_3$ and $x'_0x'_1x'_2x'_3$ such that $\lambda(s,x_0x_1x_2x_3)=\lambda(s,x'_0x'_1x'_2x'_3)$, $x_0\ne x'_0$, a contradiction. Thus s_2 is a 1-step state. By Lemma 2, $|\lambda(s_2,X)|=|\lambda(s_{2j},X)|=|\lambda(s_{2jk},X)|=1$, $\lambda(s_{2j1},X)=\lambda(s_{2j2},X)$ (j,k =1,2), and $\lambda(s_{21},X)\ne\lambda(s_{22},X)$. Since s is a 3-step state, it is easy to see that (a) follows; (b) By symmetry we need only to prove "⇒". Suppose $e_5=e_6$, $e_7\ne e_8$, then $e_5=e_6\in Y=\{e_7,e_8\}$. Thus $e_5=e_6=e_7$ or e_8. Without loss of generality let $e_5=e_6=e_7$, then $e_1\ne e_3$, $e_2\ne e_3$, i.e., $e_3\notin\{e_1,e_2\}=Y$, a contradiction. "⇔" follows. Since s is a 3-step state, by its definition, it is not difficult to see that the remainder of (b) hold.

(2). Assume that some s_{2k} is a 0-step state, by Lemma 3, s_{2j} is a 0-step state (j=1,2). By Lemma 1, $|\lambda(s_{2jk},X)|=1$ (j,k=1,2), by Lemma 6, s_2 is a 3-step state. Let $e_1=\lambda(s_{21},x)=\lambda(s_{22},x')$. Since s is a 3-step state, $e_5\ne e_9$. By Lemma 1, $e_9=e_{10}$, $e_{11}=e_{12}$, where $s_{211}=\delta(s_{21},x)$, $s_{221}=\delta(s_{22},x')$. Since $e_9=e_{10}$, $e_{11}=e_{12}$, to prove "⇒", suppose $e_5=e_6$, $e_9\ne e_{11}$, then $e_5=e_6\in\{e_9,e_{11}\}=Y$. On the other hand, $\{e_1,e_3\}=\lambda(s_{21},X)=Y$. There exist $x_0x_1x_2x_3$ and $x'_0x'_1x'_2x'_3$ such that $\lambda(s,x_0x_1x_2x_3)=\lambda(s,x'_0x'_1x'_2x'_3)$, $x_0\ne x'_0$, a contradiction. Thus "⇒"follows. By the same arguments "⇐"follows. Since s is a 3-step state, clearly, if $e_5=e_6$ then $e_5\ne e_9$. Now assume $e_5\ne e_6$, by the same arguments as Lemma 6, the remainder of (b) hold.

Lemma 8. Assume that Ω holds. Then s, s_i (i=1,2) are 3-step states iff s_{ij} is a 0-step state (i,j=1,2). Assume s, s_i (i=1,2) are 3-step states, then $|\lambda(s_{ijk},X)|=1$ (i,j,k=1,2). Denote $\{e_{ijk}\}=\lambda(s_{ijk},X)$ (i,j,k=1,2), then (a) $e_{i11}=e_{i12}$ iff $e_{i21}=e_{i22}$ (i=1,2); (b) $e_{111}=e_{112}=e_{121}=e_{122}$ iff $e_{211}=e_{212}=e_{221}=e_{222}$. If $e_{111}=e_{112}=e_{121}=e_{122}$, then $e_{111}\ne e_{211}$; if $e_{111}\ne e_{112}$, then $\lambda(s_{1j},x)=\lambda(s_{2k},x')$ iff $e_{1j1}\ne e_{2k1}$.

Proof: "⇒" Since s, s_i (i=1,2) are 3-step states, $|\lambda(s,X)|=|\lambda(s_i,X)|=1$ (i=1,2), $\lambda(s_1,X)=\lambda(s_2,X)$. Since $s\in S_0$, by Proposition 2 in Ref.[6], $s_i\in S_0$ (i=1,2). By Lemma 3, we consider three cases. Case 1. s_{ij} is a 0-step state (i,j=1,2); Case 2. s_{ij} (i,j=1,2) are not 0-step states; Case 3. Some s_{mj} is a 0-step state while some s_{nk} is not a 0-step state, $m\ne n$. Next we prove Cases 2 and 3 don't occur. Suppose Case 2 holds. Since s_j (j=1,2) are 3-step states, by Lemma 2, $\lambda(s_{i1},X)=\lambda(s_{i2},X)$ (i=1,2). Note $s\in S_0$, by Lemma 4, s is a 2-step state, a contradiction. Suppose Case 3 holds and let s_{mj} be a 0-step state, s_{nk} not be. Since s_n is a 3-step state, $\lambda(s_{n1},X)=\lambda(s_{n2},X)$. Note $s_n\in S_0$, $\cup_{j,k=1,2}\lambda(s_{njk},X)=Y$. Clearly, $\lambda(s_{n1},X)=\lambda(s_{n2},X)\subset Y=\lambda(s_{m1},X)=\lambda(s_{m2},X)$, $\lambda(s_{mjk},X)\subset\cup_{j,k=1,2}\lambda(s_{njk},X)$. There exist $x_0x_1x_2x_3$ and $x'_0x'_1x'_2x'_3$ such that $\lambda(s,x_0x_1x_2x_3)=\lambda(s,x'_0x'_1x'_2x'_3)$, $x_0\ne x'_0$, a contradiction. Thus "⇒"follows. To prove "⇐", assume that s_{ij} is a 0-step state (i,j=1,2). By Lemma 6, s_i (i=1,2) are 3-step states. Since s is an l-step state ($0\le l\le 3$), by Lemmas 1, 2, and 4, s is a 3-step state. Assume that s, s_i (i=1,2) are 3-step states, then s_{ij} (i,j=1,2) are 0-step states, by Lemma 1, $|\lambda(s_{ijk},X)|=1$ (i,j,k=1,2). (a) It is immediate from Lemma 6. (b) By the same arguments as Lemma 7, (b) follows.

Lemma 9. Assume that Ω holds. If some s_{mj} is a 0-step state, then s and s_m are 3-step states, s_n is a 1-step state or a 3-step state ($m\ne n$).

Proof: Assume that s_{mj} is a 0-step state, by Lemma 6, s_m is a 3-step state. By Lemma 3, s_n is not a 0-step state. Since M is weakly invertible with delay 3, s is an l-step state ($0\le l\le 3$). By Lemmas 1, 2, and 4, s is a 3-step state. Since s_n is an l-step state ($1\le l\le 3$), by Lemma 5, s_n is not a 2-step state. Therefore by Lemmas 7 and 8, s_n is a 1-step state or a 3-step state.

Lemma 10. Assume that Ω holds. Then $|\lambda(s_{1j},X)|=1$ (j=1,2) and $\lambda(s_{11},X)=\lambda(s_{12},X)$ iff $|\lambda(s_{2j},X)|=1$ (j=1,2) and $\lambda(s_{21},X)=\lambda(s_{22},X)$.

Proof: By symmetry we need only to prove "⇒". Assume that $|\lambda(s_{1j},X)|=1$ (j=1,2), $\lambda(s_{11},X)=\lambda(s_{12},X)$. By Lemma 2, s_1 is not a 1-step state. Next we consider three cases of s_1. Case 1. s_1 is a 0-step state. By Lemma 6, the conclusion follows; Case 2. s_1 is a 2-step state. By Lemmas 1, 2, 4, and 5, there are three subcases of s to discuss: s is a 0-step state or a 1-step state, or 2-step state. It is immediate from Lemmas 1or 2, or 4, respectively; Case 3. s_1 is a 3-step state. By Lemmas 1, 2, 4, 7, and 8, there are three subcases of s to discuss: s is a 0-step state or a 1-step state, or 2-step state. It is immediate from Lemmas 1or 2, or 4, respcectively.

Lemma 11. Assume that Ω holds. Then $|\lambda(s_{1ij},X)|=1$ $(i,j=1,2)$ and $\lambda(s_{111},X)=\lambda(s_{112},X)=\lambda(s_{121},X)=\lambda(s_{122},X)$ iff $|\lambda(s_{2ij},X)|=1$ $(i,j=1,2)$ and $\lambda(s_{211},X)=\lambda(s_{212},X)=\lambda(s_{221},X)=\lambda(s_{222},X)$. If this case occurs, then $\lambda(s_{111},X)=\lambda(s_{112},X)=\lambda(s_{121},X)=\lambda(s_{122},X)\neq\lambda(s_{211},X)=\lambda(s_{212},X)=\lambda(s_{221},X)=\lambda(s_{222},X)$.

Proof: By symmetry we need only to prove "$\Rightarrow$". Assume $|\lambda(s_{1ij},X)|=1$ $(i,j=1,2)$, $\lambda(s_{111},X)=\lambda(s_{112},X)=\lambda(s_{121},X)=\lambda(s_{122},X)$, by Lemma 4, s_1 is not a 2-step state. Next we consider three cases of s_1. Case 1. s_1 is a 0-step state; Case 2. s_1 is a 1-step state; Case 3. s_1 is a 3-step state. In the first two cases, it is immediate from Lemmas 8 and 7, respectively. In Case 3, since $s_1\in S_0$, $\lambda(s_{11},X)\cup\lambda(s_{12},X)=Y$. By Lemma 3, s_{1j} $(j=1,2)$ are 0-step states. By Lemma 9, s is a 3-step state, and s_2 is a 3-step state or a 1-step state. Thus it is immediate from Lemmas 8 and 7, respectively.

Lemma 12. Let M be a c-order SIM FA $C(M_a,f)$, $M_a=\langle S_a,Y_a,\delta_a,\lambda_a\rangle$ be cyclic, $X=Y=\{0,1\}$, $w_{3,M}=2$, $c\geq 3$, if M is WI with delay 3, then there exist mappings h_0 from $X^{c-1}\times S_a$ to $\{0,1\}$, h_1 from $X^{c-2}\times S_a$ to $\{0,1\}$, h_2 from $X^{c-3}\times S_a$ to $\{0,1\}$, f_0 from $X^c\times S_a$ to Y, f_1 from $X^{c-1}\times S_a$ to Y, f_2 from $X^{c-2}\times S_a$ to Y, f_3 from $X^{c-3}\times S_a$ to Y, such that

(2.1) $h_0(x_{-c},\dots,x_{-2},s_a)=0\rightarrow h_0(x_{-c+1},\dots,x_{-1},\delta_a(s_a))=1\wedge h_1(x_{-c+2},\dots,x_{-1},\delta_a^2(s_a))=1$, $h_0(x_{-c},\dots,x_{-2},s_a)=1\wedge h_0(x_{-c+1},\dots,x_{-1},\delta_a(s_a))=1\wedge h_1(x_{-c+1},\dots,x_{-2},\delta_a(s_a))=0\rightarrow h_1(x_{-c+2},\dots,x_{-1},\delta_a^2(s_a))=1$, $h_0(x_{-c},\dots,x_{-2},s_a)=1\wedge h_1(x_{-c+1},\dots,x_{-2},\delta_a(s_a))=1\rightarrow h_2(x_{-c+2},\dots,x_{-2},\delta_a^2(s_a))=0$, $h_0(x_{-c},\dots,x_{-2},s_a)=0\wedge h_1(x_{-c+1},\dots,x_{-2},\delta_a(s_a))=1\rightarrow h_2(x_{-c+1},\dots,x_{-3},\delta_a(s_a))=1$, $h_0(x_{-c},\dots,x_{-3},0,s_a)=0\wedge h_0(x_{-c},\dots,x_{-3},1,s_a)=0\wedge h_1(x_{-c+1},\dots,x_{-3},x_{-2},\delta_a(s_a))=0\rightarrow h_1(x_{-c+1},\dots,x_{-3},x'_{-2},\delta_a(s_a))=0(x_{-2}\neq x'_{-2})$, $h_2(x_{-c},\dots,x_{-4},s_a)=1\rightarrow h_1(x_{-c},\dots,x_{-3},s_a)=1$, $h_1(x_{-c},\dots,x_{-3},s_a)=1\rightarrow h_0(x_{-c},\dots,x_{-2},s_a)=1$.

(2.2) $f_0(x_{-c},\dots,x_{-2},0,s_a)+f_0(x_{-c},\dots,x_{-2},1,s_a)=h_3(x_{-c+1},\dots,x_{-2},\delta_a(s_a))$, if $h_0(x_{-c},\dots,x_{-2},s_a)=0\wedge h_1(x_{-c+1},\dots,x_{-2},\delta_a(s_a))=0$; $h_3(x_{-c},\dots,x_{-3},s_a)=h_4(x_{-c+1},\dots,x_{-2},\delta_a(s_a))+1$, if $h_0(x_{-c},\dots,x_{-3},0,s_a)=1\wedge h_0(x_{-c},\dots,x_{-3},1,s_a)=1\wedge h_1(x_{-c},\dots,x_{-3},s_a)=0\wedge h_2(x_{-c+1},\dots,x_{-3},\delta_a(s_a))=0$; $f_0(x_{-c},\dots,x_{-3},0,0,s_a)+f_0(x_{-c},\dots,x_{-3},1,0,s_a)=f_1(x_{-c+1},\dots,x_{-3},0,0,\delta_a(s_a))+f_1(x_{-c+1},\dots,x_{-3},1,0,\delta_a(s_a))+1$, if $h_0(x_{-c},\dots,x_{-3},0,s_a)=0\wedge h_0(x_{-c},\dots,x_{-3},1,s_a)=0\wedge h_1(x_{-c+1},\dots,x_{-2},\delta_a(s_a))=0$; $f_0(x_{-c},\dots,x_{-3},x_{-2},0,s_a)+f_1(x_{-c},\dots,x_{-3},x'_{-2},s_a)=f_1(x_{-c+1},\dots,x_{-2},0,\delta_a(s_a))+f_2(x_{-c+1},\dots,x'_{-2},\delta_a(s_a))+1$, if $h_0(x_{-c},\dots,x_{-3},x_{-2},s_a)=0\wedge h_0(x_{-c},\dots,x_{-3},x'_{-2},s_a)=1\wedge h_1(x_{-c+1},\dots,x_{-2},\delta_a(s_a))=0$ $(x_{-2}\neq x'_{-2})$; $f_0(x_{-c},\dots,x_{-2},0,s_a)+f_0(x_{-c},\dots,x_{-2},1,s_a)=h_4(x_{-c+2},\dots,x_{-2},\delta_a^2(s_a))+1$, if $h_0(x_{-c},\dots,x_{-2},s_a)=0\wedge h_1(x_{-c+1},\dots,x_{-2},\delta_a(s_a))=1\wedge h_2(x_{-c+2},\dots,x_{-2},\delta_a^2(s_a))=0$.

$$(2.3)\ f(x_{-c},\dots,x_0,s_a)=\begin{cases} f_0(x_{-c},\dots,x_{-1},s_a)+x_0, & \text{if } h_0(x_{-c},\dots,x_{-2},s_a)=0;\\ f_1(x_{-c},\dots,x_{-2},s_a)+x_{-1}, & \text{if } h_0(x_{-c},\dots,x_{-2},s_a)=1\wedge h_1(x_{-c},\dots,x_{-3},s_a)=0;\\ f_2(x_{-c},\dots,x_{-3},s_a)+x_{-2}, & \text{if } h_1(x_{-c},\dots,x_{-3},s_a)=1\wedge h_2(x_{-c},\dots,x_{-4},s_a)=0;\\ f_3(x_{-c},\dots,x_{-4},s_a)+x_{-3}, & \text{if } h_2(x_{-c},\dots,x_{-4},s_a)=1.\end{cases}$$

where (2.4) $h_3(x_{-c},\dots,x_{-3},s_a)=f_1(x_{-c},\dots,x_{-3},0,s_a)+f_1(x_{-c},\dots,x_{-3},1,s_a)$, $h_4(x_{-c},\dots,x_{-4},s_a)=f_2(x_{-c},\dots,x_{-4},0,s_a)+f_2(x_{-c},\dots,x_{-4},1,s_a)$.

Proof: Denote $T_1(x_{-2})=(x_{-c},\dots,x_{-2},s_a)$, $T_1(x_{-2}x_{-1})=(x_{-c+1},\dots,x_{-1},\delta_a(s_a))$, $T_1(x_{-2}x_{-1}x_0)=(x_{-c+2},\dots,x_0,\delta_a^2(s_a))$, $T_1(x_{-2}x_{-1}x_0x_1)=(x_{-c+3},\dots,x_1,\delta_a^3(s_a))$, $T_2(x_{-3})=(x_{-c},\dots,x_{-3},s_a)$, $T_2(x_{-3}x_{-2})=(x_{-c+1},\dots,x_{-2},\delta_a(s_a))$, $T_2(x_{-3}x_{-2}x_{-1})=(x_{-c+2},\dots,x_{-1},\delta_a^2(s_a))$, $T_2(x_{-3}x_{-2}x_{-1}x_0)=(x_{-c+3},\dots,x_0,\delta_a^3(s_a))$, $T_3(x_{-4})=(x_{-c},\dots,x_{-4},s_a)$, $T_3(x_{-4}x_{-3})=(x_{-c+1},\dots,x_{-3},\delta_a(s_a))$, $T_3(x_{-4}x_{-3}x_{-2})=(x_{-c+2},\dots,x_{-2},\delta_a^2(s_a))$, $T_3(x_{-4}x_{-3}x_{-2}x_{-1})=(x_{-c+3},\dots,x_{-1},\delta_a^3(s_a))$, $s(x_{-2}x_{-1})=\langle x_{-c},\dots,x_{-1},s_a\rangle$, $s(x_{-2}x_{-1}x_0)=\langle x_{-c+1},\dots,x_0,\delta_a(s_a)\rangle$, $s(x_{-2}x_{-1}x_0x_1)=\langle x_{-c+2},\dots,x_1,\delta_a^2(s_a)\rangle$, $s(x_{-2}x_{-1}x_0x_1x_2)=\langle x_{-c+3},\dots,x_2,\delta_a^3(s_a)\rangle$. Define $f_0(x_{-c},\dots,x_{-1},s_a)=f(x_{-c},\dots,x_{-1},0,s_a)$, $f_1(x_{-c},\dots,x_{-2},s_a)=f(x_{-c},\dots,x_{-2},0,0,s_a)$, $f_2(x_{-c},\dots,x_{-3},s_a)=f(x_{-c},\dots,x_{-3},0,0,0,s_a)$, $f_3(x_{-c},\dots,x_{-4},s_a)=f(x_{-c},\dots,x_{-4},0,0,0,0,s_a)$. $h_0(T_1(x_{-2}))=1$ iff $s(x_{-2}^0)$ is not a 0-step state, $h_1(T_2(x_{-3}))=1$ iff $f(x_{-c},\dots,x_{-3},0,x_{-1},x_0,s_a)$ doesn't rely on x_{-1} and x_0, $h_2(T_3(x_{-4}))=1$ iff $f(x_{-c},\dots,x_{-4},0,x_{-2},x_{-1},x_0,s_a)$ doesn't rely on x_{-2},x_{-1},x_0. Clearly, $h_2(T_3(x_{-4}))=1\rightarrow h_1(T_2(x_{-3}))=1$,

$h_1(T_2(x_{-3}))=1\to h_0(T_1(x_{-2}))=1$.Since M_a is cyclic, $M=C(M_a,f)$ is strongly conn-ected. Then $|W^M_{3,s}|=2$, $\forall s\in S$.

Clearly, by Lemmas 3, 10, 11, $h_0(T_1(x_{-2}))=1$ iff $s(x^1_{-2})$ is not a 0-step state, $h_1(T_2(x_{-3}))=1$iff $f(x_{-c},\ldots,x_{-3},1,x_{-1},x_0,s_a)$ doesn't rely on x_{-1} and x_0, $h_2(T_3(x_{-4}))=1$ iff $f(x_{-c},\ldots,x_{-4},1,x_{-2},x_{-1},x_0,s_a)$ doesn't rely on x_{-2},x_{-1},x_0.

To prove (2.1), assume $h_0(T_1(x_{-2}))=0$, then By Lemma 1, $h_0(T_1(x_{-2}x_{-1}))=1\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}))=1$. Assume $h_0(T_1(x_{-2}))=1\wedge h_0(T_1(x_{-2}x_{-1}))=1\wedge h_1(T_2(x_{-3}x_{-2}))=0$, then $|\lambda(s(x_{-2}x_{-1}),X)|=|\lambda(s(x_{-2}x_{-1}x_0),X)|=1$, $\lambda(s(x_{-2}\,x^0_{-1}),0)\neq\lambda(s(x_{-2}\,x^1_{-1}),0)$. Thus $s(x_{-2}x_{-1})$ is a 1-step state. By Lemma 2, $h_1(T_2(x_{-3}x_{-2}x_{-1}))=1$. Assume $h_0(T_1(x_{-2}))=1\wedge h_1(T_2(x_{-3}x_{-2}))=1$, then $|\lambda(s(x_{-2}x_{-1}),X)|=1$, $\lambda(s(x_{-2}x_{-1}x_0),x_1)=\lambda(s(x_{-2}\,x^0_{-1}),0)$, $\forall x_0,x_1\in X$. Since $|W^M_{3,s(x_{-2},x_{-1})}|=2$, $\cup_{x_0,x_1\in X}\lambda(s(x_{-2}x_{-1}),X)=Y$, thus $h_2(T_3(x_{-4}x_{-3}x_{-2}))=0$. Assume $h_0(T_1(x_{-2}))=0\wedge h_1(T_2(x_{-3}x_{-2}))=1$, then $s(x^0_{-2})$, $s(x^1_{-2})$ are 0-step states, $\lambda(s(x_{-2}x_{-1}x_0),x_1)=\lambda(s(x_{-2}\,x^0_{-1}),0)$, $\forall x_{-1},x_0,x_1\in X$. By Lemma 6, $h_2(T_3(x_{-4}x_{-3}))=1$. Assume $h_0(T_1(0))=0\wedge h_0(T_1(1))=0\wedge h_1(T_2(x_{-3}x_{-2}))=0$, $s(x_{-2}x_{-1})$, $\forall x_{-2},x_{-1}\in X$ are 0-step states. By Lemma 8, $h_1(T_2(x_{-3}\,x'_{-2}))=0$ $(x_{-2}\neq x'_{-2})$.

To prove (2.2), assume $h_0(T_1(x_{-2}))=0\wedge h_1(T_2(x_{-3}x_{-2}))=0$, then $s(x^0_{-2})$, $s(x^1_{-2})$ are 0-step states. By Lemma 1, $|\lambda(s(x_{-2}x_{-1}x_0),X)|=1$, $\forall x_{-1},x_0\in X$. Since $h_1(T_2(x_{-3}x_{-2}))=0$, $\lambda(s(x_{-2}\,x^0_{-1}),0)\neq\lambda(s(x_{-2}\,x^1_{-1}),0)$, $\forall x_{-1}\in X$. By Lemma 6, $\lambda(s(x^0_{-2}),0)=\lambda(s(x^1_{-2}),0)$ iff $\lambda(s(x^{00}_{-2}),0)=\lambda(s(x^{10}_{-2}),0)$. Then $\lambda(s(x^0_{-2}),0)+\lambda(s(x^1_{-2}),0)=\lambda(s(x^{00}_{-2}),0)+\lambda(s(x^{10}_{-2}),0)$. Thus $f_0(x_{-c},\ldots,x_{-2},0,s_a)+f_0(x_{-c},\ldots,x_{-2},1,s_a)=h_3(T_2(x_{-3}x_{-2}))$. Assume $h_0(T_1(0))=1\wedge h_0(T_1(1))=1\wedge h_1(T_2(x_{-3}))=0\wedge h_2(T_3(x_{-4}x_{-3})=0$, then $|\lambda(s(x_{-2}x_{-1}),X)|=1$, $\forall x_{-2},x_{-1}\in X$. Since $h_1(T_2(x_{-3}))=0$, by Lemma 10, $\lambda(s(x^0_{-2}),0)\neq\lambda(s(x_{-2}1),0)$, $\forall x_{-2}\in X$. By Lemma 3, $\langle x_{-c-1},\ldots,x_{-3},i,\delta_a^{-1}(s_a)\rangle$ $(i=0,1)$ are 0-step states, or neither is, where $s(x_{-2}x_{-1})$ is the successor state of $\langle x_{-c-1},\ldots,x_{-3},i,\delta_a^{-1}(s_a)\rangle$, $\forall x_{-2},x_{-1}\in X$. In the first case, since $h_2(T_3(x_{-4}x_{-3})=0$, by Lemma 6, $\lambda(s(x_{-2}x_{-1}x_0),x_1)=\lambda(s(x_{-2}\,x^0_{-1}),0)$, $\forall x_{-k}\in X$ $(k=-2,-1,0,1)$, $\lambda(s(x^{00}_{-2}),0)\neq\lambda(s(x^{00}_{-2}),0)$, and $\lambda(s(00),0)=\lambda(s(10),0)$ iff $\lambda(s(000),0)\neq\lambda(s(100),0)$. Then $\lambda(s(00),0)+\lambda(s(10),0)=\lambda(s(000),0)+\lambda(s(100),0)+1$. Thus $f(x_{-c},\ldots,x_{-3},0,0,0,s_a)+f(x_{-c},\ldots,x_{-3},1,0,0,s_a)=f(x_{-c+1},\ldots,x_{-3},0,0,0,0,\delta_a(s_a))+f(x_{-c+1},\ldots,x_{-3},1,0,0,0,\delta_a(s_a))+1$, i.e., $h_3(T_2(x_{-3}))=h_4(T_2(x_{-3}x_{-2}))+1$, where $h_4(T_3(x_{-4}))=f_2(T_2(0))+f_2(T_2(1))$. In the second case, by Lemma 2, $\langle x_{-c-1},\ldots,x_{-3},i,\delta_a^{-1}(s_a)\rangle$ $(i=0,1)$ are 1-step states. By the same arguments and using Lemma 7, $h_3(T_2(x_{-3}))=h_4(T_2(x_{-3}x_{-2}))+1$. Assume $h_0(T_1(0))=0\wedge h_0(T_1(1))=0\wedge h_1(T_2(x_{-3}x_{-2}))=0$, using (2.1), $h_1(T_2(x_{-3}\,x'_{-2}))=0$ $(x'_{-2}\neq x_{-2})$. Since $h_0(T_1(x_{-2}))=0$, $\forall x_{-2}\in X$, $s(x^0_{-2})$ and $s(x^1_{-2})$ are 0-step states. By Lemma 1, $|\lambda(s(x_{-2}x_{-1}x_0),X)|=1$, $\forall x_{-2},x_{-1},x_0\in X$. Since $h_1(T_2(x_{-3}x_{-2}))=0$, by Lemma 6, $\lambda(s(x_{-2}\,x^0_{-1}),0)\neq\lambda(s(x_{-2}\,x^1_{-1}),0)$. By Lemma 8, $\lambda(s(00),0)=\lambda(s(10),0)$ iff $\lambda(s(000),0)\neq\lambda(s(100),0)$. Then $\lambda(s(00),0)+\lambda(s(10),0)=\lambda(s(000),0)+\lambda(s(100),0)+1$. Thus $f_0(x_{-c},\ldots,x_{-3},0,0,s_a)+f_0(x_{-c},\ldots,x_{-3},1,0,s_a)=f_1(T_1(00))+f_1(T_1(10))+1$. Assume $h_0(T_1(x_{-2}))=0\wedge h_0(T_1(x'_{-2}))=1\wedge h_1(T_2(x_{-3}x_{-2}))=0(x_{-2}\neq x'_{-2})$, then $s(x^0_{-2})$ and $s(x^1_{-2})$ are 0-step states. By Lemma 9, $\langle x_{-c-1},\ldots,x_{-2},\delta_a^{-1}(s_a)\rangle$ is a 3-step state, $\langle x_{-c-1},\ldots,x'_{-2},\delta_a^{-1}(s_a)\rangle$ is a 3-step state or a 1-step state $(x_{-2}\neq x'_{-2})$, where $s(x_{-2}x_{-1})$ is the successor state of $\langle x_{-c-1},\ldots,x_{-3},i,\delta_a^{-1}(s_a)\rangle$, $\forall x_{-2},x_{-1}\in X$. Since $h_0(T_1(x'_{-2}))=1$, $s(x'^0_{-2})$, $s(x'^1_{-2})$ are not 0-step states. By Lemma 8, $\langle x_{-c-1},\ldots,x'_{-2},\delta_a^{-1}(s_a)\rangle$ is a 1-step state. By Lemma 2, $\lambda(s(x'_{-2}\,x_{-1}x_0),x_1)=\lambda(s(x'_{-2}\,x^0_{-1}),0)$, $|\lambda(s(x'_{-2}\,x_{-1}),X)|=1$, $\forall x_{-1},x_0,x_1\in X$. Since $h_1(T_2(x_{-3}x_{-2}))=0$, by Lemma 6, $\lambda(s(x_{-2}\,x^0_{-1}),0)\neq\lambda(s(x_{-2}\,x^1_{-1}),0)$, $\forall x_{-1}\in X$. By Lemma 11, $\lambda(s(x'^{00}_{-2}),0)\neq\lambda(s(x'^{10}_{-2}),0)$. By Lemma 7, $\lambda(s(x^0_{-2}),0)=\lambda(s(x'^0_{-2}),0)$ iff $\lambda(s(x^{00}_{-2}),0)\neq\lambda(s(x'^{00}_{-2}),0)$. Then $\lambda(s(x^0_{-2}),0)+\lambda(s(x'^0_{-2}),0)=\lambda(s(x_{-2}00),0)+\lambda(s(x'^{00}_{-2}),0)+1$. Thus $f_0(x_{-c},\ldots,x_{-2},0,s_a)+f_1(T_1(x'_{-2}))=f_1(T_1(x^0_{-2}))+f_2(T_2(x_{-3}\,x'_{-2}))+1$. Assume $h_0(T_1(x_{-2}))=0\wedge h_1(T_2(x_{-3}x_{-2}))=1\wedge h_2(T_3(x_{-4}x_{-3}x_{-2}))=0$, then $s(x^0_{-2})$ and $s(x^1_{-2})$ are 0-step states. By Lemma 1, $\lambda(s(x_{-2}x_{-1}x_0x_1),x_2)=\lambda(s(x_{-2}x_{-1}x_00),0)$, $|\lambda(s(x_{-2}x_{-1}x_0),X)|=1$, $\forall x_{-1},x_0,x_1,x_2\in X$. Since $h_1(T_2(x_{-3}x_{-2}))=1$, by Lemma 6, $\lambda(s(x_{-2}x_{-1}x_0),x_1)=\lambda(s(x^{00}_{-2}),0)$, $\forall x_{-1},x_0,x_1\in X$. Since $h_2(T_3(x_{-4}x_{-3}x_{-2}))=0$, by Lemma 11, $\lambda(s(x_{-2}\,x^{00}_{-1}),0)\neq\lambda(s(x_{-2}\,x^{10}_{-1}),0)$, $\forall x_{-1}\in X$. Then by Lemma 6, $\lambda(s(x^0_{-2}),0)=\lambda(s(x^1_{-2}),0)$ iff $\lambda(s(x^{000}_{-2}),0)\neq\lambda(s(x^{100}_{-2}),0)$. Thus $f_0(x_{-c},\ldots,x_{-2},0,s_a)+f_0(x_{-c},\ldots,x_{-2},1,s_a)=h_4(T_3(x_{-4}x_{-3}x_{-2}))+1$.

To prove (2.3), assume $h_0(T_1(x_{-2}))=0$, then $s(x_{-2}^0)$ and $s(x_{-2}^1)$ are 0-step states. Clearly, $\lambda(s(x_{-2}x_{-1}),x_0)=\lambda(s(x_{-2}x_{-1}),0)+x_0$, $\forall x_{-1},x_0\in X$. Then $f(x_{-c},\ldots,x_0,s_a)=f_0(x_{-c},\ldots,x_{-1},s_a)+x_0$. Assume $h_0(T_1(x_{-2}))=1\wedge h_1(T_2(x_{-3}))=0$, then $\lambda(s(x_{-2}x_{-1}),x_0)=\lambda(s(x_{-2}x_{-1}),0)$, $\forall x_{-1}\in X$. Let $e=\lambda(s(x_{-2}x_{-1}),0)$, $x'_{-1}\neq x_{-1}$. Since $h_1(T_2(x_{-3}))=0$, $\lambda(s(x_{-2}x_{-1}),0)\neq\lambda(s(x_{-2}x'_{-1}),0)$. Thus $\lambda(s(x_{-2}x'_{-1}),0)=e+1$. Then $f(x_{-c},\ldots,x_0,s_a)=\lambda(s(x_{-2}x_{-1}),0)=\lambda(s(x_{-2}^0),0)+x_{-1}=f_1(T_1(x_{-2}))+x_{-1}$. Assume $h_1(T_2(x_{-3}))=1\wedge h_2(T_3(x_{-4}))=0$, then $\lambda(s(x_{-2}x_{-1}),x_0)=\lambda(s(x_{-2}^0),0)$, $\forall x_{-1},x_0\in X$. Let $e=\lambda(s(x_{-2}^0),0)$, $x'_{-2}\neq x_{-2}$. Since $h_2(T_3(x_{-4}))=0$, $\lambda(s(x_{-2}^0),0)\neq\lambda(s(x'^0_{-2}),0)$. Thus $\lambda(s(x'^0_{-2}),0)=e+1$. Then $f(x_{-c},\ldots,x_0,s_a)=\lambda(s(x_{-2}^0),0)=\lambda(s(00),0)+x_{-2}=f_2(T_2(x_{-3}))+x_{-2}$. Assume $h_2(T_3(x_{-4}))=1$, then $\lambda(s(x_{-2}x_{-1}),x_0)=\lambda(s(00),0)$, $\forall x_{-2},x_{-1},x_0\in X$. Let $e=\lambda(s(00),0)$, $x'_{-3}\neq x_{-3}$. By Lemma 11, $\lambda(\langle x_{-c},\ldots,x_{-3},0,0,s_a\rangle,0)\neq\lambda(\langle x_{-c},\ldots,x'_{-3},0,0,s_a\rangle,0)$.Thus $\lambda(\langle x_{-c},\ldots,x'_{-3},0,0,s_a\rangle,0)=e+1$. Then $f(x_{-c},\ldots,x_0,s_a)=\lambda(s(x_{-2}x_{-1}),x_0)=f_3(T_3(x_{-4}))+x_{-3}$.

3 Binary WI SIM Finite Automata with Delay 3 of Which $w_{3,M}$=1 and 8

Lemma 13. Let M be a c-order SIM FA $C(M_a,f)$, $M_a=\langle S_a,Y_a,\delta_a,\lambda_a\rangle$ be cyclic, $X=Y=\{0,1\}$. If $c\geq 3$, $w_{3,M}=1$, M is weakly invertible with delay 3, then there exists a mapping f_3 from $X^{c-3}\times S_a$ to Y such that

$$f(x_{-c},\ldots,x_0,s_a)=f_3(x_{-c},\ldots,x_{-4},s_a)+x_{-3}.$$

Proof: Since M_a is cyclic, $C(M_a,f)$ is strongly connected. Then $|W_{3,s}^M|=w_{3,M}=1,\forall s\in S$. Thus $\lambda(s(x_{-2}x_{-1}),x_0)=\lambda(s(00),0)$, $\forall x_{-2},x_{-1},x_0\in X$. Since M is weakly invertible with delay 3, $\lambda(\langle x_{-c},\ldots,x_{-4},0,0,0,s_a\rangle,0)\neq\lambda(\langle x_{-c},\ldots,x_{-4},1,0,0,s_a\rangle,0)$. Thus $f(x_{-c},\ldots,x_0,s_a)=\lambda(\langle x_{-c},\ldots,x_{-4},0,0,0,s_a\rangle,0)+x_{-3}=f_3(x_{-c},\ldots,x_{-4},s_a)+x_{-3}$, where $f_3(x_{-c},\ldots,x_{-4},s_a)=f(x_{-c},\ldots,x_{-4},0,0,0,0,s_a)$.

Lemma 14. Let M be a c-order SIM FA $C(M_a,f)$, $M_a=\langle S_a,Y_a,\delta_a,\lambda_a\rangle$ be cyclic, $X=Y=\{0,1\}$. If $c\geq 3$, $w_{3,M}=8$, M is weakly invertible with delay 3, then there exists a mapping f_0 from $X^c\times S_a$ to Y such that

$$f(x_{-c},\ldots,x_0,s_a)=f_0(x_{-c},\ldots,x_{-1},s_a)+x_0.$$

Proof: Since M_a is cyclic, $C(M_a,f)$ is strongly connected. Then $|W_{3,s}^M|=8$, $\forall s\in S$. Thus $\lambda(s(x_{-2}x_{-1}),0)\neq\lambda(s(x_{-2}x_{-1}),1)$. Then $f(x_{-c},\ldots,x_0,s_a)=\lambda(s(x_{-2}x_{-1}),0)+x_0=f_0(x_{-c},\ldots,x_{-1},s_a)+x_0$, where $f_0(x_{-c},\ldots,x_{-1},s_a)=f(x_{-c},\ldots,x_{-1},0,s_a)$.

4 Binary WI SIM Finite Automata with Delay 3

Theorem 1. Let M be a c-order SIM FA $C(M_a,f)$, $M_a=\langle S_a,Y_a,\delta_a,\lambda_a\rangle$ be cyclic, $X=Y=\{0,1\}$, $c\geq 3$. Then M is weakly invertible with delay 3, if one of the following conditions holds:

(a) There exists a mapping f_0 from $X^c\times S_a$ to Y such that

$$f(x_{-c},\ldots,x_0,s_a)=f_0(x_{-c},\ldots,x_{-1},s_a)+x_0;$$

(b) There exists a mapping f_3 from $X^{c-3}\times S_a$ to Y such that

$$f(x_{-c},\ldots,x_0,s_a)=f_3(x_{-c},\ldots,x_{-4},s_a)+x_{-3};$$

(c) There exist mappings h_0 from $X^{c-1}\times S_a$ to $\{0,1\}$, h_1 from $X^{c-2}\times S_a$ to $\{0,1\}$, h_2 from $X^{c-3}\times S_a$ to $\{0,1\}$, f_0 from $X^c\times S_a$ to Y, f_1 from $X^{c-1}\times S_a$ to Y, f_2 from $X^{c-2}\times S_a$ to Y, f_3 from $X^{c-3}\times S_a$ to Y, such that (2.1), (2.2) and (2.3) hold, where h_3 and h_4 are defined by (2.4).

Proof: Assume that one of conditions (a), (b) and (c) holds. In case of (a), M is weakly invertible with delay 0; In case of (b), it is easy to verify that M is weakly invertible with delay 3. Below we discuss the case of (c); Assume that (c) holds, let $s=\langle x_{-c},\ldots,x_{-1},s_a\rangle$, $s_i=\langle x_{-c+1},\ldots,x_{-1},i,\delta_a(s_a)\rangle$, $s_{i,j}=\langle x_{-c+2},\ldots,x_{-1},i,j,\delta_a^2(s_a)\rangle$, $s_{i,j,k}=\langle x_{-c+3},\ldots,x_{-1},i,j,k,\delta_a^3(s_a)\rangle$ $(i,j,k=0,1)$, other notations used below are referred to the proof of Lemma 12. Since M_a is cyclic, $\lambda(s,x_0)=f(x_{-c},\ldots,x_0,\lambda_a(s_a))=f(x_{-c},\ldots,x_0,s_a)$. By (2.1), $h_2(T_3(x_{-4}))=1\rightarrow h_1(T_2(x_{-3}))=1$, $h_1(T_2(x_{-3}))=1\rightarrow h_0(T_1(x_{-2}))=1$. Thus, to prove s is a t-step state with $0\leq t\leq 3$, there are two main cases to consider.

Case 1. $h_0(T_1(x_{-2}))=0$. By (2.3), $\lambda(s,x_0)=f_0(x_{-c},\ldots,x_{-1},s_a)+x_0$. Thus $\lambda(s,0)\neq\lambda(s,1)$. Hence s is a 0-step state;

Case 2. $h_0(T_1(x_{-2}))=1$. By (2.3), $\lambda(s,0)=\lambda(s,1)$. Next we further consider $h_0(T_1(x_{-2}x_{-1}))$.

Subcase 2-1. $h_0(T_1(x_{-2}x_{-1}))=0$. By (2.3), $\lambda(s_i,0)\neq\lambda(s_i,1)$ (i=0,1). By (2.1), $h_0(T_1(x_{-2}x_{-1}x_0))=1$, $h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=1$, $\forall x_0\in X$. Then by (2.3), $\lambda(s_{i,j},0)=\lambda(s_{i,j},1)$, $\lambda(s_{i,j,k},0)=\lambda(s_{i,j,k},1)$, $\lambda(s_{i,j,0},0)=\lambda(s_{i,j,1},0)$ (i,j,k=0,1). Since $h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=1\rightarrow h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=1$, we further consider $h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))$.

Subcase 2-1-1. $h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=1$. By (2.3), $\lambda(s_{i,j,k},x)=\lambda(s_{i,0,0},0)$, $\lambda(s_{0,0,0},0)\neq\lambda(s_{1,0,0},0)$ (i,j,k=0,1), $\forall x\in X$. Hence s is a t-step state ($2\le t\le 3$).

Subcase 2-1-2. $h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=0$. Since $h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=1\wedge h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=0$, by (2.3), $\lambda(s_{i,0,0},0)\neq\lambda(s_{i,1,0},0)$ (i=0,1). Since $h_1(T_2(x_{-3}x_{-2}x_{-1}))=1\rightarrow h_0(T_1(x_{-2}x_{-1}x_0))=1$, we further consider $h_1(T_2(x_{-3}x_{-2}x_{-1}))$.

Subcase 2-1-2-1. $h_1(T_2(x_{-3}x_{-2}x_{-1}))=1$. Since $h_0(T_1(x_{-2}x_{-1}))=0\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}))=1$, by (2.1), $h_2(T_3(x_{-4}x_{-3}x_{-2}))=1$, $\lambda(s_{0,0},0)=\lambda(s_{0,1},0)=\lambda(s_{1,0},0)=\lambda(s_{1,1},0)$. It suffices to show that whether $\lambda(s_{0,0,0},0)=\lambda(s_{1,0,0},0)$ holds, if $\lambda(s_0,0)=\lambda(s_1,0)$. Since $h_0(T_1(x_{-2}x_{-1}))=0\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}))=1\wedge h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=0$, by (2.2), $f_0(x_{-c+1},\ldots,x_{-1},0,\delta_a(s_a))+f_0(x_{-c+1},\ldots,x_{-1},1,\delta_a(s_a))=h_4(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))+1$. By (2.4), $f_0(x_{-c+1},\ldots,x_{-1},0,\delta_a(s_a))+f_0(x_{-c+1},\ldots,x_{-1},1,\delta_a(s_a))=f_2(T_2(x_{-3}x_{-2}x_{-1}^0))+f_2(T_2(x_{-3}x_{-2}x_{-1}^1))+1$. On the other hand, since $h_0(T_1(x_{-2}x_{-1}))=0$, by (2.3), $f_0(x_{-c+1},\ldots,x_{-1},x_0,\delta_a(s_a))=f(x_{-c+1},\ldots,x_{-1},x_0,0,\delta_a(s_a))$, $\forall x_0\in X$. Since $h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=1\wedge h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=0$, $\forall x_0\in X$. By (2.3), $f_2(T_2(x_{-3}x_{-2}x_{-1}x_0))=f(x_{-c+3},\ldots,x_0,0,0,0,\delta_a^3(s_a))$, $\forall x_0\in X$. Then $\lambda(s_0,0)+\lambda(s_1,0)=\lambda(s_{0,0,0},0)+\lambda(s_{1,0,0},0)+1$. Thus $\lambda(s_0,0)=\lambda(s_1,0)$ iff $\lambda(s_{0,0,0},0)\neq\lambda(s_{1,0,0},0)$. Hence s is a 3-step state.

Subcase 2-1-2-2. $h_1(T_2(x_{-3}x_{-2}x_{-1}))=0$. Since $h_1(T_2(x_{-3}x_{-2}x_{-1}))=0\wedge h_0(T_1(x_{-2}x_{-1}x_0))=1$, $\forall x_0\in X$, by (2.3), $\lambda(s_{i,0},0)\neq\lambda(s_{i,1},0)$ (i=0,1). It suffices to show whether $\lambda(s_{0,0},0)=\lambda(s_{1,0},0)$ and $\lambda(s_{0,0,0},0)=\lambda(s_{1,0,0},0)$ hold, respectively, if $\lambda(s_0,0)=\lambda(s_1,0)$. Since $h_1(T_2(x_{-3}x_{-2}x_{-1}))=0\wedge h_0(T_1(x_{-2}x_{-1}))=0$, by (2.2), $f_0(x_{-c+1},\ldots,x_{-1},0,\delta_a(s_a))+f_0(x_{-c+1},\ldots,x_{-1},1,\delta_a(s_a))=h_3(T_2(x_{-3}x_{-2}x_{-1}))$. By (2.3), $f_0(x_{-c+1},\ldots,x_{-1},x_0,\delta_a(s_a))=f(x_{-c+1},\ldots,x_{-1},x_0,0,\delta_a(s_a))$, $\forall x_0\in X$. Using (2.4), $h_3(T_2(x_{-3}x_{-2}x_{-1}))=f_1(T_1(x_{-2}x_{-1}^0))+f_1(T_1(x_{-2}x_{-1}^1))$. Since $h_1(T_2(x_{-3}x_{-2}x_{-1}))=0\wedge h_0(T_1(x_{-2}x_{-1}x_0))=1$, by (2.3), $f_1(T_1(x_{-2}x_{-1}x_0))=f(x_{-c+2},\ldots,x_{-1},x_0,0,0,\delta_a^2(s_a))$. Thus $\lambda(s_0,0)+\lambda(s_1,0)=\lambda(s_{0,0},0)+\lambda(s_{1,0},0)$. Hence $\lambda(s_{0,0},0)=\lambda(s_{1,0},0)$ if $\lambda(s_0,0)=\lambda(s_1,0)$. Since $h_0(T_1(x_{-2}x_{-1}^0))=1\wedge h_0(T_1(x_{-2}x_{-1}^1))=1\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}))=0\wedge h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=0$, by (2.2), $h_3(T_2(x_{-3}x_{-2}x_{-1}))=h_4(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))+1$. Using (2.4), $h_3(T_2(x_{-3}x_{-2}x_{-1}))=f_1(T_1(x_{-2}x_{-1}^0))+f_1(T_1(x_{-2}x_{-1}^1))$, $h_4(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=f_2(T_2(x_{-3}x_{-2}x_{-1}^0))+f_2(T_2(x_{-3}x_{-2}x_{-1}^1))$. Since $h_1(T_2(x_{-3}x_{-2}x_{-1}))=0\wedge h_0(T_1(x_{-2}x_{-1}x_0))=1$, by (2.3), $f_1(T_1(x_{-2}x_{-1}x_0))=f(x_{-c+2},\ldots,x_0,0,0,\delta_a^2(s_a)))$, $\forall x_0\in X$. On the other hand, since $h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=1\wedge h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=0$, by (2.3), $f_2(T_2(x_{-3}x_{-2}x_{-1}x_0))=f(x_{-c+3},\ldots,x_0,0,0,0,\delta_a^2(s_a))$. Then $\lambda(s_{0,0},0)+\lambda(s_{1,0},0)=\lambda(s_{0,0,0},0)+\lambda(s_{1,0,0},0)+1$. Thus $\lambda(s_{0,0},0)=\lambda(s_{1,0},0)$ iff $\lambda(s_{0,0,0},0)\neq\lambda(s_{1,0,0},0)$. Therefore, if $\lambda(s_0,0)=\lambda(s_1,0)$ then $\lambda(s_{0,0},0)=\lambda(s_{1,0},0)$ and $\lambda(s_{0,0,0},0)\neq\lambda(s_{1,0,0},0)$. Hence s is a 3-step state.

Subcase 2-2. $h_0(T_1(x_{-2}x_{-1}))=1$. Since $h_1(T_2(x_{-3}x_{-2}))=1\rightarrow h_0(T_1(x_{-2}x_{-1}))=1$, we consider $h_1(T_2(x_{-3}x_{-2}))$.

Subcase 2-2-1. $h_1(T_2(x_{-3}x_{-2}))=0$. Since $h_0(T_1(x_{-2}x_{-1}))=1\wedge h_1(T_2(x_{-3}x_{-2}))=0$, by (2.3), $\lambda(s_i,0)=\lambda(s_i,1)$, $\lambda(s_0,0)\neq\lambda(s_1,0)$ (i=0,1). Therefore s is a 1-step state.

Subcase 2-2-2. $h_1(T_2(x_{-3}x_{-2}))=1$. By (2.3), $\lambda(s_0,0)=\lambda(s_0,1)=\lambda(s_1,0)=\lambda(s_1,1)$. Since $h_0(T_1(x_{-2}))=1\wedge h_1(T_2(x_{-3}x_{-2}))=1$, by (2.1), $h_2(T_3(x_{-4}x_{-3}x_{-2}))=0$. Since $h_2(T_3(x_{-4}x_{-3}x_{-2}))=1\rightarrow h_1(T_2(x_{-3}x_{-2}x_{-1}))=1$, $h_1(T_2(x_{-3}x_{-2}x_{-1}))=1\rightarrow h_0(T_1(x_{-2}x_{-1}x_0))=1$, $\forall x_{-1},x_0\in X$, we further consider the following cases.

Subcase 2-2-2-1. $h_1(T_2(x_{-3}x_{-2}x_{-1}))=1\wedge h_2(T_3(x_{-4}x_{-3}x_{-2}))=0$. By (2.3), $\lambda(s_{i,j},0)=\lambda(s_{i,j},1)$, $\lambda(s_{i,0},0)=\lambda(s_{i,1},0)$, $\lambda(s_{0,0},0)\neq\lambda(s_{1,0},0)$ (i,j=0,1). Therefore s is a 2-step state.

Subcase 2-2-2-2. $h_1(T_2(x_{-3}x_{-2}x_{-1}))=0$. We consider three cases.

Subcase 2-2-2-2-1. $h_0(T_1(x_{-2}x_{-1}0))=0\wedge h_0(T_1(x_{-2}x_{-1}^1))=0$. By (2.1), $h_0(T_1(x_{-2}x_{-1}x_0x_1))=1$, $\forall x_0,x_1\in X$. There are two cases to consider.

Subcase 2-2-2-2-1-1. $h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=1$. Since $h_0(T_1(x_{-2}x_{-1}x_0))=0\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=1$, $\forall x_0\in X$. By (2.1),

$h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=1$, by (2.3), $\lambda(s_{i,j,k},0)=\lambda(s_{i,j,k},1)=\lambda(s_{i,0,0},0)$, $\lambda(s_{0,0,0},0)\neq\lambda(s_{1,0,0},0)$ (i,j, k=0,1). Thus s is a 3-step state.

Subcase 2-2-2-2-1-2. $h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=0$. Since $h_0(T_1(x_{-2}\,x_{-1}^0))=0\wedge h_0(T_1(x_{-2}\,x_{-1}^1))=0\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=0$, by (2.1), $h_1(T_2(x_{-3}x_{-2}x_{-1}\,x_0'))=0$ ($x_0\neq x_0'$). Since $h_0(T_1(x_{-2}x_{-1}x_0x_1))=1\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=0$, $\forall x_0,x_1\in X$, by (2.3), $\lambda(s_{i,j,k},0)=\lambda(s_{i,j,k},1)$, $\lambda(s_{i,j,0},0)\neq\lambda(s_{i,j,1},0)$ (i,j,k=0,1). By subcase 2-1-2-2, it suffices to show whether $\lambda(s_{0,0,0},0)=\lambda(s_{1,0,0},0)$ hold, if $\lambda(s_{0,0},0)=\lambda(s_{1,0},0)$. Since $h_0(T_1(x_{-2}\,x_{-1}^0))=0\wedge h_0(T_1(x_{-2}\,x_{-1}^1))=0\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=0$, by (2.2), $f_0(x_{-c+2},\ldots,x_{-1},0,0,\delta_a^2(s_a))+f_0(x_{-c+2},\ldots,x_{-1},1,0,\delta_a^2(s_a))=f_1(T_1(x_{-2}\,x_{-1}^{00}))+f_1(T_1(x_{-2}\,x_{-1}^{10})+1$. Since $h_0(T_1(x_{-2}x_{-1}x_0))=0$, by (2.3), $f_0(x_{-c+2},\ldots,x_{-1},x_0,0,\delta_a^2(s_a))=f(x_{-c+2},\ldots,x_0,0,0,\delta_a^2(s_a))$. Since $h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=0\wedge h_0(T_1(x_{-2}x_{-1}x_0x_1))=1$, $\forall x_0,x_1\in X$, by (2.3), $f_1(T_1(x_{-2}x_{-1}x_00))=f(x_{-c+3},\ldots,x_0,0,0,0,\delta_a^3(s_a))$. Thus $\lambda(s_{0,0},0)+\lambda(s_{1,0},0)=\lambda(s_{0,0,0},0)+\lambda(s_{1,0,0},0)+1$. Hence if $\lambda(s_{0,0},0)=\lambda(s_{1,0},0)$, then $\lambda(s_{0,0,0},0)\neq\lambda(s_{1,0,0},0)$. Therefore s is a 3-step state.

Subcase 2-2-2-2-2. $h_0(T_1(x_{-2}\,x_{-1}^0))=1\wedge h_0(T_1(x_{-2}\,x_{-1}^1))=1\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}))=0$. Since $h_0(T_1(x_{-2}x_{-1}x_0))=1\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}))=0$, $\forall x_0\in X$, by (2.3), $\lambda(s_{i,j},0)=\lambda(s_{i,j},1)$, $\lambda(s_{i,0},0)\neq\lambda(s_{i,1},0)$ (i,j=0,1). Since $h_0(T_1(x_{-2}x_{-1}))=1\wedge h_0(T_1(x_{-2}x_{-1}x_0))=1\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}))=0$, by (2.1), $h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=1$, $\forall x_0\in X$. Since $h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=1\rightarrow h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=1$, we consider the following two cases.

Subcase 2-2-2-2-2-1. $h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=1$. By (2.3), it is easy to see that s is a 3-step state.

Subcase 2-2-2-2-2-2. $h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=0$. Since $h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=0\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=1$, by (2.3), $\lambda(s_{i,j,k},0)=\lambda(s_{i,j,k},1)=\lambda(s_{i,j,0},0)$, $\lambda(s_{i,0,0},0)\neq\lambda(s_{i,1,0},0)$ (i,j,k=0,1). It suffices to show whether $\lambda(s_{0,0,0},0)=\lambda(s_{1,0,0},0)$ holds, if $\lambda(s_{0,0},0)=\lambda(s_{1,0},0)$. Since $h_0(T_1(x_{-2}x_{-1}x_0))=1\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}))=0\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}x_0))=1$, $\forall x_0\in X$, by (2.2), $h_3(T_2(x_{-3}x_{-2}x_{-1}))=h_4(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))+1$. Using (2.4), by the same arguments as above, $\lambda(s_{0,0},0)+\lambda(s_{1,0},0)=\lambda(s_{0,0,0},0)+\lambda(s_{1,0,0},0)+1$. Thus if $\lambda(s_{0,0},0)=\lambda(s_{1,0},0)$, then $\lambda(s_{0,0,0},0)\neq\lambda(s_{1,0,0},0)$. Therefore s is a 3-step state.

Subcase 2-2-2-2-3. $h_0(T_1(x_{-2}x_{-1}x_0))=0\wedge h_0(T_1(x_{-2}x_{-1}\,x_0'))=1$ ($x_0\neq x_0'$). Without loss of generality, let $h_0(T_1(x_{-2}\,x_{-1}^0))=0$, $h_0(T_1(x_{-2}\,x_{-1}^1))=1$. By (2.3), $\lambda(s_{0,j},0)\neq\lambda(s_{0,j},1)$ (j=0,1). By (2.1), $h_1(T_2(x_{-3}x_{-2}x_{-1}))=0$, $h_0(T_1(x_{-2}\,x_{-1}^0\,x_1))=1$, $\forall x_1\in X$. Since $h_1(T_2(x_{-3}x_{-2}x_{-1}))=0\wedge h_0(T_1(x_{-2}\,x_{-1}^1))=1$, by (2.3), $\lambda(s_{1,j},0)=\lambda(s_{1,j},1)$, $\lambda(s_{1,0},0)\neq\lambda(s_{1,1},0)$ (j=0,1). Since $h_0(T_1(x_{-2}x_{-1}))=1\wedge h_0(T_1(x_{-2}\,x_{-1}^1))=1\wedge h_1(T_2(x_{-3}x_{-2}x_{-1}))=0$, by (2.1), $h_1(T_2(x_{-3}x_{-2}\,x_{-1}^1))=1$. Since $h_0(T_1(x_{-2}\,x_{-1}^0\,x_1))=1$, $\forall x_1\in X$, we further consider $h_1(T_2(x_{-3}x_{-2}\,x_{-1}^0))$.

Subcase 2-2-2-2-3-1. $h_1(T_2(x_{-3}x_{-2}\,x_{-1}^0))=1$. By (2.1), $h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=1$, by (2.3), $\lambda(s_{i,j,k},0)=\lambda(s_{i,j,k},1)=\lambda(s_{i,0,0},0)$, $\lambda(s_{0,0,0},0)\neq\lambda(s_{1,0,0},0)$ (i,j,k=0,1). Therefore s is a 3-step state.

Subcase 2-2-2-2-3-2. $h_1(T_2(x_{-3}x_{-2}\,x_{-1}^0))=0$. Since $h_0(T_1(x_{-2}\,x_{-1}^0\,x_1))=1\wedge h_1(T_2(x_{-3}x_{-2}\,x_{-1}^0))=0$, $\forall x_1\in X$, by (2.3), $\lambda(s_{0,j,k},0)=\lambda(s_{0,j,k},1)$, $\lambda(s_{0,j,0},0)\neq\lambda(s_{0,j,1},0)$ (j,k=0,1). Since $h_1(T_2(x_{-3}x_{-2}\,x_{-1}^0))=0$, by (2.1), $h_2(T_3(x_{-4}x_{-3}x_{-2}x_{-1}))=0$. Since $h_1(T_2(x_{-3}x_{-2}\,x_{-1}^1))=1$, by (2.3), $\lambda(s_{1,j,k},0)=\lambda(s_{1,j,k},1)=\lambda(s_{1,j,0},0)$, $\lambda(s_{1,0,0},0)\neq\lambda(s_{1,1,0},0)$ (j,k=0,1). Using subcase 2-1-2-2, $\lambda(s_{0,0,0},0)=\lambda(s_{0,1,0},0)$ if $\lambda(s_{0,0},0)=\lambda(s_{0,1},0)$. It suffices to show whether $\lambda(s_{0,0,0},0)=\lambda(s_{1,0,0},0)$ holds, if $\lambda(s_{0,0},0)=\lambda(s_{1,0},0)$. Since $h_0(T_1(x_{-2}\,x_{-1}^0))=0\wedge h_0(T_1(x_{-2}\,x_{-1}^1))=1\wedge h_1(T_2(x_{-3}x_{-2}\,x_{-1}^0))=0$, by (2.2), $f_0(x_{-c+2},\ldots,x_{-1},0,0,\delta_a^2(s_a))+f_1(x_{-c+2},\ldots,x_{-1},1,\delta_a^2(s_a))=f_1(x_{-c+3},\ldots,x_{-1},0,0,\delta_a^3(s_a))+f_2(x_{-c+3},\ldots,x_{-1},1,\delta_a^3(s_a))+1$. By the same arguments as above, we can conclude that s is a 3-step state.

To sum up, if condition (c) holds, then any state s of M is a t-step state ($0\leq t\leq 3$). Therefore M is weakly invertible with delay 3.

5 Binary Feedforward Inverse Finite Automata

Theorem 2. Let M be a c-order SIMFA $C(M_a,f)$, $M_a=\langle S_a,Y_a,\delta_a,\lambda_a\rangle$ be cyclic, $X=Y=\{0,1\}$, $c\geq 3$. Then if one of the following conditions holds, M is a feedforward inverse with delay 3.

(a) There exists a mapping f_0 from $X^c \times S_a$ to Y such that $f(x_{-c},\ldots,x_0,s_a)=f_0(x_{-c},\ldots,x_{-1},s_a)+x_0$;

(b) There exists a mapping f_3 from $X^{c-3} \times S_a$ to Y such that $f(x_{-c},\ldots,x_0,s_a)=f_3(x_{-c},\ldots,x_{-4},s_a)+x_{-3}$;

(c) There exist mappings h_0 from $X^{c-1} \times S_a$ to $\{0,1\}$, h_1 from $X^{c-2} \times S_a$ to $\{0,1\}$, h_2 from $X^{c-3} \times S_a$ to $\{0,1\}$, f_0 from $X^c \times S_a$ to Y, f_1 from $X^{c-1} \times S_a$ to Y, f_2 from $X^{c-2} \times S_a$ to Y, f_3 from $X^{c-3} \times S_a$ to Y, such that (2.1), (2.2) and (2.3) hold, where h_3 and h_4 are defined by (2.4).

Proof: Since M_a is cyclic, M is strongly connected. By Theorem 2 in Ref.[6], M is a feedforward inverse with delay 3 iff M is weakly invertible with delay 3. Therefore, by Theorem 1, M is a feedforward with delay 3 if one of conditions (a), (b) and (c) holds.

Acknowledgement The authors would like to thank professor Tao Ren-Ji for his helpful guidance, professor Li Ang-Sheng for his valuable suggestions and the anonymous referees for their helpful comments.

References:

[1] Tao RJ. Invertibility of Finite Automata. Beijing: Science Press, 1979 (in Chinese).

[2] Tao RJ. Relationship between bounded error propagation and feedforward invertibility. Kexue Tongbao, 1982,27(7):406–408 (in Chinese with English abstract).

[3] Tao RJ. Some results on the structure of feedforward inverses. Scientia Sinica (A), 1983,(12):1073–1078 (in Chinese with English abstract).

[4] Bao F. On the structure of *n*-ary feedforward inverses with delay 1 [MS. Thesis]. Beijing: Institute of Software, the Chinese Academy of Sciences, 1986 (in Chinese with English abstract).

[5] Zhu X. On the structure of binary feedforward inverses with delay 2. Journal of Computer Science and Technology, 1989,4(2): 163–171.

[6] Tao RJ, Chen S. Structure of weakly invertible semi-input-memory finite automata with delay 1. Journal of Computer Science and Technology, 2002,17(4):369–376.

[7] Tao RJ, Chen S. Structure of weakly invertible semi-input-memory finite automata with delay 2. Journal of Computer Science and Technology, 2002,17(6):682–688.

[8] Tao RJ, Chen S. Input-Trees of finite automata and application to cryptanalysis. Journal of Computer Science and Technology, 2000,15(4): 305–325.

附中文参考文献:

[1] 陶仁骥.有限自动机的可逆性.北京:科学出版社,1979.

[2] 陶仁骥.误差传播有界与前馈可逆的关系.科学通报,1982,27(7):406–408.

[3] 陶仁骥.关于前馈逆的结构的若干结果.中国科学(A 辑),1983,(12):1073–1078.

[4] 鲍丰.关于 *n* 元延迟 1 步前馈逆的结构[硕士学位论文].北京:中国科学院软件研究所,1986.

WANG Hong-Ji was born in 1968. He is a Ph.D. candidate at the Institute of Software, the Chinese Academy of Sciences. His current research areas are automata theory, cryptography and information security.

YAO Gang was born in 1975. He is an assistant professor at the State Key Laboratory of Information Security, the Institute of Software, the Chinese Academy of Sciences. His current research areas are automata theory, cryptography and information security.