P.O.Box 8718, Beijing 100080, China	Journal of Software Jan. 2007,18(1):40-49
E-mail: jos@iscas.ac.cn	ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2006 by *Journal of Software*

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

WANG Hong-Ji, YAO Gang

Full-Text PDF Submission Back

WANG Hong-Ji1,2, YAO Gang3,
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)
Authors information: 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.
Corresponding author: WANG Hong-Ji, Phn: +86-10-82625471, E-mail: whj@gcl.iscas.ac.cn, http://lcs.ios.ac.cn
Received 2005-01-26; Accepted 2005-04-18

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(Ma,f) with delay 3, where the state graph of Ma is cyclic, the characterizations of the structures are given when its minimal 3-output weight is 1, 2, and 8, respectively. Because C(Ma,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.

Wang HJ, Yao G. On the structure of binary feedforward inverse finite automata with delay 3. *Journal of Software*, 2007,18(1):40-49.
DOI: 10.1360/jos180040
http://www.jos.org.cn/1000-9825/18/40.htm

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Ma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(Ma,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(Ma,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.

基金项目：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)

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.