# 《有限自动机及在密码学中的应用》

## 书籍信息

版 次：1<br>
页 数：<br>
字 数：<br>
印刷时间：2008年09月01日<br>
开 本：16开<br>
纸 张：胶版纸<br>
包 装：精装<br>
是否套装：否<br>
国际标准书号ISBN：9787302175308

## 内容简介

本书主要研究有限自动机的可逆性理论及其在密码学上的应用。此外，也讨论自治有限自动机和拉丁阵，它们与有限自动机单钥密码的标准形有关。

有限自动机是被认为是密码的自然模型。本书作者提出并发展了RaRb风变换方法，用它彻底解决了有限域上（拟）线性有限自动机的结构问题。与经典的线性系统“ 传输函数方法 ”不同，RaRb变换方法可推广到非线性有限自动机；大量弱可逆有限自动机及其弱逆可用它产生，这就导致基于有限自动机的公开钥密码（简记为FAPKC）的提出。

本书可用作计算机科学和数学专业高年级和研究生课程的参考书。

## 目 录

Foreword by Arto Salomaa
Preface
1. Introduction
1.1 Preliminaries
1.1.1 Relations and Functions
1.1.2 Graphs
1.2 Definitions of Finite Automata
1.2.1 Finite Automata as Transducers
1.2.2 Special Finite Automata
1.2.3 Compound Finite Automata
1.2.4 Finite Automata as Recognizers
1.3 Linear Finite Automata
1.4 Concepts on Invertibility
1.5 Error Propagation and Feedforward Invertibility.
1.6 Labelled Trees as States of Finite Automata
2. Mutual Invertibility and Search
2.1 Minimal Output Weight and Input Set
2.2 Mutual Invertibility of Finite Automata
2.3 Find Input by Search
2.3.1 On Output Set and Input Tree
2.3.2 Exhausting Search
2.3.3 Stochastic Search
3. Ra Rb Transformation Method
3.1 Suificient Conditions and Inversion
3.2 Generation of Finite Automata with Invertibility
3.3 Invertibility of Quasi-Linear Finite Automata
3.3.1 Decision Criteria

3.3.2 Structure Problem
4. Relations Between Transformations
4.1 Relations Between Ra -Rb Transformations
4.2 Composition of Ra Rb Transformations
4.3 Reduced Echelon Matrix
4.4 Canonical Diagonal Matrix Polynomial
4.4.1 Ra Rb Transformations over Matrix Polynomial
4.4.2 Relations Between Ra Rb Transformation and Canonical Diagonal Form
4.4.3 Relations of Right-Parts
4.4.4 Existence of Terminating Re Rb Transformation Sequence
5. Structure of Feedforward Inverses
5.1 A Decision Criterion
5.2 Delay Free
5.3 One Step Delay
5.4 Two Step Delay
6. Some Topics on Structure Problem
6.1 Some Variants of Finite Automata
6.1.1 Partial Finite Automata
6.1.2 Nondeterministic Finite Automata
6.2 Inverses of a Finite Automaton
6.3 Original Inverses of a Finite Automaton
6.4 Weak Inverses of a Finite Automaton
6.5 Original Weak Inverses of a Finite Automaton
6.6 Weak Inverses with Bounded Error Propagation of a Finite Automaton
7. Linear Autonomous Finite Automata
7.1 Binomial Coefficient
7.2 Root Representation
7.3 Translation and Period
7.3.1 Shift Registers
7.3.2 Finite Automata
7.4 Linearization
7.5 Decimation
8. One Key Cryptosystems and Latin Arrays
8.1 Canonical Form for Finite Automaton One Key Cryptosystems
8.2 Latin Arrays
8.2.1 Definitions
……
9 Finite Automaton Public Key Crytosystems
References
Index

版权信息

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问www.tushupdf.com