
Contents

PREFACE	xxi
1 INTRODUCTION	1
1.1 Cellular Automata Applications	3
1.2 Overview of the Book	4
2 CA AND ITS APPLICATIONS: A BRIEF SURVEY	6
2.1 Introduction	6
2.2 Initial Phase of Development	6
2.3 CA-Based Models	7
2.3.1 CA as Parallel Language Recognizer,	7
2.3.2 Biological Applications of CA,	8
2.3.3 CA as Parallel and Image Processing	
Systems,	8
2.4 New Phase of Development	9
2.4.1 Polynomial Algebraic Characterization of CA	
Behavior,	13
2.4.2 Matrix Algebraic Characterization of CA,	16
2.5 Other Developments Under the New Phase of	
Activities	16
2.5.1 Probabilistic Analysis of CA Behavior,	16
2.5.2 CA-Based Models for Physical Systems,	17
2.5.3 CA Machines (CAMs),	17
2.5.4 Fractional Dimensions in CA,	18

2.6	Consolidation in the VLSI Era	18
2.6.1	Pseudorandom Pattern Generation,	18
2.6.2	Pseudoexhaustive Test Pattern Generation,	19
2.6.3	Deterministic Test Pattern Generation,	19
2.6.4	Signature Analysis,	21
2.6.5	CALBO (Cellular Automata Logic Block Observer),	22
2.6.6	Error Correcting Codes,	22
2.6.7	Low-Cost Associative Memory,	23
2.6.8	Finite-State Machine (FSM) Synthesis,	23
2.6.9	Synthesis of Easily Testable Combinational Logic,	23
2.6.10	Mod- p Multiplier,	24
2.6.11	Pattern Classification,	24
2.6.12	General and Perfect Hashing,	24
2.6.13	Design of a CA-Based Cipher System,	24
2.6.14	Modeling Amino Acid and Protein Chain,	25
2.7	Summary	25

3 GROUP CA CHARACTERIZATION

26

3.1	Introduction	26
3.2	Characterization of the State-Transition Behavior	27
3.3	Group Properties of CA	29
3.3.1	Cycle Set Characterization of Group CA,	33
3.3.2	Characterization of Group CA with Inverse State-Transition Function,	34
3.3.3	Correlation of Length of a CA and a Group Rule,	35
3.3.4	Isomorphism between a CA and an LFSR Generating Exhaustive Pattern,	37
3.4	A Class of Null Boundary Group CA	38
3.5	Group Properties of Periodic Boundary CA (PBCA) with Rules 90 and 150	41
3.6	Analysis of Intermediate Boundary CA (IBCA)	42
3.6.1	Maximum-Length IBCA Configurations,	44
3.7	Phase Shift of PN-Sequences Generated by CA	48
3.8	Programmable CA (PCA)	52
3.9	Summary	54

4	CHARACTERIZATION OF NONGROUP CA	56
4.1	Introduction	56
4.2	General Characterization of Linear Nongroup CA	58
4.2.1	Uniformity of the Tree-Structure in the State-Transition Diagram of a Linear Nongroup CA,	63
4.2.2	Characterization of Cyclic States,	66
4.2.3	Characterization of States in a Tree,	67
4.2.4	Characterization of States in an n -Tree ($n \geq 6$),	67
4.3	Characterization of Linear Multiple-Attractor Cellular Automata	69
4.3.1	Construction of Multiple-Attractor CA (MACA),	73
4.4	Characterization of Complemented Additive CA	78
4.4.1	General Characterization of Cyclic Behavior,	78
4.5	Behavior of Complemented CA Derived from Multiple-Attractor Linear CA	81
4.5.1	An Acyclic State as the Complement Vector,	82
4.5.2	A Nonzero Attractor as the Complement Vector,	85
4.6	Characterization of $D1^*CA$	87
4.7	Summary	95
5	CA AS A UNIVERSAL PATTERN GENERATOR	96
5.1	Introduction	96
5.2	Pseudoexhaustive Pattern Generation	97
5.2.1	Analysis of PN Sequences Generated by a Primitive Polynomial,	98
5.2.2	Vector Space Theoretic Characterization,	103
5.2.3	Identification of $n; m$ / Code Space and Exhaustive Pattern Generation by an m -Space,	107
5.2.4	CA as Pseudoexhaustive Test Pattern Generator,	113
5.3	On-Chip Deterministic Test Pattern Generation	117
5.3.1	Overview of the Scheme,	117
5.3.2	Selection of a Primitive Polynomial,	118
5.3.3	Selection of CA/LFSR Structures,	120

- 5.3.4 Generation of Test Patterns with Multiple Seeds, 123
- 5.4 Exhaustive Two- and Three-Pattern Generation Capability of a CA 127
 - 5.4.1 Generation of Two-Pattern Test Vectors, 128
 - 5.4.2 Generation of Three-Pattern Test Vectors, 129
 - 5.4.3 90=150 CA as Exhaustive Two-/Three-Pattern Generator, 130
 - 5.4.4 CA Selection Strategy for Generation of a Given -Pattern Set, 132
 - 5.4.5 Experimental Results, 134
- 5.5 Summary 136

6 CA-BASED ERROR CORRECTING CODE

137

- 6.1 Introduction 137
- 6.2 Review of Error Correcting Codes 138
 - 6.2.1 Bit Error Correcting/Detecting Codes, 138
 - 6.2.2 Byte Error Detecting/Correcting Codes, 143
- 6.3 Design of Random Bit Error Correcting Codes 146
 - 6.3.1 CA-Based Error Correcting Code (CAECC), 146
 - 6.3.2 Decoding of CA-Based Error Correcting Code, 157
 - 6.3.3 Complexity Analysis, 168
- 6.4 CA-Based Byte Error Correcting Code 169
 - 6.4.1 Generation of CA-SbEC-DbED Code, 169
 - 6.4.2 Decoding Scheme, 172
 - 6.4.3 Generation of CA-DbEL/DbEC Code, 177
 - 6.4.4 Implementation—Design of DbEL Cell, 181
 - 6.4.5 General Design Methodology, 183
 - 6.4.6 t -Byte Error Locating Code, 184
 - 6.4.7 Reduction of Decoding Time, 185
- 6.5 CA Array-Based Diagnosis of Board-Level Faults 186
 - 6.5.1 Board-Level Fault Diagnosis Using Cellular Automata Array, 187
 - 6.5.2 Encoding Output Responses of the Chips for Space Compression, 190
 - 6.5.3 Time Compression of Check Symbols, 192
 - 6.5.4 Syndrome Generation, 192
 - 6.5.5 Detecting the t Number of Faulty Chips out of N Chips, 192
 - 6.5.6 Performance, 198
- 6.6 Summary 201

7	DESIGN OF CA-BASED CIPHER SYSTEM	202
7.1	Introduction	202
7.1.1	Permutation Groups,	204
7.2	Permutation Representation of CA States	205
7.2.1	Permutation Representation of CA Having Equal Cycles of Even Length,	206
7.3	Definition of Fundamental Transformations	206
7.4	PCA-Based Block Cipher Scheme	208
7.4.1	Number of Enciphering Functions,	210
7.5	Stream Cipher Strategy	211
7.5.1	Key Stream Generators,	212
7.5.2	PCA-Based Stream Cipher Scheme,	215
7.6	Invulnerability of the Scheme	217
7.6.1	Block Ciphers,	217
7.6.2	Stream Ciphers,	217
7.7	Summary	218
8	GENERATION OF HASHING FUNCTIONS	219
8.1	Introduction	219
8.2	CA-Based Scheme for General Hashing	221
8.2.1	Analysis of CA-Based Hashing Scheme,	222
8.2.2	Implementation and Experimental Results,	224
8.3	Perfect Hashing	229
8.4	TPSA CA-Based Perfect Hashing Scheme	230
8.4.1	CA-Based Perfect Hashing,	232
8.5	Performance Evaluation of CA-Based Perfect Hashing Scheme	239
8.5.1	Performance Evaluation,	239
8.6	Summary	241
9	CA-BASED TESTABLE LOGIC SYNTHESIS	242
9.1	Introduction	242
9.2	Extended Characterization of $D1*CA$	243

- 9.3 Synthesis of Testable FSM 244
 - 9.3.1 State Encoding Strategy, 246
 - 9.3.2 Testing Scheme, 248
 - 9.3.3 Fault Coverage, 252
 - 9.3.4 Experimental Results, 253
 - 9.3.5 Comparison of Test Time and Design Effort, 255
- 9.4 BIST Structure for Testing Combinational Logic 256
 - 9.4.1 New Results on D1*CA Behavior, 256
- 9.5 CA-Based Distributed BIST 263
- 9.6 Test Methodology 267
 - 9.6.1 Test Procedure, 268
 - 9.6.2 Discussions on Fault Coverage, 269
- 9.7 Experimental Results 269
 - 9.7.1 Test Parallelism and Fault Diagnosis, 271
- 9.8 Summary 273

10 THEORY AND APPLICATION OF TWO-DIMENSIONAL CA 274

- 10.1 Introduction 274
- 10.2 Introduction to Two-Dimensional Cellular Automata 274
 - 10.2.1 Basic Concepts, 274
 - 10.2.2 Partitioning of the T Matrix, 277
 - 10.2.3 Characterization of 2-D CA, 278
 - 10.2.4 Cycle Length for RVN CA, 280
 - 10.2.5 Calculation of Depth and Cycle Length for Nongroup RVN CA, 284
- 10.3 Parallel PRPG Using 2-D CA 288
 - 10.3.1 Generating Test Patterns of Any Desired Length, 294
 - 10.3.2 Applications of 2-D CA as a BIST Structure, 295
 - 10.3.3 Pseudorandom Testing of Combinational Logic Circuits, 297
- 10.4 Design of Pseudoassociative Memory Using Cellular Automata 299
 - 10.4.1 CA-Based Hashing Scheme, 300
 - 10.4.2 The Hardware for Pseudoassociative Memory, 303
 - 10.4.3 Simulation Results, 305
 - 10.4.4 Estimation of Worst-Case Performance, 307

10.4.5 Design of a Pseudoassociative Memory Chip, 312	
10.5 Summary 313	
<i>BIBLIOGRAPHY</i>	314
<i>INDEX</i>	327
<i>ABOUT THE AUTHORS</i>	339

List of Figures

2.1	A Typical CA Cell	9
2.2	CA with Different Boundary Conditions: (a) Null Boundary, (b) Periodic Boundary, and (c) Intermediate Boundary	11
2.3	State-Transition Diagram of a Uniform CA with Rule 90 Having (a) Periodic Boundary Condition, and (b) Null Boundary Condition	13
3.1	The State-Transition Diagram of a Maximum-Length Group CA	32
3.2	The State-Transition Diagram of a Nonmaximum-Length Group CA	32
3.3	A Four-Stage LFSR Corresponding to $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$; $a_i \in \{0, 1\}$; $D = 1; 2; 3$ or 3	37
3.4	The State-Transition Diagram of a Nonmaximum-Length Group CA	41
3.5	A CA Cell That Can Be Configured with Rules 90=150	42
3.6	An Intermediate Boundary CA with Rule 90 Applied to Two Extreme Cells	43
3.7	A Maximum-Length Null Boundary CA with Rule 90; 150; 90; 150	48
3.8	A Three-Cell Programmable CA Structure and a PCA Cell	53
3.9	A More General PCA Cell with Three Control Lines	54
3.10	A PCA Cell with All Possible Additive Rules	54
3.11	A PCA Cell with XNOR Rule and Modified Control Lines	55

4.1	Structure and State-Transition Graph of a Four-Cell Linear Null Boundary CA with Rule $\{102, 60, 90, 60\}$	57
4.2	Structure and Behavior of a Four-Cell Linear Null Boundary CA with Rule $\{102, 102, 60, 60\}$	58
4.3	Structure and Behavior of a Four-Cell Complemented CA	59
4.4	State-Transition Diagram of a Multiple-Attractor CA	69
4.5	Structure and Behavior of a Four-Cell Complemented CA	87
4.6	State-Transition Diagram of a Four-Cell D1*CA with Rule Vector $\{90; 102; 102; 102\}$	88
4.7	State-Transition Diagram of Dual CA with Rule Vector $\{165; 102; 102; 102\}$	88
4.8	State-Transition Diagram of Five-Cell D1*CA with Rule Vector $\{90; 102; 102; 102; 102\}$	94
5.1	An Example A Matrix (a) and B Matrix (b) Corresponding to the 4-Degree Primitive Polynomial $x^4 \in \mathbb{C}[x]$	98
5.2	(a) $O_2 = \{A, B, D, \dots\}$, (b) C Matrix Corresponding to the Primitive Polynomial $x^3 \in \mathbb{C}[x]$, (c) C Matrix Corresponding to the Dual Primitive Polynomial $x^3 \in \mathbb{C}[x^2]$	101
5.3	(a) Cycle of Length 15, Which Is the Four-Dimensional Cyclic Subspace Generated for CA Having Rule Vector $\{90, 150, 90, 90, 90, 90, 150, 90\}$ with $x^4 \in \mathbb{C}[x]$ as Its Minimal Polynomial (the M Matrix); (b) a Four-Space; (c) a Three-Space	111
5.4	Store and Generate Scheme	117
5.5	An Example Pattern Set and Its Augmentation to Fit a PN Sequence Corresponding to a Given Polynomial	118
6.1	Data Communication from a Source to a Destination	137
6.2	A Simplified Model of a Coding System	138
6.3	The Syndrome Decoding Scheme	140
6.4	Organization of a Byte-Oriented Memory	144
6.5	Generation of Check Bits	147
6.6	Overview of the Decoding Scheme	163
6.7	The General Decoding Scheme	166
6.8	A Four-Cell Null Boundary CA with Rule Vector $\{102; 150; 60; 60\}$ as Signature Analyzer	170
6.9	Computation of the Check Bytes	172
6.10	Byte Position Counted from Left and Right	173
6.11	The SbEC-DbED Decoding Scheme	176
6.12	R-S Decoder Architecture	177
6.13	Decoding Scheme for SbEC-DbED Code	178
6.14	Architecture for the Basic Cell of DbEL Code	182
6.15	The Correction Scheme	182
6.16	Cascadable Architecture for Locating Three-Byte Errors	184
6.17	Configuration of Model Board	188
6.18	CAA-Based Self-Diagnosable Board	189

6.19	Space Compressor	191
6.20	Detection Scheme for 1-Chip Fault	194
6.21	Cascadable Architecture for Locating 3-Chip Faults	197
6.22	Hardware Savings in the CAA Approach Compared with the Straightforward Approach	200
6.23	Hardware Savings in the CAA Approach Compared with the MISR-Based Approach	200
7.1	The State-Transition Diagram of a Maximum-Length Group CA	205
7.2	The State-Transition Diagram of a Nonmaximum-Length Group CA	206
7.3	Block Diagram of the Circuit for a Block Cipher Scheme	209
7.4	PCA-Based Pseudorandom Pattern Generator	213
7.5	Two-Stage PCA-Based Pseudorandom Pattern Generator	214
7.6	Proposed Stream Cipher Scheme	216
8.1	State-Transition Diagram of a Multiple-Attractor CA	220
8.2	Structure and State-Transition Graph of (a) a Four-cell Noncomplemented TPSA CA (CA_1) with Rule Vector $h102, 60, 150, 60i$ and (b) Its Complemented Counterpart (CA_1^0)	231
8.3	State-Transition Graph of TPSA CA with Rule $h102, 90, 90, 60i$ and the Complemented CA with Complement Vector $[0010]^T$	236
9.1	Relationship of States in a $D1*CA$ and Its Dual	244
9.2	Block Diagram of a CA-Based FSM Design	245
9.3	A CA Cell and the State Transitions	245
9.4	The BIST Scheme	257
9.5	State-Transition Diagram of a Five-Cell $D1*CA$	258
9.6	A CA Cell and Its Autonomous/Interrupt Mode Transitions	263
9.7	$D1*CA$ -Based BIST	264
9.8	(a) Scan-Path-Based Design and (b) Distributed BIST Structure	272
10.1	Two-Dimensional CA	275
10.2	Five-Neighborhood Dependency	276
10.3	State Transitions for Nongroup CA	285
10.4	Different CA Rows Generate Patterns for Different Circuits	289
10.5	State-Time Diagrams for LFSR, 1-D CA, and 2-D CA	291
10.6	Variation of Bit Density with Number of Patterns	292
10.7	Feeding Data in Parallel to Four Scan Paths	296
10.8	Key-to-Address Translation in Hashing	301
10.9	CA-Based Hashing Scheme	302
10.10	Selection of Bits to Form the Key	302
10.11	The Proposed Scheme	303

List of Tables

2.1	Additive CA Rules	11
2.2	Maximum-Length Hybrid CA Rules	20
3.1	Logic Function of Rules 60, 102, 204 and Their Complemented Counterpart	39
3.2	CA Having Cycles of Even Length	41
3.3	n -Cell CA Having Even-Length Cycles for $n = 8$ and 16	41
3.4	Extreme Cells' Connections of IBCA	43
3.5	18 Different IBCA for a Primitive Polynomial	47
3.6	Number of IBCA for Different Length	48
3.7	PN Sequences of CA Cells	49
3.8	Phase Shift with Respect to 0th Cell	49
3.9	Phase Shift of Each Cell with Respect to 0th	53
4.1	Examples of Pseudoexhaustive Bit Positions	73
4.2	Conditions to Be Satisfied by the Attractors	76
4.3	Number of MACA with Different Number of Attractors	78
4.4	Maximum Cycle Length	92
4.5	Number of Components and Their Cycles	95
5.1	The C Matrix Corresponding to the 4-Degree Primitive Polynomial $x^4 + cx + 1$ and the Range and Offset Associated with Every 3-Tuple	100
5.2	Primitive Polynomials, Their Range and Offset	102
5.3	States Lying on 15-Length Cycle of the CA in Example 5.1	106

5.4	The 3-Space, Decimal Value, and Range	113
5.5	CA with Different Characteristic Polynomials and Their Factors	113
5.6	Range Associated with the Tuples	116
5.7	Polynomial Fitting in a Pattern Set	119
5.8(a)	Finding a Best-Fit Primitive Polynomial P	120
5.8(b)	Finding a Best-Fit Primitive Polynomial P^0	121
5.9	Experimental Results for Generation of Deterministic Pattern Set	124
5.10	Experimental Results of Generating Test Patterns for Delay Faults	135–136
6.1	CA for 4-Distance Code	154
6.2	Comparison of Hsiao and CAECC Codes	155
6.3	CA for Arbitrary t -Distance Codes	156
6.4	CA for 5-Distance Codes	158
6.5	CA for Higher-Distance Codes	159
6.6	Error Vector versus Syndrome	167
6.7	Throughput and Area for 4bEL Code	186
6.8	Hardware Overheads in Different Schemes	199
7.1	CA Having Equal Cycles of Even Length	207
7.2	CA Having Even-Length Cycles of Length $L \geq 8$ and 16	208
8.1	Dispersion Coefficients for Different CA and Clustering Lengths	225
8.2	Average Access and Maximum Probe for CA-Based Scheme	227
8.3	Average Access and Maximum Probe for Division Method	228
8.4	Comparison of Different Hashing Methods	228
8.5	CPU Time on HP 9000/807 System	229
8.6	Number of n -Bit TPSA CA (n)	237
8.7	Minimum n -Bit Numbers Required to Have q Levels Free in All CA (nq)	238
8.8	Average and Maximum Address-Bit Requirements for Perfect Hashing of 100 Random Set of Numbers	240
8.9	Timing Comparison of Different Hashing Methods	241
9.1	Performance Comparison with Respect to Area and Delay	254
9.2	Number of Components and Their Cycles	261
9.3	Description of Control Lines	265
9.4	Truth Table of CL	266
9.5	Modified Truth Table	266
9.6	Performance Comparison with Respect to Area and Delay	270
10.1	Results of Randomness Tests	288
10.2	Comparison of Randomness	290
10.3	Tests for Randomness	293

10.4	CA Configurations for Maximal Cycle Length	295
10.5	Fault Coverage (in Percentage) Using 1-D CA and 2-D CA	297
10.6	Fault Coverage (in Percentage) Using 1-D CA and 2-D CA	298
10.7	Fault Coverage Using Multiple Seeds	298
10.8	Micro-Operations in Normal Mode	304
10.9	Micro-Operations in Hash Mode	305
10.10	Average Number of Probes p_{av}	306
10.11	Exponential Distribution	307
10.12	Gaussian Distribution	308
10.13	Uniform Distribution	308
10.14	Performance of Different CA	310–311