

## Contents

<i>List of figures</i>	<i>page</i> xii
<i>List of tables</i>	xiii
<i>Acknowledgements</i>	xv
<b>1 Introduction</b>	<b>1</b>
1.1 Pseudo-random sequences	1
1.2 LFSR sequences	2
1.3 FCSR sequences	3
1.4 Register synthesis	5
1.5 Applications of pseudo-random sequences	6
<b>PART I ALGEBRAICALLY DEFINED SEQUENCES</b>	<b>13</b>
<b>2 Sequences</b>	<b>15</b>
2.1 Sequences and period	15
2.2 Fibonacci numbers	16
2.3 Distinct sequences	18
2.4 Sequence generators and models	19
2.5 Exercises	22
<b>3 Linear feedback shift registers and linear recurrences</b>	<b>23</b>
3.1 Definitions	23
3.2 Matrix description	27
3.3 Initial loading	30
3.4 Power series	32
3.5 Generating functions	39
3.6 When the connection polynomial factors	40
3.7 Algebraic models and the ring $R[x]/(q)$	45
3.8 Families of recurring sequences and ideals	53
	vii

viii	<i>Contents</i>	
3.9	Examples	64
3.10	Exercises	66
<b>4</b>	<b>Feedback with carry shift registers and multiply with carry sequences</b>	69
4.1	Definitions	70
4.2	$N$ -adic numbers	72
4.3	Analysis of FCSRs	79
4.4	Initial loading	83
4.5	Representation of FCSR sequences	85
4.6	Example: $q = 37$	87
4.7	Memory requirements	88
4.8	Random number generation using MWC	90
4.9	Exercises	94
<b>5</b>	<b>Algebraic feedback shift registers</b>	96
5.1	Definitions	96
5.2	$\pi$ -adic numbers	98
5.3	Properties of AFSRs	105
5.4	Memory requirements	108
5.5	Periodicity	114
5.6	Exponential representation and period of AFSR sequences	115
5.7	Examples	120
5.8	Exercises	131
<b>6</b>	<b><math>d</math>-FCSRs</b>	133
6.1	Binary $d$ -FCSRs	133
6.2	General $d$ -FCSRs	136
6.3	Relation between the norm and the period	137
6.4	Periodicity	140
6.5	Elementary description of $d$ -FCSR sequences	144
6.6	An example	149
6.7	Exercises	150
<b>7</b>	<b>Galois mode, linear registers, and related circuits</b>	151
7.1	Galois mode LFSRs	151
7.2	Division by $q(x)$ in $R[[x]]$	153
7.3	Galois mode FCSRs	154
7.4	Division by $q$ in the $N$ -adic numbers	157
7.5	Galois mode $d$ -FCSRs	157
7.6	Linear registers	160
7.7	Exercises	163

<i>Contents</i>		ix
<b>PART II PSEUDO-RANDOM AND PSEUDO-NOISE SEQUENCES</b>		165
<b>8 Measures of pseudo-randomness</b>		167
8.1 Why pseudo-random?		167
8.2 Sequences based on an arbitrary alphabet		169
8.3 Correlations		175
8.4 Exercises		189
<b>9 Shift and add sequences</b>		191
9.1 Basic properties		191
9.2 Characterization of shift and add sequences		194
9.3 Examples of shift and add sequences		196
9.4 Further properties of shift and add sequences		197
9.5 Proof of Theorem 9.4.1		200
9.6 Arithmetic shift and add sequences		204
9.7 Exercises		207
<b>10 m-sequences</b>		208
10.1 Basic properties of m-sequences		208
10.2 Decimations		210
10.3 Interleaved structure		211
10.4 Pseudo-noise arrays		212
10.5 Fourier transforms and m-sequences		214
10.6 Cross-correlation of an m-sequence and its decimation		217
10.7 The Diaconis mind-reader		226
10.8 Exercises		228
<b>11 Related sequences and their correlations</b>		230
11.1 Welch bound		230
11.2 Families derived from a decimation		231
11.3 Gold sequences		232
11.4 Kasami sequences, small set		233
11.5 Geometric sequences		235
11.6 GMW sequences		237
11.7 $d$ -form sequences		239
11.8 Legendre and Dirichlet sequences		239
11.9 Frequency hopping sequences		240
11.10 Optical orthogonal codes		242
11.11 Maximal sequences over a finite local ring		244
11.12 Exercises		247

<b>12</b>	<b>Maximal period function field sequences</b>	250
12.1	The rational function field AFSR	250
12.2	Global function fields	261
12.3	Exercises	263
<b>13</b>	<b>Maximal period FCSR sequences</b>	264
13.1	$\ell$ -sequences	264
13.2	Distributional properties of $\ell$ -sequences	267
13.3	Arithmetic correlations	271
13.4	Tables	275
13.5	Exercises	276
<b>14</b>	<b>Maximal period <math>d</math>-FCSR sequences</b>	283
14.1	Identifying maximal length sequences	283
14.2	Distribution properties of $d$ - $\ell$ -sequences	285
14.3	Exercises	292
<b>PART III REGISTER SYNTHESIS AND SECURITY MEASURES</b>		293
<b>15</b>	<b>Register synthesis and LFSR synthesis</b>	295
15.1	Sequence generators and the register synthesis problem	295
15.2	LFSRs and the Berlekamp–Massey algorithm	296
15.3	Blahut’s Theorem	304
15.4	The Günther–Blahut Theorem	305
15.5	Generating sequences with large linear span	311
15.6	Exercises	320
<b>16</b>	<b>FCSR synthesis</b>	322
16.1	$N$ -adic span and complexity	322
16.2	Symmetric $N$ -adic span	329
16.3	Rational approximation	334
16.4	Exercises	346
<b>17</b>	<b>AFSR synthesis</b>	347
17.1	Xu’s rational approximation algorithm	348
17.2	Rational approximation in $\mathbb{Z}$	352
17.3	Proof of correctness	353
17.4	Rational approximation in function fields	360
17.5	Rational approximation in ramified extensions	362
17.6	Rational approximation in quadratic extensions	363
17.7	Rational approximation by interleaving	369
17.8	Rational function fields: $\pi$ -adic vs. linear span	372
17.9	Exercises	375

<i>Contents</i>		xi
<b>18</b>	<b>Average and asymptotic behavior of security measures</b>	376
18.1	Average behavior of linear complexity	377
18.2	Average behavior of $N$ -adic complexity	384
18.3	Asymptotic behavior of security measures	388
18.4	Asymptotic linear complexity	390
18.5	Asymptotic $N$ -adic complexity	393
18.6	Consequences and questions	401
18.7	Exercises	402
<b>PART IV</b>	<b>ALGEBRAIC BACKGROUND</b>	405
<i>Appendix A</i>	<b>Abstract algebra</b>	407
A.1	Group theory	407
A.2	Rings	414
A.3	Polynomials	428
<i>Appendix B</i>	<b>Fields</b>	432
B.1	Field extensions	432
B.2	Finite fields	434
B.3	Quadratic forms over a finite field	442
B.4	Algebraic number fields	448
B.5	Local and global fields	451
<i>Appendix C</i>	<b>Finite local rings and Galois rings</b>	453
C.1	Finite local rings	453
C.2	Examples	455
C.3	Divisibility in $R[x]$	457
C.4	Tools for local rings	458
C.5	Galois rings	462
<i>Appendix D</i>	<b>Algebraic realizations of sequences</b>	464
D.1	Alternate representations of $\pi$ -adic numbers	464
D.2	Continued fractions	471
D.3	Exercises	480
	<i>Bibliography</i>	481
	<i>Index</i>	491

## Figures

3.1	An LFSR of length $m$ .	page 24
3.2	An LFSR of length 4 over $\mathbb{F}_2$ .	25
3.3	An LFSR of length 3 over $\mathbb{F}_3$ .	26
3.4	$R[[x]]$ as an inverse limit.	37
3.5	Phase taps: $b_n = a_{n+2} + a_{n+5}$ .	67
3.6	The graph $G_5$ .	67
4.1	An FCSR of length $m$ .	71
4.2	$\mathbb{Z}_N$ as an inverse limit.	77
5.1	Diagram of an AFSR.	97
6.1	$d$ -FCSR.	135
6.2	Parallelogram for $q = 5 + 2\pi$ .	149
7.1	Galois LFSR.	152
7.2	Division by $q(x)$ .	154
7.3	Galois FCSR.	154
7.4	Division by $q$ in $\mathbb{Z}_N$ .	157
7.5	Galois 2-FCSR.	158
7.6	Galois/Fibonacci LFSR.	163
7.7	Division by 5 in $\mathbb{Z}_3$ .	164
8.1	Generalized feedback shift register of length $k$ .	174
11.1	Gold sequence generator.	232
11.2	Geometric sequence generator.	235
12.1	Algebraic model for AFSR.	255
15.1	The Berlekamp–Massey algorithm.	299
15.2	LFSR with feedforward function.	312
15.3	Nonlinear combiner.	315
15.4	Cascaded clock controlled shift register of height = 3	318
16.1	The Euclidean rational approximation algorithm.	339
16.2	Rational approximation algorithm for 2-adic integers.	341
17.1	Xu's rational approximation algorithm.	351
18.1	A plot of $\delta_n^G(\mathbf{a})$ for $B = .25$ .	391
A.1	The Euclidean algorithm.	420
A.2	A lattice with basis $(5, 1), (3, 4)$ .	426
D.1	$R_\pi$ as an inverse limit.	465
D.2	Rational continued fraction expansion.	472

## Tables

3.1	States of the LFSR over $\mathbb{F}_2$ with $q(x) = x^4 + x^3 + 1$ .	page 26
3.2	States of the LFSR over $\mathbb{F}_3$ with $q(x) = x^3 + 2x - 1$ .	26
4.1	Comparison of LFSRs and FSRs.	70
4.2	The states of a 2-adic FCSR with $q = 37$ .	88
5.1	The states of an AFSR with $R = \mathbb{Z}$ , $p = \pi = 2$ , and $q = 27$ .	121
5.2	The states of an AFSR with $R = \mathbb{Z}[\pi]$ , $\pi = 2^{1/2}$ , and $q = 3\pi - 1$ .	122
5.3	The first 15 states of an AFSR over $\mathbb{Z}[\pi, \gamma]$ with $\pi^2 = 2$ , $\gamma^2 = \gamma + 1$ , and $q = (2\gamma + 3)\pi - 1$ .	124
5.4	One period of an AFSR over $\mathbb{Z}$ with $\pi = 3$ and $q = 43 = \pi^3 + 2\pi^2 - 2$ .	125
5.5	The states of an AFSR with $R = \mathbb{Z}$ , $\pi = 2$ , and $q = 27 = 16\pi - 5$ .	125
5.6	The states of an AFSR with $R = \mathbb{Z}$ , $\pi = 2$ , and $q = 27 = 6\pi^2 + 3 \cdot \pi - 3$ .	126
5.7	One period of an AFSR over $\mathbb{F}_2[x]$ with $\pi = x^2 + x + 1$ and $q = \pi^2 + x\pi + x$ .	127
5.8	One period of an AFSR over $\mathbb{F}_2[x, y]/(y^2 + x^3 + 1)$ with $\pi = x^2 + y$ and $q = \pi^2 + y\pi + 1$ .	128
5.9	Monomials $yx^i$ as sums of powers of $\pi$ .	129
5.10	The first 16 states of an AFSR over $\mathbb{F}_2[x]$ with $\pi = x^2 + x + 1$ and $q = \pi^2 + x\pi + x$ .	129
5.11	The states of an AFSR over the Gaussian domain using $S_2$ .	131
6.1	Model states for $q = 5 + 2\pi$ .	150
8.1	Numbers of occurrences of values of $H$ .	177
9.1	Properties of $L$ versus properties of $\mathbf{a}$ .	198
10.1	Cross-correlation of quadratically decimated sequences.	221
11.1	Cross-correlation for Gold sequences.	234
13.1	Values of $q$ giving rise to binary $\ell$ -sequences for length $\leq 11$ .	276
13.2	Values of $q$ giving rise to binary $\ell$ -sequences for length 12 and 13.	277
13.3	Values of $q$ giving rise to ternary $\ell$ -sequences for $q \leq 10\,000$ .	278
13.4	Values of $q$ giving rise to 5-ary $\ell$ -sequences for $q \leq 10\,000$ .	279
13.5	Values of $q$ giving rise to 6-ary $\ell$ -sequences for $q \leq 10\,000$ .	280
13.6	Values of $q$ giving rise to 7-ary $\ell$ -sequences for $q \leq 10\,000$ .	281
13.7	Values of $q$ giving rise to 10-ary $\ell$ -sequences for $q \leq 10\,000$ .	282
14.1	Values of $q$ giving rise to binary 2- $\ell$ -sequences for length $\leq 11$ .	284

15.1	Translation between continued fraction convergents and Berlekamp–Massey approximations.	304
B.1	Quadratic forms in characteristic 2.	439
B.2	Classification of quadratic forms over $\mathbb{F}_q$ .	444
B.3	Number of solutions to $Q(x) = u$ .	445
B.4	Number of solutions to $Q(x) + L(x) = u$ .	446
B.5	The quadratic form $\text{Tr}(cx^d)$ , $d = 1 + q^i$ .	447
B.6	$\gcd(b^n \pm 1, b^j \pm 1)$ .	447