
Contents

1. Introduction	1
1.1 Introduction to Fast Algorithms	1
1.2 Applications of Fast Algorithms	6
1.3 Number Systems for Computation	8
1.4 Digital Signal Processing	9
1.5 History of Fast Signal Processing Algorithms	17
Problems	18
Notes	19
2. Introduction to Abstract Algebra	20
2.1 Groups	21
2.2 Rings	25
2.3 Fields	29
2.4 Vector Spaces	33
2.5 Matrix Algebra	36
2.6 The Integer Ring	43
2.7 Polynomial Rings	47
2.8 The Chinese Remainder Theorems	56
Problems	62
Notes	64

3. Fast Algorithms for Short Convolutions	65
3.1 Cyclic Convolution and Linear Convolution	66
3.2 The Cook-Toom Algorithm	68
3.3 Winograd Short Convolution Algorithms	76
3.4 Design of Short Linear Convolution Algorithms	84
3.5 Polynomial Products Modulo a Polynomial	89
3.6 Design of Short Cyclic Convolution Algorithms	91
3.7 Convolution in General Fields and Rings	97
3.8 Complexity of Convolution Algorithms	99
Problems	109
Notes	113
4. Fast Algorithms for the Discrete Fourier Transform	114
4.1 The Cooley-Tukey Fast Fourier Transform	115
4.2 Small-Radix Cooley-Tukey Algorithms	118
4.3 The Good-Thomas Fast Fourier Transform	127
4.4 The Goertzel Algorithm	131
4.5 Fourier Transforms Computed by Using Convolutions	133
4.6 The Winograd Small Fast Fourier Transform	142
Problems	152
Notes	153
5. Number Theory and Algebraic Field Theory	155
5.1 Elementary Number Theory	155
5.2 Finite Fields Based on the Integer Ring	162
5.3 Fields Based on Polynomial Rings	165
5.4 Minimal Polynomials and Conjugates	167
5.5 Cyclotomic Polynomials	169
5.6 Primitive Elements	172
Problems	174
Notes	175
6. Computation in Surrogate Fields	176
6.1 Convolution in Surrogate Fields	177
6.2 Fermat Number Transforms	180
6.3 Mersenne Number Transforms	182
6.4 Convolution Algorithms for Finite Fields	185
6.5 Complex Convolution in Surrogate Fields	188
6.6 Integer Ring Transforms	193
6.7 Chevillat Number Transforms	196

6.8	The Preparata-Sarwate Algorithm	196
	Problems	200
	Notes	201
7.	Fast Algorithms and Multidimensional Convolutions	202
7.1	Nested Convolution Algorithms	203
7.2	The Agarwal-Cooley Convolution Algorithm	208
7.3	Splitting Algorithms	215
7.4	Iterated Algorithms	219
7.5	Polynomial Representation of Extension Fields	225
7.6	Convolution with Polynomial Extension Fields	228
7.7	The Nussbaumer Polynomial Transforms	230
7.8	Fast Convolution of Polynomials	233
	Problems	237
	Notes	239
8.	Fast Algorithms and Multidimensional Transforms	240
8.1	Small-Radix Cooley-Tukey Algorithms	241
8.2	Nested Transform Algorithms	246
8.3	The Winograd Large Fast Fourier Transform	251
8.4	The Johnson-Burrus Fast Fourier Transform	258
8.5	Splitting Algorithms	261
8.6	An Improved Winograd Fast Fourier Transform	266
8.7	The Nussbaumer-Quandalle Permutation Algorithm	268
	Problems	280
	Notes	282
9.	Architecture of Filters and Transforms	283
9.1	Convolution by Sections	284
9.2	Algorithms for Short Filter Sections	289
9.3	Iterated Filter Sections	292
9.4	Symmetric and Skew-Symmetric Filters	297
9.5	Decimating and Interpolating Filters	303
9.6	Autocorrelation and Crosscorrelation	306
9.7	Construction of Transform Computers	313
9.8	Limited-Range Fourier Transforms	318
	Problems	319
	Notes	320

10. Fast Algorithms Based on Doubling Strategies	322
10.1 Halving and Doubling Strategies	323
10.2 Data Structures	327
10.3 Fast Algorithms for Sorting	328
10.4 A Recursive Radix-Two Fast Fourier Transform	330
10.5 Fast Transposition	333
10.6 Matrix Multiplication	336
10.7 A Recursive Euclidean Algorithm	339
10.8 Computation of Trigonometric Functions	344
Problems	350
Notes	351
11. Fast Algorithms for Solving Toeplitz Systems	352
11.1 The Levinson and Durbin Algorithms	353
11.2 The Trench Algorithm	362
11.3 The Berlekamp-Massey Algorithm	368
11.4 A Recursive Berlekamp-Massey Algorithm	376
11.5 Methods Based on the Euclidean Algorithm	379
Problems	385
Notes	386
12. Fast Algorithms for Trellis and Tree Search	387
12.1 Trellis and Tree Searching	388
12.2 The Viterbi Algorithm	392
12.3 The Stack Algorithm	395
12.4 The Fano Algorithm	399
Problems	404
Notes	405
Appendix A. A Collection of Cyclic Convolution Algorithms	407
Appendix B. A Collection of Winograd Small FFT Algorithms	418
References	427
Index	435