

Contents

Chapter 1 Introduction

1.1	Introductory Remarks	1
1.2	Notations	2
1.3	The Structure of the Book	3

Chapter 2 Elements of Number Theory and Polynomial Algebra

2.1	Elementary Number Theory	4
2.1.1	Divisibility of Integers	4
2.1.2	Congruences and Residues	7
2.1.3	Primitive Roots	11
2.1.4	Quadratic Residues	17
2.1.5	Mersenne and Fermat Numbers	19
2.2	Polynomial Algebra	22
2.2.1	Groups	23
2.2.2	Rings and Fields	24
2.2.3	Residue Polynomials	25
2.2.4	Convolution and Polynomial Product Algorithms in Polynomial Algebra.	27

Chapter 3 Fast Convolution Algorithms

3.1	Digital Filtering Using Cyclic Convolutions	32
3.1.1	Overlap-Add Algorithm	33
3.1.2	Overlap-Save Algorithm	34
3.2	Computation of Short Convolutions and Polynomial Products	34
3.2.1	Computation of Short Convolutions by the Chinese Remainder Theorem	35
3.2.2	Multiplications Modulo Cyclotomic Polynomials	37
3.2.3	Matrix Exchange Algorithm	40
3.3	Computation of Large Convolutions by Nesting of Small Convolutions.	43
3.3.1	The Agarwal-Cooley Algorithm.	43
3.3.2	The Split Nesting Algorithm	47
3.3.3	Complex Convolutions	52
3.3.4	Optimum Block Length for Digital Filters	55
3.4	Digital Filtering by Multidimensional Techniques	56
3.5	Computation of Convolutions by Recursive Nesting of Polynomials	60
3.6	Distributed Arithmetic	64

3.7	Short Convolution and Polynomial Product Algorithms	66
3.7.1	Short Circular Convolution Algorithms	66
3.7.2	Short Polynomial Product Algorithms	73
3.7.3	Short Aperiodic Convolution Algorithms	78

Chapter 4 The Fast Fourier Transform

4.1	The Discrete Fourier Transform	80
4.1.1	Properties of the DFT.	81
4.1.2	DFTs of Real Sequences.	83
4.1.3	DFTs of Odd and Even Sequences	84
4.2	The Fast Fourier Transform Algorithm	85
4.2.1	The Radix-2 FFT Algorithm	87
4.2.2	The Radix-4 FFT Algorithm	91
4.2.3	Implementation of FFT Algorithms	94
4.2.4	Quantization Effects in the FFT	96
4.3	The Rader-Brenner FFT.	99
4.4	Multidimensional FFTs	102
4.5	The Bruun Algorithm	104
4.6	FFT Computation of Convolutions	107

Chapter 5 Linear Filtering Computation of Discrete Fourier Transforms

5.1	The Chirp z -Transform Algorithm.	112
5.1.1	Real Time Computation of Convolutions and DFTs Using the Chirp z -Transform.	113
5.1.2	Recursive Computation of the Chirp z -Transform.	114
5.1.3	Factorizations in the Chirp Filter	115
5.2	Rader's Algorithm	116
5.2.1	Composite Algorithms.	118
5.2.2	Polynomial Formulation of Rader's Algorithm	120
5.2.3	Short DFT Algorithms	123
5.3	The Prime Factor FFT	125
5.3.1	Multidimensional Mapping of One-Dimensional DFTs.	125
5.3.2	The Prime Factor Algorithm	127
5.3.3	The Split Prime Factor Algorithm.	129
5.4	The Winograd Fourier Transform Algorithm (WFTA).	133
5.4.1	Derivation of the Algorithm	133
5.4.2	Hybrid Algorithms	138
5.4.3	Split Nesting Algorithms.	139
5.4.4	Multidimensional DFTs	141
5.4.5	Programming and Quantization Noise Issues	142
5.5	Short DFT Algorithms	144
5.5.1	2-Point DFT	145
5.5.2	3-Point DFT	145

5.5.3	4-Point DFT	145
5.5.4	5-Point DFT	146
5.5.5	7-Point DFT	146
5.5.6	8-Point DFT	147
5.5.7	9-Point DFT	148
5.5.8	16-Point DFT	149
 Chapter 6 Polynomial Transforms		
6.1	Introduction to Polynomial Transforms	151
6.2	General Definition of Polynomial Transforms	155
6.2.1	Polynomial Transforms with Roots in a Field of Polynomials	157
6.2.2	Polynomial Transforms with Composite Roots	161
6.3	Computation of Polynomial Transforms and Reductions	163
6.4	Two-Dimensional Filtering Using Polynomial Transforms	165
6.4.1	Two-Dimensional Convolutions Evaluated by Polynomial Transforms and Polynomial Product Algorithms	166
6.4.2	Example of a Two-Dimensional Convolution Computed by Polynomial Transforms	168
6.4.3	Nesting Algorithms	170
6.4.4	Comparison with Conventional Convolution Algorithms	172
6.5	Polynomial Transforms Defined in Modified Rings	173
6.6	Complex Convolutions	177
6.7	Multidimensional Polynomial Transforms	178
 Chapter 7 Computation of Discrete Fourier Transforms by Polynomial Transforms		
7.1	Computation of Multidimensional DFTs by Polynomial Transforms	181
7.1.1	The Reduced DFT Algorithm	182
7.1.2	General Definition of the Algorithm.	186
7.1.3	Multidimensional DFTs	193
7.1.4	Nesting and Prime Factor Algorithms	194
7.1.5	DFT Computation Using Polynomial Transforms Defined in Modified Rings of Polynomials.	196
7.2	DFTs Evaluated by Multidimensional Correlations and Polynomial Transforms	201
7.2.1	Derivation of the Algorithm	201
7.2.2	Combination of the Two Polynomial Transform Methods	205
7.3	Comparison with the Conventional FFT.	206
7.4	Odd DFT Algorithms	207
7.4.1	Reduced DFT Algorithm. $N=4$	209
7.4.2	Reduced DFT Algorithm. $N=8$	209
7.4.3	Reduced DFT Algorithm. $N=9$	209
7.4.4	Reduced DFT Algorithm. $N=16$	210

Chapter 8 Number Theoretic Transforms

8.1	Definition of the Number Theoretic Transforms	211
8.1.1	General Properties of NTTs	213
8.2	Mersenne Transforms	216
8.2.1	Definition of Mersenne Transforms	216
8.2.2	Arithmetic Modulo Mersenne Numbers	219
8.2.3	Illustrative Example.	221
8.3	Fermat Number Transforms	222
8.3.1	Definition of Fermat Number Transforms	223
8.3.2	Arithmetic Modulo Fermat Numbers	224
8.3.3	Computation of Complex Convolutions by FNTs	227
8.4	Word Length and Transform Length Limitations	228
8.5	Pseudo Transforms	230
8.5.1	Pseudo Mersenne Transforms	231
8.5.2	Pseudo Fermat Number Transforms.	234
8.6	Complex NTTs.	236
8.7	Comparison with the FFT	239

Appendix A Relationship Between DFT and Convolution Polynomial Transform Algorithms

A.1	Computation of Multidimensional DFT's by the Inverse Polynomial Transform Algorithm	241
A.1.1	The Inverse Polynomial Transform Algorithm	241
A.1.2	Complex Polynomial Transform Algorithms	244
A.1.3	Round-off Error Analysis	246
A.2	Computation of Multidimensional Convolutions by a Combination of the Direct and Inverse Polynomial Transform Methods	247
A.2.1	Computation of Convolutions by DFT Polynomial Transform Algorithms	248
A.2.2	Convolution Algorithms Based on Polynomial Transforms and Permutations.	249
A.3	Computation of Multidimensional Discrete Cosine Transforms by Polynomial Transforms	251
A.3.1	Computation of Direct Multidimensional DCT's	251
A.3.2	Computation of Inverse Multidimensional DCT's	253

Appendix B Short Polynomial Product Algorithms 255

Problems	263
References	269
Subject Index	275