

Contents

Preface	vii
1 Introduction	1
1.1 Digital Signal Processing	2
1.2 Digital Communications	4
2 Mathematical Fundamentals	7
2.1 Algebraic Fields	7
2.2 Elementary Number Theory	11
2.3 Extension Fields	15
2.3.1 Fields of Characteristic 2	17
2.3.2 Fields That Mimic the Complex Field	19
2.3.3 Fields That Cannot Mimic the Complex Field	19
2.3.4 Fields of Rational Functions	20
2.3.5 Cyclotomic Extensions of the Rational Field	21
2.4 Rings and Groups	23
2.5 Algebraic Integers	26
3 Sequences and Spectra	29
3.1 Weight and Complexity	29
3.1.1 Linear Complexity	30
3.1.2 Cyclic Complexity	31
3.1.3 Linear and Cyclic Complexity	32
3.2 The Fourier Transform	33
3.3 Examples of Fourier Transforms	35
3.4 Properties of the Fourier Transform	37
3.4.1 Cyclic Decimation	39
3.4.2 The Cyclic Complexity Property	42
3.4.3 Conjugacy Constraints	43
3.5 Decimation of Shift Register Sequences	45
3.6 A Universal Eigenvector	46
3.7 Bounds on the Weight of Sequences	50
3.8 The Gleason–Prange Theorem	52
4 Cyclic Codes and Related Codes	57
4.1 Theory of Reed–Solomon Codes	57
4.2 Reed–Solomon Codes in Infinite Fields	60

4.2.1	Reed–Solomon Codes in the Complex Field	60
4.2.2	Reed–Solomon Codes in the Extended Rationals	61
4.3	Reed–Solomon Codes in Finite Fields	62
4.4	Radix-2 Reed–Solomon Codes	65
4.5	Conjugacy Constraints and BCH Codes	66
5	Fast Algorithms for Convolution	71
5.1	Convolution by Blocks	71
5.2	Fast Algorithms for Cyclic Convolution	74
5.3	Convolution of Integer Sequences	80
5.4	Convolutions Using Residue Number Systems	83
5.5	Convolution of Polynomial Sequences	84
6	Solving Toeplitz Systems	89
6.1	The Sugiyama Algorithm	89
6.2	The Berlekamp–Massey Algorithm	92
6.3	Relationships Between Algorithms	97
6.4	The Levinson and Durbin Algorithms	98
7	Fast Algorithms for the Fourier Transform	105
7.1	The Cooley–Tukey FFT	105
7.2	Radix-2 Transforms	106
7.3	The Good–Thomas FFT	109
7.4	FFT Algorithms for Subblocks	111
7.5	FFT Algorithms Using Algebraic Integers	114
7.6	The Winograd FFT	115
8	Decoding of Cyclic Codes	119
8.1	Decoding of Reed–Solomon Codes	119
8.1.1	The Forney Algorithm	121
8.1.2	The Berlekamp Algorithm	122
8.2	Erasures and Errors Decoding	125
8.3	Time Domain Decoder Algorithms	127
8.3.1	A Time Domain Decoder with n^2 Steps	128
8.3.2	A Time Domain Decoder with $2tn$ Steps	129
8.3.3	A Time Domain Decoder with (More Than) $4t^2$ Steps	131
8.4	A Universal Decoder Architecture	132
	References	135
	Index	139