

Contents

		page
<i>Preface</i>		xi
<i>List of Abbreviations</i>		xiii
1 Introduction		1
1.1 Historical Notes		10
References		10
2 Basics		12
2.1 Finite Fields and Vector Spaces		12
2.1.1 Implementation of Operations on Finite Fields		13
2.1.2 Vectors in $\text{GF}(q)^n$		18
2.2 Communication Channel and Decision Rules		20
2.3 Linear Block Codes		22
2.4 Classical Codes for Erasure Channels		31
2.4.1 Reed–Solomon Codes		32
2.4.2 Other Forms of MDS Codes		36
2.4.3 Erasure Correction with RS Codes		36
2.4.4 RS Codes for Errors and Erasures		38
2.4.5 An Alternative Decoding Algorithm for RS Codes		43
2.5 Historical Notes		45
2.6 Exercises		46
References		47
3 Erasure Channel Models and Bounds		49
3.1 Memoryless Erasure Channels		49
3.1.1 Discrete Memoryless Channels		49
3.1.2 The Binary Erasure Channel		51
3.2 Bounds on the Block Error Probability		53
3.2.1 Code Ensembles		54
3.2.2 Singleton Bound		55
3.2.3 Random Coding Bounds		57
3.3 Erasure Channels with Memory		59
3.3.1 Single Burst Erasure Channels		60
3.3.2 Block Erasure Channels		61
3.3.3 Gilbert Erasure Channel		64

3.4	Historical Notes	67
3.5	Exercises	67
	References	69
4	Low-Density Parity-Check Codes	71
4.1	Basics	71
4.1.1	Tanner Graph	71
4.1.2	Regular and Irregular LDPC Codes	74
4.1.3	Encoding of LDPC Codes	75
4.2	LDPC Code Ensembles	77
4.2.1	Unstructured Irregular and Regular LDPC Code Ensembles	77
4.2.2	Partially Structured Ensembles	80
4.2.3	Protograph LDPC Code Ensemble	87
4.3	Historical Notes	89
4.4	Exercises	91
	References	93
5	Weight Distribution and Minimum Distance of LDPC Codes	96
5.1	Assignments in Tanner Graphs	96
5.2	Basics of Generating Functions	97
5.3	Weight Enumerating Functions of Replicated Codes	99
5.4	Weight Distributions of Unstructured LDPC Code Ensembles	102
5.4.1	Regular Ensembles	102
5.4.2	Irregular Ensembles	103
5.5	Weight Distributions of Protograph LDPC Code Ensembles	105
5.6	Weight Spectral Shapes	107
5.6.1	Basics	107
5.6.2	Weight Spectral Shape of Linear Random Ensembles	108
5.6.3	Weight Spectral Shape of Unstructured LDPC Code Ensembles	109
5.6.4	Weight Spectral Shape of Protograph LDPC Code Ensembles	119
5.7	Minimum Distance Analysis	123
5.8	Historical Notes	129
5.9	Exercises	129
	References	132
6	Iterative and Maximum-Likelihood Decoding of LDPC Codes	133
6.1	Iterative Decoding	133
6.1.1	Belief Propagation Decoding of Binary LDPC Codes	133
6.1.2	Belief Propagation Algorithm over the BEC	137
6.1.3	Peeling Decoding	140
6.1.4	Stopping Sets	141
6.1.5	Iterative Decoding of Nonbinary LDPC Codes	144
6.1.6	Iterative Decoding for Packet Erasures	145

6.2	Maximum-Likelihood Decoding	147
6.2.1	Structured Gaussian Elimination	149
6.2.2	Guessing Decoder	154
6.3	Historical Notes	156
6.4	Exercises	157
	References	159
7	Iterative LDPC Decoder Analysis	161
7.1	Density Evolution Analysis for Unstructured Ensembles	161
7.1.1	Extrinsic Erasure Probability Evolution on Regular and Irregular Trees	161
7.1.2	Density Evolution for Unstructured LDPC Code Ensembles	164
7.1.3	Density Evolution for Unstructured Irregular LDPC Code Ensembles	165
7.1.4	Iterative Decoding Threshold for Unstructured LDPC Code Ensembles	166
7.1.5	Stability Condition for Unstructured Ensembles	167
7.2	Extrinsic Information Transfer Analysis	168
7.2.1	EXIT Functions	168
7.2.2	EXIT Charts	169
7.3	Density Evolution Analysis for Structured Ensembles	175
7.3.1	Analysis of IRA Ensembles	175
7.3.2	Protograph Ensembles	177
7.4	Finite-Length Analysis	180
7.4.1	Stopping Set Size Enumerating Function	180
7.4.2	Union Bound on the Block Error Probability	182
7.5	Code Design for the Belief Propagation Decoder	184
7.5.1	Capacity Achieving Sequences	185
7.5.2	LDPC Code Design via Numerical Optimization	187
7.6	Code Design for Erasure Channels with Memory	189
7.6.1	Single Burst Erasure Channel	189
7.6.2	Stopping Set Pivots and Their Span	190
7.6.3	Pivot Search and Swap Algorithm	191
7.6.4	Results for the Block and Gilbert Erasure Channels	194
7.7	Historical Notes	197
7.8	Exercises	198
	References	199
8	Maximum-Likelihood LDPC Decoder Analysis	202
8.1	Asymptotic Performance Analysis	202
8.2	Finite-Length Analysis	210
8.3	Code Design for Maximum-Likelihood Decoders	212
8.4	Code Design for Channels with Memory	215
8.4.1	Single Burst Erasure Channels	215
8.4.2	Block and Gilbert Erasure Channels	218
8.5	Historical Notes	223

8.6	Exercises	225
	References	226
9	Low-Density Parity-Check Codes: Generalizations	228
9.1	Spatially Coupled Low-Density Parity-Check Codes	228
9.1.1	Protograph-Based Spatially Coupled LDPC Code Ensembles	228
9.1.2	Belief Propagation Decoding and Threshold Saturation	233
9.1.3	Windowed Decoding	236
9.1.4	Finite-Length Performance	241
9.2	Generalized Low-Density Parity-Check Codes	242
9.2.1	Tanner Graph and Parity-Check Matrix	243
9.2.2	Decoding of GLDPC Codes on Erasure Channels	246
9.2.3	GLDPC Code Ensembles	250
9.3	Low-Density Generator Matrix Codes	258
9.3.1	Code Structure	258
9.3.2	LDGM Decoding	261
9.3.3	Tornado Codes	263
9.4	Historical Notes	264
9.5	Exercises	265
	References	267
10	Polar Codes	269
10.1	Reed-Muller Codes	269
10.2	Decomposing Multi-input Multi-output Channels for Successive Cancellation Decoding	271
10.2.1	The Linear Transformation $F_2^{\otimes m}$ as a Way to Introduce Channel Polarization	274
10.3	Decoding of Polar Codes	280
10.4	SC Performance Bounds	282
10.5	Historical Notes	284
10.6	Exercises	285
	References	286
11	Fountain Codes	288
11.1	Preliminary Definitions	288
11.2	LT Codes	291
11.2.1	Encoding	291
11.2.2	Peeling Decoding	291
11.2.3	Design of the Degree Distribution	292
11.2.4	Limitations	295
11.3	Raptor Codes	297
11.3.1	Encoding	297
11.3.2	Two-Stage Decoding	297
11.3.3	Performance Analysis	298
11.4	Maximum-Likelihood Decoding of LT and Raptor Codes	299
11.4.1	Performance Analysis	299

11.5	Historical Notes	304
11.6	Exercises	305
	References	307

Appendix A	Applications of Erasure Codes	309
A.1	Reliable Data Transmission	309
A.2	Distributed Storage	311
A.2.1	Availability and Storage Efficiency	312
A.2.2	Decoding Complexity	312
A.2.3	Node Repair Problem	313
A.2.4	Access Latency	315
A.3	Further Applications	315
A.3.1	Distributed Computing	315
A.3.2	Network Coding with Application to Coded Caching	317
A.3.3	Privacy	318
	References	319

Appendix B	Random Matrices over Finite Fields	322
	References	324

<i>Index</i>		325
--------------	--	-----