

Contents

Preface — IX

Acknowledgment — XIII

Notation — XV

Of Theorems, Lemmata and Corollaries — XVII

1 Introduction — Sophisticated Channel Codes for Advanced Mobile Communications — 1

- 1.1 Oh my! Oh my! Yet Another Book About... Channel Coding — **1**
- 1.2 Of Sophisticated Channel Codes — **7**
- 1.3 General Concept of Channel Codes — **12**
- 1.4 Vector Spaces Over $\mathbb{F}_2$ — **17**
- 1.5 Linear Channel Codes — **30**
- 1.6 Syndrome and Error Detection — **51**
- 1.7 Error-Detecting and Error-Correcting Capabilities of an (n, k) Binary Linear Block Code — **53**
 - 1.7.1 Undetectable and Detectable Transmission Errors — **53**
 - 1.7.2 Transmission Error Probability Without Decoding — **54**
 - 1.7.3 Transmission Error Probability With Decoding — **68**
- 1.8 Syndrome Decoding of an $(n, k, d_{\min})$ Binary Linear Block Code ∇ — **83**
- 1.9 Some Examples of $(n, k, d_{\min})$ Binary Linear Block Codes — **92**
 - 1.9.1 Binary Linear Single-Parity Check Code — **92**
 - 1.9.2 Binary Linear Repetition Code — **93**
 - 1.9.3 Binary Maximum Distance Separable (MDS) Codes — **94**
 - 1.9.4 Self-Dual Codes — **96**
 - 1.9.5 Hamming Codes — **97**
 - 1.9.6 Simplex Codes — **98**
- 1.10 Six Strategies to Construct New Codes from Old — **100**
- 1.11 Cyclic $(n, k, d_{\min})$ Binary Linear Block Codes — **103**
- 1.12 A Primer on Number Theory — **112**
 - 1.12.1 Nulls, Units, Irreducible Numbers, Prime Numbers and Composite Numbers — **112**
 - 1.12.2 Rings, Integral Domains and Euclidean Domains — **115**
 - 1.12.3 Euclidean Algorithm — **129**
 - 1.12.4 Unique Factorization in Euclidean Domains — **152**

1.12.5	Construction of the Finite Field $\mathbb{F}_{2^n}$ —	165
1.12.6	Minimal Polynomials, Conjugates and Cyclotomic Cosets —	172
1.12.7	Finding Irreducible Polynomials —	189
1.13	Cyclic $(n, k, d_{\min})$ Binary Linear Block Codes Revisited —	193
1.13.1	Ideals and Generator Polynomials —	193
1.13.2	Check Polynomial —	198
1.13.3	Inversion Formula —	200
1.13.4	Idempotents —	201
1.13.5	Minimal Ideals and Primitive Idempotents —	206
1.14	Some Examples of Cyclic $(n, k, d_{\min})$ Binary Linear Block Codes —	216
1.14.1	Introductory Remark —	216
1.14.2	Cyclic Hamming Codes —	217
1.14.3	Cyclic Simplex Codes —	219
1.14.4	Double-error-correcting Bose–Chaudhuri–Hocquenghem (BCH) Codes —	220
1.15	Permutation Matrices —	221
1.16	Kronecker Product —	224
1.17	Reed–Muller (RM) Codes —	233
1.17.1	Definition of Reed–Muller (RM) Codes —	233
1.17.2	Properties of Reed–Muller (RM) Codes —	242
1.17.3	Punctured Reed–Muller (RM) Codes —	254
1.17.4	Constructing Reed–Muller (RM) Codes Using the Kronecker Product —	267
1.17.5	Subcodes of Reed–Muller (RM) Codes —	270
1.18	Convolutional Codes —	277
2	Convolutional Turbo Codes —	294
2.1	Rise and Fall —	294
2.2	Parallel Concatenation of Recursive Systematic Convolutional (RSC) Codes —	298
2.3	Decoding of Convolutional Turbo Codes —	304
3	Low Density Parity Check (LDPC) Codes —	313
3.1	Definition of Low Density Parity Check (LDPC) Codes —	313
3.2	Decoding of Low Density Parity Check (LDPC) Codes —	321
3.2.1	Tanner Graphs —	321
3.2.2	Log-Likelihood Ratio Processing in Parity Check Sums —	327
3.2.3	Sum Product Algorithm —	332
4	Polar Codes —	336
4.1	Channel Polarization Paradigm —	336
4.2	Recursive Definition of Generator Matrices —	351
4.3	Channel Combining Revisited —	354

- 4.4 Channel Splitting Revisited — **355**
- 4.5 Performance of Polar Codes With Finite Length — **385**

Bibliography — 389

Index — 395