Contents

Preface xiii
Acknowledgment xv
About the Companion Website xvii

1 Introduction 1
1.1 What is Distributed Source Coding? 2
1.2 Historical Overview and Background 2
1.3 Potential and Applications 3
1.4 Outline 4

Part I Theory of Distributed Source Coding 7

2 Lossless Compression of Correlated Sources 9
2.1 Slepian–Wolf Coding 10
2.1.1 Proof of the SW Theorem 15
Achievability of the SW Theorem 16
Converse of the SW Theorem 19
2.2 Asymmetric and Symmetric SW Coding 21
2.3 SW Coding of Multiple Sources 22

3 Wyner–Ziv Coding Theory 25
3.1 Forward Proof of WZ Coding 27
3.2 Converse Proof of WZ Coding 29
3.3 Examples 30
3.3.1 Doubly Symmetric Binary Source 30
Problem Setup 30
A Proposed Scheme 31
Verify the Optimality of the Proposed Scheme 32
3.3.2 Quadratic Gaussian Source 35
Contents

35 Problem Setup

36 Proposed Scheme

37 Verify the Optimality of the Proposed Scheme

38 3.4 Rate Loss of the WZ Problem

39 Binary Source Case

39 Rate loss of General Cases

41 4 Lossy Distributed Source Coding

42 4.1 Berger–Tung Inner Bound

42 4.1.1 Berger–Tung Scheme

42 4.1.2 Codebook Preparation

42 4.1.3 Encoding

43 4.1.4 Decoding

43 4.1.5 Distortion Analysis

44 44 Pr(\mathcal{E}_1) \to 0

44 44 Pr(\mathcal{E}_1^C \cap \mathcal{E}_2) \to 0

44 44 Pr(\mathcal{E}_1^C \cap \mathcal{E}_2^C \cap \mathcal{E}_3) \to 0

44 44 Pr(\mathcal{E}_4) \to 0

44 44 Pr(\mathcal{E}_5), Pr(\mathcal{E}_6) \to 0

45 4.2 Indirect Multiterminal Source Coding

45 4.2.1 Quadratic Gaussian CEO Problem with Two Encoders

46 4.2.2 Forward Proof of Quadratic Gaussian CEO Problem with Two Terminals

48 4.2.3 Converse Proof of Quadratic Gaussian CEO Problem with Two Terminals

54 4.3 Direct Multiterminal Source Coding

55 4.3.1 Forward Proof of Gaussian Multiterminal Source Coding Problem with Two Sources

59 59 Case 1: (1 - D_2) \leq \rho^2(1 - D_1)

62 62 Case 2: (1 - D_2) > \rho^2(1 - D_1)

63 4.3.2 Converse Proof of Gaussian Multiterminal Source Coding Problem with Two Sources

64 64 Bounds for R_1 and R_2

66 66 Collaborative Lower Bound

67 67 \mu\text{-sum Bound}

75 Part II Implementation

77 5 Slepian–Wolf Code Designs Based on Channel Coding

77 5.1 Asymmetric SW Coding

78 5.1.1 Binning Idea

79 5.1.2 Syndrome-based Approach
Contents

Hamming Binning 80
SW Encoding 80
SW Decoding 80
LDPC-based SW Coding 81
5.1.3 Parity-based Approach 82
5.1.4 Syndrome-based Versus Parity-based Approach 84
5.2 Non-asymmetric SW Coding 85
5.2.1 Generalized Syndrome-based Approach 86
5.2.2 Implementation using IRA Codes 88
5.3 Adaptive Slepian–Wolf Coding 90
5.3.1 Particle-based Belief Propagation for SW Coding 91
5.4 Latest Developments and Trends 93

6 Distributed Arithmetic Coding 97
6.1 Arithmetic Coding 97
6.2 Distributed Arithmetic Coding 101
6.3 Definition of the DAC Spectrum 103
6.3.1 Motivations 103
6.3.2 Initial DAC Spectrum 104
6.3.3 Depth-\(i\) DAC Spectrum 105
6.3.4 Some Simple Properties of the DAC Spectrum 107
6.4 Formulation of the Initial DAC Spectrum 107
6.5 Explicit Form of the Initial DAC Spectrum 110
6.6 Evolution of the DAC Spectrum 113
6.7 Numerical Calculation of the DAC Spectrum 116
6.7.1 Numerical Calculation of the Initial DAC Spectrum 117
6.7.2 Numerical Estimation of DAC Spectrum Evolution 118
6.8 Analyses on DAC Codes with Spectrum 120
6.8.1 Definition of DAC Codes 121
6.8.2 Codebook Cardinality 122
6.8.3 Codebook Index Distribution 123
6.8.4 Rate Loss 123
6.8.5 Decoder Complexity 124
6.8.6 Decoding Error Probability 126
6.9 Improved Binary DAC Codec 130
6.9.1 Permutated BDAC Codec 130
   Principle 130
   Proof of SW Limit Achievability 131
6.9.2 BDAC Decoder with Weighted Branching 132
6.10 Implementation of the Improved BDAC Codec 134
6.10.1 Encoder 134
   Principle 134
   Implementation 135
6.10.2 Decoder 135
   Principle 135
   Implementation 136

6.11 Experimental Results 138
   Effect of Segment Size on Permutation Technique 139
   Effect of Surviving-Path Number on WB Technique 139
   Comparison with LDPC Codes 139
   Application of PBDAC to Nonuniform Sources 140

6.12 Conclusion 141

7 Wyner–Ziv Code Design 143
  7.1 Vector Quantization 143
  7.2 Lattice Theory 146
     7.2.1 What is a Lattice? 146
         Examples 146
         Dual Lattice 147
         Integral Lattice 147
         Lattice Quantization 148
     7.2.2 What is a Good Lattice? 149
         Packing Efficiency 149
         Covering Efficiency 150
         Normalized Second Moment 150
         Kissing Number 150
         Some Good Lattices 151
  7.3 Nested Lattice Quantization 151
     Encoding/decoding 152
     Coset Binning 152
     Quantization Loss and Binning Loss 153
     SW Coded NLQ 154
     7.3.1 Trellis Coded Quantization 154
     7.3.2 Principle of TCQ 155
         Generation of Codebooks 156
         Generation of Trellis from Convolutional Codes 156
         Mapping of Trellis Branches onto Sub-codebooks 157
         Quantization 157
         Example 158
  7.4 WZ Coding Based on TCQ and LDPC Codes 159
     7.4.1 Statistics of TCQ Indices 159
     7.4.2 LLR of Trellis Bits 162
     7.4.3 LLR of Codeword Bits 163
     7.4.4 Minimum MSE Estimation 163
     7.4.5 Rate Allocation of Bit-planes 164
     7.4.6 Experimental Results 166
Part III Applications 167

8 Wyner–Ziv Video Coding 169
8.1 Basic Principle 169
8.2 Benefits of WZ Video Coding 170
8.3 Key Components of WZ Video Decoding 171
8.3.1 Side-information Preparation 171
Bidirectional Motion Compensation 172
8.3.2 Correlation Modeling 173
Exploiting Spatial Redundancy 174
8.3.3 Rate Controller 175
8.4 Other Notable Features of Miscellaneous WZ Video Coders 175

9 Correlation Estimation in DVC 177
9.1 Background to Correlation Parameter Estimation in DVC 177
9.1.1 Correlation Model in WZ Video Coding 177
9.1.2 Offline Correlation Estimation 178
Pixel Domain Offline Correlation Estimation 178
Transform Domain Offline Correlation Estimation 180
9.1.3 Online Correlation Estimation 181
Pixel Domain Online Correlation Estimation 182
Transform Domain Online Correlation Estimation 184
9.2 Recap of Belief Propagation and Particle Filter Algorithms 185
9.2.1 Belief Propagation Algorithm 185
9.2.2 Particle Filtering 186
9.3 Correlation Estimation in DVC with Particle Filtering 187
9.3.1 Factor Graph Construction 187
9.3.2 Correlation Estimation in DVC with Particle Filtering 190
9.3.3 Experimental Results 192
9.3.4 Conclusion 197
9.4 Low Complexity Correlation Estimation using Expectation Propagation 199
9.4.1 System Architecture 199
9.4.2 Factor Graph Construction 199
Joint Bit-plane SW Coding (Region II) 200
Correlation Parameter Tracking (Region I) 201
9.4.3 Message Passing on the Constructed Factor Graph 202
Expectation Propagation 203
9.4.4 Posterior Approximation of the Correlation Parameter using Expectation Propagation 204
Moment Matching 205
9.4.5 Experimental Results 206
9.4.6 Conclusion 211
## Contents

### 10 DSC for Solar Image Compression 213

10.1 Background 213
10.2 Related Work 215
10.3 Distributed Multi-view Image Coding 217
10.4 Adaptive Joint Bit-plane WZ Decoding of Multi-view Images with Disparity Estimation 217
   10.4.1 Joint Bit-plane WZ Decoding 217
   10.4.2 Joint Bit-plane WZ Decoding with Disparity Estimation 219
   10.4.3 Joint Bit-plane WZ Decoding with Correlation Estimation 220
10.5 Results and Discussion 221
10.6 Summary 224

### 11 Secure Distributed Image Coding 225

11.1 Background 225
11.2 System Architecture 227
   11.2.1 Compression of Encrypted Data 228
   11.2.2 Joint Decompression and Decryption Design 230
11.3 Practical Implementation Issues 233
11.4 Experimental Results 233
   11.4.1 Experiment Setup 234
   11.4.2 Security and Privacy Protection 235
   11.4.3 Compression Performance 236
11.5 Discussion 239

### 12 Secure Biometric Authentication Using DSC 241

12.1 Background 241
12.2 Related Work 243
12.3 System Architecture 245
   12.3.1 Feature Extraction 246
   12.3.2 Feature Pre-encryption 248
   12.3.3 SeDSC Encrypter/decrypter 248
   12.3.4 Privacy-preserving Authentication 249
   12.4 SeDSC Encrypter Design 249
   12.4.1 Non-asymmetric SW Codes with Code Partitioning 250
   12.4.2 Implementation of SeDSC Encrypter using IRA Codes 251
   12.5 SeDSC Decrypter Design 252
12.6 Experiments 256
   12.6.1 Dataset and Experimental Setup 256
   12.6.2 Feature Length Selection 257
   12.6.3 Authentication Accuracy 257
   Authentication Performances on Small Feature Length (i.e., \(N = 100\)) 257
   Performances on Large Feature Lengths (i.e., \(N \geq 300\)) 258
12.6.4 Privacy and Security 259
12.6.5 Complexity Analysis 261
12.7 Discussion 261

A Basic Information Theory 263
A.1 Information Measures 263
A.1.1 Entropy 263
A.1.2 Relative Entropy 267
A.1.3 Mutual Information 268
A.1.4 Entropy Rate 269
A.2 Independence and Mutual Information 270
A.3 Venn Diagram Interpretation 273
A.4 Convexity and Jensen's Inequality 274
A.5 Differential Entropy 277
A.5.1 Gaussian Random Variables 278
A.5.2 Entropy Power Inequality 278
A.6 Typicality 279
A.6.1 Jointly Typical Sequences 282
A.7 Packing Lemmas and Covering Lemmas 284
A.8 Shannon's Source Coding Theorem 286
A.9 Lossy Source Coding—Rate-distortion Theorem 289
A.9.1 Rate-distortion Problem with Side Information 291

B Background on Channel Coding 293
B.1 Linear Block Codes 294
B.1.1 Syndrome Decoding of Block Codes 295
B.1.2 Hamming Codes, Packing Bound, and Perfect Codes 295
B.2 Convolutional Codes 297
B.2.1 Viterbi Decoding Algorithm 298
B.3 Shannon's Channel Coding Theorem 301
B.3.1 Achievability Proof of the Channel Coding Theorem 303
B.3.2 Converse Proof of Channel Coding Theorem 305
B.4 Low-density Parity-check Codes 306
B.4.1 A Quick Summary of LDPC Codes 306
B.4.2 Belief Propagation Algorithm 307
B.4.3 LDPC Decoding using BP 312
B.4.4 IRA Codes 314

C Approximate Inference 319
C.1 Stochastic Approximation 319
C.1.1 Importance Sampling Methods 320
C.1.2 Markov Chain Monte Carlo 321
Markov Chains 321
Markov Chain Monte Carlo 321
C.2 Deterministic Approximation 322
C.2.1 Preliminaries 322
Exponential Family 322
Kullback–Leibler Divergence 323
Assumed-density Filtering 324
C.2.2 Expectation Propagation 325
Relationship with BP 326
C.2.3 Relationship with Other Variational Inference Methods 328

D Multivariate Gaussian Distribution 331
D.1 Introduction 331
D.2 Probability Density Function 331
D.3 Marginalization 332
D.4 Conditioning 333
D.5 Product of Gaussian pdfs 334
D.6 Division of Gaussian pdfs 337
D.7 Mixture of Gaussians 337
D.7.1 Reduce the Number of Components in Gaussian Mixtures 338
Which Components to Merge? 340
How to Merge Components? 341
D.8 Summary 342
Appendix: Matrix Equations 343

Bibliography 345

Index 357