

# Contents

Preface — IX

List of Figures — XIX

## 1 Introduction — 1

- 1.1 What is information? — 2
- 1.2 Why are there physical limits to information processing? — 5
  - 1.2.1 Erasure — 6
- 1.3 Quantum limits and possibilities — 8
  - 1.3.1 Copying — 8
  - 1.3.2 Cryptography — 11
- 1.4 Overview of the book — 13
- 1.5 Notes and further reading — 14

## Part I: Formalism of probability and quantum theory

## 2 Probability theory — 19

- 2.1 Boolean algebras of events — 20
- 2.2 The rules of probability — 21
  - 2.2.1 Definition — 21
  - 2.2.2 The law of total probability — 23
  - 2.2.3 Bayes' rule — 24
  - 2.2.4 The Dutch book argument — 24
- 2.3 Random variables — 26
  - 2.3.1 Joint, marginal, and conditional distributions — 26
  - 2.3.2 Vector representation — 27
- 2.4 Convexity — 28
- 2.5 Independence — 30
- 2.6 Additional exercises — 33
- 2.7 Notes and further reading — 34

## 3 Classical channels — 36

- 3.1 Definition — 36
- 3.2 Alternate definitions — 39
- 3.3 Notes and further reading — 43

## 4 Quantum probability theory — 44

- 4.1 States, effects, and measurements — 45
- 4.2 Qubits — 48

|          |                                                    |           |
|----------|----------------------------------------------------|-----------|
| 4.3      | Comparison with probability theory —               | 51        |
| 4.4      | Composite systems —                                | 52        |
| 4.4.1    | Entangled states —                                 | 52        |
| 4.4.2    | Bell bases and Weyl–Heisenberg operators —         | 53        |
| 4.4.3    | Marginal states and the partial trace —            | 55        |
| 4.4.4    | Classical-quantum states —                         | 56        |
| 4.5      | Isomorphism of operators and bipartite vectors —   | 57        |
| 4.6      | Notes and further reading —                        | 59        |
| <b>5</b> | <b>Quantum channels —</b>                          | <b>60</b> |
| 5.1      | Definition —                                       | 61        |
| 5.1.1    | First considerations —                             | 61        |
| 5.1.2    | Complete positivity —                              | 63        |
| 5.2      | Everything is a channel —                          | 65        |
| 5.3      | The Choi isomorphism —                             | 67        |
| 5.4      | The Kraus representation —                         | 70        |
| 5.5      | Two further isomorphisms —                         | 73        |
| 5.5.1    | The Jamiołkowski isomorphism —                     | 73        |
| 5.5.2    | The Liouville isomorphism —                        | 74        |
| 5.6      | Notes and further reading —                        | 76        |
| <b>6</b> | <b>Purification —</b>                              | <b>77</b> |
| 6.1      | Purification of density operators —                | 77        |
| 6.2      | Ensembles and purifications —                      | 78        |
| 6.2.1    | Schmidt decomposition —                            | 78        |
| 6.2.2    | Steering —                                         | 80        |
| 6.3      | Dilation of channels —                             | 82        |
| 6.4      | Relationship of Choi, Kraus, and Stinespring —     | 84        |
| 6.5      | Information disturbance —                          | 86        |
| 6.6      | Coherent classical information (?) —               | 88        |
| 6.6.1    | Classical information via copying —                | 88        |
| 6.6.2    | Classical information via observable restriction — | 89        |
| 6.6.3    | Consistency —                                      | 90        |
| 6.6.4    | The quantum eraser —                               | 91        |
| 6.7      | Notes and further reading —                        | 92        |
| <b>7</b> | <b>Quantum mysteries —</b>                         | <b>93</b> |
| 7.1      | Complementarity —                                  | 93        |
| 7.2      | Hidden variables —                                 | 96        |
| 7.2.1    | Hidden variables for the interferometer —          | 96        |
| 7.2.2    | Local hidden variables for the interferometer —    | 97        |
| 7.3      | Bell’s theorem and the CHSH inequality —           | 99        |

- 7.3.1 Further implications — 102
- 7.4 Notes and further reading — 103

## Part II: Resource measures

### 8 Basic resources — 107

- 8.1 Converses for classical communication — 108
  - 8.1.1 Over classical channels — 108
  - 8.1.2 Over quantum channels — 110
- 8.2 Converses for quantum communication — 111
  - 8.2.1 Over classical channels — 111
  - 8.2.2 Over quantum channels — 113
- 8.3 Assisted communication: dense coding and teleportation — 114
- 8.4 Converses for assisted classical communication — 116
  - 8.4.1 Over classical channels — 116
  - 8.4.2 Over quantum channels — 117
- 8.5 Converses for assisted quantum communication — 119
  - 8.5.1 Over quantum channels — 119
  - 8.5.2 Over classical channels — 120
- 8.6 Entanglement distillation — 121
- 8.7 Notes and further reading — 122

### 9 Discriminating states and channels — 123

- 9.1 Two approaches — 123
- 9.2 Bayesian hypothesis testing — 125
- 9.3 Neyman–Pearson hypothesis testing — 128
  - 9.3.1 Testing region — 128
  - 9.3.2 Optimal tests — 130
- 9.4 Distinguishability — 131
- 9.5 Channel distinguishability — 134
  - 9.5.1 Definition — 134
  - 9.5.2 Composability — 135
  - 9.5.3 SDP formulation — 135
  - 9.5.4 Need for entanglement — 137
- 9.6 Notes and further reading — 138

### 10 Fidelity — 140

- 10.1 Definition — 140
- 10.2 Closed-form expression — 141
- 10.3 SDP formulation — 142
- 10.4 Further properties — 144

|           |                                                           |            |
|-----------|-----------------------------------------------------------|------------|
| 10.4.1    | Achievability by measurement —                            | 144        |
| 10.4.2    | Bounds between fidelity and distinguishability —          | 145        |
| 10.4.3    | Triangle inequality —                                     | 146        |
| 10.5      | Channel fidelity —                                        | 148        |
| 10.5.1    | Definition and SDP formulation —                          | 148        |
| 10.5.2    | Comparing a channel to the identity —                     | 151        |
| 10.5.3    | Channel fidelity of unitary channels —                    | 152        |
| 10.6      | Notes and further reading —                               | 153        |
| <b>11</b> | <b>Optimal and pretty good receivers —</b>                | <b>154</b> |
| 11.1      | Optimal recovery of classical information —               | 154        |
| 11.1.1    | Definition —                                              | 154        |
| 11.1.2    | Classical case —                                          | 155        |
| 11.1.3    | SDP formulation —                                         | 155        |
| 11.1.4    | Largest and smallest values —                             | 156        |
| 11.1.5    | Monotonicity and chain rules —                            | 157        |
| 11.1.6    | Conditions on the optimal measurement —                   | 158        |
| 11.2      | Pretty good recovery of classical information —           | 158        |
| 11.3      | Optimal entanglement recovery —                           | 160        |
| 11.3.1    | Definition —                                              | 160        |
| 11.4      | Pretty good entanglement recovery —                       | 161        |
| 11.5      | Monotonicity of pretty good recoveries —                  | 163        |
| 11.6      | Notes and further reading —                               | 165        |
| <b>12</b> | <b>Entropy —</b>                                          | <b>167</b> |
| 12.1      | Entropy and relative entropy —                            | 168        |
| 12.2      | Conditional entropy and mutual information —              | 171        |
| 12.3      | Stein's lemma —                                           | 175        |
| 12.3.1    | Achievability in the quantum case —                       | 177        |
| 12.3.2    | Converse in the quantum case —                            | 178        |
| 12.4      | The data processing inequality —                          | 180        |
| 12.5      | Additional exercises —                                    | 182        |
| 12.6      | Notes and further reading —                               | 183        |
| <b>13</b> | <b>Uncertainty relations —</b>                            | <b>185</b> |
| 13.1      | Guessing games —                                          | 186        |
| 13.2      | Entropic uncertainty relations —                          | 188        |
| 13.3      | Guessing probability and fidelity uncertainty relations — | 191        |
| 13.3.1    | Statement —                                               | 191        |
| 13.3.2    | Proof of the tripartite bound —                           | 192        |
| 13.3.3    | Proof of the bipartite bound —                            | 193        |
| 13.4      | Notes and further reading —                               | 195        |

## Part III: Information processing protocols

### 14 Data compression — 199

- 14.1 Compression of classical data — 200
  - 14.1.1 Setup and basic properties — 200
  - 14.1.2 One-shot bounds — 201
  - 14.1.3 Optimal asymptotic i. i. d. rate — 202
- 14.2 Compression of quantum data — 203
  - 14.2.1 Setup and basic properties — 203
  - 14.2.2 Achievability from classical compression — 204
  - 14.2.3 Converse — 206
  - 14.2.4 Optimal asymptotic i. i. d. rate — 206
- 14.3 Notes and further reading — 207

### 15 Classical communication over noisy channels — 208

- 15.1 Setup and basic properties — 208
- 15.2 Converse — 210
- 15.3 Achievability — 212
- 15.4 Coding for i. i. d. channels — 215
  - 15.4.1 Capacity — 215
  - 15.4.2 Finite-blocklength bounds — 218
- 15.5 Classical coding over quantum channels — 220
  - 15.5.1 Recycling the CQ result — 220
  - 15.5.2 Capacity expression — 220
  - 15.5.3 Properties of the Holevo information — 221
- 15.6 Notes and further reading — 222

### 16 Information reconciliation — 223

- 16.1 Setup and basic properties — 224
- 16.2 Converse — 225
- 16.3 Achievability — 226
  - 16.3.1 Statement — 226
  - 16.3.2 Universal hashing — 227
  - 16.3.3 Syndrome decoding — 228
- 16.4 Reconciliation of i. i. d. sources — 228
- 16.5 Notes and further reading — 228

### 17 Entanglement distillation — 230

- 17.1 Setup and basic properties — 230
- 17.2 Converse — 231
- 17.3 Achievability for a special case — 231
  - 17.3.1 Linear hashing — 232

|           |                                                                  |            |
|-----------|------------------------------------------------------------------|------------|
| 17.3.2    | One-shot bound —                                                 | 233        |
| 17.3.3    | Distillation from i. i. d. states —                              | 235        |
| 17.4      | Notes and further reading —                                      | 235        |
| <b>18</b> | <b>Randomness extraction —</b>                                   | <b>236</b> |
| 18.1      | Setup and basic properties —                                     | 236        |
| 18.2      | Converse: from extraction to distillation —                      | 237        |
| 18.3      | Achievability: from reconciliation to extraction —               | 238        |
| 18.4      | Extraction from i. i. d. sources —                               | 239        |
| 18.5      | Notes and further reading —                                      | 240        |
| <b>19</b> | <b>Quantum error correction —</b>                                | <b>241</b> |
| 19.1      | Quantum communication: setup and basic properties —              | 241        |
| 19.1.1    | Definitions —                                                    | 241        |
| 19.1.2    | Reduction of worst case to average case —                        | 242        |
| 19.1.3    | Isometric encoding suffices —                                    | 242        |
| 19.1.4    | Reduction of noisy channel coding to entanglement distillation — | 243        |
| 19.2      | CSS codes —                                                      | 244        |
| 19.3      | Quantum coding theorems —                                        | 246        |
| 19.3.1    | Statement —                                                      | 246        |
| 19.3.2    | Converse —                                                       | 247        |
| 19.4      | Achievability —                                                  | 248        |
| 19.4.1    | Entanglement distillation protocol —                             | 248        |
| 19.4.2    | Rate calculation —                                               | 249        |
| 19.5      | Discussion of the achievability construction —                   | 250        |
| 19.5.1    | Complementary information —                                      | 250        |
| 19.5.2    | Error degeneracy —                                               | 251        |
| 19.5.3    | Channel degradability —                                          | 254        |
| 19.6      | Notes and further reading —                                      | 255        |
| <b>20</b> | <b>Quantum key distribution —</b>                                | <b>257</b> |
| 20.1      | Private communication over public channels —                     | 257        |
| 20.1.1    | Encryption —                                                     | 257        |
| 20.1.2    | Information-theoretic security —                                 | 257        |
| 20.1.3    | One-time pad —                                                   | 259        |
| 20.2      | Key distribution —                                               | 260        |
| 20.2.1    | Real and ideal resources —                                       | 260        |
| 20.2.2    | Approximate simulation —                                         | 261        |
| 20.3      | The BB84 protocol —                                              | 263        |
| 20.4      | Security and robustness analysis —                               | 265        |
| 20.4.1    | Sifting —                                                        | 265        |
| 20.4.2    | Information reconciliation —                                     | 266        |

- 20.4.3 Privacy amplification — 266
- 20.4.4 Security and robustness statement — 270
- 20.5 Discussion of the security proof — 270
- 20.6 Notes and further reading — 271

## **A The postulates of quantum mechanics — 273**

## **B Vectors and operators — 275**

- B.1 Linear operators — 275
- B.2 Dirac notation — 275
- B.3 Matrix representations — 277
- B.4 Tensor products — 278
- B.5 Positive operators — 280
- B.6 Operator decompositions — 281
- B.7 Inner products and norms of operators — 283
- B.8 The Schur complement — 284
- B.9 Operator monotonicity and convexity — 285
- B.10 Notes and further reading — 287

## **C Semidefinite programs — 289**

- C.1 General form — 289
- C.2 Duality — 290
- C.3 Notes and further reading — 294

## **Bibliography — 295**

## **Index of symbols — 309**

## **Index — 313**