Table of Contents

Notations xiii

Acknowledgments xv

Introduction xix

Chapter 1. Overview 1

1.1. Introduction 2
1.2. Quantum information 4
1.2.1. Principles 5
1.2.2. Imperfect quantum systems 7
1.2.3. Quantum computers 8
1.2.4. Applications of distributed quantum information 9
1.3. Quantum repeaters 10
1.3.1. Physical communication technologies 11
1.3.2. Multi-hop Bell pairs: quantum communication sessions 12
1.4. Network architectures 15
1.4.1. Semantics of distributed quantum information 16
1.4.2. Identifiers 17
1.4.3. Paths 17
1.4.4. Resource management discipline 18
1.4.5. A quantum internet 20
1.5. Conclusions 20

PART 1. FUNDAMENTALS 23

Chapter 2. Quantum Background 25

2.1. Introduction 26
2.2. Schrödinger's equation 28
2.3. Qubits 29
2.3.1. What is a qubit? 29
2.3.2. Quantum registers and weighted probabilities 30
2.3.3. Interference 32
2.3.4. Entanglement 33
2.3.5. Decoherence 34
2.3.6. Pure and mixed states and the density matrix 34
2.3.7. Fidelity 37
2.3.8. Measurement 38
2.3.9. The partial trace 39
2.4. Manipulating qubits 41
2.4.1. What is a quantum gate? 41
2.4.2. Single-qubit gates and the Bloch sphere 41
2.4.3. Global versus relative phase 44
2.4.4. Two-qubit gates 45
2.4.5. Quantum circuits 46
2.5. Bell pairs 47
2.5.1. The Bell basis 49
2.5.2. Measurement in the Bell basis 49
2.5.3. The Bell inequalities and non-locality 50
2.5.4. Experimental demonstration of violation of Bell's inequality . . . 52
2.6. The no-cloning theorem 53
2.7. Conclusion 54

Chapter 3. Networking Background 55

3.1. Concepts 56
3.1.1. Multihop communication: networks as graphs 56
3.1.2. Resources 59
3.1.3. Protocols 60
3.1.4. Naming and addressing 61
3.1.5. Security 62
3.2. Challenges in scaling up networks 63
3.2.1. Heterogeneity 63
3.2.2. Scale 64
3.2.3. Dealing with out-of-date information 64
3.2.4. Organizational needs 64
3.2.5. Misbehaving nodes 65

3.3. Design patterns 65
3.3.1. Hierarchy 65
3.3.2. Layering 66
3.3.3. Narrow waist 67
3.3.4. Multiplexing resources 68
3.3.5. Smart versus dumb networks 70
3.3.6. Distributed management and autonomy 70
3.3.7. State machines 71
3.3.8. Weak consistency and soft failure 72
3.3.9. Distributed routing protocols 73
3.3.10. Overlays, virtualization and recursion 74
3.4. The Internet 75
3.5. Conclusion 77

Chapter 4. Teleportation 79

4.1. The basic teleportation operation 79
4.2. Experimental demonstration of teleportation 82
4.3. State machines for teleportation 84
4.4. Teleporting gates 86
4.5. Conclusion 88

PART 2. APPLICATIONS 91

Chapter 5. Quantum Key Distribution 93

5.1. QKD and the purpose of cryptography 94
5.2. BB84: single-photon QKD 97
5.3. E91: entanglement-based protocol 100
5.4. Using QKD 101
5.4.1. Campus-to-campus virtual private network 101
5.4.2. Transport-layer security (TLS) 103
5.4.3. Resilience of networks dependent on QKD 104
5.5. Existing QKD networks 105
5.6. Classical control protocols 109
5.7. Conclusion 111

Chapter 6. Distributed Digital Computation and Communication 113

6.1. Useful distributed quantum states 114
6.1.1. The stabilizer representation 114
6.1.2. GHZ and W states 115
6.1.3. Graph states 116
6.2. Coin flipping 118
6.2.1. The simplest multi-party distributed quantum protocol 118

6.2.2. QKD-Based protocols 118
6.2.3. Practical, optimal quantum strong coin flipping 119
6.3. Leader election 119
6.3.1. The second simplest multi-party distributed quantum protocol . . 120
6.3.2. Tani *et al.*'s quantum protocol 120
6.4. Quantum secret sharing 121
6.4.1. Semi-classical, multi-party secret creation 121
6.4.2. The basic quantum secret sharing protocol 122
6.4.3. Verifiable quantum secret sharing and secure multi-party quantum computation 124
6.5. Byzantine agreement 126
6.5.1. The original problem 126
6.5.2. Ben-Or and Hassidim's quantum Byzantine agreement 127
6.6. Client-server and blind computation 128
6.7. Conclusion 130

Chapter 7. Entangled States as Reference Frames 131

7.1. Qubits in the environment 131
7.1.1. Precession 132
7.1.2. Quantum optical interference 133
7.2. Distributed clock synchronization 135
7.2.1. Chuang's algorithms 135
7.2.2. Jozsa *et al.*'s clock synchronization 138
7.2.3. Further work 140
7.3. Very long baseline optical interferometry 141
7.4. Conclusion 145

PART 3. LINES OF REPEATERS 147

Chapter 8. Physical Entanglement and Link-Layer Protocols 149

8.1. Creating entanglement using light 149
8.1.1. Quantum states of light 149
8.1.2. Emission 151
8.1.3. Transport 152
8.1.4. Detection 154
8.2. Memory and transceiver qubits 156
8.2.1. Gate noise 157
8.2.2. Single-qubit decoherence 158
8.2.3. Two-qubit decoherence 160
8.3. Link structure 161
8.4. State machines and protocol interactions 163

8.5. Managing density matrices in distributed software 164
8.5.1. Link-Level tracking of memory 167
8.5.2. Synchronizing higher layers 168
8.6. Examples 169
8.7. Conclusion 173

Chapter 9. Purification 175

9.1. Measurement revisited 175
9.2. Basic purification 177
9.2.1. Bit flip errors 178
9.2.2. Generalizing: incorporating phase flip errors and different Bell pairs 179
9.2.3. Multiple rounds and error redistribution 182
9.2.4. Resource consumption in multiple rounds 184
9.3. Scheduling purification 185
9.4. State machines and protocol interactions 187
9.5. More complex purification protocols 190
9.6. Experimental demonstrations 192
9.7. Conclusion 193

Chapter 10. Purification and Entanglement Swapping-Based Repeaters 195

10.1. Hardware architectures 195
10.2. Getting from here to there 197
10.2.1. Hop-by-hop teleportation 197
10.2.2. Basic entanglement swapping 200
10.2.3. Multi-hop swapping 202
10.3. Nested purification session architecture 203
10.3.1. Proof of polynomial resource growth 203
10.3.2. Problems to avoid 204
10.4. State machines and protocol interactions 206
10.5. Putting it all together 208
10.5.1. Simulating lines of repeaters 209
10.5.2. Greedy algorithm 211
10.5.3. Banded performance v. total distance 212
10.5.4. Finding the bands 212
10.5.5. Varying swapping thresholds 213
10.6. Considerations in the design of a simulator 215
10.7. Conclusion 217

Chapter 11. Quantum Error Correction-Based Repeaters 219

11.1. Quantum error correction 220
11.1.1. Steane code 221

11.1.2. Surface code 221
11.1.3. An early communication proposal 223
11.2. CSS repeaters 223
11.2.1. Protocols 225
11.2.2. Operational timing 227
11.2.3. Resources and performance 229
11.3. Surface code repeaters 230
11.3.1. Protocols 232
11.3.2. Operational timing 233
11.3.3. Resources and performance 234
11.4. Conclusion 235

Chapter 12. Finessing the Key Limitations 237

12.1. Quasi-asynchronous 238
12.1.1. Purification replacement operation 240
12.1.2. QEC-based operation 241
12.1.3. Timing variants 242
12.2. Memoryless 244
12.3. Summary: comparing quantum communication approaches 247
12.4. Conclusion 251

PART 4. NETWORKS OF REPEATERS 253

Chapter 13. Resource Management and Multiplexing 255

13.1. Simulated network and traffic 256
13.1.1. Network topology and simulator 256
13.1.2. Traffic load 258
13.1.3. Adjusting link target fidelity 258
13.2. Simulations 259
13.2.1. Circuit switching: upper and lower throughput bounds 259
13.2.2. Other multiplexing disciplines 260
13.3. Conclusion 263

Chapter 14. Routing 265

14.1. Introduction 265
14.2. Difficulties: differences between quantum and classical networks . . . 267
14.3. Problems and solutions 268
14.4. Simulation and results 270
14.4.1. The behavior questions 271
14.4.2. Simulated hardware and link costs 271
14.4.3. Simulated path candidates 274

14.4.4. Answering our behavior questions 275
14.4.5. Solving our problems 280
14.5. Conclusion 283

Chapter 15. Quantum Recursive Network Architecture 285

15.1. Review: network architecture 286
15.2. Recursive quantum requests 288
15.2.1. Processing in recursive networks 289
15.2.2. Naming a state 290
15.2.3. Defining quantum requests 291
15.3. Implementing recursion in quantum networks 294
15.3.1. Satisfying quantum requests 294
15.3.2. Paths and rendezvous points 294
15.4. Example 295
15.5. Conclusion 298

Chapter 16. Coda 301

16.1. Future development 301
16.1.1. Hardware 301
16.1.2. Making QRNA real 302
16.2. Open problems 303
16.3. Further readings for depth 304
16.3.1. Quantum repeaters and QKD 304
16.3.2. Optics and general quantum physics 304
16.3.3. Quantum computing 304
16.4. Further readings for breadth 305
16.4.1. Information theory 305
16.4.2. Dense coding 305
16.4.3. Quantum network coding 306
16.4.4. Entanglement percolation 306
16.5. Final thoughts 307

Bibliography 309

Index 331