Hiroshi Imai Masahito Hayashi (Eds.)

Quantum Computation and Information

From Theory to Experiment

With 49 Figures

Springer

Contents

Part I Quantum Computation

Quantum Identification of Boolean Oracles
Andris Ambainis, Kazuo Iwama, Akinori Kawachi, Rudy Raymond, Shigeru Yamashita . . . 3
1 Introduction . . . 3
2 Formalization . . . 5
3 General Upper Bounds . . . 8
4 Relation With Learning Theory . . . 11
5 Tight Upper Bounds for Small *M* . . . 12
6 Classical Lower and Upper Bounds . . . 14
7 Concluding Remarks . . . 15
References . . . **16**
Index . . . 18

Query Complexity of Quantum Biased Oracles
Kazuo Iwama, Rudy Raymond, Shigeru Yamashita . . . 19
1 Introduction . . . 19
2 Goldreich-Levin Problem and Biased Oracles . . . 21
2.1 The Model of Quantum Biased Oracles . . . 26
3 Upper Bounds of the Query Complexity of Biased Oracles With Special Conditions . . . 27
3.1 Basic Tools for Quantum Computation . . . 27
3.2 Quantum Biased Oracles With the Same Bias Factor . . . 28
3.3 Quantum Biased Oracles With Resettable Condition . . . 33
4 Lower Bounds of the Query Complexity of Biased Oracles . . . 34
5 Concluding Remarks . . . 39
References . . . 40
Index . . . 42

Part II Quantum Information

Quantum Statistical Inference
Masahito Hayashi . . . **45**

1 Introduction . . . 45
2 Quantum State Estimation . . . 47
2.1 State Estimation in Pure State Family . . . 47
2.2 State Estimation for Covariant Pure States Family . . . 48
2.3 State Estimation in Gaussian States Family . . . 49
2.4 State Estimation in Nonregular Family . . . 51
2.5 Estimation of Eigenvalue of Density Matrix in Qubit System . 52
3 Estimation of SU(2) Action With Entanglement . . . 52
3.1 One-Parameter Case . . . 53
3.2 Three-Parameter Case . . . 53
4 Hypothesis Testing and Discrimination . . . 54
4.1 Hypothesis Testing of Entangled State . . . 54
4.2 Distinguishability and Indistinguishability by LOCC . . . 55
4.3 Application of Quantum Hypothesis Testing . . . 55
5 Experimental Application of Quantum Statistical Inference . . . 56
5.1 State Estimation in the Two-Qubit System . . . 57
5.2 Testing of Entangled State in the SPDC System . . . 57
6 Analysis on Quantum Measurement . . . 58
6.1 Quantum Measurement With Negligible State Demolition 58
6.2 Quantum Universal Compression . . . 58
References . . . 59
Index . . . 61

Quantum Cloning Machines

Heng Fan . . . 63
1 Introduction . . . 63
2 Bužek and Hillery Universal Quantum Cloning Machine . . . 63
3 N to M UQCM (Gisin and Massar) . . . 65
4 Universal Quantum Cloning Machine for General d-Dimensional System, Werner Cloning Machine . . . 65
5 A UQCM for d-Dimensional Quantum State Proposed by Fan et al. 66
6 Further Results About the UQCM . . . 67
6.1 UQCM for 2-Level System . . . 68
6.2 UQCM for d-Level System . . . 71
7 UQCM Realized in Real Physical Systems . . . 74
8 UQCM for Identical Mixed States . . . 79
8.1 A 2 to 3 Universal Quantum Cloning for Mixed States . . . 79
8.2 General 2 to $M(M > 2)$ UQCM . . . 81
9 Phase-Covariant Quantum Cloning Machine . . . 81
10 Transformation . . . 82
11 Hilbert-Schmidt Norm . . . 84
12 Bures Fidelity . . . 88
13 Quantum Cloning for $x — y$ Equatorial Qubits . . . 90
14 Quantum Cloning Networks for Equatorial Qubits . . . 91
15 Separability of Copied Qubits and Quantum Triplicators . . . 93

15.1 Separability . . . 93
15.2 Optimal Quantum Triplicators . . . 94
16 Optimal 1 to *M* Phase-Covariant Quantum Cloning Machines . . . 96
17 Some Known Results About Phase-Covariant Quantum Cloning Machine for Qubits and Qutrits . . . 98
18 Phase-Covariant Cloning of Qudits . . . 100
19 About Phase-Covariant Quantum Cloning Machines . . . 103
20 Cerf's Asymmetric Quantum Cloning Machine . . . 103
21 Duan and Guo Probabilistic Quantum Cloning Machine . . . 106
22 A Brief Summary . . . 107
References . . . 107
Index . . . 109

Entanglement and Quantum Error Correction

Tohya Hiroshima, Masahito Hayashi . . . Ill
1 Introduction . . . 1ll
2 Entanglement Distillation . . . 1ll
2.1 Background of Concentration . . . 112
2.2 Exponents of Optimal Concentration . . . 112
2.3 Universal Entanglement Concentration . . . 113
2.4 Entanglement in Boson-Fock Space . . . 114
2.5 Computation of Distillable Entanglement of a Certain Class of Bipartite Mixed States . . . 115
3 Quantum Error Correction . . . 116
3.1 Mathematical Formulation of Quantum Channel . . . 117
3.2 Background of Information Theory and Coding Theory . . . 117
3.3 Exponential Evaluation of Quantum Error Correcting Codes . 118
3.3.1 Extensions . . . 118
3.4 Relation Between Teleportation and Entanglement Distillation . . . 119
3.5 Application to Quantum Key Distribution . . . 120
4 Basic Characteristics of Bipartite Entanglement . . . 121
4.1 Concurrence Hierarchy . . . 121
4.2 Optimal Compression Rates and Entanglement of Purification 122
4.3 Simultaneous Schmidt Decomposition and Maximally Correlated States . . . 123
4.4 Bell-Type Inequalities Via Combinatorial Approach . . . 123
4.5 Quantum Graph Coloring Game . . . 124
5 SLOCC Convertibility . . . 124
5.1 Multipartite Entanglement . . . 124
5.2 Bipartite Entanglement in Infinite-Dimensional Space . . . 126
6 Protocols Assisted by Multipartite Entangled State . . . 128
6.1 Teleportation by W State . . . 128
6.2 Remote State Preparation of Entangled State . . . 128
References . . . 129

Index 132

On Additivity Questions

Keiji Matsumoto 133
1 Introduction 133
2 Additivity Questions: Definitions and Comments 134
2.1 Holevo Capacity, Output Minimum Entropy, and Maximum Output p-Norm 134
2.2 Entanglement of Formation 137
3 Linking Additivity Conjectures 138
3.1 Channel States 138
3.2 Strong Superadditivity and Additivity of Holevo Capacity . . . 140
3.3 Equivalence Theorem by Shor, and One More New Equivalent Additivity Question 141
3.4 Group Symmetry 143
3.5 Analysis of Examples 146
3.5.1 Example 1 146
3.5.2 Example 2 147
3.5.3 Example 3 148
4 Additivity for Special Cases 149
4.1 Additivity of WH Channel 149
5 Numerical Studies on Additivity Questions 153
5.1 A Qubit Channel That Requires Four Input States 153
5.1.1 Some Useful Facts 153
5.1.2 Setup 154
5.1.3 Heuristic Construction of a Four-State Channel 154
5.1.4 Approximation Algorithm to Compute the Holevo Capacity 155
5.1.5 Numerical Verification of Four-State Channel 156
5.1.6 Numerical Check of Additivity 157
5.2 Strong Superadditivity of EoF of Pure States 159
References 161
Index 164

Part III Quantum Security

Quantum Computational Cryptography

Akinori Kawachi, Takeshi Koshiba 167
1 Introduction 167
2 Quantum One-Wayness of Permutations 168
2.1 Notations and Basic Operators 170
2.2 Worst-Case Characterization 170
2.3 Average-Case Characterization 171
2.4 Universal Tests 175

3 Quantum Public-Key Cryptosystem 176
3.1 Cryptographic Properties of QSCD^ 177
3.2 Trapdoor Property 178
3.3 Reduction From the Worst Case to the Average Case 178
3.4 Hardness of QSCD^ 179
3.5 Construction 180
3.6 Remarks 182
References 182
Index 184

Quantum Key **Distribution: Security, Feasibility and Robustness**
Xiang-Bin Wang 185
1 Introduction 185
2 Security Proof of BB84 QKD With Perfect Single-Photon Source . . 187
2.1 Hashing and Error-Correction in Classical Communication . . . 188
2.2 The Main Idea of Entanglement Purification 190
2.3 Error Test 192
2.4 Entanglement Purification by Hashing 192
2.4.1 Bit-Flip Error Correction 193
2.4.2 Phase-Flip Error Correction 194
2.5 Classicalization 195
3 Secure Key Distillation With a Known Fraction of Tagged Bits.... 196
3.1 Final Key Distillation With a Fraction of Tagged Bits 196
3.2 PNS Attack 198
4 The Decoy-State Method 200
4.1 The Main Ideas and Results 201
4.2 The Issue of Unconditional Security 206
4.3 Robustness Analysis 206
4.4 Final Key Rate and Further Studies 209
4.5 Summary 210
5 QKD With Asymmetric Channel Noise 210
5.1 Channel Error, Tested Error and Key-Bits Error 211
5.2 QKD With One-Way Classical Communication 212
5.3 Six-State Protocol With Two-Way Classical Communications. 214
6 Quantum Key Distribution With Encoded BB84 States 217
6.1 A Protocol For Collective Channel Noise 219
6.1.1 Protocol 1 and Security Proof 220
6.1.2 Protocol 2 221
6.1.3 Physical Realization 223
6.1.4 Another Protocol For Robust QKD With Swinging Objects 223
6.1.5 Summary and Discussion 224
6.2 A Protocol With Independent Noise 225
6.2.1 The Method and the Main Idea 225

6.2.2 The QPFER Code . . . 226
6.2.3 The Protocol and Its Linear Optical Realization . . . 227
6.2.4 Security Proof . . . 230
6.2.5 Subtlety of the "Conditional Advantage" . . . 230
7 Summary and Concluding Remarks . . . 231
References . . . 231
Index . . . 233

Why Quantum Steganography Can Be Stronger Than Classical Steganography
Shin Natori . . . 235
1 Introduction . . . 235
2 Definitions . . . 235
2.1 General Model of Steganography System . . . 235
2.2 Classical Model of Steganography System . . . 237
3 Related Works . . . 237
4 Quantum Steganography . . . 237
4.1 Model of Quantum Steganography System . . . 237
4.2 Comparison Between Classical and Quantum Steganography . 238
5 Conclusions and Future Work . . . 240
References . . . 240
Index . . . 240

Part IV Realization of Quantum Information System

Photonic Realization of Quantum Information Systems
Akihisa Tomita, Bao-Sen Shi . . . 243
1 Introduction . . . 243
2 Cryptography . . . 244
2.1 High-Sensitivity Photon Detector . . . 245
2.1.1 Requirement for Single-Photon Detectors . . . 245
2.1.2 Improved Single-Photon Detector for Fiber Transmission246
2.2 Single-Photon Transmission Over 150 km in a Unidirectional System With Integrated Interferometers . . . 248
2.3 Refinements Toward a Practical QKD System . . . 251
2.3.1 Temperature-Insensitive Interferometer . . . 251
2.3.2 High-Speed Operation . . . 253
3 Quantum Computation . . . 256
3.1 Measured Quantum Fourier Transform . . . 256
3.1.1 Implementation and Experimental Results . . . 256
3.1.2 Effects of Imperfection . . . 258
3.1.3 Validity of Majority Voting . . . 260
3.1.4 Toward Quantum Computers . . . 262
3.2 Control-Unitary Gates . . . 263

3.2.1 Solid-State Bell State Measurement Devices by Two-Photon Absorption . . . 264
4 Generation of Entangled Photon Pairs by SPDC . . . 265
4.1 SPDC With Two-Crystal Geometry . . . 266
4.2 Interferometric Generation of Entangled Photon Pairs . . . 269
4.3 A New Material for SPDC: Periodically Poled KTP . . . 270
5 Conclusion . . . 272
References . . . 273
Index . . . 275

Index . . . 277