## Contents

1 Mathematical Formulation of Quantum Systems .................................. 1
  1.1 Quantum Systems and Linear Algebra .................................. 1
  1.2 State and Measurement in Quantum Systems .......................... 5
  1.3 Quantum Two-Level Systems ........................................ 8
  1.4 Composite Systems and Tensor Products ........................... 10
  1.5 Matrix Inequalities and Matrix Monotone Functions ............ 15
  1.6 Solutions of Exercises ............................................. 18
  References ........................................................................ 24

2 Information Quantities and Parameter Estimation in Classical Systems ................................................. 25
  2.1 Information Quantities in Classical Systems ......................... 25
    2.1.1 Entropy ..................................................... 25
    2.1.2 Relative Entropy ........................................ 27
    2.1.3 Mutual Information ....................................... 33
    2.1.4 The Independent and Identical Condition
          and Rényi Entropy ....................................... 36
    2.1.5 Conditional Rényi Entropy ................................ 41
  2.2 Geometry of Probability Distribution Family ...................... 45
    2.2.1 Inner Product for Random Variables
          and Fisher Information .................................. 45
    2.2.2 Bregman Divergence ..................................... 50
    2.2.3 Exponential Family and Divergence ....................... 53
  2.3 Estimation in Classical Systems ..................................... 56
  2.4 Type Method and Large Deviation Evaluation ..................... 61
    2.4.1 Type Method and Sanov’s Theorem .......................... 61
    2.4.2 Cramér Theorem and Its Application to Estimation .... 64
  2.5 Continuity and Axiomatic Approach ................................. 71
  2.6 Large Deviation on Sphere ......................................... 77
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>State Evolution and Trace-Preserving Completely Positive Maps</td>
<td>197</td>
</tr>
<tr>
<td></td>
<td>5.1 Description of State Evolution in Quantum Systems</td>
<td>197</td>
</tr>
<tr>
<td></td>
<td>5.2 Examples of Trace-Preserving Completely Positive Maps</td>
<td>205</td>
</tr>
<tr>
<td></td>
<td>5.3 State Evolutions in Quantum Two-Level Systems</td>
<td>211</td>
</tr>
<tr>
<td></td>
<td>5.4 Information-Processing Inequalities in Quantum Systems</td>
<td>216</td>
</tr>
<tr>
<td></td>
<td>5.5 Entropy Inequalities in Quantum Systems</td>
<td>221</td>
</tr>
<tr>
<td></td>
<td>5.6 Conditional Rényi Entropy and Duality</td>
<td>228</td>
</tr>
<tr>
<td></td>
<td>5.7 Proof and Construction of Stinespring and Choi–Kraus Representations</td>
<td>234</td>
</tr>
<tr>
<td></td>
<td>5.8 Historical Note</td>
<td>238</td>
</tr>
<tr>
<td></td>
<td>5.8.1 Completely Positive Map and Quantum Relative Entropy</td>
<td>238</td>
</tr>
<tr>
<td></td>
<td>5.8.2 Quantum Relative Rényi entropy</td>
<td>239</td>
</tr>
<tr>
<td></td>
<td>5.9 Solutions of Exercises</td>
<td>239</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>250</td>
</tr>
<tr>
<td>6</td>
<td>Quantum Information Geometry and Quantum Estimation</td>
<td>253</td>
</tr>
<tr>
<td></td>
<td>6.1 Inner Products in Quantum Systems</td>
<td>253</td>
</tr>
<tr>
<td></td>
<td>6.2 Metric-Induced Inner Products</td>
<td>259</td>
</tr>
<tr>
<td></td>
<td>6.3 Geodesics and Divergences</td>
<td>265</td>
</tr>
<tr>
<td></td>
<td>6.4 Quantum State Estimation</td>
<td>273</td>
</tr>
<tr>
<td></td>
<td>6.5 Large Deviation Evaluation</td>
<td>278</td>
</tr>
<tr>
<td></td>
<td>6.6 Multiparameter Estimation</td>
<td>281</td>
</tr>
<tr>
<td></td>
<td>6.7 Relative Modular Operator and Quantum $f$-Relative Entropy</td>
<td>290</td>
</tr>
<tr>
<td></td>
<td>6.7.1 Monotonicity Under Completely Positivity</td>
<td>290</td>
</tr>
<tr>
<td></td>
<td>6.7.2 Monotonicity Under 2-Positivity</td>
<td>293</td>
</tr>
<tr>
<td></td>
<td>6.8 Historical Note</td>
<td>300</td>
</tr>
<tr>
<td></td>
<td>6.8.1 Quantum State Estimation</td>
<td>300</td>
</tr>
<tr>
<td></td>
<td>6.8.2 Quantum Channel Estimation</td>
<td>301</td>
</tr>
<tr>
<td></td>
<td>6.8.3 Geometry of Quantum States</td>
<td>302</td>
</tr>
<tr>
<td></td>
<td>6.8.4 Equality Condition for Monotonicity of Relative Entropy</td>
<td>303</td>
</tr>
<tr>
<td></td>
<td>6.9 Solutions of Exercises</td>
<td>304</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>318</td>
</tr>
<tr>
<td>7</td>
<td>Quantum Measurements and State Reduction</td>
<td>323</td>
</tr>
<tr>
<td></td>
<td>7.1 State Reduction Due to Quantum Measurement</td>
<td>323</td>
</tr>
<tr>
<td></td>
<td>7.2 Uncertainty and Measurement</td>
<td>329</td>
</tr>
<tr>
<td></td>
<td>7.2.1 Uncertainties for Observable and Measurement</td>
<td>329</td>
</tr>
<tr>
<td></td>
<td>7.2.2 Disturbance</td>
<td>331</td>
</tr>
<tr>
<td></td>
<td>7.2.3 Uncertainty Relations</td>
<td>332</td>
</tr>
<tr>
<td></td>
<td>7.3 Entropic Uncertainty Relation</td>
<td>339</td>
</tr>
<tr>
<td></td>
<td>7.4 Measurements with Negligible State Reduction</td>
<td>342</td>
</tr>
</tbody>
</table>
8 Entanglement and Locality Restrictions ........................................ 357
  8.1 Entanglement and Local Quantum Operations .................. 357
  8.2 Fidelity and Entanglement ........................................ 362
  8.3 Entanglement and Information Quantities ...................... 369
  8.4 Entanglement and Majorization ................................ 375
  8.5 Distillation of Maximally Entangled States .................... 380
  8.6 Dilution of Maximally Entangled States ......................... 387
  8.7 Unified Approach to Distillation and Dilution ............... 391
  8.8 Maximally Correlated State .................................... 398
  8.9 Dilution with Zero-Rate Communication ....................... 403
  8.10 Discord ................................................ 406
  8.11 State Generation from Shared Randomness .................... 412
  8.12 Positive Partial Transpose (PPT) Operations ................. 418
  8.13 Violation of Superadditivity of Entanglement Formation ..... 426
    8.13.1 Counter Example for Superadditivity of Entanglement Formation ........ 426
    8.13.2 Proof of Theorem 8.14 ................................ 428
  8.14 Secure Random Number Generation .............................. 433
    8.14.1 Security Criteria and Their Evaluation .................. 433
    8.14.2 Proof of Theorem 8.15 ................................ 436
  8.15 Duality Between Two Conditional Entropies .................... 438
    8.15.1 Recovery of Maximally Entangled State from Evaluation of Classical Information ........ 438
    8.15.2 Duality Between Two Conditional Entropies of Mutually Unbiased Basis ........ 442
  8.16 Examples ................................................ 443
    8.16.1 $2 \times 2$ System .................................. 444
    8.16.2 Werner State ....................................... 445
    8.16.3 Isotropic State ....................................... 447
  8.17 Proof of Theorem 8.2 ........................................ 450
  8.18 Proof of Theorem 8.3 ........................................ 454
  8.19 Proof of Theorem 8.8 for Mixed States ......................... 455
  8.20 Proof of Theorem 8.9 for Mixed States ......................... 456
    8.20.1 Proof of Direct Part .................................. 456
    8.20.2 Proof of Converse Part ................................ 457
  8.21 Historical Note ............................................. 459
    8.21.1 Entanglement Distillation ............................... 459
    8.21.2 Entanglement Dilution and Related Topics ................ 460
    8.21.3 Additivity ............................................. 460
    8.21.4 Security and Related Topics ............................. 461
9 Analysis of Quantum Communication Protocols .................. 491
9.1 Quantum Teleportation ........................................ 491
9.2 C-Q Channel Coding with Entangled Inputs .................... 493
9.3 C-Q Channel Coding with Shared Entanglement ................. 501
9.4 Quantum Channel Resolvability ................................ 510
9.5 Quantum-Channel Communications with an Eavesdropper ...... 516
9.5.1 C-Q Wiretap Channel ...................................... 516
9.5.2 Relation to BB84 Protocol ................................ 518
9.5.3 Secret Sharing ............................................ 520
9.5.4 Distillation of Classical Secret Key ........................ 521
9.5.5 Proof of Direct Part of C-Q Wiretap Channel
Coding Theorem ................................................. 523
9.5.6 Proof of Converse Part of C-Q Wiretap Channel
Coding Theorem .................................................. 525
9.6 Channel Capacity for Quantum-State Transmission .......... 527
9.6.1 Conventional Formulation ................................ 527
9.6.2 Proof of Hashing Inequality (8.121) ....................... 534
9.6.3 Decoder with Assistance by Local Operations ............... 534
9.7 Examples ...................................................... 541
9.7.1 Group Covariance Formulas ................................ 541
9.7.2 d-Dimensional Depolarizing Channel ....................... 543
9.7.3 Transpose Depolarizing Channel ........................... 544
9.7.4 Generalized Pauli Channel ................................ 545
9.7.5 PNS Channel .............................................. 545
9.7.6 Erasure Channel ......................................... 546
9.7.7 Phase-Damping Channel .................................. 547
9.8 Proof of Theorem 9.3 .......................................... 548
9.9 Historical Note ................................................ 552
9.9.1 Additivity Conjecture ..................................... 552
9.9.2 Channel Coding with Shared Entanglement ................ 553
9.9.3 Quantum-State Transmission .............................. 554
9.10 Solutions of Exercises ........................................ 555
References .......................................................... 565

10 Source Coding in Quantum Systems ............................. 569
10.1 Four Kinds of Source Coding Schemes
in Quantum Systems ............................................... 570
10.2 Quantum Fixed-Length Source Coding ......................... 571
10.3 Construction of a Quantum Fixed-Length Source Code ....... 574
10.4 Universal Quantum Fixed-Length Source Codes ............... 577
10.5 Universal Quantum Variable-Length Source Codes .......... 579
10.6 Mixed-State Case and Bipartite State Generation ............. 580
10.7  Compression with Classical Memory .......................... 586
10.8  Compression with Shared Randomness .......................... 590
10.9  Relation to Channel Capacities .................................. 594
10.10 Proof of Lemma 10.3 ........................................... 597
10.11 Historical Note .................................................. 599
10.12 Solutions of Exercises ............................................ 601
References ........................................................................ 603

Erratum to: Quantum Information Theory ................................. E1
Appendix: Limits and Linear Algebra ........................................ 607
Postface to Japanese version ................................................. 627
Index .................................................................................. 631
Quantum Information Theory
Mathematical Foundation
Hayashi, M.
2017, XLIII, 636 p. 24 illus., 1 illus. in color., Hardcover
ISBN: 978-3-662-49723-4