

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

2.7	Related Books.	84
2.8	Solutions of Exercises.	84
	References.	93
3	Quantum Hypothesis Testing and Discrimination of Quantum States	95
3.1	Information Quantities in Quantum Systems.	95
3.1.1	Quantum Entropic Information Quantities	95
3.1.2	Other Quantum Information Quantities	101
3.2	Two-State Discrimination in Quantum Systems	105
3.3	Discrimination of Plural Quantum States	110
3.4	Asymptotic Analysis of State Discrimination	112
3.5	Hypothesis Testing and Stein's Lemma	115
3.6	Hypothesis Testing by Separable Measurements.	121
3.7	Proof of Direct Part of Stein's Lemma and Hoeffding Bound	123
3.8	Information Inequalities and Proof of Converse Part of Stein's Lemma and Han-Kobayashi Bound	127
3.9	Proof of Theorem 3.1	137
3.10	Historical Note	138
3.11	Solutions of Exercises.	140
	References.	151
4	Classical-Quantum Channel Coding (Message Transmission)	155
4.1	Formulation of the Channel Coding Process in Quantum Systems.	156
4.1.1	Transmission Information in C-Q Channels and Its Properties.	157
4.1.2	C-Q Channel Coding Theorem	158
4.2	Coding Protocols with Adaptive Decoding and Feedback.	162
4.3	Channel Capacities Under Cost Constraint	164
4.4	A Fundamental Lemma.	166
4.5	Proof of Direct Part of C-Q Channel Coding Theorem.	167
4.6	Proof of Converse Part of C-Q Channel Coding Theorem	171
4.7	Pseudoclassical Channels	178
4.8	Historical Note	180
4.8.1	C-Q Channel Capacity.	180
4.8.2	Hypothesis Testing Approach	181
4.8.3	Other Topics	182
4.9	Solutions of Exercises.	182
	References.	193

5	State Evolution and Trace-Preserving Completely Positive Maps.	197
5.1	Description of State Evolution in Quantum Systems.	197
5.2	Examples of Trace-Preserving Completely Positive Maps.	205
5.3	State Evolutions in Quantum Two-Level Systems	211
5.4	Information-Processing Inequalities in Quantum Systems	216
5.5	Entropy Inequalities in Quantum Systems.	221
5.6	Conditional Rényi Entropy and Duality	228
5.7	Proof and Construction of Stinespring and Choi–Kraus Representations.	234
5.8	Historical Note	238
5.8.1	Completely Positive Map and Quantum Relative Entropy	238
5.8.2	Quantum Relative Rényi entropy.	239
5.9	Solutions of Exercises.	239
	References.	250
6	Quantum Information Geometry and Quantum Estimation	253
6.1	Inner Products in Quantum Systems	253
6.2	Metric-Induced Inner Products	259
6.3	Geodesics and Divergences.	265
6.4	Quantum State Estimation.	273
6.5	Large Deviation Evaluation.	278
6.6	Multiparameter Estimation	281
6.7	Relative Modular Operator and Quantum f -Relative Entropy.	290
6.7.1	Monotonicity Under Completely Positivity	290
6.7.2	Monotonicity Under 2-Positivity	293
6.8	Historical Note	300
6.8.1	Quantum State Estimation	300
6.8.2	Quantum Channel Estimation	301
6.8.3	Geometry of Quantum States.	302
6.8.4	Equality Condition for Monotonicity of Relative Entropy	303
6.9	Solutions of Exercises.	304
	References.	318
7	Quantum Measurements and State Reduction	323
7.1	State Reduction Due to Quantum Measurement	323
7.2	Uncertainty and Measurement.	329
7.2.1	Uncertainties for Observable and Measurement.	329
7.2.2	Disturbance	331
7.2.3	Uncertainty Relations.	332
7.3	Entropic Uncertainty Relation.	339
7.4	Measurements with Negligible State Reduction	342

7.5	Historical Note	346
7.6	Solutions of Exercises.	348
	References.	355
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 2×2 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

8.22	Solutions of Exercises.	461
	References.	486
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