

Masahito Hayashi

# Quantum Information

An Introduction

With 14 Figures and 10 Tables

---

# Contents

<b>Prologue</b>	<b>1</b>
<b>1 Mathematical Formulation of Quantum Systems</b>	<b>9</b>
1.1 Quantum Systems and Linear Algebra	10
1.2 State and Measurement in Quantum Systems	13
1.3 Quantum Two-Level Systems	17
1.4 Composite Systems and Tensor Products	18
1.5 Matrix Inequalities and Matrix Monotone Functions	22
<b>2 Information Quantities and Parameter Estimation in Classical Systems</b>	<b>27</b>
2.1 Information Quantities in Classical Systems	28
2.1.1 Entropy	28
2.1.2 Relative Entropy	29
2.1.3 Mutual Information	33
2.1.4 The Independent and Identical Condition and Rényi Entropy	36
2.2 Extensions to Quantum Systems	40
2.3 Geometry of Probability Distribution Family	45
2.3.1 Inner Product for Random Variables and Fisher Information	45
2.3.2 Exponential Family and Divergence	48
2.4 Estimation in Classical Systems	52
2.5 Type Method and Large Deviation Evaluation	57
2.5.1 Type Method and Sanov's Theorem	57
2.5.2 Cramér Theorem and Its Application to Estimation	59
2.6 Related Books	67
<b>3 Quantum Hypothesis Testing and Discrimination of Quantum States</b>	<b>69</b>
3.1 Two-State Discrimination in Quantum Systems	70

3.2	Discrimination of Plural Quantum States .....	72
3.3	Asymptotic Analysis of State Discrimination .....	74
3.4	Hypothesis Testing and Stein's Lemma .....	77
3.5	Hypothesis Testing by Separable Measurements .....	82
3.6	Proof of Direct Part of Stein's Lemma .....	84
3.7	Information Inequalities and Proof of Converse Part of Stein's Lemma .....	86
3.8	Historical Note .....	90
<b>4</b>	<b>Classical-Quantum Channel Coding (Message Transmission) .....</b>	<b>93</b>
4.1	Formulation of the Channel Coding Process in Quantum Systems .....	94
4.1.1	Transmission Information in C-Q Channels and Its Properties .....	95
4.1.2	C-Q Channel Coding Theorem .....	96
4.2	Coding Protocols with Adaptive Decoding and Feedback ...	99
4.3	Channel Capacities Under Cost Constraint .....	101
4.4	A Fundamental Lemma .....	102
4.5	Proof of Direct Part of C-Q Channel Coding Theorem ....	104
4.6	Proof of Converse Part of C-Q Channel Coding Theorem ..	109
4.7	Pseudoclassical Channels .....	113
4.8	Historical Note .....	115
<b>5</b>	<b>State Evolution and Trace-Preserving Completely Positive Maps .....</b>	<b>117</b>
5.1	Description of State Evolution in Quantum Systems .....	117
5.2	Examples of Trace-Preserving Completely Positive Maps ...	124
5.3	State Evolutions in Quantum Two-Level Systems .....	129
5.4	Information-Processing Inequalities in Quantum Systems ...	133
5.5	Entropy Inequalities in Quantum Systems .....	137
5.6	Historical Note .....	143
<b>6</b>	<b>Quantum Information Geometry and Quantum Estimation .....</b>	<b>145</b>
6.1	Inner Products in Quantum Systems .....	146
6.2	Metric-Induced Inner Products .....	151
6.3	Geodesics and Divergences .....	157
6.4	Quantum State Estimation .....	165
6.5	Large Deviation Evaluation .....	170
6.6	Multiparameter Estimation .....	173
6.7	Historical Note .....	182
<b>7</b>	<b>Quantum Measurements and State Reduction .....</b>	<b>185</b>
7.1	State Reduction Due to Quantum Measurement .....	185

7.2	Uncertainty and Measurement . . . . .	192
7.3	Measurements with Negligible State Demolition . . . . .	200
7.4	Historical Note . . . . .	204
<b>8</b>	<b>Entanglement and Locality Restrictions . . . . .</b>	<b>207</b>
8.1	Entanglement and Local Quantum Operations . . . . .	209
8.2	Fidelity and Entanglement . . . . .	212
8.3	Entanglement and Information Quantities . . . . .	219
8.4	Entanglement and Majorization . . . . .	224
8.5	Distillation of Maximally Entangled States . . . . .	230
8.6	Dilution of Maximally Entangled States . . . . .	237
8.7	Unified Approach to Distillation and Dilution . . . . .	241
8.8	Dilution with Zero-Rate Communication . . . . .	249
8.9	State Generation from Shared Randomness . . . . .	255
8.10	Positive Partial Transpose (PPT) Operations . . . . .	260
8.11	Examples . . . . .	266
8.11.1	$2 \times 2$ System . . . . .	266
8.11.2	Werner State . . . . .	268
8.11.3	Isotropic State . . . . .	270
8.12	Historical Note . . . . .	273
<b>9</b>	<b>Analysis of Quantum Communication Protocols . . . . .</b>	<b>275</b>
9.1	Quantum Teleportation . . . . .	276
9.2	C-Q Channel Coding with Entangled Inputs . . . . .	277
9.3	C-Q Channel Coding with Shared Entanglement . . . . .	284
9.4	Quantum Channel Resolvability . . . . .	293
9.5	Quantum-Channel Communications with an Eavesdropper . . . . .	298
9.5.1	C-Q Wiretap Channel . . . . .	298
9.5.2	Relation to BB84 Protocol . . . . .	300
9.5.3	Secret Sharing . . . . .	302
9.5.4	Distillation of Classical Secret Key . . . . .	302
9.5.5	Proof of Direct Part of C-Q Wiretap Channel Coding Theorem . . . . .	304
9.5.6	Proof of Converse Part of C-Q Wiretap Channel Coding Theorem . . . . .	305
9.6	Channel Capacity for Quantum-State Transmission . . . . .	307
9.7	Examples . . . . .	313
9.7.1	Group Covariance Formulas . . . . .	313
9.7.2	$d$ -Dimensional Depolarizing Channel . . . . .	315
9.7.3	Transpose-Depolarizing Channel . . . . .	315
9.7.4	Generalized Pauli Channel . . . . .	316
9.7.5	PNS Channel . . . . .	316
9.7.6	Erasure Channel . . . . .	317
9.7.7	Phase-Damping Channel . . . . .	318
9.8	Historical Note . . . . .	319

<b>10 Source Coding in Quantum Systems</b>	321
10.1 Four Kinds of Source Coding Schemes	
in Quantum Systems	322
10.2 Quantum Fixed-Length Source Coding	324
10.3 Construction of a Quantum Fixed-Length Source Code	327
10.4 Universal Quantum Fixed-Length Source Codes	330
10.5 Universal Quantum Variable-Length Source Codes	331
10.6 Mixed-State Case	332
10.7 Compression by Classical Memory	336
10.8 Compression by Shared Randomness	339
10.9 Relation to Channel Capacities	342
10.10 Historical Note	344
<b>A Limits and Linear Algebra</b>	347
A.1 Limits	347
A.2 Singular Value Decomposition and Polar Decomposition	349
A.3 Norms of Matrices	351
A.4 Convex Functions and Matrix Convex Functions	353
A.5 Proof and Construction of Stinespring and Choi-Kraus	
Representations	357
<b>B Proofs of Theorems and Lemmas</b>	363
B.1 Proof of Theorem 3.1	363
B.2 Proof of Theorem 8.2	364
B.3 Proof of Theorem 8.3	367
B.4 Proof of Theorem 8.8 for Mixed States	367
B.5 Proof of Theorem 8.9 for Mixed States	368
B.5.1 Proof of Direct Part	368
B.5.2 Proof of Converse Part	370
B.6 Proof of Theorem 9.3	371
B.7 Proof of Lemma 9.4	374
B.8 Proof of Lemma 10.3	380
<b>C Hints and Brief Solutions to Exercises</b>	383
<b>References</b>	401
<b>Index</b>	423