Masahito Hayashi

Quantum Information

Masahito Hayashi

Quantum Information

An Introduction

With 14 Figures and 10 Tables

Springer

Masahito Hayashi
Japan Science and Technology Agency
201 Daini Hongo White Bldg
5-28-3, Hongo, Bunkyo-ku
Tokyo 113-0033, Japan
e-mail: masahito@qci.jst.go.jp

Library of Congress Control Number: 2006923433

ISBN-10 3-540-30265-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-30265-0 Springer Berlin Heidelberg New York

Typesetting: Protago-TEX-Production GmbH, Berlin
Production: LE-TEX Jelonek, Schmidt & Vöckler GbR, Leipzig
Cover design: eStudio Calamar S.L., F. Steinen-Broo, Pau/Girona, Spain

Printed on acid-free paper 57/3100/YL 5 4 3 2 1 0

To my parents

Preface

This book is the revised English edition of the Japanese book *Introduction to Quantum Information Theory*, which systematically describes quantum information theory and was originally published by Saiensu-sha, Tokyo, Japan in May 2003. The study of information processing based on the physical principles of quantum mechanics was initiated in the 1960s. Recently, such quantum information processing has demonstrated experimentally, and its theoretical aspects have been examined more deeply and mathematically. The research field addressing the relevant theory is called Quantum Information Theory, and is now being studied by many researchers from various viewpoints.

However, only Holevo's book *Probabilistic and Statistical Aspects of Quantum Theory*, which was published back in 1980 (English version in 1982), places a heavy emphasis on the mathematical foundation of quantum information theory. Several books concerning quantum information science have been published since the late 1990s. However, they treat quantum computation, the physical aspects of quantum information, or the whole of quantum information science and are not mainly concerned with quantum information theory. Therefore, it seemed to me that many researchers would benefit from an English book on quantum information theory, and so I decided to publish the English version of my book. I hope that it will make a contribution to the field of quantum information theory.

This book was written as follows. First, the author translated the original Japanese version in cooperation with Dr. Tim Barnes. Next, the book was revised through the addition of many new results to Chaps. 8–10 and a historical note to every chapter. Several exercises were also added, so that the English version has more than 330 exercises. Hence, I take full responsibility for the content of this English version. In this version, theorems and lemmas are displayed along with the names of the reserchers who contributed them. However, when the history of the theorems and lemmas is not so simple, they are displayed without the contributing researchers' names and their histories are explained in a historical note at the end of the given chapter.

I am indebeted to Prof. Masanao Ozawa and Dr. Tohya Hiroshima for their feedback on the Japanese version, which been incorporated into the English version. I am also grateful to (in alphabetical order) Dr. Giulio Chiribella, Mr. Motohisa Fukuda, Prof. Richard Gill, Dr. Michael Horodecki, Dr. Satoshi Ishizaka, Dr. Paolo Perinotti, Dr. Toshiyuki Shimono, and Dr. Andreas Winter, for reviewing the technical aspects of the English version. Further, Dr. Tomohisa Hayakawa, Mr. Daichi Isami, Mr. Takashi Okajima, Mr. Tomotake Sasaki, Mr. Taiji Suzuki, Mr. Fuyuhiko Tanaka, and Mr. Ken'ichiro Tanaka used the draft of the English version in their seminar and verified its contents. Miss Rika Abe commented on the nontechnical parts of the book. Further, Mr. Motohisa Fukuda helped me in compiling the references. I would like to express my appreciation for their cooperation.

I also would like to thank Prof. Hiroshi Imai of the University of Tokyo and the people associated with the ERATO Quantum Computation and Information Project for providing the research environments for this English version. I would like to express my gratitude to Dr. Glenn Corey and editorial staffs of Springer for good excellent editing process. I would also like to thank Dr. Claus E. Ascheron of Springer Science+Business Media for his encouragement and patience during the preparation of the manuscript.

Tokyo, February 2006 *Masahito Hayashi*

Preface to Japanese Version

This textbook attempts to describe quantum information theory, which is a presently evolving field. It is organized so that the reader can understand its contents with very elementary prior knowledge. This research field has been developed by many researchers from various backgrounds and has matured rapidly in the last 5 years.

Recently, many people have considered that more interdisciplinary activities are needed in the academic world. Hence, education and research must be performed and evaluated on a wide scope. However, since the extreme segmentation of each research area has increased the difficulty of interdisciplinary activities. On the other hand, quantum information theory can in some sense form a bridge between several fields because it deals with topics in a variety of disciplines including physics and information science. Hence, it can be expected to contribute in some way to removing the segmentation of its parent fields. In fact, information science consists of subfields such as computer science, mathematical statistics, and Shannon's information theory. These subfields are studied in separate contexts.

However, in quantum information theory, we must return to the fundamentals of the topic, and there are fewer boundaries among the different fields. Therefore, many researchers now transcend these boundaries.

Given such a starting point, the book was written to enable the reader to efficiently attain the interdisciplinary knowledge necessary for understanding quantum information theory. This book assumes only that the reader has knowledge of linear algebra, differential and integral calculus, and probability/statistics at the undergraduate level. No knowledge of quantum mechanics is assumed.

Some of the exercises given in the text are rather difficult. It is recommended that they be solved in order to acquire the skills necessary for tackling research problems. Parts of the text contain original material that does not appear elsewhere. Comments will be given for such parts.

The author would like to thank Prof. Hiroshi Imai of the University of Tokyo, Prof. Shun-ichi Amari of the Brain Science Institute at RIKEN, Prof. Kenji Ueno of Kyoto University, and the people associated with the ERATO Quantum Computation and Information Project, the Brain Science Institute at RIKEN, and the Department of Mathematics at Kyoto University for providing me with the means to continue my research. The author also wishes to thank Prof. Hiroshi Nagaoka of the University of Electro-Communications, Prof. Akio Fujiwara of Osaka University, Prof. Keiji Matsumoto of the National Institute of Informatics, and Dr. Tomohiro Ogawa of the University of Tokyo for helpful discussions and advice. This text would not have been possible without their enlightening discussions.

I also received valuable comments from Prof. Alexander Holevo of the Steklov Mathematical Institute, Prof. Masanao Ozawa of Tohoku University, Dr. Ryutaroh Matsumoto of the Tokyo Institute of Technology, Dr. Fumiaki Morikoshi of NTT, Dr. Yodai Watanabe of RIKEN, and Dr. Mitsuru Hamada, Dr. Yoshiyuki Tsuda, Dr. Heng Fan, Dr. Xiangbin Wang, and Mr. Toshiyuki Shimono of the ERATO Quantum Computation and Information Project regarding the contents of this text. They have also earned a debt of gratitude. I would also like to thank Mr. Kousuke Hirase of Saiensu-sha for his encouragement and patience during the preparation of the manuscript.

Tokyo, December 2003 *Masahito Hayashi*

Contents

Prologue 1

1 Mathematical Formulation of Quantum Systems 9
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

2 Information Quantities and Parameter Estimation in Classical Systems 27
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

3 Quantum Hypothesis Testing and Discrimination of Quantum States 69
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

4 Classical-Quantum Channel Coding (Message Transmission) 93
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

5 State Evolution and Trace-Preserving Completely Positive Maps 117
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

6 Quantum Information Geometry and Quantum Estimation 145
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

7 Quantum Measurements and State Reduction 185
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

8 Entanglement and Locality Restrictions 207
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 2×2 System 266
8.11.2 Werner State 268
8.11.3 Isotropic State 270
8.12 Historical Note 273

9 Analysis of Quantum Communication Protocols 275
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

10 Source Coding in Quantum Systems 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

A Limits and Linear Algebra 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 Proofs of Theorems and Lemmas 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

C Hints and Brief Solutions to Exercises 383

References 401

Index 423