Graduate Texts in Physics

Graduate Texts in Physics

Graduate Texts in Physics publishes core learning/teaching material for graduate- and advanced-level undergraduate courses on topics of current and emerging fields within physics, both pure and applied. These textbooks serve students at the MS- or PhD-level and their instructors as comprehensive sources of principles, definitions, derivations, experiments and applications (as relevant) for their mastery and teaching, respectively. International in scope and relevance, the textbooks correspond to course syllabi sufficiently to serve as required reading. Their didactic style, comprehensiveness and coverage of fundamental material also make them suitable as introductions or references for scientists entering, or requiring timely knowledge of, a research field.

More information about this series at http://www.springer.com/series/8431

Masahito Hayashi

Quantum Information Theory

Mathematical Foundation

Second Edition

Springer

Masahito Hayashi
Graduate School of Mathematics
Nagoya University
Nagoya, Aichi
Japan

Original Japanese version published by Saiensu-sha Company, Ltd., Tokyo, Japan, 2004

ISSN 1868-4513 ISSN 1868-4521 (electronic)
Graduate Texts in Physics
ISBN 978-3-662-49723-4 ISBN 978-3-662-49725-8 (eBook)
DOI 10.1007/978-3-662-49725-8

Library of Congress Control Number: 2016949125

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer-Verlag GmbH Germany
The registered company address is: Heidelberger Platz 3, 14197 Berlin, Germany

The original version of the book frontmatter was revised: The additional bibliographic information on the copyright page was included. The erratum PDF is available at DOI:10.1007/978-3-662-49725-8_11

Preface

This book was originally published in Japanese by Saiensu-sha, Tokyo, Japan in May 2003. Then, the first English edition was published by Springer in 2006 with some revision from Japanese version. It has been 10 years since the publication of the first English edition. During this decade, so many remarkable progresses have been made in the area of quantum information theory. So, I decided to publish the second English edition with considerable revision to include these latest progresses.

I believe that the most important progress among this decade is the resolution of the additivity problem. This problem was proposed as a problem equivalent to various kinds of additivity problems in entanglement theory and channel capacity. To include this progress, I have added Sect. 8.13: Violation of superadditivity of entanglement formation. Since this topic needs special knowledge for classical information, I have also added Sect. 2.6: Large Deviation on Sphere. Although Sect. 2.6 is important for the understanding of quantum information, it seems that its content is partially misunderstood among quantum information researchers. So, this section is also helpful for understanding quantum information. Further, since this topic affects the channel capacity, I rewrote Sect. 9.2: C-Q Channel Coding with Entangled Inputs.

The second most important progress is considerable progress on quantum hypothesis testing. This progress has been made by so many authors. Although Chernoff bound, Hoeffding bound, and Han–Kobayashi bound in this topic had not been exactly solved at that time, these exact forms have been completely solved during this decade. To reflect this progress, I completely rewrote Chap. 3. Since the quantum Han–Kobayashi bound is closely related to the new type of quantum Rényi relative entropy, the new Chap. 3 also discusses it. Further, to make Chap. 3 more self-contained, I have moved Section: Information Quantities in Quantum Systems to Chap. 3. The content of this chapter is employed in Chap. 4 because the hypothesis testing is closely related to channel coding. Hence, I also rewrote Chap. 4 partially. Recently, this relation has been of interest for many researchers. In this revision, I emphasize this relation more strongly while this relation was discussed in the first edition. I also summarize its history in Sect. 4.10.

The third most important progress is considerable progress in conditional Rényi entropy. To discuss this issue, I newly added Sect 2.1.5: Conditional Rényi entropy and Sect 5.6: Conditional Rényi Entropy and Duality. This progress has made notable influence on entropic uncertainty relation, secure random number generation, entanglement measure, and the duality relation between coherence and information leakage. Since these four areas also have greatly progressed during this decade, I summarize them in the following new sections: Sect. 7.3: Entropic Uncertainty Relation, Sect. 8.14: Secure Random Number Generation, Sect. 8.8: Maximally Correlated State, and Sect. 8.15: Duality Between Two Conditional Entropies. Further, using the contents of Sect. 8.15, I simplified the proof in Sect. 9.6: Channel Capacity for Quantum-State Transmission. Also, based on the previously gained knowledge, I newly added Subsect. 9.6.3: Decoder with assistance by local operations.

Other topics have advanced recently, and we can list discord, Bregman divergence, and matrix convex function, among them. The first edition discussed discord, however, its treatment is not perfect. So, in the second edition, I have completed it in new Sect. 8.10: Discord. To deal with recent progress of Bregman divergence, I added Sect. 2.2.2: Bregman divergence. Recently, extremal point decomposition of matrix convex functions was completed. This decomposition brings us a more detailed analysis of quantum f-relative entropy. So, to include the decomposition, I rewrote Appendix A.4: Convex Functions and Matrix Convex Functions. Then, I have newly added Sect. 6.7: Relative Modular Operator and Quantum f-Relative Entropy.

As one of the features of this book, I have discussed the axiomatic approach, while the first edition emphasizes mainly in entanglement measure. However, this approach is also important in the entropy theory. To clarify this relation, I have newly added Sect. 2.5: Continuity and Axiomatic Approach. Also, I have added several descriptions related to this approach.

In this edition, I additionally have included around 120 new exercises, so that this edition totally has 450 exercises. I also have completed solutions for all exercises for readers' convenience. Since each chapter can be understood separately, I have organized the second edition so that each chapter contains solutions for exercises and proofs of theorems in that chapter. In particular, since Chap. 2 is composed of knowledge from classical information and has a distinguished description from existing textbooks, this chapter might be useful for readers interested only in classical information. Recently, I have published another book "Introduction to Quantum Information Science" with S. Ishizaka, A. Kawachi, G. Kimura, and T. Ogawa, which is more introductory. Since this book is more mathematically oriented, I changed the title to "Quantum Information Theory: A Mathematical Foundation."

I am grateful to Prof. Fumio Hiai, Prof. Francesco Buscemi, Dr. Motohisa Fukuda, Mr. Kengo Takeuchi, and Mr. Kosuke Ito for their comments. I would like to express my appreciation for their cooperation. 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.

Nagoya, Japan Masahito Hayashi

Preface to the First English Edition

This book is the revised and 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 began in the 1960s. Recently, some protocols of quantum information processing have been demonstrated experimentally, and their theoretical aspects have been examined more deeply and mathematically. In particular, the field that is concerned with their theoretical bounds is called quantum information theory and has been studied by many researchers from diverse 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 researchers 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.

Hongo, Tokyo, Japan Masahito Hayashi
November 2005

Preface to the Japanese Edition

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

Hongo, Tokyo, Japan Masahito Hayashi
December 2003

Contents

Notations

Basic Notations

$\|\boldsymbol{M}\|$	Number of POVM elements, p. 5
$\bar{x}$	Complex conjugate of the given number x, p. 2
$\mathcal{S}(\mathcal{H})$	Set of density matrices of given Hilbert space $\mathcal{H}$, p. 6
A^T	Transpose of a matrix A, p. 2
$\overline{A}$	Complex conjugate matrix of a matrix A, p. 2
A^*	Adjoint of a matrix A, p. 2
$[X, Y]$	Commutator of matrices A and B, p. 4
$X \circ Y$	Symmetrized product of matrices A and B, p. 4
P_ρ^M	Probability distribution when measurement is $\boldsymbol{M}$ and state is ρ, p. 6
ρ_{mix}	Completely mixed state, p. 7
Tr_A	Partial trace concerning system $\mathcal{H}_A$, p. 13
$\{X \geq 0\}$	Projection defined by (1.37), p. 16
κ_M	Pinching of PVM $\boldsymbol{M}$ (1.13), p. 8
κ_X	Pinching of Hermitian matrix X (1.14), p. 8
κ_M	Pinching of POVM $\boldsymbol{M}$ (1.15), p. 8
S_i	Pauli matrix (1.16), p. 9
ρ_x	Stokes parameterization (1.17), p. 9
$\mathcal{T}(\mathcal{H})$	Set of Hermitian matrices on $\mathcal{H}$, p. 98
$\mathcal{M}(\mathcal{H})$	Set of matrices on $\mathcal{H}$, p. 98
$\eta(x)$	$-x \log x$ (Theorem 5.12), p. 223
$\eta_0(x)$	See (5.91), p. 223

Information Quantities in Classical System

$D(p\|\|q)$	Relative entropy (2.12), p. 28
$D_f(p\|\|q)$	f-relative entropy $\sum_i p_i f\left(\frac{q_i}{p_i}\right)$ (Theorem 2.1), p. 29
$\phi(s\|p\|\|q)$	$\log(\sum_i p_i^{1-s} q_i^s)$, p. 30

$D_{1-s}(p\|q)$	Relative Rényi entropy $-\frac{\phi(s\|p\|q)}{s}$ (2.19), p. 30
$D_{\min}(p\|q)$	Minimum relative entropy (2.20), p. 30
$D_{\max}(p\|q)$	Maximum relative entropy (2.20), p. 30
$d_2(p,q)$	Hellinger distance (2.17), p. 29
$d_1(p,q)$	Variational distance $\frac{1}{2}\sum_i \|p_i - q_i\|$(2.23), p. 31
$I(X:Y)$	Mutual information $D(\mathrm{P}_{X,Y}\|\mathrm{P}_X \times \mathrm{P}_Y)$(2.30), p. 34
$I(X:Y\|Z)$	Conditional mutual information (2.31), p. 34
$I(p,Q)$	Transmission information (2.34), p. 35
$H(p)$	Entropy of distribution p (2.2), p. 26
$H(X)$	Entropy of random variable X, p. 26
$h(x)$	Binary entropy, p. 26
$\psi(s\|p)$	$\log \sum_i p_i^{1-s}$ (2.38), p. 36
$H_{1-s}(p)$	Rényi entropy $\frac{\psi(s\|p)}{s}$ (2.38), p. 36
$H_{\min}(p)$	Minimum entropy $-\log \max_i p_i$ (2.39), p. 36
$H_{\max}(p)$	Maximum entropy $\log \|\{i\|p_i > 0\}\|$ (2.39), p. 36
$H(X\|Y)$	Conditional entropy (2.5), p. 26
$H_{1+s}(X\|Y)$	Conditional Rényi entropy $\log \|\chi\| - D_{1+s}(\mathrm{P}_{XY}\|p_{\mathrm{mix},\chi} \times \mathrm{P}_Y)$ (2.74), p. 42
$H^{\uparrow}_{1+s}(X\|Y)$	Conditional Rényi entropy $\log \|\chi\| - \min_{Q_Y} D_{1+s}(\mathrm{P}_{XY}\|p_{\mathrm{mix},\chi} \times Q_Y)$ (2.75), p. 42
$H_{\min}(X\|Y)$	Conditional minimum entropy $\lim_{s\to\infty} H_{1+s}(X\|Y)$ (2.77), p. 42
$H^{\uparrow}_{\min}(X\|Y)$	Conditional minimum entropy $\lim_{s\to\infty} H^{\uparrow}_{1+s}(X\|Y)$ (2.77), p. 42
$H_{\max}(X\|Y)$	Conditional maximum entropy $\lim_{s\to-1} H_{1+s}(X\|Y)$ (2.78), p. 42
$H^{\uparrow}_{\max}(X\|Y)$	Conditional maximum entropy $\lim_{s\to-1} H^{\uparrow}_{1+s}(X\|Y)(X\|Y)$ (2.78), p. 42

Notations for Information Geometry

J_θ	Fisher information (2.103), p. 47
$l_\theta(\omega)$	Logarithmic derivative, p. 47
$\boldsymbol{J}_\theta$	Fisher information matrix, p. 47
$D^\mu(\bar{\theta}\|\theta)$	Bregman divergence (2.111), (2.116), p. 50, 51
$\nu(\eta)$	Legendre transform of μ (2.112), (2.119), p. 50, 51
$\eta(\theta)$	Expectation parameter (2.116), (2.131), p. 51, 55
$\mu(\theta)$	Potential function (Cumulant generating function) (2.128), (2.130), p. 53, 54

Notation Related to Probability

$\mathcal{P}(\Omega)$	Set of probability distributions on the probability space Ω, p. 26
$p_{\mathrm{mix},\Omega}$	Uniform distribution on Ω, p. 26
$p_{\mathrm{mix},k}$	Uniform distribution on Ω when $\|\Omega\| = k$, p. 26
p_{mix}	Uniform distribution (Simplification of the above), p. 26
$\mathrm{E}_p(X)$	Expectation of X under distribution p (2.1), p. 25
$\mathrm{V}_p(X)$	Variance of X under distribution p (2.94), p. 46
$\mathrm{Cov}_p(X, Y)$	Covariance between X and Y under distribution p (2.93), p. 45
$\kappa_p(X)$	Conditional expectation of X under distribution p (2.107), p. 48
$\kappa_{\mathfrak{U},p}(X)$	Conditional expectation of X with respect to the subspace $\mathcal{U}$ (2.110), p. 49
$p_i^{\downarrow}$	Element of $\{p_i\}$ that is reordered according to size, p. 38
$P(p, L)$	$\sum_{i=1}^{L} p_i^{\downarrow}$ (2.48), p. 38
$\hat{\mathrm{V}}_\theta(\hat{\theta})$	Mean square error of estimator $\hat{\theta}$ (2.137), p. 56
$\mathrm{Med}_p(X)$	Median of X (2.218), p. 78
$\mu_{\mathcal{H}}$	Haar measure on Hilbert space $\mathcal{H}$ (2.210), p. 77
μ_{S^n}	Haar measure on the n-dimensional sphere S^n (2.211), p. 77
$\mathrm{Med}_{S^{2l-1}}(f)$	Median of f under the Haar measure $\mu_{S^{2l-1}}$ on $S^{2l-1}\mathrm{Med}_{\mu_{S^{2l-1}}}(f)$, p. 81
$\mathrm{E}_{S^{2l-1}}$	Expectation under the Haar measure $\mu_{S^{2l-1}}$ on S^{2l-1} $\left(\mathrm{E}_{\mu_{S^{2l-1}}}\right)$, p. 82

Notations for Large Deviation

$\mathbb{N}_d$	$\{1, \ldots, d\}$, p. 61
T_n	Set of empirical distributions on $\mathbb{N}_d$ (Set of types on $\mathbb{N}_d$), p. 61
T_q^n	Set of data with the empirical distribution q, p. 61
$\beta(\{\hat{\theta}_n\}, \theta, \epsilon)$	Rate function of error probability (2.173), p. 66
$\alpha(\{\hat{\theta}_n\}, \theta)$	First-order coefficient of rate function (2.174), p. 66

Fundamental Information Quantities and Related Notations in Quantum Systems

$H(\rho)$	von Neumann entropy $-\mathrm{Tr}\,\rho\log\rho$ (3.1), p. 98
$\psi(s\|\rho)$	$\log \mathrm{Tr}\,\rho^{1-s}$, p. 98
$H_{1-s}(\rho)$	Rényi entropy $\frac{\psi(s\|\rho)}{s}$, p. 98
$H_{\min}(\rho)$	Minimum entropy $-\log\|\rho\|$, p. 98
$H_{\max}(\rho)$	Maximum entropy $\log \mathrm{Tr}\{\rho > 0\}$, p. 98

$D(\rho\|\sigma)$	Quantum relative entropy $\operatorname{Tr}\rho(\log\rho-\log\sigma)$ (3.7), p. 99
$I_\rho(A:B)$	Mutual information (5.89) (8.34), p. 223, 369
$I_\rho(A:B\|C)$	Conditional mutual information (5.90), p. 223
$\phi(s\|\rho\|\sigma)$	$\log\operatorname{Tr}\rho^{1+s}\sigma^{-s}$, p. 99
$\phi(s)$	Abbreviation of $\phi(s\|\rho\|\sigma)$, p. 99
$D_{1+s}(\rho\|\sigma)$	relative Rényi entropy $\frac{\phi(-s\|\rho\|\sigma)}{s}$ (3.9), p. 99
$D_{\max}(\rho\|\sigma)$	Maximum relative entropy $\log\|\sigma^{-\frac{1}{2}}\rho\sigma^{-\frac{1}{2}}$ (3.10), p. 99
$D_{\min}(\rho\|\sigma)$	Minimum relative entropy $-\log\operatorname{Tr}\sigma\{\rho>0\}$ (3.10), p. 99
$\tilde{\phi}(s\|\rho\|\sigma)$	$\log\operatorname{Tr}(\sigma^{\frac{s}{2(1-s)}}\rho\sigma^{\frac{s}{2(1-s)}})^{1-s}=\lim\frac{1}{n}\phi(s\|\kappa_{\sigma^{\otimes n}}(\rho^{\otimes n})\|\sigma^{\otimes n})$, p. 99
$\underline{D}_{1+s}(\rho\|\sigma)$	Sandwiched relative Rényi entropy $\frac{\tilde{\phi}(-s\|\rho\|\sigma)}{s}$ (3.13), p. 99
$b(\rho\|\sigma)$	Bures distance (3.42), p. 103
$F(\rho,\sigma)$	Fidelity $\operatorname{Tr}\|\sqrt{\rho}\sqrt{\sigma}\|$, p. 103
$d_1(\rho,\sigma)$	Trace norm distance (3.45), p. 104
$\beta_\epsilon^n(\rho\|\sigma)$	Minimum value of second error probability (3.92), p. 118
p_{guess}	Guessing probability, p. 113
$B(\rho\|\sigma)$	Maximum decreasing rate of second error probability when first error probability goes to 0 (Theorem 3.3), p. 119
$\tilde{B}(\rho\|\sigma)$	Maximum decreasing rate of second error probability when first error probability goes to 0 and measurement is separable (Theorem 3.5), p. 123
$B^\dagger(\rho\|\sigma)$	Maximum decreasing rate of second error probability when first error probability does not go to 1 (Theorem 3.3), p. 119
$B(r\|\rho\|\sigma)$	Maximum decreasing rate of first error probability when second error probability goes to 0 at rate r (3.98), p. 120
$B^*(r\|\rho\|\sigma)$	Minimum decreasing rate of first error probability when second error probability goes to 0 at rate r (3.99), p. 120
$P_{(\rho\|\sigma)}$	A distribution defined by ρ and σ, p. 110
$Q_{(\rho\|\sigma)}$	Another distribution defined by ρ and σ, p. 110

Information Quantities of c-q Channel W

$I(p,W)$	Transmission information (4.1), p. 159
$I(\boldsymbol{M},p,W)$	Classical transmission information with measurement $\boldsymbol{M}$, p. 164
$I_{1-s}(p,W)$	$-\frac{1}{s}\log\sum_x p(x)\operatorname{Tr}W_x^{1-s}W_p^s$ (4.13), p. 161
$I^\downarrow_{1-s}(p,W)$	$-\frac{(1-s)}{s}\log\operatorname{Tr}(\sum_x p(x)W_x^{1-s})^{\frac{1}{1-s}}$ (4.14), p. 162
$J(p,\sigma,W)$	$\sum_{x\in\chi}p(x)D(W_x\|\sigma)$ (Exercise 4.14), p. 176
$J_{1-s}(p,\sigma,W)$	$-\frac{1}{s}\log\sum_x p(x)\operatorname{Tr}W_x^{1-s}\sigma^s$ (4.3), p. 159
$C_c(W)$	C-q channel capacity (4.9), p. 161
$C_c^\dagger(W)$	Strong converse c-q channel capacity (4.10), p. 161
$\tilde{C}_c(W)$	C-q channel capacity with adaptive decoding and feedback (4.27), p. 164

$C_{c\|c\le K}(W)$	C-q channel capacity with a cost function, p. 164
$C^{\downarrow}_{1-s}(W)$	$\sup_{p\in P_{\rm f}(X)} I^{\downarrow}_{1-s}(p,W)$ (4.15), p. 162
$C_c(W^1,\ldots,W^M)$	C-q channel capacity for multiple receivers (4.20), p. 163
$B(R\|W)$	Reliability function (4.54), p. 172

Notations Related to c-q Channel W

Φ	Code (N,φ,Y) (Sect. 4.1.2), p. 160
$\tilde{\Phi}^{(n)}$	Feedback-allowing coding (Sect. 4.2), p. 164
$\|\Phi\|$	Size of code (4.8), p. 160
$\varepsilon[\Phi]$	Average error probability of code (4.8), p. 160
$\mathcal{P}_{\rm f}(\mathcal{X})$	Set of probability distributions with a finite support in $\mathcal{X}$ (Theorem 4.1), p. 161
$\mathcal{P}_{c\le K}(\mathcal{X})$	$\left\{p\in\mathcal{P}_{\rm f}(\mathcal{X})\middle\vert\sum_x p(x)c(x)\le K\right\}$ (Theorem 4.3), p. 167
p_{1-s}	$\operatorname{argmax}_{p\in\mathcal{P}_{\rm f}(\mathcal{X})} I^{\downarrow}_{1-s}(p,W)$ (4.62), p. 174
p'_{1-s}	$\operatorname{argmax}_{p\in\mathcal{P}_{c\le K}(\mathcal{X})} I^{\downarrow}_{1-s}(p,W)$ (Proof of Lemma 4.4), p. 176
W_p	Average state $\sum_x p(x)W_x$ (4.2), p. 159
$\sigma_{1-s\|p}$	$(\sum_x p(x)W_x^{1-s})^{\frac{1}{1-s}}/\operatorname{Tr}[(\sum_{x'} p(x')W_{x'}^{1-s})^{\frac{1}{1-s}}]$ (4.23), p. 163
$W^A\otimes W^B$	Product channel of W^A and W^B (4.4), p. 159
$W^{(n)}$	n-fold stationary memoryless channel, p. 172
$p\times W$	Correlated state (4.45), p. 170
$p\otimes\sigma$	Independent state (4.45), p. 170

Conditional Entropies in Quantum System

$H_\rho(A\|B)$	Conditional entropy $H_\rho(AB)-H_\rho(A)$ (5.88), p. 223
$H_{1+s\|\rho}(A\|B)$	Conditional Rényi entropy $-D_{1+s}(\rho\|I_A\otimes\rho_B)$ (5.112), p. 228
$\widetilde{H}_{1+s\|\rho}(A\|B)$	Conditional Rényi entropy $-\underline{D}_{1+s}(\rho\|I_A\otimes\rho_B)$ (5.113), p. 228
$H^{\uparrow}_{1+s\|\rho}(A\|B)$	Conditional Rényi entropy $\max_{\sigma_B}-D_{1+s}(\rho\|I_A\otimes\sigma_B)$ (5.114), p. 228
$\widetilde{H}^{\uparrow}_{1+s\|\rho}(A\|B)$	Conditional Rényi entropy $\max_{\sigma_B}-\underline{D}_{1+s}(\rho\|I_A\otimes\sigma_B)$ (5.115), p. 228
$H_{\min\|\rho}(A\|B)$	Conditional minimum entropy $\lim_{s\to\infty} H_{1+s\|\rho}(A\|B)$ (5.123), p. 229
$H^{\uparrow}_{\min\|\rho}(A\|B)$	Conditional minimum entropy $\lim_{s\to\infty} H^{\uparrow}_{1+s\|\rho}(A\|B)$ (5.123), p. 229
$\widetilde{H}_{\min\|\rho}(A\|B)$	Conditional minimum entropy $\lim_{s\to\infty} \widetilde{H}_{1+s\|\rho}(A\|B)$ (5.124), p. 229

$\widetilde{H}^{\uparrow}_{\min|\rho}(A|B)$ Conditional minimum entropy $\lim_{s\to\infty} \widetilde{H}^{\uparrow}_{1+s|\rho}(A|B)$ (5.124), p. 229

$H_{\max|\rho}(A|B)$ Conditional maximum entropy $\lim_{s\to -1} H_{1+s|\rho}(A|B)$) (5.125), p. 229

$H^{\uparrow}_{\max|\rho}(A|B)$ Conditional maximum entropy$\lim_{s\to -1} H^{\uparrow}_{1+s|\rho}(A|B)$ (5.125), p. 229

$\widetilde{H}_{\max|\rho}(A|B)$ Conditional maximum entropy $\lim_{s\to -1} \widetilde{H}_{1+s|\rho}(A|B)$ (5.126), p. 229

$\widetilde{H}^{\uparrow}_{\max|\rho}(A|B)$ Conditional maximum entropy $\lim_{s\to -1} \widetilde{H}^{\uparrow}_{1+s|\rho}(A|B)$ (5.126), p. 229

Notations of q-q Channels

$K(\kappa)$ Matrix representation of κ (5.4), p. 200

κ^E TP-CP map to environment (5.7), p. 201

$\kappa_{M,W}$ Entanglement-breaking channel (Example 5.4), p. 206

τ Transpose (5.14), p. 207

$\kappa_{d,\lambda}$ Depolarizing channel (5.12), p. 206

$\kappa^T_{d,\lambda}$ Transpose depolarizing channel (5.18), p. 208

κ^{GP}_p Generalized Pauli channel (5.16), p. 208

κ^{PD}_D Phase-damping channel (5.19), p. 208

$\kappa^{\mathrm{pns}}_{d,n\to m}$ PNS channel (5.21), p. 209

$\kappa^{\mathrm{era}}_{d,p}$ Erasure channel (5.22), p. 209

Quantum Fisher Information

$J_{\theta,x}$ Fisher metric based on inner product x, p. 260

$J_{\theta,s}$ SLD Fisher metric, p. 260

$J_{\theta,b}$ Bogoljubov Fisher metric, p. 260

$J_{\theta,r}$ RLD Fisher metric, p. 260

$\boldsymbol{J}_{\theta,x}$ Fisher information matrix based on inner product x (6.39), p. 262

$\boldsymbol{J}_{\theta,s}$ SLD Fisher information matrix (6.39), p. 262

$\boldsymbol{J}_{\theta,b}$ Bogoljubov Fisher information matrix (6.39), p. 262

$\boldsymbol{J}_{\theta,r}$ RLD Fisher information matrix (6.39), p. 262

Variants of Quantum Relative Entropy

$D_{c,p}(\rho\|\sigma)$ Maximum relative entropy with projective measurement $\max_{\boldsymbol{M}:PVM} D(\mathrm{P}^{\boldsymbol{M}}_{\rho}\|\mathrm{P}^{\boldsymbol{M}}_{\sigma})$ (5.42), p. 218

$D_c(\rho\|\sigma)$ Maximum relative entropy with measurement $\max_{\boldsymbol{M}:POVM} D(\mathrm{P}^{\boldsymbol{M}}_{\rho}\|\mathrm{P}^{\boldsymbol{M}}_{\sigma})$ (5.42), p. 218

$D_x^{(e)}(\rho\|\sigma)$ x-e-divergence (6.52), p. 267
$D_s^{(e)}(\rho\|\sigma)$ SLD e-divergence $2\operatorname{Tr}\rho\log\sigma^{-\frac{1}{2}}(\sigma^{\frac{1}{2}}\rho\sigma^{\frac{1}{2}})^{\frac{1}{2}}\sigma^{-\frac{1}{2}}$ (6.57), p. 268
$D_b^{(e)}(\rho\|\sigma)$ Bogoljubov e-divergence ($= D(\rho\|\sigma)$) (6.58), p. 268
$D_r^{(e)}(\rho\|\sigma)$ RLD e-divergence $\operatorname{Tr}\rho\log(\rho^{\frac{1}{2}}\sigma^{-1}\rho^{\frac{1}{2}})$(6.59), p. 268
$D_{\frac{1}{2}}^{(e)}(\rho\|\sigma)$ e-divergence with $x=\frac{1}{2}$ (6.60), p. 268
$D_x^{(m)}(\rho\|\sigma)$ x-m-divergence (6.63), p. 268
$D_b^{(m)}(\rho\|\sigma)$ Bogoljubov m-divergence ($= D(\rho\|\sigma)$) (6.66), p. 269
$D_r^{(m)}(\rho\|\sigma)$ RLD m-divergence $\operatorname{Tr}\rho\log(\sqrt{\rho}\sigma^{-1}\sqrt{\rho})$ (6.67), p. 269
$D_f(\rho\|\sigma)$ quantum f-relative entropy (6.116), p. 290

Notations Related to Quantum Information Geometry

$E_{\rho,s}(X)$ See (6.8), p. 254
$E_{\rho,b}(X)$ See (6.9), p. 254
$E_{\rho,r}(X)$ See (6.10), p. 254
$E_{\rho,p}(X)$ See (6.11), p. 254
$E_{\rho,\lambda}(X)$ See (6.12), p. 254
$\mathcal{K}_{\rho,x}(\mathcal{H})$ Kernel of $E_{\rho,x}$, p. 256
$\mathcal{M}_{\rho,x}(\mathcal{H})$ Quotient matrix space $\mathcal{M}(\mathcal{H})/\mathcal{K}_{\rho,x}(\mathcal{H})$, p. 256
$\mathcal{M}_{\rho,x}^{(m)}(\mathcal{H})$ Image of the map $E_{\rho,x}$ ($\{X\in\mathcal{M}(\mathcal{H})|P_\rho X=X\}$), p. 257
P_ρ Projection to the range of ρ, p. 257
$\langle Y,X\rangle_{\rho,x}^{(e)}$ See (6.13), p. 254
$\|X\|_{\rho,x}^{(e)}$ See (6.14), p. 255
$\langle A,B\rangle_{\rho,x}^{(m)}$ See (6.18), p. 255
$\|A\|_{\rho,x}^{(m)}$ See (6.19), p. 255
$\kappa_{\rho,x}$ See (6.21), p. 256
$L_{\theta,x}$ e representation based on inner product x (6.30), p. 260
$L_{\theta,s}$ SLD e representation (6.31), p. 260
$L_{\theta,b}$ Bogoljubov e representation, p. 261
$L_{\theta,r}$ RLD e representation (6.31), p. 260
$\Pi_{L,s}^{\theta}\rho_0$ SLD e parallel transport, p. 266
$\Pi_{L,b}^{\theta}\rho_0$ Bogoljubov e parallel transport, p. 266
$\Pi_{L,r}^{\theta}\rho_0$ RLD e parallel transport, p. 266
$\mathbf{Re}X$ Real part of matrix X, p. 3
$\mathbf{Im}X$ Imaginary part of matrix X, p. 3
$\mathbf{V}_\theta(X)$ Matrix with components $(\operatorname{Tr}\rho_\theta X^i X^j)$, p. 284
$\boldsymbol{\Delta}_{\rho,\sigma}$ Relative modular operator, p. 290

Error Criteria

$\hat{\mathrm{V}}_\theta(\boldsymbol{M}^n, \hat{\theta}_n)$	Mean square error (MSE) of estimator $(\boldsymbol{M}^n, \hat{\theta}_n)$ (6.71), p. 273
$\hat{\boldsymbol{V}}_\theta(\boldsymbol{M}^n, \hat{\theta}_n)$	Mean square error matrix (6.94), p. 281
$\hat{\boldsymbol{V}}_\theta(\{\boldsymbol{M}^n, \hat{\theta}_n\})$	Matrix of components $\hat{\mathrm{V}}_\theta^{i,j}(\{\boldsymbol{M}^n, \hat{\theta}_n\}) \stackrel{\mathrm{def}}{=} \lim n \hat{\mathrm{V}}_\theta^{i,j}(\boldsymbol{M}^n, \hat{\theta}_n)$, p. 281
$\beta(\{(\boldsymbol{M}^n, \hat{\theta}_n)\}, \theta, \epsilon)$	Rate function of error probability (6.84), p. 276
$\alpha(\{(\boldsymbol{M}^n, \hat{\theta}_n)\}, \theta)$	First-order coefficient of rate function (6.86), p. 278

Disturbances and Uncertainties

$\boldsymbol{\Delta}_1(X, \rho)$	Uncertainty of an observable (7.12), p. 330
$\boldsymbol{\Delta}_2(\boldsymbol{M}, \rho)$	Uncertainty of a measurement (7.13), p. 330
$\boldsymbol{\Delta}_3(\boldsymbol{M}, X, \rho)$	Deviation of POVM $\boldsymbol{M}$ from observable X (7.17), p. 330
$\boldsymbol{\Delta}_4(\kappa, X, \rho)$	Disturbance of X caused by κ (7.23), p. 332
$\boldsymbol{\Delta}_4(\boldsymbol{\kappa}, \boldsymbol{X}, \boldsymbol{\rho})$	Disturbance of X caused by $\boldsymbol{\kappa}$ (7.25), p. 332
$\varepsilon(\rho, \boldsymbol{k})$	Amount of state reduction by $\boldsymbol{\kappa}$ (7.59), p. 342

Information Quantities of q-q Channel κ and State ρ

$F_e(\rho, \kappa)$	Entanglement fidelity for TP-CP κ (8.18), p. 365
$F_e(\rho, \boldsymbol{\kappa})$	Entanglement fidelity for an instrument (8.29), p. 366
$I(\rho, \kappa)$	Transmission information of q-q channel κ (8.35), p. 370
$I_c(\rho, \kappa)$	Coherent information (8.37), p. 370
$\tilde{I}_c(\rho, \kappa)$	Pseudocoherent information (8.48), p. 372
$H_e(\kappa, \rho)$	Entropy exchange $H((\kappa \otimes \iota_R)(\lvert x\rangle\langle x\rvert))$, p. 372
$\chi_\kappa(\rho)$	Holevo information (9.6), p. 494
$H_\kappa(\rho)$	Minimum average output entropy (9.7), p. 494

Class of Local Operations ($C =$)

$\emptyset$	Only local operations, p. 360
	Local operations and zero-rate classical communications from A to B, p. 403
$\rightarrow$	Local operations and classical communications from A to B, p. 360
$\leftarrow$	Local operations and classical communications from B to A, p. 360
$\leftrightarrow$	Local operations and two-way classical communications between A and B, p. 360
S	Separable operations, p. 361
PPT	Positive partial transpose (PPT) operations, p. 418

Entanglement Measures

$E_{sq}(\rho)$	Squashed entanglement (8.127), p. 394
$E_c(\rho)$	Entanglement of cost with zero-rate communication (8.161), p. 403
$E_f(\rho)$	Entanglement of formation (8.97), p. 387
$E_{r,S}(\rho)$	Entanglement of relative entropy with separable states $\min_{\sigma\in S} D(\rho\|\sigma)$ (8.77), p. 383
$E^{\infty}_{r,S}(\rho)$	Asymptotic entanglement of relative entropy with separable states (8.82), p. 383
$E_{1+s\|S}(\rho)$	Entanglement of relative Rényi entropy with separable states $\min_{\sigma\in S} D_{1+s}(\rho\|\sigma)$ (8.133), p. 396
$\tilde{E}_{1+s\|S}(\rho)$	Entanglement of relative Rényi entropy with separable states $\min_{\sigma\in S} \underline{D}_{1+s}(\rho\|\sigma)$ (8.134), p. 396
$E_{r,\mathrm{PPT}}(\rho)$	Entanglement of relative entropy with PPT states $\min_{\sigma:PPT} D(\rho\|\sigma)$, p. 418
$E_{\mathrm{SDP}}(\rho)$	SDP bound $\min_\sigma D(\rho\|\sigma) + \log \|\tau^A(\sigma)\|_1$, p. 418
$E_{1+s\|\mathrm{SDP}}(\rho)$	SDP bound with relative Rényi entropy (8.244) $\min_\sigma D_{1+s}(\rho\|\sigma) + \log \|\tau^A(\sigma)\|_1$, p. 425
$\tilde{E}_{1+s\|\mathrm{SDP}}(\rho)$	SDP bound with relative Rényi entropy (8.245) $\min_\sigma \underline{D}_{1+s}(\rho\|\sigma) + \log \|\tau^A(\sigma)\|_1$, p. 425
$E_p(\rho)$	Entanglement of purification (8.164), p. 404
$E_{sr}(\rho)$	Logarithm of Schmidt rank (8.113), p. 391
$C_o(\rho)$	Concurrence (8.317), p. 444

Operational Entanglement Measure with Class C

$E^C_{d,1}(\rho)$	Entanglement of distillation (8.72), p. 382
$E^{C,\dagger}_{d,1}(\rho)$	Strong converse entanglement of distillation (8.73), p. 382
$E^C_{d,2}(\rho)$	ntanglement of distillation (8.75), p. 382
$E^{C,\dagger}_{d,2}(\rho)$	Strong converse entanglement of distillation (8.76), p. 382
$E^{C,\infty}_{d,e}(\rho)$	Asymptotic entanglement of exact distillation (8.89), p. 386
$E^C_{d,e}(\rho)$	E ntanglement of exact distillation (8.89), p. 386
$E^C_{d,i}(r\|\rho)$	Exponential decreasing rate for entanglement of distillation (8.90), p. 386
$E^C_c(\rho)$	Entanglement of cost (8.107), p. 390
$E^{C,\infty}_{c,e}(\rho)$	Asymptotic entanglement of exact cost (8.112), p. 391
$E^C_{c,e}(\rho)$	Entanglement of exact cost (8.112), p. 391
$E^C_{d,i}(r\|\rho)$	Exponential decreasing rate for entanglement of cost (8.91), p. 386
$E^C_m(\rho)$	Maximum of negative conditional entropy (8.119), p. 393

$E^C_{1+s\|m}(\rho)$	Maximum of negative conditional Rényi entropy (8.131), p. 396
$\tilde{E}^C_{1+s\|m}(\rho)$	Maximum of negative conditional Rényi entropy (8.132), p. 396
$E^C_{d,L}(\rho)$	Conclusive teleportation fidelity (8.88), p. 385

Security Measures

$d_1(A:E\|\rho)$	Measure for independence $\|\rho - \rho_A \otimes \rho_E\|_1$ (8.283), p. 433
$F(A:E\|\rho)$	Measure for independence $F(\rho, \rho_A \otimes \rho_E)$ (8.284), p. 433
$I'_\rho(A:E)$	Measure for independence and uniformity $D(\rho\|\rho_{\mathrm{mix},A} \otimes \rho_E)$ (8.285), p. 434
$d_{1'}(A:E\|\rho)$	Measure for independence and uniformity $\|\rho - \rho_{\mathrm{mix},A} \otimes \rho_E\|_1$ (8.287), p. 434
$F'(A:E\|\rho)$	Measure for independence and uniformity $F(\rho, \rho_{\mathrm{mix},A} \otimes \rho_E)$ (8.288), p. 434

Other Types of Correlation

$C_d^{A\to B}(\rho)$	Measure of classical correlation (8.170), p. 407
$D(B\|A)_\rho$	Discord $I_\rho(A:B) - C_d^{A\to B}(\rho)$ (8.177), p. 408
$C_c(\rho)$	See (8.198), p. 413
$C(\rho,\delta)$	See (8.200), p. 413
$\tilde{C}(\rho,\delta)$	See (8.201), p. 413
$C(\rho)$	$C(\rho,0) = \tilde{C}(\rho,0)$ (8.203), p. 413
$C_k^{A\to B-E}(\rho)$	Optimal generation rate of secret key with one-way communication (9.82), p. 521
$C_d^{A\to B-E}(\rho)$	See (9.83), p. 521

Notations for Bipartite System

$\mathcal{H}_s$	Symmetric space, p. 408
$\mathcal{H}_a$	Antisymmetric space, p. 408
F	Flip operator $P_s - P_a$, p. 408

Entangled States

$\|\Phi_L\rangle\langle\Phi_L\|$	Maximally entangled state of size L, p. 360
σ_α	Maximally correlated state (8.142), p. 398
$\rho_{W,p}$	Werner state (8.323), p. 445
$\rho_{I,p}$	Isotropic state (8.328), p. 447

Channel Capacities

$C_c(\kappa)$	Classical capacity without entangled input states (9.1), p. 493
$C_c^e(\kappa)$	Classical capacity with entangled input states (9.2), p. 493
$C_a(\rho^{A,B})$	Amount of assistance for sending information by state $\rho^{A,B}$ (9.37), p. 502
$C_{c,e}^e(\kappa)$	Entanglement-assisted classical capacity (9.42), p. 505
$C_r(W,\sigma)$	Quantum-channel resolvability capacity (9.57), p. 511
$C_c^{B,E}(W)$	Wiretap channel capacity (9.73), p. 517
$C_{q,1}$	Quantum capacity in worst case (9.101), p. 527
$C_{q,2}$	Quantum capacity with entanglement fidelity (9.101), p. 527
$C_{q,C}^\dagger(\kappa)$	Strong converse quantum capacity (9.122), p. 535
$C_{\mathrm{SDP}}(\kappa)$	SDP bound (9.127), p. 536
$C_{c,r}(W)$	Channel capacity for sending classical information with shared randomness (10.83)
$C_{c,r}^R(W)$	Reverse channel capacity for sending classical information with shared randomness (10.82), p. 594
$C_{c,e}(W)$	Channel capacity for sending classical information with shared entanglement, p. 596
$C_{c,e}^R(W)$	Reverse channel capacity for sending classical information with shared entanglement, p. 596
$C_{c,e}^e(\kappa)$	Channel capacity for sending classical information with shared entanglement and entangled input, p. 505
$C_{c,e}^{e,R}(\kappa)$	Reverse channel capacity for sending classical information with shared entanglement and entangled input, p. 596
$C_{c,r}^e(\kappa)$	Channel capacity for sending classical information with shared randomness and entangled input, p. 505
$C_{c,r}^{e,R}(\kappa)$	Reverse channel capacity for sending classical information with shared randomness and entangled input, p. 597
$C_{q,e}(\kappa)$	Channel capacity for sending quantum states with shared entanglement and entangled input, p. 597
$C_{q,e}^R(\kappa)$	Reverse channel capacity for sending quantum states with shared entanglement and entangled input, p. 597
$C_{q,r}(\kappa)$	Channel capacity for sending quantum states with shared randomness and entangled input, p. 597
$C_{q,r}^R(\kappa)$	Reverse channel capacity for sending quantum states with shared randomness and entangled input, p. 597

Minimum Compression Rates

$R_{B,q}(p,W)$	Minimum compression rate in blind and ensemble setting (10.4), p. 572
$R_{V,q}(p,W)$	Minimum compression rate in visible and ensemble setting (10.5), p. 572

$R_{P,q}(\rho)$	Minimum compression rate in purification setting (10.15), p. 573
$R^{\dagger}_{B,q}(p,W)$	Strong converse compression rate in blind and ensemble setting (10.6), p. 572
$R^{\dagger}_{V,q}(p,W)$	Strong converse compression rate in visible and ensemble setting (10.7), p. 572
$R^{\dagger}_{P,q}(\rho)$	Strong converse compression rate in purification setting (10.16), p. 573
$R_{V,c}(p,W)$	Minimum visible compression rate with classical memory (10.60), p. 587
$R_{V,q,r}(p,W)$	Minimum visible compression rate with quantum memory and shared randomness (10.72), p. 591
$R_{V,c,r}(p,W)$	Minimum visible compression rate with classical memory and shared randomness (10.73), p. 591

Codes for Quantum Source Coding

Ψ	Blind code, p. 571
Ψ	Visible code, p. 571
Ψ_c	Visible code by classical memory, p. 586
Ψ_r	Visible code with common randomness, p. 590
$\Psi_{c,r}$	Visible code with common randomness by classical memory, p. 591

About the Author

Masahito Hayashi was born in Japan in 1971. He received the B.S. degree from the Faculty of Sciences in Kyoto University, Japan, in 1994 and the M.S. and Ph.D. degrees in Mathematics from Kyoto University, Japan, in 1996 and 1999, respectively.

He worked in Kyoto University as a Research Fellow of the Japan Society of the Promotion of Science (JSPS) from 1998 to 2000, and worked in the Laboratory for Mathematical Neuroscience, Brain Science Institute, RIKEN from 2000 to 2003, and worked in ERATO Quantum Computation and Information Project, Japan Science and Technology Agency (JST) as the Research Head from 2000 to 2006. He also worked in the Superrobust Computation Project Information Science and Technology Strategic Core (21st Century COE by MEXT) Graduate School of Information Science and Technology, the University of Tokyo as Adjunct Associate Professor from 2004 to 2007. He worked in the Graduate School of Information Sciences, Tohoku University as Associate Professor from 2007 to 2012. In 2012, he joined the Graduate School of Mathematics, Nagoya University as Professor. He also worked at the Centre for Quantum Technologies, National University of Singapore as Visiting Research Associate Professor from 2009 to 2012 and as Visiting Research Professor from 2012 to now. In 2011, he received Information Theory Society Paper Award (2011) for Information-Spectrum Approach to Second-Order Coding Rate in Channel Coding. In 2016, he received the Japan Academy Medal from the Japan Academy and the JSPS Prize from Japan Society for the Promotion of Science.

He is a member of the Editorial Board of International Journal of Quantum Information and International Journal On Advances in Security. His research interests include classical and quantum information theory, information-theoretic security, and classical and quantum statistical inference.

Prologue

Invitation to Quantum Information Theory

Understanding the implications of recognizing matter and extracting information from it has been a long-standing issue in philosophy and religion. However, recently this problem has become relevant to other disciplines such as cognitive science, psychology, and neuroscience. Indeed, this problem is directly relevant to quantum mechanics, which forms the foundation of modern physics. In the process of recognition, information cannot be obtained directly from matter without any media. To obtain information, we use our five senses; that is, a physical medium is always necessary to convey information to us. For example, in vision, light works as the medium for receiving information. Therefore, observations can be regarded as information processing via a physical medium. Hence, this problem can be treated by physics. Of course, to analyze this problem, the viewpoint of information science is also indispensable because the problem involves, in part, information processing.

In the early twentieth century, physicists encountered some unbelievable facts regarding observations (measurements) in the microscopic world. They discovered the contradictory properties of light, i.e., the fact that light has both wave- and particle-like properties. Indeed, light behaves like a collection of minimum energy particles called photons. In measurements using light, we observe the light after interactions with the target. For example, when we measure the position of the matter, we detect photons after interactions with them. Since photons possess momentum and energy, the speed of the object is inevitably disturbed.[1] In particular, this disturbance cannot be ignored when the mass of the measured object is small in comparison with the energy of the photon. Thus, even though we measure the velocity of an object after the measurement of its position, we cannot know the velocity of an object precisely because the original velocity has been disturbed by

[1]The disturbance of measurement is treated in more detail in the formulation of quantum mechanics in Chap. 7.

the first measurement. For the same reason, when we measure the velocity first, its position would be disturbed. Therefore, our naive concept of a "perfect measurement" cannot be applied, even in principle. In the macroscopic world, the mass of the objects is much larger than the momentum of the photons. We may therefore effectively ignore the disturbance by the collisions of the photons. Although we consider that a "perfect measurement" is possible in this macroscopic world, the same intuition cannot be applied to the microscopic world.

In addition to the impossibility of "perfect measurements" in the microscopic world, no microscopic particles have both a determined position and a determined velocity. This fact is deeply connected to the wave-particle duality in the microscopic world and can be regarded as the other side of the nonexistence of "perfect measurements."[2] Thus it is impossible to completely understand this microscopic world based on our macroscopic intuitions, but it is possible to predict probabilistically its measured value based on the mathematical formulation of quantum theory.

So far, the main emphasis of quantum mechanics has been on examining the properties of matter itself, rather than the process of *extracting information*. To discuss how the microscopic world is observed, we need a quantitative consideration from the viewpoint of "information." Thus, to formulate this problem clearly, we need various theories and techniques concerning information. Therefore, the traditional approach to quantum mechanics is insufficient. On the other hand, theories relating to information pay attention only to the data-processing rather than the extraction process of information. Therefore, in this quantum-mechanical context, we must take into account the process of obtaining information from microscopic (quantum-mechanical) particles. We must open ourselves to the new research field of *quantum information science*. This field is to be broadly divided into two parts: (1) *quantum computer science*, in which algorithms and complexity are analyzed using an approach based on computer science, and (2) *quantum information theory*, in which various protocols are examined from the viewpoint of information theory and their properties and limits are studied. Specifically, since quantum information theory focuses on the amount of accessible information, it can be regarded as the theory for quantitative evaluation of the process of *extracting information*, as mentioned above.

Since there have been only a few textbooks describing the recent developments in this field [1, 2], the present textbook attempts to provide comprehensive information ranging from the fundamentals to current research. Quantum computer science is not treated in this book because it has been addressed in many other textbooks. Since quantum information theory forms a part of the basis of quantum computer science, this textbook may be useful for not only researchers in quantum information theory but also those in quantum computer science.

[2]The relation between this fact and nonexistence can be mathematically formulated by (7.27) and (7.30).

History of Quantum Information Theory in Twentieth Century

Although quantum information theory has been very actively studied in the twenty first century, the root can be traced to the studies in the twentieth century. Let us briefly discuss the history of quantum information theory in the twentieth century. Quantum mechanics was first formulated by Schrödinger (wave mechanics) and Heisenberg (matrix mechanics). However, their formulations described the dynamics of microscopic systems, but they had several unsatisfactory aspects in descriptions of measurements. Later, the equivalence between both formulations were proved. To resolve this point, von Neumann [3] established the formulation of quantum theory that describes measurements as well as dynamics based on operator algebra, whose essential features will be discussed in Chap. 1. However, in studies of measurements following the above researches, the philosophical aspect has been emphasized too much, and a quantitative approach to extracting information via measurements has not been examined in detail. This is probably because approaches to mathematical engineering have not been adopted in the study of measurements.

In the latter half of the 1960s, a Russian researcher named Stratonovich, who is one of the founders of stochastic differential equations, and two American researchers, Helstrom and Gordon, proposed a formulation of optical communications using quantum mechanics. This was the first historical appearance of quantum information theory. Gordon [4, 5], Helstrom [6], and Stratonovich [7] mainly studied error probabilities and channel capacities for communications. Meanwhile, Helstrom [8] examined the detection process of optical communication as parameter estimation. Later, many American and Russian researchers such as Holevo [9, 10], Levitin [11], Belavkin [12], Yuen [13], and Kennedy [14] also examined these problems.[3] In particular, Holevo obtained the upper bound of the communication speed in the transmission of a classical message via a quantum channel in his two papers [9, 10] published in the 1970s. Further, Holevo [16, 18], Yuen [13], Belavkin, and their coworkers also analyzed many theoretically important problems in quantum estimation.

Unfortunately, the number of researchers in this field rapidly decreased in the early 1980s, and this line of research came to a standstill. Around this time, Bennett and Brassard [19] proposed a quantum cryptographic protocol (BB84) using a different approach to quantum mechanical systems. Around the same time, Ozawa [20] gave a precise mathematical formulation of the state reduction in the measurement process in quantum systems.

[3]Other researchers during this period include Grishanin, Mityugov, Kuriksha, Liu, Personick, Lax, Lebedev, Forney [15] in the United States and Russia. Many papers were published by these authors; however, an accurate review of all of them is made difficult by their lack of availability. In particular, while several Russian papers have been translated into English, some of them have been overlooked despite their high quality. For details, see [16, 17].

In the latter half of the 1980s, Nagaoka investigated quantum estimation theory as a subfield of mathematical statistics. He developed the asymptotic theory of quantum-state estimation and quantum information geometry [21]. This research was continued by many Japanese researchers, including Fujiwara, Matsumoto, and the present author in the 1990s [22–39]. For this history, see Hayashi [40].

In the 1990s, in the United States and Europe several researchers started investigating quantum information processing, e.g., quantum data compression, quantum teleportation, superdense coding, another quantum cryptographic protocol (B92), etc. [41–46]. In the second half of the 1990s, the study of quantum information picked up speed. In the first half of the 2000s, several information-theoretic approaches were developed, and research has been advancing at a rapid pace.

We see that progress in quantum information theory has been achieved by connecting various topics. This text clarifies these connections and discusses current research topics starting with the basics.

Structure of the Book

Quantum information theory has been studied by researchers from various backgrounds. Their approach can be broadly divided into two categories. The first approach is based on information theory. In this approach, existing methods for information processing are translated (and extended) into quantum systems. The second approach is based on quantum mechanics.

In this text, four chapters are dedicated to examining problems based on the first approach, i.e., establishing information-theoretic problems. These are Chap. 3, "Quantum Hypothesis Testing and Discrimination of Quantum States," Chap. 4, "Classical Quantum Channel Coding (Message Transmission)," Chap. 6, "Quantum Information Geometry and Quantum Estimation," and Chap. 10, "Source Coding in Quantum Systems." Problems based on the second approach is treated in three chapters: Chap. 5, "State evolution and Trace-Preserving Completely Positive Maps," Chap. 7, "Quantum measurements and State Reduction," and Chap. 8, "Entanglement and Locality Restrictions."

Advanced topics in quantum communication such as quantum teleportation, superdense coding, quantum-state transmission (quantum error correction), and quantum cryptography are often discussed in quantum information theory. Both approaches are necessary for understanding these topics, which are covered in Chap. 9, "Analysis of Quantum Communication Protocols."

Some quantum-mechanical information quantities are needed to handle these problems mathematically, and these problems are covered in Sects. 3.1, 5.4, 5.5, 5.6, 8.2, and 8.3. This allows us to touch upon several important information-theoretic problems using a minimum amount of mathematics. The book also includes 450 exercises together with solutions. Solving these problems should provide readers not

only with knowledge of quantum information theory but also the necessary techniques for pursuing original research in the field.

Chapter 1 covers the mathematical formulation of quantum mechanics in the context of quantum information theory. It also gives a review of linear algebra. Chapter 2 summarizes classical information theory. This not only provides an introduction to the later chapters but also serves as a brief survey of classical information theory. This chapter covers entropy, Fisher information, information geometry, estimation of probability distribution, large deviation principle. Also, it discusses the axiomatic characterization of entropy. This concludes the preparatory part of the text. Section 2.6 treats the large deviation on the sphere, which is used only in Sect. 8.13. So, a reader can skip it before stating Sect. 8.13.

Chapter 3 covers quantum hypothesis testing and the discrimination of quantum states. This chapter starts with introduction of information quantities in quantum systems. Then, this chapter serves to answer the question: If there are two states, which is the true state? The importance of this question may not at first be apparent. However, this problem provides the foundation for other problems in information theory and is therefore crucially important. Also, this problem provides the basic methods for quantum algorithm theory. Many of the results of this chapter will be used in subsequent chapters. In particular, the quantum version of Stein's lemma is discussed here; it can be used a basic tool for other topics. Furthermore, many of the difficulties associated with the noncommutativity of quantum theory can be seen here in their simplest forms. This chapter can be mainly read after Chap. 1 and Sects. 2.1 and A.3.

Chapter 4 covers classical quantum channel coding (message transmission). That is, we treat the tradeoff between the transmission speed and the error probability in the transmission of classical messages via quantum states. In particular, we discuss the channel capacity, i.e., the theoretical bound of the transmission rate when the error probability is 0, as well as its associated formulas. This chapter can be read after Chap. 1 and Sects. 2.1, 3.1, 3.5, 3.7, and 3.8.

Chapter 5 discusses the trace-preserving completely positive map, which is the mathematical description of state evolution in quantum systems. Its structure will be illustrated with examples in quantum two-level systems. We also briefly discuss the relationship between the state evolution and information quantities in quantum systems (the entropy and relative entropy). In particular, the part covering the formulation of quantum mechanics (Sects. 5.1–5.3) can be read after only Chap. 1.

Chapter 6 describes the relation among quantum information geometry, quantum information quantities, and quantum estimation. First, the inner product for the space of quantum states is briefly discussed. Next, we discuss the geometric structure naturally induced from the inner product. The theory of state estimation in quantum systems is then discussed by emphasizing the Cramér–Rao inequality. Most of this chapter except for Sect. 6.7 can be read after Chaps. 1 and 2 and Sect. 5.1. Section 6.7 can be read after Chap. 1 and Sects. 5.1, 5.4, and 6.1.

Chapter 7 covers quantum measurement and state reduction. First, it is shown that the state reduction due to a quantum measurement follows naturally from the axioms of the quantum systems discussed in Chap. 1. Next, we discuss the relation

between quantum measurement and two types of uncertainty relations, square error type uncertainty and entropic uncertainty. Finally, it is shown that under certain conditions it is possible, in principle, to perform a measurement such that the required information can be obtained while the state demolition is negligible. Readers who only wish to read Sects. 7.1 and 7.4 can read them after Chap. 1 and Sect. 5.1. Section 7.2 requires the additional background of Sect. 6.1. Section 7.3 can be read after Chap. 1 and Sects. 5.1, 5.4, 5.5, and 5.6.

Chapter 8 discusses the relation between locality and entanglement, which are fundamental topics in quantum mechanics. First, we examine state operations when the locality condition is imposed on quantum operations. Next, the information quantities related to entanglement are considered. The theory for distilling a perfect entangled state from a partially entangled state is discussed. Information-theoretic methods play a central role in entanglement distillation. Quantification of entanglement is discussed from various viewpoints. As opposite task, we discuss the entanglement of dilution, which evaluates the cost to generate a given partially entangled state. While this task is characterized by using the entanglement formation, we discuss the nonadditivity of this quantity. As another types of correlation, we discuss discord. Further, we consider the duality of conditional entropy, secure random number generation, and state generation from shared randomness.

Chapter 9 delves deeply into topics in quantum channels such as quantum teleportation, superdense coding, quantum-state transmission (quantum error correction), and quantum key distribution based on the theory presented in previous chapters. These topics are very simple when noise is not present. However, if noise is present in a channel, these problems require the information-theoretic methods discussed in previous chapters. The relationship among these topics is also discussed. Further, the relation between channel capacities and entanglement theory is also treated. The additivity problem for the classical-quantum channel capacity is discussed in Sects. 8.13 and 9.2.

Finally, Chap. 10 discusses source coding in quantum systems. We treat not only the theoretical bounds of quantum fixed-length source coding but also universal quantum fixed-/variable-length source coding, which does not depend on the form of the information source. The beginning part of this chapter, excepting the purification scheme, requires only the contents of Chaps. 1 and 2 (Sects. 2.1–2.4) and Sect. 5.1. In particular, in universal quantum variable-length source coding, a measurement is essential for determining the coding length. Hence this measurement causes the demolition of the state to be sent, which makes this a more serious problem. However, it can be solved by a measurement with negligible state demolition, which is described in Chap. 7. Then we treat quantum-state compression with mixed states and its several variants. The relations between these problems and entanglement theory are also treated. Further, we treat the relationships between the reverse capacities (reverse Shannon theorem) and these problems. Excluding Sects. 10.6–10.9, this chapter can be read after Chap. 1 and Sects. 2.1, 2.3, 3.1, 4.1, and 5.1.

This text thus covers a wide variety of topics in quantum information theory. Quantum hypothesis testing, quantum-state discrimination, and quantum-channel coding (message transmission) have been discussed such that only a minimal

amount of mathematics is needed to convey the essence of these topics. Prior to this text, these topics required the study of advanced mathematical theories for quantum mechanics, such as those presented in Chap. 5. Further, Chaps. 5 ("State Evolution and Trace Preserving Completely Positive Maps in Quantum Systems") and 7 ("Quantum Measurement and State Reduction") have been written such that they can be understood with only the background provided in Chap. 1. Therefore, this text should also be suitable for readers who are interested in either the information-theoretic aspects of quantum mechanics or the foundations of quantum mechanics

References

1. M.M. Wilde, *Quantum Information Theory* (Cambridge University Press, 2013)
2. M. Hayashi, S. Ishizaka, A. Kawachi, G. Kimura, T. Ogawa, *Introduction to Quantum Information Science* (Graduate Texts in Physics, 2014)
3. J. von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, NJ, 1955). (Originally appeared in German in 1932)
4. J.P. Gordon, Proc. IRE. **50**, 1898–1908 (1962)
5. J.P. Gordon, Noise at optical frequencies; information theory, in *Quantum Electronics and Coherent Light*, *Proceedings of the International School Physics "Enrico Fermi," Course XXXI*, ed. by P.A. Miles. (Academic, New York, 1964), pp. 156–181
6. C.W. Helstrom, Detection theory and quantum mechanics. Inf. Contr. **10**, 254–291 (1967)
7. R.L. Stratonovich, Izvest. VUZ Radiofiz., **8**, 116–141 (1965)
8. R.L. Stratonovich, The transmission rate for certain quantum communication channels. Problemy Peredachi Informatsii, **2**, 45–57 (1966). (in Russian). English translation: Probl. Inf. Transm. **2**, 35–44 (1966.)
9. A.S. Holevo, Bounds for the quantity of information transmitted by a quantum communication channel. Problemy Peredachi Informatsii. **9**, 3–11 (1973) (in Russian). (English translation: Probl. Inf. Transm. **9**, 177–183 (1975)
10. A.S. Holevo, On the capacity of quantum communication channel. Problemly Peredachi Informatsii, **15**, 4, 3–11 (1979) (in Russian). (English translation: Probl. Inf. Transm. **15**, 247–253 (1979)
11. L.B. Levitin, On quantum measure of information, in *Proceedings of the 4th All-Union Conference on Information Transmission and Coding Theory*, pp. 111–115 (Tashkent, 1969) (in Russian). English translation: *Information, Complexity and Control in Quantum Physics*, ed. by, A. Blaquiere, S. Diner, G. Lochak (Springer, Berlin, Heidelberg, New York, 1987), pp. 15–47
12. V.P. Belavkin, Generalized uncertainty relations and efficient measurements in quantum systems. Teor. Mat. Fiz. **26**, 3, 316–329 (1976). (quant-ph/0412030, 2004)
13. H.P. Yuen, M. Lax, Multiple-parameter quantum estimation and measurement of non-selfadjoint observables. IEEE Trans. Inf. Theory **19**, 740 (1973)
14. H.P. Yuen, R.S. Kennedy, M. Lax, Optimum testing of multiple hypotheses in quantum detection theory. IEEE Trans. Inf. Theory 125–134 (1975)
15. G.D. Forney, Jr., S.M. Thesis, (MIT, 1963, unpublished)
16. A.S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, (North-Holland, Amsterdam, 1982); (originally published in Russian, 1980)
17. C.W. Helstrom, Minimum mean-square error estimation in quantum statistics. Phys. Lett. **25A**, 101–102 (1976)

18. A.S. Holevo, Covariant measurements and uncertainty relations. Rep. Math. Phys. **16**, 385–400 (1979)
19. C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, (Bangalore, India, 1984), pp. 175–179
20. M. Ozawa, Quantum measuring processes of continuous observables. J. Math. Phys. **25**, 79 (1984)
21. H. Nagaoka, Differential geometrical aspects of quantum state estimation and relative entropy, in *Quantum Communications and Measurement*, ed. by V.P. Belavkin, O. Hirota, R.L. Hudson (Plenum, New York, 1995), pp. 449–452
22. A. Fujiwara, *Statistical Estimation Theory for Quantum States*, master's thesis Department of Mathematical Engineering and Information Physics, Graduate School of Engineering, University of Tokyo, Japan (1993) (in Japanese)
23. A. Fujiwara, *A Geometrical Study in Quantum Information Systems*, Ph.D. thesis, Department of Mathematical Engineering and Information Physics, Graduate School of Engineering, University of Tokyo, Japan (1995)
24. A. Fujiwara, H. Nagaoka, Quantum Fisher metric and estimation for pure state models. Phys. Lett. **201A**, 119–124 (1995)
25. A. Fujiwara, H. Nagaoka, Coherency in view of quantum estimation theory, in *Quantum Coherence and Decoherence*, ed. by K. Fujikawa, Y.A. Ono. (Elsevier, Amsterdam, 1996), pp. 303–306
26. A. Fujiwara, H. Nagaoka, An estimation theoretical characterization of coherent states. J. Math. Phys. **40**, 4227–4239 (1999)
27. M. Hayashi, *Minimization of Deviation Under Quantum Local Unbiased Measurements,* master's thesis, Department of Mathematics, Graduate School of Science, Kyoto University, Japan (1996)
28. M. Hayashi, A linear programming approach to attainable cramer-rao type bound and randomness conditions. Kyoto-Math 97–08; quant-ph/9704044 (1997)
29. M. Hayashi, A linear programming approach to attainable Cramer–Rao type bound, in *Quantum Communication, Computing, and Measurement*, ed. by, O. Hirota, A.S. Holevo, C.M. Caves. (Plenum, New York, 1997), pp. 99–108. (Also appeared as Chap. 12 of *Asymptotic Theory of Quantum Statistical Inference,*, ed. by M. Hayashi)
30. M. Hayashi, Asymptotic estimation theory for a finite dimensional pure state model. J. Phys. A Math. Gen. **31**, 4633–4655 (1998). (Also appeared as Chap. 23 of *Asymptotic Theory of Quantum Statistical Inference*, ed. by, M. Hayashi)
31. M. Hayashi, Asymptotic quantum estimation theory for the thermal states family, in *Quantum Communication, Computing, and Measurement 2*, ed. by P. Kumar, G. M. D'ariano, O. Hirota. (Plenum, New York, 2000) pp. 99–104; quant-ph/9809002 (1998). (Also appeared as Chap. 14 of *Asymptotic Theory of Quantum Statistical Inference,*, ed. by M. Hayashi)
32. M. Hayashi, Asymptotic large deviation evaluation in quantum estimation theory, in *Proceedings of the Symposium on Statistical Inference and Its Information-Theoretical Aspect*, pp. 53–82 (1998) (in Japanese)
33. M. Hayashi, Quantum estimation and quantum central limit theorem. *Sugaku*. **55**, 4, 368–391 (2003) (in Japanese); English translation is in *Selected Papers on Probability and Statistics* (American Mathematical Society Translations Series 2) vol. 277, pp. 95–123 (2009)
34. M. Hayashi, K. Matsumoto, Statistical model with measurement degree of freedom and quantum physics. RIMS koukyuroku Kyoto Univiversity, **1055**, 96–110 (1998) (in Japanese). (Also appeared as Chap. 13 of *Asymptotic Theory of Quantum Statistical Inference,* ed. by M. Hayashi)
35. K. Matsumoto, *Geometry of a Quantum State*, master's thesis, Department of Mathematical Engineering and Information Physics, Graduate School of Engineering, University of Tokyo, Japan (1995) (in Japanese)

36. K. Matsumoto, A new approach to the Cramér–Rao type bound of the pure state model. J. Phys. A Math. Gen. **35**, 3111–3123 (2002)
37. K. Matsumoto, *A Geometrical Approach to Quantum Estimation Theory*, Ph.D. thesis, Graduate School of Mathematical Sciences, University of Tokyo (1997)
38. K. Matsumoto, The asymptotic efficiency of the consistent estimator, Berry-Uhlmann' curvature and quantum information geometry, in *Quantum Communication, Computing, and Measurement 2*, ed. by P. Kumar, G. M. D'ariano, O. Hirota. (Plenum, New York, 2000), pp. 105–110
39. K. Matsumoto, Seminar notes (1999)
40. M. Hayashi (eds.), *Asymptotic Theory of Quantum Statistical Inference: Selected Papers,* (World Scientific, Singapore, 2005)
41. B. Schumacher, Quantum coding. Phys. Rev. A **51**, 2738–2747 (1995)
42. R. Jozsa, B. Schumacher, A new proof of the quantum noiseless coding theorem. J. Mod. Opt. **41(12)**, 2343–2349 (1994)
43. C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **70**, 1895 (1993)
44. C.H. Bennett, H.J. Bernstein, S. Popescu, B. Schumacher, Concentrating partial entanglement by local operations. Phys. Rev. A, **53**, 2046 (1996)
45. C.H. Bennett, S.J. Wiesner, Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys. Rev. Lett. **69**, 2881 (1992)
46. C.H. Bennett, Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)