HAYASHI, Masahito Professor

Office: Rm 355 in Sci. Bldg. A

Telephone: +81 (0)52–789–2549 (ext. 2549)

E-mail: masahito@math.nagoya-u.ac.jp

Website: http://www.math.nagoya-u.ac.jp/~masahito/index_e.html

Membership of academic societies:

IEEE (The Institute of Electrical and Electronics Engineers), The Mathematical Society of Japan, JPS (The Physical Society of Japan), IEICE (The Institute of Electronics, Information and Communication Engineers)

Research Interest:

- Quantum Information Theory
- Quantum Cryptography
- Information Theory
- Foundation of Thermodynamics

Research Summary:

My research area is mathematical theory for information and its application, especially, I have studied mathematical theory for communication, statistical inference, and cryptography. These topics have different applied aspects, and have different communities due to their historical reason. However, these topics have common mathematical aspects. Hence, a common mathematical treatment is possible for these topics. I have investigated these topics based on the common mathematical properties. In particular, I have studies these topics mainly for quantum systems but also for non-quantum (classical) system. Recently, using this method, I study the foundation of thermodynamics.

Recently, I am mainly studying the following points. One is mathematical treatment for quantum information processing based on group representation theory. Group symmetry simplifies many kinds of problems in quantum systems by removing the basis dependence. In fact, even if a given information processing problem requires a difficult analysis due to the complexity of the problem, the group symmetry simplifies the problem by reducing the complexity. Using the group symmetry, we can construct universal protocols that works independently of the basis. Since the group-theoretical approach to quantum systems are not finished, further developments are required. The second is mathematical theory for information-theoretical secrecy. Recently, I have proposed several approaches for this topic, however, their relations are not so clear and several problems still remain open. Thus, further researches are required for this topic. The third is the information theory for Markov chain. This topic can be treated via Perron-Frobenius theorem. Finally, I am also working on refining the Carnot Theorem in thermodynamics.

Major Publications:

[1] M. Hayashi and H. Nagaoka, "General formulas for capacity of classical-quantum channels," IEEE Transactions on Information Theory, **49** (2003), no. 7, 1753-1768.

[2] M. Hayashi, "Upper bounds of eavesdropper's performances in finite-length code with the decoy method," Physical Review A, **76**, (2007), 012329.
[3] M. Hayashi, "Universal coding for classical-quantum channel," Communications in Mathematical Physics **289** (2009), no. 3, 1087-1098.
[4] M. Hayashi, "Information Spectrum Approach to Second-Order Coding Rate in Channel Coding," IEEE Transactions on Information Theory, **55** (2009), no. 11, 4947 - 4966.

Awards and Prizes:

- *2011 IEEE Information Theory Society Paper Award:* "Information Spectrum Approach to Second-Order Coding Rate in Channel Coding" *IEEE Transactions on Information Theory*, Vol. 55, No. 11, 4947 - 4966 (2009). This prize is the most distinguished paper award in the information theory community.
- Japan IBM prize in the computer science section 2010: "Universal protocol in quantum information and its application to quantum key distribution" This prize is one of the most distinguished prizes in Japan among information science for researchers across Japan under 45.
- Funai Foundation for Information Technology Award in the computer science category 2010: "Universal quantum information protocol and its application to quantum cryptography"
- 2001 SITA Encouragement Award (by The Society of Information Theory and its Applications (SITA)): "Variable length universal entanglement concentration by local operations"

Education and Appointments:

1998 JSPS Research Fellow at Kyoto University
2000 Researcher, Brain Science Institute, RIKEN
2003 Research Manager, ERATO Quantum Computation and Information Project, Japan Science and Technology Agency
2007 Associate Professor, Tohoku University
2012 Professor, Nagoya University

Message to Prospective Students:

The following are candidates of topic for Master course:

> Quantum information theory, Quantum cryptography, Quantum statistical inference, Information theory.

Since these topics are linked to each other, it is possible to tackle one topic based on knowledge obtained from another topic. The following texts are useful for these topics.

- M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).
- M. Hayashi, *Quantum Information: An Introduction*, Springer (2006).
- M. Hayashi, S. Ishizaka, A. Kawachi, G. Kimura, and T. Ogawa, *Introduction to Quantum Information Science*, Graduate Texts in Physics, Springer (2014).

Since quantum information is a new area, students can relatively easily publish their own research article while the possibility depends on their efforts and their ability. Required preliminary knowledge is level 1, which corresponds to the contents for first, second, and third year courses. In particular, I ask students to master linear algebra, calculus, and elementary probability, which

contains the central limit theorem but does not necessarily contain measure theory, because they are very important for these topics. Since these topics are opened to other research area, students are required to study topics outside of mathematics. Since the above research topics are applied to practical problems, it is required not only to understand mathematically formulated problems but also to grasp the target problem itself. For doctoral course, I can supervise group-theoretical approaches to the above topics as well as the above topics themselves.