林　正人　（はやし　まさひと／Hayashi Masahito）　教授

研　究　室　理学部A館 355号室　(内線番号 2549)
電子メール　masahito@math.nagoya-u.ac.jp
http://www.math.nagoya-u.ac.jp/~masahito/index_j.html
所 属 学 会　日本数学会, 日本物理学会，電子情報通信学会，IEEE

研究テーマ

- 量子情報理論
- 情報理論
- 量子論基礎

研究テーマの概要

専門は，情報についての数学的理論とその応用であり，中でも，通信，統計的推論，セキュリティに関する数学的理論を扱っている．これらのテーマは実用面に注目すると全く異なった理論体系であり，それらの歴史的経緯も相俟って，独立にコミュニティーが形成されている．しかしながら，数学サイドからこれらのテーマを見ると，意外に共通点が多く，共通の手法で取り扱いが可能な部分が多い．このような観点から，これらのテーマについて研究を行っている．また，特に，量子力学系でのこれらのテーマを研究しているが，非量子系（古典系）のこれらのテーマについても研究している．さらに近年は，これらの手法を用いて熱力学の基礎付けに関する研究も行っている．

最近，特に以下に重点を置いて研究を行っている．１点目は，表現論をベースにした量子系での情報処理の数学的な取り扱いである．量子系は，意外に群論的対称性と相性がよく，一般に解析が困難な問題であっても，群論的対称性があると，途端に問題の自由度が減少し，解析が容易になることが多い．また，その対称性からユニバーサルに機能するプロトコルを構成することも可能であり，量子系での群論的アプローチについては，今後さらなる発展が期待できる．２点目は，情報理論的にセキュアなプロトコルの研究である．これまで量子系・古典系双方の設定で，様々な情報理論的にセキュアなプロトコルが提案されてきた．しかしながら，未だに十分に研究されていないタスクがたくさん有り，これらについて更なる研究が必要とされている．これまでになされた，情報理論的秘匿性に関する数学的理論をベースにした更なる研究が必要とされている．特に，単に情報理論的枠組みの中に閉じて議論するのではなく，計算を伴うタスクに関する情報理論的にセキュアなプロトコルについても興味を持っている．３点目は，量子論の基礎付けに関する研究である．従来このテーマについては，情報理論的な視点からのアプローチが少なかった．近年は，情報理論的な操作的視点から量子論の基礎付けを行う研究も現れてきた．このような方向性の研究にも取り組んでいる．

主要論文・著書

[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.
[5] M. Hayashi, *Quantum Information Theory: A Mathematical Foundation*, Graduate Texts in Physics, Springer (2017).

[6] M. Hayashi, *A Group Theoretic Approach to Quantum Information*, Springer (2017).
[7] M. Hayashi, *Group Representation for Quantum Theory*, Springer (2017).

受賞歴

- 2010年, 第24回「日本IBM科学賞 コンピュータ・サイエンス分野」,「量子情報におけるユニバーサルプロトコル理論の構築と量子暗号への応用」
- 2011年, 第10回　船井情報科学振興財団「船井学術賞　コンピューターサイエンス分野」,「ユニバーサル量子情報プロトコルの構築と量子暗号への応用」
- 2011年, 2011 IEEE Information Theory Society Paper Award, "Information Spectrum Approach to Second-Order Coding Rate in Channel Coding"
- 2015年, 第12回 日本学術振興会賞「有限符号長の情報理論及び量子情報理論」
- 2016年, 第12回 日本学士院学術奨励賞「有限符号長の情報理論及び量子情報理論」
- 2017年, IEEE fellow

経歴

1998年　日本学術振興会 特別研究員 (DC2)
1999年　京都大学大学院 理学研究科 数学・数理解析専攻（数学系）博士後期課程 修了
2000年　理化学研究所 脳科学総合研究センター 研究員
2003年　科学技術振興機構 ERATO 今井量子計算機構プロジェクト 技術参事
2006年　科学技術振興機構 ERATO-SORST 量子情報システムアーキテクチャ グループリーダー
2007年　東北大学 大学院情報科学研究科 准教授
2012年　名古屋大学 大学院多元数理科学研究科 教授
2020年　南方科技大学 量子科学与工程研究院 首席科学家（兼任）

学生へのメッセージ

1月を除き名大を研究休職し南方科技大学で勤務している．名大と南方科技大学との間には学術交流協定があるので，この範囲で名大の学生を指導することは可能である．この場合，オンラインでの指導がメインであるので，最低限のことを自分でこなせる学生についてのみ指導が可能となる．博士前期課程（修士課程）における少人数クラスのテーマとしては，

量子情報理論，量子統計推測，情報理論など

が挙げられる．テキストとしては，上記の [5][6][7] に加え，以下が挙げられる．

- 石坂智，小川朋宏，河内亮周，木村元，林正人,「量子情報科学入門」共立出版，2012. (英語版, Introduction to Quantum Information Science, Graduate Texts in Physics, Springer, (2014))
- M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).

比較的新しい研究分野であるので，本人の素養や努力にも依存するが，他の分野と比べて早い段階で，研究論文を執筆できるレベルに到達できる．予備知識としては，レベル1の知識（学部3年生までに学習する程度のもの）に加え，確率・統計の知識（測度論は必要ではない）の知識が必要である．特に，線型代数，確率・統計，微積分などの基礎をしっかりと理解し使いこなせるようになっていてほしい．同時に，これらの研究テーマは数学の中で閉じたものではないので，関連する数学以外の内容についても興味を持って自ら学ぶ姿勢が必要である．また，数学の応用分野であるため，数学的に定式化された問題のみを見るのではなく，数学として扱う対象となっている問題をそのものを捉えようとする姿勢が重要となる．