量子情報科学概論


東北大学　情報科学研究科
CQT, シンガポール国立大学
林　正人
東北大学 大学院情報科学研究科
Graduate School of Information Sciences.TOHOKU University
NUS
National University of Singapore
GSIS
Graduate School of Information Sciences.
TOHOKU University
DEX-SMI
TOHOKU
UNIVERSITY
CQT
Centre for
Quantum
Technologies

自己紹介

- 1994 年 3 月 京都大学理学部卒業（数学及び物理学）
- 1998 年 4 月 日本学術振興会 特別研究員
- 1999 年 3 月 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 4 月 理化学研究所 脳科学総合研究センター 脳数理研究チーム 研究員
- 2003 年 4 月 ERATO 今井量子計算機構プロジェクト 技術参事
- 2004 年 11 月 - 平成 19 年 3 月東京大学大学院 情報理工学系研究科 21世紀COE「情報科学技術戦略コア」超ロバスト計算原理プロジェクト 特任助教授(兼務)
- 2006 年 4 月 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 9 月 - 東北大学 大学院情報科学研究科（数学） 准教授
- 2009 年 9 月 - Visiting Research Associate Professor, Centre for Quantum Technologies, National University of Singapore（兼任）

量子情報科学の世界

量子情報の理論分野

量子系の数理的な体系に

基づく情報処理プロトコルの

可能性を探る

（量子数理＋情報科学）

量子情報実験

量子情報処理を

実験的に実現する

（物性物理実験）

実装化理論

量子情報処理の実現

に適した素材の研究

（物性物理理論）

現在の情報処理(コンピュータ・通信)の階層構造

アプリケーション

基本ソフトウェア　ブラウザ

ハードウェア

回路設計　誤り訂正

ネットワークプロトコル技術

(個々の物理的な要素の組み合わせ)

物理層

半導体　　光ファイバー

将来の量子情報処理の階層構造

アプリケーション？

基本ソフトウェア？　ブラウザ？

ハードウェア

数理的情報処理技術

（個々の量子デバイスの組み合わせ）

物理層

量子メモリ，量子回路
量子通信路

量子情報の理論分野

量子計算

量子アルゴリズム

量子計算量

量子情報理論

量子通信（Shannon）理論

量子統計推測

量子プロトコル

量子暗号

エンタングルメント

グラフ理論

離散数学

表現論

暗号理論

量子論基礎

情報理論

情報幾何

関数解析

統計学

量子情報の理論分野の魅力

- 量子効果による新技術
- 数学的な記述が単純な理論体系
- 複数の領域に跨る研究
- 実験分野と理論分野の結合
- 従来分野の理論的基礎に対する再考察
- 量子情報を通じた既存分野の連携

量子情報の理論分野の難解さ(敷居の高さ)

- 概念的な難しさと新しさ
  - ある概念の量子版が一意に定まらない　例:誤り訂正
  - 状況に応じて適切な量子版の適用
- 単純であるが相対的にハイレベルな数学
  - 初等確率論＋組み合わせ論だけでは不可！
  - 線型代数(行列代数)は必須
- 既存分野からの乖離
- 議論の前提が様々(論文によって異なる)

⇒ 基礎となる理論体系は整備されつつある

量子統計推測

- 統計学で扱う議論の量子版
- 統計学とは.
  - 確率分布をデータから推測することを目的とし，その際にその精度保証に必要な議論を行う.
  - 英国とインドで発展
  - 日本では，統計数理研究所，東大，広島大，九州大，阪大，東工大，筑波大などが伝統的に強い.
  - 1つの中心テーマとして，確率分布を記述するパラメータを推定する際の平均二乗誤差を最適化することがある.
  - この問題の典型的な解が，Cramer-Rao不等式.
  - 不偏推定量の平均二乗誤差はFisher 情報量の逆数よりも大きい
- 量子系の統計学（量子統計推測）では，データから密度行列を推測することを目的とする.

量子統計推測

- 1967 Helstrom: 1パラメータのときの量子Cramer-Rao 不等式
- 1973 Yuen-Lax: 量子ガウス状態族の期待値パラメータの推定（実部と虚部の同時推定）
- 1980 Holevo: 右対数微分に基づく多パラメータ版，量子Cramer-Rao 不等式, Holevo 限界
- 1989? Nagaoka: 量子版の i.i.d. 条件の導入
- 2000以後，Hayashi-Matsumoto, Guta, Jencova, Kahn: 量子版の i.i.d. 条件下で，Holevo限界が漸近的推定限界となる（漸近的ガウス性）

量子通信路符号化理論

- 通信路符号化の量子版
- 通信路符号化とは.
  - 通信路が確率遷移行列で与えられるときに，誤り確率がほぼ0になる状況において，通信速度が大きくなるように符号化を選ぶ.
  - 理論的な速度限界は通信路容量とよばれ，相互情報量の最大値 $\max_p I_p(X:Y)$ で与えられる.（Shannonの通信路符号化定理）
  - 速度 $I_p(X:Y)$ は通信路の形に依存せずに達成する符号(ユニバーサル符号)が存在する. (Csiszar-Korner)
  - 昔は（CDなどは）代数的な符号の構成法が主流.
  - 最近では，LDPC符号が主流 IEEE802(無線LAN)

量子通信路符号化理論

- 通信路符号化の量子版は一意には問題が定まらない.（→複数の量子版）
- 量子通信路を用いて古典情報を送る設定
  - 1960年代後半から，1970年代後半にかけて盛んに研究された. Holevo により，上限が得られる(Holevo限界)
  - 1998(1996) Holevo, 1997 Schumacher&Westmoreland: Holevo限界が達成可能であることが示される.
  - 2009 Hayashi: ユニバーサル符号
- 量子通信路を用いて量子情報を送る.
  - 量子誤り訂正とのよばれる.
  - 代数的にはスタビライザー符号という符号で構成される.
  - 漸近理論は，Shor, Devetak によって得られる.

量子情報源符号化理論

- 情報源符号化の量子版
- 情報源符号化とは.
  - データ圧縮の理論
  - 理論的な圧縮限界はShannonエントロピーで与えられる.（Shannon の情報源符号化定理）
  - 情報源が独立同一性を満たす場合には情報源に依存せずに，Shannonエントロピーレートまで圧縮する符号 (ユニバーサル符号)が存在する. (Csiszar-Korner, Clark-Barron)
  - より一般の情報源に対しては，Lempel-Ziv符号が有効

量子情報源符号化理論

- 微小な歪みを許す設定と許さない設定との間に，決定的な差がある.（→複数の量子版）
- 微小な歪みを許さない設定
  - 情報源にコヒーレンスがある場合には，圧縮することは不可能.（Koashi-Imoto）
- 微小な歪みを許す設定
  - von-Neumann エントロピーが圧縮限界となる.
  - ユニバーサル符号が存在(Josza-Horodecki^3, Hayashi-Matsumoto, Hayashi)

エンタングルメント理論

- もともとは，量子論の基礎付けからスタート
- 漸近理論は，情報理論と深い関係
- 混合状態のエンタングルメント基準は複数あるがどの議論においても情報理論的手法が有効
- 混合状態のエンタングルメント蒸留は，量子状態を伝送する量子通信路符号化と深い関係

量子暗号

- 複数ある量子情報処理技術の中で最も実用化に近い.
- 他の技術と比べ，必要となるデバイス技術が簡単
- 到達距離に問題があるものの，短距離の通信に関しては，現時点で必要な要素技術がほぼ揃っている
- これらの要素技術の集積化が課題となっている.
- 安全性を保証する理論研究についても改善の余地がある.

数学の応用分野の中では数学のレベルが高い

- 普遍的分野である線形代数に立脚した量子論的非可換性のため，数学のレベルが高い
- 既存の数理科学の応用分野では，応用面に重点が置かれ，数学的技巧の修練がおろそかにされている.
- 量子情報では数学的記法の洗練がなされた.
- エンタングルメント分野で解決された問題が他の分野で未解決問題であった

（2例：Rank-one approximation, Tensor rank）.

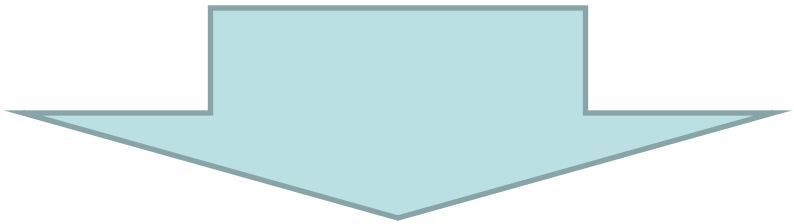
- 相対的に高いインパクトファクター（分野内での世界的なネットワークの強さ. 分野のポテンシャルの高さ）

他分野に比べ，理論分野の細分化が進んでいない

- 生命分野では，細分化が進み，数理的基礎の研究を行う研究者が直接，実験や開発レベルの研究を行うことはまれ.
- 他分野では，基礎的な数理と開発レベルの研究の双方を行うことはまれ.
- 数理的基礎に重点を置いた応用研究では，道具となる数学をあらかじめ決定してから進めることが普通である.
- 量子情報は数理的にはsolution-oriented.

世代間のギャップ

- 30代後半から40代前半の世代に研究者が集中（日本国内）.
- それより若い世代はブーム以前の状況を知らない.
- 30代後半から40代前半の世代の成果が院生の世代に伝わっていない.



ウィンタースクールの開催