計算機数理科学専攻
情報数理モデル講座

量子情報グループ

小澤正直（教授），西村治道（准教授），Francesco Buscemi（特任准教授）
岡村和弥（特任助教），Michele Dall’Arno（PD），Alok K. Pan（PD）

INFORMATION SCIENCE
NAGOYA UNIVERSITY
計算機数理科学専攻

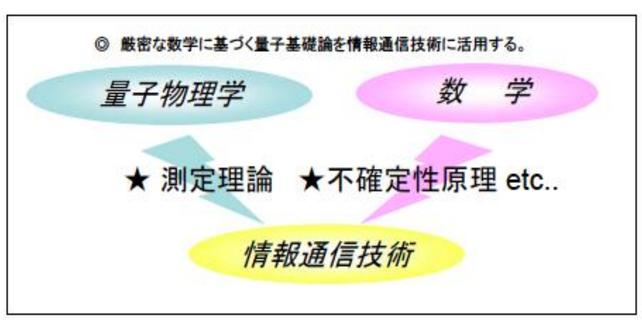
概要

小澤グループでは，自然科学として情報の研究を行っています．「情報」の自然法則を解明し，新しい技術「量子情報技術」として社会への応用を目指しています．

すべての情報は，ある物理的媒体の性質によって表現され，それは，不確定性原理の支配する量子力学の法則に従います．不確定性原理の利用によって，これまでのコンピュータの概念を変える超高速コンピュータ，「量子コンピュータ」を実現する可能性が開かれました．量子コンピュータは現在使われている暗号を解読してしまう計算能力があります．しかし，今度は，不確定性原理の利用によって，無条件に安全なことが証明される量子暗号を実現する可能性が開かれました．小規模な，量子暗号装置は既に市販されています．

量子コンピュータや量子暗号は，量子情報の基礎理論から生まれました．量子情報の研究には，量子測定，量子計算，量子通信といった重要課題があります．量子測定は，対象から情報を取り出す過程の研究で，これは量子的対象の認識論にあたります．量子計算は，量子的媒体を利用した情報処理の過程の研究で，量子コンピュータの技術開発に応用されます．量子通信は，量子的媒体を利用した情報伝送の過程の研究で，量子暗号の技術開発に応用されます．

小澤グループでは，量子物理学の法則に基づいて，これらの量子情報の研究を推進しています．特に，これらの量子情報プロセスの数理モデルを厳密に扱う数学的方法を開発して，世界をリードする成果を上げています．



量子通信

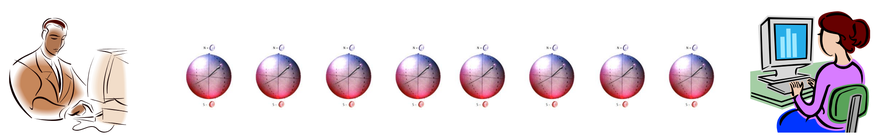
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left\{|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle\right\}$$

情報伝送の過程（量子暗号に応用）

量子通信理論は，従来の0,1で表現される情報（古典情報）を量子通信路，すなわち量子状態を用いて伝送することで，より効率的に通信できるか，さらに通信路に雑音がある場合にうまく通信できるかなど，通信理論を量子論の枠組みで評価します．

1940年代にShannonによって古典的電磁場を媒体とする通信の通信路容量が明らかにされました．しかし，1960年初頭のレーザーの発見に伴い，Gordon等によって量子的電磁場の法則から新しい量子通信路容量の公式が提案されましたが，その証明は未解決問題として残されました．小澤教授は1993年にYuenとの共著論文でこの問題を解決し，電磁場の量子通信路容量の研究の先駆けとなりました．近年の小澤グループの研究では，Shannonの理論を現実的な量子通信路（多くのノイズを含む上，限られた回数しか使用できないような量子通信路）に一般化することを試みています．このような研究はワンショット量子情報理論と呼ばれています．最近の成果として，量子通信路の量子通信容量をワンショットの設定で特徴づけることに成功しました．この成果は，実用的な量子通信ネットワークの詳細な評価を行う新たな方策を切り開くものです．

量子通信理論は量子暗号において重要な役割を果たします．代表的な量子暗号として知られているのが1984年に提案されたBennettとBrassardによる量子鍵配送です．これは，秘密に情報を共有するためにその秘密情報を量子状態に符号化して送り，不確定性原理の利用によってその情報を盗聴を検出するという暗号プロトコルで，最も実用に近いとされる量子情報技術です．小澤グループでは，量子鍵配送を始めとした量子暗号に小澤の不等式を適用することで，すぐれた性能を持つ量子暗号方式の可能性を究明しています．



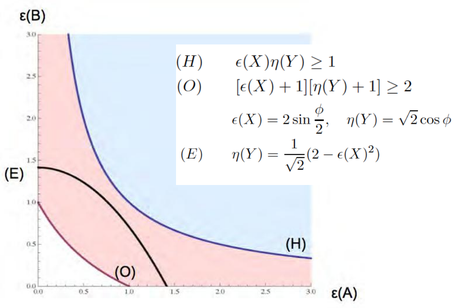
量子測定

対象から情報を取り出す過程（量子の認識論）

量子測定理論は，量子情報の研究すべての分野の基礎を担う理論です．量子測定の概念を数学的に特徴づける問題は，1932年に発表されたvon Neumannの研究以来の課題とされてきました．小澤教授は，1984年の論文で，量子測定の概念が作用素環上の完全正値写像値測度（インストルメント）によって完全に数学的に特徴づけられることを示して，量子測定理論の基礎を確立しました．1988年にはインストルメントの理論に基づいて，重力波検出限界に関するYuen-Caves論争を解析し，標準量子限界を打破する測定のモデルを構築して論争を解決しました．この研究で，1927年にHeisenbergが提唱した測定誤差と擾乱に関する不等式の不備が明らかになり，2003年に普遍的な関係を表現した不等式（**小澤の不等式**）を発表しました．小澤の不等式は2012年にウィーン工科大学の長谷川准教授のグループにより，中性子を用いて検証実験が行われました．その結果，Heisenbergの不等式には破れが生じる一方で小澤の不等式は成立することが検証されました．さらに2013年，東北大学の枝松教授のグループによる量子情報技術の実装に有望な光子を用いた実験でも，小澤の不等式の正しさは検証されています．現在，小澤グループでは，上記の小澤教授の成果に基づいて，測定理論や量子情報理論への応用を模索しています．

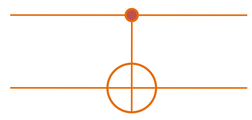
$$(\mathrm{H}) \quad \epsilon(A)\epsilon(B) \geq \frac{1}{2}|\langle [A,B] \rangle| \quad \text{Heisenbergの不等式}$$

$\epsilon(A), \epsilon(B)$：物理量 A, B の測定誤差
$\sigma(A), \sigma(B)$：物理量 A, B の標準偏差
$|\langle [A,B] \rangle|$：物理量 A, B の非可換性係数



$$(\mathrm{O}) \quad \epsilon(A)\sigma(B) + \sigma(A)\epsilon(B) + \epsilon(A)\epsilon(B) \geq \frac{1}{2}|\langle [A,B] \rangle| \quad \text{小澤の不等式}$$

量子計算

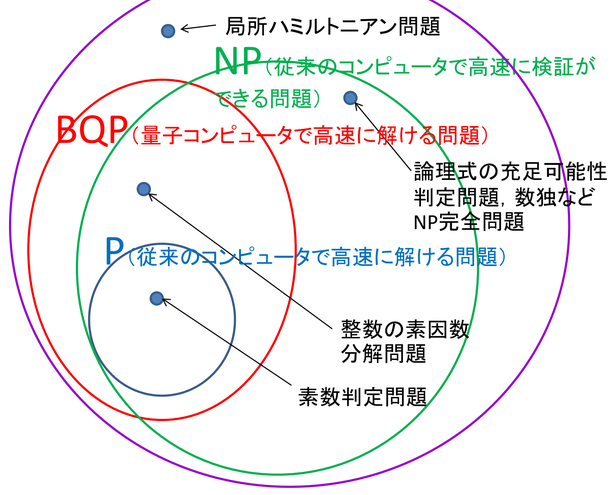


情報処理の過程（量子コンピュータに応用）

量子計算理論は，量子コンピュータの計算能力とその限界を明らかにするための理論です．1994年に発表されたShorの量子アルゴリズムは，従来のコンピュータで高速に解けないとされていた整数の素因数分解を，量子コンピュータにより高速に行うことができるというものでした．整数の素因数分解の困難性は，現在インターネットで標準的に用いられているRSA暗号が拠りどころとしているものであったため，量子計算理論はShorの発見以後，急速に盛んになりました．Shorの発見後20年を経ようとしている現在も，新しい量子アルゴリズムの開発や，逆に量子コンピュータの限界を探究することで，量子コンピュータでさえ高速に解読できない暗号システムの構築などが活発に研究されています．

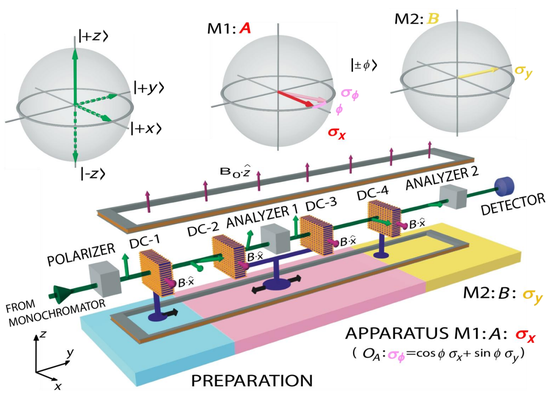
小澤グループでは，量子計算の生みの親Deutschが提唱した量子コンピュータの数学的モデルである量子Turing機械と量子回路の計算量的同等性について，どの程度の精度で成り立つかを厳密な形で追究するなど，量子コンピュータの計算理論に関する数学的基盤を構築しました．また，最近では既存と異なるタイプの高速化を達成する量子アルゴリズムを京都大学の岩間教授のグループと共同で開発したり，量子コンピュータで高速に検証できる問題のクラス構造を探究するなど，量子コンピュータでできること，できないことを計算機科学，物理，数学の多方面の角度から研究しています．

量子コンピュータの計算能力

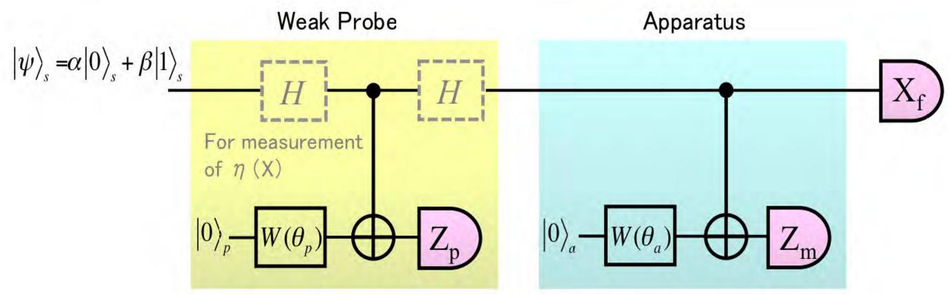


小澤の不等式検証実験


物理の根幹 新たな数式
不確定性原理 名大教授の予測、実証
朝日新聞2012年1月16日朝刊一面



中性子を用いた小澤の不等式の検証実験装置
J. Erhart, S. Sponar, G. Sulyok, G. Badurek, M. Ozawa, Y. Hasegawa, Nature Physics (2012)



光子と偏光を用いた小澤の不等式の検証実験装置を表わす量子回路
S.-Y. Barek, M. Ozawa, K. Kaneda, K. Edamatsu, Scientific Report (2013)


物理の基本 不確定性原理に「欠陥」
新理論 光使い検証
東北大など
日本経済新聞2013年7月18日朝刊