東北大学 大学院情報科学研究科 数学教室

情報基礎数理学 III

小澤正直（教授）

木村元（学振特別研究員 PD）
天野博邦，吉村直樹（修士課程２年）
松本悠，三木繁彰　（修士課程１年）

小澤研究室では，量子情報および量子力学の基礎に関する問題を中心に情報数理と理論物理学の研究を行っています．原子や素粒子が活躍するミクロな世界では，私たちの日常的な感覚では想像もつかないような不思議な現象が絶えず起こっています．２０世紀の人類は，このような現象に内在する規則性を追及し，現在量子論として知られる深遠な数理に支配された基礎法則を明らかにしてきました．２１世紀を迎えた今，我々の研究室では厳密な数学を武器に，量子の世界にさらなるメスをいれ，基礎物理学へのさらなる貢献，また応用面としても，今後，発展が期待される量子情報技術への理論的寄与を目的とし，日々研究活動を進めております．

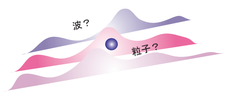
量子論とは？

自然界は我々が考えているよりもずっと巧妙にできており、数学に支配された法則が確かに存在しています。全ての物質は原子、さらにはミクロな素粒子で構成されているのは聞いたことがあるでしょう。１mmの百万分の１よりももっと小さな世界を舞台とし、その極微な世界で展開される現象をつかさどるのが量子論の法則です。このミクロな世界では、我々の想像を超える数多くの現象が起きています。例えば、原子は粒子として振る舞い、また同時に波としても振る舞います。このような振る舞いは、あまりにも直観からかけ離れているため、究極的には物の存在のあり方すら問われているのです。

量子力学小史

電子や原子の従う新しい力学の発見
行列力学(Heisenberg, 1925)
波動力学(Schroedinger, 1926)
その後スピン等様々な自由度、電磁場など
様々な物理の対象まで一般化される。
朝永振一郎ら電磁場の量子力学の
建設でノーベル賞を受賞(1965)

ふたをした箱にサイコロが入っています。ふたを開けて中を見る（観測する）と、「１」の目が出ていました。
さてあなたは、ふたを開ける前からサイコロの目が「1」であったと考えますか？



量子論によると、あなたがふたを空けてサイコロの目を確認する以前のことをあれこれいうことはできません。あえて言うならば、サイコロは「１」から「６」までの全ての目が同時に重ね合わさった状態にあるのです。（この例は、あくまでもミクロな世界のたとえ話ですが、我々の大きさくらいのマクロなスケールでも、全てはミクロな原子の寄せ集めであることを忘れてはいけません。）

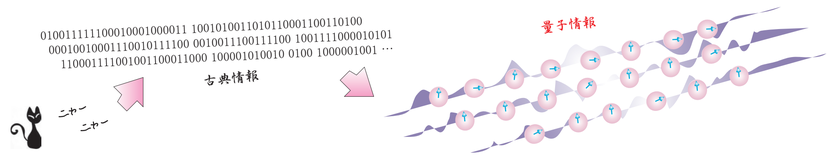
科学的な意味においては、「存在」は「観測」によって確認される必要があります。ある有名な物理学者は、「観測なしで存在を問うことは、針の先に何人天使が座れるかを議論するようなものだ」とまで言っています。この他にも、ミクロな世界ではたくさんの非日常的な現象が数多く起きており、我々物理学者の頭を常に悩ましてきたのです。２０世紀を通じて物理学者たちは、量子論の法則を難しい数学で記述し、不思議な現象を説明したり予言したりすることができるようになってきましたが、現在でも世界中の物理学者の中（アインシュタイン！も含む）で量子論を”理解している”と言い切れる人は一人もいないのです。このように直観がまったく働かない世界を研究するには、厳密で信頼性を持つ数学がもっとも重要となります。

あなたもぜひこの不思議で深遠な世界に飛び込み、チャレンジしてみませんか？

量子情報理論とは？

現在の情報化社会において、皆さんは「情報」と聞いてどのようなイメージを思い浮かべますか？　コンピュータやテレビから発せられる情報から構築される世界は、実在する世界なのでしょうか？さて、我々の世界は全て量子論などの物理法則で支配されています。ですから、「情報」そのものも究極的には物質に付随した概念なのです。例えば現在のコンピュータの基本となるデジタル情報「０」と「１」は、簡単にいうと電気信号が流れるか流れないか、という物理現象と対応しています。
左の解説では、量子論は微視的な世界が支配するとても不思議な法則であると説明しましたが、近年我々はこの不思議さを情報資源として活用し、従来考えることのできなかった夢のような情報通信技術を展開することができることがわかってきました。

今までの量子論の探索は、いわば自然界がどのように創られているのかを追求してきましたが、これからはその不思議な現象が持つ可能性を明らかにすることも課題となっています。これが現在最も注目を集める一分野であり、なおますますの発展を続ける量子情報理論と呼ばれる一大パラダイムです。すなわち量子物理学を土台として、情報を微視的な世界に乗せ、情報資源一般の可能性を探る研究分野なのです。



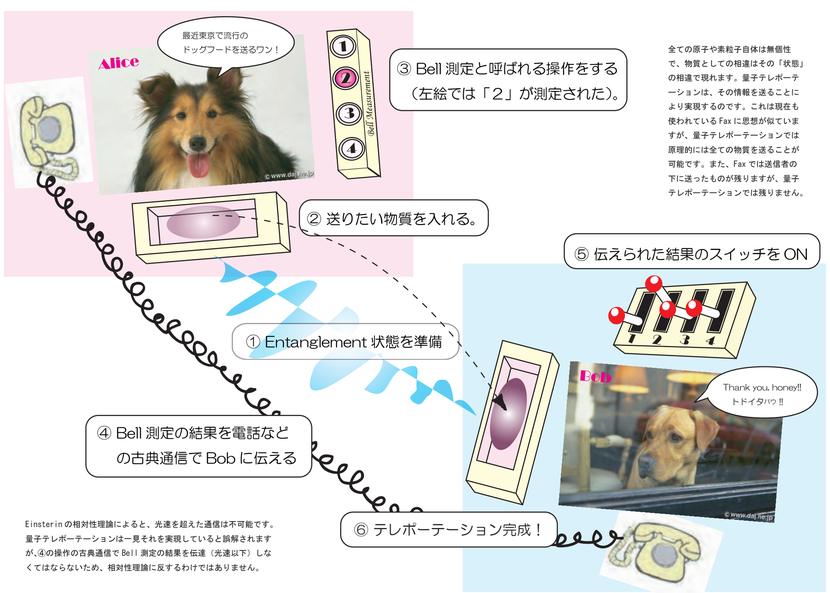
量子論の法則をたくみに利用すると、下に紹介するような、従来のコンピュータをはるかに越える性能を持つ量子コンピュータや、SF の世界でしかあり得なかったようなテレポーテーションなどの技術が現実に可能となります。

量子情報理論がもたらす夢の技術たち！

量子テレポーテーション

テレポーテーションなど書いたら SF の話でトンデモ科学と思われてしまうかもしれませんが，れっきとした物理学です。つまり、自然界の法則（量子論）を利用することで、実現可能な技術であることがわかりました。それが、1993 年に IBM の Bennett らにより発見された「量子テレポーテーション」です。これによると、何キロも離れた場所に物質をテレポートすることが可能となります。現在ではミクロな光子（光の粒）のテレポーテーションが実験で確認されています。ゆくゆくは、大きな物質も簡単にテレポーテーションすることが可能になるかもしれません。

ただし、東京とニューヨーク間に事前に Entanglement と呼ばれる絡み合いを事前に用意しておく必要がある。その絡み合いに送りたい物質の情報を付与することで、テレポーテーションが可能となる！！

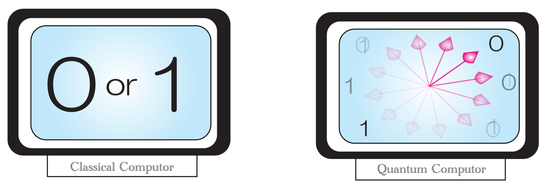


全ての原子や素粒子自体は無個性で、物質としての相違はその「状態」の相違で現れます。量子テレポーテーションは、その情報を送ることにより実現するのです。これは現在も使われている Fax に思想が似ていますが、量子テレポーテーションでは原理的には全ての物質を送ることが可能です。また、Fax では送信者の下に送ったものが残りますが、量子テレポーテーションでは残りません。

Einsterin の相対性理論によると、光速を超えた通信は不可能です。量子テレポーテーションは一見それを実現していると誤解されますが、④の操作の古典通信で Bell 測定の結果を伝達（光速以下）しなくてはならないため、相対性理論に反するわけではありません。

量子コンピュータ

現代社会においてコンピュータの恩恵を受けていない人はほとんどいないのではないでしょうか．人間には不可能な大量情報処理を瞬時に行い，計算だけでなく，インターネットや日常の情報管理にまで幅広く応用されており，その重要性は今後ますます高まることでしょう．量子コンピュータは，量子論の奇妙な性質を応用することで，現在のコンピュータの性能をはるかに上回る超高速コンピュータを実現します．例えば現在の最速スーパーコンピュータで数千年かかる計算を数十秒でこなすことが出来るようになるのです．



量子ビットと呼ばれている０と１との重ね合わせ状態をビットを複数利用する！！

量子コンピュータが実現されると…

① 超高速素因数分解による暗号解読

現在，Ｗｅｂ上の暗号として広く使われているＲＳＡ暗号と呼ばれるものがありますが，その安全性は素因数分解の困難性に基づいています．（人間はおろか，現在の高速コンピュータでも，３００桁程度の数の素因数分解を行うには莫大な時間がかかります．）量子コンピュータはこの素因数分解をはるかに高速に計算（多項式時間）可能であり，そのアルゴリズムはＳｈｏｒのアルゴリズムとして知られています．つまり，量子コンピュータが実現されると，高速計算ができる恩恵と同時に，（ＲＳＡ）暗号解読ができてしまうというマイナス？面もあります…（右の量子暗号を参照）．

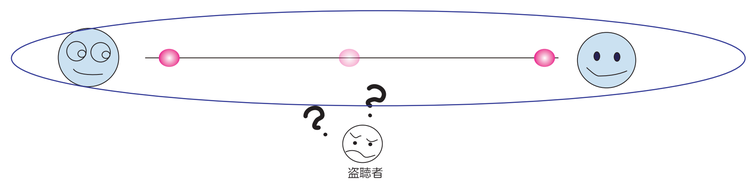
② 超高速ファイル検索

従来のコンピュータでは，n 個のファイルの中から１個のファイルを検索するのに必要なステップ数はおよそ n/2 ステップが必要でした．量子コンピュータは，ファイル検索にかかるステップ数を√n にまで落とすことができ，そのアルゴリズムはＧｒｏｖｅｒのアルゴリズムとして知られています．上述のＳｈｏｒのアルゴリズムほど画期的でないにしても，広い応用が期待されています．

量子コンピュータは，量子論を応用した原理的には実現可能な技術ですが，微視的な現象をコントロールする技術は難しく，いつ実現（実用化）されるかはまだまだわかりません．専門家によっても，今世紀中という人もいれば，５００年かかるという人もいます．現在多くの実験物理学者が，超伝導素子、非線形光学、レーザー冷却、量子ドット、核磁気共鳴などによる実現法を模索して研究を続けています．

量子暗号

現代の情報化社会では，情報を盗聴されることなく秘密に通信を行うことは，政府や企業のみならず個人のレベルでも大変重要な課題です．それを実現するのが「暗号」であり，すなわち第三者に漏れないように当事者間でのみ解読できるようにした特殊な記号や文字を利用します．暗号の歴史は古く，何千年も前から用いられていましたが，量子論の性質を利用すると，今の技術はおろか，今後どのような革新的技術が開発されたとしても，絶対に解読できない暗号が実現できます．それが量子暗号です．



量子暗号とは，別名量子鍵配送とも言われ，暗号を作るために正規のユーザのみが知れる鍵（ビット列）を量子の特性を利用して正規のユーザが共有します．万が一盗聴者がいて，鍵の情報を盗み取ろうすると，正規のユーザがそれを必ず検知できるのです！

左の量子コンピュータにて説明したように，現代のコンピュータでも解読が難しく（計算量的に）安全とされているＲＳＡ暗号は，量子コンピュータが実現されれば簡単に解読できるようになってしまいます．そのために，量子コンピュータはおろか，何を用いても盗聴ができない，量子暗号の重要性は大変大きいです．幸い？なことに，現在量子コンピュータの実現は技術的な困難により遅れていますが，量子暗号は実現化されており，既に製品化もされているくらいです．ただしその性能は，せいぜい２，３百キロメートル程度でしか用いることはできず，例えば日本とアメリカを量子暗号で結ぶことはできていません．

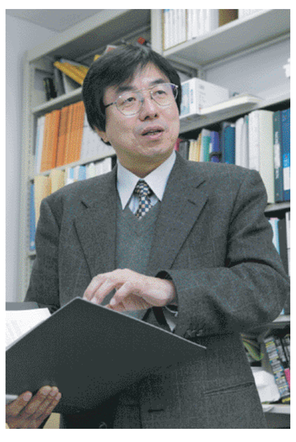
その他にも

ここに紹介したものは量子情報理論がもたらす技術革新の一例であり，他にも古典情報処理を超える大容量通信など数多くの応用が考えられます．最近ナノテクノロジーという言葉をよく耳にしますが，この微細加工技術の先に待っているのが上で紹介したような量子情報テクノロジーであり，恐らく今後「量子」という言葉を聞く機会が飛躍的に増えることになるかもしれません．ぜひ覚えておいてください！

小澤先生の研究紹介

物理学の常識に挑む数学者

ハイゼンベルクの不確定性原理は打ち破れる
そんな衝撃的な主張で物理学者の度肝を抜いた
数学者の小澤正直は数学理論という武器を使って
物理学の常識を問い続ける



小澤正直（おざわ まさなお）

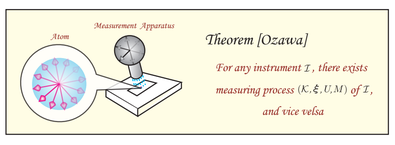
東北大学大学院情報科学研究科教授

- 現代物理学の常識とされるハイゼンベルクの不確定性原理を書き直し，新たな定式化を提唱した。
- 仕事時間の大半は紙と鉛筆で計算している。「数学は，見えないところにあるはずのものを探す可能性の科学。探していた式が見つかった時は嬉しいですね」。
- バッハの音楽が好き。複数の旋律が重なり合いながら展開していく構造的な面白さに惹かれるという。

日経サイエンス 2004 年 9 月号より抜粋

①　量子測定理論及び量子力学の解釈問題の研究

量子測定の概念を数理物理学的に特徴づける量子オペレーション測度（完全正写像値測度）の一般理論とそれに基づく量子確率論を確立し、その理論を応用して、重力波検出限界に関するYuen-Caves 論争を解決した．



Theorem [Ozawa : Uncertainty Relation]

$$\Delta q \cdot \sigma_p + \Delta p \cdot \sigma_q + \Delta p \cdot \Delta q \geq \frac{\hbar}{2}$$

called Ozawa' s Inequality

Δq : *Noise of Position*
Δp : *Disturbance of Momentum*
σ_q : *Standard Deviation of Position*
σ_p : *Standard Deviation of Momentum*

また，測定誤差と擾乱の一般理論を構築し、Heisenberg の不確定性原理を打破する測定装置のモデルを示し、新たに測定誤差と擾乱に関する普遍的不確定性原理を確立。現在小澤の不等式として知られている。これらの成果に基づいて、測定理論と量子力学の解釈問題を研究している。

②　量子計算量理論の研究及び量子計算の基礎物理学的研究

量子計算機のアルゴリズム的性能限界を究明する目的で、量子 Turing 機械と一様量子回路族の計算量理論の基礎を確立した。量子計算機の物理学的性能限界を究明する目的で、モデルによらない誤差解析法を開発し、量子論理素子の精度について、保存法則から導かれる標準量子限界を導いた。これらの成果に基づいて、量子計算の実現可能性及び限界性能の研究を行っている。

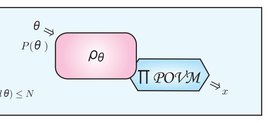
③　量子情報理論の研究

量子測定理論の成果を応用し、量子推定理論、量子情報理論の基礎を確立して、電磁場の究極的情報容量を導いた。これらの成果に基づいて、情報量、測定精度、擾乱、エンタングルメント、計算量の相互関係を研究している。

Theorem [Yuen, Ozawa]

$$I(\theta:x) \leq S(\rho) - \int S(\rho_\theta)\, P(d\theta) \quad \textit{(Holevo Bound)}$$

$$\Rightarrow \max I(\theta;x) = (N+1)log(N+1) - NlogN \quad \textit{under} \int \mathrm{Tr}[a^\dagger a\, \rho_\theta] P(d\theta) \leq N$$



④　超準解析学・量子集合論の研究

強制法と超準解析学を統一し、その作用素環論への応用を研究し、1952 年に提出された I 型環の構造に関する Kaplansky 予想を解決した。超有限 Heisenberg 群のユニタリ表現論を確立し、電磁場の位相作用素の問題の解決を導いた。これらの成果に基づいて、無限小解析学の基礎と数理物理学への応用を研究している。また，量子集合論の研究とその量子力学の解釈問題への応用への研究をしている。