～新しいコンピュータの可能性を探る～

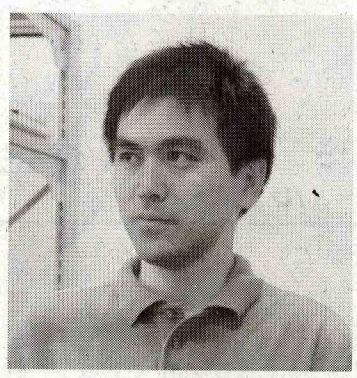
第2回 量子コンピュータ

今回は、量子力学の性質を利用した量子コンピュータと、その周辺の技術を取り上げる。量子テレポーテーションの技術研究をする古澤明助教授（工学系研究科）の協力で量子コンピュータの現状に迫るとともに、量子暗号の実用化へ向けて研究を進める今井浩教授（情報理工学系研究科）に話を聞いた。

（取材・構成　金丸洋輔、上梅裕史）

量子コンピュータの仕組み

不確定性原理を克服



古澤　明（ふるさわ　あきら）助教授
（工学系研究科）

●古典力学的コンピュータから量子力学的コンピュータへ

古典力学的コンピュータでは、多数の電子（電圧）により一つのビットの状態が0か1かで記述される。つまり、電圧が0の位置にあるか1の位置にあるかでビットの状態が決定されるのだ。古典力学的コンピュータは、この0と1の状態を切り替えることで計算を行っている。

LSIでは多数のトランジスタが0と1との状態の切り替えを行っており、現在は約1000個の電子で一つのトランジスタを制御している。LSIの性能が上昇すると、より少ない数の電子でトランジスタを制御できる。2年でLSIの性能が2倍になるというムーアの法則に従えば、2020年には一つのトランジスタを一個以下の電子で制御することになるという。トランジスタを制御する電子数が少なくなってくると、電子の振る舞いはニュートン力学ではなく量子力学により記述される。つまり、コンピュータの高性能化が進むと必然的にニュートン力学的な制御の限界に達し、量子力学的な制御を受けるようになるのだ。

●量子エンタングルメント

量子力学の世界では古典力学の世界とは異なり、独立した振る舞いをしない二つの粒子が存在する。これらをEPRペアと呼ぶ。量子力学では、EPRペアと呼ぶ。量子力学では、EPRペアである二つの量子は互いに影響しあいながら存在しているのだ。これら二つの量子の振る舞いは二つの波動関数の積で表すことができず、一方の量子の性質が決まるともう一方の性質も決定される。例えば、一方の電子のスピンがプラスなら、もう一方の電子のスピンは必ずマイナスになる。

このように、二つの量子が表裏一体の性質を持っていることをEPR相関と呼ぶが、より一般的に複数の量子間でこのような相関が存在することを量子エンタングルメント（量子もつれ）と呼ぶ。この量子エンタングルメントが量子コンピュータの根幹なのだ。

●量子テレポーテーション

ハイゼンベルグの不確定性原理によると、量子の運動量と量子の位置を同時に知ることはできない。観測により片方を知ることはできても、観測した瞬間に量子状態が壊れてしまい、もう片方を知ることはできなくなるからだ。

ところが量子テレポーテーションでは、全ての情報を量子から量子に移送することができる。まず送信者は、受信者にEPRペアBとCを渡しておく。ここで、BとCは量子力学的に表裏の関係にある。そして、送信者は送信したい量子Aに対して、新たに量子BとEPR相関をつくる。もちろん、AとBも量子力学的に表裏の関係となる。この操作の後、測定を行うため、量子AとBは壊れてなくなってしまうが、BとCのEPR相関を通して量子Aの情報は量子Cに伝わる。

超並列処理で高速化

●量子コンピュータの仕組み

量子コンピュータが、量子コンピュータに高い並列性を与えている。

古典力学的コンピュータでは、入力されたそれぞれの信号に対してのみ並列処理を行っていた。しかし量子力学的コンピュータでは、重ね合わせられた波動関数で記述される全ての状態において並列なのだ。つまり、量子力学的並列は古典力学的並列よりも次元が高く、そのため量子力学的コンピュータの計算処理速度は極めて速い。

●量子コンピュータの問題点

「いくら計算速度が速くても、計算結果が取り出せなければ意味がありません。量子力学では測定により量子状態が壊れてしまいますから、うまく情報を取り出すためのアルゴリズムが必要なのです」と古澤助教授は話す。つまり、量子力学的コンピュータで問題を解くためには、問題ごとにアルゴリズムを構築する必要があるわけだ。

また、量子状態は壊れやすいため、量子が欠損して情報が伝わらなくなる可能性がある。これには、多数の量子に同じ情報を担わせることで、欠損をカバーする方法が考えられている。

「情報伝達に用いる量子の数を多くすると、それだけ多くのリソースを食います。計算速度の速いコンピュータでも、その分リソースを食うようなら意味がありません。結局は、量子力学的コンピュータと古典力学的コンピュータのどちらが同じリソースのもとで速いかという比較になるでしょう」

●量子コンピュータの将来性

量子コンピュータの活躍が期待されているのはセキュリティの分野だ。量子コンピュータは、情報化社会の安全を図るのに重要な役割を担うと考えられている。素因数分解のアルゴリズムは既に考え出されており、これを用いれば現在の暗号技術は無力化してしまうという。現在の暗号技術は、古典的アルゴリズムでは解くのに極めて時間が掛かる素因数分解により情報の安全性を保っているが、量子コンピュータならば素因数分解を短時間のうちに行うことができるからだ。

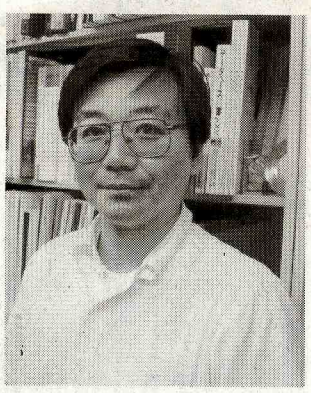
しかし、高度な計算が可能な量子コンピュータの実現にはまだ遠いという。「2量子間の量子テレポーテーションは成功しました。これから3量子間の量子テレポーテーションの実験を試みようとしているところです」と古澤助教授は話す。

量子コンピュータの実現には、多数の量子の間で量子エンタングルメントをつくらなければならない。現在はまだ、数量子間の量子エンタングルメントをつくっている段階なのだ。

「10量子ビット程度の量子コンピュータでも、量子テレポーテーションによってネットワーキングすれば擬似的に大きなコンピュータになります。しかし、それが可能になるのは10年以上後でしょう。現在はまだ量子コンピュータの黎明期なので、実用機が実現した場合、社会にどのようなインパクトを与えるかはわかりませんね」

量子暗号の理論

究極の安全性を保証



今井　浩（いまい　ひろし）教授
（情報理工学系研究科）

○なぜ量子暗号か

現在インターネット上での商取引などに利用されている暗号は、極めて難解な素因数分解を用いた公開鍵暗号である。この暗号システムでは、今の古典力学的コンピュータでは到底処理は解くのにヒトの一生がかかってしまうほどの素因数分解も短時間で処理することができるからだ。そこで、究極の安全性を保証するセキュリティ技術として量子暗号が注目されている。

「現在のコンピュータのデバイス技術は、間もなくナノメートル単位の技術に深化するでしょう。すると、量子力学の影響が出てきて、古典力学が通用しなくなる。古典力学コンピュータは、発展に限界があるのです。量子の問題は乗り越えなければならない壁ですが、発想を転換すると究極の安全性を持つ暗号の素材でもあります」。今井浩教授はこう話している。

○量子暗号の仕組み

量子暗号の「究極」の安全性とはすなわち、盗聴者の存在を検知することができ、また、盗聴者が通信内容を盗み見ることができないということである。では、なぜこのようなことが絶対に可能なのだろうか。

量子は、粒子と波の性質を併せ持つ。量子暗号では、量子の中では最も安定している光子の、波としての性質を利用している。一例を挙げれば、ある量子が縦波であれば（偏光が縦であれば）1、横波であれば（偏光が横であれば）0の情報を持つと分かっているとき、受信者は十字型の受信器を用いることで100％正しく受信できる。

また、光子は波なので、偏光が傾いた状態も検出できる。量子力学の基本的性質より、45度（135度）傾いた偏光を、＋型の受信器が縦と受信する確率、横と受信する確率はどちらも50％である（この場合、×型の受信機ならば100％正しく受信できる）。

従って、発信者と受信者が伝達方法について予め決め事をしておけば、受信者は100％正しく受信できる一方、受信器の形がわからない盗聴者は、傍受しても0か1か正しく受信する確率は50％なので、盗聴は完全に不可能となる。なぜなら、情報は0と1の並びで表現されるため、その並びを多くすれば盗聴できる確率は指数関数的に小さくなるからだ。例えば、僅か20個の光子で情報を送っても、盗聴者が20個の0と1の並びを全て当てられる確率はたった100万分の1である。

加えて、光子の状態は測定されると必ず変化するので、傍受されたときも常にその検知が可能となる。量子暗号は、古典力学的コンピュータの暗号の弱点をすべて克服しているのだ。

○実用化に向けて

一つの光子が1ビットの情報を伝送する量子暗号では、特に長距離通信では微弱な光子でも検出できる受信器が必要となる。一方、光子がない状態でも受信器が誤って光子を認識してしまっては困る。従来技術は、この問題に受信器の検出効率を高めることで対処してきたが、限界があった。そんな中、今井教授らは二つの受信器を併用することで誤差を少なくし、実用的な条件下で従来技術の約3倍にあたる130kmの伝送距離を実現したのだ。このシステムであれば大都市圏をカバーでき、量子暗号の実用化へ大きく前進したといえる。

だが、量子暗号による通信が全世界的に行われるためには、まだまだ課題も多い。「更に通信距離を伸ばすためには、壊れやすい光子を同状態で保存する技術などが必要になりますが、これらはまだ実現が難しい。今は、デバイス研究などの比較的地道な研究しかできませんが、この研究が量子コンピュータの実現に繋がり、今のITを乗り越える量子情報技術の世界を実現するでしょう」