物理学

量子コンピューターとは何か

Quantum computing

EMANUEL KNILL 2010年1月28日号 Vol. 463 (441-443)

量子力学を利用したコンピューターの開発レースが続いている。

こうしたマシンは、かつては手に負えないと思われていた物理学、数学、暗号の問題を解決し、情報技術に革命を起こし、物理学の基本を明らかにする可能性がある。

その日が来るのは、いつだろう？

量子コンピューターとは何か？

それは、伝統的なコンピューターでありながら、量子情報にアクセスし、これを利用できるマシンのことだ。古典的、つまりこれまでのコンピューターでは、情報は0か1の値をとる「ビット」の列として表現されてきた。しかし、量子情報処理では、「キュービット」（量子ビット）を使って表現される。1つのキュービットとは、「0と1という値に対応する2つの区別可能な量子状態をもった量子系」である。2値というところは古典系と同じだが、異なる点は、キュービットは量子系であるため、「重ね合わせの原理」が成り立つところだ。つまり、その状態は、2つの量子状態の任意の組み合わせ、すなわち「重ね合わせ」となる。したがって、一連のキュービット列もまた、そのビット列の量子状態の任意の重ね合わせになる。その結果どうなるか。量子干渉（量子力学的な干渉現象）を利用できるようになり、表現できる情報の種類が大幅に増えるのだ。

キュービットは何から作るのか？

最初に提案されたのは、光子（光の量子）を利用する方法だった。この方法では、1個の光子が偏光子を通り抜けるか抜けないかで、2つの区別可能な量子状態を得る。偏光子というのは、偏光サングラスと同じものと考えればよい。ほかにも

いろいろな方法でキュービットを作ることができる。例えば、原子トラップやイオントラップで捕らえた原子やイオンとか（図1）、超伝導回路内の電子の集合的な行動、つまりマクロな振る舞いなどだ。原子やイオンの場合なら、電子と原子核の異なる配置を2つの量子状態に対応させればよい。また超伝導回路の場合であれば、荷電している / していないといった系の荷電状態とか、超伝導電流の向き（例えば、時計回り / 反時計回り）を、2つの量子状態に対応させればよい。

量子情報はどのように操作するのか？

多数のキュービットの状態に対して、初期化、制御、測定という順番で物理的操作を実行する（10～11ページのBOX1を参照）。BOX1の例では、重ね合わせ・オラクル・干渉の3つが制御操作に当たる。これを実行する仕組みを「量子ゲート」とよぶが、いわば古典的な論理ゲートの量子版である。

量子コンピューターは、古典的コンピューターより速いのか？

ある種の問題は、量子コンピューターを使えばはるかに速く解くことができる。また、量子コンピューターは古典的コンピューターを拡張したものであるため、一般論としては、常に同等以上の速さにはなる。しかし、キュービットの操作にかか

るコストや、文書処理などの応用プログラム自体がもっている制限があり、何でもかんでもスピードアップの恩恵が得られるわけではない。

その可能性が最初に認識されたのはいつか？

20世紀後半から、量子系が実際の応用に使える可能性が認識され始めた。そもそも、古典的なコンピューターを使って量子現象をシミュレーションするのは難しい。しかし研究者は、量子系を直接操作すれば、この困難を回避できることに気が付いた。ここから「量子系を使って効率よく計算する」という量子コンピューティングのアイデアが生まれた。しかし当時はアカデミックな興味の対象にとどまっていた。

研究が本格化したきっかけは何か？

それは、1994年に、Peter Shor が大きい数を非常に効率よく因数分解できる量子アルゴリズムを開発したことだった。その背景にあったのは、計算理論における「神託（オラクル）問題」だ。これは、内部機構を知ることができない「ブラックボックス」が付随した複雑な問題で、それを量子コンピューターで解決する例がいくつも発表され、方法もしだいに洗練されていった。こうした中で Shor のアルゴリズムが発表されたが、彼のアルゴリズムは、インターネットを利用した

図 1. イオントラップ量子コンピューティング研究室の想像図。現在物理的に実現されているキュービット（量子ビット）は、すべて顕微鏡サイズである。実際は、超伝導回路、ナノスケールの半導体の島、固体中の不純物、分子の核、電磁力を利用してトラップされた原子やイオンなどの中に、閉じ込められている。しかし、閉じ込めを行うのに必要な装置は、全体としてはかなり大きくなる。ここに描かれているのは、2 個のトラップされたイオン（青い球）からなる「2 キュービット系」の実験装置。一連の拡大図が示しているように、トラッピングには、電極の配列、銅製の容器、ガラス製の真空槽などが必要である。この閉じ込め装置のほかに、キュービットにコードされた量子情報を操作する装置群も必要になる。具体的には、キュービットの状態の初期化・制御・測定をする装置で、そのために、レーザー、光学装置、系にパルス状の電磁場をかける電子装置がいる。そしてもちろん古典的なコンピューターと、これらを動かす科学者も必要になる（テーブル上の装置の構成は、D.Leibfried によるスケッチをもとにした）。

通信や売買に広く使用されている暗号を、簡単に解読できてしまうのだ。このインパクトが大きかった。こうして量子コンピューティングの強みが明確になり、それが本当に実現可能かどうか、検討する必要性が生じたのだ。

因数分解のほかに、どんな計算に向いているか？

量子アルゴリズムを利用すると劇的に速く解決できるのは、因数分解のように、問題の構造がよくわかっている数学問題だ。また、開発のきっかけの 1 つとなった量子現象のシミュレーションにおいて、指数関数的に高速化できるケースが見つまっている点は重要だ。これは任意の量子モデルを試す「バーチャル実験室」となるからである。また、最適化問題や

積分問題も、劇的というほどではないが、かなりの高速化が期待できる。さらに、異なるグループ間でやりとりされる情報量の削減に関する問題も、量子アルゴリズムを使うことで指数関数的に速く解決できることが理論的に立証されている。

それだけか？

まだまだたくさんある！ 既に私たちも持っている多くの基本的な量子アルゴリズムツールは、広く応用することができる。こうしたツールの探求は今も続いている。ただし、量子コンピューターを使ったほうが効率よく解決できる問題を、識別したり分類したりする方法はまだ知られていない。いずれにせよ、今の私たちには想像もできないような応用があるのは確実だ。

量子コンピューターを製作するには何が必要か？

キュービットを実現するには、2 つの区別可能な量子状態を保持できる物理媒体が必要だ。ここで、キュービットは十分に隔離されていなければならない。特に、キュービットの周囲の環境が、その量子状態を「感じる」ことができてはならない。さもないと、干渉を利用するのに必要とされるアナログな量子状態の振幅（10～11 ページの BOX1 を参照）の特性が不安定化し、デコヒーレンス（量子状態の喪失）が起きてしまうからである。デコヒーレンスは、通常の巨視的な世界では重ね合わせの効果が観測されない理由の 1 つになっている。その一方で、キュービットの状態を操作するためには、計算誤りやデコヒーレンスが起らないよう、きちんと制御された方法で隔離状態を破る必要がある。つまり、ほかのキュービットに影響を及ぼすことなく、個々のキュービットやキュービット対の状態にアクセスして、これらを変更できなければならない。この操作は、古典的なコンピューターで、1 つまたは 2 つのビットに回路素子を作用させるのと同じようなものである。

「量子もつれ」は必要ないのか？

量子もつれ（エンタングルメント）というのは、離れたところにある複数の量子系の間に生じる一種の結合状態のことである。これらが結びついている仕組みは、個々の系の状態の古典的な組み合わせでは説明できない。このことから想像できるように、量子もつれは、異なるグループ間や量子コンピューター間における「量子通信」の、重要なカギを握っている。例えば十分に純粋な量子もつれを利用すれば、離れたキュービットどうしを結びつけ、2 キュービットのゲートを作用させることもできる。量子コンピューティングでは、本来はキュービットどうしが離れている必要はない。しかし、いったん物理媒体中の個々のキュービットが特定されると、それらの間の量

子もつれを考えることができるのだ。多くの研究者が、まず、量子もつれの兆候を探し出そうとしている。しかしながら、量子もつれだけでは量子コンピューターは強力なものにならないことがわかっていてる。例えば、光子キュービットは量子もつれ状態になりやすいが、量子コンピューティングには利用しにくいことがわかっていてる。

量子状態の振幅のアナログ性が、問題を起こさないか？

先に答えをいえば「問題にならない」だ。しかし、その理由が解明されるまでには多くの研究を要した。もともと、ほとんどの研究者が、古典的なアナログ（デジタルではない）コンピューターの製作において遭遇する困難は、量子コンピューターの製作にも当てはまるだろうと感じていた。特に、コンピューターからの出力が望ましい答えに十分近くなるようにするためには、ゲートが増えるほ

ど、量子ゲートにはますます高い精度が要求されるようにみえた。コンピューターのゲートの基礎となる物理的相互作用は、連続的な範囲の値をとるパラメーターに依存するので、一般に、高い精度を直接達成するのは現実的でないと考えられる。これについては、「量子誤り訂正法」を用いることで、あまり多くの資源を必要とせず、任意の精度で量子コンピューティングをデジタル化できることが判明している。

量子誤り訂正法はうまく機能するのか？

量子誤り訂正法によって、物理的合理性をもった計算誤りやデコヒーレンス過程の影響については、すべて除去することができる。その前提となるのは、量子コンピューターを製作するための要件を十分に満たすことだ。また、特にキュービットの物理的操作は、十分正確に行われねばならない。ただし、量子誤り訂正法は、考えられるどんな誤りでも訂正できるわ

けではない。量子誤り訂正法の究極のテストは、「スケーラブル」なマシン、つまり、キュービット数とゲート数について、（コストを除いて）はっきりとした限界のない量子コンピューターを実際に製作してみせることだ。こうしたスケーラビリティの実現を阻む根本的な障害は知られていないので、もしそれができなかったとしたら、新しい物理学が誕生することになる。

キュービットの物理的操作には、どの程度の精度が必要か？

キュービットの状態の初期化・制御・測定に必要とされる精度は、多くの要素によって決まってくる。例えば、主にどのような誤りがあるか（古典的なコンピューティングよりはるかに多くの種類がある）、キュービットを保持している物理媒体にどのような制約が課せられているか、どの誤り訂正法を選択するか、といったことである。誤りを完全に訂正

BOX 1

a. 初期化 ここに示した計算では、2つのキュービットが必要である。キュービットは、スピン 1/2 の粒子（銅製の容器の中の青い球）として表す。粒子の量子状態（スピンの左回りであるか

右回りであるか）は、それぞれ 0 と 1 のビット値に対応している。図には示していない強い相互作用により、キュービットを初期化して左回りの状態（矢印）にしてから、銅製の容器中に隔離

してデコヒーレンス（量子状態の喪失）過程から保護する。2 キュービット状態は、00、01、10、11 という 4 つの可能な量子状態の波動関数と見なすことができる。それぞれの量子状態が波動

関数の振幅を与える。初期状態の振幅はすべて 00 という量子状態にある（赤い丸）。
b. 重ね合わせ 計算は、初期状態を「均一な重ね合わせ状態」に変化させる操作

する方法はいくつかあるが、いずれも多数のキュービットとゲートを追加する必要がある。ここで追加しなければならないキュービットとゲートの個数は、基本的な物理的操作の精度によって決まり、精度が限界まで低下していくにつれ、追加する個数は無限に増えていく。この限界は場合によって異なるものの、実用的なスケラビリティを達成するためには、量子ゲートを作用させること、つまり制御操作で誤りが生じる確率は、0.0001未満でなければならないとされている（誤りが生じる確率は、量子過程の精度の低さを大ざっぱに定量化する方法だ）。一方、キュービットの状態の初期化と測定のための要件はもっと緩やかであり、私自身は、こうした場合の誤りが生じる確率は0.01未満を目標とするのが妥当であろうと提案している。すべての基本的な物理的操作の誤り確率が数パーセントという高さであっても、スケラビリティは達成できるという示

唆もある。この基準が実用的であるかどうかは、現時点では不明である。

十分に高い精度の量子ゲートは実際に製作されたのか？

まだである。高精度の量子ゲートの製作は、量子コンピューティングに関する主な挑戦課題のうち、まだ達成できていないものの1つである。

十分な精度の量子ゲートが製作されていないのに、何ができるというのか？

既に、数キュービットの興味深い量子状態が作り出されている。また、ちょっとした量子コンピューティングや誤り訂正プロトコルを実行し、そのステップの挙動を調べる実験も行われている。長い計算に用いるには精度が足りないが、こうした実験は有用だ。中程度の質のキュービットを多数使った試みが提案され、実験的な取り組みも進んでいる。これによって、各種の超伝導を説明するモデル

など、さまざまな量子モデルについて、実際にシミュレーションや測定をしてみようというわけだ。

現在、いくつかのキュービットを使った量子コンピューティングまで実現しているのか？

イオントラップを利用する方法については、8キュービットまでの量子状態や量子過程が量子コンピューティングに使えることが、実験的に証明されている。しかし、既存の実験系は、せいぜいが、初期段階の量子レジスター（キュービットの集合体）でしかないと考えられる。利用できるキュービットの個数は固定されていて、しかも数が少ないからである。どんな装置を1キュービットレジスター、2キュービットレジスター、…、nキュービットレジスターとよぶのか、今のところ一般的な基準はない。私自身は、量子レジスターは次のような条件を満たしているべきだと考えている。第一に、ハードウェアを手動で再構成することなく、

から始まる。具体的な操作は、ここでは、レンズを通り抜けてきた光（赤）で粒子を照射することだ。これによってできた新しい波動関数は、それぞれの量子状態で同じ振幅をもっている。もしもこの状態を測定としたなら（まだやってはいけない）、個々の量子状態が観察される確率は、振幅の2乗になる（この場合は $0.5^2=0.25$ ）。なお、図の丸印の色と濃淡は、位相と振幅の大きさを表している（赤は正の位相、青は負の位相）。また、キュービットがいくつあっても波動関数を可視化することはできるが、量子状態の数は指数関

数的に大きくなるので膨大になる。

c. オラクル 次にブラックボックス（オラクル）を作用させて計算させる。ここで、ブラックボックスの振る舞いを予想するのは困難であり、実際に使ってみるしかない。このブラックボックスは、すべての量子状態が同時に関連する1つの状態に、いっぺんに作用する。つまり「量子並列計算」を利用していることになる（これは、古典的な並列計算とは全く別なものだ）。この場合、ブラックボックスの振る舞いとは、1つの量子状態の振幅の位相を変化させて、それに「印

を付ける」ことにほかならない。では、いったい、どの量子状態の位相の振幅を変化させたのだろうか？この時点で量子状態を測定しても何もわからない。なぜなら、測定結果の確率は振幅のみによって決まるからである。

d. 干渉 次に、干渉を利用して、印を付けた量子状態に振幅を集中させる。波動関数についていえば、干渉計に通したときのように、振幅を組み換えることになる。ここでその役割を担うのは、先ほどとは別の種類の光（青）である。

e. 測定 キュービットの状態は、系を隔離している容器を開けて、スピンの向きをチェックすることで測定される。ゼロでない振幅は1つだけなので、その結果は決定論的であり、印を付けられた位置が明らかになる。ここでの場合、印は10にある。

多くのアルゴリズムでは、ゼロでない振幅が多数あり、結果の測定は確率論的である。ここでの量子コンピューティングは、ブラックボックスを1回作用させるだけでよかった。これに相当する古典的コンピューティングなら、3回作用させる必要があった。

（著者）

任意の計算を行えること。第二に、小規模なレジスターよりも、巧妙に量子の特性を利用して、十分な精度で計算を行えること。第三に、レジスターの系のキュービットの個数を増やし、将来的にはスケーラビリティの達成をめざせそうな実際的な方法があること。この基準で考えるなら、1 キュービットのレジスターは既に実現しており、2 キュービットのレジスターが実現する日も近い。

量子コンピューティングの主要な技術にはどんなものがあるか？

核磁気共鳴 (分子の核スピンに関連したキュービット) や光の性質 (光子が運ぶキュービット) を利用して、多くの実験が行われている。現在の形式では、この2つの技術が、実用的なスケーラビリティの限界である約 10 キュービットに近づいている。また、スケーラビリティへの実用的な道筋がわかっている技術の中では、イオントラップのキュー

ビットを利用するものが現時点では最も進んでいる。数十キュービットからなる量子レジスターを最初に実現するのは、おそらくこの技術だろう。さらに、超伝導技術が、先行する技術にかなり迫っている。超伝導回路中では、キュービットの量子状態は多数の電子の集合的な振る舞いを利用するため、この技術がこんなに急速に進むとは私には想像できなかった。その他、いくつかのアプローチが研究されており、出番を待っている。遠くない将来、トラップされた多数の原子やイオンが、特殊な量子シミュレーションに使われるかもしれない。

長期的にはどの技術がいちばんよいか？

将来的には、古典的なゲートに近いもので、速度も同程度のキュービットが使えるようになるだろう。理想的には、古典的な計算の仕組みとほとんど変わらない形で、量子特性を発揮する基本素子ができ、それですべての計算を実行できると

よい。その実現に必要とされる技術は、まだわかっていない。

量子コンピューターの性能が古典的なコンピューターの性能を追い越すのはいつか？

多くの研究者は、量子コンピューターが^{ちやうちょ}実用化される時期を予測するのに躊躇する。私自身は、自分が生きているうちに、量子デバイスでおもしろい計算ができるだろうと考えているが、予期せぬ障害に遭遇しても失望することはないだろう。■

(翻訳：三枝小夜子)

Emanuel Knill、米国商務省国立標準技術研究所 (NIST) 数学計算科学部門。

さらに興味のある方へ
Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2001).
Preskill, J. *Quantum Computation* (lecture notes)
www.theory.caltech.edu/people/preskill/ph219/#lecture
Spec. Issue on Implementations of Quantum Computers
Fortsch. Phys. **48**, nos 9–11 (2000).
Nakahara, M. & Ohmi, T. *Quantum Computing: From Linear Algebra to Physical Realizations* (CRC Press, 2008).
Ladd, T. D. et al. Quantum computers *Nature*
doi:10.1038/nature08812 (in the press).