

量子コンピュータ研究の 現在と展望

根本香絵 (国立情報学研究所)

量子コンピュータとは

この数年、量子コンピュータの研究開発は世界的な盛り上がりを見せている。そんな中、そもそも「量子コンピュータ」とは何か、という質問もよく受ける。専門的な定義云々という話ではなく、ざっくりいって「量子コンピュータ」とは何か、その将来はどう見えているのか、その客観的で世界標準的な解説というものを、本稿では試みてみよう。

まず、量子コンピュータはまだコンピュータと呼ばれるほどのハードウェアができていないため、このことがいろいろな誤解を生んでいる。一番多いのは、「量子」を使っているのが量子コンピュータというものだが、これは大いに注意を要する。そもそも、私たちが毎日使っているコンピュータをはじめとして情報処理を担うハードウェアは、ほとんどが量子力学的な「量子効果」を利用しているからだ。したがって「量子コンピュータとは何か?」といったときに、ハードウェアが量子力学に基づいていることや、量子効果を用いているということ自体は、何の証拠にもならない。

こういった「量子効果」と、「量子コンピュータ」が代表する量子情報技術とを区別するために、従来の量子効果に基づく技術革新を第一次量子革命、これから私たちが経験していくと考えられている量子コンピュータや量子センサなど量子情報を活用した技術を第2次量子革命と呼ぶことがある¹⁾。この第2次量子革命の核心となる量子情報を理解することが、量子情報処理

を理解する上で重要となる。

本題に戻ると、量子コンピュータとはすなわち、量子計算を実行するハードウェアである。その上で行われる情報処理そのものも量子的たらざる得ないことから、ソフトウェアの原理も量子的でなければならない。

では量子計算とは何だろうか?

量子コヒーレンス

量子計算を理解するには、量子コヒーレンスを理解する必要がある。量子計算においては、量子コヒーレンスと呼ばれる量子性が、情報(データ)を担い、計算を実行する。量子的な性質は大変壊れやすく、重ね合わせ状態を制御する量子計算では、高度な量子状態制御が必要とされるので、まず量子コヒーレンスとは何かについて具体的に見ていこう。

量子コヒーレンスは、量子力学が許す重ね合わせ状態に基づいて説明できる。重ね合わせ状態とは、古典的には区別できる2つの状態が重ね合わさった状態である。たとえば、0と1からなる1ビットを量子化して量子ビットにしたとしよう。量子コンピュータでは量子ビットが量子計算の情報単位である。混乱を避けるために、情報処理(計算)を古典情報処理(古典計算)と呼び、量子情報処理(量子計算)と区別することにする。さて0と1は、「0であれば1でなく、1であれば0でない」という相反する事象である。量子情報処理においても、0か1かを測定する(計算基底で測定

する) とき、やはり0と1は相反する事象となる。ところが、量子ビットの状態は、0か1かのどちらかに決まっているのではなく、0と1の重ね合わせをとり得るのである。「とり得る」というよりも、むしろその方が一般的な状態であるということが出来る(図-1参照)。

少し横道にそれるが、量子情報処理における測定は、古典情報処理のそれとは異なるので、少し言及しておきたい。量子ビットが0と1の重ね合わせの状態である場合に、量子ビットを計算基底で測定することを考えよう。その測定結果は、0か1になるわけだが、どちらの事象が出るのかは確率的になる。ここで1つ注意しておきたいことは、デジタル信号の0と1では、0と1の間に物理的な値が存在する(電圧なら0にあてた電圧と1にあてた電圧の間の電圧をとることは、物理的には可能である)、量子ビットの0と1の間の値は物理的に存在しない(図-2参照)。測定結果は0か1のどちらかであり、その出現確率は、測定前の状態の重ね合わせ方による。重ね合わせの割合に応じて、その出現確率が決まってくる。これが、量子力学が確率的といわれるゆえんである。しかしながら、重ね合わせ状態は一意に決まった状態であり、そこでは確率性を伴わないことには留意しておくべきであろう。

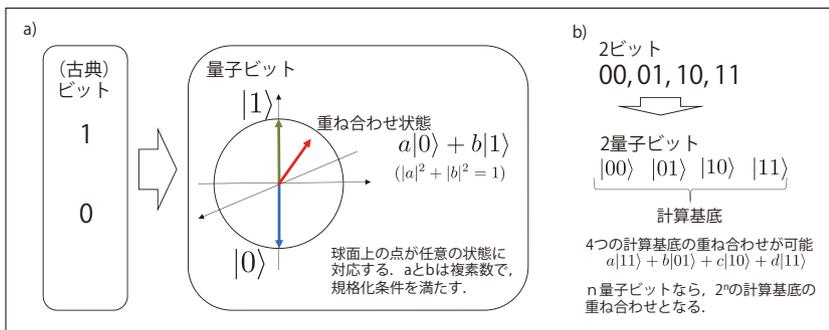
本題に戻ると、この重ね合わせ状態こそが「量子情報」であり、この量子情報の操作が量子情報処理となる。この量子情報には、重ね合わせの在り方に示され

る測定時の出現確率の割合とともに、位相情報が含まれている。この位相を維持することが、量子コヒーレンスの維持には必須である。蛇足ながら、重ね合わせの割合と、測定結果の出現確率というのは、位相情報を考えていないという意味で、十分に量子情報的な見方ではないということができる。

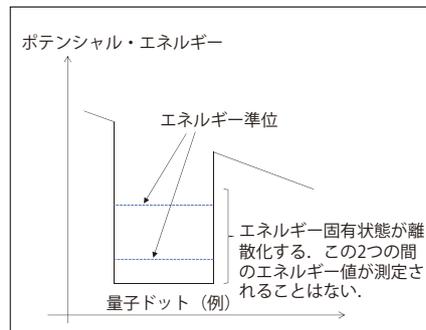
量子計算の原理

量子情報が定義されたので、本章では量子計算について見ていこう。量子計算とは、ひとことでいうと量子情報(つまり、重ね合わせ状態の割合と位相)を操作することで計算を進めていくことである。情報処理の専門家である諸兄はすでにお気づきのことと思うが、量子情報は連続的に変化する、いわばアナログ量である。このことから、量子計算では誤り訂正が重要な位置を占める。この点に留意しながら、量子計算について概観していこう。

量子計算を実行するには、この重ね合わせ状態を操作することが必須である。古典計算では、ANDやNOTゲートなど、ゲートという考え方でデータを処理するのと同じように、量子計算でも、論理ゲートが考えられる。この論理ゲートは、1つの状態から、ほかの状態へマップする働きを持つため、離散的な演算である。ここが少しややこしいのだが、演算そのものは離



■図-1 重ね合わせ状態：a) 右図は量子ビット1つがとる重ね合わせ状態を示す。ビットの0と1を計算基底とすると、任意の状態は $|0\rangle$ と $|1\rangle$ の重ね合わせで表すことができる。ここで $|0\rangle$ ($|1\rangle$)はビットの0(1)に対応する量子状態を指す。左図は量子ビットの数を2つに増やした場合、このとき計算の基底は00, 01, 10, 11の4つをとるので、量子ビット2つの全体に対する任意の状態はこの4つの状態の重ね合わせで記述できる。量子ビットの数が増えると、計算基底は量子ビット数に対して指数的に増え、一般的な状態は、これら計算基底となる状態の重ね合わせ(線形結合)となる。

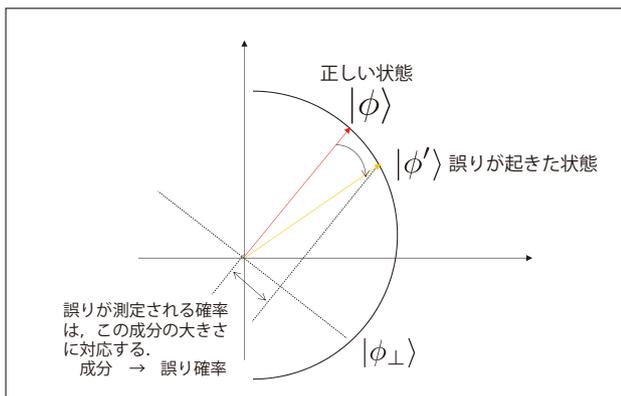


■図-2 準位の離散化：量子力学では、物理量が離散化することが多いことが大きな特徴である。これは古典力学では起こらない。エネルギー準位が離散化されているところで、エネルギーを測定した場合、エネルギーとしては離散値しかとらないため、エネルギー固有値の間の値が測定されることはない。

散的でも、量子情報は連続的に動き得るため、理論ゲートが100%正確でないかぎり、量子情報に誤差を生ずることになる。この量子計算の持つアナログ的な性質は、量子コンピュータ研究が注目され出した1990年代には、量子コンピュータの可能性に対する最も大きな壁であった。

特に、初期の量子コンピュータにおける否定的な見解は、必要な量子性を保てないということに基づく議論であった²⁾。その後、量子情報をいかに守るかという問題は、量子コンピュータ上の誤り訂正の原理の発見によって解決の見通しが得られ、量子コンピュータ研究は大きく前進することとなる。量子誤り訂正では、アナログ的に起こるエラーをデジタル化することで誤り訂正を可能にする³⁾。1つの量子ビットの情報を多数の量子ビットに担わせる誤り訂正符号はさまざまなものが考え出されており、現在の量子コンピュータ研究に用いられている誤り訂正符号のほとんどは、表面誤り訂正符号などのトポロジカル誤り訂正符号と呼ばれる一群である。

ここで、誤り訂正の原理を少し説明しておく。古典計算では、何らかの理由で0が1へ、または1が0へ変化してしまうことで誤りが起こるわけだが、量子計算では、量子情報(量子状態)が連続的に変化し、あるべき重ね合わせの状態からほんの少しでもずれることで誤りが起こる。この少しのずれをデジタル化することは、



■ 図-3 誤りのデジタル化：図は誤りのデジタル化の概念を示す。誤りはあるべき状態から連続的にずれるのに対し、シンドローム測定により、正しい状態かそれを直交する状態のどちらかに射影される。その際、直交する状態へ射影される確率が誤り確率となり、状態のずれの大きさに対応する。

誤りのない正しい状態と完全に誤った状態(正しい状態と直交した状態)へ射影することと考えればよい(図-3参照)。このとき、古典計算の0と1のフリップに相当するエラー、つまりXエラーと同時に、位相がフリップするZエラーという2つのタイプのエラーが出てくる³⁾。これを訂正可能にするためには、複数の量子ビットを用いて冗長性を持たせた空間で1量子ビットを符号化し、正しい状態と完全に誤った状態とへ射影する機能を持つシンドローム測定によって、誤りを訂正しながら同時に誤りを検知する。誤りが検知された場合は、誤り訂正符号によってどのように操作すると誤りが直せるのかが分かる仕掛けになっている。この作業は、誤りのために増加したエントロピーをシンドローム測定によって捨てる作業を繰り返し行うものと見ることもできる。

それでは、量子コヒーレンスが失われていく過程では、どうことが起こるのであろうか。量子状態の重なりは、古典的に考えると、0のときと1のときの両方の情報が、その状態の中に格納されていることになる。これが、量子計算では、並列計算が可能で、それが故にスピードアップが期待できるとされる理由である。ところが、量子状態に量子デコヒーレンス(量子コヒーレンスの消失)が起こると、状態の中に格納されていた0と1に関する重ね合わせの情報は、0と1の存在確率に置き換わってしまう。つまり、そのときには確率を用いた古典計算と変わらなくなってしまうことができる。量子コヒーレンスの消失は、まさに量子情報の喪失なのである。

さて、誤り訂正が可能になり、量子情報処理が必要な精度で実行できるハードウェアができれば、いよいよ情報処理の出番である。量子計算が約束する計算の高速化を図りたい。重ね合わせの持つ並列的な性質を使って計算の高速化を引き出すのである。具体的な量子アルゴリズムとしては、ご周知のようにShorのアルゴリズムを初めとしてさまざまな量子アルゴリズムがこれまでに考案されている^{☆1)}。誤り訂正もそうであったように、量子情報の理論は、従来の情報処理の概念

☆1) <https://math.nist.gov/quantum/zoo/>

を拡張して生み出されてきているので、今後さまざまな量子情報への拡張を図っていくことで、新しいアプリケーションの創出がいろいろと期待できる分野である。

そのときの1つのヒントは、量子状態が並列計算的な情報を持っていながら、通常の並列計算とは異なることである。量子情報では、その並列計算的な情報へアクセスすることができないという性質を持っている。計算が終了した時点では、情報は古典的になっている(状態が重ね合わせになっていない)ので、それを読み出すことができるが、計算の途中ででてきている量子情報を読み出すことはできない。ほかにも量子情報に特化した性質があり、たとえば、量子情報は局所的な情報操作の結果を量子コンピュータ全体で共有したり、個々の量子ビットの位相情報変化を1つにまとめて格納できるといった性質を合わせ持っている。こういった性質をうまく利用できれば、新しい量子アルゴリズムやアプリケーションの発見につながる。

さて、ここでもう一度ハードウェアに戻り、量子計算がすなわち量子状態操作であることを踏まえると、量子コンピュータ実装の歴史と課題が理解しやすい。次の章から、現在の量子コンピュータの研究動向と、今後どのような研究指針が必要となってくるのかについて概観していこう。

1990年代からの量子コンピュータ研究経緯

まず、量子コンピュータの実装にかかる研究の流れを概観していこう。量子コンピュータの研究は、1990年代から数回にわたり世界的な盛り上がりを見せてきた。1990年代は、量子コンピュータに必要な原理の理論的解明が飛躍的に進んだのが特徴的で、2000年に入ってから、それらの実験的な検証が急速に進んだ。特に2、3年前から始まった世界的に大規模な量子コンピュータ研究開発の盛り上がりの最も大きな特徴は、量子コンピュータ・アーキテクチャにあるとあってよい。これには

量子コンピュータの実装理論の発展により、量子コンピュータの全容が見えてきたことが背景にある。当然、今現在の大規模に進められている各国の量子コンピュータ開発も量子コンピュータ・アーキテクチャに基づいた研究開発である。世界的に今までにない規模でデバイス開発から理論まで、さまざまな知識背景を持つ研究者が結集して研究にあたり、量子コンピュータを初めて誤り耐性のある量子情報処理システムとして捉えた研究開発が始まっている。

これまで見てきたように誤り訂正は重要で、量子コンピュータ実装化研究は、誤り耐性のある量子コンピュータ(しばしばゲート型量子コンピュータや、デジタル量子コンピュータ、または最近では万能型量子コンピュータ等と呼ばれることもある)を可能にする技術体系を生み出す方向で強力に推し進められている。この筆頭が、グーグルやIBMの開発する量子コンピュータである。たとえば、IBMは50量子ビット搭載の量子コンピュータを昨年発表しており、この数年で数十から数百量子ビットからなる量子コンピュータが次々に登場すると期待されている。ただ、数百という量子ビットの数は、誤り耐性のある量子コンピュータの実装にはまだ数が足りない。したがって、しばらくは誤り耐性なしで動作させることを考え、量子ビットの数が追いついてきたところで、シームレスに誤り耐性量子コンピュータへ移行することが予想される(このようないわば過渡的な量子コンピュータを、最近では近似型万能量子コンピュータと呼んだりすることもあるようである)。

誤り耐性のない量子コンピュータにおいては、計算ステップとともに、データを担う量子ビットに誤りが蓄積する⁴⁾。一方で、誤り耐性量子コンピュータの出現にはまだまだ時間がかかるために、ある程度の誤りを許しながら、量子計算としての優位性を発揮する何かを発見することが大変重要である。

一方、量子コンピュータと並んで取り上げられるものに量子シミュレーションがある。元々、シミュ

レーションは解きたい系やモデルをそれとは別のシステム等を用いてシミュレートことであり、概念上は同列に議論するものではない。最も分かりやすい量子シミュレーションは、量子コンピュータ上で解きたい問題をシミュレートすることであろう。これは私たちがコンピュータを用いて日々行っているシミュレーションそのものと同じ考え方である。これをデジタル量子シミュレーションという^{☆2}。

量子シミュレーションの現代的な課題は、まず、先ほどの有限の精度、規模の量子コンピュータにおける有効なアプリケーションを提示する役割、そしてもう1つは、特定のシミュレーションに特化させることでハードウェアの大規模化を図ることである。後者を量子シミュレータと呼ぶ場合がある。量子シミュレータの実装上の利点としては、量子コンピュータのような量子ビットの個別制御ではなく、量子シミュレータのグローバル制御を許すため、制御系の簡略化ができる。これは、量子コンピュータ・アーキテクチャの観点からだけでなく、数10mK(ミリ絶対温度)と言った極低温下で制御ラインの生み出す熱の大きさといった実用上のファクタとしても大変有効である^{☆3}。

専用機としての量子シミュレーション、つまり量子シミュレータの開発では、量子ビットの数が増えてきているところが注目に値する。ただし、量子シミュレーションの説明で、量子アニーリングや量子断熱計算があたかも量子シミュレータを意味するように語られているのを見受けるが、これはミスリーディングである^{☆4}。元々、量子アニーリングや量子断熱計算は量子計算の一種であり、誤り訂正も必要

となる^{☆4}。量子シミュレータを目指した取り組みの中で、最も大規模なものを開発しているのは現在のところD-WAVEで、2,000量子ビットを搭載したマシンが昨年リリースされている。D-WAVEの量子シミュレータがどこまで量子情報处理的であるのかはこれまでの多く議論されてきた。現在のところ、量子シミュレーションでは、量子情報処理が期待する計算の高速化が得られていないという意味で、量子情報処理にはなっていないというのが一般的な見解のようである⁶⁾。しかし、これはハードウェアがまったく量子的に動作していないということを意味せず、むしろ一定の量子性があるのではないかと考えられている。したがって、この種の取り組みでは将来的に、量子アニーリングや量子断熱計算のような量子情報処理、そして本来的な量子情報処理としての量子シミュレーションという両方の実装の可能性があり、その際、量子シミュレータが実現できる規模(量子ビット数)は大きなインパクトを発揮するだろう。将来へ向けた取り組みが期待される。

さて、これで主要なものはおよそすべて概観したことになる。せっかくの機会なので、番外編ともいえる量子計算に特化した古典計算機に言及しておこう。量子コンピュータ研究に触発されて始まった古典計算の専用機のことだが、日本ではこれが意外に盛んである。光を用いたネットワーク型のものやCMOS技術を用いた専用機などが開発されている。基本的には従来技術の上にシステムを開発しているため、実装化が比較的容易であり、汎用機よりも大規模な計算が可能となることが期待できる利点がある。しかしながら、計算の原理は古典計算なので、この種の取り組みは将来的にも量子コンピュータや量子シミュレータへ移行することはない。

☆2 現在の量子コンピュータの開発では誤り耐性量子コンピュータに至らないため、本来必要な誤り実装については考慮にいれないで議論されることも多い。

☆3 量子シミュレーションをもう少し物理実験的にやろうという試みもある。これは量子エミュレーションと呼んで区別する場合がある(シニア層にはご存じの方も多いと思うが、昔計算機の計算力があまりなかったときに、本物ではない実機のモデルを作って実験的に解析する手法のことである。風洞実験などの量子版と考えると)。情報処理を専門とする研究者から見ると、これはほとんど実験の世界で、情報処理と呼べるかどうかは甚だ疑問があるが、こういったものも含めて広義の量子シミュレーションとして議論されている場合も実は多いので、シミュレーションの方法について吟味する必要がある。

☆4 これらの量子計算の方法における誤り訂正理論は、ゲートに基づく方法と比較するとまだ未発達の部分も多い。

今後の課題

量子コンピュータと量子シミュレータは、世界的に大規模な研究開発が進められ、すでに数十量子ビットのマシンの開発計画が発表されており、遅かれ早かれ数十量子ビットのマシンを使ってみるようになるだろうと期待されている。そこで、研究の関心はむしろソフトウェア的なところへ移りつつある。

大雑把に言って、量子コンピュータの大きさが決まっているとすれば、量子コンピュータが生み出す複雑性は計算ステップ数に依存する。計算ステップ数が十分に短ければ、古典コンピュータでも解けると期待できるからである。誤りの蓄積と計算ステップ数の増加（複雑性の増加）とはトレードオフになるので、規模的にも、精度的にも制約のある量子コンピュータでどのような優位性が発揮できるのか、つまり誤り訂正なしの数十量子ビットのマシンで何ができるのかが、まず最も主要かつ重要な課題である。この課題に向けては、多角的に取り組んでいく必要があり、現在までの情報処理発展の歴史に多くのヒントがあるように思う。

その中でもシンギュラリティをもたらすような量子アルゴリズムや量子アプリケーションはキラークラス・アプリケーションと呼ばれ、この発見に大きな関心が集まっている。中でも量子化学や物性理論などへの応用としての量子シミュレーション、量子機械学習などが注目されているようである。そのほかにもさまざまなものが考えられており、未知のことも多いことから、研究への新規参入も盛んだ。ここで研究開発の視点としては、指数的計算高速化といった量子がもたらす本質的なシンギュラリティのみに専念するのではなく、アプリケーションという観点から、実用上のシンギュラリティも十分に視野に入れるべきである。古典コンピュータで手に負えないような問題でなくても、量子コンピュータによって数桁速くなるというようなものも実用上利点を発揮できる可能性はある。または安全性を付与できる、超小型、超軽量であるといった、十分な付加価値が付与できるというのも魅力的である。量子コンピュータの実機を使って

みるということもできるようになりつつある中、情報処理が培ってきた英知をどう応用するかが、これからの量子情報の将来を担っているといえるだろう。

ハードウェアの制御の中にも情報処理の発展が待たれる。誤りをどのように制御していくかはやはり大きな課題で、物理的な量子制御には必ず限界があり、数十量子ビットという小さな量子コンピュータに特化した新しい誤り制御の方法の探求が必要である。そして、こういったマシンの動作を検証するための理論立ても必要となる。もう少し上の技術レイヤでは、量子アプリケーションや量子アルゴリズムから起こした量子回路の最適化や、実装上の量子回路の忠実性を検証する検証理論の確立などが必要である。また一方で、量子コンピュータを制御するのは古典コンピュータであり、誤り訂正や制御のための高速な情報処理なども必要で、今後この新しい諸課題に対して、学際的な研究が発展することを期待したい。最適化や検証にかかる理論の重要性は、量子コンピュータの実装に向けてこれからさらに増していくだろう。

(2018年2月13日受付)

参考文献

- 1) Dowling, J. P. and Milburn, G. J. : Quantum Technology : The Second Quantum Revolution, DOI: 10.1098/rsta.2003.1227 (2003).
- 2) Unruh, W. G. : Maintaining Coherence in Quantum Computers, Phys. Rev. A., 51:992 (1995).
- 3) Devitt, S. J., Nemoto, K. and Munro, W. J. : Quantum Error Correction for Beginners, Rep. Prog. Phys.76, 076001 (2013).
- 4) Nemoto, K., Devitt, S. and Munro, W. J. : Noise Management to Achieve Superiority in Quantum Information Systems, DOI: 10.1098/rsta.2016.0236 (2017).
- 5) Aharonov, D., Dam, W. V, Kempe, J., Landau, Z., Lloyd, S. and Regev, O. : Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation, SIAM Journal of Computing, Vol.37, Issue1, p.166-194 (2007), Conference Version in Proc. 45th FOCS, p.42-51 (2004).
- 6) Rønnow, T. F. et al. : Defining and Detecting Quantum Speedup, Science 19, 1252319 (2014).

根本香絵 nemoto@nii.ac.jp

お茶の水女子大学大学院卒業、博士(理学)。専門は理論物理学、量子情報・計算、量子複雑系。豪州クイーンズランド大学・英国ウエールズ大学研究員を経て、2003年より国立情報学研究所助教授(准教授)、2010年より現職。米国物理学会および英国物理学会フェロー。