量子コンピュータの現状と可能性

技術解説

藤　井　啓　祐*

State of the art and prospects of quantum computing

Key Words：quantum information, quantum computer, quantum mechanics

はじめに

最近、「量子コンピュータ」というキーワードを新聞やインターネットでよく聞くようになった。しかし、量子コンピュータのアイデア自体は古く、80年代までさかのぼる。書籍「ご冗談でしょう、ファインマン先生」（岩波現代文庫）でも有名なノーベル賞を受賞した物理学者R.ファインマンが、1981年に「自然をシミュレーションしたければ、量子力学の原理でコンピュータを作らなければならない」と指摘した[1]ことに端を発し、1985年にオックスフォード大学の物理学者D.ドイッチュによって定式化された[2]。それから30年以上たち、今になってなぜ、量子コンピュータが話題になっているのだろうか。一つは、量子力学的にふるまうミクロな系を制御する技術、いわゆる量子技術が着実に発展してきた結果、量子コンピュータを構成するための要素技術が確立されつつあることである。我々が日常的に使っているコンピュータの歴史になぞらえると、1940年代後半に発見されたトランジスタが、1960年代に入り実用化され、60年代後半にマイクロプロセッサIntel 4004が登場する前夜といったところかもしれない。このような技術的進展を背景に、Google、IBM、Intel、MicrosoftといったITの巨人たちが、軒並み量子コンピュータの開発に乗り出してきたことも大きな影響を与えている。IBMやGoogleは、数十量子ビット程度の実際に動く量子コンピュータを実現している。IBMはその量子コンピュータをクラウド化し、インターネット経由で誰でも使えるような環境を提供している[3]。Googleや、他の量子コンピュータハード開発のベンチャー企業たちも近々クラウドで量子コンピュータを提供することになりそうだ。一方、Microsoftは量子コンピュータ上で動くソフトウェアの開発環境の整備も行っている。5年前に比べると間違いなく量子コンピュータは確実に身近な存在になってきている。しかし、量子コンピュータは、現在我々が使うコンピュータと動作原理が全く異なる。「量子力学」の原理に従って計算を行うコンピュータであり、量子力学を知らない人には参入障壁が少し高いかもしれない。本技術解説では、このような参入障壁を下げより多くの人に量子コンピュータについて知ってもらうことを狙いとし、量子コンピュータの歴史、仕組み、未来について解説したい。

* Keisuke FUJII
1983年12月生まれ
京都大学大学院　工学研究科　原子核工学専攻博士後期課程（2011年）
現在、大阪大学大学院　基礎工学研究科　システム創成専攻　教授　工学博士
TEL：06-6850-6278
E-mail：fujii@qc.ee.es.osaka-u.ac.jp

量子コンピュータの歴史

まず、現在にいたるまでの量子コンピュータ研究の歴史を見ていくことにする。量子コンピュータがその動作原理の基礎を置く量子力学は、粒子の運動を記述するニュートン力学、波の運動を記述する電磁気学を「量子」として統合する形で1920年ごろに構築された。一方、情報科学の歴史をみてみると、量子力学が発展を迎えていた1930年代にA.チューリングが、計算する機械が満たすべき性質を抽象化し、チューリング機械を定式化した。また、1940年代には、C.シャノンが、情報の量を定量化する情報理論を構築し、情報科学の端緒を切ることになった。そして、1940年代には、真空管やスイッチング回路を用いたコンピュータの構築が進められ、ENIACやEDVACなどの現在に繋がるコンピュー

タの元祖とも呼ぶべきものが運用されていた。EDVACプロジェクトに参加していたJ.フォン・ノイマンは、プログラム内蔵型のノイマンアーキテクチャについて（諸説あるが）報告している。同時に、ノイマンは数学者および理論物理学者でもあり、量子力学の数学的な基礎づけにおいても重要な仕事をしている。まさに天才的な研究者である。しかし、コンピュータと量子力学の両方の黎明期に両分野で重要な貢献をした、この天才的な研究者でもってしても、量子コンピュータには至らなかった。

しばらく、量子力学と情報科学はまったく交わることなくそれぞれ独自に進化を続ける。この2つが交わるきっかけとなったのは80年代に起きた一つのムーブメントだった。80年代当時、コンピュータの発熱がすでに問題となりつつあった。発熱するということはエネルギーを消費しているので、電気代がかかる。発熱しないコンピュータを作ることができれば省エネのコンピュータが作れると考えたのだ。このとき、そもそもなぜ計算に発熱（エネルギーの消費）が必要なのだろうか？というのが研究者の間で問題になった。従来の情報科学的アプローチだけでは、この問いかけに答えることはできなかった。情報処理の究極的な限界は、情報を担っている物理系が従う物理法則によって決まる。このような背景から、当時IBMに所属する研究者であったR.ランダウアの掲げた「informaiton is physical」というスローガンのもと情報と物理の融合研究が1980年代に進む。そのような中で、ノーベル物理学賞を素粒子分野でとったR.ファインマンが、「自然は量子力学で動いているので、自然を効率よくシミュレーションしたければ、量子力学の原理で動くコンピュータを作らないといけない」という指摘をする[1]。また、同時期にD.ドイッチュは、「君たちは間違った物理をつかっている（物理はNANDやANDなどの古典論理ではなく、量子力学によって動いている）」。その後、D.ドイッチュは量子力学で動く量子チューリングマシンを定式化し、現在につながる量子コンピュータの端緒を切った[2]。

80年代にはじまった量子コンピュータの研究であるが、当初は情報と物理の融合領域に魅せられたマニアックな研究者たちの集まりであった。それが90年代中頃になると、より多くの研究者が興味を持つきっかけが訪れる。P.ショアによる素因数分解アルゴリズムの発見である[4]。素因数分解は、15＝3×5のような、単純な問題であるが、整数のケタ数が増えていくにつれて分解するために必要な計算時間が指数的に伸びていき、現在のところこの問題を効率よくとくアルゴリズムは知られていない。この難しさにもとづいて、暗号（RSA暗号）の安全性が担保されているくらいだ。この難しい問題を、従来のコンピュータとはまったく別の原理で動作する量子コンピュータはいとも簡単に解いてしまう。これをきっかけに、物理学および情報科学の多くの研究者が興味をもつようになり、一気に量子情報科学という新たな学術領域が形成されていった。実験側も、1998年に固体で世界初の量子ビットが、当時NECに在籍していた中村・蔡（現東京大学、東京理科大学）らによって実現されるなど[5]、理論・実験両面から非常に活気づいていた。これが今からみると、量子コンピュータの第一次ブームである。

2000年代中頃にはいると、この量子コンピュータブームは停滞期を迎えることになる。理論側では簡単にできるような研究はやり尽くされてしまい、難しい問題が残される。実験側では、量子ビットの数がなかなか増えず、大規模な量子コンピュータの実現の難しさが浮き彫りになる。私が研究を始めたのは2005年頃で、この停滞期の真っ只中であった。もちろん、新聞やニュースで量子コンピュータが話題になることや、量子コンピュータをユーザーとして利用したいと興味をもつ企業はほとんどなかった。

このような量子コンピュータが再び注目をあつめるようになったのは、2010年代に入ってからである。カナダのD-WAVEという会社が量子コンピュータを商用化し売り出しているという。これは、当初ドイッチュが提案した量子コンピュータとは異なるもので、超伝導量子ビットを用いてプログラマブルな磁性体（スピングラス）を実現したというものであり、量子アニーリングマシンと呼ばれている。スピングラスの低エネルギー状態の計算は、複雑な組み合わせ最適化問題と対応するため、特定の組み合わせ最適化問題の近似解をえる専用マシンとして利用されている。この量子アニーリングマシンに興味をもったGoogleが、このマシンを購入し複数の量子コンピュータの理論・実験の研究者を交えて研究を開始する。この中にいた一人が、米国カリフォルニア州立大学サンタバーバラ校で超伝導量子コンピュ

ータの研究を行っていたJ. マルチネスである。マルチネスは、同時期（2014年）に超伝導量子ビットをチップに並べ超高精度で制御する、という究極のエンジニアリングを実現する[6]。研究の過程からD-WAVEの専用マシンには限界があることも見えてきたGoogleは、2014年9月にマルチネスをグループごと抱え込み、超伝導量子ビットを用いた量子コンピュータのデバイス開発に乗り出すことを決定した[7]。このインパクトは大きく、これまで大規模な量子コンピュータには否定的だった研究者たちもこぞって大規模化に向けた取り組みを展開するほど、潮目が一瞬にして変化した瞬間であった[8]。80年代から量子コンピュータの基礎研究をつづけてきたIBMも人員を増やし、量子コンピュータの研究を加速させ、2016年にはクラウドで小規模な量子コンピュータを公開した。さらには、Intel、Microsoftなど、ITの巨人たちが次々と量子コンピュータ領域に参入していき、現在、第二次の量子コンピュータブームが形成されるに至った。

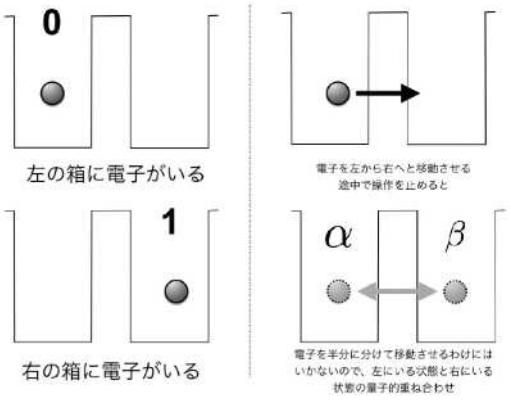
量子の世界の不思議

続いて、量子コンピュータの動作原理の基礎となる量子力学は、電子や原子などのミクロな世界を記述するための物理学であり、半導体、MRI（核磁気共鳴画像法）、レーザーなど身の回りの技術を影で支えている（詳しくは、「量子技術2.0～量子コンピュータから次世代MRIまで」根来誠　生産と技術2017年　夏号を参照されたい）。量子コンピュータはこのような縁の下の力持ちである量子力学を表舞台に引っ張りだし、その不思議な性質を積極的に活用するコンピュータである。従って、量子コンピュータの原理や従来コンピュータとの違いをしるためには、少々量子力学の知識を必要とするので、少し解説したい。

古典ビットと量子ビット

従来のコンピュータでは、**0**と**1**の2つの変数、ビット、で情報が表現されている。スイッチのオン・オフ、電圧の高低、コンデンサーに貯まった電荷状態とそうでない状態など異なる2つの状態を用いて**0**と**1**を物理的に表現している。このビットに対して演算を施すことによって計算をすることになる。従来のコンピュータ上では、ビットは必ず**0**か**1**かどちらか一方を取っている必要がある。しかし、計算の原理を量子力学へと拡張すると、量子力学では**重ね合わせ状態**という、**0**であるか**1**であるかがまだ確定しておらずどちらの値をとる可能性もある状態が、許されているため、より一般的な**量子ビット**によって情報を表現することになる。

例えば、電子1つを使って情報を表現することを考えよう。図のように左側の箱に電子がいる場合は**0**、右側に電子に箱がいる場合を**1**とすることにしよう。量子力学の世界では電子は必ずしも、どちらか一方の箱にいる必要はなく、右側の箱にいる状態と左側の箱にいる状態の重ね合わせ状態をとることが許されている。日常的にはこのような現象は起こらないので重ね合わせ状態を直感的に受け入れることは難しいかもしれないが、以下のような感じである。最初に、電子を左の箱に入れ**0**状態を準備したとし、電圧をかけるなどして、電子を左から右に転送して**1**状態にしようとする（ビットの反転）。電子が完全に右側に移動しきるまえに、転送を止めてしまう。電子がたくさんいる場合には、半分の電子が転送される、といった帰結がありうるが、いまは電子1つで情報を表現するという究極的な状況を考えている。このとき、電子は左にいるのか右にいる



のかよくわからなくなった曖昧な重ね合わせ状態をとれる。この**0**と**1**が重ね合わさった状態が**量子ビット**である。

このような量子ビットを従来のコンピュータで表現するならばどのように記述する必要があるかを説明しよう。従来のビットであれば、**0**もしくは**1**の1つの整数によって簡単に記述できた。その重ね合わせを許す量子ビットの場合は、どの程度**0**でどの程度**1**であるかを表すために2つの連続値をもつ複素数αとβを用いたベクトルとして

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

のように記述し、状態ベクトルと呼ぶ。ここで、|>の記号はケットと呼ばれ、量子状態を表す複素数ベクトルという量子状態という型を表すシンボルだと思ってほしい。$|\psi>$はψという名前をもった状態ベクトルを表している。状態ベクトルの要素である複素数の値αとβは複素確率振幅とよばれ、どの程度の重みで**0**状態と**1**状態が重ね合わさっているかという量を表している。確率振幅と呼ばれる理由は、この量子ビットを**0**であるか**1**であるか測定をしてしまい、曖昧な重ね合わせ状態を強制的に**0**もしくは**1**へと確定させたときの確率が、この複素数の絶対値の2乗によって決まる。つまり$|\alpha|^2$の確率で**0**、$|\beta|^2$の確率で**1**に確定する。このため、この複素ベクトルは規格化

$$|\alpha|^2 + |\beta|^2 = 1$$

されている必要がある。

従来のビットに対応する**0**や**1**をこの複素ベクトルで書くと

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

のようになる。**0**と**1**が重ね合わさった状態は、2つのベクトルの和として

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$

のように記述される。

量子アルゴリズム

量子ビットが**1**つしかなければ、先に見たように2つの複素数を用いたベクトルにすぎない。しかし、量子ビットが複数に増えると状況は一転する。ビットが**N**個あった場合、すべて**0**からすべて**1**まで2^N通りのパターンがあるわけだが、量子ビットが**N**個ある場合はこの2^N通りのすべてのパターンの重ね合わせ状態がゆるされていることになる。それぞれの状態がどのような重みで重ね合わさっているかを表現するためには、2^N個の複素確率振幅が必要となるため、2^N次元ベクトルとして表現される。つまり、量子ビット列が表現できる状態を従来コンピュータで書き出すと量子ビットの数に対して指数関数的なメモリが必要になる。いわば、量子コンピュータは、指数関数的に大きな規格化された複素ベクトルを物理状態として確保し、それに対して、指数関数的に大きなユニタリ行列を物理現象として作用させるようなコンピュータになっている。このような量子コンピュータの挙動を従来コンピュータでシミュレーションしようとすると、たった50量子ビットであっても16ペタバイト（ペタは10の15乗）のメモリーが必要になり、現在世界最高性能のスーパーコンピュータをもってしてもシミュレーションすることが難しい。

量子アルゴリズムは、このような巨大複素ベクトルの確保とそれに対するユニタリ行列の作用によってうまく問題を解くように設計されている。量子アルゴリズムによって高速に解が得られるような問題が今ではたくさん知られている[7]。大きくわけると、(i) そもそも問題に「量子」が関連するものと、(ii) 一見量子には関係しないが特定の条件が満たされると量子コンピュータによって高速化されるもの、である。(i) については、創薬や材料設計において重要になる、分子や物質のエネルギーや物性値を得るという用途である。この場合、そもそも分子や材料の物性は電子の量子力学的な振る舞いによって決まるので、従来のコンピュータでは、この量子力学的なふるまいを互換性がない従来コンピュータで無理やり解いてきた。量子力学と互換性のある量子コンピュータであれば、このような量子力学的なふるまいを、計算コストをかけずに取り込むことができるので計算を加速させることができる。

もう一つの場合 (ii) については、先に述べた素因

数分解 [4] のように、一見量子とは関係ないが、量子コンピュータが有効である場合だ。他にも、行列のスパース（疎）性など特定の条件が成立した場合の逆行列計算 [6]、そしてそれを利用したサポートベクトルマシンや主成分分析などの機械学習を指数的に加速できることが知られている。これらに共通する点は、非常に大きなサイズの行列の固有値を求めるようなアルゴリズムになっていることだ。量子力学は量子ビットに対して指数的に大きな次元になる線形代数構造を自然にもつので、この線形代数構造を利用した、固有値の推定によって、素因数分解や逆行列計算の高速化が可能となっている。

量子コンピュータの現状とNISQ

素因数分解アルゴリズムなど、指数関数的な高速化が可能となるアルゴリズムは非常に複雑な構成になっているため、現在実現しているレベルの小規模な量子コンピュータで実行することは難しい。一方で、現在実現しているレベルの量子コンピュータであっても特定の問題において従来コンピュータでシミュレーションすることは難しい潜在能力を有している。このような従来コンピュータに対する量子コンピュータの優位性を実験的に検証する試みは量子超越（quantum computational supremacy）と呼ばれている。

まさに、この原稿を書いている2019年10月に、Googleが量子超越に到達したという情報がNASAのウェブサーバーからのリークによって周知の事実となっている。Googleは、53量子ビットを集積化することに成功し、非常に高い精度で量子演算を実行したとのことである。実際に、Googleが実現した計算はランダムな量子演算を作用させるという、いわば量子コンピュータをもちいた量子乱数生成である。量子演算は、先に述べたように、巨大なベクトルに対するユニタリ行列の作用として記述できるので、Googleは量子ビット数を少なくした量子計算や、一部の演算を取り除くなど、従来コンピュータでのシミュレーションを容易にして、量子コンピュータからの結果が十分高い信頼度があることを検証している。一方で、53量子ビットを最大限に利用した計算に要する時間は数分であるのに対して、現在世界最高レベルのスーパーコンピュータを用いてもシミュレーションに1万年かかると結論づけている。つまり、定量的にスーパーコンピュータよりも圧倒的に量子コンピュータによる計算が高速であることが示されたことになる。ただし、計算結果自体はあまり意味をもつものではない。

このようなすでに実現している、もしくは、近未来的に実現する小・中規模の量子コンピュータは、Noisy Intermediate-Scale Quantum computer（NISQ）[7] と呼ばれ、その潜在能力を有効利用しようという試みが行われている。中でも、量子コンピュータから生成される量子状態を変分法の試行状態として用いる、変分量子固有値求解法 [8,9] が注目を集めている。例えば、化学や材料計算で重要となる量子多体系の基底状態の計算は、ハミルトニアンと呼ばれるエネルギーを表すエルミート行列Hの最小固有値と固有ベクトルを求める問題である。量子ビットの回転角度などをパラメータ付き量子演算$U(\theta)$を用いて量子コンピュータから生成された量子状態

$$|\psi(\vec{\theta})\rangle = U(\theta_n)U(\theta_{n-1})\cdots U(\theta_1)|00...0\rangle$$

に対してエネルギー期待値を最小化

$$\theta^* = \arg\min_{\vec{\theta}} \langle\psi(\vec{\theta})|H|\psi(\vec{\theta})\rangle$$

することによって最小固有値の近似を得ることができる。また、実際に量子状態を用いて得られたパラメータを用いて、実際に基底状態 $|\psi(\theta^*)\rangle$ を生成することもできる。

さらに、量子多体系の基底状態の計算だけではなく、最近ではハミルトニアンを取り替えることによって様々な応用がなされている。Hを教師データと量子コンピュータのからの出力との誤差になるようにすれば、パラメータ付き量子状態をモデルとした教師あり学習ができる [10,11]。また、あるベクトル $|b\rangle$ と行列Aに対して

$$H = A^\dagger(I - |b\rangle\langle b|)A$$

とすれば、最小固有値の固有ベクトルは

$$A^{-1}|b\rangle$$

を規格化した状態となっており、線型連立方程式の解法として用いることができる [12]。$|b\rangle$ やAは量子ビット数Nに対して指数関数的に大きな次元を有する。ただし、ベクトル $|b\rangle$ が量子状態として与えられていることや、Aが疎行列であるなど、量子

コンピュータ上で効率よく実行できるためには様々な条件も付く。以上のような、量子状態から計算されるコスト関数を用いた変分アプローチは、量子古典ハイブリッド変分アルゴリズムと呼ばれている。

まとめ

本稿では、量子コンピュータの発展や注目される経緯、そして現状を紹介した。量子コンピュータの基礎となる量子技術は、21世紀になって地道に発展してきた新たなテクノロジーフロンティアである。ますます、量子を自在に操れるようになってきているが、人類はまだまだ量子をうまく利用するための経験に乏しい。近年のハードウェアの進展とともに、それを用いて「量子の経験」を積み、うまく量子コンピュータを活用する方法を見つけだすことが期待されている。

[1] Feynman, Richard P. "Simulating physics with computers." *International journal of theoretical physics* 21.6-7 (1982): 467-488.

[2] Deutsch, David. "Quantum theory, the Church－Turing principle and the universal quantum computer." *Proc. R. Soc. Lond. A* 400.1818 (1985): 97-117.

[3] https://www.research.ibm.com/ibm-q/

[4] Shor, Peter W. "Algorithms for quantum computation: Discrete logarithms and factoring." *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*. Ieee, 1994.

[5] Nakamura, Yasunobu, Yu A. Pashkin, and J. S. Tsai. "Coherent control of macroscopic quantum states in a single-Cooper-pair box." *Nature* 398.6730 (1999): 786.

[6] Harrow, Aram W., Avinatan Hassidim, and Seth Lloyd. "Quantum algorithm for linear systems of equations." *Physical review letters* 103.15 (2009): 150502.

[7] Preskill, John. "Quantum Computing in the NISQ *era and beyond." arXiv preprint arXiv:1801.00862* (2018).

[8] Peruzzo, Alberto, et al. "A variational eigenvalue solver on a photonic quantum processor." *Nature communications* 5 (2014): 4213.

[9] Kandala, Abhinav, et al. "Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets." *Nature* 549.7671 (2017): 242.

[10] Mitarai, Kosuke, et al. "Quantum circuit learning." *Physical Review A* 98.3 (2018): 032309.

[11] Havlíček, Vojtěch, et al. "Supervised learning with quantum-enhanced feature spaces." *Nature* 567.7747 (2019): 209.

[12] Xu, Xiaosi, et al. "Variational algorithms for linear algebra." *arXiv preprint arXiv*:1909.03898 (2019).