

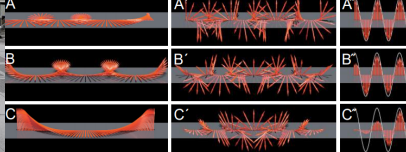
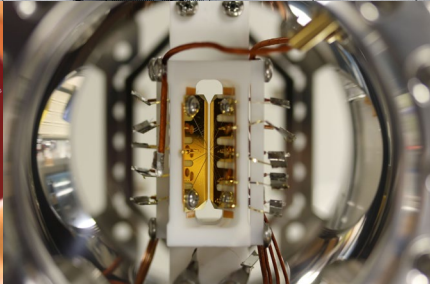
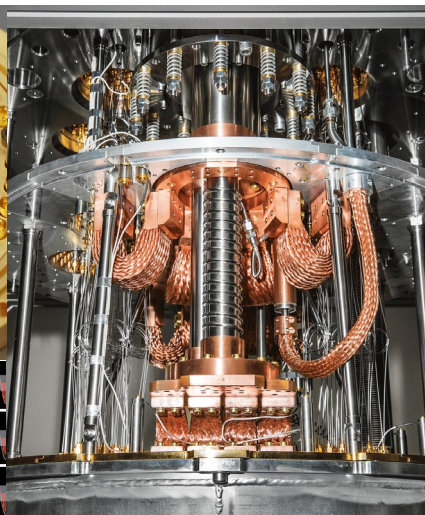
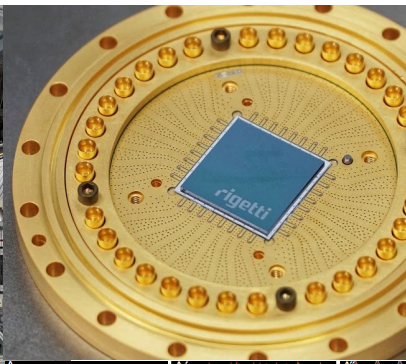
MIT Technology Review

Published by KADOKAWA / ASCII



Quantum Technologies

ここまで来た！量子テクノロジー最前線

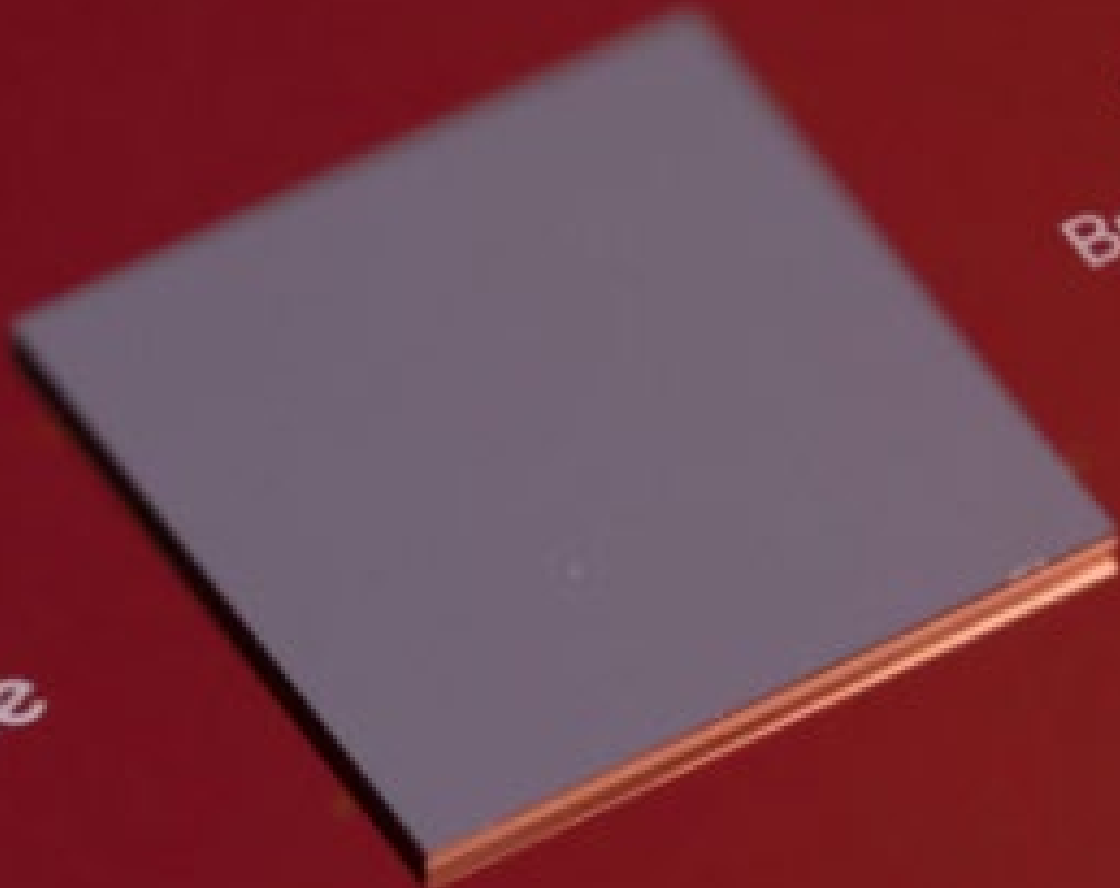


CONTENTS

- 001 量子コンピューター覇権争い
グーグルは量子超越性を実証できるのか？
- 007 量子コンピューター時代も
インテルが勝てるこれだけの理由
- 010 新方式の量子コンピューターが
50 量子ビット超を達成
- 014 量子コンピューターは
なぜ必要なのか？
- 025 米スタートアップ、
量子コンピューターで機械学習の実行に成功
- 029 マイクロソフトが
量子プログラミング言語を作る理由
- 033 欧州が 10 億ユーロを投じる
量子技術開発計画の最新ロードマップ
- 039 機械式ナノデバイスが開く、
量子インターネットへの道
- 042 量子暗号を使った大陸間ビデオ会議、
中国「墨子号」で成功
- 046 量子もつれを利用する
「量子暗号」の新手法、中国の研究者が実証
- 050 量子コンピューターが開く、
セキュリティの新しい扉

従来のスーパーコンピューターの領域をはるかに超えた計算ができるとされている、量子コンピューターを巡る動きが活発化しています。最近では、IBM やインテル、グーグルといったプレイヤーに加えて、スタートアップ企業も開発に参入。「量子超越性」をいち早く達成しようと競っています。このeムックでは、MIT テクノロジーレビューが 2017 年 10 月～ 2018 年 3 月にかけて掲載した記事から、量子コンピューターの動向を伝える記事をピックアップ。加えて、量子暗号や量子通信といった量子テクノロジーに関する最新研究も紹介します。

Google



Bristol

量子コンピューター覇権争い グーグルは量子超越性を 実証できるのか？

by Will Knight

Photo by Google

グーグルが、量子超越性に必要とされているキュービット数をクリアした量子コンピューティング・チップを開発した。しかし、量子超越性の達成をどのように実証するのか、本当に役に立つのか、など課題はまだ多い。高まり過ぎた期待に応えられず、過去の人工知能と同様に「冬の時代」に入ってしまう恐れすらある。

72 という数は大きな数字ではないかもしれないが、量子コンピューティングの世界では極めて大きな数だ。グーグルは 2018 年 3 月 5 日に「ブリッスルコーン (Bristlecone)」という名の新たな 72 量子ビット (キュービット) の量子コンピューティング・チップを発表した。キュービットは量子コンピューターにおける基本的な演算単位だ。これまでの最高記録保持者は IBM が 2017 年に発表した 50 キュービットのプロセッサだった。

グーグルの量子コンピューター開発を主導するカリフォルニア大学サンタバーバラ校のジョン・マルティニス教授は、まださらなるテストを

する必要があると言う。だがマルティニス教授は 2018 年中、あるいは数カ月のうちにこの新しいチップが「量子超越性」を実現できる可能性が極めて高いと考えている。量子超越性とは、量子コンピューターが現在で最高性能のスーパーコンピューターの計算能力を超える段階を意味する。

グーグルか、もしくは他のチームが量子超越性の達成を表明した暁には、エキサイティングな新時代の到来を告げるトップ記事があふれかえるだろう。量子コンピューターは新薬の発見、新素材の発明、暗号解読に寄与すると考えられている。

だが現実はもっと複雑だ。「『量子超越性』という言葉を好む研究者はあまりいないでしょう」と

オックスフォード大学の量子専門家であるサイモン・ベンジャミン教授はいう。「その言葉は非常に人の心を惹きつけますが、少し紛らわしいところがあり、量子コンピューターにできることを誇大宣伝しています」。

量子コンピューターの構成要素

その理由を理解するために、背景の事情を簡単に説明しよう。量子コンピューターの魔法の力はキュービットにある。情報を1または0として保存する従来のコンピューターのビットと違い、キュービットは1と0の多重状態で存在できる。この現象は「重ね合わせ」と呼ばれている。キュービットはまた、物理的につながっていなくても「もつれ」と呼ばれるプロセスを通じて互いに影響を与えることができる。

要するに、従来のコンピューターではビットがいくらか増えたところで、計算能力にそれほど大きな違いは起こらない。だが量子コンピューターでキュービット数が増えると、計算能力は飛躍的

に高まる。原理的には、現在最高のスーパーコンピューターを負かすのにそれほど多くのキュービットを必要としないのは、それが理由だ。

だがキュービットを作り出すにはエンジニアリングの驚くべき離れ業が必要とされる。たとえば、宇宙空間よりも低い温度に保たれた超伝導回路の作成などだ（グーグルがこの方法を採用している）。極低温は超伝導回路を外部世界から遮断するために必要になる。「ノイズ」と呼ばれる温度の変化やごくわずかな振動の現象は、キュービットの「デコヒーレンス」や、ただでさえ不安定な量子状態が失われる原因となり得る。そんなことが起こったら、すぐさま処理にエラーが忍び込んでくる。

キュービットの数が増えるほど、エラーも多くなる。追加のキュービットや賢いソフトウェアを使うことでエラーは修正できるが、それによって量子コンピューターの多くの計算能力が損なわれる。過去数年間における超冷却技術とその他の分野における発展で、スピントップされた状態で効率的に管理できるキュービットの数は増えた。だ

が、処理能力と複雑性は、依然として常にせめぎ合っている。

量子超越性達成の望みは過去に打ち砕かれたことがある。兼ねてより研究者たちは、量子超越性を達成するには49キュービットの機械で十分だろうと考えていた。だが2017年、IBMの研究チームが49キュービットの量子システムを従来のコンピューターでシミュレーションすることに成功した。従来のコンピューターも進歩しているのだ。特に中国は、コンピューター技術に大きな投資をしており、いまや世界トップレベルのコンピューター2台を擁している。

グーグルの決定的な瞬間

それでもなお、カナダのペリメーター理論物理研究所（Perimeter Institute for Theoretical Physics）のダニエル・ゴッテスマン博士は、より優れたアルゴリズムとデジタル・コンピューターは量子超越性のしきい値を少し上に移動させるかもしれないが、それでも量子コンピューター

がしきい値を実際に上回るには、おそらくあと数千キュービットで足りるだろう、との見方を示す。ブリッスルコーンの72キュービットがあれば、勝負するには十分だという。

マルティニス教授たちはブリッスルコーンを使って量子超越性の実証を目指すテストを計画している。量子超越性のベンチマークの厳密な定義は、テストで実施するタスクが従来のコンピューターには遂行不可能であることだ。だがこのことは厄介な問題を引き起こす。量子コンピューターが出した答えが正しいかどうかをどうやって現実に判断するのかということだ。シリコンのビットを使うコンピューターでは答えの正誤を確認できないのだから。

この問題に対処するためにグーグルのチームは、ギリギリの所まで行く計画だ。量子コンピューターを使って、現在のスーパーコンピューターの能力のまさに限界のアルゴリズムを解かせるのである。「アルゴリズムが飛躍的に複雑になっていることも示せます」とマルティニス教授は説明する。たった1キュービット増やすだけで量子コン

コンピューターは、従来のコンピューターがしかるべき時間内に扱えるのを、はるかに超えた処理を実行できるだろう。

呼び名の問題

もしグーグルがすばらしいベンチマークを達成したとしても、量子コンピューターの管理に伴う複雑性とコストにより、有用性には限界があるだろう。

分子の正確な設計などの潜在的に有望な応用分野はいくつか存在する。しかし、ほとんどの問題の解決には、従来のコンピューターのほうが依然として優秀で速く、はるかに経済的である。「量子コンピューターを使うのは、道を横切るのにジャンボ機をチャーターするようなものです」とオックスフォード大学のベンジャミン教授は話す。

ベンジャミン教授は、「量子超越性」よりもむしろ、「量子無類性 (inimitability)」の達成について語るべきだと提案する。量子無類性と

は、つまり、量子コンピューターだけに可能な特定のタスクを実行できることだ。「量子有利性 (advantage)」や「量子優位性 (ascendancy)」といった呼び名を提唱している研究者もいる。

重要なのは、言い回しよりも意味だ。人工知能 (AI) などのテクノロジーは、実際に離陸するまでに何度かのハイプ・サイクルを経験した。現時点での期待があまりに高まり過ぎると、量子コンピューターがそれに応えられない恐れがある。それは量子コンピューター分野のスタートアップ企業に大金を投じてきた投資家が離れるきっかけとなる可能性がある。

「量子超越性」という言葉の提唱者でさえ、自身が一役買った熱狂を沈めようとしている。カリフォルニア工科大学の理論物理学者、ジョン・プレスキル教授は 2011 年に、あるスピーチの中でこの言葉を生み出した。2018 年 1 月、プレスキル教授は論文を発表し、量子コンピューティングは彼が「NISQ (ノイズが多い中間段階の量子)」と呼んでいる、キュービット数が 50 から数百になる局面に入ろうとしていると述べた。プレス

キル教授は「『ノイズが多い』とは、キュービットのコントロールが不完全であることを意味します。ノイズの多さは量子デバイスが近いうちに成し遂げられることに重大な制約をもたらします」と述べる。同教授は依然として量子コンピューターは社会を変えるような影響力を持つと確信しているが、変化が起こるのは「何十年も先のこともかもしれない」という。

ノイズの問題は議論の別れる争点だ。エルサレムにあるヘブライ大学のジル・カライ教授は、ノイズが引き起こす問題は非常に大きいため、量子コンピューターが実際に役に立つことはないだろうと主張している。多くの専門家はそれに異議を唱えている。メリーランド大学の合同量子情報コンピュータ科学研究所 (Joint Center for Quantum Information and Computer Science) のアンドリュー・チャイルズ共同責任者は「ノイズは制御可能です。どの程度容認できるかを理解しさえすればよいのです」という。

グーグルの量子コンピューター開発を主導するマルティニス教授も、人々の期待をうまくいなす

必要があることを承知している。マルティニス教授のチームが使おうとしているアルゴリズムは、量子コンピューターの能力をテストするのに極めて特化したもので、何か実用的なことを成し遂げるためのものではない。「量子超越性に到達したらすぐに、私たちは量子コンピューターが本当に役に立つことができると示したくなるでしょう」とマルティニス教授はいう。✚



量子コンピューター時代も インテルが勝てるこれだけの理由

量子コンピューターの開発競争では超伝導素子が有力で、シリコン素子は時代遅れのように見られている。

しかし、シリコン素子は膨大な生産設備がすでにあることに加えて、最近では、キュービットの作成において有望であることを示す論文も発表されている。

何十年もの間シリコンチップは、あらゆる種類のコンピューティング機器の中核であった。しかし、信じがたいほど強力な新しいタイプの技術である量子コンピューターの開発競争では、他の材料にその座を譲ってしまっている。新たな進歩があれば、シリコンを今以上に魅力あるものにできるかもしれない。

理論上、シリコンは強力な次世代のコンピューターを構築する際の有力な候補になるはずだ。シリコン製コンピューター・チップの生産に適した膨大なインフラはすでにある。加えて、シリコン

ベースのアプローチを使って、キュービット、つまり量子ビットを作成する方法がすでに存在している。

キュービットは、量子コンピューターの基本となる構成要素だ。1つのキュービットは、同時に2つの状態（0と1）を取ることができ、これを「重ね合わせ」と呼ぶ。重ね合わせによって膨大な量の並列処理が可能となり、もっともパワフルな従来のコンピューターの能力を凌駕する。

しかし、シリコンベースのアプローチは、キュービットを作り出すための別の手段、たとえば極低

温まで冷やしたアルミニウムのような超伝導材料を使用する方法と比べて、今ひとつ人気がない。シリコンが敬遠されてきたのは、1つには、シリコンベースのアプローチで作るキュービットは制御が難しく、そのキュービットで構築する機械をうまく拡張できるかどうか不明だからだ。

チップの巨大企業インテルは、「スピン・キュービット」によってそうした懸念に対処できるのではないかと考えている。基本的な考えは、非常に小さいマイクロ波のパルスを使ってシリコン・デバイス上で電子のスピンを制御し、そのスピンを使って効率的にキュービットを作り出すというものだ。

学者たちはこのアプローチをより効率的にする方法を研究してきた。ネイチャー誌に2月14日に掲載された論文によると、オランダのデルフト工科大学とウィスコンシン大学マディソン校の研究者たちは、スピン・キュービットを使って2量子ビットの機械をプログラムしたという。そして、量子コンピュータの実効性のテストに通常使わ

れる、データベース検索などのいくつかのアルゴリズムの実行に成功した。

論文の著者の一人であるトーマス・ワトソン博士によると、研究チームは、機械内の「ゲート」を調整するより良い方法や、基本的な量子回路を見つけるといったことに重きを置いて研究を進めていったという。ワトソン博士は、シリコンベースのシステムによって、最終的には他のアプローチよりもっと高密度にキュービットを詰め込めるようになると考えている。キュービットは互いに近づくほど、隣接するキュービットに影響を及ぼしやすくなるので、機械の計算能力が高まるというわけだ。

しかし、重要なのはくっついていることだけではない。キュービット同士が、近くにあるものと同じように遠くのものにも影響を及ぼすことができれば、コンピューターはずっと柔軟な計算能力を持つようになるはずだ。そのことに注目したのが、プリンストン大学、ドイツのコンスタンツ大学、メリーランド州の共同量子研究所（Joint Quantum Institute）/ 米国国立標準技術研究所

(NIST) の研究者たちだ。ネイチャー誌で発表された論文では、マイクロ波の光子を使って遠隔のキュービットを連結させる方法が解説されている。

シリコンベースのキュービットがもっと真剣に検討されるようになるにはまだまだ研究が必要だが、可能性はある。シリコンベースのキュービットは超伝導キュービットよりも長い時間量子状態にとどまっているため、キュービット上でより多くの命令を実行できる。シリコンベースのキュービットは比較的高い温度でも機能するため、機能を維持させるための複雑な設備も必要ない。

これらすべてのことからインテルは、シリコンベースの技術によって、量子コンピューターを大量のキュービットに拡張することがもっと容易になると考えている。本当に役に立つ商用システムを構築するには大量のキュービットへの拡張は不可欠であり、だからこそインテルはワトソン博士のような研究者たちを支援しているのだ。さらにインテルは、自社の先進的なトランジスター技術を扱うのと同じ工場で、何千という小型のキュービットアレイを搭載するウエハーの製造を始める

ことも計画している。

もっとも、シリコンの熱烈なファンであっても、量子コンピューター開発レースの賭けで丸損しないようにしておくことには抜かりがない。インテルは超伝導キュービットも開発しているのだ。👉

(Martin Giles)

**eムックは、MITテクノロジーレビュー
有料会員限定サービスです。
有料会員はすべてのページ（残り44ページ）を
ダウンロードできます。**

ご購入はこちら



<https://www.technologyreview.jp/insider/pricing/>

No part of this issue may be produced by any mechanical, photographic or electronic process, or in the form of a phonographic recording, nor may it be stored in a retrieval system, transmitted or otherwise copied for public or private use without written permission of KADOKAWA CORPORATION.

本書のいかなる部分も、法令または利用規約に定めのある場合あるいは株式会社 KADOKAWA の書面による許可がある場合を除いて、電子的、光学的、機械的処理によって、あるいは口述記録の形態によっても、製品にしたり、公衆向けか個人用かに関わらず送信したり複製したりすることはできません。