

量子コンピュータ

藤本 康暉, 津崎 隆広

Koki FUJIMOTO, Takahiro TSUZAKI

1 はじめに

近年、コンピュータは私たちの生活に欠かせない存在になっている。コンピュータは仕事、研究、娯楽など様々な目的で使われ性能も日々向上している。しかし、成長を続けるコンピュータでも解くことができない問題が3つ存在している。

1つ目は、計算できるように問題設定できない問題である。2つ目は、問題設定はできても、それが解けないことを証明できる問題である。3つ目は、解き方がわかっても、解くのに手間のかかる問題である。

3つの問題のうち、3つ目の問題の解決策として注目されているのが、量子コンピュータである。

2 量子コンピュータ

2.1 量子とは

量子は、量子力学において原子をより細かく分けた電子、陽子、中性子または光を構成する光子などの原子よりも小さな存在である。量子は、量子力学以外の物理法則の影響を受けず、2つの異なる性質を同時に保持できる。

量子の例として、電子の特徴を Fig. 1 に示す。

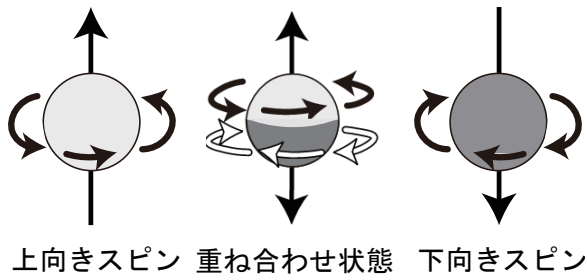


Fig.1 電子の特徴

電子はスピンと呼ばれる自転運動をしている。スピンは上向きと下向きの2種類ある。上向きのスピンは電子が左回りに、下向きのスピンは右回りに自転している。また、自転している向きには電流が流れる。電子は2種類のスピンを1つの電子に同時に保持することができる。2つの性質を同時に保持する状態を重ね合わせ状態と呼ぶ。

量子コンピュータは、電子の重ね合わせ状態を利用して、ビットを0、1の2つに加えて、0、1を同時に保持できる量子ビットを持つ。

2.2 量子ビット特徴

量子ビットはビットごとに指輪型の回路を持つ¹⁾。Fig. 2に量子ビットのイメージを示す。

各回路には電子が1つ格納されている。重ね合わせ状態

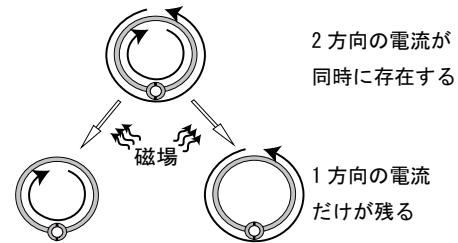


Fig.2 量子ビットのイメージ

の電子のスピンにより、回路は右回りと左回りの電流が同時に存在する状態になっている。電流の流れる向きで0、1を表現することで、0と1を同時に保持する状態を実現している。

量子ビットから0か1のどちらかの値を取り出す際は、横磁場という制御信号をかける。横磁場は回路に流れる電流のどちらか一方の回転だけを残し、1つの値を取り出すことができる。

量子コンピュータ以外のコンピュータは、3ビットの情報を表す場合、000や010のように1つの情報しか表すことができない。しかし、量子コンピュータは、量子ビットにより000から111まで、8つの全ての状態を1つのビット列で同時に扱うことができる²⁾。

2.3 方式

実用化している量子コンピュータは、量子ゲート方式と、量子アニーリング方式の2つの方式がある。2つの方式の特徴を Table 1 に示す。

Table1 開発済みの量子コンピュータの方式

	量子ゲート方式	量子アニーリング方式
開発組織	IBM 社	D-Wave 社
演算方法	1 組ずつ演算	まとめて演算
汎用性	高い	低い (最適化問題のみ)
ビット数	7 ビット	2048 ビット
開発段階	試作品を公開	商用に製品化

量子ゲート方式はあらゆる用途に対応するのを目指す方式で、家庭用パソコンとしての普及を目標にしている。

一方、量子アニーリング方式は、組み合わせ最適化問題に特化した方式で、組み合わせ最適化問題以外の演算能力は低い。ただし、量子アニーリング方式は汎用化を目指さない分、量子ゲート方式より開発が進んでいる。

2.4 利点

量子コンピュータは、他のコンピュータより速く計算することができる。特に、量子コンピュータは組み合わせ最適化問題を得意とする。

組み合わせ最適化問題とは、条件を満たす組合せの中で、最適なものを求める問題である。組み合わせ最適化問題を、毎秒 1.0×10^{16} 回計算できるスーパーコンピュータと、量子コンピュータで解くのにかかる時間を Table 2 に示す。

Table2 計算に要する時間

組み合わせ数	計算時間 (s)	
	スーパーコンピュータ	量子コンピュータ
1	1.0×10^{-16}	1.0×10^{-16}
1.2×10^2	1.2×10^{-14}	1.1×10^{-15}
3.7×10^6	3.7×10^{-10}	1.9×10^{-13}
2.4×10^{18}	2.4×10^2	1.5×10^{-7}
2.7×10^{32}	2.7×10^{16}	1.6

組み合わせ最適化問題の例として、カーナビのルート探索や、荷物の配送ルートが挙げられる。量子コンピュータは、数万、数億の組み合わせを、量子ビットによって同時に計算することができるため、組み合わせ最適化問題を短時間で解くことができる。

2.5 問題点

量子コンピュータは、優れた演算能力により他のコンピュータでは現実的に解くことができなかった問題を解くことができる。ただし、現実的に解くことができなかった問題は現在の暗号も含む。

現在の暗号は、暗号を解く鍵を求めるための計算量を膨大し、全てのパターンを調べるために、100年以上かかるようにすることで安全性を確保している。量子コンピュータは並列処理により、短時間で全ての組み合わせを求めることができるため、既存のあらゆる暗号を数時間程度で解ける。

また、量子の重ね合わせ状態は非常に不安定である。重ね合わせ状態を維持するには、回路内の電気抵抗を可能な限り0に近づける必要がある。しかし、電気抵抗を0に近づけるには、超電導状態と呼ばれる、超低温状態にしなければならない。低温状態を維持するためには冷却設備が必要となるため、膨大な運用コストが発生する。

2.6 解決策

量子コンピュータに解読できない暗号として、量子暗号が注目されている。Fig. 3に量子暗号のイメージを示す。

量子暗号では、暗号を解読するための鍵を光に変えて送る。量子は誰かに観測されると状態が変化し、元の状態に復元できない特性、不確定性原理を持つ。量子の鍵は第三者に盗聴されると、不確定性原理により量子の内容が変化し、盗聴の形跡が残る。盗聴が判明した瞬間にその回線を破棄して、新しい鍵を用意すれば、安全に鍵を送ることができる。量子暗号はコンピュータの計算能力が向上して

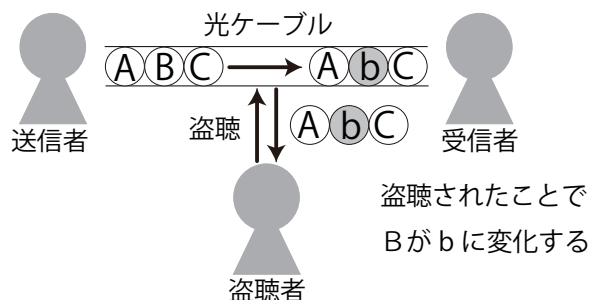


Fig.3 量子暗号のイメージ

も、盗聴の形跡が残るので、今後のコンピュータの発展にも対応できると注目されている。

また、膨大な運用コストがかかる問題の解決策として、新しい方式の量子コンピュータが研究されている。

量子コンピュータの新方式、レーザーネットワーク方式は日本で開発されている。新方式は、量子ビットに電子の代わりに光を利用する。超電導状態を維持するための冷却設備は必要ないため、新方式は常温でも稼働することができる。また、冷却設備が必要ない分、運用コストを大幅に削減できる。新方式は現在開発中であるため、試作品は存在せず、演算方法も未定である。

3 量子コンピュータに関わる最新動向

量子コンピュータは人工知能分野への応用が期待されている。

量子コンピュータの得意とする組み合わせ最適化問題は、人工知能の機械学習、ディープラーニングの処理のなかで最も時間のかかる処理である。量子コンピュータを導入することで、人工知能が最適な対応を短時間で見つけ出すことが期待されている。現在、GoogleやNasa、IBMなどの世界の大手企業は人工知能の開発に力を入れているため、量子コンピュータの開発競争を行っている。

4 今後の展望

IBM社はIBM Quantum Experienceという5ビットの量子コンピュータにクラウドを通じてアクセスできるサービスを開始している。D-Waveは約1年ごとに量子コンピュータが扱えるビットを2倍にしている。また、レーザーネットワーク式の試作品も今年に公開予定である。今後も量子コンピュータの開発、改良が急速に進むと予想される。

特に、レーザーネットワーク方式は運用コストを大幅に抑えることができ、常温でも稼働することから、家庭用のコンピュータとしての実用化も考えられる。コンピュータの革命はもう目前に迫っている。

参考文献

- 1) 西森秀稔, 大関真之, 量子コンピュータが人工知能を加速する, 日経BP社, pp14-37, 2016
- 2) 竹内 繁樹, 量子コンピュータ 超並列計算のからくり, 講談社, pp12-26, pp52, 2005