基本演算を操る量子コンピュータの真価
～ゲート型量子コンピュータの計算能力の分析～

The real worth of quantum computers with elementary operations
Anal ysisof computational powe r of gate -base dquantum compute rs

メディア情報研究部
高橋　康博 Yasuhiro Takahashi

プロフィール

NTT コミュニケーション科学基礎研究所 メディア情報研究部 主任研究員。1998年東北大学理学部数学科卒業。2000年同大学院理学研究科数学専攻博士前期課程修了。同年日本電信電話株式会社入社。2008年電気通信大学大学院電気通信学研究科情報通信工学専攻博士後期課程修了。博士（工学）。量子計算理論の研究に従事。情報処理学会、電子情報通信学会各会員。

現在のコンピュータでは実行不可能な超高速計算が、量子コンピュータでは可能になると期待されています。量子コンピュータと現在のコンピュータの大きな違いの一つは情報の表現にあります。現在のコンピュータは、0または1のどちらか一方の値をもつ「ビット」により情報を表現します。一方で、量子コンピュータにおいて情報を表現する「量子ビット」は、0または1だけでなく、例えば0が30%で1が70%というような0と1の重ね合わせを表現できます（図1）。量子ビットの個数が増えれば、より多くの状態の重ね合わせが表現できます。この重ね合わされた状態を用いた並列処理が量子コンピュータの特徴の一つです。

量子ビットを利用した情報の表現については共通ですが、様々な方式の量子コンピュータが提案されています。これまで世界で最も研究されてきた量子コンピュータをゲート型と呼びます。現在のコンピュータと同様に、解きたい問題に対し、基本演算（ゲート）の組み合わせで表現されるアルゴリズムを人間が構築し、これを実行します（図2）。言わば、基本演算を積極的に操る量子コンピュータです。一方で、近年活発に議論されているアニーリング型は、解きたい問題に依存して量子状態の遷移のおよその方向性を指定するだけであり、その後は量子状態の自然な状態遷移に任せることで、最終的に得られる状態が問題の解になることを期待します。

我々の目標は、計算能力について、現在のコンピュータに対する量子コンピュータの優位性を理論的に証明し、そのような優位性を示す量子コンピュータを実現することです。ゲート型については計算能力の理論的な分析が可能であり、現在のコンピュータより計算能力が高いという証拠が示されているため、我々はゲート型に焦点を当てています。しかし、ゲート型は他の方式と比較して、実現に要求される技術水準が高いという問題があります。本講演では、ゲート型量子コンピュータによる超高速計算の実現へのハードルを大きく下げる二つの成果を紹介します。

ゲート型の実現を難しくしている原因の一つは、複雑な重ね合わせ状態を利用することです。このような状態は外界からの影響を受けやすく、現在の技術では短時間で状態が崩壊してしまいます。この問題に対処する一つの方法は、アルゴリズムのステップ数を制限し、量子状態の崩壊前にアルゴリズムの実行を完了させることです。しかし、このような制限はゲート型量子コンピュータの計算能力を著しく低下させる可能性があるため、ステップ数を制限したゲート型量子コンピュータの計算能力の分析は重要な研究テーマになっています。

我々は論理和関数（入力ビット中に1があれば1を、そうでない場合は0を出力する関数）の計算に着目しました。これは論理和関数が少ないステップで計算できれば、様々な量子アルゴリズムが少ないステップで実行できるからです。この関数を計算する従来方法では、入力ビット数が増えるにつれてステップ数も増えます。一方で、我々は、入力ビット数に依存せず一定のステップ数でこの関数が計算できることを示しました[1]。この成果は10年来の未解決問題の解決であり、暗号の安全性の基礎となる離散対数問題を従来より少ないステップで解くことに応用できます。ステップ数を制限した状況においても、ゲート型量子コンピュータによる超高速計算が可能であることを示した成果です。

ゲート型の実現を難しくしているもう一つの原因は、0に初期化された多数の量子ビットを必要とすることです。現在の技術では、少数の初期化量子ビットしか用意できず、このような状況では意味のある問題はほとんど解けません。我々は、少数の初期化量子ビットに加え、現実的に用意しやすい未初期化量子ビット（どんな初期状態でも良い量子ビット）を使うことで計算能力が大幅に向上することを示しました[2]。初期化量子ビット数を制限した状況においても、ゲート型量子コンピュータの高い計算能力を引き出すことに繋がる成果です。

利用できる基本演算を現実的なものに制限する等、ゲート型量子コンピュータに関する検討課題は残っています。このような課題を解決し、ハードウェア研究と融合することで、ゲート型量子コンピュータによる超高速計算が実現されると考えています。また、ゲート型と他の方式との融合が、さらなる高速化を生み出すと期待しています。我々は今後もゲート型量子コンピュータの真価を明らかにする研究を続けていきます。

図1:電子スピン（ある軸についての回転）の向きを利用した量子ビット

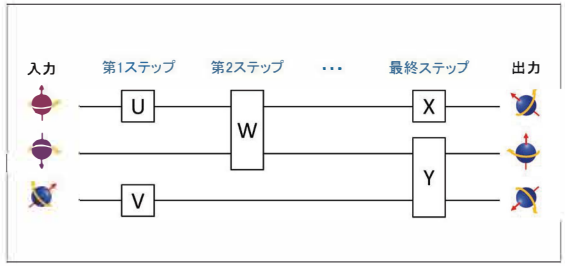

図2:ゲート型量子コンピュータにおける計算の模式図。入力量子状態に対し、基本演算（ゲート）を適用して状態を遷移させ、出力量子状態を得る

関連文献

[1] Y. Takahashi, S. Tani, "Collapse of the hierarchy of constant-depth exact quantum circuits," *Computational Complexity*, Vol. 25, Issue 4, pp. 849-881, 2016.
[2] Y. Takahashi, S. Tani, "Power of uninitialized qubits in shallow quantum circuits," in *Proc. 35th International Symposium on Theoretical Aspects of Computer Science (STACS)*, pp. 57:1-57:13, 2018.