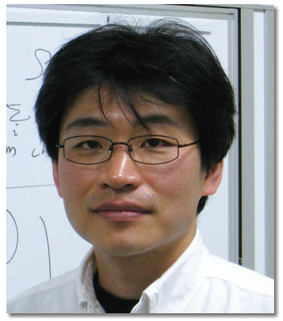
研究講演

因数分解だけではない量子計算の魅力

～量子探索技術の可能性を探る～

Quantum computing beyond integer factorization

Exploring the potential of quantum search



協創情報研究部
谷　誠一郎
Seiichiro Tani

プロフィール

NTT コミュニケーション科学基礎研究所 協創情報研究部
主任研究員(特別研究員)。
電子情報通信学会 情報・システムソサイエティ 論文賞受賞。

■現在のコンピュータと量子コンピュータ

英国の数学者Alan M. Turingにより計算機モデルが考案されて以来、コンピュータは著しい発展を遂げました。しかし、現在のコンピュータも、原理的にはTuringのモデルと同じです。これからも、この計算機モデルに基づいたコンピュータは、進歩を遂げていくでしょう。一方で、世の中で解くことが要請される問題の中には、そのような進歩を遂げてもなお、原理的に、大幅な高速化が期待できないものがあります。

量子コンピュータは、量子力学的な性質を利用した、将来のコンピュータです。Turingのモデルとは原理的に異なるため、現在のコンピュータの延長線上では解くことが難しい問題でも、高速に解くことが期待され、世界中で研究が進められています。量子コンピュータを動かすためには、現在のコンピュータと同様に、ハードウェアを動かす手順(＝アルゴリズム)が必要です。そして、アルゴリズムの善し悪しが計算速度を大きく左右するというのも、現在のコンピュータと同じです。このため、量子コンピュータのハードウェアが完成したとしても、それを用いて難しい問題を高速に解くためには、優れた量子アルゴリズムが欠かせないのです。従来のアルゴリズムは量子コンピュータ上では使えないため、優れた量子アルゴリズムを発見するための研究を行う必要があります。

■素因数分解量子アルゴリズムのインパクト

量子アルゴリズムの代表例が、素因数分解を、現在のコンピュータよりも指数倍高速に行う量子アルゴリズムです。これは、1994年にPeter W. Shor [1] によって発見されました。素因数分解は、長年の研究にもかかわらず、Turingのモデル上で高速に解く方法がいまだ見つかっていない難しい問題です。実際、インターネット等で使用されている暗号は、素因数分解の困難性を安全性の根拠としています。このため、Shorの発見は、「量子コンピュータが完成したら、現在使用されている暗号が役に立たなくなる」という意味でも非常に大きなインパクトがありました。この発見を機に、世界中で量子コンピュータの研究が盛んになったといっても過言ではありません。これまで、Shorの素因数分解アルゴリズムが、量子アルゴリズムの代表選手としてしばしば取り上げられてきたのも当然と言えます。

しかし、よく考えてみると、便利に使われている暗号が破られてしまうことは、うれしくないことです。専門的には、Shorの量子アルゴリズムの拡張もよく研究されており、素因数分解を含むもっと広範な問題群も高速に解けることが知られています。しかし、現時点では、身近な問題との関連は薄く、そのメリットを理解するのは難しいかもしれません。

■量子探索アルゴリズムとその発展

本講演では、1996年にLov K. Grover [2] が発見した、量子探索アルゴリズム(以下、量子探索)に端を発する研究領域を中心に、我々の研究成果を交えてご紹介します。このアルゴリズムが解く探索問題とは、1からのNの番号がついているN個のデータの中から所望のデータを探し出す問題です(図1)。Turingのモデルに基づくコンピュータであれば、最悪N回程度のデータアクセスが必要ですが、量子コンピュータがあれば$\sqrt{N}$回程度のデータアクセスで済ますことができます。これは、素因数分解の場合のように指数倍のスピードアップではありませんが、それでもNが巨大であれば、著しいスピードアップにつながります(図2)。探索問題の最大の特徴は、問題設定の単純さと、それゆえの応用範囲の広さにあります。実際、探索問題は、様々な問題の部分問題として現われます。この部分問題を発見し、量子探索を適用することにより、元の問題を極めて高速に(効率良く)解くことができます。 例えば、通信ネットワークの形状を最適化する際に重要な、グラフの性質検査を高速化できる事例や、あるいは、量子通信を用いた分散計算では、極めて少ない通信量で計算できる事例が知られています。これらの量子アルゴリズムの特筆すべき点は、Turingのモデルでは理論的に到達し得ない高速化・低通信量を達成しているところにあります。

■今後の展開

量子情報科学の研究は、抽象レベルから、量子回路などの実装レベル(関連展示番号09)にいたるまで、この20年間、世界中で非常に精力的に行われてきました。それでもなお、未解明な問題が数多くあります。量子コンピュータを用いて高速に解ける問題をうまく分類し、その限界を明確にするため、我々は、さらに研究を推進していきます。

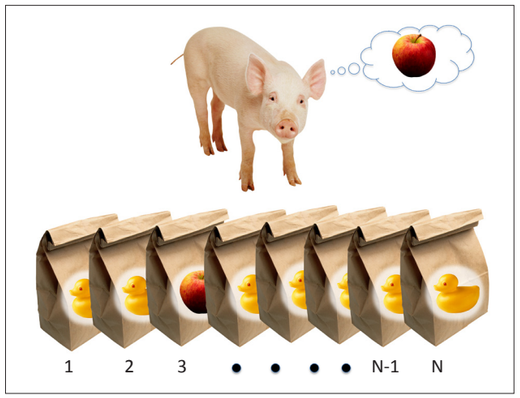


図1：探索問題のイメージ

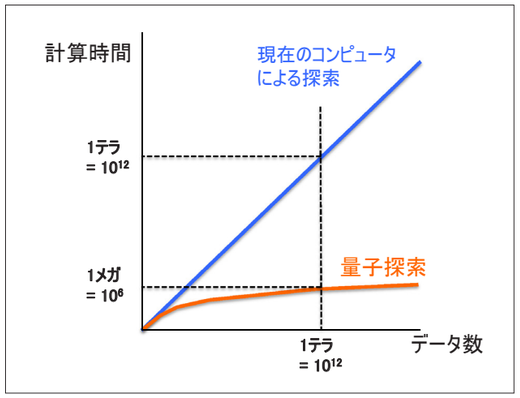


図2：探索問題を解くため要する計算時間（理論値）の比較

【関連文献】

[1] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” in *Proc. 35th Annual IEEE Symposium on Foundations of Computer Science*, pp. 124-134, 1994.
[2] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proc. 28th Annual ACM Symposium on Theory of Computing*, pp. 212-219, 1996.