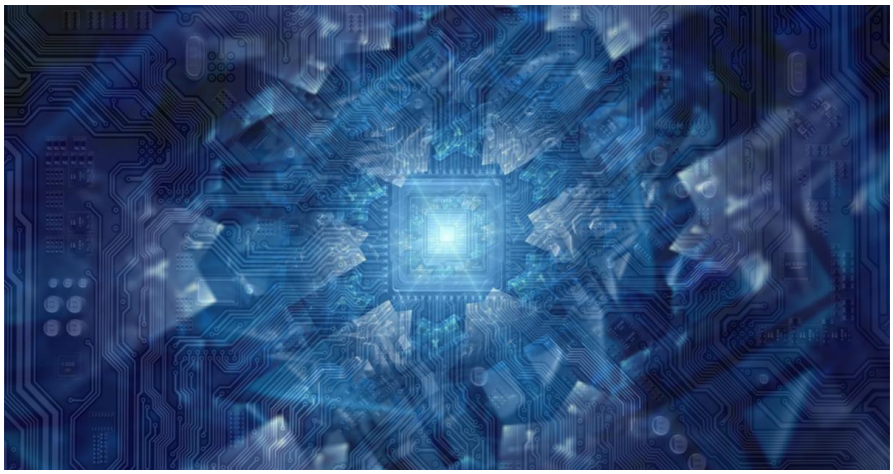


１量子ビットしか使えない量子コンピューターでも古典コンピューターより強かった

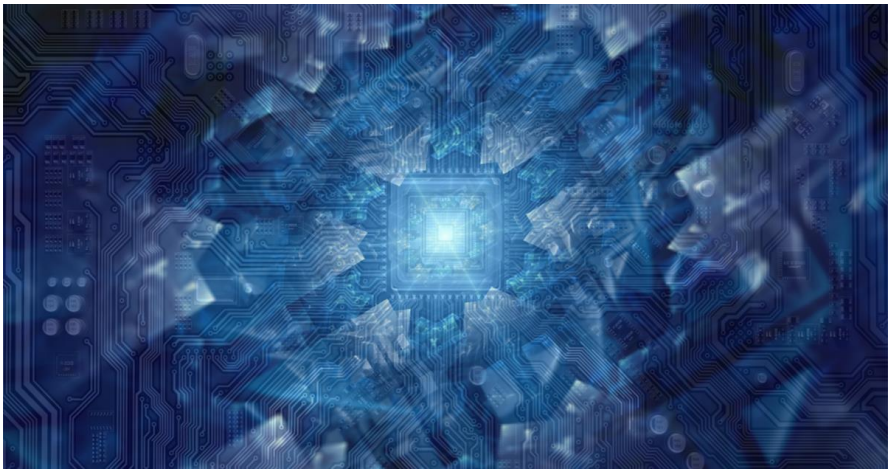
ポイント

- **実質的に１量子ビットしか使えない「弱い」量子コンピューターが、古典コンピューターよりも「強い」のかどうか不明であった。**
- **そのような弱い量子コンピューターが、ある場面では古典コンピューターより高速であることを計算量理論的基盤に基づいて証明した。**
- **現在、世界中で進んでいる量子スプレマシー研究の理論的基盤を整備する結果であり、当該分野の研究をさらに加速することが期待できる。**

概要

大量の量子ビットを自由自在に使用し、任意の量子アルゴリズムを走らせ、完全にエラー耐性のある巨大な量子コンピューターを実現することは量子計算の研究者らの究極のゴールですが、それはまだ遠い未来のことかもしれません。そこで、近い将来に実現できる技術のみで作られる「弱い」量子コンピューターでも、古典コンピューターより「強い」ことを示す理論的・実験的研究が注目を集めています。京都大学基礎物理学研究所 森前智行 講師および理学研究科 藤井啓祐 特定准教授らの研究グループは、国立情報学研究所 小林弘忠 特任研究員、名古屋大学大学院情報学研究科 西村治道 准教授、東京大学先端科学技術研究センター 玉手修平 特任助教、日本電信電話株式会社 谷誠一郎 上席特別研究員らと共同で、実質的に１量子ビットしか使えないような「弱い」量子コンピューターでも、ある場面では古典コンピューターより「強い」ことを、理論的に証明しました。また、今回発見した手法は、他のタイプの弱い量子計算モデルにも応用することができ、それらのモデルについても、従来よりも強固な計算量理論的基盤で古典コンピューターに対する優位性（量子スプレマシー）を証明しなおすことにも成功しました。

本研究成果は、日本時間 2018 年 5 月 18 日午前 1 時に米国物理学会の学術誌「Physical Review Letters」にオンライン掲載されました。



１．背景

量子コンピューターとは、ミクロの世界を説明する物理理論「量子力学」に基づいて動作するコンピューターのことです。いくつかの問題については、現在、我々が使っているコンピューター（古典コンピューター）を遥かに凌駕する超高速計算が可能であることが理論的に分かっています。現在、理論的な研究だけでなく、量子コンピューターを実現する実験的研究も世界中で行われており、大学などの研究機関以外に Google や IBM といった企業も数十量子ビットからなる量子コンピューターを実現しています。

大量の量子ビットを自由自在に扱い、任意の量子アルゴリズムを完全にエラー耐性のある状態で実行できるような巨大な万能量子コンピューターを実現することが量子計算の研究者たちの究極のゴールですが、それはまだ遠い未来のことかもしれません。そこで、小さなサイズに限定して、あるいは、万能ではなく、特定のアルゴリズムのみを走らせることを目標として、近い将来に実現できるレベルの「弱い」量子コンピューターで、古典コンピューターに対する優位性（量子スプレマシー）を示そうとする研究が盛んに行われています。

これまで、様々な「弱い」量子計算モデルが研究されてきました。例えば、相互作用の無い光の粒子を使った量子コンピューター（ボソンサンプリング）や、交換する量子ゲートのみからなる量子コンピューター、ランダムに量子ゲートが実現される量子コンピューターなどがあり、それらのいくつかは、すでに実験的に実現されていたり、あるいは近い将来に実現が目指されていたりします。中でも、「one-clean qubit モデル」と呼ばれるモデルは、1998 年に米国ロスアラモス研究所の研究者らによって提案された最も古いモデルの１つです。通常の量子計算においては、きれいに初期化された量子ビットが好きなだけ使えるという仮定をしていますが、この one-clean qubit モデルでは、きれいに初期化された量子ビットは１つしか使えません。このように、非常に制限されたモデルであるため、一見するととても弱そうに見えますが、意外なことに、結び目不変量である Jones 多項式の計算など、現在、古典コンピューターで効率的に計算する方法が知られていない量を効率的に計算できることが示されています。そのため、one-clean qubit モデルは、古典計算機よりは少し「強い」だろう、と予想されていました。

しかしながら、このような例は、one-clean qubit モデルが古典コンピューターより「強い」ことを示す証拠としては不十分です。なぜなら、単に「今のところ Jones 多項式を計算する効率的な古典アルゴリズムが知られていない」というだけで、もし将来、効率的な古典アルゴリズムが発見されれば、one-clean qubit モデルの古典コンピューターに対する優位性が無くなってしまいます。近年、「多項式階層の無限性」と呼ばれる

より強固な計算量理論的基盤に基づいて、one-clean qubit モデルの古典に対する優位性が理論的に証明されました。しかし、この証明では出力量子ビットを 3 つ以上測定する必要があるため、1 量子ビットしか測定できない本来の one-clean qubit モデルでも量子スプレマシーが出るかどうかは、この 20 年間未解決の問題として残されていました。

２．研究手法・成果

本研究では、one-clean qubit モデルにおいて、1 量子ビットの測定のみでも量子スプレマシーが得られることを初めて理論的に証明しました。これにより、20 年来の未解決問題が初めて解かれたことになります。証明には、従来とは全く違う新しい手法が用いられました。従来の証明には postBQP という計算量クラスを利用していたため、事後選択用と結果出力用に最低 3 つの量子ビットを測定する必要がありました。今回は NQP という NP の量子版を使うことにより、 1 つの量子ビットの測定のみで十分になりました。

さらに、今回の新しい手法は、これまで研究されてきた他の弱い量子計算モデル（相互作用無しの光粒子量子コンピューター、交換するゲートのみからなる量子コンピューター、ランダムゲートからなる量子コンピューター）にも応用することができ、これらのモデルの量子スプレマシーを、従来より強い計算量理論的基盤で証明しなおすことにも成功しました。従来の結果は、「もし、このモデルが古典計算機で効率的にシミュレートできたら多項式階層が第三レベルで崩壊する」というものでしたが、今回は「もし、このモデルが古典計算機で効率的にシミュレートできたら多項式階層が第二レベルで崩壊する」に改良することができました。多項式階層とは P と NP を一般化したものであり、P=NP が信じられていないように、多項式階層の崩壊も計算機科学においては信じられていません。また、第二レベルでの崩壊の方が第三レベルでの崩壊よりも、より P=NP に近く、より起こりにくそうであると考えられています。したがって、今回の結果は、従来の結果よりも、より強固な計算量理論的基盤で量子スプレマシーを証明していることになっています。

３．波及効果、今後の予定

現在、世界中で多くの研究者が量子スプレマシーの実現にむけて研究を行っています。本研究は、それらの理論的基盤を整備するものであり、今後の量子計算の理論的、実験的研究の発展に大きく寄与すると期待できます。また、量子スプレマシーの研究は、単に古典に対する優位性を示すだけでなく、有用な量子アルゴリズムの開発につながることも目指しています。one-clean qubit モデルを使った高速な量子アルゴリズムを開発するのは、今後の重要な課題です。

４．研究プロジェクトについて

本成果は、以下の事業・研究領域・研究課題による支援を受けて行われました。

- 科学技術振興機構（JST） 戦略的創造研究推進事業（CREST）「冷却原子の高度制御に基づく革新的光格子量子シミュレーター開発」（課題番号：JPMJCR1673）
- 科学技術振興機構（JST） 戦略的創造研究推進事業（さきがけ）研究領域「量子の状態制御と機能化」研究課題名「知的量子設計による量子計算・量子シミュレーションの新機能創出」（課題番号：JPMJPR1668）
- 日本学術振興会（JSPS） 基盤研究（A）研究課題名「孤立量子多体系における熱力学第二法則」（課題番

号：16H02211）
- 科学技術振興機構（JST） 戦略的創造研究推進事業（ERATO）「中村巨視的量子機械プロジェクト」（課題番号：JPMJER1601、研究総括：中村泰信）
- 科学技術振興機構（JST） 戦略的創造研究推進事業（ACT-I）研究領域「情報と未来」研究課題名「古典検証者によるセキュアクラウド量子コンピューティング」（課題番号：JPMJPR16UP）
- 科学技術振興機構（JST） 戦略的創造研究推進事業（さきがけ）研究領域「量子の状態制御と機能化」研究課題名「セキュアクラウド量子計算における量子スプレマシー」（課題番号：JPMJPR176A）
- 文部科学省（MEXT） 新学術領域「多面的アプローチの統合による計算限界の解明」研究課題名「量子力学からの計算限界解明へのアプローチ」（課題番号：24106009）、研究課題名「計算量的仮定に基づくノンユニバーサル量子計算の研究 -SBQP と多項式階層」（課題番号：15H00850）
- 日本学術振興会（JSPS)若手研究（B)研究課題名「量子対話型証明とハミルトニアンに基づく検証つきセキュアクラウド量子計算」（課題番号：17K12637）
- 日本学術振興会（JSPS） 基盤研究（A）研究課題名「量子論の基礎原理に関する数学的研究」（課題番号：26247016）
- 日本学術振興会（JSPS）基盤研究（A）研究課題名「量子プロトコル理論の線的展開」（課題番号：16H01705）
- 日本学術振興会（JSPS） 基盤研究（C）研究課題名「量子通信及び量子計算を限定した量子対話型証明の解析」（課題番号：16K00015）

＜用語解説＞

古典コンピューター：我々が現在使っている古典力学に基づいて動作するコンピューター。計算の基本単位をビットとし、それぞれのビットが 0 か 1 のどちらかの状態をとることによって、2 進数で演算を行う。なお、本稿でいうコンピューターの「強い」「弱い」とは、計算能力・速度の相対的な差を指す。

量子アルゴリズム：量子コンピューター上で用いるアルゴリズム。アルゴリズムとは、コンピューターが問題を計算する方法や手順をいう。

量子ビット：通常のコンピューターでは 0 と 1 のビットを使って情報をエンコードするが、量子ビットとは、0 と 1 の量子力学的重ね合わせも可能となるようなビットのこと。

計算量理論：計算に要するリソース（時間、メモリ、通信量など）について研究する学問分野。

量子ゲート：量子ビットを操作するゲート演算。

量子ビットの初期化：量子ビットを 0 の状態にすること。

Jones 多項式：ひもを「切らずに」動かす操作について、不変な量、すなわち同じ結び目には同じ値を対応させるものを結び目不変量という（結び目が同じとは、ある二つの結び目について、切らずに連続的に変形させた結果、一方を他方に重ね合わせることができる状態をいう）。Jones 多項式は、この結び目不変量の一例で、1984 年に数学者ヴォーン・ジョーンズが発見した。統計力学や量子論など数学・物理学のさまざまな分野と関係があることが分かり、研究されている。

多項式階層の無限性と崩壊：多項式階層とは、P と NP（下記解説を参照）の関係を一般化して得られる階層のことであり、P=NP が信じられていないように、計算機科学の分野では、多項式階層は崩壊しないと信

じられている（多項式階層の無限性）。P=NP は第ゼロレベルの崩壊に対応している。第三レベルでの崩壊よりも第二レベルでの崩壊の方がより起こらなさそうであると考えられている。

P：入力のサイズに対し多項式時間で古典計算機によって解くことのできる判定問題（yes か no で答えることのできる問題）の集合。つまり、古典計算機で「簡単に」解ける判定問題の集合。

NP：解が正しいことを検証することが多項式時間でできる判定問題の集合。例えば、全ての都市を一回だけ巡って戻ってこられるようなルートは存在するか？という問題は、全てのパターンをしらみつぶしに調べると膨大な時間（指数時間）がかかるため、自分でルートを発見するのは簡単ではなさそうであるが、もし仮にそのようなルートを教えてもらえれば、その正しさは容易に検証できる。P に属する問題は当然 NP に属すが、両者が一致する（P=NP）ことはないと信じられている。

postBQP：事後選択を可能とする量子計算機が多項式時間で解ける判定問題の集合のこと。

＜論文タイトルと著者＞

タイトル： Impossibility of classically simulating one-clean-qubit model with multiplicative error

著者：Keisuke Fujii, Hirotada Kobayashi, Tomoyuki Morimae, Harumichi Nishimura, Shuhei Tamate, and Seiichiro Tani

掲載誌：Physical Review Letters

DOI：10.1103/PhysRevLett.120.200502