公開

研 究 終 了 報 告 書

「定数時間量子アルゴリズムの設計」

研究期間： 2018 年 10 月～2022 年 3 月
研 究 者： 森 立平

1．　研究のねらい

量子コンピュータ開発の進展はここ数年大変めざましく、実用的な量子コンピュータの実現は現実味を帯びてきた。量子コンピュータを現実的に活用するためには近い将来実現するような、能力が制限された量子コンピュータで動作する量子アルゴリズムの開発が必要不可欠である。そのような問題意識に基づき、本研究課題では定数時間で動作するような量子アルゴリズムを開発することを目的とする。特に従来の量子アルゴリズム開発では用いられてこなかった理論計算機科学の道具(論理関数のフーリエ解析など)を用いて定数時間量子アルゴリズムの開発をする。

また、近い将来実現するような、能力が制限された量子コンピュータが現在の洗練された古典コンピュータにできないような計算ができること(量子超越性)を理論的に証明することは理論的にも現実の量子コンピュータ開発の指針としても非常に重要である。理論的な立場から量子超越性を証明することもまた本研究課題の目的である。

2．　研究成果

（1）概要

本研究課題の研究成果を大きく 3 つの小テーマに分けて説明する。

(A). 非適応的測定型量子計算

測定型量子計算は万能な量子計算能力を持つことが知られている量子計算のモデルである。測定型量子計算ではグラフ状態と呼ばれる量子状態を用意し、それを 1 qubit ずつ順番に測定していく。この時、各測定はそれまでの測定結果に依存して決める。そうすることで、最終的にゲート型の量子計算の計算結果と同じ量子状態を生成することができる。ここで、各 qubit の測定は一般的にそれまでの測定結果に依存しているため、同時に測定することはできない。これを同時測定することにすれば、量子状態を保持する時間は qubit 数に依存しない定数時間で済むことになる。この計算モデルを非適応的測定型量子計算と呼ぶ。本研究では非適応的測定型量子計算の中でもベルの不等式などの非局所性ゲームに関連する量子計算モデルに注目し、その計算能力を特徴付けることに成功した。

(B). 量子動的計画法

最近 Ambainis らによって巡回セールスマン問題等の NP 困難な問題に対する量子アルゴリズムが開発された。この量子アルゴリズムは指数時間かかるものであるが、現在知られている最速の古典アルゴリズムと比べて多項式の高速化がなされている。この量子アルゴリズムは動的計画法と呼ばれる古くから知られている古典アルゴリズムを高速化するものである。本研究ではこのアイデアに基づき、よく知られている NP 困難な問題であるグラフ彩色問題を解く量子アルゴリズムを開発した。グラフ彩色問題に対して現在知られている最速の古典アルゴリズムよりも高速な量子アルゴリズムを初めて示した。

(C). ランダム量子回路の量子超越性

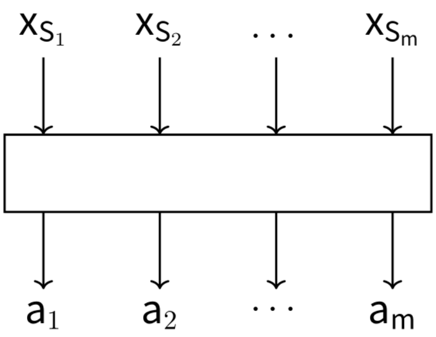
最近 Google によって 53 qubit の量子コンピュータが開発され、ランダムな量子回路を実行するタスクを高速に解いた。また、同様のタスクを古典コンピュータで解くと 1 万年かかるため、量子超越性が達成されたと主張した。この主張を裏付けるためにランダム量子回路のシミュレーションが古典コンピュータにとって本当に困難な問題であることを理論的に示すことを目標に研究した。その結果、ランダム量子回路の出力確率をある程度の誤差で近似する問題が古典コンピュータにとって困難であることを示すことができた。この結果は理論計算機科学の最高の国際会議である FOCS 2021 に採択された。

（2）詳細

(A). 非適応的測定型量子計算

非適応的な測定型量子計算に排他的論理和を計算する弱い計算機を付加した量子計算モデルの計算能力について研究した。これはベルの不等式で用いられる CHSH ゲーム等の XOR ゲームのプロトコルを量子計算モデルと見なしたものである。この量子計算モデルでは入力の部分集合の排他的論理和に従って、あらかじめ用意したグラフ状態を同時測定し、その測定結果の排他的論理和を計算結果とする(図 1)。

$$\text{For } S \subseteq \{1,2,\dots,n\}, \quad x_S := \bigoplus_{i\in S} x_i.$$



$$\bigoplus_{i=1}^{m} a_i = f(x_1,\dots,x_n)$$

図 1 非適応的量子計算の計算モデル

この計算モデルの複雑さは使用する qubit の数である。理論計算機科学で用いられる論理関数のフーリエ解析を用いることで、この量子計算モデルで必要な qubit 数の下界を導出した。また、比較的簡単に示すことができる上界と合わせることで、与えられた論理関数の計算に必要な qubit 数の精密な上下界を得ることができた。その結果、「この量子計算モデルで効率的に計算できる ⇔ 論理関数を F2-多項式として表したときの次数が低い」という特徴付けを得ることができた(主な研究成果リスト 3)。この結果は理論計算機科学の高度な道具を用いたからこそ得られたものである。また、この量子計算モデルを 2 段にすることで、多数決関数など、F2-多項式としての次数が高い論理関数も効率的に計算できることを証明した。

(B). 量子動的計画法

最近 Ambainis らによって開発された巡回セールスマン問題に対する量子アルゴリズムは古典の動的計画法に対して非自明な方法で Grover のアルゴリズムを適用するものであった。本研究では良く知られた NP 困難な問題であるグラフ彩色問題に対する量子ルゴリズムを開発した。グラフ彩色問題とは与えられたグラフの頂点にある条件を満たすように色を塗る問題である。ここで条件とは「辺で接続された頂点は異なる色で彩色しなければならない」というものである。この条件を満たすグラフの例を図 2 に示す。

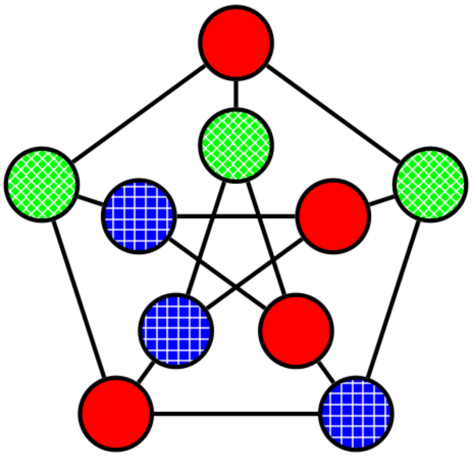


図 2 グラフ彩色の例

このようなグラフ彩色に必要な色の数の最小値(彩色数)を求めるのがグラフ彩色問題である。上記のグラフの例の場合、3 色で塗ることができるが 2 色で塗ることはできないので、彩色数は 3 である。このグラフ彩色問題を解く、現在最速の古典アルゴリズムの計算量は $\tilde{O}(2^n)$ である。ここで n はグラフの頂点数である。本研究では Grover のアルゴリズムを非自明な方法で用いることにより $\tilde{O}(1.914^n)$ 時間の量子アルゴリズムを導出した(主な研究成果リスト 2)。グラフ彩色問題に対して古典アルゴリズムよりも高速な量子アルゴリズムを初めて示したことになる。

また、一方で Ambainis らの考えた hypercube 上の動的計画法に対する量子アルゴリズムを一般化し、hyperlattice 上の動的計画法を解く量子アルゴリズムの解析をした。この量子アルゴリズム自体は Ambainis らの量子アルゴリズムの自然な一般化であり、特筆するよなものではないが、その計算時間の解析は遥かに複雑である。我々は解析的組み合せ論で用いられる鞍点法を使うことによってその複雑な解析を行い、量子アルゴリズムの計算時間を精密に解析した。私が知る限り、この鞍点法が量子情報の分野で用いられた例はこれまでにない。その結果、hyperlattice 上の動的計画法に対しても量子アルゴリズムは古典アルゴリズムよりも高速であることが分かった。この結果は 2020 年の 2 月から 3 月にかけて、さきがけの研究費で招聘したラトビア大学の Jevgēnijs Vihrovs とその他の研究者との共同研究である。Jevgēnijs Vihrovs とはその後も交流は続いており、これからも共同研究を続ける予定である。

(C). ランダム量子回路の量子超越性

最近 Google は 53 qubit の量子コンピュータを開発し、ランダムな量子回路を実行する計算タスクを高速に解いたと主張した。また、同様の計算は古典計算機で1万年かかると主張した。一方、IBM はすぐに反論をし、現在最高のスーパーコンピュータであれば 2.5 日で計算ができると主張した。IBM が想定する一般的なシミュレーション方法では 1 qubit 増えると必要なメモリが倍になる。そのため、qubit の数が 1つか2つ 増えると IBM の反論は成立しなくなる。一方で何か他の方法で効率的に古典シミュレーションができるのではないか？という疑問がある。そこで、ランダム量子回路の出力のサンプリング問題が古典コンピュータにとって本当に困難な問題であることを証明することを研究の目標とした。この目標はまだ完全には達成されていないが、関連する結果としてランダム量子回路の出力確率の近似計算が古典コンピュータにとって困難であることを理論的に示すことができた（主な研究成果リスト 1)。この結果は理論計算機科学の最高の国際会議である FOCS 2021 に採択された。

任意に与えられた量子回路の出力確率の近似計算が古典コンピュータにとって困難であることは先行研究によって証明されている。この研究ではランダムな量子回路の出力の近似計算をすることができると仮定すると任意に与えられた量子回路の出力確率の近似計算ができることを示すことで、ランダム量子回路の問題の古典的困難性を証明した。ランダムな量子回路の出力確率から任意に与えられた量子回路の出力確率を近似するために多項式補間の手法を用いた。これは先行研究でも用いられているアイデアである。ランダムな量子回路の出力確率と任意に与えられた量子回路の出力確率が同一の多項式上の点となるように多項式を設計し、ランダムな量子回路の出力確率に基づいて多項式を推定するという手法である。

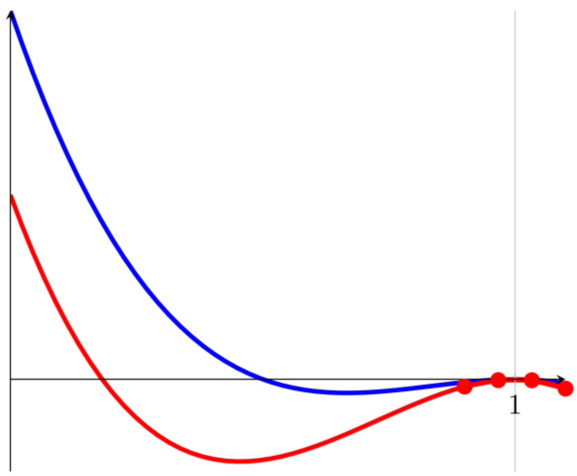


図 3 多項式補間によって増幅される誤差

図 3 に示す上側の曲線が真の出力確率を表す多項式である。この多項式は 1 付近ではランダム量子回路の出力確率に対応する。一方で 0 では任意に与えられた量子回路の出力確率に対応する。この 1 付近の値に基づいて 0 での値を推定する必要があるが、ランダム量子回路の出力確率は近似的に得られるために、1 付近の値には誤差がある。この誤差

を含む値に基づいて 0 での値を推定すると、その誤差は大きなものになる。図 3 の下側の曲線が誤差を含む値に基づいて補間された多項式である。この誤差の大きさの精密な上界を導出したことが技術的には主な貢献である。
この研究は修士学生の近藤泰大と IBM と MIT に所属する研究者である Ramis Movassagh との共同研究である。Ramis Movassagh は非常にパワフルな研究者であり、今も共同研究が続いている。

3．　今後の展開

(A). **非適応的測定型量子計算**

この量子計算モデルはかなり現実的なものであり、GHZ 状態と呼ばれる量子状態さえ作ることができれば、後は 1 qubit 毎独立に同時測定すればよいだけである。しかし、計算能力はあまり高くないので、この量子計算モデルを応用する必要がある。私の研究(主な研究成果リスト 1)より、この量子計算モデルを 2 段に重ねると計算能力が上昇し、多数決関数などの F2-多項式としての次数が大きな論理関数も効率的に計算ができることが証明されている。これらの知見を用いて、大きなサイズの GHZ 状態を生成する問題と平行して、理論の面から重要なアプリケーションを見つけることが必要である。また、GHZ 状態以外の生成しやすいグラフ状態を用いる研究も有望だと考えている。実現のためのタイムスパンは 10～20 年と推定する。

(B). **量子動的計画法**

量子動的計画法のアルゴリズムは Grover のアルゴリズムと QRAM を用いるために、実現にはかなりの時間がかかると思われる。QRAM については計算時間とのトレードオフがあると考えられ、QRAM の使用量が少ない量子アルゴリズムの研究がこれからされていくと考えられる。実現のためのタイムスパンは 30 年以上と推定する。

(C). **ランダム量子回路の量子超越性**

ランダム量子回路の出力結果のサンプリング自体は、大きな誤差を含むものではあるが、既に Google によって実装されている。まだ、この問題の量子超越性を理論的に証明することができていないが、仮に証明できたとして、その量子超越性を達成する大きさの誤差でランダム量子回路の出力をサンプリングすること自体は数年以内にできるかもしれない。どちらかというと理論的な量子超越性の証明の方に時間がかかると考えている。

4．　自己評価

本研究課題で得られた 3 種類の研究成果のそれぞれは良い結果であると考えている。特に(C). **ランダム量子回路の量子超越性**の研究は理論計算機科学の最高の国際会議である FOCS 2021 に採択されている。一方で当初の研究課題であった「定数時間量子アルゴリズムの設計」という目標に完璧に合致しているものは(A). **非適応的測定型量子計算**だけで、他の 2 つは関連はあるものの少しずれたものになっている。本来の目標に完璧に合致している (A) の研究をもっと進められればよかったと反省している。実際に (A) は私自身、理論と社会的意義の両面から強く興味を持っている問題である。社会・経済への波及効果

という意味でも（A）の研究の重要性を感じている。さきがけの研究期間では萌芽的な研究で終わってしまったが、これからも（A）の研究を続けてブレイクスルーを生み出したい。

(B). 量子動的計画法 が社会的に実装されるには時間がかかると考えられるが、結果自体はインパクトがあるものなので、この研究分野の発展には寄与していると考えている。これからもこの手法を発展させた様々な量子アルゴリズムが開発され、量子コンピュータ実現の期待を後押しするものと考えている。(C) の研究はアルゴリズムや計算モデルを開発するものではないが、現実に達成された実験結果の重要性を理論的に保証するという意味で、社会への影響は大きいと考えている（Google の量子超越性の発表が社会的にも注目されたことからも明らかであろう）。

5．　主な研究成果リスト

（１）代表的な論文（原著論文）発表

研究期間累積件数：4 件

1. Y. Kondo, R. Mori, and R. Movassagh, “Improved robustness of quantum supremacy for random circuit sampling,” accepted for the publication in the Proceedings of IEEE Symposium on Foundation of Computer Science (FOCS) 2021.
ランダム量子回路の出力確率の近似計算が古典コンピュータにとって困難であることを計算量的な仮定から示した。より正確なステートメントは以下のものである。あるアーキティクチャ（量子回路のゲートの配置だけを指定して、実際に配置されるゲートは指定しないもの）が存在して、そのアーキティクチャ上のランダム量子回路の出力確率を加法的誤差 $\exp(-\Omega(m \log m))$ で計算することは #P 困難である。ここで m は量子回路のゲート数である。
2. K. Shimizu and R. Mori, “Exponential-time quantum algorithms for graph coloring problems,” in the Proceedings of Latin American Theoretical Informatics (LATIN), LNCS, 2020, vol.12118, Springer, Cham, pp.387-398.
よく知られている NP 困難問題であるグラフ彩色問題に対する量子アルゴリズムを開発した。従来知られている最速の古典アルゴリズムの計算量が 2^n 程度であることに比べて、この論文で示された量子アルゴリズムは 1.914^n 時間で n 頂点のグラフ彩色問題を解くことができる。これは QRAM を使う量子アルゴリズムであるが、QRAM を用いない量子アルゴリズムでもグラフ 20-彩色問題が $(2-\varepsilon)^n$ 時間で解けることも示した。
3. R. Mori, “Periodic Fourier representation of Boolean functions,” Quantum Information & Computation, 2019, vol.19, no.5&6, pp.0392-0412.
ある種の非適応的量子計算のモデルの計算能力について明らかにした。理論計算機科学で用いられる論理関数のフーリエ解析を拡張し、周期的フーリエ表現という概念を導入した。それを用いて「この量子計算モデルで効率的に計算できる ⇔ F2-多項式として表したときの次数が小さい」という特徴付けを得た。また、この量子計算モデルを 2 段にすることで多数決関数などの F2-多項式としての次数が大きい関数が効率的に計算できることを示した。

（２）特許出願

なし

研究期間全出願件数:0 件(特許公開前のものも含む)

(3)その他の成果(主要な学会発表、受賞、著作物、プレスリリース等)

国際ワークショップ主催 (2 件)

Workshop on Quantum Algorithms and Lower Bounds 2020, 2 月 13-14 日.
http://q.c.titech.ac.jp/QAL20

Workshop on Quantum Algorithms and Lower Bounds 2021, 9 月 21-22 日.
http://q.c.titech.ac.jp/QAL21