

科学研究費助成事業 研究成果報告書

平成 26 年 5 月 26 日現在

機関番号：11301

研究種目：挑戦的萌芽研究

研究期間：2011～2013

課題番号：23650001

研究課題名(和文)量子力学に基づく新しい計算モデルの構築に向けて

研究課題名(英文)Towards construction of a new computation model based on quantum mechanics

研究代表者

田中 一之(Tanaka, Kazuyuki)

東北大学・理学(系)研究科(研究院)・教授

研究者番号：70188291

交付決定額(研究期間全体)：(直接経費) 2,800,000円、(間接経費) 840,000円

研究成果の概要(和文)：本研究は、従来の量子計算機とは異なった測定ベースの量子力学的計算モデルを提案して、その計算能力や計算効率について、旧来の計算モデルと比較しながら計算理論的に考察することを主題としている。とくに、深さ固定の多項式サイズ量子回路において、非有界なファンアウト・ゲートを加えると多項式時間での古典模倣ができなくなる場合があることを示した。また、無限次元状態空間における観測量の測定によって計算可能集合たちを表す新しい量子計算機について考察した。

研究成果の概要(英文)：In this research, we consider new measurement-based quantum computation models, and study their classical simulability and complexity effects. Among others, we show that some constant-depth quantum circuits followed by unbounded fan-out gates can not be classically simulated in polynomial time. We also propose a new type of quantum computer which represents computable sets via the measurement of an observable in an infinite dimensional state space.

研究分野：総合領域

科研費の分科・細目：情報学・情報学基礎

キーワード：量子計算論

1. 研究開始当初の背景

1980年頃に Benioff らがその概念を導入して以来、量子計算機は古典的な計算機よりも効率よく計算を行えるものとして、理論と実験両面から多くの研究がなされてきた。その発展において様々な種類の量子計算モデルが導入されているが、そのほとんどは量子チューリング機械や量子回路のように、よく知られた古典的仕組みの直接的な量子化である。これらの計算モデルでは、有限次元の量子系において、ユニタリ的時間発展を基本操作と考え、それらの操作の最後に観測によって得られる量子情報を古典的情報に置き換えて出力する。ところが、このような量子コンピュータの計算では、観測のみを繰り返し行うことによって実現できることがわかり、2000年あたりから測定ベースの量子計算が盛んに研究されるようになった。ユニタリ的時間発展と異なって、一般に観測は不可逆的現象であるから、測定ベースの計算モデルは量子的情報を維持しない「単方向」のものである。また、自然に対応する古典的計算モデルを持たないという意味でも非常に興味深い。

量子情報技術の進歩は昨今目覚ましいものがあるが、アルゴリズムもしくは計算量の観点においては、Shor の多項式時間因数分解 (1994) と Grover の検索アルゴリズム (1996) 以来際立った進展はないようにも見える。とくに、量子計算の計算量に関する問題は定式化さえも難しいものが多く、より一般的な枠組みで問題を立て直して検討することが解決につながる可能性がある。そのため量子計算機と古典計算機の計算能力の差を厳密に理解することが当面有力なアプローチとなるだろう。近年、定数深さの量子回路や可換量子回路のような、極めて単純な量子計算機の計算過程でさえ、古典計算機により模倣可能でないことがわかってきており、このようなモデルの性質を調べ、その拡張について考えることは、単に個別の問題の解決に留まらず、広く量子計算一般に対する新たな知見を得ることにつながるだろう。

2. 研究の目的

本研究は、従来の量子計算機とは異なる測定ベースの量子力学的計算モデルを提案し、その計算能力や計算効率について、旧来の計算モデルと比較しながら計算理論的に考察することを目的としている。

量子計算機と古典計算機の計算能力の差を厳密に理解することは量子情報処理研究における重要な問題の1つである。このような差を理解するための自然なアプローチは、量子計算機の計算過程が古典計算機により多項式時間で模倣可能かどうかを調べることである。深さ固定の多項式サイズ量子回路において、一連の単一キュービット測定を許せば、古典計算による模倣は一般に多項式時間では困難だが、唯一の単一キュービット測

定では古典計算による模倣も多項式時間でできることが知られている。しかし、後者に非有界なファンアウト・ゲートを加えた場合の古典模倣の困難さについては知られていなかった。古典模倣が多項式時間でできる量子回路とできない量子回路の壁を論理的に明らかにすることにより、量子計算の計算複雑さとアルゴリズム一般に対しても新しい知見を得ることが期待できる。

3. 研究の方法

量子計算機と古典計算機の計算能力の差を理解するための1つの自然なアプローチは、量子計算機の計算過程が古典計算機により多項式時間で模倣可能かどうかを調べることである。近年、定数深さ量子回路や可換量子回路のような、極めて単純な量子計算機の計算過程でさえ、古典計算機により模倣可能でないことが示されている。我々は、定数深さ量子回路の古典模倣可能性に焦点を当てる。2004年、Terhal らは高々2量子ビット上のゲートからなり、多項式個の出力量子ビットをもつ定数深さ量子回路が古典模倣可能でないことを示した。一方、出力量子ビットが1つの場合は古典模倣可能であることが示されている。一般に、小さい深さの回路研究では、非有界ゲートの存在と計算能力との関係が議論されるが、出力量子ビットが少ない場合の定数深さ量子回路において、非有界ゲートの存在が古典模倣可能性に与える影響は調べられていない。

そこで我々は、出力量子ビットが1つの定数深さ量子回路を考える。ただし、量子回路は、高々2量子ビット上のゲートに加え、非有界トフォリゲート(論理積ゲート)と非有界ファンアウトゲート(コピーゲート)を利用できるとする。このようなゲートは、定数深さ量子回路の計算能力を調べる研究において用いられるゲートである。そして、非有界トフォリゲートをもつ定数深さ量子回路が古典模倣可能かどうかを調べる。

4. 研究成果

我々は、BQP が PH に含まれないという自然な仮定の下で、1つの非有界トフォリゲートをもつ定数深さ量子回路は、弱い意味でさえ古典模倣可能でないことを示した。弱い意味での古典模倣とは、量子回路の出力確率分布に近い確率分布を古典計算機により多項式時間で生成することである。また、我々は、 $P=PP$ でないという自然な仮定の下で、2つの非有界ファンアウトゲートをもつ定数深さ量子回路は、強い意味での古典模倣が可能でないことを示した。強い意味での古典模倣とは、量子回路の出力確率を古典計算機により多項式時間で近似的に計算することである。

出力量子ビットが1つの定数深さ量子回路が非有界ゲートを含まなければ、上で述べたように、(強い意味で)古典模倣可能である。

従って、我々の成果は、非有界ゲートの存在という観点から、量子計算機と古典計算機の境界を明確にしたものである。

非有界ゲートを認めた定数深さ量子回路の古典模倣可能性については今まで調べられていない。たった1つの非有界トフォリゲートまたは2つの非有界ファンアウトゲートの存在を認めるだけで、古典模倣可能でなくなるという成果はいくぶん直観とは反するもので、興味深い。現実的な量子計算機を構築するには、短時間で量子ビットの状態が崩壊してしまう、いわゆるデコヒーレンス問題に対処する必要があるが、定数深さ量子回路はこのような問題に対処するのに有用であり、現実的にも意味があるモデルである。古典模倣可能性の定義において、古典計算機による指数関数的に小さい模倣誤差のみを認めていて(他の従来研究も同様であるが)強すぎる定義のように見える。多項式的に小さい誤差の扱いについて検討すべきだろう。

[今後の課題] 最も検討したい問題は、古典模倣可能性の定義を見直した上で定数深さ量子回路の古典模倣可能性を再検討することである。例えば多項式的に小さい模倣誤差を認める古典模倣可能性の定義の上で検討したい。また、定数深さ量子回路をある意味でより単純化したモデルである可換量子回路の古典模倣可能性について、今回の研究で得られた証明方法を応用しながら検討したい。より弱い古典模倣可能性の定義の下で、より単純な量子回路の古典模倣の困難さを明確にしていきたい。また、無限次元状態空間における観測の測定によって計算可能集合たちを表現する新しい量子計算機の構想については、すべての計算的枚挙可能集合がこれで表せることがまだ証明できておらず、この問題を解決することが今後さらに重要な課題になる。

5. 主な発表論文等

(研究代表者、研究分担者及び連携研究者には下線)

[雑誌論文](計 8件)

Y. Takahashi, T. Yamazaki and K. Tanaka, Hardness of Classically Simulating Quantum Circuits with Unbounded Toffoli and Fan-Out Gates, Quantum Information and Computation, 査読有, 14 巻, 2014 年, 1149-1164, <http://www.rintonpress.com/journals/qiconline.html#v14n910>

C. S. Calude and K. Tadaki, Spectral representation of some computably enumerable sets with an application to quantum provability, Lecture Notes in Computer Science, 査読有, 7956 巻, 2013 年, 43-54, 10.1007/978-3-642-39074-6_6

Y. Takahashi, T. Yamazaki and K. Tanaka,

Hardness of Classically Simulating Quantum Circuits with Unbounded Toffoli and Fan-Out Gates, Lecture Notes in Computer Science, 査読有, 8087 巻, 2013 年, 801-812, 10.1007/978-3-642-40313-2_70

N. Peng, K. Higuchi, T. Yamazaki and K. Tanaka, Relative randomness for Martin-Loef random sets, Lecture Notes in Computer Science, 査読有, 7318 巻, 2012 年, 581-588, 10.1007/978-3-642-30870-3_58

K. Yoshii and K. Tanaka, Infinite games and transfinite recursion of multiple inductive definitions, Lecture Notes in Computer Science, 査読有, 7318 巻, 2012 年, 374-383, 10.1007/978-3-642-30870-3_38

K. Tadaki, Fixed point theorems on partial randomness, Annals of Pure and Applied Logic, 査読有, 162 巻, 2012 年, 763-774, 10.1016/j.apal.2011.09.018

K. Tadaki, Phase transition between unidirectionality and bidirectionality, Lecture Notes in Computer Science, 査読有, 7060 巻, 2012 年, 203-223, 10.1007/978-3-642-27654-5_16

Ahmad Termimi Ab Ghani and Kazuyuki Tanaka, Network Games with and without Synchronicity, Lecture Notes in Computer Science, 査読有, 7037 巻, 2011 年, 87-103, 10.1007/978-3-642-25280-8_9

[学会発表](計 8件)

K. Tanaka, Reverse Mathematics on Measure-Theoretic Probability (Plenary talk), Asian Logic Conference, 2013 年 09 月 18 日, 中国・中山大学

Y. Takahashi, T. Yamazaki and K. Tanaka, Hardness of Classically Simulating Quantum Circuits with Unbounded Toffoli and Fan-Out Gates, The 38th International Symposium on Mathematical Foundations of Computer Science (MFCS 2013), 2013 年 8 月 30 日, オーストリア・Institute of Science and Technology

K. Tanaka, Infinite Games and Reverse Mathematics, Fourth Workshop on Game-Theoretic Probability and Related Topics, 2012 年 11 月 14 日, 東京大学

N. Peng, K. Higuchi, T. Yamazaki and K. Tanaka, Relative randomness for Martin-Loef random sets, CiE 2012, 2012 年 6 月 19 日, 英国ケンブリッジ大学

K. Yoshii and K. Tanaka, Infinite games and transfinite recursion of multiple inductive definitions, CiE 2012, 2012 年 6 月 19 日, 英国ケンブリッジ大学

K. Yoshii and K. Tanaka, Infinite games and Reverse Mathematics, Workshop on Proof Theory and Computability Theory, 2012 年 2 月 22 日, 東京晴海

K. Tadaki, Robustness of statistical

mechanical interpretation of algorithmic information theory, ALC 2011, 2011 年 12 月 19 日, ニュージーランド・Victoria University of Wellington

Ahmad Termimi Ab Ghani and Kazuyuki Tanaka, Network Games with and without Synchronicity, GameSec 2011, Conference on Decision and Game Theory for Security, 2011 年 11 月 14 日, 米国・メリーランド大学

〔図書〕(計 2 件)

田中一之、東京大学出版会、「ゲーデルに挑む」, 2012、総ページ数 176

田中一之、東京大学出版会、「チューリングと超パズル」, 2013、総ページ数 266

〔産業財産権〕

出願状況(計 0 件)

名称:

発明者:

権利者:

種類:

番号:

出願年月日:

国内外の別:

取得状況(計 0 件)

名称:

発明者:

権利者:

種類:

番号:

取得年月日:

国内外の別:

〔その他〕

ホームページ等

6. 研究組織

(1) 研究代表者

田中 一之 (TANAKA, KAZUYUKI)

東北大学・大学院理学研究科・教授

研究者番号: 70188291

(2) 研究分担者

只木 孝太郎 (TADAKI, KOHTARO)

中央大学・研究開発機構・機構准教授

研究者番号: 70407881

山崎 武 (YAMAZAKI, KAKESHI)

東北大学・大学院理学研究科・准教授

研究者番号: 30336812

(3) 連携研究者

()

研究者番号: