様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　１４　日現在

機関番号：　３４３１５
研究種目：　新学術領域研究（研究領域提案型）
研究期間：　2012～2016
課題番号：　２４１０６００９

研究課題名（和文）量子力学からの計算限界解明へのアプローチ

研究課題名（英文）An Approach to Understand the Limitations of Computation based on Quantum Mechanics

研究代表者

山下　茂（Yamashita, Shigeru）

立命館大学・情報理工学部・教授

研究者番号：３０３６２８３３

交付決定額（研究期間全体）：（直接経費）　　25,200,000円

研究成果の概要（和文）：量子力学特有の現象を利用した計算および通信の次世代の方式として、量子計算・量子通信と呼ばれる方式が提案され、現在までに多くの研究が行われてきている。この計算・通信方式は、現在使われている方式に比べてある状況では圧倒的に能力が高い可能性があることがわかっている。しかし、量子計算・量子通信の能力について完全には明らかになっていない。そのため、本研究課題では、量子計算および量子通信について計算量的なアプローチで、今まで知られていなかった能力に関しての解析を行い、新たな知見を得た。また、量子計算・量子通信の能力を解析するテクニックを用いて現在の計算方式の能力を解析する新たな研究成果も得た。

研究成果の概要（英文）：Quantum computation and communication is a paradigm for next generation computation and communication that exploits phenomena specific to quantum mechanics. This paradigm has been the subject of thorough investigations in past years. While it is known that it can be in several situations significantly more powerful than the paradigms currently used for computation and communication, its full power is nevertheless still not completely understood. In this project we have investigated the power of quantum computation and communication from the perspective of computational complexity. We discovered new capabilities of quantum models, constructed new techniques for analyzing them and then obtained new insights into the full power of quantum computation and communication. We also showed how to apply these new techniques to analyze the power of current models of computation and communication, and in this way obtained new results applicable to the current models as well.

研究分野：　計算機科学

キーワード：　量子計算　量子通信　量子力学　量子情報　計算モデル　量子対話型証明　量子回路

１．研究開始当初の背景

量子計算は RSA 暗号を瞬時に解読する Shor の量子アルゴリズム等に代表されるように従来の計算（以下、古典計算）を真に凌駕すると考えられている。そのため、量子計算の計算能力や古典計算との差異を明らかにするために、量子計算や量子通信の能力に関して多くの考察が積み上げられてきている。しかし、量子計算の能力を議論するための、通常の計算モデルに基づく計算量理論のような体系付けられた理論は未整備であると言わざるを得ない状況である。そのため、量子計算や量子通信の能力を議論するために、エンタングルメント等の量子力学特有の現象が計算能力に与える本質的な根源を突き止める息の長い研究が必須であると考えられている。

２．研究の目的

本研究課題では計算限界の究明のために、量子計算の能力の本質的な根源を突き止めることを目指した。それにより、量子力学特有の現象が計算能力や通信の能力にどのように影響するのかを定量的に議論するための枠組みを将来的には創出できることを期待している。そのために、まず、量子計算や量子通信が古典的な枠組みの計算や通信に対して、どのようなアドバンテージをいかなる状況で持つのかを定量的に議論することを目的とした。具体的には、(1) 通信を含む量子計算に関する研究、(2) 計算能力の解析手法に関する研究、(3) 新たな量子計算モデルに関する研究、の３項目について、それぞれの分野で新たな知見を得ることを目指した。

３．研究の方法

研究目的で述べた 3 研究項目ごとに班員をグループ分けし、各班員が持つ専門的知識や得意とする解析技法を最大限活かせるようにする一方で、各年度において研究プロジェクト会議を開催し、メンバー間で研究成果・方針の共有化を行った。また、領域の各研究計画班とはワークショップの開催等を通じて連携を取り、本研究課題による量子計算的知見や解析技法を計算限界究明のテクニックとして用いることを検討した。

４．研究成果

具体的な研究目的とした３つの項目に関して、主な成果をそれぞれ以下で述べる。

(1) 通信を含む量子計算に関する研究

通信を含む量子計算に関する研究に関して、最も良く研究されている対話型証明において、完全性誤りをゼロにできることはプロトコルの解析を簡素化する上で重要である。本研究課題では、量子対話型証明において完全性誤りをゼロにするための新しい手法を考案した。さらに、NP の量子版である QMA に対して、完全性誤りをゼロにできるかという１０年来の未解決問題に進展を与えた。QMA は、何らかの命題が真であるかを検証したいもの（検証者）が量子状態を証明者と呼ばれるものから受け取り、多項式時間量子計算によって検証を行うという量子対話型証明の特別な場合である。本研究課題では、証明者と検証者が事前に定数サイズの EPR 対を共有していれば QMA プロトコルは完全性誤りをゼロにできることを明らかにした。この事実は、わずか定数サイズの EPR 対さえ取り除くことができれば１０年来の未解決問題が肯定的に解決することを意味しており、QMA の完全性誤りをゼロにする方向へ歩を進めた結果といえる。またこの成果は、定数サイズの EPR 対が量子対話型証明の文脈で有効に働くことを示した最初の例であり、エンタングルメントの量子対話型証明における効果に新たな視点を与えるものである。なお、本研究課題で提案した手法は、同じグループの後続の研究などに有効に利用されており、手法の面でも後続の研究に影響を与えている。

(2) 計算能力の解析手法に関する研究

計算能力の解析手法に関する研究としては、量子計算の能力の解析に使われる手法を用いて、古典計算に関する新たな知見を幾つか得た。それについて以下で述べる。

１つめの結果として、量子計算に使われる解析に基づき古典計算における正方行列積の計算量の改良を行った。行列乗算の計算量を求める問題は、理論計算機科学及び Algebraic Complexity Theory (代数計算量理論)の中核の問題でありながら、未だ解決されていない。特に、二つの $n \times n$ 正方形行列の積の場合、その積はおよそ $O(n^2)$ 時間で計算できると予測されているものの、計算量の上限としては $O(n^{2.38})$ しか知られていない。具体的には、Coppersmith と Winograd が 1987 年に $O(n^{2.376})$ 時間を達成するアルゴリズム（以下、CW アルゴリズム）を提案してから、20 年間以上改良されなかったが、2010 年に Stothers がようやくその計算量を $O(n^{2.374})$ に下げることに成功した。その改良の基本的なアイデアは、元々の CW アルゴリズムの 2 乗を解析することであった。2012 年に Vassilevska Williams が、CW アルゴリズムの４乗を解析することによって、その計算量をさらに $O(n^{2.373})$ に改良した。次のステップとして、一般の r の場合の CW アルゴリズムの 2 べき乗（2^r 乗）の解析が自然に挙げられ、その解析によって得られる計算量が $O(n^2)$ に収束するという可能性があるので、$r > 2$ の場合の解析が注目されていた。しかし、r が 3 以上の場合、従来の手法ではその解析を行うのに指数時間かかるため、現実的には不可能であった。そこで、その解析を行う多項式時間の一般的なアプローチを提案した。また、そのアプローチを適用することによって、CW アルゴリズムの 16 乗までの解析を行って、

正方形行列乗算の計算量を $O(n^{2.3729})$に改良することに成功した。提案手法が量子計算によく使われているテンソル解析と凸最適化に基づく技法であることから、量子計算から得た着想と知見を用いたからこそ、この改良に成功できたと言える。

上述した新しいアルゴリズムを含み、上述の行列積アルゴリズムはすべてCoppersmith-Winograd法（CW法）という手法に従って得られている。本研究課題では、量子計算の解析手法に触発された行列積アルゴリズムの計算量の解析方法も開発し、CW法及びより一般的な手法の限界を明らかにすることに成功した。この成果により、現在の行列積アルゴリズムの構成方法を用いる限りでは、$O(n^2)$時間アルゴリズムが構成できないことだけでなく、本研究課題で提案したアルゴリズムの計算量すらほとんど改良できないことも証明できた。

上記に加えて、古典・量子計算の計算能力の究明を目指し、その計算能力の新しい解析手法も構築した。本研究課題では特に三角形発見問題をはじめとする基礎的なグラフ問題の複雑さに着目した。まず質問計算量の枠組みで、量子ウォークと組み合わせ的な手法を用いて、従来のアルゴリズムより高速な量子アルゴリズムを開発することに成功した。その後、この量子アルゴリズムの対象を疎グラフ上の三角形発見問題にも拡張した。古典計算では疎グラフ上の三角形発見問題を効率よく扱えるアルゴリズムが知られていないため、量子計算の優位性を示唆する新たな例となる。

また、三角形発見問題は分散計算モデルにおいても極めて重要な問題である。近年様々な基礎的な問題との関連が発見され、注目を集めてきたが、今まで三角形発見問題を効率よく解く分散アルゴリズムが知られていなかった。ここで、上述の（質問計算量の枠組みでの）量子アルゴリズムを分散計算の枠組みでの古典アルゴリズムに改変することに成功し、三角形発見問題を劣線形時間で解く初めての分散アルゴリズムを開発することができた。この成果は本領域A03班（公募班）のメンバーと共同で行われた学際的な研究であり、分散計算分野で最も権威のある国際会議PODCに採録された。

量子計算の解析に用いる考え方を応用した他の研究として、任意のNP問題について解の有無を決定する問題と解を探索する問題についての計算困難性の関係について非適応的な困難性帰着を用いた場合にどの程度計算困難性に差が出るのかについて情報理論的モデルの下でその困難性の差について解析を行った。特に、解がnビット長の場合、解の有無が分かるアルゴリズムを非適応的に$O(n^2)$回呼び出せば解を発見できるアルゴリズムが知られていたが、この呼び出し回数が漸近的に最適である、つまり任意のアルゴリズムにおいて少なくとも解を発見するためには$\Omega(n^2)$回の呼び出し回数が必要であることを証明した。

(3) 新たな量子計算モデルに関する研究

本研究課題では、DQC1 モデルと呼ばれる「初期状態においてわずかな量子ビットしか純粋状態として準備できない（あとはランダムな状態しか使えない）」という環境下において、計算誤りを大きく減らすための一般的な方法を提案した。より詳細には次の成果を得た。① $O(\log n)$ 個の純粋量子ビットが準備できるモデルで計算誤りが定数で解ける問題は、２個の純粋量子ビットが準備できるモデルでも解けて、かつ計算誤りは指数的に小さくできる。② $O(\log n)$ 個の純粋量子ビットが準備できるモデルで計算誤りが定数で解ける問題は、DQC1 モデル（１個の純粋量子ビットが準備できるモデル）でも解けて、かつ計算誤りは多項式的に小さくできる。また、上記の成果を得るための手法をもとにして、DQC1 モデルが（通常の量子計算モデルより弱いものの）真に量子的な計算モデルであるという計算量理論的証拠を与えることに成功した。さらには、トレース推定と呼ばれる量子物理学で重要な推定問題が、計算量理論的に厳密な意味で DQC1 モデルを正確に特徴付ける問題であることも解明した。なお、DQC1 モデルは NMR 量子計算の数学的モデルとして物理的には盛んに研究がなされてきたが、計算量理論的な研究はほとんどなされておらず、それゆえ本研究課題の成果は DQC1 モデルの計算量理論的基盤を固めるという意義も持っている。

別の研究として、量子オートマトンの能力の解析に関する研究を行い、以下に挙げる成果を得た。まず初めに、ある種のプロミス付き問題に対して、量子カウンタオートマトンでは誤りなく解くことができるが、古典決定性カウンタオートマトンでは解くことができないことを示した。この結果は、量子カウンタオートマトンと古典カウンタオートマトンの間に能力の差があることを示すものである。オートマトンが特定の問題を解けないことを示すには、反復補題を適用することが多いが、プロミス付き問題に対しては単純に反復補題を適用することができない。本研究課題では、反復補題を適用するのではなく、オートマトンの動作を直接解析することでの証明に成功した。さらに、量子アルゴリズムの設計手法を逆に古典アルゴリズムに応用することで、古典オートマトンに関する新しい結果を得た。具体的には、確率ブラインドカウンタオートマトンおよび決定性（非ブラインド）カウンタオートマトンで認識できるが、決定性ブラインドカウンタオートマトンでは認識できない言語が存在することを示した。この目的のために言語 EQ*を確率ブラインドカウンタオートマトンで認識するためのアルゴリズムを開発した。先行研究では、そのようなアルゴリズムは存在しないと

予測されていたものであり、この予測を覆したという意味でも興味深い結果と言える。

従来の量子回路のモデルと異なるTopological Quantum Computation (TQC) 向けの量子回路についての研究も行った。TQCの場合は、通常の量子回路と違って、2 量子ビットに相互作用するCNOTが複数ある時に、それらの CNOT が同時できるかどうかは、量子ビットを空間に配置して CNOT に相当する部分を線分で結んだ時に交わりがなければ同時に実行できるという特殊な性質を持つ。この性質を利用して、量子ビットの配置によって回路の論理的な実行時間が変わることに注目して、3 次元空間により効率的に量子回路を実現するために、論理量子ビットを 2 次元に配置する新しい量子回路のモデルを考案し、1 次元に配置するよりも有利な場合があることを明らかにして、厳密に最適な論理量子ビットの配置を求める手法を開発した。

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 61 件）

① Tomoyuki Morimae, Harumichi Nishimura and François Le Gall, Modified Group Non-Membership is in Promise-AWPP relative to group oracles, 査読あり, Quantum Information and Computation 17(3&4), pp. 242-250, 2017

② Seiseki Akibue and Mio Murao, Network Coding for Distributed Quantum Computation Over Cluster and Butterfly Networks, IEEE Trans. Inf. Theor., 査読あり,Vol. 62, No. 11, pp. 6620-6637, 2016
DOI: 10.1109/TIT.2016.2604382

③ Tomoyuki Morimae and Harumichi Nishimura, Quantum interpretations of AWPP and APP, Quantum Information and Computation 16(5&6), 査読あり, pp. 498-514, 2016

④ Masaki Nakanishi, Miki Matsuyama and Yumi Yokoo, A Fast Quantum Computer Simulator Based on Register Reordering, IEICE Trans. Inf. & Syst, 査読あり, Vol. E99-D, No. 2, pp.332-340, 2016
DOI: 10.1587/transinf.2015EDP7260

⑤ Yasuhiro Takahashi, Seiichiro Tani, Takeshi Yamazaki,Kazuyuki Tanaka, Commuting Quantum Circuits with Few Outputs Are Unlikely to be Classically Simulatable, Quantum Information and Computation, 査読あり, Vol. 16 No. 3&4, pp. 251-270, 2016

⑥ Iordanis Kerenidis, Mathieu Laurière, François Le Gall and Mathys Rennela, Information Cost of Quantum Communication Protocols, Quantum Information and Computation, 査読あり, Vol. 16 No. 3&4, pp. 181-196, 2016

⑦ Kohtaro Kato, Fabian Furrer and Mio Murao, Information-theoretical Analysis of Topological Entanglement Entropy and Multipartite Correlations, Phys. Rev. A, 査読あり, Vol. 93, 022317, 2016
DOI: 10.1103/PhysRevA.93.022317

⑧ Stacey Jeffery, Robin Kothari, François Le Gall and Frédéric Magniez. Improving Quantum Query Complexity of Boolean Matrix Multiplication Using Graph Collision, Algorithmica, 査読あり, Vol. 76 No. 1, pp. 1-16, 2016
DOI: 10.1007/s00453-015-9985-x

⑨ Eiichiro Fujisaki, Akinori Kawachi, Ryo Nishimaki, Keisuke Tanaka, and Kenji Yasunaga, Post-Challenge Leakage Resilient Public-Key Cryptosystem in Split State Model, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 査読あり, Vol. E98-A, No. 3, pp. 853-862, 2015
DOI: 10.1587/transfun.E98.A.853

⑩ Hirotada Kobayashi, François Le Gall and Harumichi Nishimura, Stronger Methods of Making Quantum Interactive Proofs Perfectly Complete, SIAM Journal on Computing, 査読あり, Vol. 44(2), pp. 243-289, 2015
DOI: 10.1137/140971944

⑪ Shojun Nakayama, Akihito Soeda, and Mio Murao, Quantum Algorithm for Universal Implementation of the Projective Measurement of Energy, Phys. Rev. Lett., 査読あり, Vol. 114, 190501, 2015
DOI: 10.1103/PhysRevLett.114.190501

⑫ Jisho Miyazaki, Michal Hajdušek, and Mio Murao, An Analysis of the Trade-off between Spatial and Temporal Resources for Measurement-based Quantum Computation, Phys. Rev. A, 査読あり,

Vol. 91, 052302, 2015
DOI: 10.1103/PhysRevA.91.052302

⑬ Kosuke Nakago, Michal Hajdušek, Shojun Nakayama and Mio Murao, Parallelizable Adiabatic Gate Teleportation, Phys. Rev. A, 査読あり, Vol. 92, 062316, 2015
DOI: 10.1103/PhysRevA.92.062316

⑭ Akinori Kawachi, Proving Circuit Lower Bounds in High Uniform Classes, Interdisciplinary Information Sciences, 査読あり, Vol. 20, No. 1, pp. 1-26, 2014
DOI: 10.4036/iis.2014.1

⑮ Andrej Bogdanov, Akinori Kawachi, and Hidetoki Tanaka, Hard Functions for Low-Degree Polynomials over Prime Fields, ACM Transactions on Computation Theory, 査読あり, 5(2): 5, 2013
10.1145/2493246.2493248

⑯ Marcos Villagra, Masaki Nakanishi, Shigeru Yamashita and Yasuhiko Nakashima, Tensor Rank and Strong Quantum Nondeterminism in Multiparty Communication, IEICE Trans. Inf. & Syst., 査読あり, Vol.E96-D, No.3, pp. 1-8, 2013
DOI: 10.1587/transinf.E96.D.1

⑰ Takahiko Satoh, François Le Gall and Hiroshi Imai, Quantum Network Coding for Quantum Repeaters, Phys. Rev. A 査読あり, Vol. 86, 032331, 2012
DOI: 10.1103/PhysRevA.86.032331

⑱ François Le Gall, Quantum Private Information Retrieval with Sublinear Communication Complexity, Theory of Computing, 査読あり, Vol. 8, pp. 369-374, 2012.
DOI: 10.4086/toc.2012.v008a016

⑲ François Le Gall, Shota Nakagawa and Harumichi Nishimura, On QMA Protocols with Two Short Quantum Proofs, Quantum Information and Computation, 査読あり, Vol.12 No.7&8, pp. 589-600, 2012.

⑳ Gábor Ivanyos, François Le Gall and Yuichi Yoshida, On the Distance between Non-isomorphic Groups, European Journal of Combinatorics, 査読あり, Vol. 33 No. 4, pp. 474-476, 2012
DOI: 10.1016/j.ejc.2011.10.009

〔学会発表〕(計 91 件)

① François Le Gall, Further Algebraic Algorithms in the Congested Clique Model and Applications to Graph-Theoretic Problems, the 30th International Symposium on Distributed Computing (DISC 2016), 2016 年 9 月 27 日, Paris (France)

② François Le Gall, Quantum Communication Complexity of Distributed Set Joins, 41st International Symposium on Mathematical Foundations of Computer Science, 2016 年 8 月 24 日, Krakow (Poland)

③ Harumichi Nishimura, Space-efficient error reduction for unitary quantum computation, the 43rd International Colloquium on Automata, Languages, and Programming, 2016 年 7 月 12 日, Rome (Italy)

④ Harumichi Nishimura, Power of quantum computation with few clean qubits, the 43rd International Colloquium on Automata, Languages, and Programming, 2016 年 7 月 12 日, Rome(Italy)

⑤ Shigeru Yamashita, A Pre-Optimization Technique to Generate Initial Reversible Circuits with Low Quantum Cost, 2016 IEEE International Symposium on Circuits and Systems, 2016 年 5 月 25 日, Montreal (Canada)

⑥ François Le Gall, Quantum Algorithm for Triangle Finding in Sparse Graphs, the 26th International Symposium on Algorithms and Computation, 2015 年 12 月 11 日, 名古屋マリオットアソシアホテル (愛知県・名古屋市)

⑦ Masaki Nakanishi, Classical and Quantum Counter Automata on Promise Problems, 20th International Conference on Implementation and Application of Automata, 2015 年 8 月 20 日, Uppsala (Sweden)

⑧ François Le Gall, Generalized Quantum Arthur-Merlin Games, the 30th Computational Complexity Conference, 2015 年 6 月 19 日, Portland (U.S.A.)

⑨ François Le Gall, Fast Matrix Multiplication: Limitations of the Coppersmith-Winograd Method, 47th ACM Symposium on Theory of Computing, 2015

年 6 月 17 日, Portland (U.S.A.)

⑩ François Le Gall, Improved Quantum Algorithm for Triangle Finding via Combinatorial Arguments, 55th Annual IEEE Symposium on Foundations of Computer Science, 2014 年 10 月 20 日, Philadelphia (U.S.A.)

⑪ François Le Gall, Powers of Tensors and Fast Matrix Multiplication, 39th International Symposium on Symbolic and Algebraic Computation, 2014 年 7 月 23 日, 神戸大学 (兵庫県・神戸市)

⑫ François Le Gall, Algebraic Complexity Theory and Matrix Multiplication, 39th International Symposium on Symbolic and Algebraic Computation, 2014 年 7 月 22 日, 神戸大学 (兵庫県・神戸市)

⑬ Akinori Kawachi, The Query Complexity of Witness Finding, the 9th International Computer Science Symposium in Russia, 2014 年 7 月 11 日, Moscow (Russia)

⑭ François Le Gall, Quantum Complexity of Matrix Multiplication, Satellite Workshop of ICALP 2013 on Quantum and Classical Complexity, 2013 年 7 月 7 日, University of Latvia (Riga, Latvia)

⑮ Seiichiro Tani, Collapse of the Hierarchy of Constant-Depth Exact Quantum Circuits, 2013 IEEE Conference on Computational Complexity, 2013 年 6 月 6 日, Stanford (U.S.A.)

⑯ François Le Gall, Time-Efficient Output-Sensitive Quantum Algorithms for Boolean Matrix Multiplication, the 23rd International Symposium on Algorithms and Computation, 2012 年 12 月 21 日, Taipei (Taiwan)

⑰ Shigeru Yamashita, An Optimization Problem for Topological Quantum Computation, IEEE 21st Asian test symposium, 2012 年 11 月 20 日, 朱鷺メッセ (新潟県・新潟市)

⑱ François Le Gall, Faster Algorithms for Rectangular Matrix Multiplication, the 53rd Annual IEEE Symposium on Foundations of Computer Science, 2012 年 10 月 23 日, New Brunswick (U.S.A.)

６．研究組織

(1)研究代表者

山下 茂（YAMASHITA, Shigeru）
立命館大学・情報理工学部・教授
研究者番号：30362833

(2)研究分担者

河内 亮周（KAWACHI, Akinori）
徳島大学・大学院理工学研究部・講師
研究者番号：00397035

中西 正樹（NAKANISHI, Masaki）
山形大学・地域教育文化学部・准教授
研究者番号：40324967

ルガル フランソワ（LE GALL, Francois）
京都大学・情報学研究科・准教授
研究者番号：50584299

西村 治道（NISHIMURA, Harumichi）
名古屋大学・情報科学研究科・准教授
研究者番号：70433323

(3)連携研究者

小林 弘忠（KOBAYASHI, Hirotada）
国立情報学研究所・情報学プリンシプル研究系・ 特任研究員
研究者番号：60413936

谷 誠一郎（TANI, Seiichiro）
ＮＴＴコミュニケーション科学基礎研究所・ 上席特別研究員
研究者番号：70396183

根本 香絵（NEMOTO Kae）
国立情報学研究所・情報学プリンシプル研究系・ 教授
研究者番号：80370104

村尾 美緒（Murao, Mio）
東京大学・理学系研究科・教授
研究者番号：30322671

(4)研究協力者

伊藤 剛志（Ito, Tsuyoshi）
NEC ラボラトリーズアメリカ・研究員