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　　９　日現在

機関番号：　１３９０１
研究種目：　基盤研究(C)（一般）
研究期間：　2013～2016
課題番号：　２５３３００１２

研究課題名（和文）量子検証システムの計算量的解析

研究課題名（英文）Complexity theoretic analysis of quantum verification systems

研究代表者
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

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：量子検証システムとは，証明者と呼ばれる強力な計算能力をもつものと検証者と呼ばれる多項式時間量子計算が行えるものの間の通信システムであり，その目的は検証者が決定問題の入力がYESか否かを効率的に検証することにある．本研究では，計算量理論の観点から量子検証システムの計算能力とその計算量的限界を研究した．とくに，QMAと呼ばれる非対話型の量子検証システムや１ラウンドの量子対話型証明システムを探究し，これらのシステムの簡素化を行ったり，基本的な性質を明らかにした．

研究成果の概要（英文）：The quantum verification system is the communication system between two parties called a prover, which has strong computational power, and a verifier, which can do polynomial-time quantum computation. The aim of the system is to make the verifier verify whether any input of a decision problem is YES. In this research, we have studied the computational power and the limit of quantum verification systems from the view of computational complexity. In particular, we have investigated the non-interactive quantum verification system called QMA and the one-round quantum interactive proof system, and have given several simplifications of their systems and clarified their basic properties.

研究分野：　量子計算，計算量理論

キーワード：　量子コンピュータ　対話型証明　NP

１．研究開始当初の背景

NP は証明者と呼ばれる全能のパーティが検証者と呼ばれる現実的な能力しか持たないパーティに証拠の候補を送るという通信プロトコルの観点で捉えられる．この観点から，検証者が証明者と対話を行うことで検証を行う対話型証明系や YES/NO 以外の情報を全く検証者に与えないゼロ知識証明系など計算量理論的にも暗号理論的にも重要な概念が，NP の一般化として説明できる．NP の重要性を鑑みると，NP の量子版が量子計算量理論の歴史において比較的早い段階である 1990 年代の終わり頃に Knill, Kitaev, Watrous らによって提案されたことは自然である．今日ではこの概念は（厳密には NP の確率版である MA の量子版に対応することから）QMA（Quantum Merlin-Arthur proof system）と呼ばれ，計算量理論の研究者のみならず，情報理論や物理学の研究者によっても盛んに研究が行われている．研究の方向性は２つに分かれる．１つは個々の問題の計算量的困難性に焦点を絞り，その問題が QMA に含まれるのか，あるいは QMA 困難なのかを明らかにするといったものである．もう１つは QMA という計算量クラス及びそれを下支えする検証システムの NP システムを凌駕する可能性や計算量的限界の研究である．このクラスは興味深いことに NP（あるいはその確率版 MA）と異なり，証明者が複数になると検証システムの性能が向上する可能性が小林ら，Aaronson らなどの研究により示唆されている．さらに Blier と Tapp の成果では，証拠の候補を送る通信量を NP システムに比して指数的に低減した証明者２名の QMA システムが提案され，検証の誤り確率に関して（実用上十分ではないものの）古典では困難と考えられる値を達成できることが示された．しかしこれら最近の活発な研究にもかかわらず，QMA システムの計算量的理解はおよそ満足できるものとは程遠いものであった．

２．研究の目的

本研究では，QMA システムとその一般化に関して，通信量，誤り確率及び証明者間のエンタングルメント量というシステムの性能を示すパラメータの関係について解析する．これにより，QMA システムの性能に関する量的評価を行うとともに，エンタングルメントの効果に対する計算量理論からの見解を与える．具体的には，まず QMA システムの片側誤り化へ向けてのアプローチを模索する．第二に指数的に通信量を制限した多証明者 QMA の誤り確率低減の可能性を調査する．さらには QMA システムの一般化である量子対話型証明への成果の拡張も模索する．

３．研究の方法

本研究の基本的アプローチは，量子通信計算量の観点から QMA プロトコルを検討することであり，証明者と検証者の量子通信としてのエンタングルメントの効果などを通じて QMA プロトコルの可能性や限界を探究するというものである．量子計算量理論的解析手法を利用して QMA プロトコルの片側誤り化や成功確率の改良などを行うとともに，それらの成果の量子対話型証明への応用を目指す．

研究体制としては基本的にすべての研究を応募者が行うものであるが，研究分野が量子情報科学及び計算量理論にまたがる分野であり，研究推進には幅広い知識を必要とするため，小林博士（NII），Le Gall 准教授（京都大学），森前准教授（群馬大学），Cleve 教授（Waterloo 大学）らの国内外の共同研究者との研究協力を適宜行う．

４．研究成果

(1) １ラウンド量子対話型証明の計算構造の解析

検証者が検証に必要な量子情報を一方向で受け取るだけでなく，必要な量子情報を送るべき証明者にランダムなビット列を送ることができるような１ラウンドの双方向通信によるプロトコルに対して，プロトコルを片側誤り化する十分条件が多項式サイズの量子状態を共有することであることを証明した．また，１ラウンド対話型量子証明系に関する自然な計算量クラスとして「検証者がベル量子もつれ状態を証明者に送付し，証明者が検証者に量子状態を送付する」という形で１ラウンドの対話が実行されるものを導入し，その計算量クラスについての基本的性質を調査した．とくに，対話の前にさらに定数回の古典情報による対話を許すと当該計算量クラスが変わるのか否かを詳細に解析した．その結果，当該計算量クラスは，そのような変更に対して不変なクラスであることが明らかになった．これは古典の計算量クラスにおける同様の現象の量子版ともいえる現象であり，このクラスの理解を一歩推し進めたといえる成果である．さらにその計算量クラスを特徴付ける完全問題をいくつか提示した．

(2) 弱い量子計算能力の検証者による QMA システムの検証能力の研究

検証者が Clifford 回路に制限された QMA システムを解析した．Clifford 回路は量子誤り訂正などで使用される重要な量子ゲートである Clifford ゲートからなる回路であるが，この回路は古典の計算機で効率的に模倣可能であることが知られている．しかしながら，このような弱い能力を持つ量子回路に制限された検証者をもつ QMA プロトコルは，通常の QMA プロトコルとなんら計算能力が変

わらないことが明らかにされた.

(3) 多項式階層の量子版に関する研究

非対話型量子証明系は計算量クラス NP の量子版とみなすことができるが，従来の計算量クラスには NP の論理構造の階数を多段化（NP は一段）した多項式階層と呼ばれる計算量クラスのグループがあり，計算量理論において基礎概念の１つとなっている．本研究では，階数が二段であるような計算量クラスの量子版を特徴付ける完全問題を新しく与えることに成功した．具体的には，量子物理系を特徴付けるハミルトニアンの標準的な数学的形式といえる局所ハミルトニアンにおいて，その冗長性を判定する問題を適切な形で定式化することにより，完全問題として提示できることを証明した.

(4) 量子計算の古典計算による摸倣可能性への量子計算量理論的アプローチ

量子計算の古典計算による効率的な模倣の可能性を，「古典計算量クラスにおける多項式階層の崩壊」というありえそうにない帰結に結びつけることにより，「量子計算が古典計算で効率的にはできないことを行っている」という計算量的証左を与える研究を始めた．本研究では，そのような方向性で従来研究において使用されていた量子計算量クラスと異なる量子計算量クラスとして，量子版 NP の１つである NQP というクラスに着目することで，多項式階層の崩壊がより大きなレベルで生じることを発見した．このことは，量子計算の古典計算による模倣不可能性に対するより信頼性のある計算量的証左を与えたことになる.

(5) 古典計算量クラスの量子計算的解釈

多項式時間量子計算を特徴付ける計算量クラス BQP の最良の上界として知られる古典計算量クラス AWPP について，その量子計算的特徴付けを与えることに成功した．この成果は，事後選択と呼ばれる仮想的な操作を認めた多項式時間量子計算によって古典計算量クラスを特徴付けるものであり，直感的な理解が容易でない計算量クラスに対して量子計算の枠組みを使った操作論的な解釈を与えるものである.

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６件）

[1] Tomoyuki Morimae, Harumichi Nishimura. Quantum Interpretation of AWPP and APP. Quantum Information and Computation 16, pp. 498-514, 2016. 査読有
URL:http://www.rintonpress.com/xxqic16/qic-16-56/0498-0514.pdf

[2] Tomoyuki Morimae, Masahito Hayashi, Harumichi Nishimura, Keisuke Fujii. Quantum Merlin-Arthur with Clifford Arthur. Quantum Information and Computation 15, pp. 1420-1430, 2015. 査読有
URL:http://www.rintonpress.com/xxqic15/qic-15-1516/1420-1430.pdf

[3] 西村治道. 量子情報の基礎（招待論文）. 情報処理 55, pp. 682-688, 2015. 査読なし.

[4] Hirotada Kobayashi, Francois Le Gall, Harumichi Nishimura. Stronger methods of making quantum interactive proofs perfectly complete. SIAM Journal on Computing 34, pp. 243-289, 2015. 査読有
DOI: http://dx.doi.org/10.1137/140971944

[5] Harumichi Nishimura. Quantum network coding - How can network coding be applied to quantum information? （招待論文）, Proceedings of 2013 IEEE International Symposium on Network Coding, 5pages, 2013. 査読なし
DOI: 10.1109/NetCod.2013.6570840

[6] Kazuo Iwama, Harumichi Nishimura. Recovering strings in oracles: quantum and classic（招待論文）. International Journal of Foundations of Computer Science 24, pp. 979-993, 2013. 査読なし
DOI: 10.1142/S0129054113400261

〔学会発表〕（計１７件）

[1] Harumichi Nishimura, Power of quantum computation with few clean qubits. Workshop around BQP（招待講演）. 2015 年 12 月 7 日～8 日. Centre for ELC, Tokyo (Japan).

[2] 西村治道. 量子版 NP と量子版 AM の計算複雑さ. 第３３回量子情報技術研究会（招待講演）. 2015 年 11 月 24 日～25 日. NTT 厚木研究センタ（厚木市）.

[3] 森前智行, 西村治道. AWPP の量子計算による解釈. 第３３回量子情報技術研究会. 2015 年 11 月 24 日～25 日. NTT 厚木研究センタ（厚木市）.

[4] 森前智行, 林正人, 西村治道, 藤井啓佑. Quantum Merlin-Arthur with Clifford Arthur. コンピュテーション研究会. 2015 年 10 月 2 日. 法政大学市ヶ谷キャンパス（東京

都千代田区).

[5] 藤井啓佑, 小林弘忠, 森前智行, 西村治道, 玉手修平, 谷誠一郎. Impossibility of classically simulating one-clean-qubit computation. コンピュテーション研究会. 2015 年 9 月 1 日. 信州大学長野（工学）キャンパス（長野市).

[6] 森前智行, 西村治道. Quantum Interpretation of AWPP. コンピュテーション研究会. 2015 年 9 月 1 日. 信州大学長野(工学）キャンパス（長野市).

[7] 西村治道. 量子計算量クラス－P と NP の量子版とその先（招待講演). 基礎物理学研究所研究集会「量子制御技術の発展により拓かれる量子情報の新時代」. 2015 年 7 月 13 日～16 日. 京都大学基礎物理学研究所(京都市).

[8] Hirotada Kobayashi, Francois Le Gall, Harumichi Nishimura. Generalized quantum Arthur-Merlin games. 30th Conference on Computational Complexity (CCC2015). 2015 年 6 月 17 日～19 日. Portland, Oregon (USA).

[9] Harumichi Nishimura. Quantum network coding and the current status of its studies. International Symposium on Information Theory and Its Applications（招待講演）. 2014 年 10 月 27 日～29 日. Melbourne (Australia).

[10] Harumichi Nishimura. Generalized quantum Arthur-Merlin game. ELC Workshop at the University of Tokyo on Quantum Complexity Theory（招待講演）. 2014 年 8 月 18 日. Tokyo (Japan).

[11] Francois Le Gall, Harumichi Nishimura, Seiichiro Tani. Quantum algorithms for finding constant-sized sub-hypergraph. 20th International Conference on Computing and Combinatorics. 2014 年 8 月 4 日～6 日. Atlanta (USA).

[12] Francois Le Gall, Harumichi Nishimura. Quantum algorithm for matrix product over semirings. 14th Scandinavian Symposium and Workshops. 2014 年 7 月 2 日～4 日. Copenhagen (Denmark).

[13] 川崎涼, 西村治道. 局所ハミルトニアンの非冗長性の計算量. コンピュテーション研究会. 2014 年 6 月 13 日～14 日. 松山（愛媛).

[14] Harumichi Nishimura. Quantum Arthur and quantum Merlin（招待講演）. 5th Nagoya Winter Workshop on Quantum Information, Measurement, and Foundations (NWW2014). 2014 年 3 月 7 日. Nagoya (Japan).

[15] Francois Le Gall, 西村治道, 谷誠一郎. 定数サイズ部分ハイパーグラフ発見に対する量子アルゴリズム. 第２９回量子情報技術研究会. 2013 年 11 月 18 日. 早稲田大学(東京都新宿区).

[16] 小林弘忠, Francois Le Gall, 西村治道. Stronger methods of making quantum interactive proofs perfectly complete. コンピュテーション研究会. 2013 年 6 月 24 日. 奈良女子大学（奈良市).

[17] Francois Le Gall, 西村治道. Quantum algorithms for matrix products over semirings. 第２８回量子情報技術研究会. 2013 年 5 月 27 日. 北海道大学（札幌市).

〔その他〕
ホームページ等

研究者のホームページ
http://www.math.cm.is.nagoya-u.ac.jp/~hnishimura

研究者総覧「情報知」
http://www.is.nagoya-u.ac.jp/research/jhc.html

６．研究組織
(1)研究代表者
西村治道（NISHIMURA HARUMICHI）
名古屋大学・情報学研究科・准教授
研究者番号：70433323