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

令和　２ 年　 ６ 月　 １ 日現在

機関番号：１３９０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2019
課題番号：１６Ｋ００００１５

研究課題名（和文）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

研究課題名（英文）Analysis of quantum interactive proofs with restricted quantum communication and computation

研究代表者
西村　治道（Nishimura, Harumichi）

名古屋大学・情報学研究科・教授

研究者番号：７０４３３３２３

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：量子対話型証明は1ラウンドの検証システムである量子NPシステムの自然な拡張であり，無限の能力を持つパーティ（証明者）と多項式時間の能力を持つパーティ（検証者）の間で複数回のラウンドが認められている．量子対話型証明は量子計算量理論の主要トピックでありながら，まだ十分に探究されていない部分，未解決のまま残された課題も多い．そこでこのモデルをよりきめ細かな形で調査するため，本研究では幾つかの方法で量子通信や量子計算が制限された量子対話型証明の計算能力と計算限界を研究した．さらに，本研究で得られた量子対話型証明の解析技法を使ってDQC1モデルのような制限された量子計算モデルの能力を明らかにした．

研究成果の学術的意義や社会的意義
量子計算は近年社会的に大きな注目を集めている．特に従来の計算機で効率的に行えないような何らかのタスクを近未来的に実現可能な量子計算機で行えるかという問題は，量子超越性と呼ばれて世界的に研究が加速している．しかしながら，量子計算機の計算能力の理論的解明は量子超越性の理論を含めて道半ばである．本研究の研究成果は，量子計算機の真の能力を明らかにするための基盤を固めるという学術的意義を持っている．また，近未来的に実現可能な量子計算による検証を意識して，制限された量子対話型証明の研究を行うとともに量子超越性の理論に対する貢献を行ったことで，社会的にも意義のある成果と考えられる．

研究成果の概要（英文）：The quantum interactive proofs is a natural extension of the quantum NP systems (one-round verification system) where multiple rounds of interaction are allowed between a unlimitedly powerful party (prover) and a polynomial-time computable party (verifier). While the quantum interactive proof is one of main topics in quantum computational complexity, it still has many unexplored points and the computational power has been unknown. To investigate this model in a more fine grained way, we have studied the computational power and the limitation of quantum interactive proofs by restricting quantum communication and computation in several approaches. Moreover, we have shown the power of restricted quantum computation models such as DQC1 models by using the analysis of quantum interactive proofs that are obtained in this research.

研究分野：量子計算

キーワード：量子計算　対話型証明　計算量理論

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

量子対話型証明は２０００年頃に導入された量子計算モデルの１つで，従来の古典力学をベースとした計算（古典計算）における対話型証明モデルの量子版である．対話型証明モデルは計算能力無限のパーティ（証明者）と計算能力が多項式時間などに制限されたパーティ（検証者）の対話によって，検証者が単独では検証できないような問題を検証するための計算モデルである．量子版になることで，証明者，検証者が量子計算機を利用できるようになり，２者間の通信で量子通信が利用できるようになったりする．量子対話型証明モデルは，研究開始当初の時点ですでに１５年以上の歴史のある量子計算モデルであり，それゆえ最も基本的なモデルの検証能力が古典計算量クラス PSPACE と一致することなど，いくつかの基盤的な事実は知られていた．しかしながら，暗号的応用や実装を意識した場合に重要とされる通信回数や量子計算能力を制限した量子対話型証明モデルは，古典の対話型証明モデルに比べて未開な部分が非常に多く，研究の進展が待たれるような状況であった．

研究者自身の研究状況としては，前身研究である基盤研究(C)「量子検証システムの計算量的解析」において，量子対話型証明モデルの特別な場合である量子 NP システムの検証能力を計算量理論的に探究するとともに，量子対話型証明モデル自体についてもその誤り確率の低減化に関する成果を得ていて，本研究を進めるための様々な解析技法や知見などを蓄えつつあった．また，前身研究以前にも，検証者が量子オートマトンという非常に弱い計算モデルの場合に関する量子対話型証明の理論を研究していて，今回の研究の着眼はその延長線上に得られたものであった．

２．研究の目的

本研究では，量子対話型証明モデルにおいて，証明者と検証者の間の通信回数や検証者の計算能力を制限した場合を考え，その場合における量子対話型証明モデルの検証能力を詳細に検討した．これにより，量子対話型証明モデルの暗号理論への応用や将来的な実装に向けて有用でかつ堅牢な理論的基盤の構築を目指した．また，その研究の途上で必要となる DQC1 モデルのような計算能力を制限した量子計算モデル自体の計算量理論的理解も進めることで，量子対話型証明モデル以外の量子計算モデルについてもその能力や計算限界を明らかにすることを目的とした．

３．研究の方法

研究の第一段階では，計算能力を制限した量子計算モデル（弱い量子計算モデル）の中で物理的側面については盛んに研究されてきたもの（例えば DQC1 モデル）を，計算量理論の立場から再検討し，その計算能力についての理論を展開することで，量子対話型証明モデルにおける計算能力の制限された検証者そのものの能力を理解しようとした．その後，そのような弱い量子計算モデルを検証者とする量子対話型証明モデルについて，前身研究やこれまでの研究で得た量子対話型証明モデルに関する解析技法や知見をもとに，その検証能力の計算量的特徴づけを行った．また，国際会議や国内の研究会，セミナーで参加や発表を行うことで，量子対話型証明モデルを研究する国内外の研究者と適宜協力し，必要となった専門知識や解析に関する知見などを補った．

４．研究成果

（１）DQC1 モデルの量子超越性

DQC1 モデルは NMR 量子計算を想定してモデル化された弱い量子計算モデルである．DQC1 モデルはもともと物理的に動機づけられた量子計算モデルであることから，主に物理学者によってその物理的側面が研究されてきた．このモデルは，初期状態が１量子ビットを除いてランダムであるという状況での量子計算機を表現している．通常の多項式時間量子計算よりも計算能力が弱いと予想される一方で，古典計算機では多項式時間では計算できないかもしれない問題が多項式時間で解けることが知られていた．しかし，古典計算機により多項式時間で模倣できないことを，計算量理論的に起こりえないと考えられる命題に帰着させることで証拠付けようとする「量子超越性」については，本研究以前は未解決であった．

本研究では，DQC1 モデルが量子超越性を持つという事実を初めて証明した．より厳密には，DQC1 モデルによって生成される確率分布が，古典計算機により多項式時間で正確に模倣可能であるならば，計算量理論における多項式階層が第二階層まで崩壊するという，起こりえないと考えられる命題に帰着させることに成功した．さらに，その成果を１量子ビットの準備にすら物理的なエラーが入ったモデルに拡張した．これらの成果は物理における代表的な雑誌である Physical Review Letters や Physical Review A で発表された．その後，この成果を改良する成果やこの成果の証明アイデアを利用した論文が発表されるなどしており，本研究の成果は量子超越性の理論において一定の評価を得ている．

（２）DQ1 モデルの計算量理論の整備

（１）で述べたように，DQC1 モデルは物理的側面の研究は盛んになされてきたが，計算量理論については，理論計算機科学者の参入が多くなかったこともあって，本研究以前はあまり多くのことがわかっていなかった．本研究では，（１）の成果を得る過程で，DQC1 モデルおよびその拡張モデルに関する計算量クラスを厳密に定義した．そして，その計算量クラスの頑健性を示すためにこれらのモデルの誤り確率の低減化を行うプロトコルを開発した．また，計算量クラスを特徴付ける問題である完全問題についても，その誤り確率に対する頑健性を部分的に示すことができた．本成果は理論計算機科学におけるトップレベルの国際会議 ICALP に採択された．さらには，（１）の成果とともに，近年増加しつつある DQC1 モデルの計算量理論的研究の先駆けとなった．

（３）検証者の量子メモリが制約された量子対話型証明の誤り確率の低減化

量子計算機において量子ビットの個数を増やすことは最も重要であるが，実装面において容易でない作業である．それゆえ量子ビットの個数を押さえた量子計算機の計算能力の研究は，近未来的な量子計算機の計算能力を測るうえでも重要である．

本研究では，検証者の量子計算能力を制限した量子対話型証明モデルとして，検証者の量子計算機の量子ビット数が制限された状況を考え，その場合における誤り確率の低減化を検討した．その結果，１ラウンドの量子対話型証明で検証者の量子回路がユニタリである場合に，既存研究より効率的な誤り確率の低減化プロトコルを発見した．そしてこの結果を用いて，量子メモリが入力サイズに対して対数のオーダである場合，ユニタリな検証者をもつ１ラウンドの量子対話型証明は，証明者からのメッセージが検証能力に何ら影響を与えないことを明らかにした．本成果もまた ICALP に採択されたことから，国内外における一定の評価を得たといえる．

（４）事後選択能力を備えた量子計算の計算能力の解明

事後選択とはある事象が起こったという条件の下での議論であり，物理や計算の現象を理解する上でしばしば導入される概念である．量子計算における事後選択の最もよく知られた成果は，２００５年の Aaronson による古典計算量クラス PP の事後選択付き多項式時間量子計算で判定可能な問題のクラス PostBQP による特徴づけである．この成果は古典計算量クラスで基本的なクラスである PP が量子計算の言葉でわかりやすく特徴付けられただけでなく，量子超越性の理論などにも応用されている．本研究では，事後選択付きの１ラウンド量子対話型証明で検証可能な問題のクラスが PSPACE と一致することを明らかにした．この成果は，PSPACE という PP 以上にメジャーな計算量クラスに対して，１ラウンド量子対話型証明という量子計算の言葉を用いた特徴付けを与えたと考えられる．

また，本研究では前身研究で得られた古典の計算量クラス AWPP の量子計算量クラスによる特徴づけを用いて，群非同型性判定問題に関連するある代数的な問題が AWPP に属することも証明した．

（５）量子計算機で効率的に解ける問題の古典計算機による検証

量子計算機は今日 IBM などによりクラウドサービスとして提供され始めたが，そのようなクラウドサービスで将来的に課題となるのが，量子計算機の古典計算機による検証である．これは，量子計算機を持つと主張するサーバが本当に量子計算をできるのかを，古典計算機しか持たないクライアントによって検証するという課題である．この「量子計算機の古典計算機による効率的検証」は近年世界的に多くの注目を集める課題であるが，この問題に対する従来の成果は何らかの条件を仮定することでこの課題を解決しようというものである．

本研究では，何らかの条件を付ける代わりに，量子計算機で効率的に解ける問題の中から古典的に検証可能な問題を探索する方向を模索した．対話型証明の知見をもとにして，サーバを証明者，クライアントを検証者とする対話型証明として捉え，量子計算機で効率的に解ける２つの問題に対する古典計算機による効率的検証プロトコルを与えることに成功した．１つは群の位数を決定するという代数的問題であり，古典の計算量理論でも盛んに研究されている問題である．この問題は２０００年に Watrous によって量子計算機により多項式時間で解けることが知られていたが，今回の成果により，この問題は証明者が多項式時間量子計算機である場合に古典計算機によって効率的に検証可能な問題であることが分かった．もう１つは制限された量子回路により生成された２つの確率分布の識別に関する問題である．この問題については，証明者が多項式時間量子計算機である場合に古典計算機によって１ラウンドの対話型証明で検証可能であることを示すことができた．

５．主な発表論文等

〔雑誌論文〕　計5件（うち査読付論文　5件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Fujii Keisuke、Kobayashi Hirotada、Morimae Tomoyuki、Nishimura Harumichi、Tamate Shuhei、Tani Seiichiro	４．巻 120
２．論文標題 Impossibility of Classically Simulating One-Clean-Qubit Model with Multiplicative Error	５．発行年 2018年
３．雑誌名 Physical Review Letters	６．最初と最後の頁 200502-1～6
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevLett.120.200502	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Morimae Tomoyuki、Takeuchi Yuki、Nishimura Harumichi	４．巻 2
２．論文標題 Merlin-Arthur with efficient quantum Merlin and quantum supremacy for the second level of the Fourier hierarchy	５．発行年 2018年
３．雑誌名 Quantum	６．最初と最後の頁 106-1～30
掲載論文のDOI（デジタルオブジェクト識別子） 10.22331/q-2018-11-15-106	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Morimae Tomoyuki、Fujii Keisuke、Nishimura Harumichi	４．巻 95
２．論文標題 Power of one nonclean qubit	５．発行年 2017年
３．雑誌名 Physical Review A	６．最初と最後の頁 42336
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevA.95.042336	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Morimae Tomoyuki、Nishimura Harumichi	４．巻 17
２．論文標題 Merlinization of complexity classes above BQP	５．発行年 2017年
３．雑誌名 Quantum Information and Computation	６．最初と最後の頁 959-972
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Tomoyuki Morimae, Harumichi Nishimura, Francois Le Gall	４．巻 17
２．論文標題 Modified group non-membership is in promise-AWPP relative to group oracles	５．発行年 2017年
３．雑誌名 Quantum Information and Computation	６．最初と最後の頁 0242-0250
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計12件（うち招待講演　1件／うち国際学会　7件）

１．発表者名 西村治道
２．発表標題 量子計算量クラスについて
３．学会等名 ImPACT未来開拓研究会2018（招待講演）
４．発表年 2018年

１．発表者名 Francois Le Gall, Tomoyuki Morimae, Harumichi Nishimura, Yuki Takeuchi
２．発表標題 Interactive Proofs with Polynomial-Time Quantum Prover for Computing the Order of Solvable Groups
３．学会等名 43rd International Symposium on Mathematical Foundations of Computer Science (MFCS2018)（国際学会）
４．発表年 2018年

１．発表者名 Tomoyuki Morimae, Harumichi Nishimura
２．発表標題 Rational proofs for quantum computing
３．学会等名 18th Asian Quantum Information Science Conference (AQIS2018)（国際学会）
４．発表年 2018年

１．発表者名
Francois Le Gall, Tomoyuki Morimae, Harumichi Nishimura, Yuki Takeuchi

２．発表標題
Interactive proofs with polynomial-time quantum prover for computing the order of solvable groups

３．学会等名
18th Asian Quantum Information Science Conference (AQIS2018) (国際学会)

４．発表年
2018年

１．発表者名
Francois Le Gall, Harumichi Nishimura, Ansis Rosmanis

２．発表標題
Quantum Advantage for the LOCAL Model in Distributed Computing

３．学会等名
36th International Symposium on Theoretical Aspects of Computer Science (STACS2019) (国際学会)

４．発表年
2019年

１．発表者名
森前智行、西村治道

２．発表標題
Merlinization of complexity classes above BQP

３．学会等名
第37回量子情報技術研究会

４．発表年
2017年

１．発表者名
佐伯元春、西村治道

２．発表標題
make10の一般化について

３．学会等名
第13回組合せゲーム・パズル研究集会

４．発表年
2018年

１．発表者名
Keisuke Fujii, Hirotada Kobayashi, Tomoyuki Morimae, Harumichi Nishimura, Shuhei Tamate, Seiichiro Tani

２．発表標題
Power of quantum computation with few clean qubits

３．学会等名
43rd International Colloquium on Automata, Languages, and Programming (ICALP2016)（国際学会）

４．発表年
2016年

１．発表者名
Bill Fefferman, Hirotada Kobayashi, Cedric Yen-Yu Lin, Tomoyuki Morimae, Harumichi Nishimura

２．発表標題
Space-efficient error reduction for unitary quantum computations

３．学会等名
43rd International Colloquium on Automata, Languages, and Programming (ICALP2016)（国際学会）

４．発表年
2016年

１．発表者名
Bill Fefferman, Hirotada Kobayashi, Cedric Yen-Yu Lin, Tomoyuki Morimae, Harumichi Nishimura

２．発表標題
Space-efficient error reduction for unitary quantum computations

３．学会等名
16th Asian Quantum Information Science Conference (AQIS2016)（国際学会）

４．発表年
2016年

１．発表者名
西村治道

２．発表標題
メモリ限定量子計算量について

３．学会等名
研究会「量子情報と有限長の新展開」

４．発表年
2016年

１．発表者名
藤井啓祐，小林弘忠，森前智行，西村治道，玉手修平，谷誠一郎

２．発表標題
Power of quantum computation with few clean qubits

３．学会等名
第35回量子情報技術研究会

４．発表年
2016年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

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

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考