科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　　６　日現在

機関番号：　１３９０１
研究種目：　若手研究(B)
研究期間：　2010～2013
課題番号：　２２７０００１４

研究課題名（和文）量子通信計算量とその応用に関する研究

研究課題名（英文）Research on quantum communication complexity and its applications

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）　　2,200,000円、（間接経費）　　660,000円

研究成果の概要（和文）：量子通信計算量は量子計算量理論の主要トピックの一つであり，複数のパーティが共同で何らかの関数の計算を行う上で必要な量子通信の量を測ることを目的とする．本研究では，量子通信計算量の量子ネットワーク符号，量子質問計算量，量子対話型証明への応用を研究した．これらの計算および通信モデルの可能性とその限界が通信量の観点から探究された．とくに，一般的な量子ネットワーク符号プロトコルの構築や量子対話型証明プロトコルのパラメータの改善に成功した．

研究成果の概要（英文）：Quantum communication complexity is one of main topics on quantum complexity theory, and its aim is to measure the amounts of quantum communication among multiple parties for computing some function. In this research, we have studied the applications of quantum communication complexity to quantum network coding, quantum query complexity, and quantum interactive proofs. The possibilities and limits of these computing/communication models have been investigated based on how much communication is needed. In particular, we have succeeded in constructing general quantum network coding protocols and improving some parameters of quantum interactive proofs.

研究分野：　量子計算量理論

科研費の分科・細目：　情報学・情報学基礎

キーワード：　量子通信通信量　ネットワーク符号　質問計算量　対話型証明

１．研究開始当初の背景

量子通信計算量の研究には，２つの方向性がある．１つは古典の通信計算量に比べ著しい通信量の削減可能性の研究である．もう１つの方向は量子通信計算量の応用の模索である．古典の通信計算量の応用はVLSI理論，回路計算量など幅広いが，古典と量子の差から同様の概念に対する応用が量子通信計算量でも必ずしも可能というわけではない．例えば代表的応用の一つとして 1998 年の Buhrman らによる量子質問計算量と量子通信計算量の関連付けがある．しかし，量子通信計算量の応用は古典に比べるとまだ多くなく，より多くの応用を模索することが求められていた．

報告者が本格的に量子通信計算量の研究に従事することとなったのは，量子ネットワーク符号の研究を始めてからであった．量子ネットワーク符号は，2000 年に Ahlswede らによって始められたネットワーク符号の量子版といえ，量子情報をネットワーク上で効率的に通信するために 2007 年に報告者らによって研究の端緒が切られた分野である．報告者は研究を推進するにつれ，この分野の研究には量子通信計算量の研究が密接に関連していて，量子通信計算量の研究を進めることが量子ネットワーク符号の可能性を探究する上で大きな役割を果たすと考えた．

２．研究の目的

量子通信計算量の応用として，まず量子ネットワーク符号のさらなる展開を目指し，量子ネットワーク符号の可能性の理解を深める．報告者は 2007 年に量子ネットワーク符号では基本的限界として，特定のネットワーク上で（補助的な計算資源がない限り）完全に量子情報を送るために経路途上の符号化は役に立たないという成果を与えた．その一方で，2009 年には量子ネットワークに加えて補助的な古典通信路を認めると，量子ネットワーク符号がある種の条件のもと有効に働くことも示していた．本研究では，量子ネットワーク符号の可能性とその限界を一般のネットワークへ拡張することを目指す．

また，量子質問計算量や量子対話型証明など他の通信を含む量子計算モデルへの応用も模索する．量子質問計算量は前述の Buhrman らの成果により，量子通信計算量と密接な関係があり，質問量を通信量とみなすことで量子質問計算量の上下界を調べることが可能となる．量子対話型証明は，全能の証明者との量子通信を通じて，多項式時間の検証者が問題例の真偽を検証するシステムとみなすことができるので，量子通信の量からそのシステムの能力を計算量理論的に研究する．

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量子アルゴリズムや量子プロトコルを検討することで，それらの可能性や限界を探究するというものであった．量子通信計算量そのものの研究よりもむしろ他のモデルへの応用の研究が中心であり，具体的には量子ネットワーク符号，量子質問計算量，量子対話型証明への応用を目指した．

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，研究推進には幅広い知識を必要としたため，岩間教授（京都大），小林博士（NII），レイモンド博士（IBM），ルガル特任准教授（東京大），モンタナロ博士（当時ケンブリッジ大），ジョーダン博士（NIST）など国内外の共同研究者との研究協力を適宜行った．

４．研究成果

(1) 一般のネットワークにおける量子ネットワーク符号の可能性 [主要論文 7,15 など]

本研究開始前の 2009 年に，古典の補助通信路を認められた量子ネットワーク符号は，古典の線形ネットワーク符号において効率的通信が可能となるマルチプルユニキャスト型ネットワークのすべてで量子情報の効率的通信が可能となるという成果が，報告者らによって報告されていた．本研究では，この成果を線形と限らない一般のネットワーク符号に拡張した．これによって，古典の補助通信路を認めた量子ネットワーク符号の可能性が，古典ネットワーク符号と同様のレベルまで一般的な形で明らかにされた．さらに得られた手法は，マルチキャスト型のネットワークにおける量子状態の共有にも応用された．

(2) 量子通信計算量と量子質問計算量の関係 [主要論文 1]

1998 年に Buhrman らは，量子質問計算量モデルにおける量子アルゴリズムを量子通信計算量モデルにおけるプロトコルに変換する方法を与えた．この変換方法は非常に一般的かつ強力で，量子通信計算量の上界などを与えるうえで有用な基本的結果であるが，変換において対数のオーバーヘッドが生じる．本研究では，このオーバーヘッドをなくすことが可能かを検討し，オーバーヘッドが避けられないような例を考案した．本研究の成果により，Buhrman らの変換の最適性が明らかにされた．

(3) 高度な質問を認めた量子質問計算量モデルの解析 [主要論文 4,20 など]

量子質問計算量の標準的なモデルでは，量

子アルゴリズムは入力として与えられるビット列に対して質問したい場所を指定して質問しつつ計算を進めることにより，入力がある性質を満たすか（や入力そのもの）を出力することが求められる．一方で，質問の方法がより高度になると（例えば入力と質問を表すビット列の内積），質問計算量が下がるのは自然である．この場合，古典の質問計算量ではその限界として情報理論的下界がよく用いられるが，量子において情報理論的下界は通用しない．本研究では，高度な質問を認めた量子質問計算量の理解を深めるため，部分列質問など古典でよく研究されている高度な質問をもとにした量子質問計算量モデルを研究し，古典の情報理論的下界を破る量子アルゴリズムや量子質問計算量の下界を与えた．

(4) 対数的量子通信計算量を持つ多証明者量子非対話型証明の解析 [主要論文 3 など]

量子非対話型証明は，通信が証明者から検証者への一方向通信に制限された量子対話型証明の特別な場合であり，NP の量子版と考えられる．古典の場合と異なり，証明者が複数存在する場合が単独の場合と異なる可能性が指摘されており，とくに 2009 年に Blier と Tapp は，証明者が 2 人の場合において（通常は多項式長のところを）わずか対数長の量子証明による NP 完全問題に対するプロトコルを提案した．本研究では，彼らのプロトコルと PCP 定理の結果を組み合わせることで，彼らのプロトコルの健全性と呼ばれるパラメータ（問題例が NO のときに検証者が NO と判定する確率）を改善した．

(5) 量子対話型証明における完全性パラメータの解析 [主要論文 2,23 など]

量子対話型証明における重要なパラメータとして完全性がある．これは問題例が YES のときに検証者が YES と判定する確率である．完全性が 1 の場合，完全性誤りがないことになり，対話型証明のプロトコル自身において望ましいのは勿論のこと，対話型証明を暗号プロトコルなどに応用する上でも望ましい．本研究では，量子対話型証明のプロトコルを完全性誤りがないプロトコルに変換する幾つかの方法を提案した．その結果，証明が古典であるような量子非対話型証明は常に完全性誤りをなくすことができることや，（証明が量子である普通の）量子非対話型証明は証明者と検証者が事前に定数量の量子もつれを共有することで完全性誤りをなくすことができることを証明した．

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５件）

[1] Ashley Montanaro, Harumichi Nishimura, Rudy Raymond, Unbounded-error quantum query complexity, Theoretical Computer Science 412(35), pp.4619-4628 (2011). 査読有

[2] Stephen P. Jordan, Hirotada Kobayashi, Daniel Nagaj, Harumichi Nishimura, Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems, Quantum Information & Computation 12(5-6), pp.461-471 (2012). 査読有

[3] Francois Le Gall, Shota Nakagawa, Harumichi Nishimura, On QMA protocols with two short quantum proofs, Quantum Information & Computation 12(7-8), pp.589-600 (2012). 査読有

[4] Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, Junichi Teruyama, Quantum counterfeit coin problems, Theoretical Computer Science 456, pp.51-64 (2012). 査読有

[5] Kazuo Iwama, Harumichi Nishimura, Recovering strings in oracles: quantum and classic, International Journal of Foundations of Computer Science 24, pp.979-993 (2013). 招待論文

〔学会発表〕（計２１件）査読付国際会議論文５件含む

[6] Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, Junichi Teruyama, Quantum counterfeit coin problems, 3rd Annual Meeting of the Asian Association for Algorithms and Computation (AAAC2010), Pohang (Korea) April 17-19, 2010. 査読有

[7] Hirotada Kobayashi, Francois Le Gall, Harumichi Nishimura, Martin Roetteler, Perfect quantum network communication protocol based on classical network coding, IEEE International Symposium on Information Theory 2010 (ISIT2010), Austin (USA), June 13-18, 2010; in Proceedings of ISIT2010, pp. 2686-2690, 2010. 査読有

[8] 西村治道, 量子ネットワーク符号, 第 13 回情報論的学習理論ワークショップ, 東京, 2010 年 11 月 4－6 日. 招待講演

[9] 岩間一雄, 西村治道, Rudy Raymond, 照山順一, Quantum counterfeit coin problems, 第 23 回量子情報技術研究会, 東京, 2010 年 11 月 15－16 日; 第 23 回量子情報技術研究会資料, pp.24-29 (2010).

[10] 中川翔太, 西村治道, Blier-Tapp QMA プロトコルの健全性について, 第 23 回量子情報技術研究会, 東京, 2010 年 11 月 15-16 日; 第 23 回量子情報技術研究会資料, pp.132-135 (2010).

[11] Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, Junichi Teruyama, Quantum counterfeit coin problems, 21st International Symposium on Algorithms and Computation (ISAAC2010), Jeju (Korea), December 15-17, 2010; in Proceedings of ISAAC2010, Lecture Notes in Computer Science 6506, pp.73-84 (2010). 査読有

[12] Hirotada Kobayashi, Francois Le Gall, Harumichi Nishimura, Martin Roetteler, Constructing quantum network coding schemes from classical nonlinear protocols, 14th Workshop on Quantum Information Processing (QIP2011), Sentosa (Singapore), January 10-14, 2011. 査読有

[13] Richard Cleve, Kazuo Iwama, Francois Le Gall, Harumichi Nishimura, Seiichiro Tani, Junichi Teruyama, Shigeru Yamashita, Reconstructing strings from substrings with quantum queries, 4th Annual Meeting of the Asian Association for Algorithms and Computation (AAAC2011), Hsinchu (Taiwan), April 16-17, 2011. 査読有

[14] 小林弘忠, Francois Le Gall, 西村治道, Martin Roetteler, Constructing quantum network coding schemes from classical nonlinear protocols, コンピュテーション研究会, 長野, 2011 年 5 月 11 日; COMP2011-15, pp.25-31 (2011).

[15] Hirotada Kobayashi, Francois Le Gall, Harumichi Nishimura, Martin Roetteler, Constructing quantum network coding schemes from classical nonlinear protocols, IEEE International Symposium on Information Theory 2011 (ISIT2011), Saint Petersburg (Russia), July 31-August 5, 2011; in Proceedings of ISIT2011, pp. 109-113, 2011. 査読有

[16] Francois Le Gall, 中川翔太, 西村治道, On QMA protocols with two short quantum proofs, 第 25 回量子情報技術研究会, 東京, 2011 年 11 月 21－22 日; 第 25 回量子情報技術研究会資料, pp.21-26 (2011).

[17] Francois Le Gall, 中川翔太, 西村治道, On QMA protocols with two short quantum proofs, 数理解析研究所研究集会：アルゴリズムと計算理論の新展開(2011 年冬の LA シンポジウム), 京都, 2012 年 1 月 30 日－2 月 1 日; 数理解析研究所講究録 1799, pp.73-80 (2012).

[18] Richard Cleve, Kazuo Iwama, Francois Le Gall, Harumichi Nishimura, Seiichiro Tani, Junichi Teruyama, Shigeru Yamashita, Improved quantum algorithms for reconstructing strings from substrings, 5th Annual Meeting of the Asian Association for Algorithms and Computation (AAAC2012), Shanghai (China), April 21-22, 2012. 査読有

[19] Richard Cleve, 岩間一雄, Francois Le Gall, 西村治道, 谷誠一郎, 照山順一, 山下茂, Reconstructing strings from substrings with quantum queries, コンピュテーション研究会, 堺, 2012 年 4 月 27 日; COMP2012-2, pp.7-14 (2012).

[20] Richard Cleve, Kazuo Iwama, Francois Le Gall, Harumichi Nishimura, Seiichiro Tani, Junichi Teruyama, Shigeru Yamashita, Reconstructing strings from substrings with quantum queries, 13th Scandinavian Symposium and Workshops (SWAT2012), Helsinki (Finland), July 4-6, 2012; in Proceedings of SWAT2012, Lecture Notes in Computer Science 7357, pp. 622-633 (2012). 査読有

[21] Harumichi Nishimura, Reducing error probabilities of quantum Merlin-Arthur proof systems, Japan-Singapore Workshop on Multi-user Quantum Networks, Singapore (Singapore), September 17-20, 2012.

[22] 大和雅英, 西村治道, 衝突の列挙に関する量子質問計算量, 第 27 回量子情報技術研究会, 横浜, 2012 年 11 月 27 日－28 日; 第 27 回量子情報技術研究会資料, pp. 154-157 (2012).

[23] Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura, Stronger methods of making quantum interactive proofs perfectly complete, 4th ACM Conference on Innovations in Theoretical Computer Science (ITCS2013), Berkeley (USA), January 9-12, 2013; in Proceedings of ITCS2013, pp. 329-352 (2013). 査読有

[24] Stephen Jordan, Hirotada Kobayashi, Francois Le Gall, Daniel Nagaj, and Harumichi Nishimura, Towards Perfect Completeness in QMA, 16th Workshop on Quantum Information Processing (QIP2013), Beijing (China), January 21-25, 2013. 査読有

[25] Harumichi Nishimura, Quantum network coding – How can network coding be applied to quantum information?, 2013 IEEE International Symposium on Network Coding (NetCod2013), Calgary (Canada), June 7-9, 2013. 招待講演

[26] 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, 奈良, 2013年6月24日; COMP2013-24, pp.31-38 (2013).

〔図書〕（計１件）

[27] 西村治道, 電子情報通信学会ハンドブック「知識ベース　知識の森」Ｓ２群５編３章１節（量子計算理論）および６群２編６章２節（通信計算量）, 2011年3月一般公開.

〔その他〕

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

６．研究組織
(1)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
報告者番号：70433323