

科学研究費助成事業 研究成果報告書

平成 27 年 6 月 22 日現在

機関番号：12601

研究種目：基盤研究(A)

研究期間：2011～2014

課題番号：23240001

研究課題名(和文)量子グラフ理論確立による量子計算能力の限界解明

研究課題名(英文)Understanding the Limitation of Quantum Computation by Quantum Graph Theory

研究代表者

今井 浩 (IMAI, HIROSHI)

東京大学・情報理工学(系)研究科・教授

研究者番号：80183010

交付決定額(研究期間全体)：(直接経費) 37,100,000円

研究成果の概要(和文)：量子計算能力の限界解明を目指して、研究分担者・連携研究者らにより多角的に研究を進め、次のような成果をあげた。

(1) 測定ベース量子計算等の量子計算モデルの離散・物理構造に着目し、量子回路最適化や状態変換可能性・測定の汎用実装法・周期グラフ状態の万能計算性について成果を得た。(2) グラフの点マイナー理論を適用して、量子情報の観点からイジング分配関数の効率的計算法を考察し、量子グラフ彩色について量子非局所性での計算量理論での還元性を導入した解析法を提案した。(3) 量子多証明者対話証明について、量子AMゲームに関する統一的成果を得た。(4) 古典回路設計理論で重要なBDDを量子計算と結びつけた。

研究成果の概要(英文)：To understand the limitations of power of quantum computing, researchers in the group collaborated with one another from the point of multi-facet views from computer science to physics, and obtained the following results.

(1) Focusing on Measurement-Based Quantum Computing (MBQC) and other modes for quantum computation with their discrete and physical structures, optimization and transformability on quantum circuits, and universal measurement schemes were studied. Also, MBQC-universality of Platonic and Archimedean periodic graph were shown. (2) Based on graph vertex-minor theory with rank widths were applied to efficiently computing the partition function of Ising mode. (3) A quantum multi-prover interactive system for quantum Arthur-Merlin game was treated in a unified manner. (4) A new connection of Binary Decision Diagrams (BDD), which have vast applications in computer science, with quantum computing, especially MBQC, was revealed.

研究分野：量子情報科学

キーワード：量子計算理論 量子グラフ理論 量子コンピュータ 計算量理論 グラフマイナー理論

1. 研究開始当初の背景

情報技術が社会基盤となり身近に情報機器があふれる一方で、最先端のコンピュータはこれからの自然科学・社会科学の研究を自動車の衝突シミュレーションから DNA 構造の解析まで広範な計算処理により支える重要性が増大している。しかし、スパコンを始め現在の計算モデルに基づく先端コンピュータは、VLSI の微細化、並列化そして消費電力の諸限界に直面している。

量子コンピュータは、今の VLSI 微細化で顕在化する量子力学効果を計算過程に生かし、量子力学に従った操作で動作する。1980年代に Feynman が量子コンピュータを構想した際、現在のスーパーコンピュータ開発の1つの有力な対象分野である量子力学シミュレーションが、量子コンピュータでこそ高速に行えることが期待され、実際にそれが可能なことがわかってきた。一方で、量子力学の諸問題を高速に解くのが困難であることも判明しつつあり、基底状態のエネルギ計算は量子対話証明クラス QMA 完全であることが示されている。

量子コンピュータは、社会基盤となった情報システムのセキュリティに深いインパクトを与え、それが量子計算研究と量子コンピュータデバイス開発を進める原動力にもなってきた。しかし、分野全体で効率的量子アルゴリズムの開発は、着実に深化する一方で、Shor, Grover アルゴリズムのインパクトの大きさの壁に直面している感がある。

本研究では、この壁を打破して真に現コンピュータを凌駕する量子計算の研究に新展開をもたらすことを目指す。本申請の研究メンバは、研究業績の項にあるように ERATO その他のプロジェクトを通して量子暗号システムのイノベーション推進から新しい量子セキュアプロトコル提案、量子計算における代数アルゴリズム・量子対話証明計算量・量子通信計算量そして量子情報の基礎理論確立の研究を進めてきた。その中で、物理実現も含めた諸々の量子計算モデルを土台とし、量子対話証明等から見えてきたグラフ理論の深い関係に着目し、量子グラフ理論を創設して、それによって量子計算の研究に新しい面を展開し、量子計算能力の解明を目指す研究提案に至った。

2. 研究の目的

現コンピュータの諸限界を乗り越えるモデルとしての量子計算の計算能力解析を目指し、(1) 量子多証明者対話証明系に基づいた量子パーフェクトグラフ理論を精緻化し、そこから量子計算の量子通信計算量・量子通信路容量の諸問題にフィードバックした研究展開を行い、(2) 物理実現の観点から提案されている測定ベース量子計算とトポロジ

カル量子計算の両モデルについて、そこで現れるグラフ・結び目等の離散構造を解析し、そして(3) 格子構造と結び目と関連するグラフマイナー理論の成果やイジングモデルに関する不変多項式を量子計算モデルに展開するとともに、量子測定に対応した点中心のグラフマイナー理論を量子計算の観点から研究推進する。グラフ理論との関係を明らかにすることで、量子アルゴリズム設計で壁に直面しているところを対象領域拡張により乗り越えることを目指した。

3. 研究の方法

現行コンピュータにおける諸限界を乗り越えるモデルとしての量子計算の計算能力を解析し、新たな情報処理の可能性を切り開くことを目指し、次の3点を研究の軸に据えて取り組んだ：

(a) 複数の量子計算モデルを解析して個々と複数モデル間の変換時に現れる離散数理論問題をさらに抽出することを行い、全体研究の土台とし、研究組織の中で物理面からとコンピュータ科学面からの研究推進を両面から実施して融合研究成果をもたらし、(b) グラフマイナーとパーフェクトグラフについての量子グラフ理論をまず確立し、この理論を軸に互いに波及する量子力学と離散数理論の問題を解析し、それとともにグラフと統計物理の接点であるイジングモデルにおいても同様の研究を進め、格子グラフの拡張である周期グラフの万能量子計算性についても示し、(c) 量子多証明者対話証明の量子彩色数の発展への研究と計算量クラス QMA, QMA(2)による量子力学と離散数理論の特徴づけを通して、量子計算量理論における展開を図るとともに、これらの研究解析の道具を他の問題に適用してコンピュータ科学における成果を創出することを目指した。

上記の3つの研究テーマについて、研究メンバ間で役割分担した上で追究していくのと同時に、相互に連携しながら最終目標の達成を目指して研究を進めた。

4. 研究成果

4年間の研究活動を通して、最終的に以下の成果を得ることができた。

(1) 複数量子計算モデルでの離散数理論および物理実現からの研究【今井・村尾・山下】：物理実現に基づき、数理的に能力差の有無を示すことができる測定ベース量子計算・トポロジカル量子計算や量子回路など複数の量子計算モデルを対象として、それぞれの有する離散構造の解析を通して、量子回路・レイアウト最適化や状態変換可能性・測定の汎用実装に関するアルゴリズムなどについて広く成果を得ることができた。測定ベ

ース量子計算に関する種々の物理的考察に関する成果を、村尾が中心となつて得ることができた。逆方向に正方格子グラフを拡張した三角形格子、ハニカム格子、カゴメ格子をさらに包含する周期グラフについて、その上でのグラフ状態が測定ベース量子計算において万能性を有することを示した。また、原子再配置問題を量子コンピュータ研究での1つの方法論として、アルゴリズムによる解決を与えた。

(2) 量子グラフ理論の確立【今井・山下・Le Gall】: 研究代表者らによる従来の研究成果の中から、これまでの周期グラフ等に関する研究成果に加え、グラフマイナー理論の立場の今井の知見をマトロイド理論に関する研究協力者の知見と合わせて、測定ベース量子計算に関してさらなる応用の可能性を含めた研究指針を見出している。特に、グラフマイナーで点が中心的役割を果たす点マイナー理論と階数幅の理論を適用して、量子情報の観点からイジングモデルの分配関数計算に関する知見に至るまでの展開に今井を中心として図ることができた。

量子グラフ彩色については、量子非局所性の研究で新たな研究をもたらす量子グラフ彩色での計算量理論での還元性を導入した解析法を提案した。

また、関連してグラフのカットの劣モジュラ性最大化について、多面的な考察も行い、イジングモデルとグラフのカットの1対1対応に着目して近年注目を浴びている量子アニーリングとの関係解明につながる端緒も得ている。

(3) 多証明者量子対話証明と実数計算量解明【今井・Le Gall・河村】: 量子多証明者対話証明について、ジャーナル論文を発表するとともに、量子Arthur-Merlinゲームに関する一般化を示すことができている。実数計算量の解析も行い、さらにこれらの過程で得た知見を量子アルゴリズムへと昇華した成果を発表することもできている。

(4) 計算解析・研究情報データベース構築推進【今井・山下】: 回路設計・解析において多数の実績がある山下とともに、古典回路設計理論で重要な2分決定グラフBDDを量子計算において活用するアイデアを展開することができ、国際会議での論文発表を実現した。これは、BDDと量子情報でのテンソルネットワークを結びつけ、その階数幅(エンタングルメント幅)との対応をつけた。量子計算そのものが学際的な分野にまたがるものであるが、コンピュータ科学の論理合成等で研究されてきたBDDと量子情報との新たな関係を見出した成果となっている。

また量子計算全般とその周辺に関する研究成果も関連研究として多数上げることができた。

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 65 件)

- [1] N. Fu, A. Hashikura, and H. Imai, Proximity and Motion Planning on I_1 -embeddable Tilings, Proceedings of The Eighth International Symposium on Voronoi Diagrams in Science and Engineering, 査読有, pp.150-159, 2011
- [2] A. Hashikura, N. Fu, and H. Imai, Distance and Axis Decomposition of I_1 -embeddable Tilings, Proceedings of the 14th Korea-Japan Joint Workshop on Algorithms and Computation, 査読有, pp.130-136, 2011
- [3] Y. Matsumoto, S. Moriyama, H. Imai, and D. Bremner, Matroid Enumeration for Incidence Geometry, Discrete and Computational Geometry, Vol.47, 査読有, pp.17-43, 2011
- [4] T. Tanuma, H. Imai, and S. Moriyama, Revisiting Hyperbolic Voronoi Diagrams in Two and Higher Dimensions from Theoretical, Applied and Generalized Viewpoints, Transactions on Computational Science, 査読有, Vol.14, pp.1-30, 2011
- [5] S. Yamashita and M. Nakanishi, An Efficient Framework to Utilize Grover Search, Journal of Nanjing University of Posts and Telecommunications, 査読有, Vol.31, No.2, pp.85-94, 2011
- [6] S. Yamashita, Logic Level Circuit Optimization for Topological Quantum Computation, Proceedings of the Dagstuhl Seminar 11502: Design of Reversible and Quantum Circuits, 査読有, 2011
- [7] M. Villagra, M. Nakanishi, S. Yamashita and Y. Nakashima, Quantum Query Complexity of Hamming Distance Estimation, Proceedings of the 11th Asian Conference on Quantum Information Science, 査読有, pp.103-104, 2011
- [8] A. Matsuo, S. Yamashita, Changing the Gate Order for Optimal LNN Conversion, Proceedings of the 3rd Workshop on Reversible Computation, 査読有, pp.175-186, 2011

- [9] R. Cleve, K. Iwama, F. Le Gall, H. Nishimura, S. Tani, J. Teruyama and S. Yamashita, Reconstructing Strings from Substrings with Quantum Queries, SWAT 2012, LNCS 7357, 査読有, pp.388-397, 2012
- [10] A. Soeda, P. S. Turner and M. Murao, Entanglement Cost of Implementing Controlled-Unitary Operations, Phys. Rev. Lett., 査読有, 107, 180501, 2011.
- [11] Y. Nakata and M. Murao, Simulating Typical Entanglement with Many-Body Hamiltonian Dynamics, Phys. Rev. A., 査読有, 84.052321, 2011
- [12] J. Fukawa, F. Le Gall, and H. Imai, Quantum Coloring Games via Symmetric SAT Games, Proceedings of the 11th Asian Quantum Information Science Conference, 査読有, pp.43-44, 2012
- [13] S. Yamashita, S. Minato, and D. M. Miller, Synthesis of Semi-Classical Quantum Circuits, Journal of Multiple-Valued Logic and Soft Computing, 査読有, pp.99-114, 2012
- [14] J. Hide, Y. Nakata and M. Murao, Entanglement and the Interplay between Staggered Fields and Couplings, 査読有, Phys. Rev. A.85.042303, 2012
- [15] T. Satoh, F. Le Gall, and H. Imai, Quantum Network Coding for Quantum Repeaters, Physical Review A, 査読有, Vol.86, 032332:1-8, 2012
- [16] N. Fu, A. Hashikura and H. Imai, Geometrical Treatment of Periodic Graphs with Coordinate System Using Axis-fiber and an Application to a Motion Planning, Proceedings of the 9th International Symposium on Voronoi Diagrams in Science and Engineering (ISVD 2012), 査読有, pp.115-121, 2012
- [17] N. Fu, Y. Hirakuri, H. Imai, and A. Motoyama, Quantum States Associated with 2D Periodic Graph, Proceedings of the 12th Asian Quantum Information Science Conference(AQIS 2012), 査読有, pp.44-45, 2012
- [18] J. Fukawa, F. Le Gall, and H. Imai, Quantum Coloring Games via Symmetric SAT Games, Proceedings of the 11th Asian Quantum Information Science Conference, 査読有, pp.43-44, 2012
- [19] Shigeru Yamashita, An Optimization Problem for Topological Quantum Computation, IEEE 21st Asian Test Symposium, 査読有, pp.61-66, 2012
- [20] Francois Le Gall, Quantum Private Information Retrieval with Sublinear Communication Complexity, Theory of Computing, 査読有, Vol.8, pp.369-374, 2012
- [21] Francois Le Gall, Shota Nakagawa and Harumichi Nishimura, On QMA Protocols with Two Short Quantum Proofs, Quantum Information and Computation, 査読有, Vol.12, pp.589-600, 2012
- [22] Gabor Ivanyos, Francois Le Gall and Yuichi Yoshida, On the Distance Between Non-Isomorphic Groups, European Journal of Combinatorics, 査読有, Vol.33, pp.474-476, 2012
- [23] Norie Fu, Akihiro Hashikura, and Hiroshi Imai, Proximity and Motion Planning on 1-Rigid Planar Periodic Graphs, Transactions on Computational Science, 査読有, Vol.8110, pp.72-91, 2013
- [24] Marcos Villagra, Masaki Nakanishi, Shigeru Yamashita, Yasuhiko Nakashima, Tensor Rank and Strong Quantum Nondeterminism in Multi-party Communication, IEICE Transactions on Information and Systems, 査読有, Vol.E96-D, pp.1-8, 2013
- [25] Yoshifumi Nakata, Peter S. Turner, Mio Murao, Phase-Random States: Ensembles of States with Fixed Amplitudes and Uniformly Distributed Phases in a Fixed Basis, Phys. Rev. A, 査読有, Vol.86, 12301, 2013
- [26] J. P. Garner, O. C. O. Dahlsten, Y. Nakata, M. Murao and V. Vedral, A General Framework for Phase and Interference, New J. Phys., 査読有, Vol.15, 93044, 2013
- [27] M. Hajdusek and M. Murao, Direct Evaluation of Pure Graph State Entanglement, New J. Phys., 査読有, Vol.15, 13039, 2013

- [28] K. Fujii, Y. Nakata, M. Ohzeki and M. Murao, Measurement-Based Quantum Computation on Symmetry Breaking Thermal States, *Phys. Rev. Lett.*, 査読有, Vol.110, 120502, 2013
- [29] A. Kawamura, H. Ota, C. Rosnick, and M. Ziegler, Computational Complexity of Smooth Differential Equations, *Lecture Notes in Computer Science*, 査読有, Vol.7464, pp.578-589, 2012
- [30] S. Yamashita, S. Hiratsuka, S. Devitt, K. Nemoto, Qubit Arrangement Problems for Topological Quantum Computation, *Proceedings of the 13th Asian Quantum Information Science Conference 2013 (AQIS 2013)*, 査読有, pp.181-182, 2013
- [31] M. Hajdusek and M. Murao, Direct Evaluation of Pure Graph State Entanglement, *New Journal of Physics*, 査読有, Vol.15, 13039, 2013
- [32] Francois Le Gall and Yuichi Yoshida, Property Testing for Cyclic Groups and Beyond, *Journal of Combinatorial Optimization*, 査読有, Vol.26, No.4, pp.636-654, 2013
- [33] Francois Le Gall, Quantum Weakly Nondeterministic Communication Complexity, *Theoretical Computer Science*, 査読有, Vol.486, pp.43-49, 2013
- [34] K. Kato, F. Furrer and M. Murao, Information-Theoretical Formulation of Anyonic Entanglement, *Physical Review A*, 査読有, Vol.90, 62325, 2014
- [35] H. Hiraishi and H. Imai, BDD Operations for Quantum Graph States, *Reversible Computation*, *Lecture Notes in Computer Science*, 査読有, Vol.8507, pp.216-229, 2014
- [36] Jean-Francois Baffier, Vorapong Supakitpaisarn, Hidefumi Hiraishi, and Hiroshi Imai, Parametric Multiroute Flow and its Application to Robust Network with k Edge Failures, *Lecture Notes in Computer Science*, 査読有, Vol.8596, pp.26-37, 2014
- [37] N. A. B. Adnan, S. Yamashita, S. J. Devitt, K. Nemoto, 2D Qubit Layout Optimization for Topological Quantum Computation, *Lecture Notes in Computer Science*, 査読有, Vol.8507, pp.176-188, 2014
- [38] N. A. B. Adnan, K. Hoshi, S. Yamashita, Mapping Patterns with More Than Two Gates for Quantum Cost Reduction, 第31回量子情報技術研究会資料, 査読有, pp.111-112, 2014
- [39] Mehdi Mhalla, Mio Murao, Simon Perdrix, Masato Someya, Peter S. Turner, Which Graph States are Useful for Quantum Information Processing?, *Lecture Notes in Computer Science*, 査読有, Vol.6745, 2014
- [40] A. Soeda, S. Akibue and M. Murao, Two-party LOCC Convertibility of Quadpartite States and Kraus-Cirac Number of Two-Qubit Unitaries, *Journal of Physics A: Mathematical and Theoretical*, 査読有, Vol.47, 424036, 2014
- [41] Francois Le Gall, Quantum Complexity of Boolean Matrix Multiplication and Related Problems., *Lecture Notes in Computer Science*, 査読有, Vol.8808, pp.176-191, 2014
- [42] Francois Le Gall and Harumichi Nishimura, Quantum Algorithms for Matrix Products over Semirings, *Proceedings of the 14th Scandinavian Symposium and Workshops on Algorithm Theory (SWAT 2014)*, 査読有, LNCS 8503, pp.331-343, 2014
- [43] Francois Le Gall, Harumichi Nishimura and Seiichiro Tani, Quantum Algorithms for Finding Constant-sized Sub-hypergraphs, *Proceedings of the 20th Annual International Computing and Combinatorics Conference (COCOON 2014)*, 査読有, LNCS 8591, pp.429-440, 2014
- [44] Francois Le Gall, Improved Quantum Algorithm for Triangle Finding via Combinatorial Arguments, *Proceedings of the 55th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2014)*, 査読有, pp.216-225, 2014
- [45] Francois Le Gall, Powers of Tensors and Fast Matrix Multiplication, *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation (ISSAC 2014)*, 査読有,

pp.296-303, 2014

- [46] Akitoshi Kawamura, Hiroyuki Ota, Carsten Rosnick Martin Ziegler, Computational Complexity of Smooth Differential Equations, Logical Methods in Computer Science, 査読有, Vol.10, pp.1-15, 2014
- [47] A. Kawamura, H. Ota, C. Rosnick, and M. Ziegler, Computational Complexity of Smooth Differential Equations, Logical Methods in Computer Science, published online, 査読有, Vol.10, No.1, 2014
- [48] S. Hirahara and A. Kawamura, On Characterizations of Randomized Computation Using Plain Kolmogorov Complexity, Mathematical Foundations of Computer Science 2014, Lecture Notes in Computer Science, 査読有, Vol.8635, pp.348-359, 2014
- [49] A. Kawamura and H. Ota, Small Complexity Classes for Operators in Analysis, Mathematical Foundations of Computer Science 2014, Lecture Notes in Computer Science, 査読有, Vol.8635, pp.432-444, 2014
- [50] Stacey Jeffery, Robin Kothari, Francois Le Gall and Frederic Magniez, Improving Quantum Query Complexity of Boolean Matrix Multiplication Using Graph Collision, Algorithmica, 査読有, published online, 2015
- [51] Hirotada Kobayashi, Francois Le Gall and Harumichi Nishimura, Stronger Methods of Making Quantum Interactive Proofs Perfectly Complete, SIAM Journal on Computing, 査読有, published online, 2015
- [52] S. Nakayama, A. Soeda and M. Mura, Quantum Algorithm for Universal Implementation of Projective Measurement of Energy, Physical Review Letters, 査読有, Vol.114, 190501, 2015
- [53] Hidefumi Hiraishi, Hiroshi Imai, Yoichi Iwata, Bingkai Lin, Parameterized Algorithms to Compute Ising Partition Function, Proceedings of the 9th Hungarian-Japanese Symposium on Discrete Mathematics and Its Application, 査読有, to appear, 2015
- [54] J. Miyazaki, M. Hajdusek and M.

Mura, Analysis of the Trade-off between Spatial and Temporal Resources for Measurement-Based Quantum Computation, Physical Review A, 査読有, to appear, 2015

など

〔学会発表〕(計 43 件)

〔その他〕

ホームページ

<http://qci.is.s.u-tokyo.ac.jp/qci/qgc/>

6. 研究組織

(1)研究代表者

今井 浩(IMAI, Hiroshi)

東京大学・大学院情報理工学系研究科・教授
研究者番号：80183010

(2)研究分担者

山下 茂(YAMASHITA, Shigeru)

立命館大学・情報理工学部・教授

研究者番号：30362833

23 年度～25 年度は研究分担者として、26 年度は連携研究者として参加。

松本 啓史(MATSUMOTO, Keiji)

国立情報学研究所・情報学プリンシプル研究系・准教授

研究者番号：60272390

23 年度のみ研究分担者。24 年度以降は連携研究者として参加。

(3)連携研究者

村尾 美緒(MURAO, Mio)

東京大学・大学院理学系研究科・教授

研究者番号：30322671

研究開始時は、東京大学・大学院理学系研究科・准教授。平成 27 年 1 月より同・教授。

ルガル フランソワ(LE GALL, Francois)

東京大学・大学院情報理工学系研究科・特任准教授

研究者番号：50584299

研究開始時は、東京大学・大学院情報理工学系研究科・特任講師。平成 24 年 4 月より同・特任准教授。

河村 彰星(KAWAMURA, Akitoshi)

東京大学・総合文化研究所・講師

研究者番号：20600117

23 年度～26 年度の研究計画期間中は、東京大学・大学院情報理工学系研究科・助教。平成 27 年 4 月より、東京大学・総合文化研究科・講師。