

機関番号：12601

研究種目：基盤研究 (B)

研究期間：2008 ～ 2010

課題番号：20300002

研究課題名 (和文) 量子相関ゲームによる古典・量子両面での離散・連続最適化と
計算量の新展開研究課題名 (英文) Quantum-Classical Correlation Games and New Analyses of
Discrete-Continuous Optimization and Computational Complexity

研究代表者

今井 浩 (HIROSHI IMAI)

東京大学・大学院情報理工学系研究科・教授

研究者番号：80183010

研究成果の概要 (和文)：

現在のコンピュータの限界を超えるモデルとして量子計算を対象とし、そのパワーの源である量子相関を解析した。古典力学では現れない相関をもたらす量子相関について、離散最適化の観点からカット多面体を軸とする方法、連続最適化の観点から量子最大破れを解析し、また計算量の観点から対話型証明系との同値性を示し、量子相関の体系的に解明した。さらに量子計算モデル及び量子情報の研究へ展開をはかり、離散・連続の幾何構造を解明した。

研究成果の概要 (英文)：

Quantum Computing overcomes the barriers of current classical computers through computational power via quantum effects. This research focuses on quantum correlation as such effects. We analyze quantum correlation in a unified way as follows: (1) revealing discrete aspects of quantum correlation by the theory of cut polytopes in combinatorial optimization, (2) investigating maximum quantum violations by continuous optimization, and (3) analyzing quantum correlation by multi-prover interactive proof in computational complexity theory. Furthermore, problems in new quantum computational models and quantum information are explored through discrete and continuous geometric structures.

交付決定額

(金額単位：円)

	直接経費	間接経費	合計
2008 年度	5,500,000	1,650,000	7,150,000
2009 年度	4,700,000	1,410,000	6,110,000
2010 年度	4,400,000	1,320,000	5,720,000
総計	14,600,000	4,380,000	18,380,000

研究分野：総合領域

科研費の分科・細目：情報学・情報学基礎

キーワード：量子コンピュータ、量子計算、アルゴリズム、量子情報、離散数学

1. 研究開始当初の背景

量子情報科学は、量子力学原理で動作する新情報処理方式を研究開発する分野であり、次世代を切り拓く新計算モデル・通信モデルである。1994年にShorにより素因数分解が量子コンピュータで効率よく解けることが示され、量子計算が既存の計算モデルを凌駕しうる衝撃を与えた。以来、1990年代後半

のGroverのデータベース探索、2000年頃からの量子ウォーク、Shorのアルゴリズムの一般化の隠れ部分群問題へと量子計算研究が進展してきた。これらは特に現代の公開鍵暗号や共有鍵暗号という社会基盤に対する脅威となるというインパクトを与え続けている。一方で、量子暗号は物理的原理と量子情報理論に基づいて安全な暗号を提供する究極の建設的インパクトを与えており、これは

量子情報科学の普遍性・多面性を顕著に示している。現在では、量子暗号システムでセキュリティ度が定量的に保証されたデモンストレーションがなされる一方、量子コンピュータ実現にはまだ時間がかかると予想され、量子アルゴリズム研究も深化しているものの、広がり面での現状の問題も顕在化し、量子通信暗号と量子計算研究の間に距離感が生じてきている。そこでこれを打開して、量子情報科学全体を包括する研究原理が期待されていた。

2. 研究の目的

本研究では、情報科学の基礎は離散的構造にあるという立場から、量子情報処理での組み合わせ論を構築することを目指す。そのために、量子情報空間の離散幾何理論を構成していく。そこでは、量子状態が点として表され、状態間の近接関係が量子ダイバージェンスによって表される量子情報幾何での計算幾何が第一の対象となる。量子相関を凸多面体論から扱う計算幾何手法が第二の対象となる。研究グループメンバーのこれまでの量子情報・離散システム論の成果を量子情報幾何空間の離散構造解析に昇華することを行い、この離散幾何構造に基づいた種々の最適化技法の開発を行う。

また、本研究は計算量理論と関係する多証明者の場合の量子相関ゲームに基づく量子情報処理プロトコルの基礎を与えることも目指す。これは実現すると、対話証明モデルが計算量理論の真髄をついていることに基づき対話証明モデルがもつ通信の側面を洗い出して、量子暗号の次に魅力ある対象としての次世代量子通信の提示が期待できる。

さらに、量子計算モデルの研究にも着目し、測定ベース量子計算で現れる規則的グラフの研究も進め、その連続・離散幾何構造を明らかにすることも目指した。

3. 研究の方法

本研究課題においては研究目的に含まれる要素が多岐にわたることから、以下のように3方向から同時にアプローチを行う方法で研究を遂行した。

(1) 2証明者の基本的量子相関ゲームでの量子破れ最大化を、一般化 Bell 不等式のうち、最も基本的で小さな CHSH 不等式から順次対象を拡大して、量子最大破れの値を求めるための方法論を展開し、その範囲を広げる。2証明者の場合の一般化 Bell 不等式の量子最大破れを求める問題の計算量はまだわかっていないが、たとえ NP 困難であっても実際の実験系で用いる規模のもので量子最大破れを求めることは非常に意義があることで

ある。量子情報の諸問題での最適化手法の展開をもたらすことにも取り組む。

(2) 量子相関ゲームは、上述したように半定値計画・多項式計画という連続最適化研究やグラフのカットという離散最適化と関係する。さらに量子エンタングルメントの構造を明らかにする離散構造のとして有向マトロイドに着目し、量子エンタングルメントと Grassmann-Plücker 関係式の関係に基づき、有向マトロイド実現性判定とその先のデータ整備を行う。

(3) 量子状態を用いて測定によって計算を実現していく新方式として注目されているクラスタ状態による計算も調査し、量子相関ゲームの設定との関係を調べる。量子相関ゲームそのものの繰り返しを計算とするモデルについて、それに新たな操作を加えることによって実現できる量子計算について研究を推進し、グラフ等の問題へのフィードバックを考える。

4. 研究成果

(1) 本研究では、情報科学の基礎が離散的構造にあるという立場から、量子情報処理において組合せ論を構築することを目指している。研究計画初年度であった 20 年度においては、まず量子 Bell 不等式の最大化問題を半定値計画を用いて解析することを目指して、計算解析と離散構造の両面から研究を進めた。離散構造の最たるものである有向マトロイドについては、その基礎である Grassmann-Plücker 関係式によって、純粋な量子状態において量子もつれを解析できることがわかっており、本研究では有向マトロイドの実現可能性判定問題の研究を進めることによって、数値計算により組合せ的判定が行えることを示し、さらに大規模化対処に有用な知見を得ることに成功した。大規模化の検討を可能にするために、離散構造列挙に関してこれまで未到達の領域に挑戦して列挙実現も行い、そこで得られた成果を今後データベースとして活用するための整備も行った。

(2) 量子状態の成す空間の連続性を離散化して、これまで計算が困難であった問題に対する解決を目指した研究も進めた。具体的には、従来の 1 量子ビット (2 準位系) の量子通信路容量計算についての研究メンバーの既存成果をさらに発展させて、3 準位系量子状態の量子通信路の容量を計算するために、量子状態空間で計算幾何の最少包含球アルゴリズムの適用ができることを基礎的性質から証明し、実際に 3 準位系量子通信路における容量計算に適用した。この方法では、受信量子状態を離散化したレベルで最適な容量が計算可能となり、他の局所改善法に基づく方

法では最適性に関して保証できない課題を克服している。一方で、離散化による計算量増大への対処が今後の課題となっている。

(3) 量子情報処理を組合せ論の観点から調べることにより、量子情報処理の設計問題を解析し、量子情報空間の離散幾何理論の構築を行った。まず、量子状態が点として表され、状態間の近接関係が量子ダイバージェンスによって表される量子情報幾何での計算幾何については、双曲幾何との対応を調べ、それによる近接関係を Voronoi 図を通して調べることを行った。また、その応用として、古典情報処理でのセンサーネットワークの研究にも関連づけることができた。

(4) 量子相関ゲームの研究において、カット多面体による統一的 Bell 不等式の導出方式を与えるしかを、**Mathematical Programming** ジャーナルにおいて発表し、1つの理論として確立した。また、量子相関の対話証明の計算量理論との関係を明らかにし、古典計算量理論でのいわゆるユニークゲーム予想についても考察を加えることができた。多項式計画そのものの研究進展も数理計画全般の中で推進・注視し、それを本研究計画に反映させて量子相関ゲームでの最適化技法に融合させるという課題に取り組んだ。計算においては、半定値計画および多項式計画の並列実装の活用など、より大規模な問題が解けるようにした。最終年度の研究では、多証明者の場合の量子相関ゲームの解析も行い、従来未解決であったランク1測定とランクが2以上の測定によって量子相関ゲームで能力差が出ることを新たに示し、これについては来年度以降に成果発表を行う準備を順調に進めている。

(5) 量子情報がナノテクノロジー技術と関連する点に着目し、原子の表面結晶構造に現れるグラフや測定ベース量子計算方式で現れる正方格子等のグラフについて、それらの構造を解析するとともに、その解析結果の性質を用いた原子操作の設計問題や量子計算がユニバーサルになるクラスのグラフ問題を明らかにした。総体として量子情報における離散幾何・組合せ解析を実現した。

特に、表面原子結晶格子構造において隣接原子対を交換を繰り返して所望の特定原子の配置を実現する問題に対して、最適交換操作列を離散最適化と計算幾何の技法で求める方法を与えた。このために、格子グラフの離散・連続幾何構造を解析し、それをまた測定ベース量子計算の成果へと拡張することができた。

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 11 件)

N. Fu, H. Imai and S. Moriyama, Voronoi Diagrams on Periodic Graphs. Proceedings of 2010 International Symposium on Voronoi Diagrams in Science and Engineering (ISVD 2010), 査読有, 2010, pp.189-198.

T. Tanuma, H. Imai and S. Moriyama, Revisiting Hyperbolic Voronoi Diagrams from Theoretical, Applied and Generalized Viewpoints. Proceedings of 2010 International Symposium on Voronoi Diagrams in Science and Engineering (ISVD 2010), 査読有, 2010, pp.23-32.

H. Miyata, S. Moriyama, and H. Imai, Deciding Non-Realizability of Oriented Matroids by Semidefinite Programming. Pacific Journal of Optimization, 査読有, Vol. 5, 2009, pp. 211-224

D. Avis, H. Imai and T. Ito, Generating Facets for the Cut Polytope of a Graph by Triangular Elimination. Mathematical Programming, 査読有, Vol.112, No.2, 2008, pp.303-325.

N. Fu and H. Imai, Shiftability of Atoms on a Lattice to Any Configuration in Minimum Moves. Proceedings of the Japan-Korea Workshop on Algorithms and Computation (WAAC 2008), 査読有, 2008, pp.28-35.

K. Kato, M. Oto, H. Imai and K. Imai, Computational Geometry Analysis of Quantum State Space and Its Applications, In 'Generalized Voronoi Diagram: A Geometry-Based Approach to Computational Intelligence' (M. L. Gavrilova, ed.), Springer, October 2008, pp.67-108.

K. Kato, H. Imai and K. Imai, Smallest Enclosing Ball Problem in a Quantum State Space and Its Application. Proceedings of the 5th International Symposium on Voronoi Diagrams in Science and Engineering (ISVD 2008), 査読有, 2008, pp.123-132.

T. Takahashi, S. Moriyama and H. Imai, A Note on the Upper Bound Derived by Semidefinite Programming for the Maximum Quantum Violation of Bell Inequalities. Proceedings of the 8th Asian Confe-

rence on Quantum Information Science, 査読有, Vol.1, 2008, pp.127-128.

N. Fu and H. Imai, Solvability of Sliding Atoms Puzzle on a Lattice. Proceedings of the 8th Asian Conference on Quantum Information Science, 査読有, 2008, pp.165-166.

H. Miyata, S. Moriyama and H. Imai, Analyzing Geometric Realizability Problems by Semidefinite Programming. Proceedings of the Kyoto RIMS Workshop on Computational Geometry and Discrete Mathematics, 査読有, 2008, pp.6-9.

Y. Matsumoto, S. Moriyama, H. Imai and D. Bremner, Large Scale Matroid Enumeration and Analysis of Orientation. Proceedings of the Kyoto RIMS Workshop on Computational Geometry and Discrete Mathematics, 査読有, 2008, pp.10-13.

〔学会発表〕(計9件)

今井浩, 幾何から量子そしてその先, 「計算幾何学の発展と未来」研究集会, 2011年3月11日, 京都大学.

今井浩, 夫紀恵, 森山園子, 量子グラフ状態による情報処理, 「ナノ量子情報エレクトロニクスの進展」シンポジウム, 2010年12月22日, 東京大学.

今井浩, Feynmann の2つの提唱からグラフと計算量への展開, 電子情報通信学会第23回量子情報技術研究会, 2010年11月15日, 東京大学.

橋倉彰宏, 夫紀恵, 今井浩, periodic graph の static graph に関する一考察, 電子情報通信学会コンピュテーション研究会, 2010年9月29日, 長岡技術科学大学.

H. Imai, Quantum Computational Geometry and Quantum Cryptography, Keynote, 2009 International Workshop on Computing, 2009年6月16日, Academia Scinica (台湾, 台北市).

H. Imai, Standardization Directions of Geographic Information, Japanese-Austrian Workshop on Natural Language and Spatio-Temporal Information, 2009年9月30日, 東京大学山上会館.

H. Imai, Guaranteeing the Security Quantitative for a Generalized Decoy State Quantum Key Protocol Incorporating Finite Statistics, Invited Talk, 国際シンポジウム「量子技術に関する物理」, 2008年11月28日, 奈良県新公会堂.

今井浩, 今井桂子, 松本宜丈, 森山園子, BDD を用いたグラフの Tutte 多項式計算の再考察, 電子情報通信学会コンピュテーション研究会, 2008年10月10日, 東北大学.

今井浩, 量子情報と組合せ・半定値最適化, 招待講演, 組合せ最適化セミナー, 2008年7月29日, 京都大学数理解析研究所.

〔図書〕(計0件)

〔産業財産権〕

○出願状況(計0件)

○取得状況(計0件)

〔その他〕

なし

6. 研究組織

(1) 研究代表者

今井 浩 (HIROSHI IMAI)

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

なし

(3) 連携研究者

なし