様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　６　月　２８　日現在

機関番号：　９４３０５
研究種目：　基盤研究(C)（一般）
研究期間：　2013～2015
課題番号：　２５３３００２１

研究課題名（和文）非可換群上の量子フーリエ変換とその応用

研究課題名（英文）Quantum Fourier Transform over Non-Abelian Groups and Its Application

研究代表者

河野　泰人（Kawano, Yasuhito）

日本電信電話株式会社ＮＴＴコミュニケーション科学基礎研究所・メディア情報研究部・主任研究員

研究者番号：４０３９６１８０

交付決定額（研究期間全体）：（直接経費）　　2,100,000円

研究成果の概要（和文）：量子コンピュータは、量子重ね合わせを利用して超高速計算を実行する次世代のコンピュータで、人工知能などへの応用が期待されている。量子コンピュータの計算速度は、量子アルゴリズムと呼ばれる専用のソフトウェアによってもたらされる。そのため、量子コンピュータの実用化には、量子アルゴリズムの研究が欠かせない。本研究では、非可換群上の量子フーリエ変換を利用して、従来から知られた因数分解を高速に実行する量子アルゴリズムを拡張し、人工知能に応用可能な高速の量子アルゴリズムを新たに提案した。本研究の成果は、人工知能の他、ポスト量子暗号と呼ばれる次世代暗号の研究にも応用できる。

研究成果の概要（英文）：A quantum computer, which is expected to be the next generation machine, achieves high-performance computing using superpositions of qubits. Its performance depends on the quantum algorithms. The study of quantum algorithms is then necessary for practical applications of quantum computers. We proposed the fastest quantum Fourier transform over non-abelian groups at this moment. In addition, we proposed a new quantum algorithm that solves lattice problems by generalizing a known algorithm that factors large composite integers. Our result can be applied to the studies of artificial intelligence and the next-generation post-quantum public-key cryptography.

研究分野：　量子情報科学

キーワード：　量子コンピュータ　量子アルゴリズム　量子フーリエ変換　量子暗号　ポスト量子暗号　格子暗号　非可換群　表現論

１．研究開始当初の背景

近年、量子コンピュータを取り巻く研究環境は大きく変わり、基礎研究だけでなく、実用化を視野に入れた研究が盛んになってきている。例えば、グーグルは D-wave 社（カナダ）の販売する量子コンピュータを導入し、量子人工知能の研究に取り組んでいる。また、日本でも、革新的研究開発推進プログラム（ImPACT）の山本喜久プログラム・マネージャーが指揮するプロジェクト「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」において、コヒーレントイジングマシンによる大規模な人工スピンネットワークの生成に成功している。これらの量子コンピュータは、量子アニーリングと呼ばれる方法を採用し、理論的に予想される量子コンピュータの性能の一部しか引き出していない。しかし、遠い将来にしか実用化されないと思われてきた量子コンピュータが部分的には実現可能であり、古典コンピュータを上回る性能を発揮することを実証した点において、大きな意義がある。

量子コンピュータが注目を集めたのは、1994 年にショーア（現 MIT 教授）が因数分解を高速に解く量子アルゴリズムを発表したことに始まる。因数分解の困難さはインターネットで使用される RSA 暗号の安全性の根拠となっているため、量子コンピュータが開発されれば RSA 暗号が解読されるという結果は、当時の暗号研究に大きな衝撃を与えた。この発表が契機となり、現在、暗号研究分野では、量子コンピュータでも解けない公開鍵暗号―ポスト量子暗号と呼ばれる―の研究が盛んに行われている。ポスト量子暗号では、量子コンピュータが得意とする長い周期を発見する問題（因数分解はこのような問題の一つである）の使用を避け、それ以外の問題をもとにプロトコルを設計する。一方、量子アルゴリズム研究の分野では、ショーアの発表以降、ショーアのアルゴリズムの拡張が研究されてきた。ショーアのアルゴリズムの主要部分は量子フーリエ変換であるため、量子フーリエ変換の拡張とその応用に関する研究は、早期の頃からたくさんの研究が行われている。しかし、周期を発見する問題以外への応用は容易ではなく、現在、ポスト量子暗号で使用される問題に対する効率的な量子アルゴリズムは見つかっていない。また、人工知能で研究対象とされる NP 問題に対して、古典コンピュータよりも高速な量子アルゴリズムは提案されているものの、そうした問題を効率的に解く量子アルゴリズムも発見されていない。

量子コンピュータを使って、古典コンピュータに対する指数的な高速化を目指す場合、そこで使用される量子アルゴリズムの主要部分は限定される。そのような方法のうち、現時点で最も成功しているのは、量子フーリエ変換である。ショーアのアルゴリズムで用いられる量子フーリエ変換は可換群上の量子フーリエ変換であり、非可換群上の量子フーリエ変換は、その自然な拡張である。非可換群上の量子フーリエ変換は、非可換群を取り換えることにより異なる変換となり、応用できる問題も変化する。中でも、最も注目されている非可換群は、２面体群と対称群である。２面体群はポスト公開鍵暗号の一種である格子暗号に、そして、対称群は人工知能の研究対象であるグラフ同型性判定問題に応用できるからである。

研究代表者と研究分担者は、2008 年から 3 年間、科研費基盤研究（C）「行列分解を用いた量子回路設計とその応用」により、量子フーリエ変換の拡張とその応用に関する研究に取り組んだ。そして、研究終了後も引き続き研究を行い、本科研費の申請時点（2012 年秋）で、対称群上の量子フーリエ変換を効率的に実行する量子回路の構成に部分的に成功していた。本科研費においては、これらの研究成果をさらに発展させ、非可換群上の量子フーリエ変換を効率的に実行する量子回路を開発し、格子問題やグラフ同型性判定問題などの問題に応用することにより、ポスト量子暗号や人工知能研究、およびこれに関連する研究分野に対するハイ・インパクトな研究成果の発表を目指した。

２．研究の目的

本研究の目的は、非可換群上の高速な量子アルゴリズムの開発、およびその量子アルゴリズムの応用により、ポスト量子暗号や人工知能の研究に必要な実用的問題に対する効率的量子アルゴリズムを発見し、量子コンピュータ上に実装して、それらの問題を実用時間で解くことにより、従来の古典コンピュータだけではなし得ない高度な ICT 社会を実現することにある。ショーアのアルゴリズムは、量子コンピュータ開発の重要性を認識させ、同時に、量子コンピュータに対する巨額の研究開発投資を促すきっかけとなった。特に、北米では、暗号解読、および人工知能研究の進展を目指して、量子コンピュータの開発に投資する出資者が数多く現れた。D-wave の成功は、こうした旺盛な投資によってもたらされたものである。近年、北米では量子コンピュータの開発を目標として、量子コンピュータの研究グループを拡充する大学や研究機関が増えている。量子コンピュータの研究対象として、ポスト量子暗号や人工知能の問題を選んでいるのは、これらの分野における問題が量子アルゴリズムの長年の重要問題だということだけでなく、近年、社会的に特に注目度が高く、豊富な応用が期待でき、量子コンピュータの開発投資に寄与する可能性が高いからである。また、目的を実現するためには、今後、量子アルゴリズムの理論的な研究に限定せず、実際の量子コンピュータへの実装も必要となってくるだろう。

３．研究の方法

研究を 2 つの課題に分割し、それぞれについて、以下の方法で研究を進めた

研究課題１は、「数式処理を用いた非可換群上のフーリエ変換アルゴリズムの研究」である。すでに述べたとおり、研究代表者らは対称群上の量子フーリエ変換に関して、既存の量子回路を高速化するアルゴリズムに関する部分結果を得ていた。この研究成果をベースにして、量子アルゴリズムをさらに改良し、対称群上の古典フーリエ変換に関する、世界最高速のアルゴリズムの提案を目指した。この課題達成のために、古典コンピュータ上での数式処理ソフトを用いた研究を重視した。実際、効率的な量子アルゴリズム構成のために用いたアイディアは、数式処理ソフトで量子フーリエ変換を実装し、実行する過程で見つかったものである。

研究課題２は、「非可換群上のフーリエ変換の応用に関する研究」である。この研究は、課題１で得られた量子フーリエ変換を利用するため、課題１よりも半年遅れて、研究初年度の後半から研究が始まった。従来、量子フーリエ変換を応用する場合、標準アルゴリズムと呼ばれているショーアのアルゴリズムの自然な拡張が知られている。この標準アルゴリズムの理論的な枠組みを踏襲しつつ、新たなアイディアを投入し、量子アルゴリズムの発見に取り組んだ。研究課題１と同様、ここでも数式処理ソフトでのシミュレーション実験を重視している。実際、量子アルゴリズムの開発にあたって、Mathematica によるシミュレーション実験を重ね、得られたデータをもとに量子アルゴリズムを改良している。研究開始当初、研究対象とする問題はグラフ対称性判定問題だったが、新しい量子アルゴリズムの発見が困難だと判断し、格子問題に照準を変え、研究を進めた。

本研究の学術的な特色として、量子アルゴリズムの設計にコンピュータによる設計支援を取り入れている点が挙げられる。従来、量子回路（アルゴリズム）の設計は人間の直感と手計算に頼っており、それゆえ、設計に関して限界があった。本研究では、数式処理技術を用いた量子回路の設計支援を積極的に取り入れることによって、量子アルゴリズムの発見に取り組んだ点が、新たな試みとして注目される。

４．研究成果

2 つの課題「研究課題１．数式処理を用いた非可換群上のフーリエ変換アルゴリズムの研究」および「研究課題２．非可換群上のフーリエ変換に関する研究」のそれぞれについて、以下のような研究成果が上がった。

まず、課題１に関する研究成果をまとめる。本研究計画の初年度に、対称群上の量子フーリエ変換を実行する量子回路を効率化し、量子情報技術研究会 QIT（Quantum Information Technology Symposium，北大，日本）、国際会議 ISSAC2013（International Symposium on Symbolic and Algebraic Computation，ノースウェスタン大，アメリカ）、国際会議 QIP2014（Conference on Quantum Information Processing，バルセロナ，スペイン）で発表した。さらに、この量子アルゴリズムを、Mathematica のプログラムで古典コンピュータ上に実装し、処理時間を計測した。本研究計画の二年目に、このアルゴリズムをさらに改良し、対称群上の量子フーリエ変換として現時点で世界最速のアルゴリズムを ISSAC2014（International Symposium on Symbolic and Algebraic Computation，神戸大，日本）で発表した。この研究の論文は、ACM のジャーナル CCA (Communications in Computer Algebra)から出版された。最終年度には、それらの研究成果をまとめた論文が、海外ジャーナル Journal of Symbolic Computation(Elsevier)に採録された。この論文の雑誌掲載は、本科研費終了後の本年度 7 月の予定だが、Web 上では電子版が既に公開されている。

課題 2 に関する研究成果は、以下のとおりである。格子問題に対する量子アルゴリズムの研究は、研究計画初年度の後半から開始した。そして、研究計画 2 年目に、特定の場合に従来よりも高速に解ける量子アルゴリズムを開発し、特許出願をした。研究計画 3 年目に、上記の量子アルゴリズムを拡張し、新しい量子アルゴリズムの開発にほぼ成功した。得られた量子アルゴリズムは格子問題に関するアルゴリズムで、上記のような特定の場合に限らず、格子問題に応用することができる。この成果の部分結果は国際会議 QIP2016（Conference on Quantum Information Processing，バンフ，カナダ）で発表済みで、それをさらに発展した結果を論文に執筆中である。また、研究計画書の課題 2 に掲載した新たな研究分野への応用の一環として、量子暗号の安全性自動証明に関する研究にも取り組み、得られた成果が海外ジャーナル Journal of Symbolic Computation (Elsevier)に採録された。この論文は、最終年度 3 月に雑誌掲載済みである。

研究課題１はほぼ計画通りに研究が進み、満足できる成果が得られた。また、研究課題２については、計画進捗は少し遅れたものの、最終的に当初目標としていた量子アルゴリズムの発見には成功し、ほぼ満足できる結果だった。また、当初予定していた計画を超えた成果として、量子暗号に関する研究成果も得られ、全体を通してみれば、本科研費の研究は、十分な成果を挙げたと評価している。

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　2 件）

Yasuhito Kawano and Hiroshi Sekigawa: Quantum Fourier transform over symmetric groups --- improved result, Journal of Symbolic Computation, Volume 75, pp. 219-243 (July-August 2016).

Takahiro Kubota, Yoshihiko Kakutani, Go Kato, Yasuhito Kawano, and Hideki Sakurada: Semi-automated verification of security proofs of quantum cryptographic protocols, Journal of Symbolic Computation, Volume 73, pp. 192-220 (March-April 2016).

〔学会発表〕（計　6 件）

Yasuhito Kawano and Hiroshi Sekigawa: Quantum Algorithm for Lattice Problems, Conference on Quantum Information Processing (QIP 2016), Banff, Canada (January 11-15, 2016).

Yasuhito Kawano and Hiroshi Sekigawa: Quantum Fourier Transform over Symmetric Groups --- Improved Result, ACM Communications in Computer Algebra, Volume 48, No. 3, Issue 189, pp.127-129, DOI 10.1145/2733693.2733708 (September 2014).

Yasuhito Kawano and Hiroshi Sekigawa: Quantum Fourier Transform over Symmetric Groups --- Improved Result, Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation (ISSAC 2014), pp. 31-33, Kobe University, Kobe, Japan (July 23-25, 2014).

Yasuhito Kawano and Hiroshi Sekigawa: Quantum Fourier Transform over Symmetric Groups --- Improved Result, XVII Conference on Quantum Information Processing (QIP 2014), Barcelona, Spain (February 2-6, 2014).

Yasuhito Kawano and Hiroshi Sekigawa: Quantum Fourier Transform over Symmetric Groups, Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation (ISSAC 2013), pp. 227-234, Northeastern University, Boston, USA (June 26-29, 2013).

Yasuhito Kawano and Hiroshi Sekigawa: QFT Algorithm over Symmetric Groups, The 28th Quantum Information Technology Symposium (QIT28), pp. 62-63, Hokkaido University, Japan (May 27-28, 2013).

〔産業財産権〕

○出願状況（計　1 件）

名称：量子演算方法
発明者：河野泰人
権利者：日本電信電話株式会社
種類：特許
番号：2014184315
出願年月日：2014 年 9 月 10 日
国内外の別： 国内

６．研究組織
(1)研究代表者
河野泰人（日本電信電話株式会社 NTT ｺﾐｭﾆｹｰｼｮﾝ科学基礎研究所・メディア情報研究部・主任研究員）

研究者番号：40396180

(2)研究分担者
関川浩（東京理科大学・理学部・教授）

研究者番号：00396178