様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年６月１２日現在

機関番号：12601
研究種目：研究活動スタート支援
研究期間：2010～2011
課題番号：22800006
研究課題名（和文）　量子計算技術による計算機代数の新展開

研究課題名（英文）　New Developments in Computer Algebra using Techniques from Quantum Computing

研究代表者
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・講師
研究者番号：50584299

研究成果の概要（和文）：
代数的な構造を備えている問題をより効率的に取り扱うために、量子計算技術による新しいアプローチを開発した。主な成果として、性質検査という枠組で特定の群のクラスを区別するアルゴリズムの構築に成功し、ブール行列積を求める高速の量子アルゴリズムも構築した。また、このアプローチを通信理論と暗号理論にも応用し、量子誤り訂正符号の復号化問題が NP-困難であることを示し、プライバシー保護などの制約下での量子情報の通信が効率的に行える新しい手法も提示した。

研究成果の概要（英文）：
We developed new approaches based on techniques from quantum computing to efficiently handle computational problems with an algebraic structure. Among our main results, we constructed new algorithms for distinguishing, in the framework of property testing, classes of groups, and new quantum algorithms for computing efficiently the product of two Boolean matrices. As applications of these novel approaches, we succeeded in proving the hardness of decoding problems arising in quantum communication, and in constructing new protocols for several tasks such as privacy-preserving communication.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２０１０年度	1,250,000	375,000	1,625,000
２０１１年度	1,110,000	333,000	1,443,000
年度			
年度			
年度			
総　計	2,360,000	708,000	3,068,000

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：アルゴリズム、計算機代数、量子計算

１．研究開始当初の背景

(1)量子コンピュータは量子力学の法則に基づく新しい計算パラダイムである。1994 年に因数分解と離散対数問題を速く解く量子アルゴリズムが発表され、情報科学や暗号の世界に大きなインパクトを与えた。そのあと 1990 年代後半は量子探索という手法が発見され、2000 年代からは量子ウォークなど新しいテクニックがさらに提案され、様々な量子アルゴリズムが構築されてきた。

(2)知られている量子アルゴリズムの中で、代数的な構造を持つ問題を解くアルゴリズムが多い。主な例として、因数分解の拡張である隠れ部分群問題や可解群上の問題などが挙げられる。しかし、こういった量子アルゴリズムが多数存在するにも関わらず、問題の代数的な構造との正確な関係がまだ明らかになっておらず、大きな課題がたくさん残っていた。

２．研究の目的
本研究の目的は、数学的な構造を備えている計算問題を効率的に取り扱うために、新しいアプローチを開発することである。代数的な構造を持つ既知の計算問題に対して、従来のアルゴリズムより高速な量子アルゴリズムの構築を目標としている。構造が明らかでない計算問題に対しては、代数的な要素を特定し、計算量の究明を目指す。また、このアプローチを通信理論や暗号理論の諸問題に応用し、新しい量子プロトコルを構築することも目標としている。

３．研究の方法
(1)まずは性質検査、線形代数、符号理論、ネットワーク通信、暗号理論という五つの枠組みに分けて本研究のアプローチを推進した。それぞれの枠組みにおいて、問題の数学的な要素を特定し、古典・量子アルゴリズムの適用性及び限界を厳密に究明した。

(2)次にそれぞれの枠組みで得られた成果の統一を目指した。共通点を特定するとともに、アプローチを少しずつ拡張した。

(3)得られた成果を国内・国際会議などで発表することに力を注ぎ、本研究の成果の周知を行った。

４．研究成果
本研究により、以下の成果が得られた。

(1)性質検査という枠組みで、特定の群のクラスを区別する問題に着目し、古典の質問計算量の強い下界を初めて導いた。この成果によって、従来のコンピュータの計算能力の限界を明らかにする事とともに、量子コンピュータの優位性を確立した。また、巡回群に対しては多項式時間アルゴリズムを構築することに成功した。この手法を一般の可換群にさらに拡張し、同型でない二つの群の距離の最小値を求めるという、１９９２年にDrapalによって提示された離散数学の未解決問題を解くことに成功した。

(2)行列の積を計算する問題も研究の対象にした。この問題は数学や計算機科学において極めて重要な問題でありながら、行列積の計算量が未だ明らかになっていない。しかしながら、スペシャルケースであるブール行列に着目し、この問題の組合せ論的な要素を特定することによって積の計算を高速化する新しい手法を導き、ブール行列積を求める高速の量子アルゴリズムの構築に成功した。

(3)量子計算や量子通信の実現に必要不可欠な量子誤り訂正符号(量子 stabilizer 符号)にも着目した。従来古典符号の復号化問題の計算量が解明されている一方で、量子符号の場合計算量が、正確的に明示されていなかった点において、量子誤り訂正符号の代数的な構造を用いて、復号化問題が NP-困難であることを示した。この結果によって、McEliece暗号をはじめ、復号化問題に基づく公開鍵暗号の量子系への拡張の基盤を築いた。

(4)ネットワーク上で情報を効率的に送信する技法であるネットワーク符号についても研究を進め、古典ネットワーク符号化が可能である全てのネットワーク形状において、同じ形状の量子ネットワークでも古典通信の補助的利用のもとに、量子情報の完全な伝送が効率的に行えることを示した。さらに、既存の結果より伝送の際、必要な補助的古典通信の量を大幅に削減することにも成功した。

(5)代数学に基づく多者間セキュア計算プロトコルの構成にも取り組んだ。プライバシーを考慮した情報検索という暗号理論の基礎的な問題に着目し、１個のデータベースの場合、データベースのサイズより少ない通信量（準線形計算量）の量子プロトコルを構成することに初めて成功した。古典通信のみを用いた場合、そのようなプロトコルが存在しないため、この成果によって量子情報の優位性のさらなる確立が示されたことになる。

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８件）

① F. Le Gall, Improved Output-Sensitive Quantum Algorithms for Boolean Matrix Multiplication, Proceedings of the 23rd Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2012), 査読有, 2012, pp.1464-1476, http://siam.omnibooksonline.com/2012SODA/data/papers/183.pdf

② F. Le Gall, Y. Yoshida, Property Testing for Cyclic Groups and Beyond, Journal of Combinatorial Optimization, 査読有, 2012, 印刷中,
DOI: 10.1007/s10878-011-9445-8

③ G. Ivanyos, F. Le Gall, Y. Yoshida, On the distance between non-isomorphic groups, European Journal of Combinatorics, 査読有, Vol.33, No.4, 2011, pp.474-476,
DOI : 10.1016/j.ejc.2011.10.009

④ S. Aaronson, F. Le Gall, A. Russell, S. Tani, The One-Way Communication Complexity of Subgroup Membership, Chicago Journal of Theoretical Computer Science, 査読有, 2011,
DOI:10.4086/cjtcs.2011.006

⑤ Y. Inui, F. Le Gall, Quantum Property Testing of Group Solvability, Algorithmica, 査読有, Vol.59, No.1, 2011, pp.35-47,
DOI: 10.1007/s00453-009-9338-8

⑥ H. Kobayashi, F. Le Gall, H. Nishimura, M. Roetteler, Constructing Quantum Network Coding Schemes from Classical Nonlinear Protocols, Proceedings of the 2011 IEEE International Symposium on Information Theory (ISIT 2011), 査読有, 2011, pp. 109-113,
DOI: 10.1109/ISIT.2011.6033701

⑦ M.-H. Hsieh, F. Le Gall, NP-hardness of Decoding Quantum Error Correction Codes, Physical Review A, 査読有, Vol.83, 2011, 052331,
DOI:10.1103/PhysRevA.83.052331

⑧ H. Kobayashi, F. Le Gall, H. Nishimura, M. Roetteler, Perfect Quantum Network Communication Protocol Based on Classical Network Coding, Proceedings of the 2010 IEEE International Symposium on Information Theory (ISIT 2010), 査読有, 2010, pp. 2686 - 2690,
DOI:10.1109/ISIT.2010.5513644

〔学会発表〕(計 15 件)

① 佐藤貴彦, ルガル フランソワ, 量子中継器ネットワークのための量子ネットワークコーディング, 第 25 回量子情報技術研究会 (QIT 25), 2012 年 1 月 22 日, 大阪大学

② F. Le Gall, S. Nakagawa, H. Nishimura, On QMA Protocols with Two Short Quantum Proofs, 第 25 回量子情報技術研究会 (QIT 25), 2012 年 1 月 21 日, 大阪大学

③ F. Le Gall, Improved Output-Sensitive Quantum Algorithms for Boolean Matrix Multiplication, 15th Workshop on Quantum Information Processing (QIP 2012), 2011 年 12 月 15 日, Montreal (カナダ)

④ J. Fukawa, H. Imai, F. Le Gall, Quantum Coloring Games via Symmetric SAT Games, 11th Asian Quantum Information Science Conference (AQIS 2011), 2011 年 8 月 25 日, Busan (韓国)

⑤ F. Le Gall, Property Testing for Cyclic Groups and Beyond, 17th Annual International Computing and Combinatorics Conference (COCOON 2011), 2011 年 8 月 16 日, Dallas (アメリカ)

⑥ R. Cleve, K. Iwama, F. Le Gall, H. Nishimura, S. Tani, J. Teruyama, S. Yamashita, Reconstructing Strings from Substrings with Quantum Queries, 4th Annual Meeting of the Asian Association for Algorithms and Computation (AAAC 2011), 2011 年 4 月 17 日, HsinChu (台湾)

⑦ H. Kobayashi, F. Le Gall, H. Nishimura, M. Roetteler, Constructing Quantum Network Coding Schemes from Classical Nonlinear Protocols, 14th Workshop on Quantum Information Processing (QIP 2011), 2011 年 1 月 13 日, Singapore (シンガポール)

⑧ ルガル フランソワ, 量子ネットワーク符号, 第 23 回量子情報技術研究会 (QIT 23), 2010 年 11 月 15 日, 東京大学

⑨ F. Le Gall, Quantum Algorithms for Algebraic Problems, Workshop on Post-Quantum Security Models, 2010 年 10 月 12 日, Paris (フランス)

⑩ F. Le Gall, An Efficient Quantum Algorithm for some Instances of the Group Isomorphism Problem, 第 22 回量

子情報技術研究会（QIT 22），2010 年 5 月 11 日，大阪大学

〔その他〕
ホームページ
http://francoislegall.com/

６．研究組織
(1)研究代表者
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・講師
研究者番号：50584299