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　 ２ 日現在

機関番号：１２６０１
研究種目：若手研究(B)
研究期間：2012～2015
課題番号：２４７００００５

研究課題名（和文）代数問題に対する量子アルゴリズムの新展開とその応用

研究課題名（英文）New developments and applications of quantum algorithms for algebraic problems

研究代表者
ルガル　フランソワ（LE GALL, FRANCOIS）

東京大学・情報理工学（系）研究科・准教授

研究者番号：５０５８４２９９

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：本研究の目的は、代数問題を解くための新しいアプローチを開発することである。研究期間内に得られた最も重要な成果として、行列乗算を計算する新しいアルゴリズムの構築が挙げられる。行列乗算の計算は数学及び理論計算機科学の中核問題であり、1969年に巧妙な行列積アルゴリズムが示されて以来、70年代と80年代にその研究が盛んに行われてきた。我々は、正方形行列の乗算及び長方形行列の乗算を従来のアルゴリズムより速く計算するアルゴリズムを構築し、20年来できなかった改良を行うことに成功した。

研究成果の概要（英文）：The purpose of this research is to develop new approaches to solve algebraic problems. The most significant achievements realized during the four years of this project are the design of new algorithms for matrix multiplication. Computing the product of two matrices is one of the most fundamentals problems in mathematics and computer science. Research on matrix multiplication algorithms started in 1969, and then flourished in the 70s and the 80s. Our main achievements are the construction of new algorithms computing the product of two square matrices or two rectangular matrices faster than all previously known algorithms, which gives the first improvements in 20 years.

研究分野：アルゴリズム、計算量理論、量子計算

キーワード：代数問題　量子計算　アルゴリズム

１．研究開始当初の背景

Quantum computation is a computation paradigm proposed in the early 90s that is based on the principles of quantum mechanics. Part of its power comes from its ability to handle computational problems that possess an appropriate algebraic structure in a way incomparable to classical algorithms. One of the main research directions has then been to clarify for which computational problems such an exponential speed-up can be obtained. Very quickly, a framework called the Hidden Subgroup Problem (HSP) was introduced to characterize computational problems with an algebraic structure that are candidate for exponential speed-up. For a decade, and with only few exceptions, research on algebraic aspects of quantum computation has been driven by the HSP. The HSP is nevertheless not the main motor of research on quantum algorithms anymore, and other approaches are needed.

２．研究の目的

The main purpose of this research is to further explore new approaches and develop new techniques to handle algebraic problems on a quantum computer. The core principle of this project is to combine in a novel way the latest developments in computer algebra with the latest developments in quantum computing, in order to design new quantum techniques and then obtain new quantum algorithms.

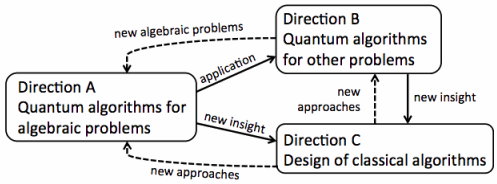
３．研究の方法

This research program has been implemented by focusing on the following three research directions.

Direction A: design of quantum algorithms for algebraic problems.
Direction B: design of quantum algorithms for other computational problems with an implicit algebraic structure.
Direction C: design of classical algorithms.

The execution of this research program started by taking a new look at the techniques developed in previous works, generalizing them and investigating extensions to other algebraic structures. This approach directly leaded to new results, and also enabled us to get a deeper insight into quantum algorithms for algebraic problems, learn the limitation of these techniques, and understand where new approaches were needed.

These findings were then used to progressively investigate new approaches and new targets, by working out in parallel each of Directions A, B and C, and studying their interplay, as described in the following figure.



４．研究成果

This research project has been successful and has leaded to several significant results in both quantum computing and classical computing.

The most important results obtained are related to the design of efficient classical algorithms for matrix multiplication. Matrix multiplication is naturally one of the most important problems in mathematics and computer science. Indeed, thousands algorithms in many areas of computer science are based on algorithms for matrix multiplication. During the four years of this research project, we have developed techniques to construct classical matrix multiplication algorithms via techniques from quantum computing. The main achievements of this line of research are as follows.

(1) Faster algorithms for rectangular matrix multiplication. We have obtained the first improvement of the asymptotic complexity of rectangular matrix multiplication in more than fifteen years. We also showed that this new algorithm has a deep impact in several areas of computer science. For instance, we constructed a faster algorithm for the All Pairs Shortest Paths problem in directed graphs with bounded weights, improving over Zwick's algorithm developed in 2002.

(2) Faster algorithms for square matrix multiplication. We succeeded in constructing a faster algorithm for square matrix multiplication as well. More precisely, we showed the new upper bound $\omega < 2.3728639$ on the exponent of matrix multiplication. The key technique to obtain this result was showing how to analyze powers of tensors efficiently via techniques inspired from quantum computing. This result received the Distinguished Paper Award at the 39th International Symposium on Symbolic and Algebraic

Computation (ISSAC 2014).

(3) Limitations of the laser method. We have also investigated the limits of the approaches described above. We showed in particular that any algorithm for square matrix multiplication designed by the same approach cannot have complexity linear in the input size. This strongly indicates that other approaches will be needed to make significant further progress on the computational complexity of matrix multiplication.

Another significant contribution of this research project is the design of quantum algorithms for computational problems, by exploiting the implicit algebraic structure of these problems. We have designed several quantum algorithms and protocols during the four years of the project. The two most fundamental achievements are as follows.

(4) Quantum interactive proofs. We have made a significant step towards a proof of one of the main open problems in the field of quantum interactive proofs: showing that any non-interactive quantum protocol can be made perfectly complete (i.e., its error can be reduced to zero on yes instances). More precisely, we have shown that non-interactive protocols can be made perfectly complete assuming that the players initially share a constant number of quantum particles.

(5) Faster quantum algorithms for triangle finding. Triangle finding, which asks whether a given graph contains a triangle, is one of the most studied computational problems in quantum computation. Recently, fast quantum algorithms for this problem have been designed using powerful quantum techniques (learning graphs, nested quantum walks), and matching lower bounds on the complexity of triangle finding have been shown for weighted graphs. Rather surprisingly, we succeeded in constructing a faster quantum algorithm for triangle finding in the case of unweighted graphs. This quantum algorithm is based on simple quantum walks combined with combinatorial arguments exploiting the structure of the input graph and its implicit algebraic structure, and shows for the first time that in the quantum query complexity setting unweighted versions of triangle finding are easier than its weighted versions.

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 17 件）

① S. Jeffery, R. Kothari, F. Le Gall, F. Magniez. Improving Quantum Query Complexity of Boolean Matrix Multiplication Using Graph Collision. Algorithmica, 印刷中. DOI: 10.1007/s00453-015-9985-x. 査読有

② F. Le Gall, H. Nishimura, S. Tani. Quantum Algorithms for Finding Constant-sized Sub-hypergraphs. Theoretical Computer Science, Vol. 603 No. P3, pp. 569-582, 2016. DOI: 10.1016/j.tcs.2015.10.006. 査読有

③ I. Kerenidis, M. Laurière, F. Le Gall, M. Rennela. Privacy in Quantum Communication Complexity. Quantum Information & Computation, Vol. 16 Nos. 3&4, pp. 181-196, 2016. http://www.rintonpress.com/journals/qiconline.html#v16n34. 査読有

④ H. Kobayashi, F. Le Gall, H. Nishimura. Stronger Methods of Making Quantum Interactive Proofs Perfectly Complete. SIAM Journal on Computing, Vol. 44 No. 2, pp. 243-289, 2015. DOI: 10.1137/140971944. 査読有

⑤ F. Le Gall, S. Nakajima. Quantum Algorithm for Triangle Finding in Sparse Graphs. Proceedings of the 26th International Symposium on Algorithms and Computation (ISAAC 2015), Lecture Notes in Computer Science Vol. 9472, pp. 590-600, 2015. DOI: 10.1007/978-3-662-48971-0_50. 査読有

⑥ A. Ambainis, Y. Filmus, F. Le Gall. Fast Matrix Multiplication: Limitations of the Coppersmith-Winograd Method. Proceedings of the 47th ACM Symposium on Theory of Computing (STOC 2015), pp. 585-593, 2015. DOI: 10.1145/2746539.2746554. 査読有

⑦ H. Kobayashi, F. Le Gall, H. Nishimura. Generalized Quantum Arthur-Merlin Games. Proceedings of the 30th Computational Complexity Conference (CCC 2015), pp. 488-511, 2015. DOI: 10.4230/LIPIcs.CCC.2015.488. 査読有

⑧ F. Le Gall, H. Nishimura. Quantum

Algorithms for Matrix Products over Semirings. Proceedings of the 14th Scandinavian Symposium and Workshops on Algorithm Theory (SWAT 2014), Lecture Notes in Computer Science Vol. 8503, pp. 331-343, 2014. DOI: 10.1007/978-3-319-08404-6_29. 査読有

⑨ F. Le Gall. Improved Quantum Algorithm for Triangle Finding using Combinatorial Arguments. Proceedings of the 55st Annual IEEE Symposium on Foundations of Computer Science (FOCS 2014), pp. 216-225, 2014. DOI: 10.1109/FOCS.2014.31. 査読有

⑩ F. Le Gall. Powers of Tensors and Fast Matrix Multiplication. Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation (ISSAC 2014), pp. 296-303, 2014. DOI: 10.1145/2608628.2608664. 査読有

⑪ F. Le Gall, Y. Yoshida. Property Testing for Cyclic Groups and Beyond. Journal of Combinatorial Optimization, Vol. 26 No. 4, pp. 636-654, 2013. DOI: 10.1007/s10878-011-9445-8. 査読有

⑫ F. Le Gall. Quantum Weakly Nondeterministic Communication Complexity. Theoretical Computer Science, Vol. 486, pp. 43-49, 2013. DOI: 10.1016/j.tcs.2012.12.015. 査読有

⑬ T. Satoh, F. Le Gall, H. Imai. Quantum Network Coding for Quantum Repeaters. Physical Review A, Vol. 86, 032331, 2012. DOI: 10.1103/PhysRevA.86.032331. 査読有

⑭ F. Le Gall. Faster Algorithms for Rectangular Matrix Multiplication. Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2012), pp. 514-523, 2012. DOI: 10.1109/FOCS.2012.80. 査読有

⑮ R. Cleve, K. Iwama, F. Le Gall, H. Nishimura, S. Tani, J. Teruyama, S. Yamashita. Reconstructing Strings from Substrings with Quantum Queries. Proceedings of the 13th Scandinavian Symposium and Workshops on Algorithm Theory (SWAT 2012), Lecture Notes in Computer Science Vol. 7357, pp. 388-397, 2012. DOI: 10.1007/978-3-642-31155-0_34. 査読有

⑯ F. Le Gall. Quantum Private Information Retrieval with Sublinear Communication Complexity. Theory of Computing, Vol. 8, pp. 369-374, 2012. DOI: 10.4086/toc.2012.v008a016. 査読有

⑰ F. Le Gall, S. Nakagawa, H. Nishimura. On QMA Protocols with Two Short Quantum Proofs. Quantum Information and Computation, Vol. 12 Nos. 7&8, pp. 589-600, 2012. http://www.rintonpress.com/journals/qiconline.html#v12n78. 査読有

〔学会発表〕（計 7 件）

① F. Le Gall. 疎グラフ上での三角形発見問題の量子アルゴリズム. 第 33 回量子情報技術研究会, 2015 年 11 月 25 日, NTT 厚木研究開発センタ（神奈川県・厚木市）

② F. Le Gall. Improved Quantum Algorithm for Triangle Finding using Combinatorial Arguments. The 18th Conference on Quantum Information Processing, 2015 年 1 月 22 日,シドニー工科大学,シドニー（オーストラリア）

③ F. Le Gall. Algebraic Complexity Theory and Matrix Multiplication. The 39th International Symposium on Symbolic and Algebraic Computation, 2014 年 7 月 23 日,神戸大学（兵庫県・神戸市）

④ F. Le Gall. Quantum Algorithms for Matrix Multiplication. 13th Asian Quantum Information Science Conference, 2013 年 8 月 26 日, チェンナイ（インド）

⑤ F. Le Gall. Quantum Complexity of Matrix Multiplication. Satellite Workshop of ICALP 2013 on Quantum and Classical Complexity, 2013 年 7 月 7 日, リガ（ラトビア）

⑥ F. Le Gall. Quantum algorithms for finding constant-sized sub-hypergraphs over 3-uniform hypergraphs. 第 29 回量子情報技術研究会研究会, 2013 年 11 月 18 日, 早稲田大学（東京都）

⑦ F. Le Gall. Quantum Algorithms for Matrix Products over Semirings. 第 28 回量子情報技術研究会研究会, 2013 年 5 月 28 日, 北海道大学（北海道・札幌市）

〔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・准教授
研究者番号： 50584299

(2)研究分担者

（　　）

研究者番号：

(3)連携研究者

（　　）

研究者番号：