様式 C-19

科学研究費補助金研究成果報告書

平成　23　年　5　月　13　日現在

機関番号：94305
研究種目：基盤研究 C
研究期間：平成 20 年度　～平成 22 年度
課題番号：20500024
研究課題名（和文）　行列分解を用いた量子回路設計とその応用

研究課題名（英文）　Quantum Circuit Design using Matrix Decomposition and its application

研究代表者　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
人間情報研究部　主任研究員　河野　泰人

研究者番号：40396180

研究成果の概要（和文）：以下のアルゴリズムの提案や応用を行なった．1）拡張クリフォード群の効率的な量子回路設計と離散対数問題への応用．2）行列分解アルゴリズムの効率化．3）行列分解を用いた d-順位系上の量子回路設計方法の提案．4）効率的な量子回路の等価性判定方法の提案．5）BDD の拡張概念 DDMF の提案と大規模量子回路設計への応用．6）量子プッシュダウンオートマトンの計算能力の解明．7）LNN 上の効率的な量子回路設計方法の提案．8）効率的な SAT アルゴリズムの提案．

研究成果の概要（英文）：We proposed the following algorithms and applications: 1) Efficient quantum algorithms for the extended Clifford group and its application to the discrete logarithm problem. 2) An efficient matrix decomposition algorithm. 3) A matrix decomposition algorithm that constructs efficient quantum circuit on qudits. 4) An efficient equivalence checking algorithm of quantum circuits. 5) DDMF, a quantum version of BDD, and its application to constructing large-scale quantum circuits. 6) A new result about computational complexity class of quantum pushdown automata. 7) An algorithm that converts normal quantum circuits to efficient quantum circuits on LNN. 8) An efficient algorithm that solves SAT problems using quantum walk.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
20 年度	1,200,000 円	360,000 円	1,560,000 円
21 年度	1,000,000 円	300,000 円	1,300,000 円
22 年度	1,000,000 円	300,000 円	1,300,000 円
年度			
年度			
総　計	3,200,000 円	960,000 円	4,160,000 円

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：量子計算理論

１．研究開始当初の背景

1994 年，Shor（現 MIT 教授）は因数分解や離散対数問題を高速で解く量子アルゴリズムを発表し，量子状態を効率的に制御できれば，ある種の問題は現在のコンピュータ（古典コンピュータ）よりもはるかに高速に計算が可能なことを示した．この研究を契機に量子コンピュータの計算能力と，その応用

に関する研究の必要性が明らかになってきた．その主な研究テーマとして，以下の３つを挙げることができる．

まず，第一に，新しい効率的な量子アルゴリズムの発見とその応用である．これまで，古典アルゴリズムより高速な量子アルゴリズムが数多く提案されてきた．（例として，http://math.nist.gov/quantum/zoo/を参照のこと．）しかし，古典アルゴリズムよりも指数的に速い量子アルゴリズムは数えるほどしかない．また，Shor のアルゴリズムや Grover の検索アルゴリズムを除くと，応用の明確な量子アルゴリズムも少ない．そのため，新しい効率的な量子アルゴリズムとその応用に関する研究は，もっとも重要な課題と位置づけられている．

第二に，量子アルゴリズムのハードウェア上での効率的な実装に関する問題である．量子コンピュータのハードウェアモデルとして量子回路が用いられるが，実際に開発される量子コンピュータでは隣接キュービット間での演算しかできない可能性が高い．そのため，より現実的な量子計算モデルとして，LNN（Linear Nearest Neighbor）モデルなどが提唱されている．こうした現実的なモデルと量子回路との間では多項式時間のオーバーヘッドで回路変換が可能だが，オプティマルな回路変換の方法は未解決である．

第三に，より根本的な問題として，量子コンピュータと古典コンピュータの原理的な計算能力の違いも解明が望まれている重要なテーマである．この領域は量子計算量理論として知られ，古典計算量理論と並んで高度に理論的な分野である．

２．研究の目的

上記のような背景のもと，本研究は，効率的な量子アルゴリズムの発見とその応用，実現性の高い量子計算モデル上での効率的な量子回路の構成方法，量子コンピュータの原理的な計算能力などの重要課題に対して，古典コンピュータにおける回路設計の手法を応用することにより，新たな知見を得ることを目的としている．古典コンピュータにおける回路設計は非常に長い歴史があり，多くの研究成果が得られている．また，コンピュータによる自動設計が取り入れられており，人間による直感の効きにくい量子アルゴリズムの設計において，強力な武器になることが期待される．

３．研究の方法

具体的には，以下の論文で示す筆者らが提案した行列分解を利用した効率的な量子回路設計手法を応用した．

中島裕美，河野泰人，関川浩：量子回路の自動設計手法，情報処理, Vol. 47, No. 12, pp. 1335-1340, 2006

また，古典回路の効率化で用いられる BDD やグラフ理論を利用し，量子回路の効率化とその応用方法に関する研究を進めた．さらに，量子プッシュダウンオートマトンに着目し，量子アルゴリズムと古典アルゴリズムとの性能の違いを研究した．

４．研究成果

この研究により，以下の成果が得られた．

１）量子フーリエ変換を含む重要な群として知られる拡張クリフォード群に対する効率的な量子回路を構成し，その応用により，離散対数問題を従来の 2/3 のキュービット数で実行する量子アルゴリズムを提案した．

２）以下の論文で発表した行列分解アルゴリズムを改良し，複素アダマール行列の分類への応用方法を示した．
Y. Nakajima, Y. Kawano, and H. Sekigawa: A new algorithm for producing quantum circuits using KAK decompositions, Quantum Information and Computation 6(1), pp. 67-80 (2006).

３）d-準位系を対象にサイン-コサイン分解を用いて行列を分解することでサイズの小さい量子回路を生成する手法を提案した．d=2 の場合は漸近的に最適であることを示すことができ，また，d≠2 の場合でも，量子ビット数が少ない場合は既存の手法に比べサイズの小さい回路を生成できることを示した．

４）量子回路を設計する際に，回路の最適化の変形を行った際に，その変形が正しいかを検証する必要があり，それを等価性判定と呼ぶ．これに対し，従来の回路設計で使われている miter というものに対して，それを可逆回路に拡張した reversible miter というアイデアを用いて，実際に等価性判定アルゴリズムを実装した．ランダムな回路を生成してその等価性判定の性能を評価したところ，従来の手法よりもより効率がいいことが分かった．

５）現在までに提案されている量子回路設計手法は，ほとんどが大規模な量子回路を扱うことができない．そこで，大規模な量子回路でも組織的に設計できる手法として，Decision Diagrams for a Matrix Function (DDMF)と呼ばれる 2 分決定木をトラバースすることにより，多くの有用な量子回路が効率的に設計できる手法の開発を行った．

６）量子計算モデルに関する研究として量子プッシュダウンオートマトンを取り上げ，空スタック受理の場合は量子モデルのほうが古典モデルよりも能力が弱くなりうることを示した．

７）量子回路を LNN 上の回路に変換する新しい手法を考案した．具体的には，今年度は隣接互換グラフと呼ばれるデータ構造を利用することにより，ゲート順序も考慮して LNN アーキテクチャへの最適な変換を行うことが出来る問題の定式化に成功した．この手法により，エラー訂正符号として有名は Steane 符号のエンコーディング回路を LNN アーキテクチャへ最適に変換することが出来た．また，AQFT の回路に関して，今まで知られている最良の手法の結果を改善することもできた．

８）量子ウォークに関する研究を行い，①直線上の量子ウォークの振る舞いを解析的な手法で近似 ②量子ウォークと古典ウォークのハイブリッドな計算手法を用いる SAT アルゴリズムの開発を行った．

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４件）

①S. Yamashita, S. Minato, and D. M. Miller: Synthesis of Semi-Classical Quantum Circuits, Journal of Multiple-Valued Logic and Soft Computing, Vol. 17, pp.99-114 (2011).

②Y. Hirata, M. Nakanishi, S. Yamashita, and Y. Nakashima: An Efficient Conversion of Quantum Circuits to a Linear Nearest Neighbor Architecture, Quantum Information and Computation, vol.11, no.1&2, pp.142-166 (2011).

③Y. Nakajima, Y. Kawano, H. Sekigawa, M. Nakanishi, S. Yamashita and Y. Nakashima: Synthesis of quantum circuits for d-level systems by using Cosine-Sine decomposition, Quantum Information and Computation, Vol. 9, No.5&6, pp. 423 - 443 (2009).

④S. Yamashita, S. Minato, and D. M. Miller: DDMF: An Efficient Decision Diagram Structure for Design Verification of Quantum Circuits under a Practical Restriction, IEICE Trans. Fundamentals, Vol. E91-A, pp. 3793 – 3802 (2008).

〔学会発表〕（計１７件）

①Y. Kawano: Hidden Shift Problem for Quadratic Functions on a Product of Cyclic Groups, The 14th Workshop on Quantum Information Processing 2011 (2011 年 1 月 11 日）シンガポール

② M. Nakanishi: On the weakness of one-way quantum pushdown automata under empty-stack acceptance, The 14th Workshop on Quantum Information Processing 2011 (2011 年 1 月 10 日）シンガポール

③Y. Kawano and H. Sekigawa: Matrix Decomposition and its Application to Complex Hadamard matrices, The 14th Workshop on Quantum Information Processing 2011 (2011 年 1 月 10 日）シンガポール

④松尾惇士, 山下茂: ゲート順序を考慮した LNN アーキテクチャへの変換手法, 第 23 回量子情報技術研究会,（2010 年 11 月 15 日）東京大学

⑤ D. Yokomine, M. Nakanishi, S. Yamashita, and Y. Nakashima, A SAT Solver Based on Quantum and Classical Random Walk, The 10th Asian Conference on Quantum Information Science 2010 (AQIS2010), (2010 年 8 月 29 日）東京大学

⑥M. Villagra, M. Nakanishi, S. Yamashita, and Y. Nakashima: Asymptotics of Quantum Walks on the Line with Phase Parameters, The 10th Asian Conference on Quantum Information Science 2010 (AQIS2010), (2010 年 8 月 29 日）東京大学

⑦S. Yamashita, S. Minato, and D. M. Miller: Synthesis of Semi-Classical Quantum Circuits, The 2nd Workshop on Reversible Computation, (2010 年 7 月 3 日）ドイツ

⑧S. Yamashita and I. Markov: Fast Equivalence-checking for Quantum Circuits, NANOARCH'10, (2010 年 6 月 16 日）アメリカ.

⑨M. Nakanishi: On the Weakness of One-Way Quantum Pushdown Automata, Fourth International Conference on Quantum, Nano and Micor Technologies (ICQNM2010), (2010年2月11日）St.Maarten.,

Netherlands Antilles, オランダ

⑩Y. Kawano and H. Sekigawa: Application of Matrix Decomposition to Finding Complex Hadamard Matrices, The 13th Workshop on Quantum Information Processing 2010, (2010年1月20日) チューリッヒ工科大, スイス

⑪河野泰人, 関川浩：行列分解と複素アダマール行列への応用，電子通信学会量子情報技術研究会, (2009年11月4日) 電気通信大学.

⑫ S. Yamashita: Adaptive Equivalence-checking for Quantum Circuits, Reed-Muller Workshop 2009, (2009年5月24日) 那覇

⑬Y. Hirata, M. Nakanishi, S. Yamashita, and Y. Nakashima: An Efficient Method to Convert Arbitrary Quantum Circuits to Ones on a Linear Nearest Neighbor Architecture, The Third International Conference on Quantum, Nano and Micro Technologies, (2009年2月2日) Fiesta Americana Condesa Cancun, メキシコ.

⑭Y. Kawano and H. Sekigawa: Producing quantum circuits of the extended Clifford group, The 12th Workshop on Quantum Information Processing 2009, (2009年1月14日) Santa Fe, アメリカ.

⑮Y. Kawano: Efficient Algorithm of the Extended Clifford Group, The 8th Asian conference on Quantum Information and Science 2008, (2008年8月28日) KIAS, 韓国.

⑯S. Yamashita, S. Minato, and D. M. Miller: An Efficient Verification of Quantum Circuits under a Practical Restriction, IEEE 8th International Conference on Computer and Information Technology (CIT2008), (2008年7月8日) University of Technology, オーストラリア.

⑰S. Yamashita, S. Minato and D. M. Miller: An Efficient Verification of Quantum Circuits under a Practical Restriction, IEEE International Workshop on Logic Synthesis, (2008年6月4日) Granlibakken Lodge, アメリカ.

〔図書〕(計０件)

〔産業財産権〕

○出願状況（計３件）
①名称：量子演算方法，量子演算装置
発明者：河野泰人，高橋康博，加藤豪
権利者：NTT
種類：特許
番号：特願 2011-001394
取得年月日：2011年1月6日
国内外の別：国内

②名称：量子演算方法，量子演算装置
発明者：河野泰人，高橋康博，加藤豪
権利者：NTT
種類：特許
番号：特願 2010-205566
取得年月日：2010年9月14日
国内外の別：国内

③名称：行列分解装置，行列分解方法及びプログラム
発明者：河野泰人，関川浩
権利者：NTT
種類：特許
番号：特願 2009-24348
出願年月日：2009年10月22日
国内外の別：国内

○取得状況（計０件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

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・協創情報研究部・主任研究員）
研究者番号：４０３９６１８０

(2)研究分担者
関川浩（東海大学・理学部・准教授）
研究者番号：００３９６１７８

山下茂（立命館大学・情報理工学部・教授）
研究者番号：３０３６２８３３

中西正樹（山形大学・地域教育文化学部・准教授）
研究者番号：４０３２４９６７

(3)連携研究者
（　　）

研究者番号：