

機関番号：34315

研究種目：若手研究（B）

研究期間：2007～2010

課題番号：19700010

研究課題名（和文）エラー訂正を考慮した効率の良い量子回路設計手法に関する研究

研究課題名（英文）Efficient Quantum Circuit Design Methods Considering Error Correction

研究代表者

山下 茂（YAMASHITA SHIGERU）

立命館大学・情報理工学部・教授

研究者番号：30362833

研究成果の概要（和文）：

エラーに耐性のある量子回路設計を効率的に設計するために、以下のような手法の考案および評価を行った。(1) 耐故障性量子計算におけるエラー訂正回数の削減手法、(2) 多準位系を用いた量子回路設計、(3) 効率的な LNN 回路設計手法、(4) 量子回路の効率的な等価性判定手法、(5) 大規模な量子回路の効率的な設計手法、(6) 量子ウォークの解析手法。

研究成果の概要（英文）：

The following methods have been proposed and evaluated for error robust quantum circuit design. (1) A method to reduce the number of error corrections for fault-tolerant quantum computation, (2) A circuit design method to use a multilevel quantum system, (3) Efficient LNN circuit design methods, (4) An efficient verification method for quantum circuits, (5) An efficient design method for large quantum circuits, and (6) An analysis of quantum walks.

交付決定額

（金額単位：円）

	直接経費	間接経費	合計
2007 年度	500,000	0	500,000
2008 年度	600,000	180,000	780,000
2009 年度	900,000	270,000	1,170,000
2010 年度	600,000	180,000	780,000
年度			
総計	2,600,000	630,000	3,230,000

研究分野：情報学基礎

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

1. 研究開始当初の背景

現在の計算機の方式では、LSI の微細化が原子のレベルまで進めばその性能が原理的な限界に突き当たると考えられている。また、現在の計算方式では、大きな数の因数分解のように現実的な時間では計算不可能であると考えられている問題も多い。それに対し、原子レベルの量子状態をうまく制御して計算を行う計算機（量子計算機）は、前述の因数分解なども現実的な時間で計算可能であ

り、21 世紀のナノテクノロジーの研究成果の恩恵により実現される次世代の計算機として注目されている。日本では量子計算の実現に関する物理の方面からの研究に関しては、国および民間からの潤沢な研究資金により活発に研究が行われている。しかし、量子計算に関しての計算機科学の視点からの研究は、諸外国に比べて日本では圧倒的に少ない。量子計算の潜在的な能力は示唆されているが、それを具体的にどのような状況で、どの

ように利用すれば有効に利用できるかという方法論に関してはほとんど知られていないため、たとえ量子計算機が物理的に実現したとしても、すぐにそれを有用に使いこなすことはできない。そのため、計算機システムとして利用する方法論の計算機科学的な視点からの研究も重要であることは明らかである。実際、欧米では量子計算に関する計算機科学的な側面の基礎研究も活発に行われている。今日の計算機システムにおいてその基本ソフトウェア(OS)などの核となる技術がほぼ外国に押さえられていることを鑑みると、将来の量子計算機システムの利用方法の中核技術でも同じことが起こらないように、日本でも今のうちから量子計算機の利用方法を計算機科学の視点から検討する基礎研究を地道に行っていくべきだと考えられる。

2. 研究の目的

量子計算が実現した時にそれを使いこなすために重要な技術として、量子回路設計の研究は大変重要である。量子回路設計とは、所望の計算を行う量子アルゴリズムを、量子的な操作の基本列(量子ゲートと呼ばれる)に変換する作業である。量子計算では、我々が計算したい問題は、通常(複数の)ブール関数で記述できる。そのため、全体の量子アルゴリズムの中で、あるブール関数を計算する部分(量子オラクルと呼ばれることが多い)は問題ごとに設計が本質的に必要で、その他の部分は問題ごとに変わらない量子的な特殊な構造をもっているので回路設計の対象とする必要はない。このことは、今までに知られている Grover のアルゴリズムや Shor のアルゴリズムでも成り立つため、量子回路設計において実用的な観点で最も重要な部分は、量子オラクルの設計であると考えられる。そのため、量子オラクルの設計に関しては、多くの研究が行われてきている。本研究では、量子オラクル回路の設計に関して、既存の回路設計の研究を発展させて、物理的なエラーなどを考慮してより現実的な状況に即した回路設計手法の確立を目指す。

3. 研究の方法

量子アルゴリズムをエラーの影響が少なくなるように実現するには、アルゴリズムを実現する量子回路をエラーの影響が少ないと考えられる回路モデルで実現することが重要であると考えられる。そのためにまずエラー訂正符号を実現する量子回路設計に関して効率の良い手法が存在するかを検討した。続いて、現在最も操作エラーが少ないと考えられている量子計算の実現モデルである Linear Nearest Neighbor (LNN) アーキテクチャ上で動作する量子回路に一般の量子回路を変換する手法に関して、いくつか検討

を行った。また、そのような回路変換手法を実際に用いるためには、回路変換の等価性を保障するために、回路の検証手法が必要となる。そこで、量子回路の検証手法についても検討を行った。また、状況によっては物理的な実現が容易であると考えられている多準位系を用いて回路設計する手法に関しても検討を行った。

4. 研究成果

前項の研究の結果以下のような研究成果をあげた。

(1) 耐故障性量子計算におけるエラー訂正回数削減手法

Shor により各量子ゲートが完全に動作しない状況でもフォールトトレラントに計算を実行する耐故障性量子計算の手法が提案されている。その手法は、演算に用いる量子ビットを量子誤り訂正符号(具体的には Steane 符号)で符号化して、各基本演算の前後で、量子誤り訂正により逐一エラーを訂正する手法である。しかし、量子誤り訂正は計算ステップ数が大きいのに加え、誤り訂正自体で誤りを生じる可能性がある。そのため、全体の計算結果の信頼性を保ったまま、量子誤り訂正回路を挿入する場所を極力少なくする種々の手法を開発した。

(2) 多準位系を用いた量子回路設計

量子回路設計にエラーを考えた場合多準位系を用いたほうが現実的となる場合もあると考えられる。そこで多準位系の量子ゲートによる量子回路設計のために、与えられた任意の n 次元のユニタリ行列を効率よく基本量子ゲートの積に変換する手法を考案した。具体的には、従来からある Cosine-Sine 分解における分割のサイズを適切に調整することにより、ある程度の規模の入力数ならば従来手法よりも少ない基本ゲート数で与えられたユニタリ行列を分解することができることを示した。d-準位系の場合、 $d=2$ の場合は提案手法が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。

(3) 効率的な LNN 回路設計手法

現在最も実現の可能性が高いと考えられている量子計算の実現モデルである Linear Nearest Neighbor (LNN) アーキテクチャは比較的エラーが少ないと考えられる。LNN アーキテクチャ上で実現可能な量子回路を設計する手法として以下の2つの新しい手法を考案した。

任意の量子回路を LNN アーキテクチャ

上で実現できるように SWAP ゲートを挿入して回路を変換する手法を考案した。提案手法は、ナイーブな手法に比べて少ない計算時間で SWAP ゲートの数を削減することができ、また、今までに報告されている人手で設計された回路をより少ない SWAP ゲート数での LNN 上の量子回路へ変換できることを確認した。

量子回路を LNN 上の回路に変換する際に、加える SWAP ゲートが比較的少ない場合には、厳密な意味で最小個数の SWAP ゲートの追加ですむ新しい手法を考案した。その手法のアイデアは、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ように問題の定式化を行ったことである。この手法により、エラー訂正符号として有名な 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。

(4) 量子回路の効率的な等価性判定手法

LNN アーキテクチャへ量子回路を変化する際に、回路の最適化や、SWAP ゲートの挿入などの回路変形を行う。そのような変形を行った際に、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考案した。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よいことが分かった。さらに、単純に回路全体をユニタリ行列に変換してから等価性を判定するよりも多くの場合で効率的に量子回路の等価性判定が高速にできる手法も考案し、ベンチマーク回路で実際に手法が有効であることを確認した。

(5) 大規模な量子回路の効率的な設計手法

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を考案しその有効性を示した。

(6) 量子ウォークに関する研究

量子ウォークの性能解析行い、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を行い、また、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9件)

1. S. Yamashita and M. Nakanishi: An Efficient Framework to Utilize Grover Search, Journal of Nanjing University of Posts and Telecommunications, Vol. 31, No. 2, pp. 85-94 (2011), 査読有.
2. Y. 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), 査読有.
3. S. 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), 査読有.
4. S. Yamashita and I. L. Markov: Fast equivalence-checking for quantum circuits, Quantum Information and Computation, Vol. 10, No. 9&10, pp. 721-734 (2011), 査読有.
5. 山下茂: 量子探索アルゴリズムとその利用, 電子情報通信学会会誌, Vol. 93, No. 9, pp. 785-791 (2010), 査読無.
6. 柴田章博, 中田尚, 中西正樹, 山下茂, 中島康彦: 量子計算の並列シミュレーションにおける通信量削減手法, 電子情報通信学会論文誌 D Vol. J93-D, No. 3, pp. 253-264 (2010), 査読有.
7. Y. 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), 査読有.
8. S. Tani, M. Nakanishi and S. Yamashita: Multi-Party Quantum Communication Complexity with Routed Messages, IEICE transactions on Information and Systems, Vol. E92-D, No.2, pp. 191-199 (2009), 査読有.
9. S. 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), 査読有.

〔学会発表〕(計32件)

1. 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(東京都)
2. M. 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(東京都)
3. 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(東京都)
4. S. Yamashita, S. Minato, D. M. Miller: Synthesis of Semi-Classical Quantum Circuits, 2nd Workshop on Reversible Computation, 2010年7月3日, プレーメン(ドイツ)
5. S. Yamashita and I. Markov: Fast Equivalence-checking for Quantum Circuits, NANOARCH'10, 2010年6月16日, アナハイム(アメリカ)
6. Marcos Villagra, Masaki Nakanishi, Shigeru Yamashita and Yasuhiko Nakashima: Discrete Quantum Walks on the Line with Phase Parameters, The International Conference on Quantum Information and Technology, 2009年12月3日, NII(東京都)
7. 谷誠一郎, 中西正樹, 山下茂: Quantum Communication Protocols with Public Coins, 情報処理学会アルゴリズム研究会, 2009年9月15日, 鳥取環境大学(鳥取県)
8. Antti Vihman, Takashi Nakada, Masaki Nakanishi, Shigeru Yamashita and Yasuhiko Nakashima: An efficient middle-level framework for quantum circuit simulation on multiple simulator platforms, SWoPP2009, 2009年8月4日, フォレスト仙台(宮城県)
9. S. Yamashita: Adaptive Equivalence-checking for Quantum Circuits, Reed-Muller Workshop 2009, 2009年5月24日, Naha Culture Center(沖縄県)
10. Y. 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 (ICQNM 2009), 2009年2月2日, Fiesta Americana Condesa Cancun(メキシコ)
11. A. Ambainis, K. Iwama, M. Nakanishi, H. Nishimura, R. Raymond, S. Tani, and S. Yamashita: Average/Worst-Case Gap of Quantum Query Complexities, The Twelfth Workshop on Quantum Information Processing (QIP2009), 2009年1月14日, SANTA FE, NEW MEXICO(アメリカ)
12. A. Ambainis, K. Iwama, M. Nakanishi, H. Nishimura, R. Raymond, S. Tani and S. Yamashita: Quantum Query Complexity of Boolean Functions with Small On-Sets, the 19th International Symposium on Algorithms and Computation (ISAAC 2008), 2008年12月17日, Gold Coast International Hotel(オーストラリア)
13. Y. Hirata, M. Nakanishi, S. Yamashita, and Y. Nakashima: An Efficient Method to Convert Arbitrary Quantum Circuits to Ones on a Linear Nearest Neighbor Architecture, 第19回量子情報技術研究会, 2008年11月20日, 東京大学(東京都)
14. A. Ambainis, K. Iwama, M. Nakanishi, H. Nishimura, R. Raymond, S. Tani and S. Yamashita: Quantum Query Complexity of Boolean Functions with Small On-Sets, 第19回量子情報技術研究会, 2008年11月20日, 東京大学(東京都)
15. 柴田章博, 中田尚, 中西正樹, 山下茂, 中島康彦: 量子計算の並列シミュレーションにおける通信量削減手法, SWoPP2008, 2008年8月6日, アバンセ(佐賀県)
16. S. 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 (CIT 2008), 2008年7月8日, University of Technology, Sydney(オーストラリア)
17. K. Iwama, H. Nishimura, M. Paterson, R. Raymond and S. Yamashita: Polynomial-Time Construction of Linear Network Coding, ICALP 2008,

- 2008年7月7日, Reykjavik University (アイスランド)
- S. Tani, M. Nakanishi and S. Yamashita: Multi-Party Quantum Communication Complexity with Routed Messages, 14th Annual International Computing and Combinatorics Conference (COCOON 2008), LNCS 5092 (2008), 2008年6月27日, Mercure Teda Dalian Hotel (中国)
- 21 S. Yamashita and I. Markov: Equivalence-checking for Reversible Circuits, IEEE International Workshop on Logic Synthesis (IWLS 2008), 2008年6月4日, Granlibakken Lodge (アメリカ)
- 22 柴田章博, 中田尚, 中西正樹, 山下茂, 中島康彦: 並列量子計算シミュレータにおける通信量削減手法の提案, 第18回量子情報技術研究会, 2008年5月22日, 東京大学(東京都)
- 23 Masaki Nakanishi, Seiichiro Tani and Shigeru Yamashita: An almost optimal quantum string sealing protocol and its security analysis, the First AAAC (Asian Association of Algorithms and Computation) Annual Meeting, 2008年4月26日, University of Hong Kong (中国)
- 24 Y. Murakami, M. Nakanishi, M. Hagiwara, S. Yamashita and Y. Nakashima: A quantum secure direct communication protocol for sending a quantum state and its security analysis, The 2008 Symposium on Cryptography and Information Security (SCIS2008), 2008年1月23日, フェニックス・シーガイア・リゾート(宮崎県)
- 25 K. Iwama, H. Nishimura, R. Raymond and S. Yamashita: Unbounded-Error Classical and Quantum Communication Complexity, the Eleventh Workshop on Quantum Information Processing, 2007年12月21日, India International Centre (インド)
- 26 K. Iwama, H. Nishimura, M. Paterson, R. Raymond and S. Yamashita: Fidelity-Efficient Quantum Network Coding, the Eleventh Workshop on Quantum Information Processing, 2007年12月18日, India International Centre (インド)
- 27 Y. Nakajima, Y. Kawano, H. Sekigawa, M. Nakanishi, S. Yamashita and Y. Nakashima: Synthesis of quantum circuits for d-level systems using KAK decomposition, the Eleventh Workshop on Quantum Information Processing, 2007年12月18日, India International Centre (インド)
- 28 K. Iwama, H. Nishimura, R. Raymond and S. Yamashita: Unbounded-error classical and quantum communication complexity, 18th International Symposium on Algorithms and Computation (ISAAC2007), 2007年12月17日, Sendai Excel Hotel Tokyu (宮城県)
- 29 S. Tani, M. Nakanishi and S. Yamashita: An analysis of quantum communication complexity depending on network topologies, 第17回量子情報技術研究会, QIT2007-83, pp. 150-153, 2007年11月22日, 岡山光量子科学研究所(岡山県)
- 30 S. Yamashita and M. Nakanishi: A Practical Framework to Utilize Quantum Search, the 2007 IEEE Congress on Evolutionary Computation (CEC2007), (CD-ROM), 2007年9月28日, Swissôtel The Stamford (シンガポール)
- 31 Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, Shigeru Yamashita: Unbounded-Error One-Way Classical and Quantum Communication Complexity, ICALP 2007, 2007年7月9日, University of Wrocław (ポーランド)
- 32 岩間一雄, 西村治道, ルディーレイモンド, 山下茂: 非有界誤り一方向量子および古典通信計算量, 第16回量子情報技術研究会, QIT2007-26, pp. 106-111, 2007年5月18日, NTT厚木研究開発センター(神奈川県)
- [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]
ホームページ等
<http://www.ngc.is.ritsumeai.ac.jp/~ger/>
6. 研究組織
(1) 研究代表者
山下 茂 (YAMASHITA SHIGERU)
立命館大学・情報理工学部・教授
研究者番号: 30362833