

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25年 6月10日現在

機関番号：11501

研究種目：若手研究（B）

研究期間：2009 ～ 2011

課題番号：21700016

研究課題名（和文） 実装容易性を考慮した量子情報処理

研究課題名（英文） Implementation-Oriented Quantum Information Processing

研究代表者

中西 正樹（NAKANISHI MASAKI）

山形大学・地域教育文化学部・准教授

研究者番号：40324967

研究成果の概要（和文）：

量子計算機は次世代の計算機として注目を集めているが、その実装に際しては様々な制約が課せられる。したがって、そのような制約の元でも量子計算機が従来の計算機に比べて優れていることを示すことが重要である。本研究では、さまざまな制約に対応する量子計算機のモデルを提案し、そのモデルの元で量子計算機の優位性を示した。さらには特定の状況下では量子計算機が従来の計算機よりも能力が劣ることも示し、量子計算機が苦手とする状況を解明した。

研究成果の概要（英文）：

Quantum computers have attracted much attention recently. It is known that many restrictions are imposed on implementing quantum computers. Thus, it is important to investigate restricted models of quantum computation. In this research, we proposed several implementation-oriented quantum computation models, and investigated the ability of such models. We showed that even in such restricted models, quantum computers can be more powerful than classical computers. We also showed that in a particular case, quantum computers can be less powerful than classical computers because of the restriction of reversibility.

(金額単位：円)

	直接経費	間接経費	合計
2009年度	800,000	240,000	1,040,000
2010年度	800,000	240,000	1,040,000
2011年度	800,000	240,000	1,040,000
年度			
年度			
総計	2,400,000	720,000	3,120,000

研究分野：情報科学

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，量子計算モデル，量子オートマトン，量子計算量理論

1. 研究開始当初の背景

次世代の計算パラダイムとして、量子力学の枠組みで情報処理を考える「量子情報処理」が近年注目を集めている。量子情報処理は一般に「量子計算」と「量子（暗号）通信」に大別されるが、そのどちらの分野においても、従来の情報処理（古典情報処理と呼ぶ）と比較して、大きな優位性を持つことがわかって

いる。例えば、量子計算の分野においては1994年にショアによって多項式時間で素因数分解を行うアルゴリズムが開発され（素因数分解は古典計算機を用いると指数時間かかると予想されている）、大きな注目を集めた。また、量子暗号の分野においては、無条件安全な暗号プロトコルが開発されるなど目覚ましい発展を遂げている。

このような量子情報処理における理論的な研究成果の発展の一方で、それらのアルゴリズムや通信プロトコルを実際に実装する際の問題点がいろいろと指摘されている。つまり、将来実現されるであろう量子計算機は、使用できる演算やメモリのアクセス方法に何らかの制約がついたものであるという予想がなされている。その一方で素因数分解をはじめとする様々な量子アルゴリズムは、理想的な量子計算機のモデルの上で成り立つものである。このため、現在までに開発された量子アルゴリズムを実際の(理想的ではない)量子計算機上で実行した場合に、大きなオーバーヘッドがかかってしまう、あるいは、そもそも実行ができないといった可能性が考えられる。

2. 研究の目的

上記の背景を踏まえ、本研究では、実装上の問題点を考慮した「現実的な」量子計算機のモデルを構築し、その上での量子アルゴリズムの評価を行うことを目的とした。また、同様に、量子通信プロトコルにおいても、「現実的な」量子通信デバイスのモデルを考えた上で、その能力の解析等を行う。目標としては、そのような「現実的なモデル」であっても、従来の古典情報処理と比べて優位性があることを示すことを目指した。

具体的に取り組んだ課題は以下の通りである。

- (1) 「理想的な量子計算機アーキテクチャ上で動作するアルゴリズムを LNN アーキテクチャ向けに効率よく変換する手法の開発」

実装の容易性を考慮した「現実的な量子計算機のモデル」を考え、理想的な量子計算機上で動くアルゴリズムを、現実的な量子計算機のモデル上で動くように自動変換する手法を開発を目的とした。具体的には Linear Nearest Neighbour (LNN) アーキテクチャと呼ばれるメモリへのアクセス方法を制限した量子計算機のモデルを対象にした。この LNN アーキテクチャとは、隣同士に並んだ量子ビットにのみ演算が行えるという量子計算機のモデルであり、現実的な量子計算機の実装のひとつとして注目されている。

- (2) 「現実的な量子計算機のモデルを提案し、その能力を理論的に解析する。量子計算機の実装の際に、技術上妥協しても良い点(つまり、制約を付けても良い点)と必要不可欠な技術(実現できなければ量子計算機の能力を落としてしまう点)を明らかにする。」

LNN アーキテクチャ以外の現実的な量子計算機のモデルを考え、その計算能力を理論的に解析した。LNN アーキテクチャへは高々多項式回の量子演算のオーバーヘッドで理想的な量子計算機アーキテクチャから変換可能である(つまり計算能力は多項式倍の範囲で等価)が、それ以外の現実的なモデルでは、場合によっては、計算能力が弱くなってしまう可能性がある。つまり、特定の関数を計算する際の計算量に超多項式的なギャップが生じる、あるいはそもそも計算不可能となる可能性がある。したがって、本研究では計算能力を落とすことなくどこまで実装の容易なモデルを構築できるかを調査することを目的とした。このことは、言い換えれば、本研究により得られた知見を元に、実際の量子計算機の実装において技術的にどの部分が不可欠で、どの部分は妥協できるかを示唆することにもなる。

- (3) 「量子ウォークの振る舞いの解析」

次に、現実的な量子計算機のモデル上で効率よく動作する新しいアルゴリズムの開発に向けた研究が必要と考えられる。つまり、現実的なモデルの特徴をうまく利用し、(理想的なモデルと比較して)できるだけ少ないオーバーヘッドで問題を解くアルゴリズムである。そこで、量子アルゴリズムの枠組みの一つである量子ウォークに着目し、実装容易性を考慮して線上の量子ウォークを取り上げ、その振る舞いの解析を行うことを考えた。量子ウォークの振る舞いについてはシミュレーションによる解析は様々に行われているが、本研究では振る舞いを閉形式で表現することを目的とした。これにより量子ウォークを用いたアルゴリズムの開発、解析が容易になることが期待される。

- (4) 「多者間量子通信プロトコルの通信計算量の解析」

計算モデルとして分散計算のモデルを考え、その通信量に焦点を当てた解析を行う。これは、各計算機の処理時間ではなく、計算機間の通信がボトルネックとなるような状況での評価と考えることができる。

量子通信計算量に関しては過去にも様々な研究がなされているが、本研究では「多者間」かつ「強量子非決定性計算」のモデルを取り上げた。さらに、入力を与え方として(一般的に用いられている)各プレイヤーが自分の入力のみを知るこ

とができる Number-in-Hand モデルの他に、各プレイヤーが自分の入力以外をすべて知ることができる Number-on-Forehead モデルを対象とした。これらのモデルに対し、通信計算量の上界、下界を求めることを目的とした。

その他、量子計算機シミュレータの開発等、様々な観点から現実的な量子計算モデルにおける能力の解析を行うことを目的とした。

3. 研究の方法

以下、「研究の目的」の各項目に対応する形で研究の方法を説明する。

- (1) 「現実的な」量子計算機のモデルとして Linear Nearest Neighbour (LNN) アーキテクチャを取り上げた。理想的な量子計算機向けのアルゴリズムが与えられた場合、量子ビットのスワップを適宜行うことにより、LNN アーキテクチャに変換できるが、このスワップの回数をできるだけ少なくすることが望ましい。このスワップ演算の挿入を自動的に行う手法の開発を行った。

具体的には、「最適なスワップ演算の挿入」を求める問題は NP 完全問題であると予想されるため、発見的手法を用いたアプローチを用いた。

- (2) 量子計算機のモデルとして量子プッシュダウンオートマトンを取り上げた。量子プッシュダウンオートマトンが持つスタックに対する操作は、量子計算機の可逆性の制約が大きく影響するため、そのような状況での量子計算モデルの限界を調べた。

古典計算モデルにおけるプッシュダウンオートマトンでは空スタック受理と最終状態受理は等価であるということが知られている。しかしながら、量子計算モデルにおいては、スタック上の記号の削除が必ずしも可逆演算とならないため両受理モデルにおいて能力の差が生じることが考えられる。この点を考慮しつつ、量子プッシュダウンオートマトンの能力の解析を行った。

- (3) 線上の量子ウォークに対し、その振る舞いを閉形式で表現するための解析を行った。

具体的には、時間 t における各量子状態の確率振幅および各頂点に到達する確率を閉形式で求めることになる。使用する量子コインは symmetric $SU(2)$ とし、コインパラメータの関数として確率振幅を表現するのが目標である。この解析に際

しては、フーリエ解析や最急降下法等の手法を用いている。

- (4) 多者間量子通信計算量について、強非決定性量子通信モデルを対象とし、その能力の解析を行った。

具体的には、各プレイヤーの入力に対する出力を表す通信テンソルを考えた際、通信テンソルの階数によって通信計算量を特徴づけることを考えた。また、得られた結果の応用として、内積計算を一般化したものを考え、それに対して、強非決定性量子通信計算量と有界誤り量子通信計算量の差異を示すことを考えた。

その他、量子計算機シミュレータの開発を含め、実装容易性を考慮した量子計算機のモデルに関する研究を行った。

4. 研究成果

以下、「研究の目的」および「研究の方法」の各項目に対応する形で研究成果を説明する。

- (1) 一般の量子回路を LNN アーキテクチャ量子回路に変換する手法を開発した。この際、挿入されるスワップ演算の最小化を行っている。実際の回路に適用し、従来知られている最適な回路と同等な回路を生成できることを示した。この結果は、従来の「特定の回路向けにカスタマイズした回路最適化手法」を用いることなく、一般化した回路最適手法で従来と同等な回路を生成できたという意味で重要なものと考えられる。

- (2) 空スタック受理の量子プッシュダウンオートマトンにおいて、従来のプッシュダウンオートマトンよりも能力が弱くなる場合があることを示した。

具体的には、特定の言語について、その言語を古典確率プッシュダウンオートマトンでは認識できるが、量子プッシュダウンオートマトンでは認識できないことを示している。

この結果は、量子計算機が苦手とする状況を解明し、量子計算機の限界を示した結果と考えることができる。

- (3) 線上の量子ウォークについて、量子コインを symmetric $SU(2)$ とした際の時刻 t における各量子状態の確率振幅および各頂点に到達する確率を閉形式で表現した。量子ウォークの解析はシミュレーションにより行われているものが多い中で、閉形式で表現できたことは重要な結果であると考えられる。

- (4) 強量子非決定性通信モデルを考え、多者間通信において量子計算通信量の上界、下界の特徴づけを行った。

具体的には非決定性通信テンソルの階数を用いた通信計算量の特徴づけを行っている。NIH モデルに対しては階数の対数が通信計算量の下界を与え、NOH モデルに対しては階数の対数が通信計算量の上限を与えることを示している。

また、この結果の応用として、内積計算の一般化について、強非決定量子計算と有界誤り量子計算の差異を示した。この結果は通信計算モデルにおいて NQP が BQP に含まれないことを示しており、通信モデルにおける計算量クラスの重要な結果となっている。

上記の量子計算モデルに対する結果に加えて、量子計算機シミュレータの開発を含め、様々な量子計算モデルに関する解析を行い、量子計算機の限界を調べた。

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 5 件)

- ① M. Villagra, M. Nakanishi, S. Yamashita, and Y. Nakashima, “Tensor Rank and Strong Quantum Nondeterminism in Multiparty Communication,” *IEICE Trans. Inf. & Syst.*, 査読有, Vol. E96-D, No. 1, 2013, pp. 1-8, 10.1587/transinf.E96.D.1
- ② M. Villagra, M. Nakanishi, S. Yamashita, and Y. Nakashima, “Quantum walks on the line with phase parameters,” *IEICE Trans. Inf. & Syst.*, 査読有, vol. E95-D, no. 3, 2012, pp. 722-730, 10.1587/transinf.E95.D.722
- ③ Y. Hirata, M. Nakanishi, S. Yamashita, and Y. Nakashima, “An Efficient Conversion of Quantum Circuits to a Linear Nearest Neighbor Architecture,” *Quantum Information & Computation*, 査読有, vol. 11, no. 1& 2, 2011, pp. 142-166, <http://portal.acm.org/citation.cfm?id=2011393>
- ④ 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*, 査読有, vol. J93-D, no. 3, 2010, pp. 253-264,

http://search.ieice.org/bin/summary.php?id=j93-d_3_253&category=D&year=2010&lang=J&abst=

[学会発表] (計 9 件)

- ① M. Villagra, “Tensor rank and strong quantum nondeterminism in multiparty communication,” The 9th Annual Conference on Theory and Applications of Models of Computation (TAMC2012), May 17, 2012, 北京・Institute of Software Chinese Academy of Science (中国)
- ② M. Villagra, “Quantum query complexity of hamming distance estimation,” The 11th Asian Quantum Information Science Conference 2011 (AQIS2011), August 27, 2011, 釜山・Korea Institute for Advanced Technology (韓国)
- ③ M. Nakanishi, “On the weakness of one-way quantum pushdown automata under empty-stack acceptance,” 14th Workshop on Quantum Information Processing, January 10, 2011, セントーサ・The Capella (シンガポール)
- ④ M. Villagra, “Asymptotics of Quantum Walks on the Line with Phase Parameters,” Asian Conference on Quantum Information Science 2010 (AQIS2010), August 29, 2010, 東京都・東京大学
- ⑤ D. Yokomine, “A SAT Solver Based on Quantum and Classical Random Walk,” Asian Conference on Quantum Information Science 2010 (AQIS2010), August 29, 2010, 東京都・東京大学
- ⑥ M. Nakanishi, “On the Weakness of One-Way Quantum Pushdown Automata,” The Fourth International Conference on Quantum, Nano and Micro Technologies (ICQNM2010), February 11, 2010, セントマーチン・Sonesta Maho Beach Resort & Casino (オランダ領アンティル)

6. 研究組織

(1) 研究代表者

中西 正樹 (NAKANISHI MASAKI)

山形大学・地域教育文化学部・准教授

研究者番号：40324967