様式 C-19

科学研究費補助金研究成果報告書

平成２２年　６月　１日現在

研究種目：若手研究（Ｂ）
研究期間：2006～2008
課題番号：18700011
研究課題名（和文）　量子－古典協調計算の能力について

研究課題名（英文）　On the Power of Quantum-Classical Co-operation Models

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：量子－古典協調計算を対象に様々な計算モデルを取り上げ，その能力の解析や，効率的な量子アルゴリズムの提案を行った．また，量子暗号技術についても研究を行い，古典情報だけでなく量子情報も送信できる秘匿通信手法の提案，文字列に対する最適な量子封印プロトコルの提案を行った．さらに並列計算機向けの高速量子計算機シミュレーション手法を開発した．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	700,000	0	700,000
2007 年度	900,000	0	900,000
2008 年度	600,000	180,000	780,000
年度			
年度			
総　計	2,200,000	180,000	2,380,000

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：量子計算，量子暗号，量子計算機シミュレータ，量子－古典協調計算

１．研究開始当初の背景

量子力学の枠組みを使う計算機として量子計算機が注目されている．量子計算機上では量子効果により，状態の重ね合わせや干渉が起きる．この性質を利用することにより，従来の計算機(以下，古典計算機)より高速に計算を行える可能性が指摘されており，多項式時間因数分解アルゴリズムなどが開発されている．しかし，これらのアルゴリズムでは非常に多くの量子ビットを自由に制御できることが必要になり，現段階あるいはこの先しばらくの間に到達できる技術では実装することが困難である．言い換えると，実際の量子計算機の実現に際しては，扱える量子ビット数やオペレーションの回数に何らかの制約を課すことが必要である．そのような状況では，行いたい計算を純粋に量子計算機のみを用いて処理するのではなく，古典計算機，あるいは古典メモリ等の古典デバイスの補助を受けながら計算を行うのが現実的である．

２．研究の目的

上述の背景を踏まえ，本研究では，以下の３点を目的とした．

(1) 量子-古典協調計算モデルの能力の形式的な解析

使用できる量子計算資源の量が制限され

ている状況では，量子-古典協調計算モデルを用いることにより，可逆性等の量子計算特有の制約を緩和することが可能となるため，純粋に量子デバイスのみで実装された計算機よりも優位な点が出てくることが期待される．

本研究では，量子－古典協調計算モデルについて，その能力の解析を行い，使うことのできる量子計算資源が制限されているような状況において，古典計算機の補助により，純粋な量子計算機よりも(そして，もちろん純粋な古典計算機よりも)効率的に計算が可能であることを示すことを目的とした．

(2) 「計算」以外の量子情報処理への量子-古典協調動作の応用

量子情報処理には純粋に計算を行う以外にも様々なアプリケーションが存在することに着目し，それらのアプリケーションにおいても，古典計算資源の補助による優位性を示すことを第２の目的とした．純粋な計算以外のアプリケーションとして，具体的には，量子封印などの量子暗号分野のプロトコルを対象にする．これらのプロトコルにおいて古典計算資源を補助的に使うことで，安全性を保ったまま使用する量子計算資源の量を減らす等の効果が得られることが期待される．

(3) 量子計算機シミュレータの開発

(1), (2) は量子計算の振る舞いの「形式的な」解析を行う研究である．しかしながら，量子計算機は前述したように確率振幅と呼ばれる値に基づいて状態が遷移するある種の確率計算機であり，場合によっては，形式的な解析のほかに，シミュレーションによる解析が有効に働く場合がある．そのため，かねてより量子計算機のシミュレータの開発が盛んに行われていている．特に本研究で取り扱う「確率振幅に基づく状態遷移と古典的な確率に基づく状態遷移が共に起こるような状況」では，ますます解析が困難になるため，シミュレータの重要性が大きくなる．そこで，本研究の第３の目的としては，量子計算機シミュレータの開発を行う．

３．研究の方法

(1) 量子-古典協調計算モデルの能力の形式的な解析

２つの計算機 A と B がネットワークでつながっていて，A が n ビットの入力 x を持ち，B が n ビットの入力 y を持っている状況で，関数 f(x,y)を計算するのに A と B の間で何ビットのデータをやり取りしなければならないか(通信量とよぶ)という問題は分散計算を考えるときの基本的な問題である．このとき，A,B が量子計算機を持っており，通信には量子ビットを用いることができ，さらに，A,B が共通の(古典の)乱数にアクセスできるモデルを考える．これは確率振幅に基づく確率と，従来の古典的な確率の両方を取り入れた量子-古典協調計算モデルとみなすことができる．このモデル上で特定の関数を計算する場合の通信量の上下界を求め，古典プロトコルや，量子通信のみで古典の共通乱数を使用しないプロトコルとの能力の比較を行った．

さらに，量子オートマトンについて，その認識する言語のクラスの特徴づけを行うことにより，計算能力を解析した．

(2) 「計算」以外の量子情報処理への量子-古典協調動作の応用

量子封印プロトコルの開発を行うために，量子封印の安全性の妥当な定義づけを行う必要がある．既存の指標としては確率をもとにしたものしか提案されていなかったが，情報量にもとづく安全性の指標の提案を行った．その後，提案した安全性指標を満たす量子封印プロトコルを開発した．

また，秘匿通信プロトコルとして，古典情報だけでなく量子情報も送信できるものを開発するために，忠実度を用いた量子秘匿通信の安全性の指標の提案等を行った．その後，具体的な量子秘匿通信の開発に取り組んだ．

(3) 量子計算機シミュレータの開発

シミュレーションの高速化のため，並列計算機上にシミュレータを実装することを考えた．並列計算機ではノード間通信がボトルネックとなるため，まずは予備実験として並列計算機上で単純にシミュレータを実装した際の通信量の見積もりを行った．その後，通信量を減らすためのスケジューリングや，回路の等価変換の手法を開発した．

４．研究成果

(1) 量子プッシュダウンオートマトンの計算能力について，空スタック受理のモデルにおいては古典プッシュダウンオートマトンよりも能力が劣る場合があることを示した．通常，量子計算モデルは古典計算モデルに比べて能力が高くなると期待されるが，その逆の結果が示されたことが興味深い．

(2) 並列計算機を用いた量子計算機シミュレータを開発した．ノード間の通信量を削減するために，シミュレーション対象の回路をあらかじめ等価な回路に変換し，シミュレーション実行時のデータの移動を少なくすることで高速化を図っている．

(3) 量子回路の設計手法に関する成果とし

て次の２点が挙げられる．
① 量子アルゴリズムがユニタリ行列で与えられたとき，行列分解を行うことで基本量子ゲートの列として量子回路を生成する手法を考案した．
② 量子回路が与えられたときに，それを LNN アーキテクチャに変換する手法を開発した．LNN アーキテクチャとは線上に量子ビットが並んだ構成をとり，隣り合う量子ビットにのみ演算が可能であるというアーキテクチャである．提案手法では，既知の手法と比較して変換後の回路の量子ゲート数を少なくできることを実験により示した．

(4) 量子分散計算アルゴリズムに関する研究を行い，以下に示す結果を得た．
任意のトポロジのネットワークで接続された２者間で分散計算を行う際の通信量について，その下界を求める手法を提案した．また，この手法を応用し，リング上の k 者間で DISTINCTNESS 問題を解く量子分散アルゴリズムの上下界を求めた．

(5) n ビット論理関数に対する量子質問計算量の解析を行った．結果として，質問計算量が論理関数の on-set (真理値表に現れる１の個数) によって特徴付けられることを示した．

(6) 古典情報だけでなく，量子情報も直接相手に送信できる「量子直接秘匿通信プロトコル」を開発した．また，従来とは異なる忠実度に基づいた安全性の評価を行った．

(7) メッセージの開封確認を行うことのできるプロトコルに量子封印プロトコルがある．本研究では，文字列に対する量子封印プロトコルを提案し，その最適性を証明した．

その他，量子アルゴリズムに関する研究など，多方面にわたり研究を行った．

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 14 件）

① 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 年 3 月．（査読有り）
② M. Nakanishi, "On the Weakness of One-Way Quantum Pushdown Automata," Proc. of the Fourth International Conference on Quantum, Nano and Micro Technologies (ICQNM2010), pp.83-87, February 2010.（査読有り）
③ 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 & Computation, vol.9, no.5&6, pp.423-443, May 2009.（査読有り）
④ S. Tani, M. Nakanishi, and S. Yamashita, "Multi-Party Quantum Communication Complexity with Routed Messages," IEICE Trans. Inf. & Syst., vol.E92-D, no.2, pp.191-199, February 2009.(査読有り)
⑤ 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," Proc. of the Third International Conference on Quantum, Nano and Micro Technologies(ICQNM 2009), pp.26-33, February 2009.(査読有り)
⑥ 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," Proc. of the 19th International Symposium on Algorithms and Computation (ISAAC 2008), pp. 907-918, December 2008.(査読有り)
⑦ M. Nakanishi and Y. Murakami, "A Method of Randomizing a Part of an FPGA Configuration Bitstream," Proc. of 2008 International Symposium on Information Theory and its Applications(ISITA2008), pp.1493-1496, December 2008.（査読有り）
⑧ S. Tani, M. Nakanishi, S. Yamashita, "Multi-Party Quantum Communication Complexity with Routed Messages," Proc. of the 14th Annual International Computing and Combinatorics Conference(COCOON2008), pp. 180-190, June 2008.(査読有り)
⑨ Y. Murakami, M. Nakanishi, S. Yamashita, Y. Nakashima, and M. Hagiwara, "A Quantum Secure Direct Communication Protocol for Sending a Quantum State and Its Security Analysis," Proc. of the 6th WSEAS International Conference on Information Security and Privacy

(ISP'07), pp.91-97, December 2007.(査読有り)

⑩ M. Nakanishi, S. Tani, and S. Yamashita, "An Information-Theoretic Security Analysis of Quantum String Sealing," Proc. of the 6th WSEAS International Conference on Information Security and Privacy (ISP'07), pp.30-35, December 2007.(査読有り)

⑪ S. Yamashita, and M. Nakanishi, "A Practical Framework to Utilize Quantum Search," Proc. of the 2007 IEEE Congress on Evolutionary Computation (CEC2007), September 2007.（査読有り）

⑫ T. Suzuki, S. Yamashita, M. Nakanishi, and K. Watanabe, "Robust Quantum Algorithms Computing OR with $\eps$-biased Oracles," IEICE Trans. Inf. & Syst., vol.E90-D, no.2 pp.395 - 402, February 2007.（査読有り）

⑬ Y. Murakami, M. Nakanishi, M. Hagiwara, S. Yamashita and Y. Nakashima, "Quantum Secure Direct Communication Protocols for Sending a Quantum State," Proc. of the 2006 International Symposium on Information Theory and its Applications (ISITA 2006), October 2006.（査読有り）

⑭ T. Suzuki, S. Yamashita, M. Nakanishi, and K. Watanabe, "Robust Quantum Algorithms with ε -Biased Oracles," Proc. of 12th Annual International Computing and Combinatorics Conference (COCOON 2006), LNCS 4112, pp. 116-125, August 2006.（査読有り）

〔学会発表〕（計 22 件）

① S. Tani, "Quantum Communication Protocols with Public Coins,"情報処理学会ＡＬ研, 2009 年 9 月 15 日, 鳥取.

② A. Vikman, "An efficient middle-level framework for quantum circuit simulation on multiple simulator platforms," SWoPP2009, 2009 年 8 月 4 日, 仙台.

③ Y. Murakami, "Quantum Secure Direct Communication Protocol without Using Quantum Memory," SCIS2009, 2009 年 1 月 20 日, 滋賀.

④ H. Nishimura, "Average/Worst-Case Gap of Quantum Query Complexities," QIP2009, 2009 年 1 月 14 日, アメリカ.

⑤ Y. Hirata, "An Efficient Method to Convert Arbitrary Quantum Circuits to Ones on a Linear Nearest Neighbor Architecture," 量子情報技術研究会, 2008 年 11 月 20 日, 大阪.

⑥ S. Yamashita, "Quantum Query Complexity of Boolean Functions with Small On-Sets," 量子情報技術研究会, 2008 年 11 月 20 日, 大阪.

⑦ M. Nakanishi, "A Method for Secure FPGA Configuration," Computer Security Symposium2008(CSS2008), 2008 年 10 月 8 日, 沖縄.

⑧ 柴田章博, "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, 佐賀.

⑨ 柴田章博, "並列量子計算シミュレータにおける通信料削減手法の提案", 量子情報技術研究会, 2008 年 5 月 22 日, 東京.

⑩ M. Nakanishi, "An Almost Optimal Quantum String Sealing Protocol and Its Security Analysis," AAAC2008, 2008 年 4 月 26 日, 香港.

⑪ 村上ユミコ, "量子状態を送信するための量子秘匿直接通信とその安全性", 暗号と情報セキュリティシンポジウム (SCIS2008), 2008 年 1 月 23 日, 宮崎.

⑫ M. Nakanishi, "A Scheme for Protecting FPGA Configuration Bitstreams," Symposium on Cryptography and Information Security (SCIS2008), 2008 年 1 月 22 日, 宮崎.

⑬ S. Tani, "An Analysis of Quantum Communication Complexity Depending on Network Topologies," 量子情報技術研究会, 2007 年 11 月 21 日, 岡山.

⑭ Y. Nakajima, "Synthesis of Quantum Circuits for d-Level Systems using KAK Decomposition," The 11th Workshop on Quantum Information Processing, 2007 年 12 月 18 日, インド.

⑮ M. Nakanishi, "Tight Bounds on Information Gains in Quantum Sealing Protocols," The Tenth Workshop on Quantum Information Processing (QIP 2007), 2007 年 1 月 31 日, オーストラリア.

⑯ Y. Murakami, "A Quantum Secure Direct Communication Protocol for Sending a Quantum State and Its Security Analysis ," The Tenth Workshop on Quantum Information Processing (QIP 2007), 2007 年 1 月 31 日, オーストラリア.

⑰ 中西正樹, "量子文字列封印における復号化率と検出率のトレードオフについて", 量子情報技術研究会, 2006 年 11 月 21 日, 京都.

⑱ 山下茂, "Pure Dephasing を考慮した量子オラクル計算モデル",量子情報技術研

究会，2006年11月21日，京都.
⑲ 竹谷昌敏，"量子封印を用いた量子認証"，量子情報技術研究会，2006年11月21日，京都.
⑳ H. Nishiyama, "An Efficient Approximation of SU(d) Using Decomposition," Asian Conference on Quantum Information Science 2006 (AQIS 2006)，2006年9月2日，中国.
㉑ Y. Murakami, "Quantum Secure Direct Communication Protocols for Transmitting Quantum States," 量子情報技術研究会，2006年5月29日，東京.
㉒ 西山寛之，"3準位量子ゲート設計のためのユニタリ行列近似"，量子情報技術研究会，2006年5月29日，東京.

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

(2)研究分担者

（　　）

研究者番号：

(3)連携研究者

（　　）

研究者番号：