

氏 名 ルディ ライモンド ハリー プテラ
RUDY RAYMOND HARRY PUTRA
 学位(専攻分野) 博 士 (情 報 学)
 学位記番号 情 博 第 217 号
 学位授与の日付 平成 18 年 3 月 23 日
 学位授与の要件 学位規則第 4 条第 1 項該当
 研究科・専攻 情報学研究科通信情報システム専攻
 学位論文題目 Studies on Quantum Query Complexities and Quantum Network
 Coding
 (量子質問計算量および量子ネットワーク符号に関する研究)
 論文調査委員 (主査)
 教授 岩 間 一 雄 教授 福 嶋 雅 夫 教授 北 野 正 雄

論 文 内 容 の 要 旨

本論文では、最先端の計算モデルである量子計算に関して、量子質問計算量及び量子ネットワーク符号の観点から議論がなされている。量子質問計算量の効率に関しては、量子有限オートマトンと確率有限オートマトンの空間効率の対比、暗号分野で有名な Goldreich-Levin 問題に関する量子質問計算量の限界、エラー付き量子オラクルに対する質問計算量の限界及びオラクル同定問題に対する量子アルゴリズムの改良に関する結果が与えられている。また量子ネットワーク符号に関しては、従来の符号と違った斬新な符号の可能性が示されている。

第 1 章と第 2 章では研究の動機と結果の概要、および量子計算の基本原則が述べられている。またそれぞれの章での目的に対してどんな結果が得られたか、重要な部分はどこかが分かりやすくまとめられている。さらに、本論文の結果を理解するための必要な土台が簡潔に述べられている。

第 3 章では量子有限オートマトンと確率有限オートマトンの空間効率の議論を行っている。量子計算機構と確率計算機構の確率計算の違いから、量子有限オートマトンは確率有限オートマトンより平方的に少ない状態数で実現できることが示されている。この結果は量子探索が古典探索より平方的に速い時間で実現できることに相当し、量子質問計算量の効率を空間計算量の効率に変換する手法を示している。

第 4 章では暗号分野において重要な問題の一つである Goldreich-Levin 問題に対するアルゴリズムの量子質問計算量の限界を与えている。さらに、第 5 章では第 4 章の手法を拡張し、一般的な問題に対するエラー付き量子オラクルに対する質問計算量の限界を、エラーのない量子オラクルに対する質問計算量と比較する形で計算している。

第 6 章ではオラクル同定問題に対する量子アルゴリズムの改良について述べている。これまで、量子探索など特定の問題に対してエラー付き量子オラクルを用いる研究は行われていたが、本章では幅広い問題をエラー付き量子オラクルを用いて効率的に解くアルゴリズムが示されている。これによって未解決だった量子学習理論問題を解くことができることも述べられている。

第 7 章では量子ネットワーク符号についての結果を与えている。古典情報理論においても比較的新しい分野であるネットワーク符号の量子版を導入し、通信における量子情報のコピーや離散的な符号化といった基本操作に対する困難を解消し、代表的ネットワークに対する量子ネットワーク符号化プロトコルを与えた。以前の研究で明かされなかった量子ランダムアクセス符号の限界も解析されている。

最後に第 8 章では、研究のまとめと今後の方針が与えられている。

論 文 審 査 の 結 果 の 要 旨

素因数分解が量子アルゴリズムによって効率的に解けることが示されて以来、量子探索等の様々な量子アルゴリズムが開

発されてきた。しかし、その計算原理の特異な性質から量子アルゴリズムの設計には古典アルゴリズムと異なる独特な手法が求められるためか、量子計算と古典計算の効率の差の議論においては依然として未解決な問題が多い。本論文では、量子と古典計算機構の効率の差を質問計算量を用いて解析し、斬新な量子アルゴリズムを与えている。また、量子ネットワーク符号という新しい符号化の概念を提案し、量子計算の新たな可能性を示している。本論文の結果は古典計算機構との比較における量子計算機構の優越さの確証及びその本質を見極める新たな側面を与える。本論文の結果について特筆すべき点は以下の通りである。

1. 量子と古典計算機構における確率計算の差だけに着目し、量子計算機構が古典計算機構よりもその計算空間が効率的に実現できることを示している。この結果は量子計算機構の優越さに関する新たな証拠を与えた。

2. エラー付き量子オラクルモデルによる解析を通して、Goldreich-Levin 問題やより一般の問題に対する計算限界を斬新な解析手法で示している。

3. オラクル同定問題に対する量子アルゴリズムを改良するだけでなく、エラー付き量子オラクルの下でロバストな量子アルゴリズムを示している。これによって、今まで問題ごとにしか扱われていなかったエラー付き量子オラクルの議論に対する一般的な枠組みを与えている。

4. 量子ネットワーク符号でネットワーク構造に基づいた量子符号化の可能性を示し、古典ネットワークだけでは決して実現できない量子プロトコルを述べている。更に、以前の研究では知られていなかった量子ランダムアクセス符号に関する限界が証明された。

エラーのないオラクルに対する量子質問計算量は今までの研究によってある程度解明されてきたが、エラー付きオラクルに対する解析について本研究の前半の結果は包括的な考察を与える先駆的なものである。また後半の量子ネットワーク符号の研究は、現代の技術でも実現可能な規模の量子ネットワークを扱っており、今後の量子計算研究には大きな影響を与えると考えられる。

以上、本研究は量子計算に関するアルゴリズムの設計と解析、およびネットワーク構造を考慮した量子情報の符号化研究の発展に関して学術上意義深い結果を導いている。よって、本論文は博士（情報学）の学位論文として価値あるものと認める。

また、平成18年2月22日に実施した論文内容とそれに関連した試問の結果合格と認めた。