

(続紙 1)

京都大学	博士（情報学）	氏名	照山 順一
論文題目	Studies on Quantum Query Complexity for Oracle Identification Problems（オラクル同定問題の量子質問計算量に関する研究）		
（論文内容の要旨） 量子計算は量子力学の法則に基づいた計算概念である．現在の計算モデルよりも高速な計算が期待され，計算機科学及びその物理との境界領域における重要な一分野となっている． 本研究ではオラクル同定問題に関して議論がなされている．オラクル同定問題とは，長さ n の 2 進列を持つオラクルが与えられ，その列をオラクルへの質問によって特定する問題である．本問題は量子計算における基本的問題の一つで，グローバー探索に代表される探索問題の一般化である．オラクル質問の形式，質問に対する答えの決定方法はオラクルモデルによって変わり，本問題の質問計算量もオラクルモデルに依存する．本研究では，2つのオラクルモデルを導入し，それらに対するオラクル同定問題の量子質問計算について議論がなされている．それぞれの問題において，量子計算を用いることによって，古典計算に対しどれだけ計算量を減少することができるのか，またその限界がどの程度なのかを解明することが本研究の目的である． 第1章では，上記の様な研究の動機，関連研究，既存結果や研究の歴史が述べられており，第2章では量子計算に関する基礎的事項が与えられている． 第3章では古くから知られている偽コイン問題を扱っている．偽コイン問題は天秤の動作をオラクルとしてとらえることによりオラクル同定問題として見ることができる．本章では，既存のアルゴリズムであるBernsteinとVaziraniのアルゴリズムと，グローバーのアルゴリズムを一般化した振幅増幅法との組み合わせによる量子アルゴリズムの構築がされている．このアルゴリズムにより，古典計算に対して質問計算量が4乗根まで減少することが示されている．この量子計算による4乗根という加速は今までに知られていない結果である．また，オラクルへの質問形式を限定した場合に構築した量子アルゴリズムが最適であることが示されている． 第4章ではDNA配列の検査に関連のあるオラクルモデルに対するオラクル同定問題を扱っている．このオラクルモデルは部分列オラクルと呼ばれ，質問として任意の長さの2進列を受け取り，その列がオラクルの持つ列の部分列か否かを返すオラクルである．本章で与えるアルゴリズムは古典的な前処理を行うことで量子計算が能力を発揮できることを見出している．この量子アルゴリズムによって，古典計算に対して質問計算量が線形倍ではあるが減少する，つまり古典計算の情報理論的下限を下回することを証明している．また，質問計算量の下界についても議論がなされている．部分列オラクルと性質の似た別のオラクルモデルを導入し，敵対者論法によって下界を与え，本問題への還元を与えることで本問題のほとんどタイトな下界を得ている．このことは，部分列オラクルにおいては量子計算の能力が発揮しづらいことを示している． 最後に第5章において，以上の結果がまとめられ，今後の方針が与えられている．			

(論文審査の結果の要旨)

量子計算の解析には、計算モデルの本質的な違いから古典計算とは異なる手法が要求される。従って、量子アルゴリズムの設計や限界証明には従来の組み合わせ的手法の枠内に入らない独特な手法を用いる必要があり、そのため、量子計算と古典計算の能力の差についてはいまだ未解決な問題が多い。

本研究では、基本的な探索問題であるオラクル同定問題に注目し、量子計算と古典計算の効率の差を質問計算量の観点から議論している。具体的には、古典的パズルである偽コイン問題で使用される天秤をモデル化した天秤オラクルと、DNA配列の検査と関わりのある部分列オラクルのそれぞれについて、量子計算がどの程度有効であるか解析を行っている。

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. 偽コイン問題がオラクル同定問題として形式化できることを示している。このオラクル同定問題に対して、質問計算量を入力サイズの4乗根まで減少させる量子アルゴリズムを与えている。量子計算における多くの結果が平方根までの減少であるのに対し、4乗根という加速を始めて発見したという意味でこの結果は大変興味深いものである。本アルゴリズムでは、天秤には常に比較的数の多いコインを載せており、それが効率の良い方法であることを示唆しているが、そのような仮定のものでは、この計算量が最適であることも証明している。
2. 部分列オラクルを用いたオラクル同定問題に対しては、直接有効なアルゴリズムはなさそうに見える。しかし、古典計算による前処理に着目し、それを理論計算機科学における基本的問題である記号列処理問題に置き換えて高度な解析を行っている。このことで、量子計算の能力が発揮できる状況を作り出した。
3. 部分列オラクルにおいて量子計算が能力を発揮しづらいことを、数学的にほとんどタイトな下界を与えることで示している。具体的には、別のオラクルモデルを導入し、そのモデルにおけるオラクル同定問題の量子質問計算量の下界を得たのちに本問題への帰着を行うというものである。解析のアイデアはシンプルではあるが独自性の高いものである。

以上、本研究はオラクル同定問題に対する量子質問計算量に関して、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のあるものと認める。

また平成25年2月18日論文内容とそれに関連した口頭試問を行った結果合格と認めた。