審 査 の 結 果 の 要 旨

氏　名　　本多　健太郎

本論文は量子計算の解析に有用な古典的手法の研究を行ったものである。量子計算とは、量子力学の法則に基づく新しい計算パラダイムである。古典計算が持たない独特の特性を持ち、独自な手法を用いて研究されてきたが、従来の解析手法も有用であり、様々な古典的手法が量子計算の研究にも役立ち得る。本論文では、古典的手法による量子計算の解析に関して、以下の二つのテーマについて研究を行っている。１．量子プログラムのための抽象解釈、２．ブラインド量子計算。テーマ１では、量子計算のプログラムの形式検証において、既存研究より精度の高い量子もつれの存在解析を可能にした古典的手法を提案する。テーマ２における主要結果は、古典公開鍵暗号に基づく公開検証可能なブラインド量子計算プロトコルの構築と解析である。

本論文は5章からなる。第１章は序論で、量子計算の概観および以上のような背景を述べ、本研究の位置づけと貢献についてまとめる。第２章では、最初に量子計算の基礎について解説があり、次にその後に必要となる、量子計算のスタビライザー形式と測定ベース量子計算について解説が与えられている。また、形式検証と暗号理論の基礎事項について述べられている。

第３章はテーマ１の研究内容に対応している。この章では、与えられた量子プログラムに対し、プログラムを実行した際に出力される量子状態に量子もつれが存在しているか判定する問題を扱う。この問題に対して既存研究では、2008年にPerdrixによって抽象解釈を用いた手法が提案されたが、１量子ビットの基底のみに基づく解析であるため、問題点が多く残り、単純なプログラムでも正しく解析できない例がいくつか挙げられる。本論文では、複数量子ビットの基底に基づく手法への拡張に成功し、既存の解析手法を大いに改善している。その改善を得るに当たって中核となるアイデアは、量子計算をスタビライザー形式で表すことである。古典的な記述方法であるスタビライザー形式を活用することによって、複数量子ビット基底に基づく量子プログラムの意味論の導入に成功している。その意味論の健全性も示し、既存研究より精度の高い量子もつれの存在解析が可能であることを厳密に証明する。また、その意味論の近似を求める計算量を定量

的に議論し、定数深さのプログラムに対して効率性を示す。最後に、スタビライザー形式をさらに拡張した意味論も提案し、その意味論の優位性を議論する。全体を通して第３章の手法と結果は、量子プログラムの自動形式検証という、今後も量子情報処理の発達によって必要不可欠となる分野に対し、様々な問題を解決しており、高く評価する。

第４章はテーマ２の内容に対応し、ブラインド量子計算プロトコルを扱う。ブラインド量子計算とは、量子計算機を持っていない者（アリス）と量子計算機を持っている者（ボブ）の間のセキュアーな委託計算である。すなわち、アリスが量子計算をボブに依頼できるが、アリスの入力、出力とアルゴリズムはボブに秘密にするというものである。先行研究では、２００５年から様々なブラインド量子計算プロトコルが提案されてきた。本論文では、「公開検証可能性」という、第三者がプロトコルが正しく実行されたか確認できる概念をその研究分野に導入し、公開検証可能性を厳密的且つ正確的に定義することに成功し、初めての公開検証可能なブラインド量子計算プロトコルを構築する。この構築の中核となるアイデアは、公開鍵暗号の古典的な技術を従来のブラインド量子計算プロトコルと組み合わせることである。得られるプロトコルの安全性の解析は従来のプロトコルの解析より困難であるが、本論文では妥当な条件の下で安全性を厳密に証明することに成功しており、このことを高く評価する。

第５章では、論文全体のまとめと結論が述べられている。今後の展望についても議論を行っている。

以上のように、本論文では、二つの古典的手法に関する研究を行い、それぞれにおいて数学的に厳密な解析に基づき、量子計算の解析のための有用性を示すことに成功している。量子プログラムの自動形式検証及びブラインド量子計算に対する相当な寄与を行っていることが認められる。

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。