様式Ｃ－１９

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２４年　６月　８日現在

機関番号：８２６２６
研究種目：若手研究（Ｂ）
研究期間：2008～2011
課題番号：２０７０００１７

研究課題名（和文）隠れ部分群問題に対する効率的量子アルゴリズムの構築可能性の分析

研究課題名（英文）Analysis of possibility of efficient quantum algorithms for Hidden Subgroup Problem

研究代表者
縫田 光司　（NUIDA KOJI）
独立行政法人産業技術総合研究所・情報セキュリティ研究センター・研究員
研究者番号：２０４３５７６２

研究成果の概要（和文）：本研究では、量子力学の原理に基づく強力な次世代型コンピュータの候補である量子コンピュータの基礎理論について、特にその上での計算に特化した量子計算アルゴリズムの観点から研究を行った。まず、量子計算の基盤となる量子情報理論について研究し、量子状態識別や量子ビットの物理原理的特徴付けに関する結果を得た。また、量子アルゴリズム分野の主要課題の一つである隠れ部分群問題について、従来手法の問題点の検討を行い今後の研究課題の整理を行った。

研究成果の概要（英文）：In this research, I studied the fundamentals of quantum computers which are based on quantum physics and are expected as a candidate of powerful new-generation computers, especially from the viewpoint of quantum algorithms specialized to the quantum computers. First, I focused on quantum information theory that is a base of quantum computation, and obtained some research results on quantum state discrimination problems and on characterizations of quantum bits from physical principles. On the other hand, I investigated Hidden Subgroup Problems (HSPs) which are one of the main research topics in the area of quantum algorithms; I revisited the known approaches to HSPs and analyzed drawbacks of these approaches, which will be future research subjects.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	800,000	240,000	1,040,000
２００９年度	700,000	210,000	910,000
２０１０年度	700,000	210,000	910,000
２０１１年度	900,000	270,000	1,170,000
年度			
総　計	3,100,000	930,000	4,030,000

研究分野：数学・情報セキュリティ
科研費の分科・細目：情報学基礎
キーワード：応用数学、量子情報理論

１．研究開始当初の背景

(1) 現在用いられているコンピュータは、物理的な観点からは古典力学的な原理に基づいて作動している。一方、従来と異なる量子力学的な原理に基づくコンピュータである量子コンピュータの概念が提唱され、基礎理論的な研究が進められてきた。これらの研究はソフトウェアとハードウェアの両面から進められているが、特にソフトウェアの観点からは、P.Shor が 1997 年の論文で発表した

成果（素因数分解の多項式時間量子アルゴリズムの考案）が、古典力学的なコンピュータと比較した量子コンピュータの優位性を示唆する画期的な成果と認識されている。この研究を契機として、近年では量子コンピュータに関する研究が世界的に活発に行われるようになっている。

(2) コンピュータを用いて安全な通信を実現する暗号技術のうち、現在最も広く用いられている方式の一つが、RSA 暗号という公開鍵暗号方式である。その安全性の根拠は整数の素因数分解の「計算困難性」であり、現在の最先端の科学技術でも巨大な整数の素因数分解を現実的な時間内に計算できないという事実が、攻撃者が暗号の復号鍵を現実的な時間内に正しく推測できないことを意味する。しかしながら、前述の Shor の研究結果は、量子コンピュータが将来的に実現された暁にはRSA暗号の安全性が崩れてしまうことを意味する。そのため、この成果は暗号・情報セキュリティ分野の広範囲に強い衝撃を与えることとなった。

(3) 以降、暗号分野では、「耐量子計算暗号」などと呼ばれる、量子コンピュータをもってしても破れない暗号方式の研究が重要課題の一つとなっている。その大きな方向性の一つが、量子コンピュータにとっても計算困難と思われる問題とそうでない問題との線引きを進め、素因数分解に代わって量子コンピュータに対抗し得る計算困難な問題を新たに提示することである。このような暗号学的な観点からも、量子コンピュータの研究の重要性が認識されている。

(4) 上述した Shor の成果以降の量子計算手法（量子アルゴリズム）分野では、Shor の研究を一般化する形で提唱された「隠れ部分群問題」という問題に対する量子アルゴリズムの考案が主要課題の一つとなっている。この問題は、数学的に抽象化された代数構造の一種である「群」を舞台とするある種の計算問題であり、舞台となる群を様々に選ぶことで、素因数分解や離散対数問題、格子最短ベクトル問題、グラフ同型問題といった計算理論における数々の重要な問題と密接な関連を持つ。そのため、隠れ部分群問題は量子アルゴリズムの分野における主要な問題の一つと考えられるようになり、世界中で数々の研究が行われてきた。さらには、ある種の群における隠れ部分群問題について予想されている「計算困難性」を安全性の根拠とする暗号方式も提案されている。しかし、隠れ部分群問題の研究の歴史はまだ浅いものであるため、その計算困難性については未だ充分に信頼できると言い難い状況である。

２．研究の目的

本研究では、量子アルゴリズム分野の主要研究課題の一つである隠れ部分群問題についての研究を行う。本問題の研究に必要となる基礎理論の整備を行うとともに、隠れ部分群問題に関する効率的な量子アルゴリズムの構築可能性ないし不可能性について新たな知見を得ることを目的とする。

３．研究の方法

(1) 量子アルゴリズムの設計や性能解析、また将来的な量子コンピュータの実装といった様々な研究課題の基礎的な道具となる量子情報理論について研究を行い、隠れ部分群問題の研究に役立つ知見を蓄える。

(2) 隠れ部分群問題の舞台となる群、および関連する数学的対象についての基礎研究を行い、隠れ部分群問題の研究に役立つ知見を蓄える。

(3) 上記の研究により得た知見を基に、隠れ部分群問題の量子アルゴリズム構築に関する既存研究成果の改善すべき点を見出し、その改善方法について検討を行う。

４．研究成果

(1) 本研究の対象である隠れ部分群問題の設定を整理すると、問題の舞台となっている群の部分群の候補に応じて量子力学的な状態（量子状態）が一つずつ対応しており、その候補から選ばれた一つの量子状態が与えられたとき、与えられた状態が元々の候補のうちどの状態であるかなるべく高い確率で判定する、という状況設定である。この問題設定は、量子情報理論における基盤的な問題の一つである「状態識別問題」の設定と極めて良く合致しており、そのため状態識別問題を詳しく研究することで隠れ部分群問題に関する有益な知見が得られるものと考え、研究を行った。その結果、量子状態の識別問題における理論的な最適成功確率を見積もる上で有効となる幾何学的手法を新たに見出すことに成功した。

より詳しくは、量子力学における基本概念である「状態」とその「観測」の概念を抽象化・一般化した理論である「一般確率モデル」における状態識別問題について研究を行った。一般確率モデルにおける状態や観測の概念は、凸集合や超平面といった幾何学的対象によって記述されるため、幾何学的な取り扱いと相性が良い。本研究では、ハーン＝バナッハの拡張定理など関数解析学の知見を応用して、ある種の状況の下で、識別成功確率の上限を厳密に達成する状態識別戦略が実際に存在することを証明し、またその戦略の幾何学的表現が持つ性質を提示した。この成

果は量子情報理論に関する主要国際会議の一つである Quantum Information Processing のポスターセッションで発表後、数理物理分野の査読付き国際論文誌 Journal of Mathematical Physics に採録されるなど、当該分野で国際的に認められている。また、それらの発表後には海外の研究グループから問い合わせを受けるなど、少なからずインパクトを与えたようである。

一般確率モデルは量子力学を包含する一般化であるため、この成果は量子情報理論の文脈にも直ちに適用可能である。今後考えられる研究の方向性としては、この成果に用いた手法を適用可能な状況をより拡大することなどが考えられる。例えば、この成果は主に状態の候補が二つである場合を想定しているが、応用上はより多くの状態候補がある場合にも適用可能な理論を構築することが重要であると考えられる。

(2) 隠れ部分群問題の研究の基盤となる量子情報理論においては、通常の情報理論における情報エントロピーの概念を拡張した量子エントロピーの概念、また量子エントロピーと関連する状態の類似性指標が重要な役割を果たしている。これらの概念は隠れ部分群問題の研究においても重要と考えられることから、量子エントロピーや状態の類似性指標について、上述した一般確率モデルの立場から研究を行い、いくつかの既知の性質に対する新たな解釈を提示するとともにいくつかの未知の性質を見出した。この成果は数理物理分野の査読付き国際論文誌 Reports on Mathematical Physics に採録されるなど、当該分野で国際的に認められている。

一般確率モデルは量子力学を包含する一般化であるため、前述の成果と同様、この成果も量子情報理論の文脈に直ちに適用可能である。今後考えられる研究の方向性としては、今回見出したもの以外の性質を探求するとともに、一般確率モデルにおける量子エントロピーや状態の類似性指標のより適切な拡張を模索することなどが考えられる。

(3) 本研究において隠れ部分群問題の考察を行う過程で、隠れ部分群問題に関する既存研究について改めて精査し、既存研究成果の理論的特徴やその改善が望まれる点について整理を行った。それらの内容を数学分野の国内シンポジウムにおいて概説講演として発表するとともに、シンポジウム講演集収録の文書としてまとめた。ここで得られた知見はその後の本研究において役立ったが、さらに文書としてまとめたことで今後の同分野の発展にも一定の貢献を果たすものと期待される。

(4) 量子アルゴリズムの設計の背後にある基本的な計算原理は、量子コンピュータの実装に用いられる量子系の物理的性質と深く関連している。特に、量子コンピュータで用いる最小記憶素子の候補と考えられている２準位量子系（キュービット）に着目し、ある物理系の振舞いがキュービットと等価になるための必要充分条件を見出した。

上述の通り、一般確率モデルは量子力学系を包含する形で一般化した物理系であることから、キュービットをその特殊ケースとして含んでいる。この研究では、一般確率モデルで記述される状態空間について、どのような「物理原理」が満たされればその状態空間が物理系としてキュービットと等価になるかを考察した。そして、キュービットと同じ３次元の自由度を持つ一般確率モデルについて、キュービットと等価になるために必要充分な「物理原理」の集合を特定した。この成果は物理学や量子情報理論の観点だけでなく、幾何学をはじめとする数学の観点からも意義深いものと考えられる。この成果は前述した量子情報理論に関する主要国際会議の一つである Quantum Information Processing のポスターセッションなど国内外の研究集会で発表し、その際には複数の研究者から問い合わせを受けるなど反響があった。この成果については、２編の論文をプレプリントサーバにおいて公表済みである他、査読付き国際論文誌での採録を目指して内容を推敲中である。

この成果は、キュービットの物理的特徴に対する新たな解釈を与えたことで、量子コンピュータの記憶素子の原材料を選定する際などに役立つ知見を与えているものと期待される。さらに理論的観点からは、この成果は幾何学分野における関心事の一つである球体の特徴付けの新たな例の提示にもなっている。今回の成果は３次元空間に限定したものであったが、今後の研究方針の一つとしてはより高次元の球体についても同様の「物理原理的」な特徴付けを模索する研究が考えられる。

(5) 隠れ部分群問題に対する主要な既存の量子アルゴリズムにおいては、舞台となる群の元を表す量子レジスタと隠れ部分群による剰余類を表す量子レジスタの２種類を用いているが、従来の手法ではこのうち後者の量子レジスタは補助的な役割でしか用いられておらず、アルゴリズムの早い段階でその情報が捨てられてしまうという特徴があった。そのため、後者の量子レジスタをより積極的に活用することで、従来の量子アルゴリズムの性能を改善できるのではないかと考察した。さらに言えば、隠れ部分群問題に関する従来の定式化の方法自体、剰余類を表す

量子レジスタの積極的活用を考慮に入れていないのではないかとも考えられる。しかし、例えば隠れ部分群問題の計算困難性を根拠とする暗号方式を考える際などは、実際上はこの量子レジスタを積極的に活用する攻撃者の存在も考慮する必要がある。以上の理由から、隠れ部分群問題の定式化の再検討も視野に入れた、剰余類を表す量子レジスタの積極的活用法について問題の整理と検討を行ったが、具体的な成果を得るまでには至らなかったことから、この点は今後の研究課題と考えている。

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９件）

① 縫田光司: "量子力学の物理原理的特徴付けと凸集合の幾何学", 北海道大学数学講究録 148 号. 59-66 (2011), 査読無, http://eprints3.math.sci.hokudai.ac.jp/2140/
② 木村元, 縫田光司, 今井秀樹: "物理原理に基づく量子ビット系の導出", 第 33 回情報理論とその応用シンポジウム(SITA2010)予稿集. CD-ROM (2010), 査読無, DOI:なし
③ Gen Kimura, Koji Nuida, Hideki Imai: "Distinguishability measures and entropies for general probabilistic theories", Reports on Mathematical Physics vol.66. 175-206 (2010), 査読有, DOI:10.1016/S0034-4877(10)00025-X
④ Koji Nuida, Gen Kimura, Takayuki Miyadera: "Optimal observables for minimum-error state discrimination in general probabilistic theories", Journal of Mathematical Physics vol.51. 093505 (2010), 査読有, DOI:10.1063/1.3479008
⑤ 縫田光司: "量子計算、量子アルゴリズムと有限群の表現論", 2009 年度表現論シンポジウム講演集. 74-85 (2009), 査読無, DOI:なし
⑥ 縫田光司: "一般確率モデルから眺める量子情報理論", 北海道大学数学講究録 140 号. 37-41 (2009), 査読無, http://eprints3.math.sci.hokudai.ac.jp/1980/
⑦ 縫田光司, 木村元, 宮寺隆之: "On two-state discrimination problems in generic probability models", 2009 年暗号と情報セキュリティシンポジウム(SCIS2009)予稿集. CD-ROM (2009), 査読無, DOI:なし

〔学会発表〕（計６件）

① 縫田光司: "量子力学の物理原理的特徴付けと凸集合の幾何学", 第 7 回数学総合若手研究集会. (2011 年 3 月 3 日). 北海道大学(札幌市)
② Koji Nuida: "On derivation of qubit systems from physical principles", 14th Workshop on Quantum Information Processing. (2011 年 1 月 10 日). The Capella(Sentosa,Singapore)
③ 縫田光司: "量子計算、量子アルゴリズムと有限群の表現論", 2009 年度表現論シンポジウム. (2009 年 11 月 18 日). フェストーネ(沖縄県)
④ 縫田光司: "On Two-State Discrimination Problems in Generic Probability Models", 2009 年暗号と情報セキュリティシンポジウム(SCIS2009). (2009 年 1 月 20 日). 大津プリンスホテル(滋賀県)
⑤ Koji Nuida: "On Minimum-Error State Discrimination Problems in Generic Probability Models", The Twelfth Workshop on Quantum Information Processing(QIP 2009). (2009 年 1 月 14 日). Santa Fe Convention Center(NM,USA)

〔その他〕

① （プレプリント） Gen Kimura, Koji Nuida, “On affine maps on non-compact convex sets and some characterizations of finite-dimensional solid ellipsoids”, e-print arXiv:1012.5350, http://jp.arxiv.org/abs/1012.5350
② （プレプリント） Gen Kimura, Koji Nuida, Hideki Imai, “Physical equivalence of pure states and derivation of qubit in general probabilistic theories”, e-print arXiv:1012.5361, http://jp.arxiv.org/abs/1012.5361

６．研究組織
(1)研究代表者

縫田　光司（NUIDA　KOJI）
独立行政法人産業技術総合研究所・情報セキュリティ研究センター・研究員
研究者番号：２０４３５７６２