様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　６　月　２４　日現在

機関番号：　１２６０１
研究種目：　若手研究(B)
研究期間：　2012～2014
課題番号：　２４７００００６

研究課題名（和文）量子プロトコルの検証のための形式手法

研究課題名（英文）Formal Methods for Verification of Quantum Protocols

研究代表者
角谷　良彦（Kakutani, Yoshihiko）

東京大学・情報理工学（系）研究科・助教

研究者番号：７０３７６６１４

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：通常の計算の枠組みでは、プログラムやプロトコルの検証を行うための様々な形式手法が研究されている。本研究では、形式手法を量子計算に応用するための考察を行った。特に、量子プロトコルの安全性を検証することを目標に、量子プロセス計算の理論的考察を行った。その結果として、量子鍵配送プロトコルの安全性の証明を、量子プロセス計算の枠組みで形式化することに成功した。

研究成果の概要（英文）：Formal methods are studied widely for verification of programs and protocols in the field of the usual computation. We have studied formal methods for quantum computation. Especially, we investigated the quantum process calculi in order to verify the security of quantum protocols. As a result, we formalized a proof of the security of the quantum key-distribution protocol in the quantum process calculus.

研究分野：　理論計算機科学

キーワード：　形式手法　量子プロトコル　セキュリティ検証　プロセス計算

１．研究開始当初の背景

近年、プログラムやプロトコルを検証するための形式手法の研究が盛んに行われている。プログラムの大規模化やプログラマの増加に伴い、かつて行われていたテストベースの方法では、プログラムの正しさを検査するのが困難になり、形式的検証の重要性が増していることが、その理由の一つである。
テストベースの検証では、書き上がったプログラムにいくつかの入力を与えて実行し、その挙動をチェックする。テスト用に準備する入力や環境のパターン数はある程度限定されることになるが、通常、プログラムは無限もしくは相当数の種類の入力や環境を受け付けるため、テストベースの手法で完全にプログラムの正しさを保証することは不可能である。それに対して、形式手法による検証はプログラムの正しさを数学的に保証するため、形式手法の設計に間違いがなければ、プログラムにバグの入り込む余地はない。適用可能な場合には、形式手法は非常に強力であるが、その分、背景となる基礎研究は重要となる。
その一方で、量子計算に関する研究もまた活発に行われている。量子通信路を使って動画を送信する実験が成功したということもあり、量子通信や量子プロトコルの研究は活発に行われている。また、量子コンピュータはまだ汎用的な実用段階にはないものの、その実現に向けて着実に成果が得られつつある状況である。
量子計算における理論的な研究では、量子コンピュータを用いる効率的なアルゴリズムや量子理論に基づく暗号プロトコルなどが提案されている。特に、量子計算と古典計算の計算能力の違いを明らかにするための研究は多い。例えば、通常のコンピュータで入力に対して多項式時間内に終了する素因数分解アルゴリズムは知られていないが、量子コンピュータを使って多項式時間内に高確率で素因数を求めるアルゴリズムは存在する。これらの研究から、量子コンピュータは古典コンピュータよりも優れた計算能力を有していると考えられている。しかしながら、その量子コンピュータを研究者以外のプログラマが利用することを想定した研究は多くは提案されていない。また、同様に、多方面から量子プロトコルが提案されるような状況もあまり想定されていない。

２．研究の目的

将来、量子コンピュータや量子通信が一般に普及すると、量子プログラムや量子プロトコルの検証の需要が高まることは容易に予想される。背景でも述べたが、プログラムの大規模化やプロトコルの複雑化が進むと、ナイーブな検証手法では十分な対処が不可能となる。量子計算についても、このままプログラムの大規模化やプロトコルの複雑化が進めば、古典的な場合と同様の問題が生じるのは明白である。そのような問題を解決するため、本研究では、量子計算に対応した形式手法について理論的な考察を行い、量子プログラムや量子プロトコルの正当性、安全性を形式的に検証することを目指す。本研究の成果は直ちに現在の社会に利用可能なものとは言えないが、量子コンピュータや量子通信の普及が進めば、いずれ必要となる技術である。

３．研究の方法

プログラムの正しさを検証するための基礎的な枠組みとしては、例えば、Hoare 論理がある。量子計算のための Hoare 論理も研究されており、それらは量子プログラムの検証に対して部分的に有効であることが知られている。しかし、既存の Hoare 論理は万能ではなく、通信を伴う量子プロトコルの検証に対してはそれほど有効な手法とは言えない。本研究では、量子プロトコルの検証が可能な枠組みについて考察する。中でも特に、量子鍵配送プロトコルの安全性を形式的に検証することに重点を置いて研究を進める。形式手法の先には検証の自動化があるが、自動検証ツールの開発も視野に入れて研究を進める。
プロトコルの安全性を証明する汎用的な手法として、対象のプロトコルを等価な別のプロトコルに変換し、変換後のプロトコルの安全性を証明することで、元の安全性を保証するというものがある。この手法を形式的に議論するには、プロトコルの等価性が問題になる。古典的な場合、プロトコルの等価性の定義や証明には、プロセス計算が有効なことが知られている。本研究では、これを量子プロトコルが扱えるよう拡張することを考える。量子プロセス計算はいくつか提案されているが、等価性については十分な研究がなされているとは言えない。
プロセス計算の等価性として、よく利用されるのは双模倣関係である。量子プロセス計算でも双模倣関係は定義されているが、工夫なしには BB84 などのプロトコルの安全性証明に利用することはできない。本研究では、双模倣を含めたプロセス計算の等価性について考察し、それを利用して量子プロトコルの安全性を検証する。
プロセス計算における等価性の概念で、双模倣と並んで重要とされるのは観察等価性である。量子プロセス計算の研究では、これまで適切な観察等価性の定義は知られていない。本研究では、量子プロセス計算の観察等価性について考察することで、プロセス計算が量子物理学で利用される数学モデルとして適切であることを示す。

４．研究成果

(1) 量子プロセス計算を量子鍵配送プロトコルの安全性証明に応用した。量子鍵配送プロトコル BB84 の安全性には、Shor と Preskill による証明が既に存在する。この証明では、BB84 の安全性を EDP を用いた別のプロトコルの安全性に帰着している。本研究では、プロトコルを量子プロセス計算におけるプロセスとして形式化し、プロトコル間の変換を双模倣として捉えることに成功した。元の安全性証明においては、プロトコルの変換は複数のステップからなっており、個々のステップの変換の前後でプロトコルが等価であることを保証している。対して、本研究の手法を利用すれば、最初と最後の 2 つのプロトコルが双模倣であることを直接示すことが可能となっている。結論が正しいかどうかを直接機械的にチェックできるという点は、形式化の利点の一つである。

(2) 上と同様の手法で、量子鍵配送プロトコル B92 の安全性証明を形式化することにも成功した。量子プロセス計算の枠組みでプロトコルやその等価性を形式化することは、他のプロトコルの安全性について証明手法の適用の可否を議論する場合にも有用である。

(3) プロトコルを量子プロセス計算の中で形式化するには、量子測定に関する問題が付随する。通常の量子計算では、測定で得られた測定値を公開するか秘匿するかを選択することができる。この概念は、プロセス計算における外部に見える遷移と見えない遷移に対応すると考えられるが、双模倣の定義による区別とは合致しないことがある。既存の量子プロセス計算には、物理的な測定行為に対して複数の形式化が存在しており、選択を誤ると、物理学的考察と双模倣との整合性が取れなくない状況が発生してしまう。本研究では、プロトコルの等価性を双模倣として捉えるために、量子測定をどのように形式化するべきかについて考察を行い、その基準を明らかにした。この研究により、今後新たな量子プロトコルが提案されても問題なく形式化することが可能となった。

(4) 量子プロセス計算の双模倣に関する理論的な考察に基づいて、量子プロトコルの等価性判定ツールの開発を行った。ツールの判定は等価性に対して完全ではないが、健全であることが保証されている。このツールを使用して、実際に BB84 と EDP が等価であることを示すことができる。

(5) 量子プロセス計算において、これまで知られていなかった観察等価性を定義した。技術的には、観察等価性の定義にはスケジューラが用いられている。スケジューラの定義を変えることでいくつかの観察等価性を定義することが可能である。本研究の観察等価性は、量子物理学における観測と密接な関係がある。量子物理学においては、状態は観測を通じてしか知ることができず、観測で区別できないものは同一視される。本研究で提案した観察等価性も、量子物理学における観測による区別に準じたものとなっている。このことは、量子プロセス計算が量子物理学におけるモデルとして利用可能なことを示している。ただし、プロセス計算が本質的に非決定性を扱うのに対して、通常の物理学では確率的でない非決定性は考慮しないため、非決定的な計算についてはより深い考察が必要である。

(6) 量子プロセス計算における双模倣と観察等価性の間の関係について考察した。物理学的には等しいとされている 2 つの現象について、プロセス計算で記述した場合、双模倣ではないが観察等価になる例が存在することを示した。これは、観察等価性が総模倣よりも量子物理学に忠実であることを示唆している。更に驚くべきことに、双模倣と観察等価性はお互いに比較不能であることが明らかになった。通常のプロセス計算では、双模倣は観察等価性に包含されることが期待されるが、量子プロセス計算には観測に関して複雑な状況が存在する。この事実は、量子計算と古典計算のある種の本質的な差異を示唆するものである。

(7) 量子計算を形式手法で扱うには、形式化された言語の存在が不可欠である。先行研究の量子 Hoare 論理では、QPL と呼ばれるプログラミング言語が対象となっている。また、量子プロセス計算も形式言語の一種である。本研究では、トポロジカル量子計算のためのプログラミング言語を新しく提案した。トポロジカル量子計算は耐障害性に優れているとされており、実装の面からも注目を集めている量子計算である。トポロジカル量子計算に関する理論的な考察は多いが、プログラミング言語の側面からの研究はまだあまり存在しない。研究は未完成であるが、今後普及する可能性のあるトポロジカル量子計算に対して、プログラミング言語を考察するという試みは重要であると考えられる。

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 3 件）

① K. Yasuda, T. Kubota, Y. Kakutani. Observational Equivalence Using Schedulers for Quantum Processes. Electronic Proceedings in Theoretical Computer Science, vol.172, 191--201, 査読有.
doi:10.4204/EPTCS.172.13

② 本多健太郎, 角谷良彦, 久保田貴大. 猫にはわかる量子プログラミング. コンピュータ・ソフトウェア, vol.31, 9-20, 査読無.
doi:10.11309/jssst.31.4_9

③ Y. Kakutani, D. Kimura. Induction by Coinduction and Control Operators in Call-by-Name. Electronic Proceedings in Theoretical Computer Science, vol.127, 101--112, 査読有.
doi:10.4204/EPTCS.127.7

〔学会発表〕（計 14 件）

① K. Yasuda, T. Kubota, Y. Kakutani. Observational Equivalence Using Schedulers for Quantum Processes. Quantum Physics and Logic, 2014/06/04--2014/06/06, 京都大学 (京都).

② T. Kubota, Y. Kakutani, G. Kato, Y. Kawano, H. Sakurada. Automated Verification of Equivalence on Quantum Cryptographic Protocols. Symbolic Computation in Software Science, 2013/07/05--2013/07/06, Hagenberg (Austria).

③ T. Kubota, Y. Kakutani, G. Kato, Y. Kawano, H. Sakurada. A Tool for Formal Verification of Equivalence on Quantum Cryptographic Protocols. 量子情報技術研究会, 2013/05/27--2013/05/28, 北海道大学 (北海道).

④ T. Kubota, Y. Kakutani, G. Kato, Y. Kawano, H. Sakurada. Automated Proof of Equivalence on Quantum Cryptographic Protocols. プログラミングおよびプログラミング言語, 2013/03/04--2013/03/06, 東山温泉 (福島県).

⑤ T. Kubota, Y. Kakutani, G. Kato, Y. Kawano, H. Sakurada. Application of a Process Calculus to Security Proofs of Quantum Protocols. Foundations of Computer Science in WORLDCOMP, 2012/07/16--2012/07/19, Las Vegas (USA).

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
角谷 良彦 (KAKUTANI, Yoshihiko)
東京大学・大学院情報理工学系研究科・助教
研究者番号：70376614

(2)研究分担者
(　　)

研究者番号：

(3)連携研究者
(　　)

研究者番号：