様式 C-19

科学研究費補助金研究成果報告書

平成２１年６月２２日現在

研究種目： 若手研究（Ｂ）
研究期間：2006～2008
課題番号：18740064
研究課題名（和文） 量子論における不確定性原理の情報理論的表現とその応用

研究課題名（英文） Information theoretical representation and its applications of uncertainty principle in quantum theory

研究代表者
宮寺 隆之（MIYADERA TAKAYUKI）
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：50339123

研究成果の概要：
量子暗号に関する問題に動機付けられ、観測量の非可換性が情報理論にどのような制限を与えるか、についていくつかの視点から調べた。具体的には、①情報撹乱定理の一般化②トレース距離とフィデリティを用いた情報撹乱定理の導出③保存量があるときの測定過程の限界をあらわす Wigner-Araki-Yanase 定理の量的表現の導出④Landau-Pollak 型不確定性関係の一般化⑤同時測定に関する不確定性原理の導出⑥量子コルモゴロフ複雑性を用いた量子暗号の安全性についての新しい定義と解析、を行った。

交付額

（金額単位：円）

	直接経費	間接経費	合 計
2006 年度	700,000	0	700,000
2007 年度	700,000	0	700,000
2008 年度	600,000	180,000	780,000
年度			
年度			
総 計	2,000,000	180,000	2,180,000

研究分野：量子物理
科研費の分科・細目：数学一般（含確率論・統計数学）
キーワード：量子論基礎・量子情報理論・量子測定

１．研究開始当初の背景

1984 年, Bennett と Brassard は物理学の基本法則である量子論を本質的に用いた、現在, BB84 プロトコルと呼ばれる鍵分配方式を提案した. この方式の単純さと, 予言する驚くべき結果は多くの研究者を惹きつけてきたが, その無条件安全性が Mayers によって証明されたのは, やっと 1996 年になってからである. しかしながらこの証明は難しく、その後も Lo-Chau, Shor-Preskill, Biham-Boyer-Boykin-Mor-Roychowdhury などいくつかの別証明が提出されてきた。このうち Biham et al. によるものは、Information-Disturbance 定理を用いている。この（古くは Peres らによって提案された）定理は盗聴者の得る情報量と鍵分配プロトコルの正規ユーザ間の検知する誤りとの関係を表したものであり、盗聴検知の機構を最も直接的に示すものである。またこの定理は、不確定性関係の情報理論的表現の一つとも考えられ、非常に興味深いものである。本研

究課題においては、この定理の一般化及びその応用を目指していた。

２．研究の目的

(1) Boykin-Roychowdhury による Information-Disturbance 定理の検討及び一般化
この定理は 2004 年に Boykin-Roychowdhury によって純粋化及び trace norm の評価により、簡単な証明方法が得られている。しかし、この定理も適用可能な状況は、送信者によって選ばれる基底が mutually unbiased な場合等、特殊な状況設定に限られている。これは、実装におけるエラーを考えた場合には不満足な結果であり、また不確定性関係の情報理論的表現としての観点からも完全なものであるとは言いがたい。実際、量子鍵分配の安全性証明に関しては、この定理を経るのではなく、エンタングルド状態の解析を行う場合には、上記の状況設定はある程度緩めることができることが知られている。そこで、我々はこの定理を、一般の非可換な観測量の組、及び等確率でない状態準備という状況設定の下でも成り立つように一般化を行いうことを目標とした。

(2) BB84 以外のプロトコルについての Information-Disturbance 定理を用いた解析及びプロトコルの提案
量子鍵分配、あるいは鍵分配に限らず量子暗号プロトコルを情報量的に安全なものにするのは、盗聴検知が可能であるためである。すなわち、まさにこの定理（を拡張したもの）が一般に成り立っていることに起因している。そこで、我々は、既存のプロトコルについてこの定理を用いた解析を行い、安全性の評価を行うことを目標とした。この解析によって、盗聴者の得る情報量について、他の方法を用いた解析よりも強力な見積もりが可能であれば、それは許されるエラー率を引き上げられることを意味する。すなわち、BB84 プロトコルのいろいろな形の安全性証明が意義深かったことと同様に、安全性証明の得られていないプロトコルの評価を行うことは言うまでもなく、既に安全であることが知られているプロトコルの別証明を与えることも非常に重要であると考えている。考えていたのは、E91 及び B92 量子鍵分配プロトコルの安全性解析、及び、量子秘密分散プロトコルにおいて adversary が存在していたときの解析、（完全に誤りを訂正するのではない）不完全な量子誤り訂正符号の解析などである。

３．研究の方法

何回かの学会参加を通して情報交換を行い、理論的研究に役立てた。

４．研究成果

我々は、まず雑誌論文⑦において、情報撹乱定理の一般化を行った。この定理は従来の、盗聴者の得る情報と、正規ユーザの検知する誤り確率、に関わるものではなく、盗聴者の得る情報量と正規ユーザの被る誤りの乱雑さとの関係であり、より調和の取れたものである。また、この研究は、学会発表⑦において更に一般の観測量を扱えるように拡張され、エントロピー型不確定性関係との関係も明らかにされた。

このエントロピー型不確定性関係は、Maassen-Uffink により提案された美しいものであるが、その適用範囲には大きな制限がある。すなわち、Krishna-Parthasarathy により一般化された形を用いても、扱えるのは二つの POVM の場合のみである。それに対して、我々は雑誌論文④において、Landau-Pollak 型と呼ばれる min-エントロピーを用いた不確定性関係を、任意の個数の一般の観測量(POVM)が扱えるように拡張することに成功した。この結果は、⑨においてメモリーに制限があるときの量子紛失通信プロトコルの問題にも適用された。

不確定性関係は、二つ以上の観測量を別々に測定するときにあらわれる制限をあらわしているが、Wigner-Araki-Yanase の定理によれば、一つの観測量を測定するときにも、それと非可換な保存量がある場合には制限が生じることがわかっている。我々は、この問題を量子情報の道具を用いて扱い、雑誌論文⑥において量的な表現を得ることに成功した。また、この結果は、元々の Wigner-Araki-Yanase の定理を超え、保存量が加法的でない場合も扱えるように、雑誌論文⑤において拡張された。その後、この定理の導出にあたり鍵となった補題が、実は量子暗号的な状況にも使えることに気づき、新たな形の情報撹乱定理を得て、学会発表⑤において発表した。この情報撹乱定理は、トレースノルムとフィデリティのトレードオフを表しており、それ自体としては意味のつきにくい量どうしではあるが、量子鍵分配など実際のプロトコルを扱う際には、使いやすく有用であることがわかった。

上記において関係していたのは、二つ以上の観測量を個別に測った際の、測定結果に対する制限―不確定性関係―の話であった。一

方、2000 年ごろより再注目されている話題に、ハイゼンベルクの 1927 年の不確定性関係の原論文と、上記の話のギャップがある。すなわち、ハイゼンベルクは粒子の位置と運動量を同時測定することを論じ、例えば運動量の測定が不可避的に位置を乱すことを主張した。位置を「乱す」ことの意味は曖昧ではあるが、これは 1929 年にロバートソンが証明した位置と運動量の個別測定と状況が異なることは明らかである。このギャップを受けて、近年、このハイゼンベルクが元々論じた、同時測定に関わる限界を導くことができないかが、研究されてきた。注目すべき研究としては、小澤・石川・Werner・Busch らによるものがある。我々は、この中で Werner の定式化を用い、その一般化を行うことに成功した。Werner は運動量と位置が、どれだけ同時測定ができるか（できないか）を論じるために、確率分布間の距離を導入し、特に Monge 距離と呼ばれる量に関して、定量的な評価を得た。しかしながら、この結果は、量子調和解析の手法に大きく依存しており、位置と運動量以外の観測量に拡張することは、全く自明ではない。我々は、この定式化において一様距離を採用、CP 写像に対する Cauchy-Schwarz 不等式を用いて、任意の物理量（POVM）に対する限界式を導くことに成功した。また副産物として、同時測定可能な POVM はどの程度、unsharp なものでなければならないか、についての必要条件も得た。これらの結果は、既存の不確定性関係とは大きくことなる領域に関与しており、これからも大きく発展する可能性があると考えている。

本研究の元々の動機は、量子暗号、特に量子鍵分配の問題と関係していた。すなわち、これまでの量子鍵分配の安全性証明は、盗聴者の情報獲得が正規ユーザのデータに生じる誤り確率と関係しており、シャノンの情報理論の意味で情報理論的にこの暗号方式は安全なものである。ところで、シャノンの情報理論で基本になるのは、確率変数である。この理論では、無論、一つ一つのデータに対して情報量を割り当てることは不可能である。一方、1960 年代に Chaitin と Kolmogorov により考え出されたアルゴリズム的情報理論は、個別のデータに情報量という概念を割り当てることができる。ここで、重要となるのは、そのデータを記述するのにどのくらいの長さのプログラムが必要か、というコルモゴロフ複雑性という概念であった。雑誌論文①において、我々は、このアルゴリズム的情報理論をはじめて量子暗号を舞台に展開した。この様な研究は、量子に限らず、暗号理論において初めてのものである。我々の扱いたいものは、量子暗号であるため、まず量子コルモゴロフ複雑性を定義しなければならないが、これについては 2001 年に Vitanyi により定義されている、量子 Turing machine への古典プログラム長という概念を用いた。その結果、BB84 量子鍵分配においては、盗聴者が秘密鍵について小さい量子コルモゴロフ複雑性を得てしまうような確率は指数関数的に小さくなることを示すことに成功した。

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　7　件）

①T. Miyadera, H. Imai
Quantum Kolmogorov Complexity and Quantum Key Distribution, Phys. Rev. A, 79 , 012324 (2009).

②T. Miyadera, H. Imai
Heisenberg's uncertainty principle for simultaneous measurement of positive-operator-valued measures (with H. Imai), Phys. Rev. A, 78 , 052119 (2008).

③S. Iriyama, T. Miyadera, M. Ohya,
Note on a universal quantum Turing machine Phys. Lett. A, 372 , 5120 (2008).

④T. Miyadera, H. Imai
Generalized Landau-Pollak Uncertainty Relation (with H. Imai) Phys. Rev. A, 76, 062108 (2007).

⑤T. Miyadera, H. Imai,
Strength of interaction for information distribution, Phys. Rev. A, 74, 064302 (2006).

⑥T. Miyadera, H. Imai,
Wigner-Araki-Yanase theorem on distinguishability, Phys. Rev. A, 74, 024101 (2006).

⑦T. Miyadera, H. Imai,
Information-Disturbance Theorem for Unbiased Observables, Phys. Rev. A, 73, 042317 (2006).

〔学会発表〕（計　9　件）

①宮寺 隆之
情報と撹乱―不確定性関係のさまざまな形―, 宮寺 隆之, 日本物理学会第６４回年次大会, シンポジウム依頼講演、立教大学、

2009/03/29

② 宮寺 隆之、今井 秀樹
Quantum Key Distribution and Quantum Algorithmic Information, SCIS2009, 大津、2009/01/22

③ T. Miyadera
Uncertainty Principle for Simultaneous Measurement of POVMs, Expository Quantum Lecture Series 2, Putra university、2008/11/27

④ T. Miyadera
Uncertainty relation between arbitrary POVM, GSIS workshop on quantum information theory, 依頼講演, 東北大学、2008/11/06

⑤宮寺 隆之、今井 秀樹,
State collapse in information transfer and its applications, SCIS2008, 宮崎、2008/01/23

⑥宮寺 隆之、今井 秀樹
Landau-Pollak 型不確定性関係の一般化, SITA2007, 三重、2007/11/28

⑦宮寺 隆之、今井 秀樹,
Information-Disturbance Theorem for General Observables, SCIS2007, 長崎、2007/01/23

⑧宮寺 隆之、今井 秀樹
情報分配に必要な相互作用と一般化された Wigner-Araki-Yanase の定理, SITA2006, 函館、2006/12/01

⑨ T. Miyadera, H. Imai
Uncertainty Principle and Oblivious Transfer, ISITA2006, ソウル、2006/11/01

６．研究組織
(1)研究代表者
宮寺 隆之 (MIYADERA TAKAYUKI)
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：50339123

(2)研究分担者
なし

(3)連携研究者
なし