

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：14301

研究種目：若手研究(B)

研究期間：2010～2014

課題番号：22740078

研究課題名(和文)一般確率論・量子論理・圏論など普遍的視点からの量子論へのアプローチ

研究課題名(英文)Foundations of quantum theory from a universal viewpoint

研究代表者

宮寺 隆之(Miyadera, Takayuki)

京都大学・工学(系)研究科(研究院)・准教授

研究者番号：50339123

交付決定額(研究期間全体)：(直接経費) 2,700,000円

研究成果の概要(和文)：量子論の基礎について、既存の手法とは異なるより普遍的な観点から研究を行った。具体的には以下の成果を得た。(1)量子コルモゴロフ複雑性による情報攪乱定理の表現(2)量子論における同時操作不可能性の概念の確立(3)同時操作不可能性の普遍的性質について順序集合を用いた解明(4)一般確率論における状態識別の表現(5)半古典的量子暗号のプロトコルの安全性の検討(6)量子測定過程に関する物理過程の解明

研究成果の概要(英文)：We studied the foundations of quantum theory from a universal point of view. Our findings include the followings: (1) some properties of quantum Kolmogorov complexity were obtained and its applicability to the quantum information was shown (2) the notion of quantum incompatibility was established (3) an order-theoretic structure behind the quantum incompatibility was revealed (4) state-discrimination problem in the convex approach was studied (5) the security of semiclassical quantum cryptography was examined (6) a limitation on the physical interaction in measurement processes was found.

研究分野：量子論基礎

キーワード：量子論基礎 量子測定 量子情報 一般確率論

1. 研究開始当初の背景

量子論の基礎に対する研究者の興味は、量子情報の発展と成熟を受けて大きく高まっていた。当時、量子論に対する一般確率論や量子論理、圏論といった数学からの新しいアプローチが芽生えつつあり、作用素(環)を用いたオーソドックスな量子論の研究とともに、他の数学との相互作用が有効であることが明らかになってきていた。

2. 研究の目的

量子測定を含む量子論の基礎に対して、一般確率論などを含んだ普遍的な(外部からの)新しい観点を持ち込むことによって、量子論の特徴を明らかにし、また量子論が何故我々の世界を記述する「正しい」理論であるのかを考えることが大きな目的であった。

3. 研究の方法

本研究は理論的研究であり、実験や数値計算など、「手による計算」以外のものは用いていない。ゆえに、研究の方向性をともにする共同研究者の存在は非常に重要である。本研究では、その後半にフィンランド・トゥルク大学の研究者である Teiko Heinosaari とスロバキア・科学アカデミーの研究者である Daniel Reitzner という共同研究者を得た。彼らとの議論を行うために、後半は年に1度の約2週間にわたる訪問を行った。また、Heinosaari氏は自分の財源を用い、年に1度ないしは2度の来日をしている。

4. 研究成果

いくつかのテーマに分けることができる。

(1) 量子コルモゴロフ複雑性の研究

情報理論における情報量とは一般に確率分布の不確定さを表すエントロピーで定義される。量子情報理論においても事情は同じで、ある状態の情報量は von Neumann エントロピーで定義され、その操作的な意味付けは古典的なエントロピーを用いてなされる。すなわち、状態の von Neumann エントロピーは、状態にどれだけの古典情報(これはエントロピーで定められる)がエンコードできるかによってあらわされる。

一般に情報理論は、情報源とそこから確率的にアウトプットされるデータを扱う。ところで、上にあげたシャノン(von Neumann)エントロピーに基づく情報量は、アウトプットされる各データにはそもそも定義されず、「データの情報量」と呼べるものではない。むしろ、これは「情報源」の情報量とでも呼ぶべきものであろう。各「データ」の情報量とは何かという問題は、1960年代に既に

考えられており、それがコルモゴロフ複雑性と呼ばれるものである。ここでは、データは0,1の長い列(ビット列)からなるとする。すると、あるデータxのコルモゴロフ複雑性(情報量)は、そのデータを出力するのに必要な最短のプログラム長で定義される。すなわち、 $x=1111111\dots1111111$ は「1を100万回出力せよ」という短いプログラムがあるため、情報量は少ない。逆になんらパターンがない場合には、そのデータそのものをプログラムに書いておくしかなく、情報量は大きいものとなる。前出のシャノンによる情報源の情報量との関係は、Brundageの定理が知られている。これは、(ある条件のもと)コルモゴロフ複雑性の期待値はシャノンエントロピーと一致するというものである。この定理は、コルモゴロフ複雑性が、シャノンエントロピーのマイクロ版としてとらえることができることを示唆している。実際、そのような視点から、Maxwellのデーモンを取り扱ったZurekの先駆的な仕事が、物理における応用として存在していた。

さて、以上は古典データに対するコルモゴロフ複雑性の話だが、量子状態に対するコルモゴロフ複雑性を定義する試みが、2000年ごろに3人の研究者(Gacs, van Dam, Vitanyi)によってなされた。このうちGacsのものは、普遍確率を量子状態に拡張することによって行われ、van Damのものは量子状態を出力する量子コンピュータに対する最短量子プログラム長として定義されている。私が採用したのはVitanyiによるものであるが、彼は量子状態を出力する量子コンピュータに対する最短古典プログラム長として量子コルモゴロフ複雑性を定義している。この3人の定義が与えられたのち、各定義についていくつかの基本的な性質は調べられたものの、それが実際に役立つかどうかは全く分かっていなかった。私は、Vitanyiによる定義が、実際に量子暗号における文脈において使えるものであることを示した。

量子暗号は情報論的暗号と呼ばれる暗号方式の一種であるが、その安全性はシャノンの情報理論を用いて定義されており、各試行におけるデータが実際に安全であるか否かについては議論をすることができなかった。しかし量子コルモゴロフ複雑性を用いれば、各データ(一回の試行における量子状態)の安全性が定式化できるはずである。私は、そのような定式化を行い、また実際その定式化のもとで既存の量子暗号方式が安全性を満たすことを示した。この安全性の肝となる部分は、不確定性関係の一つの表現である情報攪乱定理であるが、この情報攪乱定理についても量子コルモゴロフ複雑性を用いた表現を与えることに成功した。また、有限の量子メモリを持っている場合についても議論を行った。

(2) 量子測定における構造論的研究

量子論における最も基本的な操作は測定である。測定なくしては、いかなる事象も起こりえないし、情報を得ることもできない。このように物理的に重要であるというのみならず、数学的観点からも最も単純な操作であるため、他のより複雑な操作に対する構成要素として登場する。これまでに量子測定については広範な研究がなされてきたが、その代表的な研究としては、どのような物理量の組が同時測定可能か、また同時測定不可能な物理量の組に対してはどのくらい不可能かを定量化するというものがあった(不確定性関係の研究)。そこでは、より精緻な見積もりをすることが鍵となり、よりタイトな不等式を得ることが目標とされてきた。

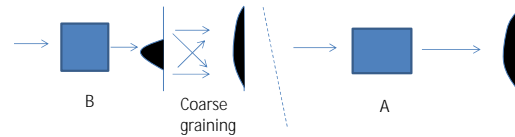
私は、Teiko Heinosaari と Daniel Reitzner とともに、これまでとは視点を変え、量子測定の構造的な側面についての研究を行った。

まず、以下発表論文の [\[1\]](#) において、我々は compatibility (同時操作可能性) という概念を導入し、その分類を行った。上記の同時測定可能という概念は、二つ(以上)の物理量が同じ測定過程の一部として記述できることと解釈できる。この概念を一般化することにより、物理量と量子チャンネルが同時操作可能である (compatible) ことや、オペレーションと量子チャンネルが同時操作可能であることなどが定義された。また、同時操作不可能な操作の場合にも、(インストゥルメントは同一ではないが) 同一の量子チャンネルを与えるようにできる場合に、弱い同時操作不可能性と定義し、そうでない場合に強い同時操作不可能性と定義した。

次に発表論文の [\[2\]](#) において、我々は物理量と量子チャンネルの同時操作可能性に焦点をあてた。物理量の測定は、不可避免的に状態の攪乱を伴うことはよく知られている。(さもなければ、逐次測定を行うことにより全ての物理量は同時測定可能になってしまう。) この同時操作不可能性は、たとえば量子暗号では本質的な役割を果たしている。(盗聴者の測定が状態の攪乱を生み出し、正規ユーザによる盗聴検知が可能となる。) ある物理量 A が与えられたときに、どの程度攪乱が与えられるかということについては、情報攪乱定理と呼ばれ、さまざまな尺度が定義され、それらについて個々に量的な不等式が得られている。我々の目的は、新たな尺度を定義することや量的な不等式を得ることでなく、これらさまざまな情報攪乱定理の背後に潜む構造を明らかにしようというものであった。このために、我々はまず物理量のなす空間と量子チャンネルのなす空間に対して、それぞれ粗視化という観点から順序構造を導入することを行った。

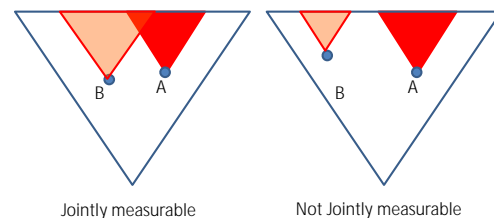
物理量のなす空間

物理量は、量子状態を古典確率分布へと写像するものととらえることができる。二つの物理量 A と B を考える。物理量 A が物理量 B より「情報的に優れている (informative)」とは写像として B にさらに古典チャンネルを適用したものが A と一致することと定義する。(下図参照)



これを $A > B$ と書くと、この二項関係は前順序関係となる。 $A > B$ かつ $B > A$ であるものを同一視すると、商集合は半順序集合となる。

この順序集合の基本的な構造は以下の通りである。最小元が存在するが、最大元は存在しない。最小元は、状態と無関係に一定の確率分布を出力するいわゆる「コイン投げ」に相当する物理量である。最大元は、もし存在すれば全ての物理量が同時測定可能であることになってしまう。実際、下図は物理量のなす空間と、その中での同時測定(不)可能な物理量の組の位置関係を表している。



ここで、左図が A と B が同時測定可能な場合である。すなわち、 A と B の上限が交わりを持てば、またそのときに限り、 A と B は同時測定可能となる。

ちなみに物理量のなす空間に極大元は多数存在している。物理量は Positive-Operator-Valued Measure (POVM=正作用素値測度) で表されるが、極大元はこの POVM の一つ一つの要素(今、離散的な測度のみ考えている)のランクが 1 であるようなものである。

量子チャンネルのなす空間

量子チャンネルのなす空間にも同様に順序構造が入れられる。すなわち、量子チャンネル \mathcal{C} があつたとき、 $\mathcal{C} \geq \mathcal{D}$ がより「攪乱的 (disturbing)」であるとは、 $\mathcal{C} = \mathcal{D} \cdot \mathcal{E}$ (ハイゼンベルク描像) とあらかずような量子チャンネル \mathcal{E} が存在することとして定義する。量子チャンネルのなす空間も、同一視を経ることにより、半順序集合となる。この半順序集合の構造は、物理量のなす空間とは異なり、

最大元と最小元の両方が存在する。最大限最も擾乱的でない量子チャネルは、恒等チャネルの同値類であり、最も擾乱的な量子チャネルは入力状態によらず同じ状態を出力するようなものである。

物理量とチャネルの関係 = 情報攪乱定理

ここで、ある物理量 A が与えられたとき、それと同時に操作可能な量子チャネル全体の集合を $C(A)$ と書くことにする。以下が成り立つ。

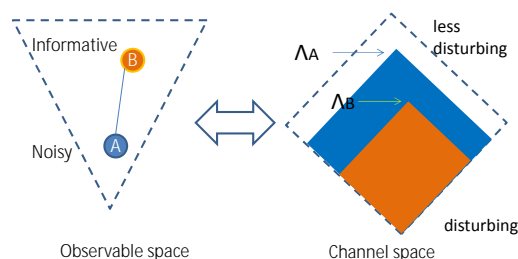
定理： $A > B$ (A が B より informative) であることと、 $C(A) \subset C(B)$ は同値

これは情報攪乱定理の質的 (構造的) 表現ともいえる結果である。また、各 $C(A)$ は以下の構造をもつ。

定理： $C(A)$ は主イデアル。すなわち、最大元をもち、それにより生成される。

この定理は物理量 A と同時に操作可能な量子チャネルのうち、最も擾乱的の少ないものが存在するということを意味している。

これらの関係を図示すると以下のように表される。



普遍的な逐次測定の存在

以下の問題を考える。測定は量子状態を乱してしまう。では、逐次測定できる物理量の組はどのようなものだろうか。これは量子非破壊測定の問題とは異なることに注意する。非破壊測定の場合には、 A の測定後に物理量 B に関する情報を得たい場合に、2 番目に行う測定の物理量を、 B そのものにとるという制約があった。ここで我々が考えている問題では、2 番目に測定する物理量として、一番目の A の測定による擾乱を加味した (変形された) B' の測定を許している。

無論、 A と B は同時測定可能でなければならない。では、 A と B が同時測定可能ならば逐次測定可能だろうか？ 実は、この問に対する答が YES であることはすぐにわかる。さらに我々は発表論文において以下の定理を示した。

定理：上記 $C(A)$ の最大元は、 A と同時測定可能な B について、 B' が存在し B を逐次測定

で実現する。

この定理の驚くべき点は、初めの A の測定が B によらないことである。この性質をもって、我々は $C(A)$ の最大元に相当する測定を用いて行う逐次測定を「普遍的な逐次測定」と呼んだ。

(3) その他

他にも一般確率論を用いた状態識別に関する研究や、量子情報理論に関する研究や、同時測定可能性と同時局在可能性の関係に関する研究などを行った。

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 12 件)

Teiko Heinosaari, Takayuki Miyadera, Universality of sequential quantum measurements, *Physical Review A* 91, 022110 (2015).

<http://dx.doi.org/10.1103/PhysRevA.91.022110>

Teiko Heinosaari, Takayuki Miyadera, Daniel Reitzner, Strongly Incompatible Quantum Devices, *Foundation of Physics* 44, 34 (2014).

[10.1007/s10701-013-9761-1](http://dx.doi.org/10.1007/s10701-013-9761-1)

Teiko Heinosaari, Takayuki Miyadera, Qualitative noise-disturbance relation for quantum measurements, *Physical Review A* 88, 042117 (2013).

<http://dx.doi.org/10.1103/PhysRevA.88.042117>

Takayuki Miyadera, Relation between information and disturbance in quantum key distribution with classical Alice, *International Journal of Quantum Information* 9, 1427 (2011).

[10.1142/S0219749911008118](http://dx.doi.org/10.1142/S0219749911008118)

Takayuki Miyadera, Relation between strength of interaction and accuracy of measurement for a quantum measurement, *Physical Review A* 83, 052119 (2011)

<http://dx.doi.org/10.1103/PhysRevA.83.052119>

Takayuki Miyadera, Quantum Kolmogorov complexity and bounded quantum memory, *Physical Review A* 83, 042316 (2011).

<http://dx.doi.org/10.1103/PhysRevA.83.042316>

Takayuki Miyadera, Uncertainty Relations for Joint Localizability and Joint Measurability in Finite-Dimensional Systems, Journal of Mathematical Physics 52, 072105 (2011).
<http://dx.doi.org/10.1063/1.3614503>

Takayuki Miyadera, Quantum Kolmogorov Complexity and Information-Disturbance Theorem, Entropy 13, 778 (2011).
10.3390/e13040778

Koji Nuida, Gen Kimura, Takayuki Miyadera, Optimal Observables for Minimum-Error State Discrimination in General Probabilistic Theories, Journal of Mathematical Physics 51, 093505 (2010).
<http://dx.doi.org/10.1063/1.3479008>

〔学会発表〕(計 5 件)

宮寺隆之、量子測定における incompatibility、若手のための量子情報セミナー、京都大学基礎物理学研究所、2014年8月8日-10日

Takayuki Miyadera, Qualitative Noise-Disturbance Relation, Quantum Information and Foundation of Quantum Mechanics, Vancouver, 2013年7月2日-7月5日

Takayuki Miyadera, Qualitative Noise-Disturbance Relation for Quantum Measurements, Workshop on Incompatible quantum measurements, Munich, 2013年9月10日-9月12日

Takayuki Miyadera, Steven Phillips, A quantum probability theoretic account of human judgement using Positive-Operator-Valued Measure, The annual meeting of cognitive science society, 札幌, 2012年8月1日-8月4日

宮寺隆之、テイコヘイノサーリ、ダニエルライツナー、量子測定における同時操作不可能性、第27回量子情報技術研究会、慶応義塾大学、2012年11月27日-11月28日

〔図書〕(計 0 件)

〔産業財産権〕

出願状況(計 0 件)

取得状況(計 0 件)

〔その他〕

6. 研究組織
(1) 研究代表者

宮寺 隆之 (Takayuki Miyadera)
京都大学・大学院工学研究科・准教授

研究者番号 : 50339123

(2) 研究分担者

(3) 連携研究者