研究課題別評価書

1. 研究課題名
　　量子通信路の可逆性と情報理論的・幾何学的保存量の評価

2. 氏名
　　小川　朋宏

3. 研究のねらい
　古典的な確率分布族における十分統計量とは，確率分布族に対する知識についての損失がないデータ処理方法のことであり「データ処理の可逆性，情報量の不変性，確率分布族の分解定理」という三つの同等な特徴付けがあった．また古典的情報幾何は，十分統計量に関して不変な性質を反映した確率分布族の幾何構造として一意に特徴付けられていた．本研究では，これらの量子状態族における対応物は何か？という問題意識の元で，量子通信路（量子操作）の可逆性と情報量の不変性に関する研究を行った．
　量子通信路は入力物理系のある量子状態族について，出力量子状態族から元の量子状態族を復元するような逆向きの量子通信路が存在するとき，可逆であるという（図1）．量子通信路の可逆性は，量子誤り訂正や量子秘密分散法といった量子状態を忠実に伝送するプロトコルにおいて，復号可能性条件を特徴付ける概念として重要である．一方，量子通信路は入力物理系のある量子状態族について，入力の変化によらず出力がただ一つの量子状態となるとき，消失的であるという．消失性は，入力の情報が出力で完全に失われていることを意味し，量子暗号や量子秘密分散法といったプロトコルにおいて，セキュリティ条件を特徴付ける概念として重要である．
　これらと同時に，量子相互情報量や Holevo 相互情報量などの不変量を考えると，量子誤り訂正や量子暗号プロトコルの符号化効率評価，安全性評価に結び付く[1]．本研究では，量子通信路の可逆性，消失性に関する漸近理論を構築し，情報理論的保存量との関係を明らかにすることを目指した．

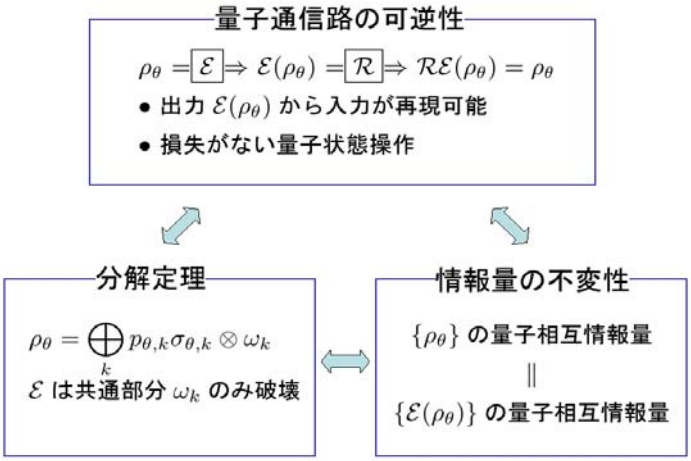

図 1：量子通信路の可逆性

　量子情報幾何は，量子状態族のつながり具合や近さを微分幾何学で表現することにより，量子推定理論における強力な道具と直感を提供する[2]．しかし，現状では推定や検定など問題によって様々な計量・接続が登場し，量子情報幾何は未完成な状況にある．本研究では，量子状態族の遷移可能性についての研究を行うことにより，統計的・操作的に意味のある幾何学的不変量を

抽出し，量子情報幾何の構築に新しい手法を提供することを目指した．

4．研究成果

4－1．量子状態族の統計的同等性（相互遷移可能性）

量子通信路がある入力量子状態族について可逆なとき，入力量子状態族と出力量子状態族は統計的に同等であると言ってよい．なぜなら，一方の量子状態族についてのあらゆる実験結果は，もう一方の量子状態族についての実験結果から再現できるからである．またこのとき，不変量である相対エントロピーや Holevo 相互情報量は，二つの量子状態族で同じ値になる．

一方，任意に与えられた二つの量子状態族について，たとえ相対エントロピーや Holevo 相互情報量といった情報量が同じであったとしても，統計的に同等であるとは結論できない（実際に反例を得た）．それでは，量子状態族の統計的性質を決定付けるような完全不変量や情報量は存在するのであろうか？本研究では統計的同等性に関して以下の成果を得た．

（1）量子 f-ダイバージェンスについての反例 [3,4]

古典的な情報理論において，Csiszar は f-ダイバージェンスと呼ばれる情報量のクラスを導入した．f-ダイバージェンスは α-ダイバージェンスを含む情報量のクラスである．古典的な場合，二つの確率分布から成る確率分布族について，α-ダイバージェンスは完全不変量であることが知られている．このことから f-ダイバージェンスが完全不変量であることが分かる．

一方，Petz は f-ダイバージェンスの量子対応物として，量子 f-ダイバージェンス(quasi-entropy)を導入した．量子 f-ダイバージェンスは量子情報理論の様々な問題において重要な役割を果たす．このことから，量子 f-ダイバージェンスが二つの量子状態から成る量子状態族についての完全不変量かも知れないと期待するのは自然である．しかし，本研究において反例を与え，量子 f-ダイバージェンスが完全不変量とはならないことを示した．

（2）統計的同等性の必要十分条件 [3]

統計的同等性に関して，作用素環論を用いた考察を行い，与えられた量子状態族から作られる Connes コサイクルが生成する von Neumann 代数の同型性に帰着する必要十分条件を与えた．また，二つの量子状態からなる状態族について完全不変量を与えた．

（3）古典的指数分布族の完全不変量 [3,5]

冒頭にも述べたように，古典的な情報幾何において Fisher 計量と α－接続は，十分統計量による不変性から定まる計量と接続という特別な意味を持っていた（[2]を参照）．本研究では，古典的指数分布族において Fisher 計量と α－接続が完全不変量であることを示した．

4－2．量子および古典通信路の漸近的可逆性 [6]

量子通信路の可逆性は，誤りゼロで量子状態を復元できるための条件であった．また，消失性は完全秘匿条件であった．現実的にも理論的にもこれらの条件はきつく，ごく小さな誤りを許したり，漸近的に誤りがゼロになることを要求すれば十分なことが多い．したがって「漸近的可逆性」「漸近的消失性」といった概念を構築し，量子相互情報量をはじめとする不変量との関係を研究する必要がある．

これらの概念は，近年めざましい発展を遂げた量子通信路に関する符号化定理と密接に結び付く．古典－量子通信路符号化定理は，量子通信路を多数回使用して古典的メッセージを漸近的に忠実に伝送する場合の符号化定理であり，通信速度の限界（通信路容量）が Holevo 相互情報量で与えられることを示す定理である．また，量子－量子通信路符号化定理は，量子通信路を多数回使用して量子状態そのものを漸近的に忠実に伝送する場合の符号化定理で，通信路容量が coherent information で表わされることを示す定理である．特に，量子－量子通信路符号化定理は，同一の量子通信路を多数回使用した定常無記憶量子通信路についての符号化定理であるが，相関を持った一般的な通信路に関しては未解決である．また，極限を用いて通信路容量が表わされているが，計算可能な簡明な式で表現できるかどうかは未解決である．本研究では漸近的可逆性について以下の成果を得た．

（1）古典的通信路の漸近的可逆性に関する特徴付け

これまで古典的通信路においても，漸近的可逆性について，情報量の保存や分解定理と結び

つける研究はなされていない．そこで，最初に古典的通信路の漸近的可逆性について考察を行った．

漸近理論においては，入力確率分布族に事前分布を与えたとき，一般的に入力側の相互情報量と出力側の相互情報量がともに発散する．よって，これらの差に注目して，差がゼロに近づくことを相互情報量の漸近的不変性とした．漸近的に誤り（量子状態の距離や情報量の差）が指数的にゼロに近づくという条件のもとで「（a）相互情報量の漸近的不変性，（b）確率分布族の漸近的分解定理，（c）通信路の漸近的可逆性」が同等であることを証明した．また，漸近的に誤りが指数的にゼロに近づくという条件をはずすと，一般的に（a）⇒（b）⇒（c）が成り立つことを示した．

量子通信路の漸近的可逆性についても上記の同等性が成立すると予想されるが，現状では未解決である．

（2）古典的相互情報量および Holevo 相互情報量の漸近的不変性

量子通信プロトコルの解析へ向けての応用例として，古典-量子通信路符号化定理を想定した解析を行った．古典-量子通信路符号化定理を本研究の文脈で述べると以下の通りである．任意に与えられた量子通信路の列に対して，通信路容量の指数的増大度の数の入力量子状態族をうまく選ぶことで，与えられた量子通信路の列が，この量子状態族について漸近的に可逆になる．

本研究ではランダムコーディングの手法を用いて，与えられた量子通信路の列に対して，通信路容量の指数的増大度の数の入力量子状態族が存在して，Holevo 相互情報量が漸近的に不変になることを証明した．

特別な場合として，古典的通信路と古典的相互情報量の漸近的不変性を含むため，古典的な場合の上記（a）を示したことになる．これは（1）より（c）と同等であったから，Shannon の通信路符号化定理の新しい証明方法を与えたことになる．また，（1）が量子通信路の場合に証明されれば，古典-量子通信路符号化定理の新しい証明方法になる．

4－3．量子仮説検定と量子通信路符号化

量子仮説検定（単純量子仮説検定）は，二つの量子状態の候補から，測定によりどちらが真の状態であるかを統計的に識別する問題である．量子仮説検定は，単純な問題であるがゆえに，量子情報理論における非可換性による困難をシンプル形で浮き彫りにする．また，量子情報理論の多くの問題は，量子仮説検定における極限定理に帰着される．

量子仮説検定では，古典的な仮説検定と同様，第一種誤り確率と第二種誤り確率のトレードオフが論じられる．これらを同時に小さくすることはできないため，以下の問題設定がなされる．

（a）第一種誤り確率を定数以下におさえたとき，第二種誤り確率の最適値が指数的に減少するときのスピード（指数）を求める問題（Stein 型）．

（b）第一種誤り確率が指数的に減少するときのスピード（指数）を与えたときに，第二種誤り確率の最適値が指数的に減少するときのスピード（指数）を求める問題（Hoeffding 型）．

（c）事前確率を与えたときに，平均誤り確率の最適値が指数的に減少するときのスピード（指数）を求める問題（Chernoff 型）．

量子仮説検定の最初の極限定理は，問題（a）の解答を与えた定理「量子 Stein の補題」[7,8]である．この定理は，第二種誤り確率の最適値が指数的に減少するときのスピードが量子相対エントロピーにちょうど等しいことを示し，量子情報理論において，古典論の「大数の法則」に代わる極限定理の役割を果たす．実際に本研究では以下を示した．

（1）量子仮説検定と量子通信路符号化 [9]

古典－量子通信路符号化定理の証明において，受信量子状態からメッセージを識別するために，単純量子仮説検定を重ね合わせることで復号器を構成した．さらに「量子 Stein の補題」を大数の法則と同様に適用することで，復号器の誤り確率が漸近的にゼロになることを証明した．

一方，（b）は未解決問題[10]であったが，Chernoff 型の問題（c）への解答が[11,12]によってもたらされたことを契機に，このブレイクスルーに基づいて，Hoeffding 型の問題（b）もただちに解決され[13,14]「量子 Hoeffding の定理」が完成した．本研究では作用素環論を用いて研究を行い，以下の成果を得た．

（2）相関を有する量子状態の識別 [15-17]

量子スピンチェイン上の相関を有する量子状態の仮説検定問題について，Chernoff 型[15]および Hoeffding 型[16]の問題に解答を与えた（図2）．また，フェルミオン(CAR algebra)上の量子状態(quasi-free state)についても同様の結果を与えた[17].

（3）量子スピンチェイン上の Gartner-Ellis 型大偏差原理 [15]

量子スピンチェイン上のオブザーバブルに対する Gartner-Ellis 型の大偏差原理について調べた．大偏差原理を満たすために量子状態が満足すべき十分条件を与え，状態が finitely correlated state または Gibbs state の場合に，この条件が満たされることを示した.

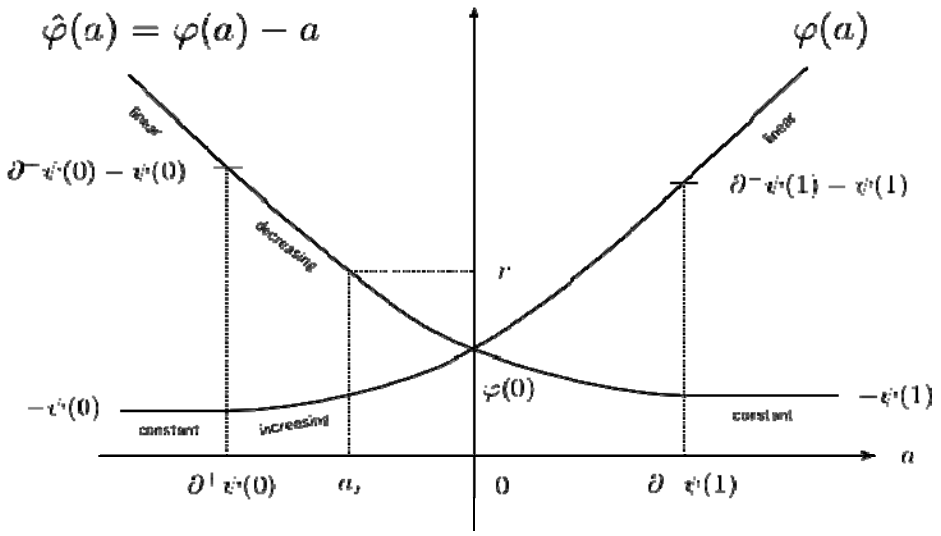

図2：量子仮説検定における誤り確率のトレードオフ曲線

4－4．量子誤り訂正条件と作用素環論 [18]

量子誤り訂正符号の非漸近的な場合の復号可能性条件について，作用素環論的特徴付けを与えた．作用素環論的に量子誤り訂正を眺めると，受信者側のオブザーバブルが成す von Neumann 代数の部分代数で，量子通信路によるデコヒーレンスの影響を本質的に受けない部分代数（multiplicative domain）が重要になることが分かった．本研究では，multiplicative domain が量子通信路のシュレーディンガー描像を介して，送信者側の符号部分空間 K 上の作用素代数 L(K) と同型な場合，そしてその時のみ，入力量子状態族は復号可能であることを証明した.

また，環境系（または盗聴者）のオブザーバブル全体が成す代数が，量子通信路のシュレーディンガー描像で，送信側では自明な代数（単位元の定数倍）になることと，上記の誤り訂正条件が同値であることを示した.

さらに可換子の議論を用いることで，「量子誤り訂正可能なこと」と「盗聴者に何も情報を伝えないこと」が等価であることを作用素環論的に証明した．作用素環論を用いるメリットは，上記の事実がほぼ自明になることである.

参考文献

[1] T. Ogawa et al., Physical Review A, 032318, 2005.
[2] S. Amari, H. Nagaoka, Methods of Information Geometry, AMS & Oxford University Press, New York, 2000.
[3] T. Ogawa and H. Nagaoka, Information and Communication, Budapest, Hungary, August, 2008.
[4] T. Ogawa and H. Nagaoka, University of Electro-Communicatios, UEC-IS-2005-5, 2005.
[5] H. Nagaoka and T. Ogawa, University of Electro-Communicatios, UEC-IS-2005-4, 2005.
[6] 小川朋宏，第 31 回情報理論とその応用シンポジウム（SITA2008), pp. 445-449, 2008.

[7] F. Hiai and D. Petz, Commun. Math. Phys., vol. 143, pp. 99-114, 1991.
[8] T. Ogawa and H. Nagaoka, IEEE Trans. Inform. Theory, vol. 46, pp. 2428-2433, 2000.
[9] T. Ogawa and H. Nagaoka, IEEE Trans. Inform. Theory, vol. 53, pp. 2261-2266 2007.
[10] T. Ogawa and M. Hayashi, IEEE Trans. Infrom. Theory, vol. 50, pp. 1368-1372, 2004.
[11] M. Nussbaum and A. Szkola, arXiv:quant-ph/0607216, 2006, to appear, Ann. Statist.
[12] K. M. R. Audenaert et al., Phys. Rev. Lett., vol. 98, p. 160501, 2007.
[13] M. Hayashi, Phys. Rev. A, vol. 76, p. 062301, 2007.
[14] H. Nagaoka, arXiv:quant-ph/0611289, 2006.
[15] F. Hiai, M. Mosonyi and T. Ogawa, J. Math. Phys., vol. 48, 123301, 2007.
[16] F. Hiai, M. Mosonyi and T. Ogawa, J. Math. Phys., vol. 49, 032112, 2008.
[17] M. Mosonyi, F. Hiai, T. Ogawa and M. Fannes, J. Math. Phys., vol. 49, 072104, 2008.
[18] 小川朋宏, 数理解析研究所講究録 1534, pp. 108-118, 2007.

5. 自己評価

本研究では量子情報理論，量子情報幾何をバックグラウンドとして，作用素環論を導入することで，量子通信路の漸近的可逆性や量子状態族の統計的同等性についての研究を行った．その際の研究指針は情報理論的・幾何学的不変量との関連であった．

量子仮説検定をはじめとして，量子状態族の統計的同等性，量子誤り訂正条件の作用素環論的特徴付けなど，これまでに述べた一定の成果を得ることができた．通信路の漸近的可逆性に関しては，相互情報量が漸近的に保存されることを示すことで通信路符号化定理を証明するという，古典情報理論においても新しい手法を導入することができた．

三年前に大きな野望を抱いて研究構想を描いたが，はるか手前で時間切れとなってしまったように思う．特に，本研究の応用として当初計画していた，量子暗号の安全性証明や量子誤り訂正符号の具体的設計については未完成である．しかし，さきがけ研究で試行錯誤する中で，当初の研究構想の多くが，それほど間違えてはいないとの手応えを得た．また，さきがけ研究の特徴を生かして，作用素環論の知識を習得することができ，この分野の研究者とディスカッションができるようになった．

6. 研究総括の見解

作用素環論を基礎に、量子仮説検定、量子状態族の統計的同等性、量子誤り訂正条件などに、精密な理論的成果を得ています。その中で古典情報理論における新しい証明の手法を開発することができたという重要な副産物もありました。それは通信路の漸近的可逆性に関しては、相互情報量が漸近的に保存されることを示して、通信路符号化定理を証明するというものです。小川さんの理解の深さと説明の丁寧さは他の研究者にも大変良い影響を与えました。若い世代の育成という面でも将来に期待できます。さきがけ研究が世に送り出した人材として誇ることができます。

7. 主な論文等

【A さきがけの個人研究者が主導で得られた成果】

①論文

1. Tomohiro Ogawa, and Hiroshi Nagaoka, Making Good Codes for Classical-Quantum Channel Coding via Quantum Hypothesis Testing, IEEE Trans. Inform. Theory, vol. 53, no. 6, pp. 2261-2266, 2007.
2. Fumio Hiai, Milan Mosonyi, and Tomohiro Ogawa, Large Deviations and Chernoff Bound for Certain Correlated States on the Spin Chain, J. Math. Phys., vol. 48, 123301, 2007.
3. Fumio Hiai, Milan Mosonyi, and Tomohiro Ogawa, Error Exponents in Hypothesis Testing for Correlated States on a Spin Chain, J. Math. Phys., vol. 49, 032112, 2008

②特許出願

なし

③受賞

なし

④著書

1. 小川朋宏, 数理科学事典(第2版):VIII, 1.9. 量子情報理論, 2009 年出版予定(丸善)

⑤学会発表

1. Tomohiro Ogawa, On Reversibility of Quantum Operations and Quantum Mutual Informations, 9th Workshop on Quantum Information Processing (QIP2006), Paris, France, January, 2006.
2. Tomohiro Ogawa, On Reversibility of Quantum Operations and Quantum Secret Sharing Schemes, 37th Symposium on Mathematical Physics ″Quantum Entanglement & Geometry, Torun, Poland, June, 2006.
3. 小川朋宏, 量子通信路の漸近的可逆性, 数理解析研究所講究録 1534, pp. 108-118, 2007.
4. Tomohiro Ogawa and Hiroshi Nagaoka, On Statistical Equivalence for Sets of Quantum States, Information and Communication, Budapest, Hungary, August, 2008.
5. 小川朋宏, 通信路の漸近十分性と通信路符号化定理, 第 31 回情報理論とその応用シンポジウム (SITA2008), pp. 445-449, 2008.

⑥招待講演

1. 小川朋宏, 量子仮説検定と量子通信路の可逆性－量子相対エントロピーの役割－, 電子情報通信学会ソサイエティ大会, 明治大学, 2008.

【B その他の主な成果】

①論文

1. Milan Mosonyi, Fumio Hiai, Tomohiro Ogawa, and Mark Fannes, Asymptotic Distinguishability Measures for Shift-Invariant Quasifree States of Fermionic Lattice Systems, J. Math. Phys., vol. 49, 072104, 2008.

②特許出願

なし

③受賞

なし

④著書

なし

⑤学会発表

なし

⑥招待講演

なし