# 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
# Study of the reversibility of quantum operations and the preservation of information-theoretical and geometrical quantities

小川朋宏
Tomohiro Ogawa
電気通信大学大学院情報システム学研究科
University of Electro-Communications

**概要：** 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．

## 【研究のねらい】

### 1. 情報理論的保存量の評価

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．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「可逆性」と対になる概念として「消失性」がある．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 相互情報量などの量子操作における不変量を考えると，量子誤り訂正や量子暗号プロトコルの符号化効率評価，安全性評価に結び着く．また，量子相互情報量についての恒等式から，可逆性と消失性に関する二者間トレードオフの解析が可能である．このトレードオフは，未知の量子状態のコピーが不可能であることを示す no-cloning 定理，未知の量子状態の消去が不可能であることを示す no-deleting 定理の自然な現れであると考えられ，量子系特有の現象である．

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．

### 2. 幾何学的保存量の評価

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[1]．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．

**【研究方法】** 量子相対エントロピーの単調性における等号成立条件[2,3]は，量子通信路による量子相対エントロピーの保存条件と，二つの量子状態から成る量子状態族に関する可逆性が同等であることを示しており重要である．また，古典的な確率分布族の分解定理に対応して，量子状態族の分解定理[4-6]が見出されていた．

筆者ら[7]は，本研究の採択に先立ち，量子秘密分散法に関して量子通信路の可逆性，消失性の観点から研究を行い，一般の量子状態族について，量子通信路の可逆性と Holevo 相互情報量の不変性が等価であることを示した．またセキュリティ条件を量子通信路の消失性としてとらえ，消失性が Holevo 相互情報量の完全損失条件と等価であることを示した．

量子秘密分散法とは量子暗号方式の一つであり，任意に与えられた量子状態を，いくつかの物理系（シェア）にエンタングルした量子状態として分散符号化することで，ある特定のシェアの組を集めると元の量子状態を復元できるが，それ以外のシェアの組では元の量子状態に関して何の情報も得られない，ということを実現する方式である．

量子通信路の可逆性，消失性に関する漸近理論構築のためには，量子相対エントロピーの単調性における等号成立条件を漸近的な場合に拡張する必要があるだろう．この単調性の等号成立条件[2,3]や，量子状態族の分解定理についての最新の証明方法[6]では, Connes コサイクルをはじめとする作用素環論の知識がふんだんに用いられている．そこで本研究の初期の段階では，研究と平行して作用素環論の知識習得にあたった．

**【研究成果】**

**1. 量子状態族の統計的同等性**

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-ダイバージェンスの反例[8,9]**

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 $\alpha$-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，$\alpha$-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[8]**

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の完全不変量を与えた．

**(3) 古典的指数分布族の完全不変量[8,10]**

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 $\alpha$–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([1]を参照)．本研究では，古典的指数分布族において Fisher 計量と $\alpha$–接続が完全不変量であることを示した．

## 2. 量子および古典通信路の漸近的可逆性

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．現実的には（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．

正確に述べると，量子通信路の漸近的可逆性とは,「量子通信路の列」と入力系の「量子状態族の列」に関する概念である．「量子通信路の列」は入力系の「量子状態族の列」について，出力量子状態から入力量子状態を漸近的に復元するような「逆向きの量子通信路の列」が存在するとき，漸近的に可逆であるという．例えば量子通信路の列として，ある量子通信路を n 回用いる定常無記憶通信路があげられる．本研究では漸近的可逆性を議論するにあたって，定常性やエルゴード性といった仮定を一切設けない「情報スペクトル的方法」[11]を用いた．

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[12,13]**

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．

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（保存）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[12,13]**

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．

## 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」[14,15]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[16]**

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[17]であったが，Chernoff 型の問題(c)への解答が[18,19]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[20,21]「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[22-24]**

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[22]および Hoeffding 型[23]の問題に解答を与えた．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[24].

**(3) 量子スピンチェイン上の Gartner-Ellis 型大偏差原理[22]**

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.

**4. 量子誤り訂正条件と作用素環論[25]**

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．

**【今後の展開】** 古典的通信路の漸近的可逆性については，ある意味予想通りの特徴付けが得られた．今後は情報理論の様々な符号化問題への応用が考えられる．一方，量子通信路の漸近的可逆性については，情報量が漸近的に保存されることを証明できたが，今後は漸近的可逆性との同等性を証明する必要がある．これができれば，量子情報理論の様々な符号化問題への応用の道が開けると考える．

量子状態族の統計的同等性と似た概念として，量子状態族の遷移可能性がある．これは任意に与えられた二つの量子状態族を一方から他方へ遷移させる量子通信路が存在するかどうかを判定する問題である．

そもそも古典的確率分布族の遷移可能性条件についてさえ，具体的な条件はあまり知られていない．今後は，古典的な場合を含めて量子状態族の遷移可能性について考察したい．目標は情報理論的・幾何学的不変量との関連を導くことであるが，遷移可能性を判定するアルゴリズムを開発することも有用であろう．これについては，エンタングルメントの理論への応用も考えられる．

**【結言】** 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づけなど，これまでに述べた一定の成果を得ることができた．

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たように思う．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．将来「あの人はさきがけで伸びた」と言われるように，さきがけ研究で得られた多くの知見を今後の研究に生かしていきたい．

**【謝辞】** 本研究の一部は Milan Mosonyi 博士，日合文雄教授，Mark Fannes 教授，長岡浩司教授との共同研究です．また本研究は当初，東京大学大学院数理科学研究科で行われました．メンバーとして受け入れて頂き，セミナーで討論をして頂きました，河東泰之教授と作用素環グループの皆様に深く感謝いたします．

本研究の機会を与えて下さり，多くのご支援を頂いた科学技術振興機構，「量子と情報」領域総括の細谷先生，同領域アドバイザーの皆様，ならびに同領域事務所の皆様に深く感謝いたします．

**参考文献**

[1] S. Amari, H. Nagaoka, Methods of Information Geometry, AMS & Oxford University Press, New York, 2000.

[2] D. Petz, Quart. J. Math. Oxford,vol. 39, pp. 907–1008, 1988.
[3] M. Ohya and D. Petz, Quantum Entropy and Its Use, Berlin, Springer, 1993.
[4] M. Koashi and N. Imoto, Phys. Rev. A, vol. 66, no. 2, 022318, 2002.
[5] M. Mosonyi and D. Petz, Lett. Math. Phys., vol. 68, pp. 19–30, 2004.
[6] A. Jencova and D. Petz, Commun. Math. Phys., vol. 263, pp. 259–276, 2006.
[7] T. Ogawa, A. Sasaki, M. Iwamoto and H. Yamamoto, Physical Review A, 032318, 2005.
[8] T. Ogawa and H. Nagaoka, Information and Communication, Budapest, Hungary, August, 2008.
[9] T. Ogawa and H. Nagaoka, University of Electro-Communicatios, UEC-IS-2005-5, 2005.
[10] H. Nagaoka and T. Ogawa, University of Electro-Communicatios, UEC-IS-2005-4, 2005.
[11] T. S. Han, Information Spectrum Methods in Information Theory, Springer, Berlin, 2003.
[12] T. Ogawa, Sendai-Workshop 2008, Sendai, Japan, September, 2008.
[13] 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.
[14] F. Hiai and D. Petz, Commun. Math. Phys., vol. 143, pp. 99–114, 1991.
[15] T. Ogawa and H. Nagaoka, IEEE Trans. Inform. Theory, vol. 46, pp. 2428–2433, 2000.
[16] T. Ogawa and H. Nagaoka, IEEE Trans. Inform. Theory, vol. 53, pp. 2261–2266 2007.
[17] T. Ogawa and M. Hayashi, IEEE Trans. Infrom. Theory, vol. 50, pp. 1368–1372, 2004.
[18] M. Nussbaum and A. Szkola, arXiv:quant-ph/0607216, 2006.
[19] K. M. R. Audenaert et al., Phys. Rev. Lett., vol. 98, p. 160501, 2007.
[20] M. Hayashi, Phys. Rev. A, vol. 76, p. 062301, 2007.
[21] H. Nagaoka, arXiv:quant-ph/0611289, 2006.
[22] F. Hiai, M. Mosonyi and T. Ogawa, J. Math. Phys., vol. 48, 123301, 2007.
[23] F. Hiai, M. Mosonyi and T. Ogawa, J. Math. Phys., vol. 49, 032112, 2008.
[24] M. Mosonyi, F. Hiai, T. Ogawa and M. Fannes, J. Math. Phys., vol. 49, 072104, 2008.
[25] 小川朋宏, 数理解析研究所講究録 1534, pp. 108–118, 2007.