様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年　６月１４日現在

機関番号：１２６１２
研究種目：若手研究（Ｂ）
研究期間：２００９～２０１２
課題番号：２１７４００６６
研究課題名（和文）　量子力学系における通信路の可逆性と情報幾何

研究課題名（英文）　Reversibility of Channels and Information Geometry in Quantum Mechanical Systems

研究代表者
小川　朋宏（OGAWA TOMOHIRO）
電気通信大学・大学院情報システム学研究科・准教授
研究者番号：００３２３５２７

研究成果の概要（和文）：量子通信路における通信路分解能(resolvability)について，定常無記憶性などの制限を一切仮定しない一般的な設定で，情報スペクトルに基づく一般公式を与えた．この結果を古典−量子盗聴通信路符号化，量子−量子通信路符号化に適用し，情報スペクトルに基づく一般的な設定で符号化定理を与えた．また，古典および古典−量子通信路において，定常無記憶通信路を含むクラスで通信路が未知の場合でも適用可能な通信路分解能符号化定理を証明することで，ユニバーサルな盗聴通信路符号化定理を与えた．

研究成果の概要（英文）：Concerning channel resolvability for quantum channels, a general formula based on the information spectrum method was proved in a general setting without any assumption such as stationary memoryless channels. The formula can be applied to show general formulas for quantum wiretap channel coding and quantum channel coding for sending quantum states. Also, showing universal channel resolvability coding theorem, which can be available for unknown channels, for a class including stationary memoryless channels, an universal wiretap channel coding theorem for classical and classical-quantum channels was given.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,000,000	300,000	1,300,000
2010 年度	700,000	210,000	910,000
2011 年度	700,000	210,000	910,000
2012 年度	700,000	210,000	910,000
総　計	3,100,000	930,000	4,030,000

研究分野：数物系科学
科研費の分科・細目：数学，数学一般（含確率論・統計数学）
キーワード：量子情報理論，情報スペクトル，通信路分解能，通信路符号化，盗聴通信路符号化，相互情報量，十分統計量

１．研究開始当初の背景

（１）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．一方，量子仮説検定の理論は近年飛躍的に発展したにもかかわらず，量子仮説検定についての情報幾何は得られていない．現状では推定・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

何の全体像は未完成である．

（２）量子通信路符号化定理など，量子情報理論における様々な符号化定理が，定常無記憶およびそれに近い状況において，めざましい発展を遂げた．また，量子仮説検定，古典−量子通信路符号化においては，情報スペクトル的方法に基づき，定常無記憶性などの仮定を一切置かない状況での符号化定理が導かれていた．一方で，量子通信路分解能符号化，古典−量子盗聴通信路符号化，量子−量子通信路符号化において情報スペクトル的方法は確立していなかった．

２．研究の目的

（１）古典的な十分統計量とは，確率分布族に対する知識の損失がないデータ処理方法のことで「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特徴付けられていた．本研究では，これらの量子系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い，操作的観点から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す．

（２）本研究では量子通信路の「漸近的可逆性」の概念を構築し，Holevo 相互情報量をはじめとする不変量の漸近的保存条件との同等性を示す．これによって，近年めざましい発展を遂げた各種の量子通信路符号化定理（メッセージ伝送／量子状態伝送／エンタングルメント補助）の統一的理論の構築を目指す．

（３）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操作が存在するかどうかを判定する問題（遷移可能性）について扱う．古典的な確率分布族について Blackwell, Sherman, Stein (BSS)の判定条件が知られているが，実際に確かめるのは困難である．古典的な場合も含めて，量子系における具体的な情報量による判定基準や，具体的な量子操作の構成方法を研究し，量子状態族の遷移可能性を判定する数値（または代数）計算アルゴリズムを開発する．

３．研究の方法

（１）通信路分解能符号化(channel resolvability coding)は，古典系・量子系の双方で，盗聴通信路符号化における盗聴者の通信路出力を統計的に制御する方法として用いられる．また，古典−量子盗聴通信路符号化定理から量子通信路符号化定理（量子状態伝送）が導かれることが知られている．このように，通信路分解能符号化は量子情報理論において鍵となる基本的な問題であるため，通信路分解能符号化定理を，より一般的な状況で構築することを目指した．また，盗聴通信路符号化は通信路符号化と通信路分解能符号化を組み合わせることで得られるが，正規通信路と盗聴通信路の特性をあらかじめ知っている必要がある．そこで，最初に古典系において通信路が未知の場合でも適用可能な通信路分解能符号化定理を証明した．

（２）量子状態族の遷移可能性において，古典的な確率分布族について BSS の判定条件が知られており，近年，量子系における対応物も知られるようになった．これは，量子通信路の入力状態のベイズ確率を様々に変化させて，出力側の測定を様々に変化させた場合の，ベイズ・コストの大小による判定条件である．しかし，一般的な通信路でこれを実際に確かめるのは古典通信路でさえ困難であるため，本研究では最初に古典通信路における判定アルゴリズムを検討した．数学的には通信路の条件を満足させながら線形方程式の解を見つける問題であり，当初は一般化逆行列を利用する方法を検討したが，数値的な安定性やアルゴリズムの容易さから，最急降下法が有効であることが分かった．そこで，量子通信路においても最急降下法を用いることにした．

４．研究成果

（１）通信路分解能符号化とは，通信路の入力アンサンブルと乱数を適切に用いることで漸近的に通信路の出力分布を所望の分布に近似する方法である．通信路分解能符号化における必要な乱数レートの下限は通信路分解能(channel resolvability)と呼ばれる．通信路分解能は通信路容量と双対的な役割を果たす重要な概念であり，近年，盗聴通信

路符号化への応用が研究されている．これまで量子通信路においては，同一の通信路を多数回使用する定常無記憶通信路およびそれに近い状況で符号化定理が与えられており，通信路分解能が Holevo 量子相互情報量に等しいことが知られていた．本研究では量子通信路における通信路分解能について，定常無記憶性などの制限を一切仮定しない一般的な設定で情報スペクトルに基づく符号化定理を与えた．この結果を古典-量子盗聴通信路符号化，量子-量子通信路符号化に適用し，情報スペクトルに基づく一般的な設定で符号化定理を与えた．

（2）盗聴通信路符号化は，二者間通信で盗聴者が介在したときに，正規通信路と盗聴通信路のノイズ差を利用することで，メッセージを安全に正規の受信者に送信する暗号通信方式である．盗聴通信路符号化は通信路符号化と通信路分解能符号化を組み合わせることで得られるが，正規通信路と盗聴通信路の特性をあらかじめ知っている必要がある．本研究では古典および古典-量子通信路において，通信路が未知の場合でも適用可能な通信路分解能符号化定理を証明した．この結果を古典および古典-量子通信路における盗聴通信路符号化に適用し，ユニバーサルな盗聴通信路符号化定理を与えた．

（3）量子通信路のノイズに関する順序について研究を行い，一方の通信路が他方の通信路にさらにノイズを付加したものとなる関係(degraded order)を効率的に判定するアルゴリズムを示した．この判定アルゴリズムは Choi 表現を用いたコスト関数を最急降下法により最小化することで実現される．さらに，この順序判定アルゴリズムを用いて量子通信路の順序と量子相互情報量の関係について数値的検証を行った．

（4）逆シャノン定理は通信路が任意に与えられたとき，通信路容量を越える符号化レート持つ適切な符号と恒等通信路を用いる事により，その通信路を再現可能なことを示したものである．一方，実用的な符号を用いてこの定理を実現できるかは明らかではない．そこで，本研究では BCH 符号を用いて逆シャノン定理を実現するアルゴリズムを開発し，符号化レートと通信路の再現成功確率について検証した．図１に符号化レートと二元対称通信路の再現成功確率を示す．ただし，n=32ー2048 は BCH 符号の符号長である．結果として，実用的な符号長で逆シャノン定理の内容が実現可能なことが示された．

（5）量子秘密分散法における一般化アクセス構造の構成アルゴリズムを量子相互情報量の二者間トレードオフに基づいて構成し，計算機実験により単純なしきい値法ではないアクセス構造を構成した．

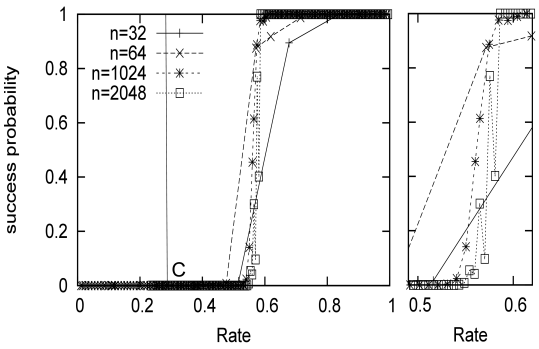

図１：符号化レートと通信路の再現成功確率

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）

〔学会発表〕（計８件）

① 岡澤太志，鈴木淳，小川朋宏，量子通信路のノイズに関する順序と情報量に関する研究，IT・ISEC・WBS 合同研究会，2013 年 03 月 07 日，関西学院大学(大阪)
② 長井大地，小川朋宏，逆シャノン定理による通信路の再現に関する研究，IT・ISEC・WBS 合同研究会，2013 年 03 月 07 日，関西学院大学（大阪）
③ Tomohiro Ogawa, Universal Resolvability and Wiretap Channel Coding for Classical-Quantum Channels, 35th Symposium on Information Theory and its Applications (SITA2012), 2012 年 12 月 13 日,別府湾ロイヤルホテル(大分県)
④ Tomohiro Ogawa, On general formulas for c-q channel resolvability, private capacity, and q-q capacity, 量子情報技術研究会（QIT27), 2012 年 11 月 27 日，慶応義塾大学
⑤ Tomohiro Ogawa, On general formulas for c-q channel resolvability, private capacity, and q-q capacity, 量子情報技術研究会（QIT27), 2012 年 11 月 27 日，慶応義塾大学
⑥ 小松知紀，小川朋宏，量子秘密分散法における一般アクセス構造に関する研究，量子情報科学ウィンタースクール 2011 ポスター発表，2011 年 2 月 24 日，東北大学川渡共同セミナーセンター(宮城県)
⑦ 小川朋宏，量子誤り訂正における作用素

代数的方法，量子情報技術研究会(QIT22)，2010年5月10日，大阪大学吹田キャンパス

⑧ 小川朋宏，量子誤り訂正符号の基礎と量子秘密分散，第13回情報論的学習理論ワークショップ(IBIS 2010)，2010年11月6日，東京大学生産技術研究所

６．研究組織

(1)研究代表者

小川　朋宏（OGAWA TOMOHIRO）
電気通信大学・大学院情報システム学研究科・准教授
研究者番号：00323527