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１８日現在

研究種目：基盤研究（B）
研究期間：2006～2008
課題番号：１８３６０１８６
研究課題名（和文）　量子ガウス通信路に対する量子符号化変調方式に関する研究

研究課題名（英文）　Quantum Coded Modulation for Quantum Gaussian Channel

研究代表者
臼田　毅（USUDA TSUYOSHI）
愛知県立大学・情報科学部・准教授
研究者番号：８０２７３３０８

研究成果の概要：21 世紀の情報通信技術の発展は，あらゆる情報通信の場面でディジタル化，特に，マルチレベル化がなされたことによるところが大きい．地上波デジタル放送，新世代携帯電話などはその代表である．本研究は，長く未来の情報通信技術と言われてきた量子情報通信を実現させ，その究極の予言を具現化することを目指し，量子通信において，アナログ（連続）からディジタル，さらにマルチレベルとした場合の情報伝送の限界，具体的な符号化や変調方式について明らかにした．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００６年度	3,700,000	1,110,000	4,810,000
２００７年度	2,300,000	690,000	2,990,000
２００８年度	2,500,000	750,000	3,250,000
年度			
年度			
総　計	8,500,000	2,550,000	11,050,000

研究分野：工学
科研費の分科・細目：電気電子工学・通信・ネットワーク工学
キーワード：情報通信工学，量子情報理論，量子ガウス通信路，符号化変調，通信路容量，量子通信

１．研究開始当初の背景

(1) 世界の動向

本研究課題の申請の前年（2004 年），量子減衰通信路の容量が，MIT グループによって明らかにされた（Classical capacity of the lossy bosonic channel: the exact solution, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, Physical Review Letters, vol.92, 027902, 2004）．次の課題は，この量子通信路容量に近づくためには，どのような変調を用い，どのような符号化および復号化を行えばよいのかを考察することであると考えられたが，それまで量子通信における符号化を考察してきたグループは，ごく少数であった．また，名古屋大学のグループが，古典の符号化変調を量子通信に適用した結果を示していた（情報理論とその応用シンポジウム）．しかし，量子一括復号の視点がなかったため，半古典的な取り扱いにとどまり，量子利得は全く得られていない．むしろ，その結果を超えるこ

とが量子利得につながるという意味で，半古典的限界を示していると位置付けることができた．

(2) 研究代表者および国内の状況

一方，研究代表者らは，申請時までに，継続的に量子通信における符号化と復号化の研究を行ってきた．その中で，2 元線形符号に対する誤り率を最小にする量子最適復号や，それを一般化した，q 元擬巡回符号に対する量子最適復号を明らかにしてきた．また，2 元の場合に対し，様々な符号化の特性を示し，量子特有の符号化の量子利得の解明に努めてきた．しかし，量子ガウス通信路の容量が明らかにされていない段階でのこれらの研究は，従来の情報理論において，2 元対称通信路などの離散的通信路の容量に近づく符号化を研究するようなものであったと考えられる．

このような中，研究代表者らは，量子符号化変調の研究に向かうことを考えるに至ったが，当時，国外では，量子符号化変調に関する議論は皆無であり，また，我が国では，NICT において世界で初めて符号化の量子利得を実証する原理実験がデモされた（Exceeding classical capacity limit in quantum optical channel, M. Fujiwara, M. Takeoka, J. Mizuno, and M. Sasaki, Physical Review Letters, vol.90, 167906, 2003）ことなどから，本研究を発展させ，将来，実験グループとリンクすることによって，我が国が，量子情報通信研究で世界をリードしていくことも期待された．

２．研究の目的

本研究の目的は，量子情報理論の示す通信の究極的限界である，量子通信路容量に近づく変調方式及び符号化を，光を媒体とする量子通信の場合について，明らかにすることであった．

１に述べたとおり，申請の前年(2004 年)，量子情報理論における永年の未解決問題であった，量子ガウス通信路の通信路容量の中で，もっとも基本的な減衰通信路の容量が，MIT グループによって明らかにされた．量子性をもつ代表的な情報媒体は光であり，量子通信は，現在の光通信技術を高度に発展させた形で実現されることが，予想されている．この光通信において，減衰通信路は，光ファイバ通信におけるファイバの伝送損失や光空間伝送におけるビーム広がりによる損失をモデル化した，もっとも重要な通信路モデルである．したがって，エネルギー制約条件下での，光通信の究極の限界が示されたといえるが，申請時点では，連続的変調（アナログ変調ともいう．つまり，無限に多くの送信信号を許す）および符号長無限大の符号化により，原理的に達成されることが証明された段階であった．一方で，それまでの量子通信の研究で，多相 PSK（位相シフトキーイング）量子信号に対する符号化なしのさまざまな研究や，2 元信号に対する符号化の研究が行われており，これらをベースに，量子通信路容量に近づくためには，どのような変調を用い，どのような符号化および復号化を行えばよいのかを考察し，さらには，それらを組み合わせた符号化変調の量子版を考察していくことが，次の課題と考えられた．

本研究課題では，まず，ディジタル変調によって，符号長無限の極限でどこまで量子通信路容量に近づけるかを明らかにすることを目指した．具体的には，多相 PSK，QAM（直交振幅変調）量子信号に対する減衰通信路における（信号数制約付き）量子通信路容量を導出し，量子ガウス通信路の容量と比較することとした．2 番目に，これを元に，2 元信号ならどの程度のエネルギーのときに量子ガウス通信路の容量に近いか，4 元信号ではどうかなどを明らかにし，量子ガウス通信路の容量に近い信号に対し，符号化を検討することとした．そして，3 番目として，量子ガウス通信路の容量に近づくことのできる最小元数の信号を用いた符号化変調方式を検討することとした．その際，量子一括復号による符号化の量子利得を得るため，符号化には 2 元線形符号を用いることとした．申請時点までに，受信平均光子数 1 個以下の場合，2 元信号でほぼ通信路容量を達成できることが知られていたが，受信光子数 20 個程度までについて，具体的な符号化変調による利得を明らかにすることとした．最後に，古典との違い，古典からの利得を明確に考察するため，ヘテロダイン受信機および個別復号を用いた場合の通信路容量，信号数制約付き通信路容量を導出し，全量子システムとの比較を行うことで，量子利得を定量的に評価することを目的とした．

３．研究の方法

以下，当初計画を示す．

(1) 離散化量子通信路容量の導出と量子ガウス通信路容量との比較

ディジタル変調によって，符号長無限の極限でどこまで量子通信路容量に近づけるかを明らかにするものである．エネルギー制約条件の下，減衰通信路を通して伝送された受

信平均光子数が 0 から 20 個程度までの特性を調べる．

具体的には，M 相 PSK（位相シフトキーイング）信号，M 値 QAM（直交振幅変調）信号による，離散化量子通信路容量を導出する．この場合，M 相，M 値といっても，どのくらいの規模の信号まで行うべきかは，計算結果を量子ガウス通信路容量と比較してみなければわからず，M は小さい値からはじめ，大きい値までを計算することになる．しかし，PSK 信号については，少なくとも，2，4，8，16，32，64 相信号について，離散化量子通信路容量の数値を導出する．これまでに，PSK 信号については，離散化量子通信路容量の解析解が知られている（Derivation of classical capacity of quantum channel for discrete information source, K. Kato M. Osaki, and O. Hirota, Physics Letters, vol.A251, 157-163, 1999）．PSK 信号については，その公式により，数値特性を計算できるはずである．必要に応じ，さらに多値の信号について，計算を行うこととするが，元の数が多い場合は，PSK 信号よりも，QAM 信号の離散化容量が大きくなることが予想される．

QAM 信号については，離散化量子通信路容量の解析解が得られていない．これを導出できればよいが，これまでに解が得られていないのは，量子 QAM 信号は対称性をもたず，その解析が極めて難しいためであり，数値計算アルゴリズムにより，離散化量子通信路容量の数値を導出する．アルゴリズムとして，量子有本アルゴリズムを用いる．したがって，量子有本アルゴリズムのプログラム化が必要である．QAM 信号については，少なくとも，16～64 値の QAM については，計算を行う．しかし，これ以上大規模のものについては，量子有本アルゴリズムによっても膨大な計算時間がかかることが予想される，

量子ガウス通信路容量との比較で，受信平均光子数が 20 個程度までに，さらに元数を増やす必要がなければ良いが，元数を増やす必要がある場合，アルゴリズムをさらに効率的にすることが必要である．その場合は，QAM 信号用にアルゴリズムを特化することで，対応する．具体的には，QAM のもつ部分対称性から，アルゴリズムの改良を考えてみる．

以上，得られた結果により，M 元信号によって，どの程度のエネルギーのときに，量子ガウス通信路の容量に近い特性が得られるかをまとめる．

(2) 量子ガウス通信路の容量に近い元数の信号による符号化特性の解析

(1)の結果に基づき，量子ガウス通信路の容量に近い元数の信号による符号化特性を考察する．これは，(1)の結果により定められる，適切な変調方式をそのまま用い，多元符号化により，量子利得を得る試みである．量子通信路容量に近づき，高信頼性を目指す符号化であるので，誤り率規準での量子利得を考察するべきだが，これまで，多元量子信号に対する，誤り率規準での符号化の量子利得はほとんど考察されていない．さらに，離散化容量は，符号長無限での伝送速度の限界を表し，量子通信路容量に超加法性があることから，かなり長い符号長でなければ，量子ガウス通信路容量に近い伝送速度で誤り率の改善を得ることは難しいことが予想される．超加法性自体が量子利得であるため，符号化なし及び有限符号長での最大相互情報量との比較から，情報量を増大させ，かつ誤り率を減少させる符号の判定を行う．

(3) 4 元及び 8 元信号を用いた量子符号化変調方式の例

古典における符号化変調は，多元信号による変調の効果を維持しつつ，2 元符号の豊富な成果を利用することが特徴である．量子通信においても，多元に比べ，2 元符号に対する多くの成果が，これまでに得られている．一例を挙げれば，任意の 2 元線形符号に対する量子最適復号を計算する公式が与えられており，力づくで計算可能なものの 100 倍以上の規模（符号語数）の符号に関する誤り率計算が可能であったり，さらに，ある種の 2 元符号については，その符号の性質を考慮することで，そのさらに１万倍以上の規模（符号長）の符号の誤り率を計算できる（A simplification algorithm for calculation of the mutual information by quantum combined measurement, S. Usami, T. S. Usuda, I. Takumi, and M. Hata, IEICE Transactions on Fundamentals., vol.E82-A, no.10, pp.2185-2190, 1999）．つまり，量子の場合も，古典と同様に，2 元符号の豊富な成果を利用することが期待できる．したがって，変調方式には多元量子信号を用い，2 元符号を用いる量子符号化変調について，考察する．まず，4 元及び 8 元といった，元数の比較的小さい量子信号を用いることで，量子符号化変調の基本特性を調べる．また，2 元符号には，ブロック符号を用い，復号は量子一括復号とする．古典符号化変調においては，信号間のユークリッド距離により，符号化と変調信号の対応がとられるが，量子符号化変調においては，量子状態信号間の距離を表すフィデリティを用い，検討する．

(4) ブロック符号による量子符号化変調の特性解析

ブロック符号による特性解析では，量子通信の技術としてのメリットを定量的に示す符号化変調方式を明らかにすることを目指

す．特に，代数的な符号を用いた場合の特性を明らかにする．符号長が長い場合については，多くの例を示すのは困難であるため，厳密な誤り率計算だけでなく，量子信頼性関数による誤り率上界などの特性も示し，各伝送速度に対し，符号化変調がどのように効くかを予想する．

(5) ヘテロダイン受信機に基づく半古典的通信路容量による結果とここまでの結果の比較考察

ヘテロダイン受信機に基づく半古典的通信路容量は，量子と古典の比較を行うためのものである．まず，離散化通信路容量とガウス通信路の容量の関係が，量子と半古典の場合で異なるかを考察する．さらに，符号化変調における量子の特有性があるか否かを考察する．

４．研究成果

以下，研究成果について，得られた順に示す．なお，通信路容量や符号化変調の特性など，グラフ等を含む詳細な結果については，発表論文等に示している．

(1) 離散化量子通信路容量の導出と量子ガウス通信路容量との比較

ディジタル変調によって，符号長無限の極限でどこまで量子通信路容量に近づけるかを明らかにするものである．エネルギー制約条件の下で，減衰通信路を通して伝送された受信平均光子数が 0 から 10 個程度までの特性を調べた．具体的には，2，4，8，16 相 PSK，16 値 QAM 信号による，離散化量子通信路容量を数値的に導出した．その結果，平均光子数が 3 個程度までなら，これらの信号によって量子ガウス通信路の容量が，ほぼ達成されることが明らかになった．これは，従来の 2 元信号の結果の 100 倍以上のエネルギーに相当する．詳細は，以下の論文等に示している．
Y. Ishida, K. Kato, and T.S. Usuda, Capacity of attenuated channel with discrete-valued input, Proceedings of the 8th International Conference on Quantum Communication, Measurement and Computing, O. Hirota, J. H. Shapiro, and M. Sasaki (Eds.), NICT Press, pp.323-326, 2007 年

(2) M 相 PSK 信号による符号化特性の解析

(1)の結果に基づき，多元信号による符号化特性を考察するものである．まず，3 相 PSK 信号に対し，擬巡回符号を適用し，復号には，3 元擬巡回符号に対して誤り率を最小にする復号であることが証明されている SRM を用いた．その結果，符号長を延ばすことで，超加法的量子利得が得られること，量子ガウス通信路容量に近づくことが確認された．

さらに，5 相および 7 相 PSK のデータを蓄積した．その結果，広い範囲で符号化なし最大相互情報量を上回る量子利得が得られることがわかった．今後，さらに大きな量子利得を得る符号化を明らかにする必要がある．詳細は，以下の論文等に示している．
佐原僚介，廣澤真一，宇佐見庄五，臼田毅，M 相 PSK 変調を用いた擬巡回符号による相互情報量，第 30 回情報理論とその応用シンポジウム，pp.193-197，2007 年

(3) 量子符号化変調の検討と多元符号に対する量子最適復号の公式の導出

4 相 PSK に対する量子符号化変調の検討を行ったが，その特性を調べるにあたり，従来の量子最適復号の公式を拡張する必要が生じ，まず，その拡張を行った．すなわち，これまで，M 元対称信号を擬巡回符号化した場合の量子最適復号は，M が素数の場合にのみ，効率的に数値計算できる公式が知られていた．そこで，本研究において，従来の結果を拡張し，M が任意の素数べきの場合についても，公式が成立することを証明した．この結果は，非素数元の対称信号である，4，8，16 相 PSK 信号等を用いた量子符号化変調の特性を調べるため，用いることができると考えられる．

(4) ブロック符号による量子符号化変調の特性解析

① ブロック符号を用いた量子符号化変調の検討

古典情報理論における，ブロック符号を用いた符号化変調のやり方を，そのまま量子符号化変調に応用することを検討した．量子利得を得るために一括復号として SRM を用いたが，符号化は 2 元線形符号化という理想的な対称性を有するものであっても，多元符号としての対称性は保証されず，したがって，SRM の最適性が保証されない，あるいは通信路行列公式を適用できないという問題が生じた．このため，今後，多元符号として対称性を有するように符号化変調を検討するべきであるという方向性が明らかとなった．

② 量子信頼性関数による多元符号化の復号誤り率の収束特性の解析

(1)に示したように，符号長無限の極限に対応する量子通信路容量の特性を明らかにしたが，符号長無限の極限ではなく，現実的な有限の符号長でのパフォーマンスを調べるため，量子ガウス通信路の量子信頼性関数と，2，4，8，16 相 PSK，16 値 QAM 変調に対する量子信頼性関数を比較した．その結果，

量子通信路容量の特性に類似し，平均光子数が小さいときは，16 元程度までの変調で，連続変調の結果とほぼ等しいパフォーマンスが得られることがわかった．詳細は，以下の論文等に示している．
S. Hirosawa, S. Usami, T.S. Usuda, and A. Ogawa, Property of reliability function for attenuated channel with discrete-valued input, Proceedings of AQIS2007, pp.161-162, 2007 年

(5) 符号化 PSK 変調に対する情報レートと誤り率の特性
符号化 PSK 変調の考察として，変調の際の信号数と符号化率により決まる情報レートを一定としたとき，信号数と符号長を変えたときに量子一括復号による最小ビット誤り率がどのように改善するかを調べた．符号化として擬巡回符号を用い，信号数を一定として符号長を変えた場合は，符号長が長くなるほどビット誤り率が改善されることが確認されたが，信号数を変えた場合は，符号長が長ければよいとは限らないことがわかった．詳細は，以下の論文等に示している．
R. Sahara, S. Usami, and T.S. Usuda, The multiple coding gain with two criteria in an attenuated quantum channel, Proceedings of ISITA2008, pp.473-478, 2008 年

(6) ヘテロダイン受信機と量子準最適受信機による最大相互情報量の比較
ここまでの本研究の結果を技術に結びつけるため，量子最適受信機よりも実現の容易な準最適受信機に着目した．その結果，多元 PSK 信号に対する量子準最適受信機による最大相互情報量は，ヘテロダイン受信機だけでなく，誤り率を最小とする量子最適受信機による相互情報量をも上回る場合があることが明らかとなった．この結果は，符号化によって量子準最適受信機の優位性が発揮されることを示している．詳細は，以下の論文等に示している．
今枝麻美，佐原僚介，臼田毅，M 相 PSK 信号に対する量子準最適受信機による最大相互情報量の特性，第 31 回情報理論とその応用シンポジウム，pp.889-894，2008 年

(7) リードソロモン符号を用いた符号化 PSK 変調の検討
量子通信に対して性能の良い符号を効率的に見つけるため，古典的に性能の良い符号を重点的に調べることの可否を明らかにするべく，リードソロモン符号を用いた符号化 PSK 変調の特性を調べた．短い符号長の場合にしらみつぶしに調べた結果として，リードソロモン符号は擬巡回符号の中で量子一括復号による相互情報量のパフォーマンスが極めて優れていることがわかった．このことは，今後の量子通信システムの設計論に対する示唆を与えるものであるといえる．詳細は，投稿中の論文等に示している．

以上，研究成果を得られた順に記してきた．本研究は，量子情報通信の実用化へのステップとして，必要な工学的考察を行ったものであるが，研究開始当初のみならず，現在に至るまで，世界で類似の研究はほとんどない．これは，情報通信の多くの研究者が量子力学の敷居を高いと考えているため，量子情報技術の研究者は理学者がほとんどであるという現状によると思われる．しかし，このように稀少な課題に取り組む本研究に対し，世界の研究者も興味がないのではなく，その重要性を認識していながら，研究困難という実情があることを，最終年度にうかがうことができた．また，同時に，今後行うべき研究についても示唆が得られた．
具体的には，平成 20 年 6 月に，量子情報分野で顕著な貢献をしている Holevo, Yuen, Bennett, Shor, Jozsa をはじめとした 13 名の研究者の集まる会議に参加する幸運に恵まれ，プロジェクトの成果を発表してきた：T.S. Usuda, Modulation, coding and decoding in classical-quantum channel, “Osamu Hirota, A True Quantum Communications Channel”, Perimeter Institute for Theoretical Physics, Waterloo, Canada, 2008 年（招待講演）（http://www.perimeterinstitute.ca/en/Events/Osamu_Hirota/Schedule/にプログラム公開）
その結果，量子通信理論のパイオニアである Holevo, Yuen らから，重要な研究であるとの高い評価を得るとともに，我々がこれまでに実施してきた符号化・変調の研究は，狭帯域（あるいは単一モード）量子通信路に関するものであり，今後さらに，広帯域量子通信路へと発展させるべきであることがわかった．また，そこでの議論から，究極の限界を示す理論予測を実験研究へとつなげる，本研究を進めるために不可欠な様々なノウハウを，世界の量子情報の研究者が使いこなせていないという意外な事実を知り，広帯域量子通信路に対する符号化，変調，多重化を明らかにする本研究は，正に，我々が実施すべき課題であるとともに，量子通信の実現化に向けて，我が国が先導的役割を果たせる可能性があることを確信した．そして，そのためには，我が国において，物理学者，数学者と情報通信の研究者のリンクが真に実現することが望まれることは，言うまでもない．

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１５件）
①佐原僚介，林祐一，宇佐見庄五，臼田毅，内匠逸，誤り率と情報量双方の規準に基づく量子利得をもつ符号の例，電気学会論文誌(C)，Vol.128，No.12，pp.1743-1744，2008年，査読有.
②R. Sahara, S. Usami, and T.S. Usuda, The multiple coding gain with two criteria in an attenuated quantum channel, Proceedings of ISITA2008, pp.473-478, 2008年，査読有.
③Y. Ishida, K. Kato, and T.S. Usuda, Capacity of attenuated channel with discrete-valued input, Proceedings of the 8th International Conference on Quantum Communication, Measurement and Computing, O. Hirota, J. H. Shapiro, and M. Sasaki (Eds.), NICT Press, pp.323-326, 2007 年，査読有.
④S. Hirosawa, S. Usami, T.S. Usuda, and A. Ogawa, Property of reliability function for attenuated channel with discrete-valued input, Proceedings of AQIS2007, pp.161-162, 2007年，査読有.
⑤石田雄樹，宇佐見庄五，臼田毅，内匠逸，2 元線形符号による情報量規準に基づく符号化の量子利得特性，電気学会論文誌 (C)，Vol.126，No.12，pp.1474-1482，2006年，査読有.

〔学会発表〕（計２８件）
①佐原僚介，伊與田賢太，宇佐見庄五，臼田毅，M 元量子信号に対する 2 つの規準による符号化の量子利得に関する考察，第 31 回情報理論とその応用シンポジウム，pp.473-478，2008年10月8日，鬼怒川.
②今枝麻美，佐原僚介，臼田毅，M 相 PSK 信号に対する量子準最適受信機による最大相互情報量の特性，第 31 回情報理論とその応用シンポジウム，pp.889-894，2008 年 10 月 10 日，鬼怒川.
③伊與田賢太，佐原僚介，臼田毅，3 元量子信号に対する符号化特性の考察，平成 20 年度電気関係学会東海支部連合大会，O-196，2008年9月19日，愛知県立大学.
④浅見侑太，服部友輔，佐原僚介，臼田毅，3ASK スクィズド状態信号の最適スクィジングパラメータの特性，平成 20 年度電気関係学会東海支部連合大会，O-201，2008 年 9 月 19 日，愛知県立大学.
⑤T.S. Usuda, Modulation, coding and decoding in classical-quantum channel, “ Osamu Hirota, A True Quantum Communications Channel”，2008 年 6 月 26 日，Perimeter Institute for Theoretical Physics, Waterloo, Canada.
⑥佐原僚介，廣澤真一，宇佐見庄五，臼田毅，M 相 PSK 変調を用いた擬巡回符号による相互情報量，第 30 回情報理論とその応用シンポジウム，pp.193-197，2007年11月28日，賢島.
⑦吉川誠広，澤田友宏，臼田毅，M 相 PSK コヒーレント状態信号に対する量子準最適受信機の改良，第 30 回情報理論とその応用シンポジウム，pp.202-207，2007年11月28日，賢島.
⑧澤田友宏，臼田毅，SRM の擬古典性，第 30 回情報理論とその応用シンポジウム，pp.294-299，2007年11月28日，賢島.
⑨服部友輔，廣澤真一，臼田毅，スクィズド状態とコヒーレント状態の離散化通信路容量の比較，平成 19 年度電気関係学会東海支部連合大会，O-363，2007年9月28日，信州大学.
⑩廣澤真一，石田雄樹，宇佐見庄五，臼田毅，小川明，M 相 PSK 変調を用いた多元符号化による相互情報量，2007年電子情報通信学会総合大会，A-6-2，2007年3月21日，名城大学.
⑪廣澤真一，石田雄樹，宇佐見庄五，臼田毅，小川明，情報量規準による量子利得を最大にする線形符号の条件，平成 18 年度電気関係学会東海支部連合大会，O-115，2006年9月28日，岐阜大学.

６．研究組織
(1)研究代表者
臼田　毅（USUDA　TSUYOSHI）
愛知県立大学・情報科学部・准教授
研究者番号：８０２７３３０８

(2)研究分担者
なし

(3)連携研究者
なし