様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　６　月　１７　日現在

機関番号：　１２６１２
研究種目：　基盤研究(C)（一般）
研究期間：　2013～2015
課題番号：　２５４２０３５７

研究課題名（和文）高信頼性通信ネットワークの構築に向けたマルチユーザ情報理論の精密化

研究課題名（英文）Refinement of Multi-User Information Theory for High-Speed Communication Network

研究代表者

八木　秀樹（Yagi, Hideki）

電気通信大学・情報理工学（系）研究科・准教授

研究者番号：６０４０９７３７

交付決定額（研究期間全体）：（直接経費）　　4,000,000円

研究成果の概要（和文）：通信ネットワークの発展に伴い，無線通信の数理モデルとなる通信路クラスに対する通信の信頼性・効率性の理論限界の解析が重要な課題となっている．本研究では，複数の定常無記憶通信路の混合分布により通信路の統計的性質が定められる無記憶混合通信路のクラスに対し，復号誤り確率をεまで許容した場合に達成できる最大符号化レート（ε通信路容量）の解析とその精密化を目的として研究を行った．さらに複数の送信機とひとつの受信機から構成される多重アクセス通信路に対し，得られた成果の拡張を検討した．また，関連する情報セキュリティや情報源符号化システムに対しても同様のアプローチから研究を行った．

研究成果の概要（英文）：With the rapid development of communication networks, the analysis of the best attainable performance of a coding system over a wireless communication channel becomes an important research topic. This study aims to analyze the asymptotically optimum coding rate (channel capacity) under the condition that the decoding error probability is upper bounded by a constant for the class of mixed memoryless channel, whose channel law is given by a mixture of multiple stationary memoryless channels. We then discuss a generalization of the obtained results to the multi-user channel, which is a mathematical model of the cognitive radio system. In addition, we investigate related source coding systems and information security.

研究分野：　情報通信工学

キーワード：　情報理論　符号理論　通信路符号化　通信路容量　二次符号化レート　情報セキュリティ

１．研究開始当初の背景

近年のネットワーク技術の発展により，ネットワーク上で複数のユーザーが同時に通信を行うマルチユーザ通信システムにおける符号化法が盛んに研究されている．情報理論の分野では，**通信路符号化**技術により，通信の**信頼性**を保証したまま**効率性**をどこまで向上させるかという限界を数理的な手法により明らかにする．符号理論の分野では，情報理論分野で明らかにされた効率性の理論限界を実現する具体的な仕組みを開発する．

通信路符号化システムでは，各**符号器**において送信者が宛先に送りたいメッセージが**符号語**（送信系列）に**符号化**され，符号語が通信路に入力される．通信路では物理的な影響により，送信系列が確率的なひずみを受ける．**復号器**は観測した受信系列から送信メッセージを推定する．この操作を**復号**と呼ぶ．これら符号器と復号器の組を**符号**という．

符号化システムの信頼性は送信メッセージの**復号誤り率**によって評価される．また，符号化システムの効率性は**符号化レート**と呼ばれる送信シンボル当たりで表現されるメッセージのビット長により測られる．『各復号器の復号誤り率を定数 ε 以下にできる符号化・復号法が存在する符号化レートの最大値』は **ε 通信路容量**と呼ばれる．情報理論分野では，与えられた通信路の ε 通信路容量を，通信路の確率的特性から計算される情報量を用いて具体的に特徴づけることを目的とする．また，近年 ε 通信路容量が明らかになっている通信路に対し，有限長の符号の符号化レートが符号長の増大とともにどのように ε 通信路容量に近づくかを表わす**二次符号化レート**の解析が進められている．一方，複数の符号器や復号器からなるマルチユーザ通信路に対しては，現在まで同様な解析結果はほとんど得られておらず，未解決な問題が多い．そこで本研究では，無線ネットワークの通信システムを念頭におき，基本的な通信路モデルに対する ε 通信路容量および二次符号化レートを解析し，得られた研究成果を複数の符号器からなるマルチユーザ通信路に展開する．

２．研究の目的

複数の定常無記憶通信路（**要素通信路**と呼ぶ）の混合確率分布により通信路の統計的性質が定められる通信路を**混合無記憶通信路**と呼ぶ．図１に混合無記憶通信路の概要を示す．混合無記憶通信路は，メッセージの送信中にひとつの要素通信路が混合比に応じて確率的に選ばれる通信路モデルを表わしており，フェーディング係数が確率的に決まり，符号語が伝送される間はその係数が変わらない性質を持つフェーディング通信路の基本的な数理モデルとなる．

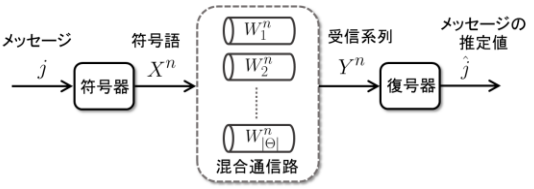

図１．　混合無記憶通信路の符号化システム

混合無記憶通信路は定常ではあるが，エルゴード性を持たない通信路の最も基本的な例であり，理論的側面のみならず応用上も重要な通信路と見なされてきた．しかしながら，その ε 通信路容量が具体的にどのように特徴づけられるかはこれまで明らかにされていなかった．そこで本研究では，混合無記憶通信路に対して，ε 通信路容量を明らかにすることを目的とする．さらに，最大二次符号化レートの解析を行い，その結果を符号器が複数のマルチユーザ通信路に拡張する．

３．研究の方法

本研究では，(i) 要素通信路の数，(ii) 通信路状態の情報の有無，(ii) 符号器の数に応じて以下の場合を議論する．

(i) 本研究では，**情報スペクトル**的手法に基づいて，誤り確率の上界式と下界式を導出する．この際に，要素通信路数が離散の場合（有限個または可算無限個）と一般の場合（非可算無限個）の場合に，誤り確率の上界式・下界式の評価が異なってくる．特に要素通信路数が一般の場合はアルファベットの有限性を仮定して議論する必要があり，本研究でもその場合に特化した技術を開発する．

(ii) 混合通信路は，符号器から符号語が送信される際に，混合比の値に応じて要素通信路が確率的に選ばれるシステムと見なすこともできる．ここで選ばれる要素通信路のインデックスを『通信路状態』と見なし，符号器または復号器通信路状態の情報を知ることができる場合の ε 通信路容量の変化を解析する．この場合も，要素通信路数が有限個または可算無限個の場合と非可算無限個の場合に分けて議論する．

(iii) 本研究で最終的な目標とするマルチユーザ通信路に対し，得られた研究成果の拡張を検討する．特に符号器の数を増やした通信システムに着目して議論を進める．

４．研究成果

（１）　要素通信路数が可算無限個の場合

要素通信路が有限または可算無限個の場合に対して，ε 通信路容量の符号長に依存しない表現を得た．特に，ε 通信路容量

が通信路への入力シンボルの確率変数と各要素通信路からの出力シンボルの間の相互情報量の累積分布関数により特徴づけられることを示した．

例１． ここで，3 つの要素通信路から構成される混合無記憶通信路を考えよう．要素通信路 i（i = 1,2,3）の通信路入力と通信路出力の間の相互情報量を Ii と表す．一般性を失うことなく，相互情報量 Ii の値は，インデックス i の値に応じて増加すると仮定する．また，要素通信路 i の混合比を $w(i)$ と表す．このとき，ε 通信路容量 $C(\varepsilon)$ の値の変化の様子を図 2 に示す．図 2 の横軸は ε の値を，縦軸は ε 通信路容量の値を表わしている．最も相互情報量が低い要素通信路 1 の混合比 $w(1)$ の値よりも ε が小さい範囲では，要素通信路 1 の相互情報量 $I1$ が ε 通信路容量となる．ε の値が $w(1)$ 以上になると，要素通信路 2 の相互情報量 $I2$ が ε 通信路容量となることが分かる．さらに ε の値が $w(1)+w(2)$ 以上になると，要素通信路 3 の相互情報量 $I3$ が ε 通信路容量となる．このように，累積混合比の値が ε を超えない範囲で要素通信路の部分集合を考え，その部分集合内の最大の相互情報量が ε 通信路容量と一致することが分かる．

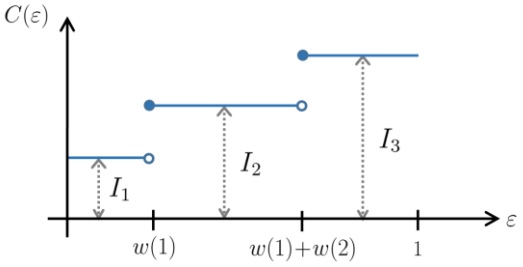

図 2. 3 つの要素通信路から構成される混合無記憶通信路の ε 通信路容量の遷移

この結果から，得られた ε 通信路容量の表現は，複数の定常無記憶情報源が混合された**混合情報源**に対する最少符号化レートの表現と双対の形となることが分かった．なお，要素通信路数が有限または可算無限個の場合，通信路への出力シンボルは有限とは限らない一般の集合と仮定しても，同様の解析結果が成り立つことを示している．

また，要素通信路間に相互情報量によるある種の順序関係が定義できる混合無記憶通信路（**Well-Ordered 通信路**と呼ぶ）に対し，最適な二次符号化レートの解析を行った．Well-Ordered 通信路に対する最適な二次符号化レートは，通常の定常無記憶通信路（シングルユーザ通信路）に対する最適な二次符号化レートを一般化した表現になることを示した．この表現から，有限長の符号を用いた時に，その最大符号化レートが ε 通信路容量に対してどれくらい差があるかを測ることが可能となり，具体的な符号設計を議論する符号理論的な立場からも大きな意義を持つ．

（２） 要素通信路数が非可算無限個の場合

次に，要素通信路が非可算無限個の場合に対して，ε 通信路容量を解析した．得られた特徴づけは，要素通信路が可算無限個の場合の拡張となっている．一方，この結果を導く課程の議論は，要素通信路が可算無限個の場合と大きく異なり，本質的に新しい解析手法の開発が必要となった．ただし，要素通信路数が可算無限個の場合と異なり，通信路からの出力シンボルの集合を有限集合と仮定する必要がある．一般の出力シンボル集合への結果の拡張は，今後の課題である．

要素通信路数が可算無限個の場合の議論を拡張し，Well-Ordered 通信路に対する最適二次符号化レートを特徴づけた．この結果も，ε 通信路容量の特徴づけと同様に，可算無限個の要素通信路の場合の一般化となっている．

（３） 通信路状態を符号器または復号器で観測できる場合の解析

送信された符号語がどの要素通信路を通るか（通信路状態）の情報が符号器または復号器で分かる場合について，ε 通信路容量がどのように変わるかを解析した．結果，復号器のみが通信路状態を知ったとしても，その通信路容量は通信路状態を知らない場合と比べて変わらないことが分かった．一方，復号器のみならず符号器も通信路状態が分かる状況では，ε 通信路容量の値は大きくなる．これは，あらかじめ符号器が選ばれる要素通信路に合わせて最適な符号を選択できることに起因する．

（４） 複数の復号器と一つの復号器から構成される多重アクセス通信路

最後に，本研究の目的の一つであるマルチユーザ通信路への結果の拡張を検討した．一般に，マルチユーザ通信路の ε 通信路容量の領域の解析は，シングルユーザ通信路への解析に比べてはるかに難しい．そこで，初めのステップとして，２つの符号器と１つの復号器から通信路が構成される**多重アクセス通信路**を対象とした．近年のコグニティブ無線技術の発展を念頭に，符号器１が符号器２の送るメッセージを観測できる状況を仮定し，混合通信路に対する ε 通信路容量の領域を特徴づけた．最適な二次符号化レートの解析については，今後の課題である．

（５） その他の研究成果

上記の研究の他，**情報源符号化**システム（データ圧縮）や情報セキュリティに関する研究成果を得た．特に，復号された系列の歪

みがあらかじめ定めた定数を超える確率（歪み超過確率）をε以下に制限したもとで，情報源系列の符号化レートを最小化する有歪み情報源符号化システムの解析を行った．定常性やエルゴード性などの確率構造を仮定しない一般の情報源に対して最少符号化レートを解析し，その表現を得た．

また，デジタルコンテンツの保護を目的とした電子指紋符号や生体データの識別を目的とした生体識別システムに対する検出器の誤り確率に関して，情報論的アプローチによる詳細な解析を行った．

５．主な発表論文等

〔雑誌論文〕（計３件）

[1] H. Yagi, T. S. Han, R. Nomura, "First- and second-order coding theorems for mixed memoryless channels with general mixture", （査読あり）IEEE Trans. Inf. Theory (採録決定) 2016 年 5 月.

[2] 新家稔央, 八木秀樹, 平澤茂一, "Forney の最尤復号法の一般化における Shulman-Feder 上界式の精密化", （査読あり）電子情報通信学会 論文誌 A, vol. J98-A, no.12, pp.680-690, 2015 年 12 月.

[3] B. M. Kurkoski, H. Yagi, "Quantization of binary-input discrete nemoryless channels", （査読あり）IEEE Trans. Information Theory, vol.60, no.8, pp.4544-4552, 2014 年 8 月.

〔学会発表〕（計１２件）

[1] 八木秀樹, “状態を有する通信路に対する最適符号化レート解析の精密化” 電子情報通信学会 技術報告誌, 2016 年 3 月.

[2] V. Yachongka, H. Yagi, "Reliability function of discrete memoryless biometrical identification systems", （査読あり）2016 RISP Int. Workshop on Nonlinear Circuits, Communications and Signal Processing (NCSP2016), Honolulu, USA, 2016 年 3 月.

[3] H. Yagi,T. S. Han, R. Nomura, "First- and second-order coding theorems for mixed memoryless channels with general mixture", （査読あり）Proc. of 2015 IEEE Int. Symposium on Information Theory (ISIT2015), pp.2969-2973, Hong Kong, China, 2015 年 6 月.

[4] H. Yagi, R. Nomura, "Variable-length coding with epsilon-fidelity criteria for general sources", （査読あり）Proc. of 2015 IEEE Int. Symposium on Information Theory (ISIT2015), pp.2181-2185, Hong Kong, China, 2015 年 6 月.

[5] R. Nomura, H. Yagi, "Information spectrum approach to fixed-length lossy source coding problem with some excess distortion probability", （査読あり）Proc. of 2015 IEEE Int. Symposium on Information Theory (ISIT2015), pp.306-310, Hong Kong, China, 2015 年 6 月.

[6] 村越礼門, 八木秀樹, "部分的協調が可能な符号器を有する一般多重アクセス通信路の通信路容量域" 第 37 回情報理論とその応用シンポジウム予稿集, 2014 年 12 月.

[7] H. Yagi, R. Nomura, "Channel dispersion for well-ordered mixed channels decomposed into memoryless channels", （査読あり）Proc. of 2014 Int. Symposium on Information Theory and its Applications (ISITA2014), pp.35-39, Melbourne, Australia, 2014 年 10 月.

[8] 八木秀樹, “通信路符号化における有限長理論” 電子情報通信学会 2014 年ソサイエティ大会講演論文集, 2014 年 9 月.

[9] R. Sekiya, E. C. Garcia-Alvarez, B. M. Kurkoski, H. Yagi, “Write-once memory codes for low-complexity decoding of asymmetric multiple access channel", （査読あり） Proc. of 2014 Int. Symposium on Information Theory and its Applications (ISITA2014), pp.623-627, Melbourne, Australia, 2014 年 10 月.

[10] H. Yagi, R. Nomura, "Single-letter characterization of epsilon-capacity for mixed memoryless channels", （査読あり）Proc. of 2014 IEEE Int. Symposium on Information Theory (ISIT2014), pp.2874-2878, Istanbul, Turkey, 2014 年 6 月.

[11] 八木秀樹, “通信路符号化の理論における新しい潮流—有限長解析” 電子情報通信学会 技術報告誌, 2013 年 11 月.

[12] 成田智哉, 八木秀樹, "無記憶公平な結託攻撃に耐性のあるユニバーサル電子指紋符号化定理と誤り指数," 第 36 回情報理論とその応用シンポジウム予稿集, 2013 年 11 月.

６．研究組織

(1)研究代表者

八木 秀樹（YAGI HIDEKI）

電気通信大学・大学院情報理工学研究科・准教授

研究者番号：60409737

(2)研究分担者

なし

(3)連携研究者

なし