

## 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 5日現在

機関番号：14301

研究種目：基盤研究（C）

研究期間：2010～2012

課題番号：22560375

研究課題名（和文） 通信路分極の数理と応用に関する基礎的検討

研究課題名（英文） Fundamental study on theory and applications of channel polarization

研究代表者

田中 利幸（TANAKA TOSHIYUKI）

京都大学・大学院情報学研究科・教授

研究者番号：10254153

研究成果の概要（和文）：2008年に新規に提案されたポーラ符号と逐次除去復号法との組み合わせは、任意の無記憶通信路に対して長符号長極限で対称通信路容量を漸近的に達成することが証明されており、かつ符号化と復号との計算複雑度が低いという点で注目を集めている誤り訂正符号である。本研究課題では、ポーラ符号が高い性能を達成する数理的基盤である通信路分極の現象についてより深く検討することによって、より高性能の符号を構成するために有用な知見を得ることを目的とした。研究成果として、すでに報告されていた復号誤り率の漸近評価を精密化することで、符号化率に依存する形で復号誤り率の漸近評価を与える結果を得た。また、多元アルファベットに対する通信路分極の現象を検討し、 $F_q$ 上の可逆な $\ell \times \ell$ 行列にもとづいて通信路分極が生じるために $\ell \times \ell$ 行列がみたすべき必要十分条件を得た。

研究成果の概要（英文）：Polar codes combined with successive-cancellation decoding, that were newly proposed in 2008, have been attracting attentions of researchers as error-correcting codes that have been proven to saturate the symmetric capacity for any memoryless channel in the limit of long codeword length, while requiring relatively low computational complexity in encoding and decoding. In this research project, aiming at obtaining understandings that will be useful in constructing codes with better performance, we have elucidated the phenomenon of channel polarization, which lays the mathematical basis for high performance of polar codes. We have obtained a result on asymptotic decoding error probability in a coderate-dependent form, by refining existing asymptotic results on decoding error probability. We have also studied channel polarization over non-binary alphabet, and have obtained a necessary and sufficient condition for an invertible  $\ell \times \ell$  matrix on  $F_q$  to induce channel polarization.

交付決定額

（金額単位：円）

	直接経費	間接経費	合計
2010年度	1,300,000	390,000	1,690,000
2011年度	1,200,000	360,000	1,560,000
2012年度	800,000	240,000	1,040,000
年度			
年度			
総計	3,300,000	990,000	4,290,000

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：通信路分極，ポーラ符号，通信路容量，通信路符号化，情報通信工学

## 1. 研究開始当初の背景

与えられた通信路に対して、通信路符号化定理によって得られる通信路容量に近い符号化率を達成し、かつ符号化、復号の計算複雑度が低いような誤り訂正符号を具体的に構成する問題は、符号理論における中心的課題であり続けている。1990年代の後半頃から注目を集めている低密度パリティ検査(LDPC)符号と確率伝搬法にもとづく反復復号法との組み合わせは、二元消失通信路に対しては上記の問題に対する具体的な回答を与えていることが示され、一般の無記憶通信路に対しても実験的にはよい性能を示しており、現在に至っても盛んに研究がなされている。

トルコの研究者 Erdal Arikan によって2008年の国際会議において発表された新規な誤り訂正符号であるポーラ符号と逐次除去復号法との組み合わせは、任意の無記憶通信路に対して長符号長極限で対称通信路容量を漸近的に達成することが証明されており、なおかつ符号化と復号との計算複雑度が符号長  $N$  に対して  $O(\text{Mlog}N)$  であるという点で、上記の問題に対する一般的な回答を与えていることになる。その一方で、有限の符号長における性能は LDPC 符号と比較すると芳しくなく、Arikan が提案したそのままの形では、実用的な復号誤り率を達成するには符号長を非常に大きくとる必要がある。ポーラ符号は、与えられた通信路に対する反復的な操作によって生じる通信路分極という現象に基づいて構成されており、通信路分極という現象を研究して理解することによって、ポーラ符号の高い性能をより深く理解するとともに、より高性能の符号を構築することにつながるものと考えられた。

## 2. 研究の目的

ポーラ符号が高い性能を達成する数理的な基盤は通信路分極にある。通信路分極の現象を数理的に詳しく研究することによって、ポーラ符号が高性能を示す仕組みをより深く理解することができると考えられる。本研究では、通信路分極の諸性質を数理的な立場から検討し、それによってより高性能の誤り訂正符号を構成するために有用な知見を引き出すことを目的とした。

具体的には、以下の研究項目に取り組むこととした。

(1) 研究を開始した時点では、ポーラ符号の符号化率が対称通信路容量未満であれば、逐次除去復号法による復号誤り率が長符号長極限でゼロに漸近すること、および符号長が  $N$  のときの復号誤り率が任意の  $\beta < 0.5$  に対して  $O(2^{-N^\beta})$  であることが Arikan と Telatar によって報告されていた。彼らの解

析をより精密化することで、符号化率に依存する形で復号誤り率の漸近評価を得ることを目的とした。

(2) Arikan が提案したポーラ符号は二元符号であるが、多元アルファベットに対するポーラ符号の構成は興味ある研究課題である。多元アルファベットに対する通信路分極の現象を検討し、多元ポーラ符号の構成に有用な知見を得ることを目的とした。

## 3. 研究の方法

研究項目(1)に関しては、まず Arikan と Telatar による復号誤り率に関する解析を詳細に検討した。その結果、彼らの解析は、通信路分極の過程に付随して定義される Bhattacharyya 過程と呼ばれる確率過程の性質を、大数の法則によって評価しているものと解釈できることがわかった。この観察にもとづいて、彼らの解析をより精密化し、Bhattacharyya 過程の性質を中心極限定理によって評価することによって、符号化率に依存する形で復号誤り率の漸近評価が得られるのではないかと考えられたため、このアプローチを具体的に試みた。

研究項目(2)に関しては、Arikan のもともとの提案を多元アルファベットの場合に素朴に拡張するには、アルファベットの大きさを  $q$  として剰余環  $\mathbb{Z}/q\mathbb{Z}$  をアルファベットとして考えるのが自然であると考えられ、通信路分極の多元への拡張を議論している Sasoglu らの研究でもそのように扱われていた。Sasoglu らの結果は、Arikan のもともとの提案を剰余環  $\mathbb{Z}/q\mathbb{Z}$  に拡張した場合には、 $q$  が素数である場合には  $q=2$  の場合と同様に任意の無記憶通信路に対して通信路分極が生じるが、 $q$  が合成数である場合にはポーラ符号の構成に使える形で通信路分極が生じない通信路が存在することを示している。彼らの結果に立脚して、当時研究代表者の研究室に大学院学生として在籍していた森立平氏は、多元アルファベットに対する通信路分極を考察するには剰余環  $\mathbb{Z}/q\mathbb{Z}$  ではなく有限体を考えるべきではないかという着想を得たため、森氏と共同で有限体上での通信路分極について検討を行った。

## 4. 研究成果

研究項目(1)に関しては、通信路分極に付随する Bhattacharyya 過程の解析を中心極限定理にもとづいて行うことで、期待通りに符号化率に依存する形で復号誤り率の漸近評価を得ることができた。具体的には、Arikan が提案した  $2 \times 2$  行列にもとづく通信路分極の議論を拡張して、Korada らが議論したように  $l \times l$  行列にもとづく通信路分極を考えたとき、それによって構成されるポーラ符号の

符号長が $\ell^n$ のときの復号誤り率を $P$ とおくと $\log(-\log_2 P) = nE + (nV)^{1/2} Q^{-1}(R/D) + o(n^{1/2})$ とあらわされることを明らかにした。ここで、 $R$ ,  $I$ はそれぞれ符号化率, 通信路容量である。また、 $E$ および $V$ はそれぞれ, 通信路分極に使用される $\ell \times \ell$ 行列に対して Korada らにより定義された $\ell$ 個の「部分距離」の値の平均と分散である。 $Q(\cdot)$ は誤差関数である。

以上の研究成果は, ローザンヌ工科大学の Hassani らによる成果と合わせた共著論文の形で, 下記雑誌論文(2)にまとめられている。

研究項目(2)に関しては,  $p$  を素数として  $q=p^n$  とおき, 位数  $q$  の有限体  $F_q$  をアルファベットとしたとき,  $F_q$  上の  $\ell \times \ell$  行列にもとづいて通信路分極が生じるために  $\ell \times \ell$  行列がみたすべき必要十分条件を得ることができた。具体的にはまず, 通信路分極に関する性質が同一であるかどうかということにもとづいて  $F_q$  上の可逆な  $\ell \times \ell$  行列の集合に同値関係を定義し, 次にこの同値関係にもとづいて行列の標準形を定義した。その上で,  $F_q$  上の可逆な  $\ell \times \ell$  行列で標準形が単位行列でないようなものが通信路分極を引き起こすためには, 基礎体を  $F_p$  とし当該行列の標準形の要素を  $F_p$  に付加して得られる拡大体が  $F_q$  に一致することが必要十分であることを示した。

また, 研究項目(1)において議論した符号化率に依存する形での復号誤り率の漸近評価の議論を, 有限体  $F_q$  をアルファベットとした場合に拡張し, 通信路分極が生じるという条件のもとで復号誤り率の二重指数の漸近形について上記と同様の結果を得た。さらに, 復号誤り率の二重指数における  $n$  の係数  $E$  を最大にするという点で, 拡張 Reed-Solomon 符号を定義する行列が  $\ell \leq q$  の場合には最適であることを示した。

以上の研究成果は, 論文プレプリント (arXiv:1211.5264v1 [cs.IT]) の形で公開しており, また雑誌論文としても投稿中である。

なお, 実数など連続値をとるアルファベットに対する通信路分極の検討や, 逐次除去復号法に代わり得る復号法の検討なども行ったが, 具体的な研究成果を得るには至らなかった。

## 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2件)

- (1) Toshiyuki TANAKA, Properties of a certain stochastic dynamical system, channel polarization, and polar codes, Journal of Physics: Conference Series, volume 233, paper number 012018, 13 pages, July 2010, 査読あり.  
doi: 10.1088/1742-6596/233/1/012018

- (2) Seyed Hamed HASSANI, Ryuhei MORI, Toshiyuki TANAKA, and Rudiger L. URBANKE, Rate-dependent analysis of the asymptotic behavior of channel polarization, IEEE Transactions on Information Theory, volume 59, issue 4, pages 2267-2276, April 2013, 査読あり.  
doi: 10.1109/TIT.2012.2228295

[学会発表] (計7件)

- (1) Ryuhei MORI and Toshiyuki TANAKA, Channel polarization on q-ary discrete memoryless channels by arbitrary kernels, Proceedings of the 2010 IEEE International Symposium on Information Theory, pages 894-898, Austin, Texas, USA, June 2010, 査読あり.  
doi: 10.1109/ISIT.2010.5513568
- (2) Toshiyuki TANAKA and Ryuhei MORI, Refined rate of channel polarization, Proceedings of the 2010 IEEE International Symposium on Information Theory, pages 889-893, Austin, Texas, USA, June 2010, 査読あり.  
doi: 10.1109/ISIT.2010.5513574
- (3) Toshiyuki TANAKA, Channel polarization: A route to capacity-achieving error-correcting codes, Workshop on Statistical Physics and Computer Science (Beijing Satellite Meeting of STATPHYS-24), July 2010, 招待講演.
- (4) Toshiyuki TANAKA, On speed of channel polarization, Proceedings of the 2010 IEEE Information Theory Workshop, Dublin, Ireland, 5 pages, August-September 2010, 招待講演.  
doi: 10.1109/CIG.2010.5592869
- (5) Ryuhei MORI and Toshiyuki TANAKA, Non-binary polar codes using Reed-Solomon codes and algebraic geometry codes, Proceedings of the 2010 IEEE Information Theory Workshop, Dublin, Ireland, 5 pages, August-September 2010, 査読あり.  
doi: 10.1109/CIG.2010.5592755
- (6) 萩原学, 森立平, 田中利幸, 今井秀樹, ポーラ符号から構成する量子誤り訂正符号の検討, 第33回情報理論とその応用シンポジウム, 24. 3, 2010年11月-12月, 査読なし.
- (7) 田中利幸, ある確率的力学系, 通信路分極とポーラ符号, 情報とダイナミクス IV 研究集会「符号と力学系 IV~重合せ・ゆ

らぎ・独立」, 2012年3月, 招待講演.

[図書] (計0件)

[産業財産権]

○出願状況 (計0件)

名称:  
発明者:  
権利者:  
種類:  
番号:  
出願年月日:  
国内外の別:

○取得状況 (計0件)

名称:  
発明者:  
権利者:  
種類:  
番号:  
取得年月日:  
国内外の別:

[その他]

ホームページ等

- (1) 論文プレプリント: Ryuhei MORI and Toshiyuki TANAKA, Source and channel polarization over finite fields and Reed-Solomon matrix, [Online]. Available as arXiv preprint: arXiv:1211.5264v1 [cs.IT], 2012. <http://arxiv.org/abs/1211.5264>

## 6. 研究組織

(1) 研究代表者

田中 利幸 (TANAKA TOSHIYUKI)  
京都大学・大学院情報学研究科・教授  
研究者番号: 10254153

(2) 研究分担者

( )

研究者番号:

(3) 連携研究者

( )

研究者番号: