科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　２２　日現在

機関番号：　１３４０１
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５６０４４７

研究課題名（和文）対称通信路におけるＰｏｌａｒ符号の符号構成法に関する研究

研究課題名（英文）Study on a construction of Polar codes for a binary symmetric channel

研究代表者
岩田　賢一（Iwata, Ken-ichi）

福井大学・工学（系）研究科（研究院）・准教授

研究者番号：８０２８４３１３

交付決定額（研究期間全体）：（直接経費）　　4,200,000円、（間接経費）　　1,260,000円

研究成果の概要（和文）：Polar符号の符号構成法における計算複雑度の改善として通信路における相互情報量の解析を行い，Polar符号の構成法に関して次の結果が得られた．
(1) 2元入力対称通信路に対する近似Polar符号の構成アルゴリズムについて，符号長Nに対してO (N) の計算複雑度で提案した．
(2) (1)で用いたKurkoski と Yagiが提案した動的計画法による量子化のアルゴリズムに対して，本研究課題の問題に対しては，SMAWKアルゴリズムを利用することが可能であることを明らかにし，近似Polar符号の構成における計算複雑量の改善できることを示した．

研究成果の概要（英文）：Arikan has proposed a new class of codes, called polar codes, based on the polarization. It is expected that polar codes will provide fundamental principles for encoding and decoding techniques with low computational and space complexities for various coding problems. We have discussed about source polarization and channel polarization with approximation, and have proposed a code construction of approximation polar code by evaluating approximate value of the information in complexity linear with respect to the codeword length N. The main results are followings:
(1) A code construction method of approximation polar codes using quantizer design an algorithm was recently proposed by Kurkoski and Yagi with complexity linear for symmetric binary-input memoryless channel or binary memoryless source.
(2) An improvement of the time complexity of the quantizer design algorithm using the SMAWK algorithm for arbitrary binary-input discrete memoryless channels.

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：　情報理論　通信路符号　情報源符号　対称通信路　Polar符号

１．研究開始当初の背景

情報理論と符号理論はディジタル情報伝送の信頼性を確保するために必要不可欠な基礎理論であり，現在の情報化社会の大きな基盤を支えている．伝送する情報を，与えられた通信路を通して任意に小さな復号誤り確率で受信者に送る符号を考えるならば，通信路容量に対して任意に近い符号化率を達成するランダム符号の存在がシャノンにより示されており，その符号化と復号化における計算複雑度およびその構成方法の計算複雑度について多くの議論がなされている．

Arıkanが2009年に提案したPolar符号[1]は，符号化と復号化における低計算複雑度にも関わらず，対称通信路に対して任意に小さな復号誤り確率で理論的限界値である通信路容量を符号化率が達成することが理論的に証明された符号であり，Polar 符号は新しい概念に基づく情報源符号と通信路符号である．より具体的には，符号化および復号化の計算複雑度が符号長 N に対して O(N log N)で，任意に小さな復号誤り確率を達成するとともに符号化効率が与えられた2元対称通信路の理論的限界値である通信路容量を漸近的に達成する符号であることが証明されていた．

Arıkan は Polar 符号の構成方法について，任意精度演算の計算複雑度を定数とし，2 元消失通信路に対する計算複雑度が O(N)である符号長Nの Polar符号の構成方法を明らかにした．一方，任意の 2 元対称通信路などより一般的な対称通信路に対する符号長 N の Polar 符号の構成方法は提案されておらず，当時，今後の課題として残されていた．これに対して，森と田中[2]は密度発展法により，密度発展法の尤度密度関数の更新演算における計算複雑度を定数として，2 元対称通信路に対して計算複雑度が O(N)である符号長 N の符号構成法を提案しており，[2]では 2 元対称通信路と 2 元加法性白色ガウス雑音通信路に対して Polar 符号の性能実験結果を示した．

Polar符号はArıkan によって2009年に提案され，本研究の申請時点(2010 年)では，Polar 符号が情報源符号と通信路符号に新たな世界の展開を構築する可能性があると考えていた．さらに，Polar 符号の原理を考えれば，情報量の分極操作という新しい概念に基づいて符号化と提案されており，多端子符号化問題を含め多くの符号化問題の理論的限界を達成する符号化法を低計算複雑度と低空間複雑度で与えるある種の基本的な操作原理をもたらすことが期待していた．研究開始当初の 2010 年においても，歪みを許した情報源符号，多端子情報源符号への拡張などが提案されつつあった．

[1] E. Arıkan, ``Channel Polarization: A Method for Constructing Capacity -Achieving Codes for Symmetric Binary-Input Memoryless Channels," IEEE Transaction on Information Theory, vol.55, no.7, pp. 3051-3073, July 2009.
[2] R. Mori and T. Tanaka, ``Performance of polar codes with the construction using density evolution," IEEE Communication Letters, vol.13, no.7, pp.519-521, July 2009.

２．研究の目的

本研究の目的は，Arıkan が Polar 符号の課題として残した符号長に対して指数関数時間の計算複雑度を要する符号構成法の改善であり，任意の対称通信路に対する Polar 符号の符号構成法を多項式時間の計算複雑度で解明することが研究目的の一つである．つまり，任意に小さなブロック誤り率のもとで符号化率が理論的限界値を達成する Polar 符号の構築を多項式時間の計算複雑度で行うことであった．

具体的には，2 元入力である対称通信路に対する Polar 符号の構成に関して，森と田中の結果を発展させることで，任意精度演算の計算複雑度を定数として，与えられた 2 元入力である対称通信路に対して符号長 N の近似 Polar 符号の符号構成を計算複雑度 O(N)で与えることを本研究の目的の一つとしていた．通信路に対して符号長 N の近似 Polar 符号の符号構成を計算複雑度 O(N)で解明することは，Polar 符号の符号構成法に関する大きな進展となると考えていた．

さらに，通信路分極(channel polarization)における本研究で考えている相互情報量に関する漸化式の展開に関する洞察は，使用する通信路に対する次数拡大の概念に関する本質な研究に通じていると考えられ，通信路符号化における情報理論と符号理論にまたがる新たな世界の概念を構築する可能性を有すると考えていた．Polar 符号の原理である情報量の分極操作に関する詳細な理解と解析は情報量の分極操作は，多端子符号化問題を含め多くの符号化問題の理論的限界を達成する符号化法を低計算複雑度と低空間複雑度で与えるある種の基本的な操作原理をもたらすことが期待され，今後の情報理論と符号理論の発展においてある種の役割を果たすと考えていた．

それゆえ，情報源もしくは通信路の再帰的な可逆変換による次数の拡大と，その拡大情報源のエントロピーもしくは拡大通信路の相互情報量についてチェインルールによる条件付情報量への分解を行い，符号長を大きくした情報量の分極操作の解析も研究の目的の一つであった．

３．研究の方法

研究の目的に述べた Arıkan が Polar 符号の課題として残した符号長に対して指数関数時間の計算複雑度を要する符号構成法の改善に関して更なる改良と評価を行う方法

として，本研究では近似 Polar 符号の構成方法の提案と解析を試みた．Polar 符号の基本原理である通信路分極 (channel polarization) における相互情報量に関する漸化式の展開を解析的に理解するため，一回の Polar 変換における相互情報量に関する漸化式を 2 元対称通信路の場合に議論した．さらに，Polar 変換後の通信路の出力アルファベットの大きさが符号長の多項式程度に制限した場合に相互情報量の範疇で近似することを提案した．さらに，一般の 2 元入力である対称通信路に関しては，与えられた通信路に対して，相互情報量が等価である 2 元対称通信路の重み和に分解し，さらに，各 2 元対称通信路に対して，上記の近似を行うことを提案した．さらに，通信路分極に対比して，無歪み情報源符号の構成においても情報源分極(source polarization)を考え，情報源分極における Polar 変換における情報量による漸化式による展開を考え，その近似を提案した．さらに，本研究では，情報量および相互情報量の近似を行うアルゴリズムにおいてある種の最適性を保証するとともに高速化について考え，SMAWK アルゴリズムを利用したアルゴリズムを提案した．

これらの通信路に相互情報量の 2 元対称通信路の重み和分解とその漸化式と近似の組み合わせにより，符号長に対して線形時間で構成可能な近似 Polar 符号の構成法を提案した．さらに，提案した近似 Polar 符号における復号誤り率に対して計算機実験を行い，その有用性を確認した．

また，これらの研究において，符号器と復号器における演算回数の最適化を考えた結果，ハミング符号における符号化と復号化における演算回数の削減および BCH 符号における復号化における演算回数の削減について検討した．

４．研究成果

(1)．まず，2 元入力対称通信路に対する近似 Polar 符号の構成アルゴリズムについて，符号長 N に対して O (N) の計算複雑度で提案した．

Arikan は 2 元入力無記憶通信路の対称通信路容量を符号長 N とともに計算量 O(N log N) の符号化および復号化で達成する Polar 符号を 提案した．Arikan の提案した Polar 符号では符号の構成には符号長に対して指数関数時間の計算複雑度を要する．Polar 符号の符号構成 法における計算複雑度の改善として通信路における相互情報量の解析を行い，Polar 符号の構成法に関して次の結果が得られた．

① Polar 符号を構成するときに与えられた 2 元入力対称通信路に対する通信路結合(channel combining)と通信路分解(channel splitting)を操作した通信路における相互情報量の考察を行い，Polar 変換に対して，与えられた 2 元入力対称通信路の Polar 変換と同じ通信路容量を有する別の 2 元対称通信路の結合の形式における再帰式を導き，発表論文等の学科発表⑩と⑪にまとめた．

② 上記の (1) の①で導いた channel combining と channel splitting による Polar 変換の操作した通信路と同じ通信路容量を有する別の 2 元対称通信路の結合の形式において，Kurkoski と Yagi が提案した動的計画法[3]を適用した通信路容量の近似を述べ，Polar 符号の近似を用いた構成法を提案し，発表論文等の学科発表⑨にまとめ発表した．

③．さらに，上記の(1)．の②の拡張として，一般の 2 元入力である対称通信路である場合への拡張を考えた結果，与えられた一般の 2 元入力である対称通信路に対して，相互情報量が等価である 2 件対称通信路の重み和による分解を考え，分解したそれぞれの 2 元対称通信路に対して，上記の(1)の②を行うことで，一般の 2 元入力である対称通信路に対する近似 Polar 符号の構成アルゴリズムの提案を符号長 N に対して O(N)で提案し，発表論文等の学科発表⑨にまとめ発表した．

④ Polar 符号の符号構成における基礎的な原理の1つとして情報量の分極操作があり，情報源もしくは通信路の再帰的な可逆変換による次数の拡大構成とチェインルールによる条件付情報量への分解を行い，符号長を大きくした極限において情報量の分極操作が可能であることを解説し，情報量の分極操作は多端子符号化問題を含め多くの符号化問題の理論的限界を達成する符号化法を低計算複雑度と低空間複雑度で与える基本的な 1 つの原理をもたらすことが期待されることを発表論文等の雑誌論文①の一部に述べた．

(2)．2 元無記憶情報源に対する近似 Polar 符号の構成アルゴリズムについて，入力長 N に対して O(N) の計算複雑度で提案した．

① (1)で述べた 2 元入力対称通信路に対する通信路結合(channel combining)と通信路分解(channel splitting)を考察と対比して，2 元無記憶情報源に対する Polar 符号の構成に関して，同様に再帰式を述べ，その近似手法を提案し，発表論文等の雑誌論文①の一部にまとめた．

② 固定長の情報源符号化と通信路符号化について，polar 符号の C プログラミングよる例を紹介するとともに計算機実験結果を発表論文等の雑誌論文①の一部にまとめた．

(3) (1)の近似 Polar 符号の構成法の提案で用いた Kurkoski と Yagi が提案した動的計画法[3]による量子化のアルゴリズムに対して，SMAWK アルゴリズム[4]を用いた計算複雑量の改善を提案した．

① Kurkoski と Yagi が提案した動的計画法による量子化のアルゴリズムに対して，

本研究課題の問題に対しては,SMAWK アルゴリズムを利用することが可能であることを明らかにし,Polar 符号の構成における計算複雑量の改善できることを示した．この内容を明確にし，発表論文等の学科発表⑥にまとめ発表した．さらに，2014 IEEE International Symposium on Information Theory において発表予定である(発表論文等の学科発表①).

(4) Polar 符号の効率的な構成法に関連して,ハミング符号における並列符号化と並列復号化における高速な回路構成について効率的な構成法のある種の最適化に関する研究を行った．さらに，ハミング符号における並列復号化における効率的かつ高速な回路の構成法の応用として，BCH 符号の並列復号化に関して研究を行った.

① まず,2 元ハミング符号について,並列符号器と並列復号器における XOR 演算回数に関して評価し，ハミング符号の情報点数の 2 倍程度の XOR 演算回数で並列符号器と並列復号器が構成できることを明らかにした(発表論文等の学科発表⑧)．さらに，拡大ハミング符号の場合について，発表論文等の学科発表⑦に述べた.

② (4)の①の内容を 2 元から q 元への拡張について，発表論文等の学科発表④と⑤に述べた.

③ (4)の①のハミング符号の並列復号器に関して,2 元 BCH 符号への応用を考え,BCH 符号の並列シンドローム計算に要する XOR 演算回数について，発表論文等の学科発表③に述べた．さらに,q 元 BCH 符号の場合への拡張を考え，発表論文等の学科発表②に述べた.

[3] B. M. Kurkoski, H. Yagi, ``Quantization of binary-input discrete memoryless channels, with applications to LDPC decoding,'' Submitted to IEEE Transactions on Information Theory, 2011.Available from http://arxiv.org/abs/1107.5637.

[4] A. Aggarwal, M.M. Klawe, S. Moran, P. Shor, and R. Wilber, ``Geometric applications of a matrix-searching algorithm,'' Algorithmica, vol.2, no.2, pp. 195-208, Nov., 1987.

５．主な発表論文等

〔雑誌論文〕（計 1 件）

① 岩田 賢一, Polar 符号の紹介 -C プログラミングによる Polar 符号の体験-, 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, 校閲有り, Vol.6, No.3, 2013, pp.175-198, http://dx.doi.org/10.1587/essfr.6.175

〔学会発表〕（計 11 件）

① Ken-ichi Iwata, Shin-ya Ozawa, Quantizer design for outputs of binary-input discrete memoryless channels using SMAWK algorithm, 2014 IEEE International Symposium on Information Theory, pp.191-195, 2014 年 6 月 29 日～7 月 4 日, Honolulu Hawaii, USA.

② 岩田 賢一, 大島 怜也, 原始 BCH 符号の並列シンドローム計算におけるある種の方法，電子情報通信学会情報理論研究会，2014 年 5 月 16 日,大分県別府市

③ 大島 怜也, 岩田 賢一, 原始 BCH 符号の並列シンドローム計算に要する XOR 演算の回数について, 電子情報通信学会 2014 総合大会, 2014 年 3 月 18 日～3 月 21 日, 新潟大学(新潟市)

④ 大島 怜也, 岩田 賢一, q 元ハミング符号の並列復号器における演算回数について，電子情報通信学会情報理論研究会，2013 年 9 月 27 日，沖縄県宜野湾市

⑤ 大島 怜也, 岩田 賢一, q 元ハミング符号の並列復号器における演算回数について，電子情報通信学会 2013 年総合大会，2013 年 3 月 18 日～3 月 21 日，岐阜大学(岐阜県)

⑥ 岩田 賢一, 小澤 伸也, 2 元入力離散無記憶通信路の出力に対する量子化アルゴリズムの SMAWK アルゴリズムを用いた高速化，電子情報通信学会情報理論研究会，2013 年 5 月 24 日，福井県あわら市

⑦ 岩田 賢一, 大島 怜也, 拡大ハミング符号の並列復号器における XOR 演算回数について，電子情報通信学会第 35 回情報理論とその応用シンポジウム, 2012 年 12 月 11 日～12 月 14 日，大分県別府市

⑧ 大島 怜也, 岩田 賢一, ハミング符号の並列符号器と並列復号器における XOR 演算回数の最適化，電子情報通信学会情報理論研究会，2012 年 9 月 28 日，群馬県

⑨ 鈴木 佑輔, 岩田 賢一, 2 入力対称通信路における近似 Polar 符号の動的計画法を用いた符号構成に関する考察，電子情報通信学会情報理論研究会，2012 年 1 月 20 日，筑波大学

⑩ 岩田 賢一, 鈴木 佑輔, 相互情報量からみるポーラ符号の紹介，電子情報通信学会 2011 年ソサイエティ大会，2011 年 9 月 15 日，北海道大学

⑪ Ken-ichi Iwata, Yusuke Susuki, Construction of Approximate Polar Codes on Binary Symmetric Channels, 7th Asia- Europe Workshop on Concepts in Information Theory, 2011 年 7 月 28 日，Boppard, Germany

〔産業財産権〕
○出願状況（計１件）

名称：符号化・復号化装置及び演算回路設定方法
発明者：岩田 賢一，福間 慎治，大島 怜也
権利者：同上
種類：特許
番号：特許第 2012-206395 号
出願年月日：2012 年 9 月 19 日
国内外の別： 国内

６．研究組織
(1)研究代表者
岩田　賢一（IWATA KEN-ICHI）
福井大学・大学院工学研究科・准教授
研究者番号：８０２８４３１３

(2)研究分担者
該当無し

(3)連携研究者
該当無し