古典–量子通信における Polar 符号による相互情報量に関する研究

岩田 直樹　　指導教員：臼田 毅

1 はじめに

Polar 符号は Arikan によって提案された通信路符号化法で，逐次除去復号との組み合わせにより符号長無限の極限において通信路容量を達成するため，注目されている [1]．最近，古典–量子通信路でも同様の結果が示された [2]．本論文では，Polar 符号の符号長が有限である場合について，量子最適復号を用いて相互情報量を計算するときに発生する計算量増大の問題を解決するために，扱う符号のクラスを固定し簡単化公式の導出を行うことで相互情報量計算の計算量を削減し，Polar 符号の量子利得特性の解明をする．

2 相互情報量公式

本論文では，古典–量子通信における符号化の量子利得特性を調べるために相互情報量の計算を行っている．しかし，相互情報量の計算は符号語数の増大により計算量が膨大になってしまい，困難になる．ここでは，その増大する計算量を抑えるために用いられている相互情報量公式 [3] について紹介する．

まず，2 元線形符号を用いて符号語状態を構成した場合，線形符号の群共変性から相互情報量は以下のようになる．

$$I(X^n;Y^n) = \log M + \sum_{j=0}^{M-1} P(j|0)\log P(j|0) \tag{1}$$

ここで，M は符号語数である．これにより，相互情報量は通信路行列の 0 行目 $P(j|0) = |(\Gamma)^{\frac{1}{2}}_{0,j}|^2$ を計算すれば求めることができる．また，$(\Gamma)^{\frac{1}{2}}_{0,j}$ に対しては以下の公式が成立する．

$$(\Gamma)^{\frac{1}{2}}_{0,j} = \frac{1}{M}\sum_{k=0}^{M-1}(-1)^{w_{\mathrm{H}}(j\cdot k)}\sqrt{\sum_{l=0}^{M-1}(-1)^{w_{\mathrm{H}}(k\cdot l)}\kappa^{w_{\mathrm{H}}(\boldsymbol{v}_l)}} \tag{2}$$

ここで，$\kappa = \langle 0|1\rangle$ でレター状態 0 と 1 の内積を表し，$w_{\mathrm{H}}(i)$ は i を 2 進数で表したときのハミング重みを表す．

以上が相互情報量公式と呼ばれており，この式を用いた場合に計算量が $O(M^3)$ 程度に抑えられる．しかし，これを用いても計算が困難なサイズの符号が存在し，そのような符号に対しては，扱う符号の符号語の重みと情報記号系列の対応がとれていれば，さらに計算量を抑えた簡単化公式を導出することができる．この簡単化公式を導出できれば，計算量を符号の持つ重みの種類程度の計算量に抑えることができる．次節では，簡単化公式導出のために扱う符号の性質について触れる．

3 $(2^m,m+2)$Polar 符号

Polar 符号は符号長が 2 の整数べき乗の符号であり，再帰的に構成可能である．符号長 2^n の Polar 符号の生成行列 G_{2^m} は

$$G_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \tag{3}$$

$$G_{2^m} = (I_{2^{m-1}} \otimes G_2)R_{2^m}(I_2 \otimes G_{2^{m-1}}), \tag{4}$$

と定義される．ただし，R_{2^m} は

$$\begin{aligned}&(x_0,x_1,\cdots,x_{2^m-1})R_{2^m}\\ &\quad = (x_0,x_2,\cdots,x_{2^m-2},x_1,x_3,\cdots,x_{2^m-1}),\end{aligned} \tag{5}$$

と定義される置換行列である．

式 (4) で定義された生成行列 G_{2^m} は $2^m \times 2^m$ の行列なので符号化率は 1 になる．そのため，Polar 符号では入力ビットのいくつかの成分を 0 と決める．このように，成分 0 と決めたビットを凍結ビットと言う．本論文で扱う $(2^m,m+2)$Polar 符号は，生成行列の行成分に 1 が少ない行と対応する入力ビットを凍結ビットとし，成分 1 と決めた情報伝送に用いるビットが $m+2$ ある符号である．

$(2^m,m+2)$Polar 符号は，重み分布と各重みの符号語に対応する情報記号系列を求めることができ，修士論文においてはどちらも導出している．本稿では，紙面の都合上，導出した重み分布の結果のみを示す．

$$\begin{aligned} A_0 &= 1\\ A_{2^{m-2}} &= 4\\ A_{2^{m-1}} &= 2^{m+2}-10\\ A_{3\cdot 2^{m-2}} &= 4\\ A_{2^m} &= 1\end{aligned} \tag{6}$$

ここで，A_n は重み n の符号語の総数を示す．式 (6) の通り，$(2^m,m+2)$Polar 符号は重みの種類は 5 種類で固定となる．これは非常に簡単な構造を持つ符号であり，本論文中では，情報記号系列との対応も与えているため，$(2^m,m+2)$Polar 符号は簡単化公式が導出可能な符号だと言える．

4 相互情報量の簡単化公式

簡単化公式とは，相互情報量公式の計算量をさらに抑えた計算式のことで，符号語の重みと情報記号系列の対応が分かっている符号を相互情報量公式に適用することで得られる計算式である．簡単化公式を導出すると，符号語数が 2^{1000} のような非常に大きな符号に対しても計算を与えることができる．

今回扱う $(2^m,m+2)$Polar 符号に関しても，前節より重み分布が分かっており，さらにそれを導出する過程で情報記号系列の対応も分かっているため，簡単化公式の導出が可能である．本稿では証明の過程は省略するが，以下に $(2^m,m+2)$Polar 符号の簡単化公式を示す．

$$\begin{aligned} I(X;Y) = {}& m+2+f_0\log f_0+4f_1\log f_1+(2^{m+2}-16)f_2\log f_2\\ &+6f_3\log f_3+4f_4\log f_4+f_5\log f_5,\end{aligned} \tag{7}$$

$$\begin{aligned} f_0 = {}& \Big\{\frac{1}{2^{m+2}}\big(r_0+2^m r_1+(2^{m-2}-1)r_2\\ &+3\cdot 2^{m-1}r_3+2^m r_4+2^{m-2}r_5\big)\Big\}^2,\\ f_1 = {}& \Big\{\frac{1}{2^{m+2}}\big(r_0-2^{m-1}r_1+(2^{m-2}-1)r_2\\ &+2^{m-1}r_4-2^{m-2}r_5\big)\Big\}^2,\\ f_2 = {}& \Big\{\frac{1}{2^{m+2}}\big(r_0-r_2\big)\Big\}^2,\\ f_3 = {}& \Big\{\frac{1}{2^{m+2}}\big(r_0+(2^{m-2}-1)r_2-2^{m-1}r_3+2^{m-2}r_5\big)\Big\}^2,\\ f_4 = {}& \Big\{\frac{1}{2^{m+2}}\big(r_0+2^{m-1}r_1+(2^{m-2}-1)r_2\\ &-2^{m-1}r_4-2^{m-2}r_5\big)\Big\}^2,\\ f_5 = {}& \Big\{\frac{1}{2^{m+2}}\big(r_0-2^m r_1+(2^{m-2}-1)r_2\\ &+3\cdot 2^{m-1}r_3-2^m r_4+2^{m-2}r_5\big)\Big\}^2,\end{aligned}$$

$$r_0 = \sqrt{1+4\kappa^{2^{m-2}}+(2^{m+2}-10)\kappa^{2^{m-1}}+4\kappa^{3\cdot 2^{m-2}}+\kappa^{2^m}},$$
$$r_1 = \sqrt{1+2\kappa^{2^{m-2}}-2\kappa^{3\cdot 2^{m-2}}-\kappa^{2^m}},$$
$$r_2 = \sqrt{1+4\kappa^{2^{m-2}}-10\kappa^{2^{m-1}}+4\kappa^{3\cdot 2^{m-2}}+\kappa^{2^m}},$$
$$r_3 = \sqrt{1-2\kappa^{2^{m-1}}+\kappa^{2^m}},$$
$$r_4 = \sqrt{1-2\kappa^{2^{m-2}}+2\kappa^{3\cdot 2^{m-2}}-\kappa^{2^m}},$$
$$r_5 = \sqrt{1-4\kappa^{2^{m-2}}+6\kappa^{2^{m-1}}-4\kappa^{3\cdot 2^{m-2}}+\kappa^{2^m}}.$$

以上が $(2^m,m+2)$Polar 符号における相互情報量の簡単化公式である．$(2^m,m+2)$Polar 符号はどれだけ符号のサイズを大きくしても重みの種類が増えず，グラム行列の固有値の種類も 6 種類で固定されるため，計算量は定数オーダーとなる．このことより，符号のサイズによらない計算量で相互情報量を求めることが可能となった．

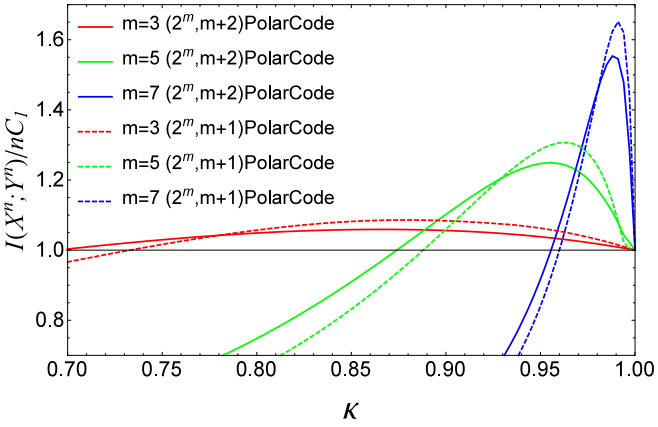

図 1　$(2^m,m+2)$Polar 符号の相互情報量と C_1 との比

5　量子利得特性

前節に示した簡単化公式を用いて $(2^m,m+2)$Polar 符号の量子利得特性について議論をする．図 1 は $m=3,5,7$ において $(2^m,m+2)$Polar 符号と，先行研究において既に簡単化公式の導出がなされている $(2^m,m+1)$Polar 符号 [4] を比較した図である．結果を見ると，符号長が短い符号で 8 しかないが，符号長 1 の通信路容量 C_1 を超え量子利得が得られているのが見てとれる．また，この図で計算しているサイズにおいては $(2^m,m+1)$Polar 符号の方が量子利得の最大値が高い値を示している．しかし，量子利得が得られる範囲は $(2^m,m+2)$Polar 符号の方が僅かに広いことも見てとれる．量子利得の得られる範囲は m の値を大きくするにつれて両符号間の差は狭まっていくが，$m=30$ まで計算した範囲においては $(2^m,m+2)$Polar 符号が常に広い範囲で得られていることが分かった．

また，量子通信路容量 C への達成度を測るために，[3] から以下のような式 AF を導入する．

$$AF = \max_{\kappa} \frac{I(X^n;Y^n)/n - C_1}{C - C_1}. \tag{8}$$

AF は 1 に近い値ほど量子通信路容量に近づいていることを示す指標である．この指標を用いた結果を表 1 に示す．表 1 から，$(2^m,m+2)$Polar 符号は $(2^m,m+1)$Polar 符号と同様に高い達成度を示す符号であることが分かった．また，今回比較対象とした $(2^m,m+1)$Polar 符号は 1 次の Reed-Muller 符号と同じ形となる符号であることも分かっており，先行研究において Simplex 符号を上回る高い量子利得特性を示す符号であることも示されている符号であるので，そのような符号と同等な量子利得特性を示す $(2^m,m+2)$Polar 符号は，符号長が有限という制限を受ける条件でも良い性能を示す符号であることが示すことができた．

6　まとめ

本論文では，Polar 符号の量子利得特性を考察するために，特性の Polar 符号クラスにおける相互情報量の簡単化公式の導出と通信路容量への達成度の評価を行った．

$(2^m,m+2)$Polar 符号における相互情報量の簡単化公式の導出と通信路容量への達成度の評価は，簡単化公式を与えることで，定数オーダーに近い計算量で相互情報量を与えることができ，サイズを大きくしても計算ができるようになった．また，$(2^m,m+2)$Polar 符号は $(2^m,m+1)$Polar 符号に対して，通信路容量の達成度は劣ってしまうが，量子利得が得られる κ の範囲は広くなるという一長一短の性質を持つ符号であることが分かり，通信の環境や目的に応じて使い分けられる選択肢を与えることができた．

しかしながら，本稿において調べた Polar 符号は Polar 符号クラス全体のごく一部分のクラスに過ぎず，Polar 符号クラス全体を調べるためにも，さらに簡単化公式の導出例を増やすこと，また，符号語の重みと情報記号系列の対応が取れない符号に対しても相互情報量の計算を少ない計算量で実現できるような計算手法を与えることが課題に挙げられる．

参考文献

[1] E. Arikan, IEEE Trans. Inf. Theory **55**, pp.3051-3073, (2009).
[2] M. M. Wilde, S. Guha, IEEE Trans. Inf. Theory **59**, pp.1175-1187, (2013).
[3] S. Usami, T.S. Usuda, I. Takumi, and M. Hata, IEICE Trans. Fundamentals. **E82-A**, pp.2178-2184, (1999).
[4] 石田雄樹, 他, 電学論 (C), **126**, no.12, pp.1474-1482, (2006).

公表論文

[1] **N. Iwata** and T. S. Usuda, ISITA2014, Proceedings of ISITA2014, pp.250-253, (2014.10).
[2] **岩田直樹**, 臼田毅, SITA2015, 岡山, pp.367-372, (2015.11).
[3] **岩田直樹**, 臼田毅, 2014 年電子情報通信学会ソサイエティ大会, 徳島大学, A-6-4, (2014.9).

他 8 件

表 1　通信路容量への達成度

m	3	5	7	10	15	20	25	30
$(2^m,m+1)$Polar 符号	0.09	0.21	0.30	0.40	0.51	0.59	0.64	0.68
$(2^m,m+2)$Polar 符号	0.07	0.18	0.27	0.37	0.48	0.56	0.62	0.66