Polar 符号とその研究動向

森 立平

京都大学 大学院 情報学研究科

2011 年 11 月 30 日

Contents

- Polar 符号と通信路分極現象 [Arıkan 2008]
- Polar 符号に関する研究紹介 I(polar 符号の性質)
    1. Polar 符号の漸近的誤り確率 [Arıkan and Telatar 2008]
    2. Polar 符号の $\ell \times \ell$ 行列への一般化 [Korada, Şaşoğlu, and Urbanke 2009]
    3. 密度発展法を用いた polar 符号の構成 [Mori and Tanaka 2009]
    4. Polar 符号の compound capacity [Hassani, Korada, and Urbanke 2009]
    5. 多元 (素体) polar 符号 [Şaşoğlu, Telatar, and Arıkan 2009]
    6. 多元 (一般の有限体) polar 符号と Reed-Solmon 行列 [Mori and Tanaka 2010]
    7. Polar 符号のより詳細な漸近的誤り確率 [Tanaka and Mori 2010] [Hassani and Urbanke 2010] [Hassani, Mori, Tanaka, and Urbanke 2011]
    8. Polar 符号の誤り確率のスケーリング [Korada, Montanari, Telatar, and Urbanke 2010] [Hassani, Alishahi, and Urbanke 2010]
    9. Polar 符号の重み分布 [Mori and Urbanke]
- Polar 符号に関する研究紹介 II(復号法とアプリケーション)

Polar 符号と通信路分極現象

Polar 符号とは

Polar 符号 [Arıkan 2008] とは

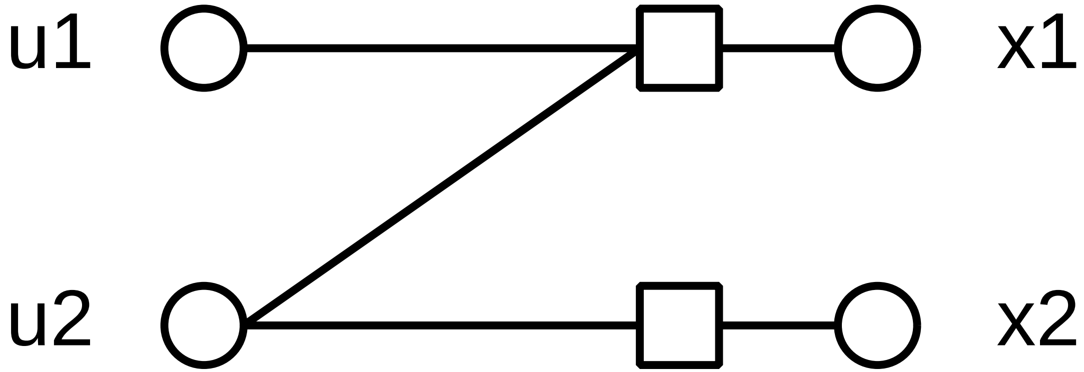
- 任意の二元離散無記憶通信路 (B-DMC)W で対称通信路容量 $I(W)$ を達成することが証明されている
- 符号化、復号の計算量が $O(N \log N)$ (N は符号長)
- 任意の $R < I(W)$ と $\epsilon > 0$ について、$P_e = o\left(2^{-N^{\frac{1}{2}-\epsilon}}\right)$

B-DMC W の対称通信路容量 $I(W)$

$$I(W) := \sum_{y \in \mathcal{Y}} \sum_{x \in \mathcal{X}} \frac{1}{2} W(y \mid x) \log \frac{W(y \mid x)}{\frac{1}{2}W(y \mid 0) + \frac{1}{2}W(y \mid 1)}$$

Polar符号の生成行列

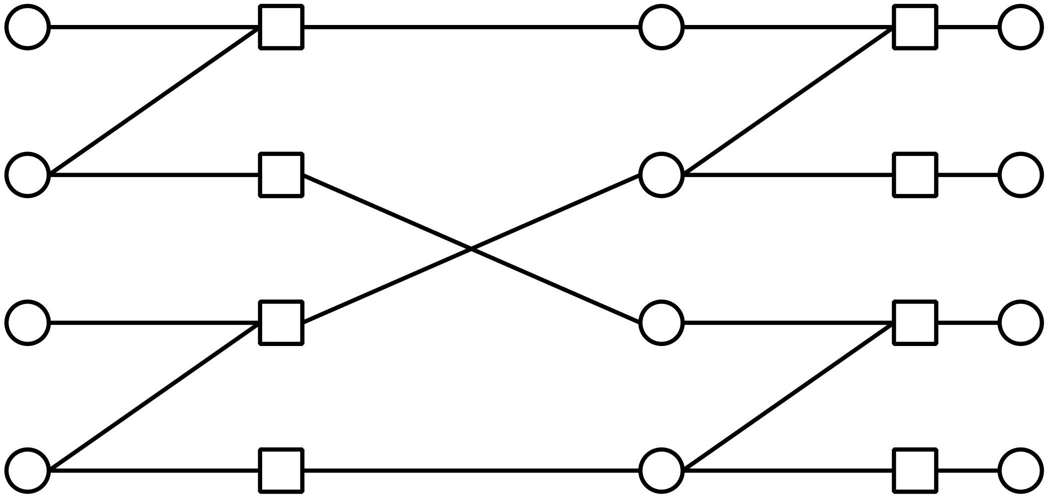
$$G_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$



$$\begin{bmatrix} u_1 & u_2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} x_1 & x_2 \end{bmatrix}$$

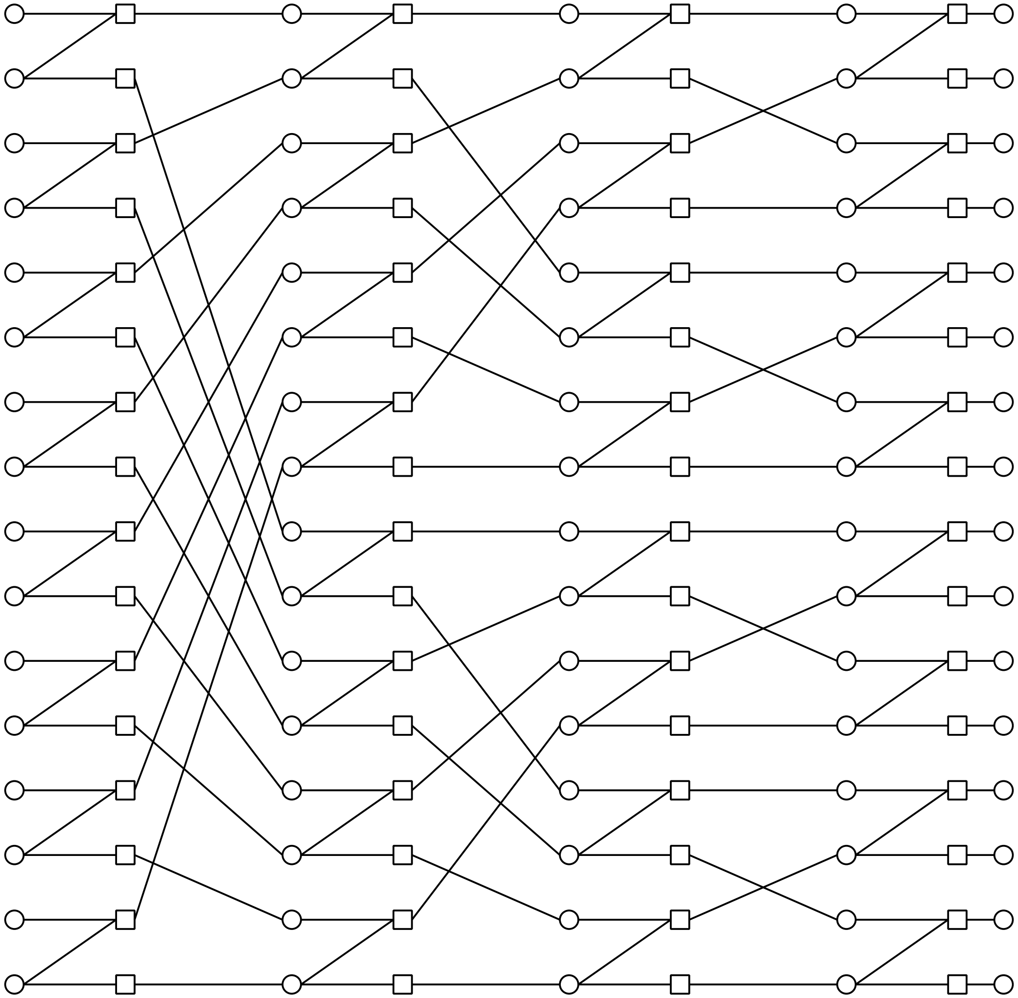
Polar 符号の生成行列

$$G_4 = \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix} \begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} \end{bmatrix}^{\otimes \mathbf{2}} = \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{bmatrix}$$

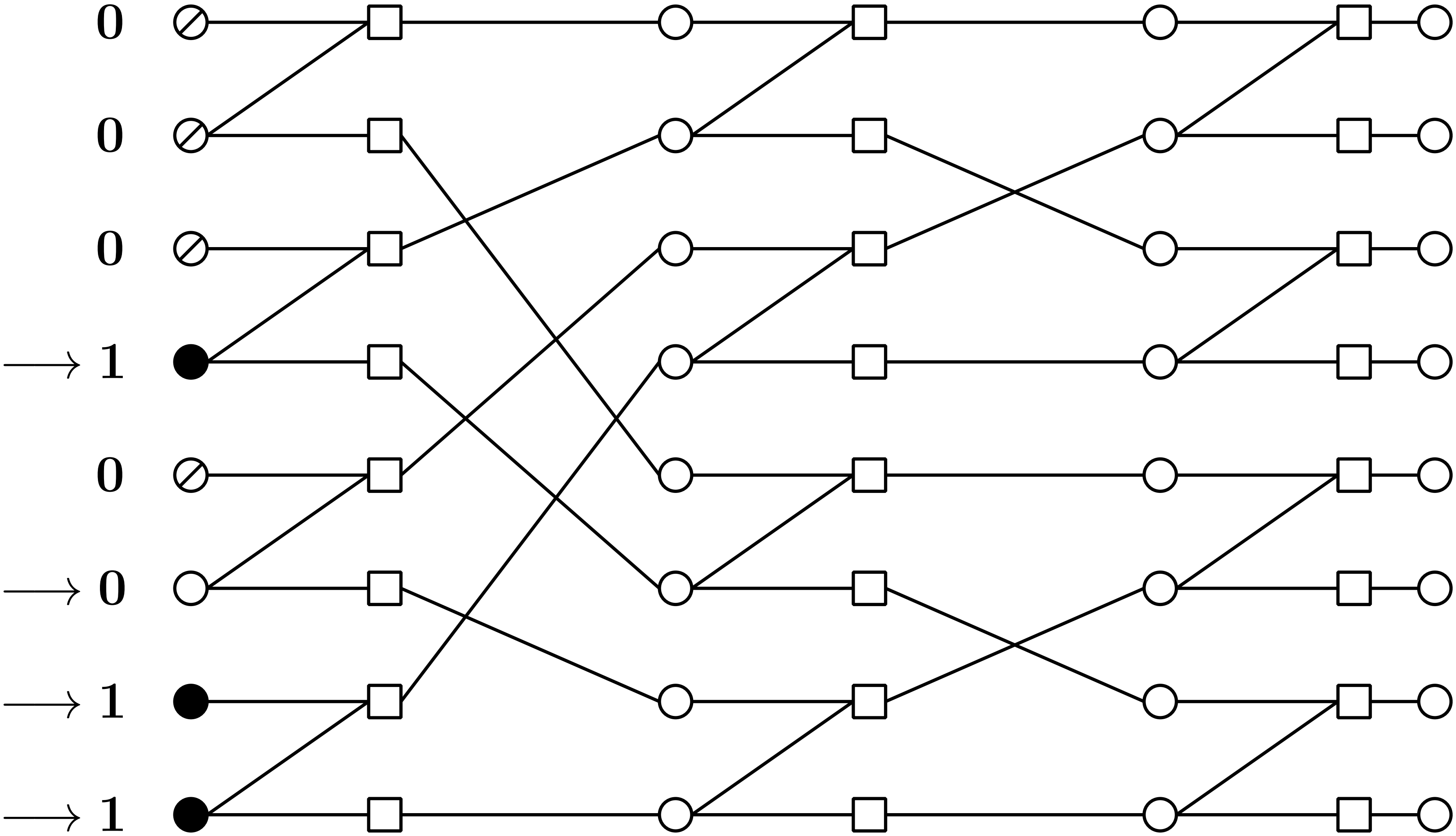


Polar 符号の生成行列

$$G_{\mathbf{2}^n} = (I_{\mathbf{2}^{n-1}} \otimes G_{\mathbf{2}}) R_{\mathbf{2}^n} (I_{\mathbf{2}} \otimes G_{\mathbf{2}^{n-1}}) = B_{\mathbf{2}^n} G_{\mathbf{2}}^{\otimes n}$$

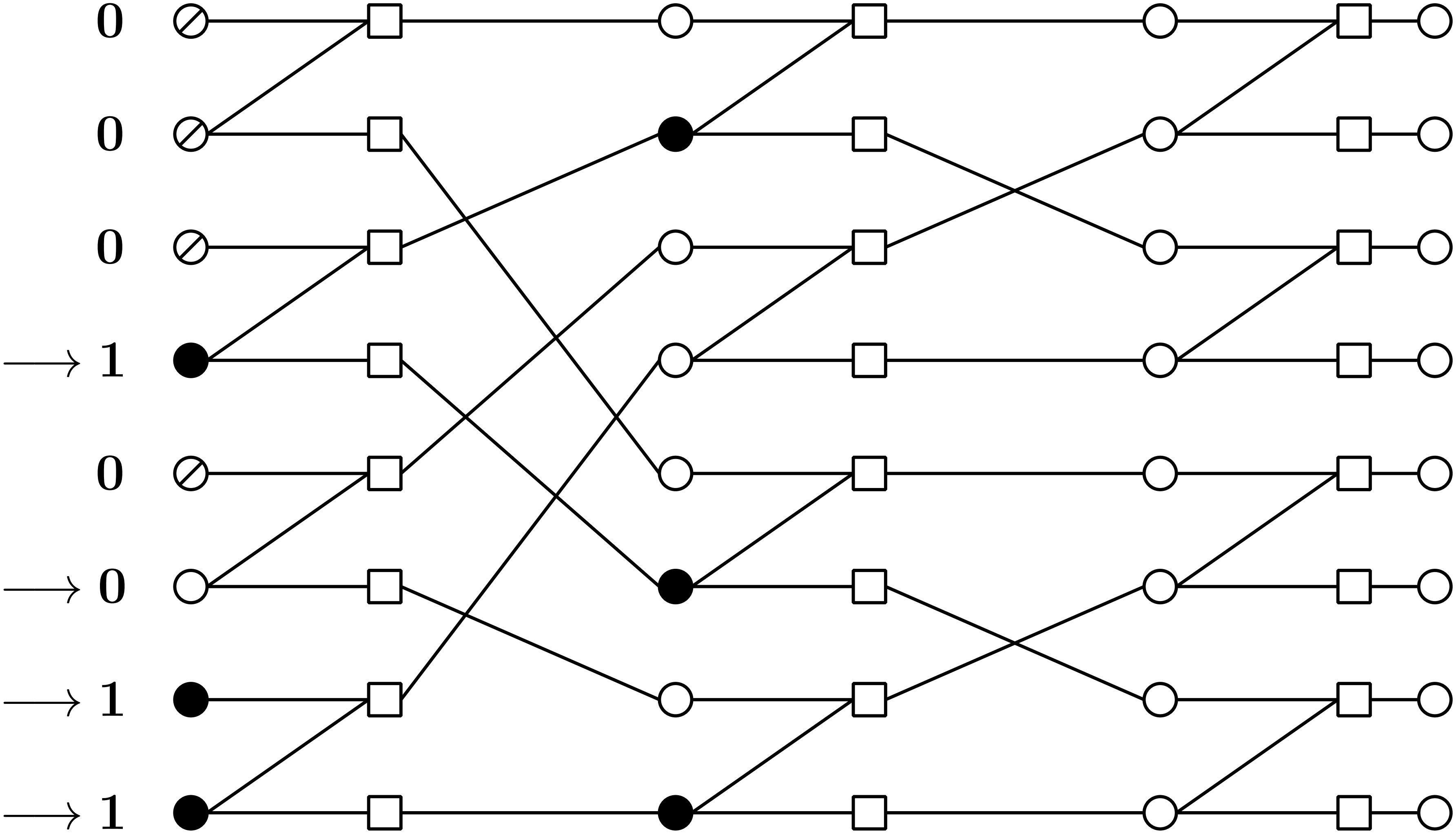


Polar 符号の符号化



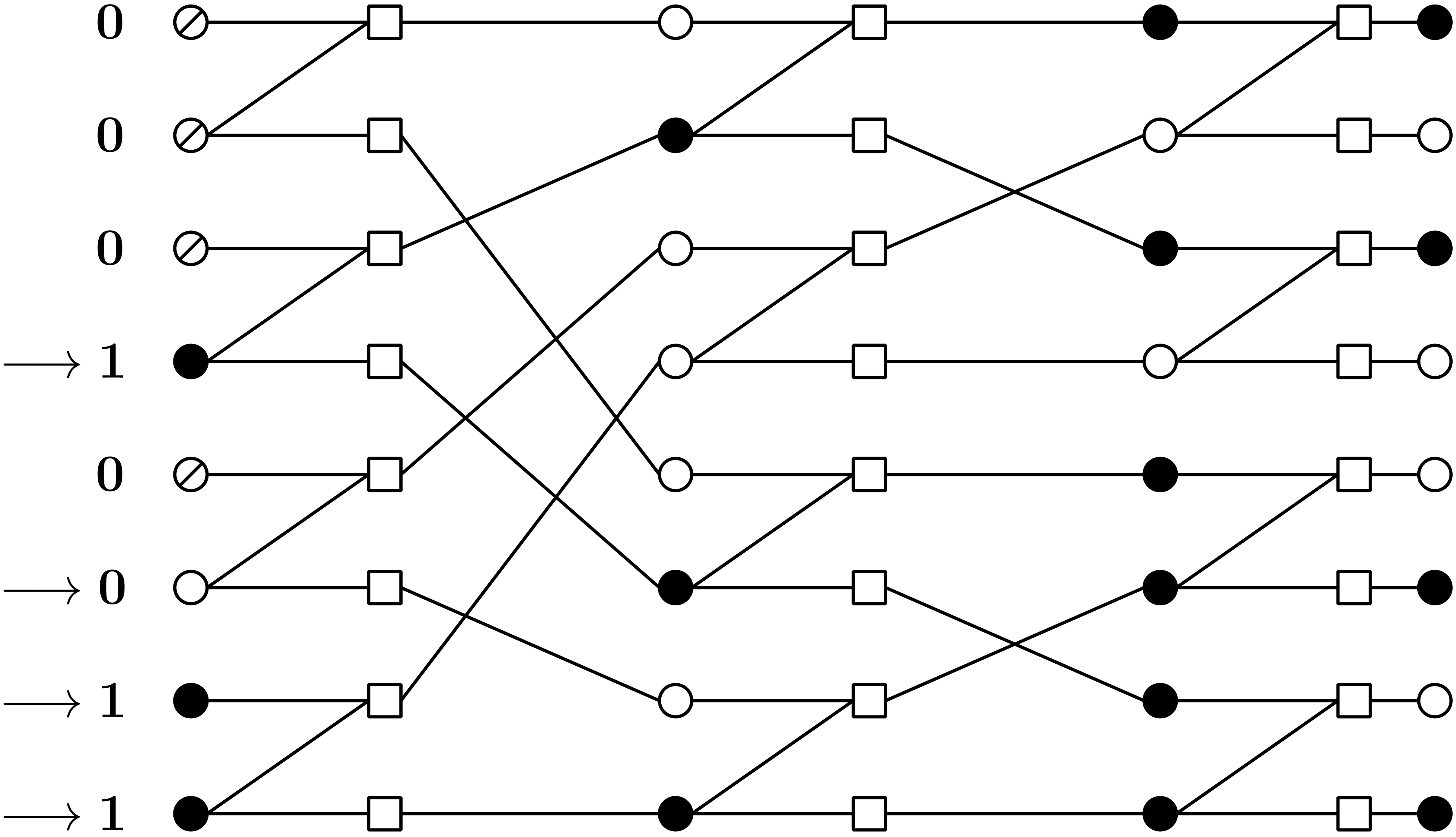
⊘ : 凍結ビット

Polar 符号の符号化



⊘ : 凍結ビット

Polar 符号の符号化



符号化の計算量 $\propto$ チェックノードの数 $= O(N \log N)$

Polar 符号の復号

Succesive cancellation (SC) decoding
インデックスが小さなビットから順番に硬判定

F: 凍結ビットのインデックスの集合

$i \in F$ のとき

$$\hat{U}_i(y_1^N, \hat{u}_1^{i-1}) = 0$$

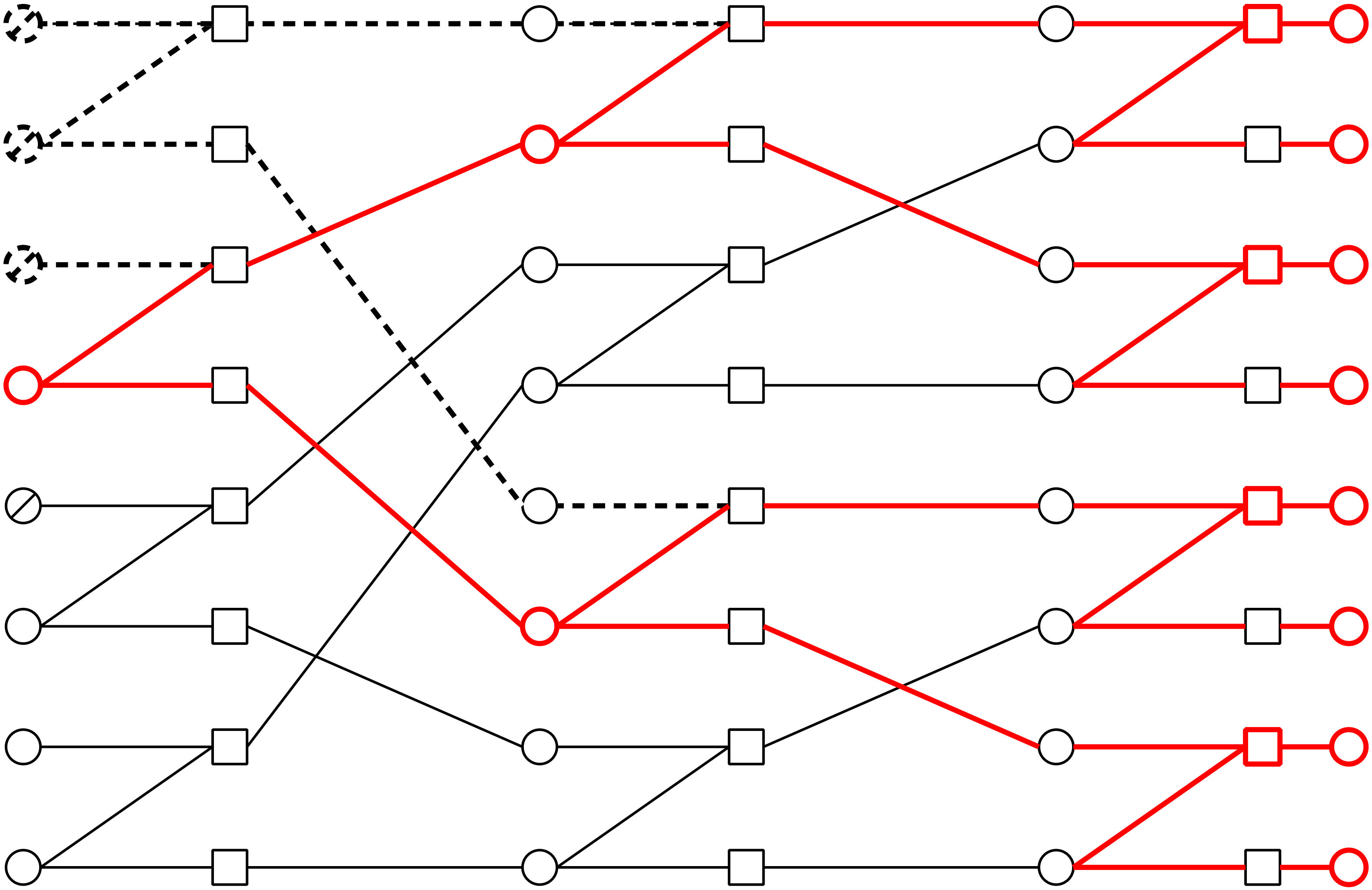
$i \notin F$ のとき

$$\hat{U}_i(y_1^N, \hat{u}_1^{i-1}) = \operatorname*{argmax}_{u_i=0,1} W_N^{(i)}(y_1^N, \hat{u}_1^{i-1} \mid u_i)$$

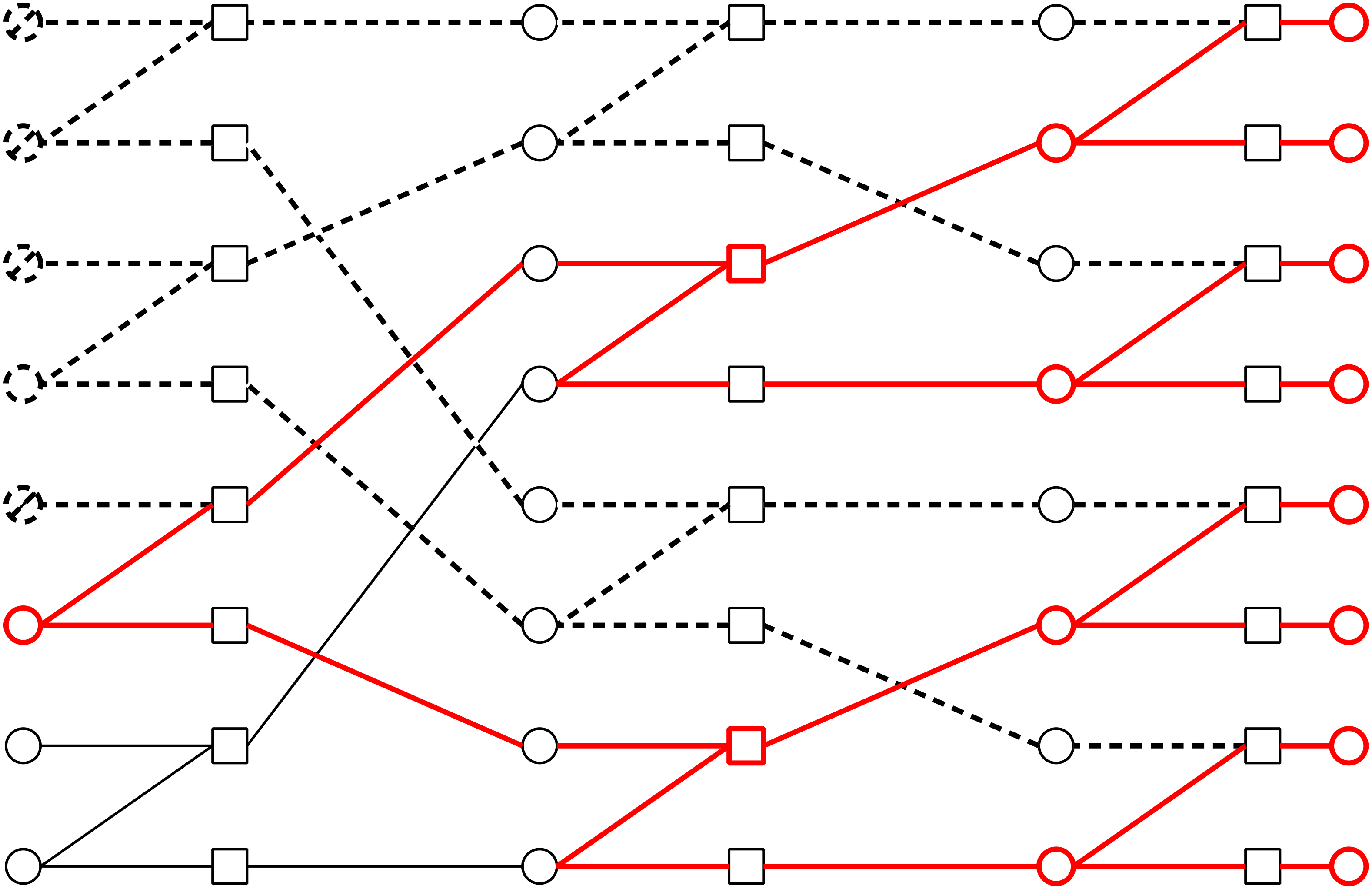
$W_N^{(i)}$ は i 番目のサブチャネル

$$W_N^{(i)}(y_1^N, u_1^{i-1} \mid u_i) := \frac{1}{2^{N-1}} \sum_{u_{i+1}^N} W^N(y_1^N \mid u_1^N G_N).$$

Polar 符号の復号



Polar 符号の復号



木の上で ML$\Longleftrightarrow$ belief propagation (BP) で計算可能

疑問

- 何故これで対称通信路容量を達成できるのか?
- どのビットを情報ビットとして選べばよいのか

↓

分極現象

分極現象

- (U_1^N, Y_1^N): $W^N(y_1^N \mid u_1^N G_N)/2^N$ に従う確率変数

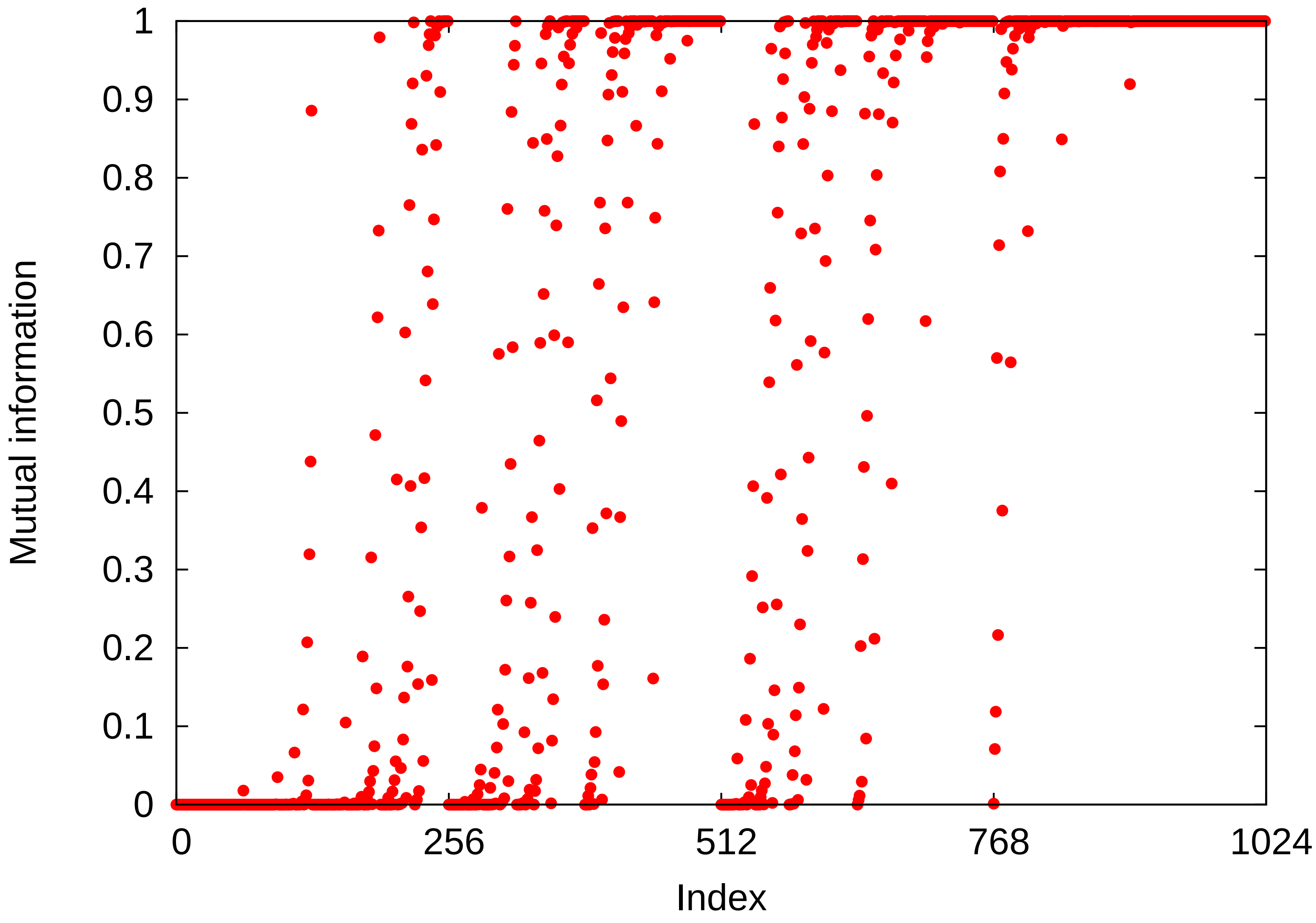
$$NI(W) = I(U_1^N; Y_1^N) = \sum_{i=1}^{N} I(Y_1^N, U_1^{i-1}; U_i) = \sum_{i=1}^{N} I(W_N^{(i)})$$

このとき右辺の N 個の相互情報量は
ほぼ 0 のものと、ほぼ 1 のものに分極

$$\lim_{N\to\infty} \frac{\left|\left\{i \in \{1, \dots, N\} \mid \epsilon < I(W_N^{(i)}) < 1-\epsilon\right\}\right|}{N} = 0$$

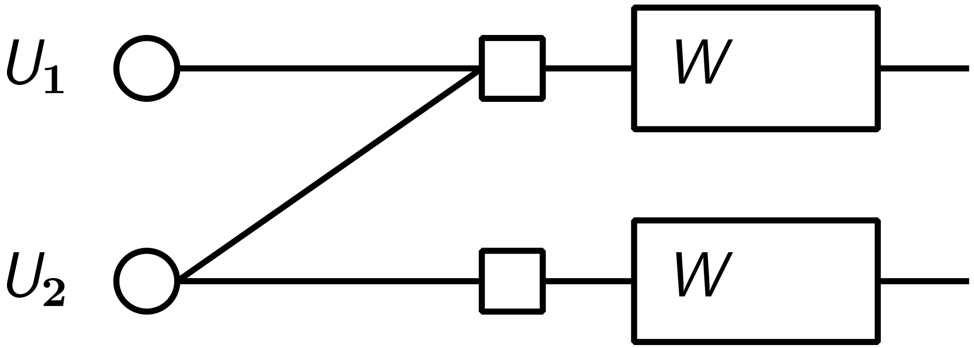
ほぼ 1 のものは $NI(W)$、ほぼ 0 のものは $N(1 - I(W))$

分極現象

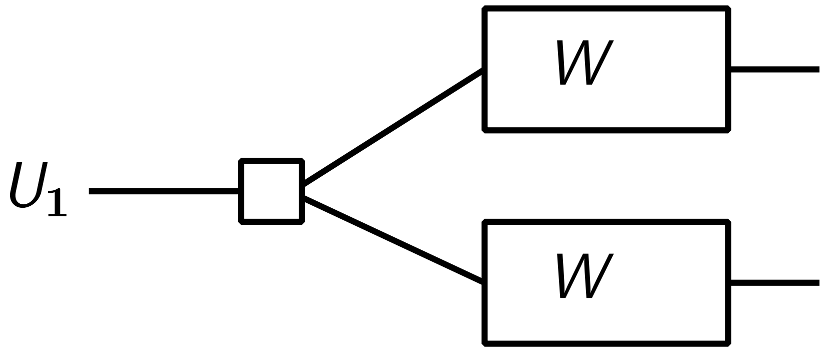


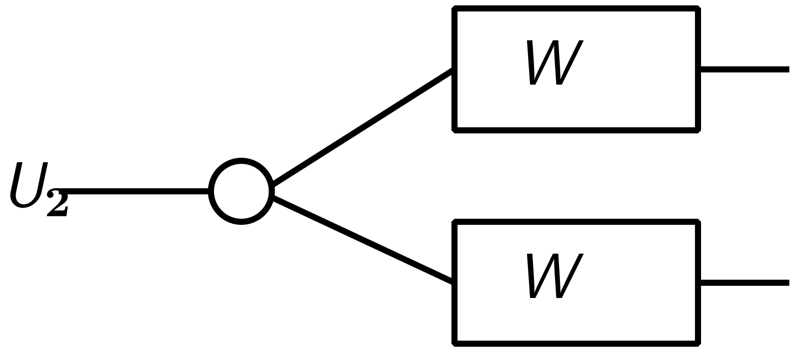
通信路は BEC(0.4)、通信路容量は 0.6、符号長は 1024

通信路分離と通信路結合



$$2I(W) = I(W^{(0)}) + I(W^{(1)})$$



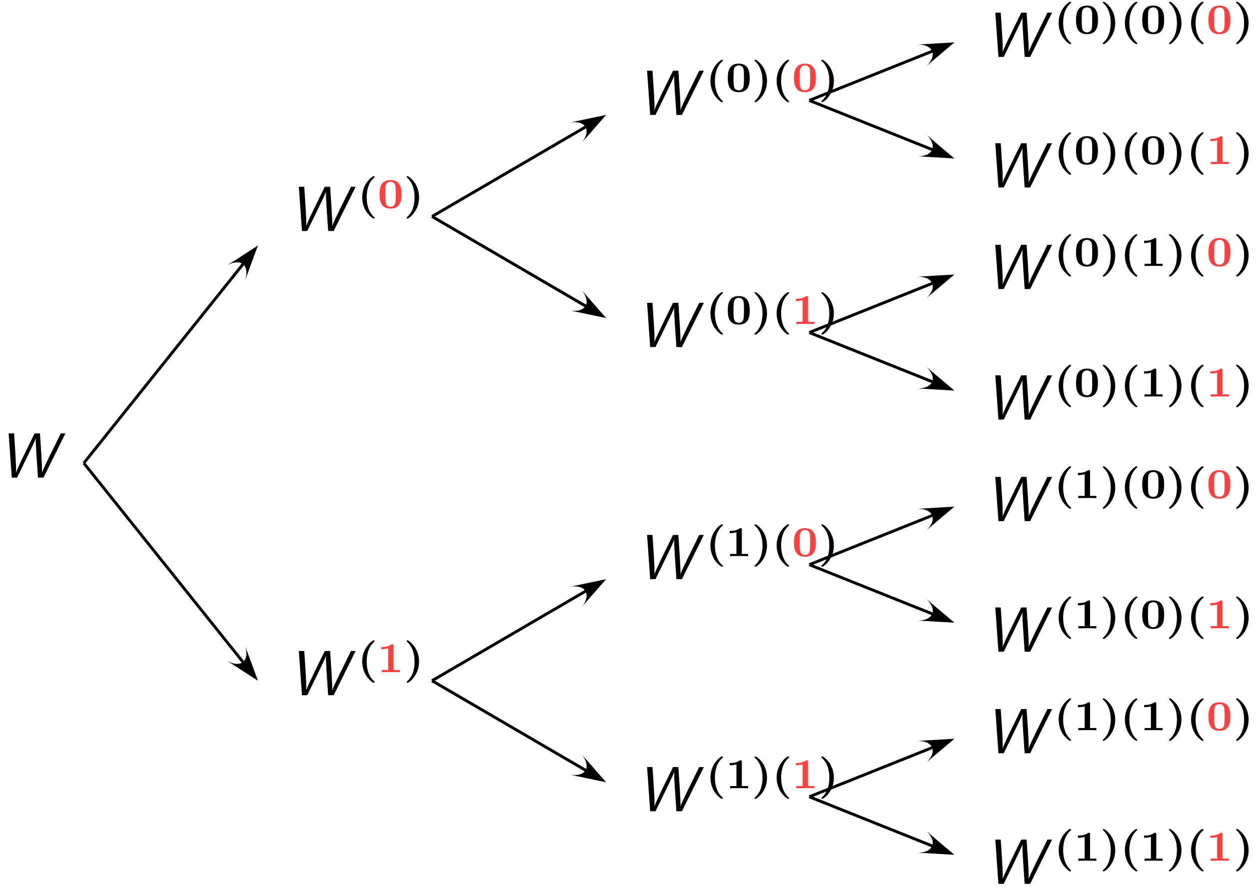


$W^{(0)}(y_1, y_2 \mid u_1)$

$W^{(1)}(y_1, y_2, u_1 \mid u_2)$

Random process $\{W_n\}$ of DMC

$$W_n := \begin{cases} W_{n-1}^{(0)} & \text{w.p.} \quad \frac{1}{2} \\ W_{n-1}^{(1)} & \text{w.p.} \quad \frac{1}{2} \end{cases}, \qquad W_0 := W \qquad \text{w.p. } 1$$



W

$W^{(0)}$

$W^{(1)}$

$W^{(0)(0)}$

$W^{(0)(1)}$

$W^{(1)(0)}$

$W^{(1)(1)}$

$W^{(0)(0)(0)}$

$W^{(0)(0)(1)}$

$W^{(0)(1)(0)}$

$W^{(0)(1)(1)}$

$W^{(1)(0)(0)}$

$W^{(1)(0)(1)}$

$W^{(1)(1)(0)}$

$W^{(1)(1)(1)}$

Polarization: $I(W_n) \to I_\infty = \begin{cases} 0, & \text{w.p.} 1 - I(W) \\ 1, & \text{w.p.} I(W) \end{cases}$ almost surely

マルチンゲール

$$\mathbb{E}[X_n \mid X_{n-1}, \ldots, X_0] = X_{n-1}$$

例 1)

$$\begin{aligned} X_0 &= 0 && \text{w.p. } 1 \\ X_n &= \begin{cases} X_{n-1} + 1 & \text{w.p. } \frac{1}{2} \\ X_{n-1} - 1 & \text{w.p. } \frac{1}{2} \end{cases} \end{aligned}$$

例 2)

$$\begin{aligned} X_0 &= 30, && \text{w.p. } 1 \\ X_n &= \begin{cases} X_{n-1} + 1 & \text{w.p. } \frac{1}{2} \\ X_{n-1} - 1 & \text{w.p. } \frac{1}{2} \end{cases}, && \text{if } X_{n-1} \neq 0, 100 \\ X_n &= X_{n-1}, && \text{if } X_{n-1} = 0, 100 \end{aligned}$$

マルチンゲールの収束定理

もし $\sup_n \mathbb{E}[|X_n|] < \infty$ ならば確率変数 X_∞ が存在して X_n は X_∞ に概収束する

例 1)
適用不可能

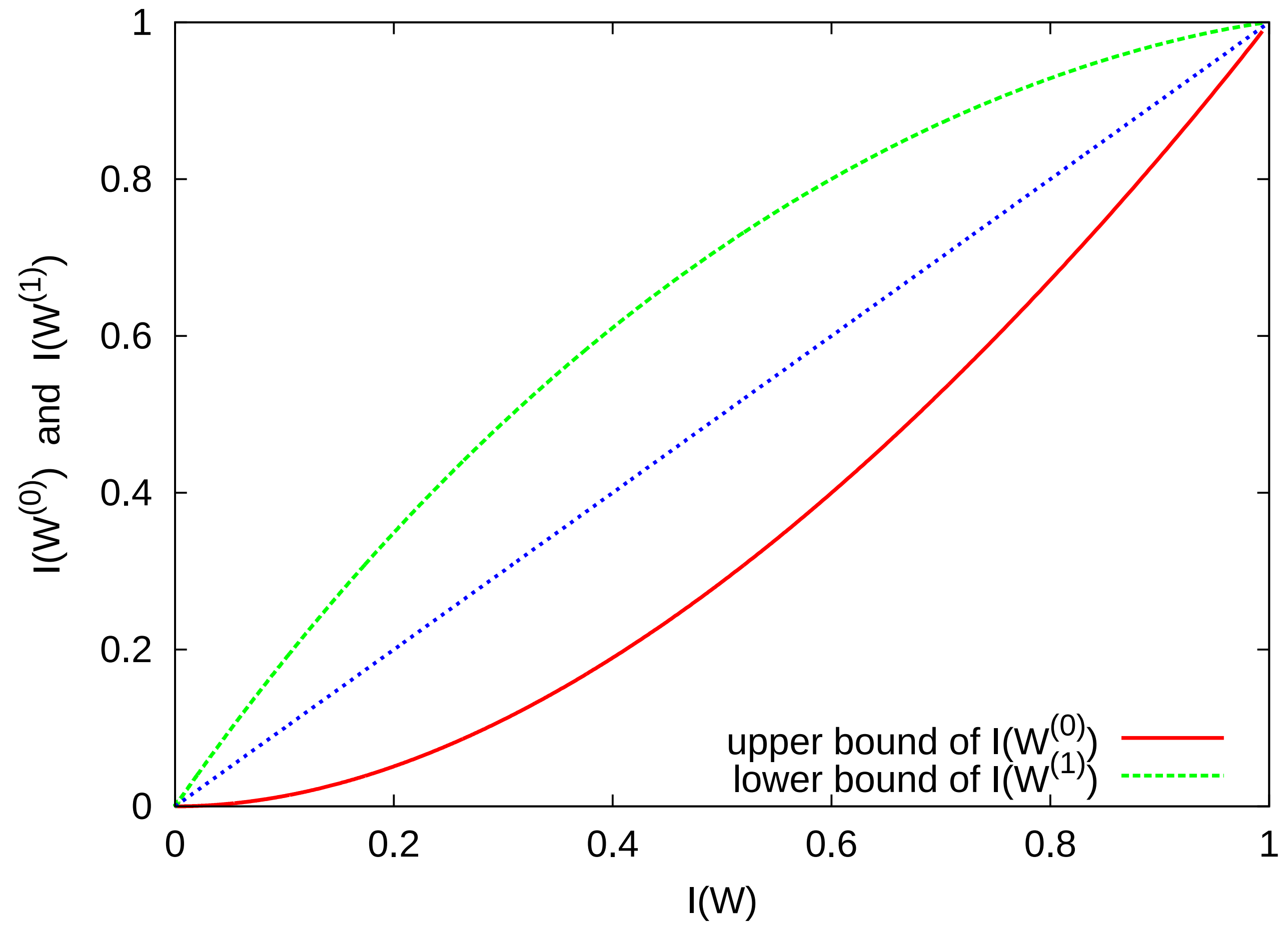
例 2)
$X_n \geq 0$ なので適用可能

$$X_\infty \in \{0, 100\} \qquad \text{w.p. } 1$$

X_n は有界なので $\mathbb{E}[X_\infty] = \lim_{n\to\infty} \mathbb{E}[X_n] = 30$
よって、

$$X_\infty = \begin{cases} 0, & \text{w.p. } 0.7 \\ 100, & \text{w.p. } 0.3 \end{cases}$$

分極の証明



0 と 1 以外は収束先に成り得ない

Polarization: $I(W_n) \rightarrow I_\infty = \begin{cases} \mathbf{0}, & \text{w.p.}\mathbf{1} - I(W) \\ \mathbf{1}, & \text{w.p.} I(W) \end{cases}$ almost surely

誤り確率の評価

$$\begin{aligned}\mathcal{B}_i &:= \{\, u_1^N, y_1^N \mid \hat{u}_1^{i-1} = u_1^{i-1}, \hat{U}_i(y_1^N, \hat{u}_1^{i-1}) \neq u_i \,\} \\ &\subseteq \{\, u_1^N, y_1^N \mid \hat{U}_i(y_1^N, u_1^{i-1}) \neq u_i \,\} =: \mathcal{A}_i.\end{aligned}$$

$$P_{\text{error}}(F) = \mathbf{Pr}\left(\bigcup_{i \in F^c} \mathcal{B}_i\right) = \sum_{i \in F^c} \mathbf{Pr}(\mathcal{B}_i) \leq \sum_{i \in F^c} \mathbf{Pr}(\mathcal{A}_i) = \sum_{i \in F^c} P_e(W_N^{(i)})$$

ある関数 $f(N) = o(1/N)$ について

$$\lim_{n \to \infty} \frac{\left|\left\{ i \in \{1, \dots, N\} \mid P_e(W_N^{(i)}) < f(N) \right\}\right|}{N} = I(W)$$

が言えればよい

対称通信路容量を達成することの証明

$$Z(W) := \sum_{y \in \mathcal{Y}} \sqrt{W(y \mid \mathbf{0}) W(y \mid \mathbf{1})}$$

$$I(W) \approx \mathbf{0} \Longleftrightarrow Z(W) \approx \mathbf{1}$$
$$I(W) \approx \mathbf{1} \Longleftrightarrow Z(W) \approx \mathbf{0}$$

$$Z(W) \geq P_e(W) \geq \frac{\mathbf{1}}{\mathbf{2}} Z(W)^{\mathbf{2}}$$

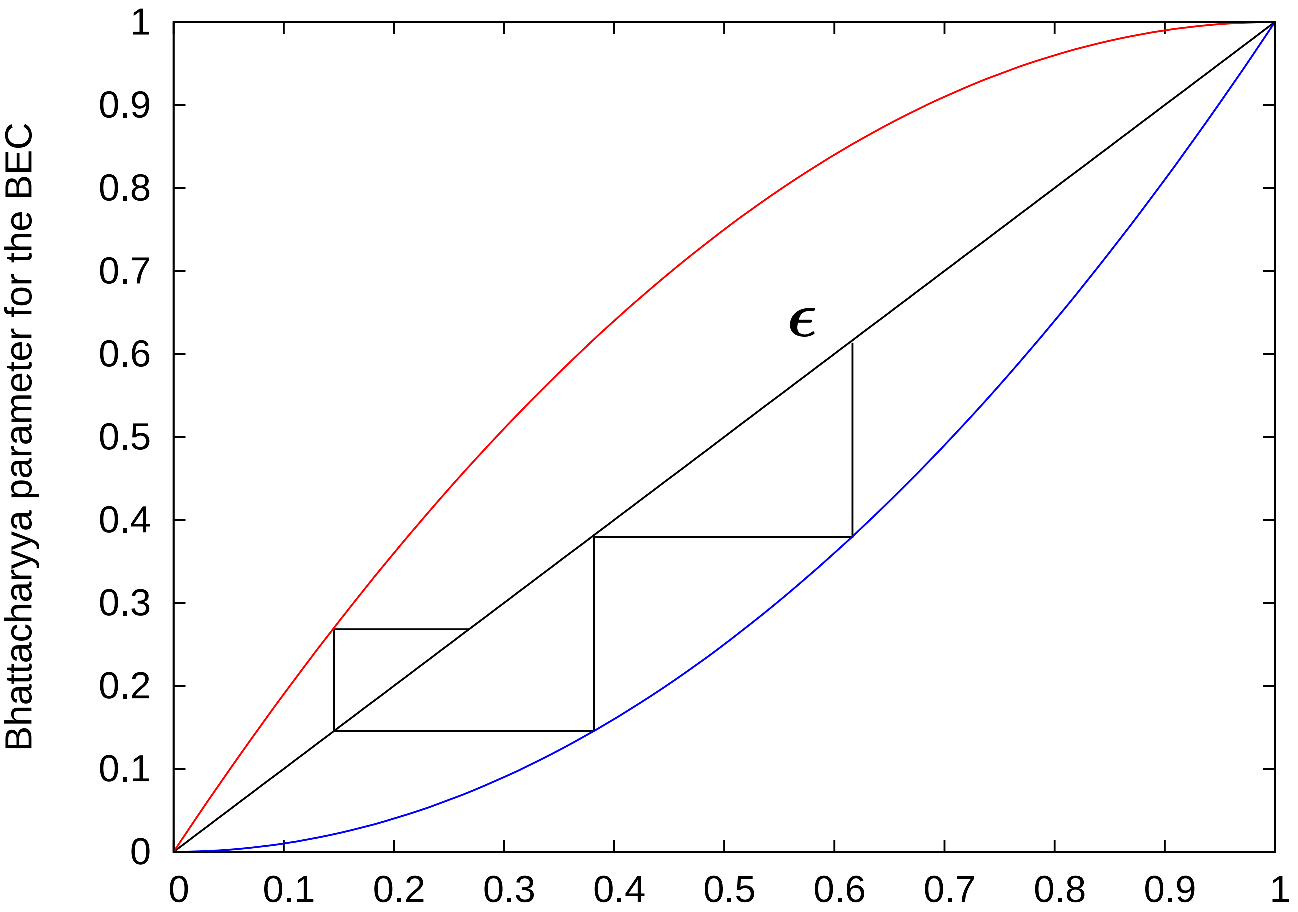
$$\lim_{n \to \infty} \frac{\left| \left\{ i \in \{\mathbf{1}, \dots, N\} \mid Z(W_N^{(i)}) < N^{-\frac{\mathbf{5}}{\mathbf{4}}} \right\} \right|}{N} = I(W)$$

[Arıkan 2008]

これらの結果から任意の $R < I(W)$ について

polar 符号のブロック誤り確率は $O(N^{-\frac{\mathbf{1}}{\mathbf{4}}})$

Bhattacharyya 定数 for BEC(ϵ)



$$Z_n = \begin{cases} Z_{n-1}^{2}, & \text{if} \qquad B_n = 1 \\ 1-(1-Z_{n-1})^{2}, & \text{if} \qquad B_n = 0 \end{cases}$$

Contents

- Polar 符号と通信路分極現象 [Arıkan 2008]
- Polar 符号に関する研究紹介 I(polar 符号の性質)
    1. Polar 符号の漸近的誤り確率 [Arıkan and Telatar 2008]
    2. Polar 符号の $\ell \times \ell$ 行列への一般化 [Korada, Şaşoğlu, and Urbanke 2009]
    3. 密度発展法を用いた polar 符号の構成 [Mori and Tanaka 2009]
    4. Polar 符号の compound capacity [Hassani, Korada, and Urbanke 2009]
    5. 多元 (素体) polar 符号 [Şaşoğlu, Telatar, and Arıkan 2009]
    6. 多元 (一般の有限体) polar 符号と Reed-Solmon 行列 [Mori and Tanaka 2010]
    7. Polar 符号のより詳細な漸近的誤り確率 [Tanaka and Mori 2010] [Hassani and Urbanke 2010] [Hassani, Mori, Tanaka, and Urbanke 2011]
    8. Polar 符号の誤り確率のスケーリング [Korada, Montanari, Telatar, and Urbanke 2010] [Hassani, Alishahi, and Urbanke 2010]
    9. Polar 符号の重み分布 [Mori and Urbanke]
- Polar 符号に関する研究紹介 II(復号法とアプリケーション)

Polar 符号の漸近的誤り確率

[Arıkan and Telatar 2008]

任意の $\beta < \frac{1}{2}$ について

$$\lim_{n\to\infty} \Pr\left(Z(W_n) < 2^{-N^{\beta}}\right) = I(W)$$

任意の $\beta > \frac{1}{2}$ について

$$\lim_{n\to\infty} \Pr\left(Z(W_n) < 2^{-N^{\beta}}\right) = 0$$

これらのことから polar 符号の誤り確率は $o\left(2^{-N^{\frac{1}{2}-\epsilon}}\right)$ かつ $\omega\left(2^{-N^{\frac{1}{2}+\epsilon}}\right)$ for any $\epsilon > 0$.

Contents

- Polar 符号と通信路分極現象 [Arıkan 2008]
- Polar 符号に関する研究紹介 I(polar 符号の性質)
    1. Polar 符号の漸近的誤り確率 [Arıkan and Telatar 2008]
    2. Polar 符号の $\ell \times \ell$ 行列への一般化 [Korada, Şaşoğlu, and Urbanke 2009]
    3. 密度発展法を用いた polar 符号の構成 [Mori and Tanaka 2009]
    4. Polar 符号の compound capacity [Hassani, Korada, and Urbanke 2009]
    5. 多元 (素体) polar 符号 [Şaşoğlu, Telatar, and Arıkan 2009]
    6. 多元 (一般の有限体) polar 符号と Reed-Solmon 行列 [Mori and Tanaka 2010]
    7. Polar 符号のより詳細な漸近的誤り確率 [Tanaka and Mori 2010] [Hassani and Urbanke 2010] [Hassani, Mori, Tanaka, and Urbanke 2011]
    8. Polar 符号の誤り確率のスケーリング [Korada, Montanari, Telatar, and Urbanke 2010] [Hassani, Alishahi, and Urbanke 2010]
    9. Polar 符号の重み分布 [Mori and Urbanke]
- Polar 符号に関する研究紹介 II(復号法とアプリケーション)

行列の指数

Polar 符号の基になる $\mathbf{2} \times \mathbf{2}$ 行列 $\begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} \end{bmatrix}$ を一般化して
$\ell \times \ell$ 行列 G に基づいた polar 符号を考える
そのとき

任意の定数 $\beta < E(G)$ について

$$\lim_{n \to \infty} \mathbf{Pr}(Z(W_n) \leq \mathbf{2}^{-N^\beta}) = I(W)$$

また、任意の定数 $\beta > E(G)$ について

$$\lim_{n \to \infty} \mathbf{Pr}(Z(W_n) \geq \mathbf{2}^{-N^\beta}) = \mathbf{1}$$

となるような $E(G) \in [\mathbf{0}, \mathbf{1})$ を行列 G の指数と呼ぶ

Polar 符号の誤り指数

[Korada, Şaşoğlu and Urbanke 2009]

$$E(G) = \frac{1}{\ell} \sum_{i=1}^{\ell} \log_\ell D_i$$

$\ell \times \ell$ 行列 G について部分距離 D_i を以下のように定める

$$\begin{aligned} D_i &:= d(g_i, \langle g_{i+1}, \dots, g_\ell \rangle), \qquad & i = 1, \dots, \ell - 1 \\ D_\ell &:= d(g_\ell, 0) \end{aligned}$$

ただし g_i は G の i 行目、$\langle g_i, \dots, g_\ell \rangle$ は $g_i, \dots, g_\ell$ で張られる部分符号

例

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

について $D_1 = 1, D_2 = 1, D_3 = 3$

Polar 符号の誤り指数

$$E(G) = \frac{1}{\ell} \sum_{i=1}^{\ell} \log_{\ell} D_i$$

また、

$$E_\ell := \max_{G \in \{0,1\}^{\ell \times \ell}} E(G) \qquad \text{について} \qquad \lim_{\ell \to \infty} E_\ell = 1$$

が成り立つ

特に、$\ell \leq 14$ のとき $E_\ell \leq \frac{1}{2}$ だが $E_{16} = 0.51828 > \frac{1}{2}$ となる

[Korada, Şaşoğlu, and Urbanke 2009]

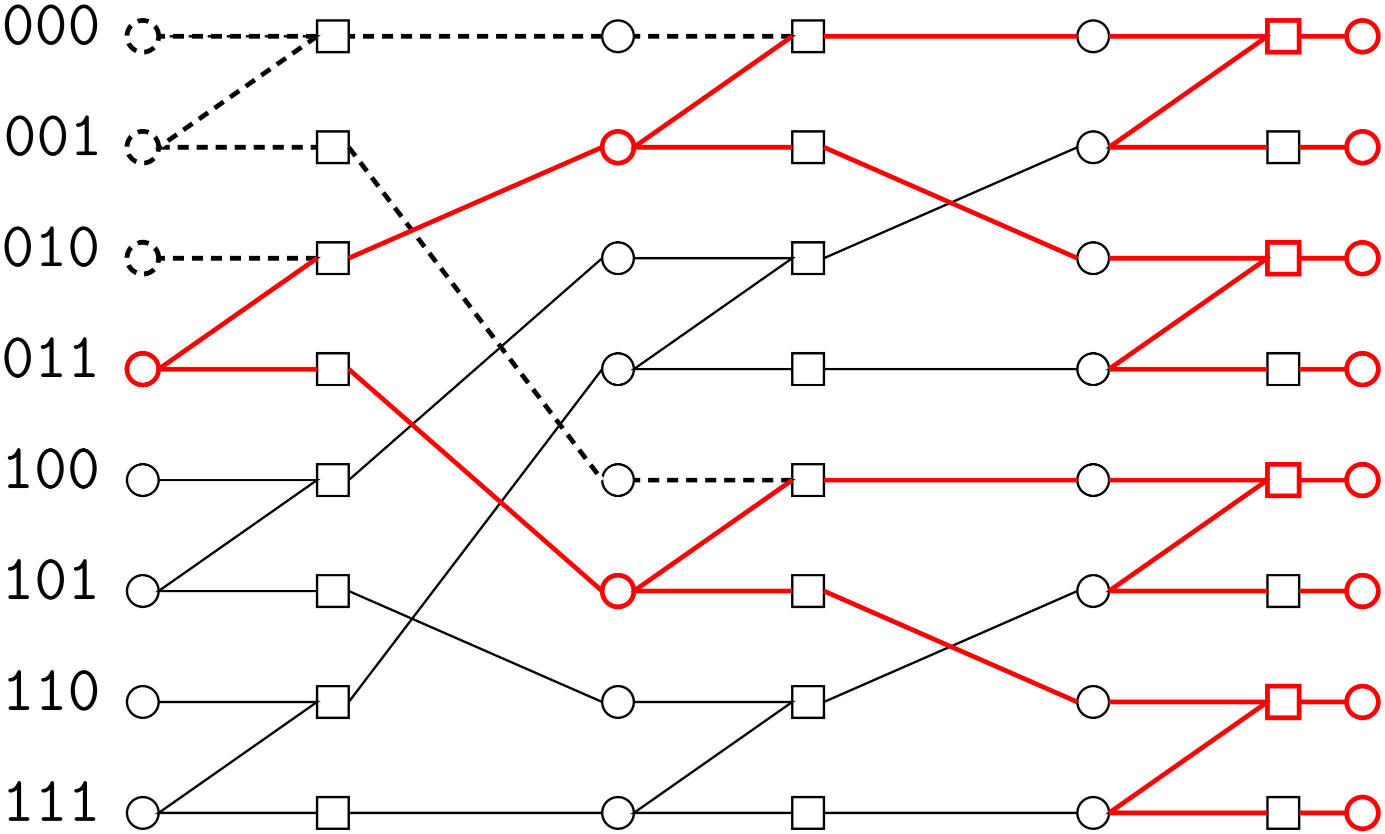
Contents

- Polar 符号と通信路分極現象 [Arıkan 2008]
- Polar 符号に関する研究紹介 I(polar 符号の性質)
  1. Polar 符号の漸近的誤り確率 [Arıkan and Telatar 2008]
  2. Polar 符号の $\ell \times \ell$ 行列への一般化 [Korada, Şaşoğlu, and Urbanke 2009]
  3. 密度発展法を用いた polar 符号の構成 [Mori and Tanaka 2009]
  4. Polar 符号の compound capacity [Hassani, Korada, and Urbanke 2009]
  5. 多元 (素体) polar 符号 [Şaşoğlu, Telatar, and Arıkan 2009]
  6. 多元 (一般の有限体) polar 符号と Reed-Solmon 行列 [Mori and Tanaka 2010]
  7. Polar 符号のより詳細な漸近的誤り確率 [Tanaka and Mori 2010] [Hassani and Urbanke 2010] [Hassani, Mori, Tanaka, and Urbanke 2011]
  8. Polar 符号の誤り確率のスケーリング [Korada, Montanari, Telatar, and Urbanke 2010] [Hassani, Alishahi, and Urbanke 2010]
  9. Polar 符号の重み分布 [Mori and Urbanke]
- Polar 符号に関する研究紹介 II(復号法とアプリケーション)

ブロック誤り確率

$$P_e(F) \leq \sum_{i \in F^c} P_e(W_N^{(i)}) \leq \frac{1}{2} \sum_{i \in F^c} Z(W_N^{(i)})$$

$Z(W_N^{(i)})$ の代わりに $P_e(W_N^{(i)})$ を直接評価



密度発展法

$$\mathbf{Pr}(\mathcal{A}_i) = \mathfrak{E}(\mathsf{a}_N^i),$$

where

$$\mathfrak{E}(\mathsf{a}) := \lim_{\epsilon \to +0} \left(\int_{-\infty}^{-\epsilon} \mathsf{a}(x) \mathrm{d}x + \frac{1}{2} \int_{-\epsilon}^{+\epsilon} \mathsf{a}(x) \mathrm{d}x \right),$$

$$\begin{aligned} \mathsf{a}_{2N}^{2i} &= \mathsf{a}_N^i \ \star \ \mathsf{a}_N^i, \\ \mathsf{a}_{2N}^{2i-1} &= \mathsf{a}_N^i \ \circledast \ \mathsf{a}_N^i, \\ \mathsf{a}_1^1 &= \mathsf{a}_W. \end{aligned}$$

$\chi(N)$: $\{\mathsf{a}_N^i(x)\}_{i=1,\ldots,N}$ を計算するのに必要な畳み込み演算 ($\star$, $\circledast$) の回数

$$\chi(N) = N + \chi\left(\frac{N}{2}\right) = N + \frac{N}{2} + \frac{N}{4} + \cdots + 1 = O(N).$$

[Mori and Tanaka 2009]

Contents

- Polar 符号と通信路分極現象 [Arıkan 2008]
- Polar 符号に関する研究紹介 I(polar 符号の性質)
  1. Polar 符号の漸近的誤り確率 [Arıkan and Telatar 2008]
  2. Polar 符号の $\ell \times \ell$ 行列への一般化 [Korada, Şaşoğlu, and Urbanke 2009]
  3. 密度発展法を用いた polar 符号の構成 [Mori and Tanaka 2009]
  4. Polar 符号の compound capacity [Hassani, Korada, and Urbanke 2009]
  5. 多元 (素体) polar 符号 [Şaşoğlu, Telatar, and Arıkan 2009]
  6. 多元 (一般の有限体) polar 符号と Reed-Solmon 行列 [Mori and Tanaka 2010]
  7. Polar 符号のより詳細な漸近的誤り確率 [Tanaka and Mori 2010] [Hassani and Urbanke 2010] [Hassani, Mori, Tanaka, and Urbanke 2011]
  8. Polar 符号の誤り確率のスケーリング [Korada, Montanari, Telatar, and Urbanke 2010] [Hassani, Alishahi, and Urbanke 2010]
  9. Polar 符号の重み分布 [Mori and Urbanke]
- Polar 符号に関する研究紹介 II(復号法とアプリケーション)

Polar 符号の compound capacity

[Hassani, Korada, and Urbanke 2009]

$\mathcal{W}$:　通信路の集合

$$C(\mathcal{W}) = \max_{P_X} \inf_{W \in \mathcal{W}} I(X;Y)$$

Polar 符号を SC 復号したときの compound capacity は

$$\lim_{N\to\infty} \sum_{i=1}^{N} \inf_{W\in\mathcal{W}} I(W_N^{(i)})$$

BEC(0.5) と BSC(0.11002) の場合は約 0.4816

Contents

- Polar 符号と通信路分極現象 [Arıkan 2008]
- Polar 符号に関する研究紹介 I(polar 符号の性質)
    1. Polar 符号の漸近的誤り確率 [Arıkan and Telatar 2008]
    2. Polar 符号の $\ell \times \ell$ 行列への一般化 [Korada, Şaşoğlu, and Urbanke 2009]
    3. 密度発展法を用いた polar 符号の構成 [Mori and Tanaka 2009]
    4. Polar 符号の compound capacity [Hassani, Korada, and Urbanke 2009]
    5. 多元 (素体) polar 符号 [Şaşoğlu, Telatar, and Arıkan 2009]
    6. 多元 (一般の有限体) polar 符号と Reed-Solmon 行列 [Mori and Tanaka 2010]
    7. Polar 符号のより詳細な漸近的誤り確率 [Tanaka and Mori 2010] [Hassani and Urbanke 2010] [Hassani, Mori, Tanaka, and Urbanke 2011]
    8. Polar 符号の誤り確率のスケーリング [Korada, Montanari, Telatar, and Urbanke 2010] [Hassani, Alishahi, and Urbanke 2010]
    9. Polar 符号の重み分布 [Mori and Urbanke]
- Polar 符号に関する研究紹介 II(復号法とアプリケーション)

多元 polar 符号

有限環 $\mathbb{Z}/q\mathbb{Z}$ 上の行列

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

での分極を考える

q が素数のとき任意の通信路が分極し、q が非素数のとき分極しない通信路が存在する
[Şaşoğlu, Telatar, and Arıkan 2009]

任意の離散無記憶通信路 W が 有限体 $\mathbb{F}_q$ 上の行列

$$\begin{bmatrix} 1 & 0 \\ 1 & \gamma \end{bmatrix}$$

で分極する必要十分条件は $\mathbb{F}_p(\gamma) = \mathbb{F}_q$
[Mori and Tanaka 2010]

Matrix with large exponent

もし G が

$$D_{\mathbf{0}} \leq D_{\mathbf{2}} \leq \cdots \leq D_{\boldsymbol{\ell}-\mathbf{1}} \tag{1}$$

を満たさなかったら G の行を置換することで $E(G') \geq E(G)$ かつ (1) を満たす G' を構成できる
[Korada, Şaşoğlu, and Urbanke 2009]

条件 (1) が成り立ってるとき D_i は $\langle g_i, \ldots, g_{\boldsymbol{\ell}-\mathbf{1}} \rangle$ の最小距離.

よって大きな $E(G)$ を持つ行列を得ることは以下を満たす符号列 $\mathcal{C}_{\mathbf{1}}, \ldots, \mathcal{C}_{\boldsymbol{\ell}}$ を得ることと等しい

- $\mathcal{C}_i$: 次元 i 符号長 ℓ の線型符号
- $\mathcal{C}_{\mathbf{1}} \subseteq \mathcal{C}_{\mathbf{2}} \subseteq \cdots \subseteq \mathcal{C}_{\boldsymbol{\ell}}$
- 符号 $\mathcal{C}_i$ の最小距離が大きい for $i \in \{\mathbf{1}, \ldots, \boldsymbol{\ell}\}$

Reed-Solomon 符号はこれらの条件を満たしている

Reed-Solomon matrix [Mori and Tanaka 2010]

Let α be a primitive element of $\mathbb{F}_q$.
A Reed-Solomon matrix $G_{\mathrm{RS}}(q)$ is defined as

$$\begin{array}{c|cccccc}
 & \alpha^{q-2} & \alpha^{q-3} & \cdots & \alpha & 1 & 0 \\
\hline
X^{q-1} & 1 & 1 & \cdots & 1 & 1 & 0 \\
X^{q-2} & \alpha^{(q-2)(q-2)} & \alpha^{(q-3)(q-2)} & \cdots & \alpha^{q-2} & 1 & 0 \\
X^{q-3} & \alpha^{(q-2)(q-3)} & \alpha^{(q-3)(q-3)} & \cdots & \alpha^{q-3} & 1 & 0 \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
X & \alpha^{q-2} & \alpha^{q-3} & \cdots & \alpha & 1 & 0 \\
1 & 1 & 1 & \cdots & 1 & 1 & 1
\end{array}.$$

Submatrix which consists of ith row to the last row is a generator matrix of extended Reed-Solomon code.
The size ℓ of RS matrix is q.
Since $G_{\mathrm{RS}}(2) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, RS matrix can be regarded as a generalization of Arıkan's binary matrix $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

Since $D_i = i + 1$, $E(G_{\mathrm{RS}}(q)) = \frac{\log(q!)}{q \log q}$

Exponent of Reed-Solomon matrix

$$E(G_{\mathsf{RS}}(q)) = \frac{\log(q!)}{q \log q}$$

q	2	4	16	64	256
$E(G_{\mathsf{RS}}(q))$	0.5	0.573120	0.691408	0.770821	0.822264

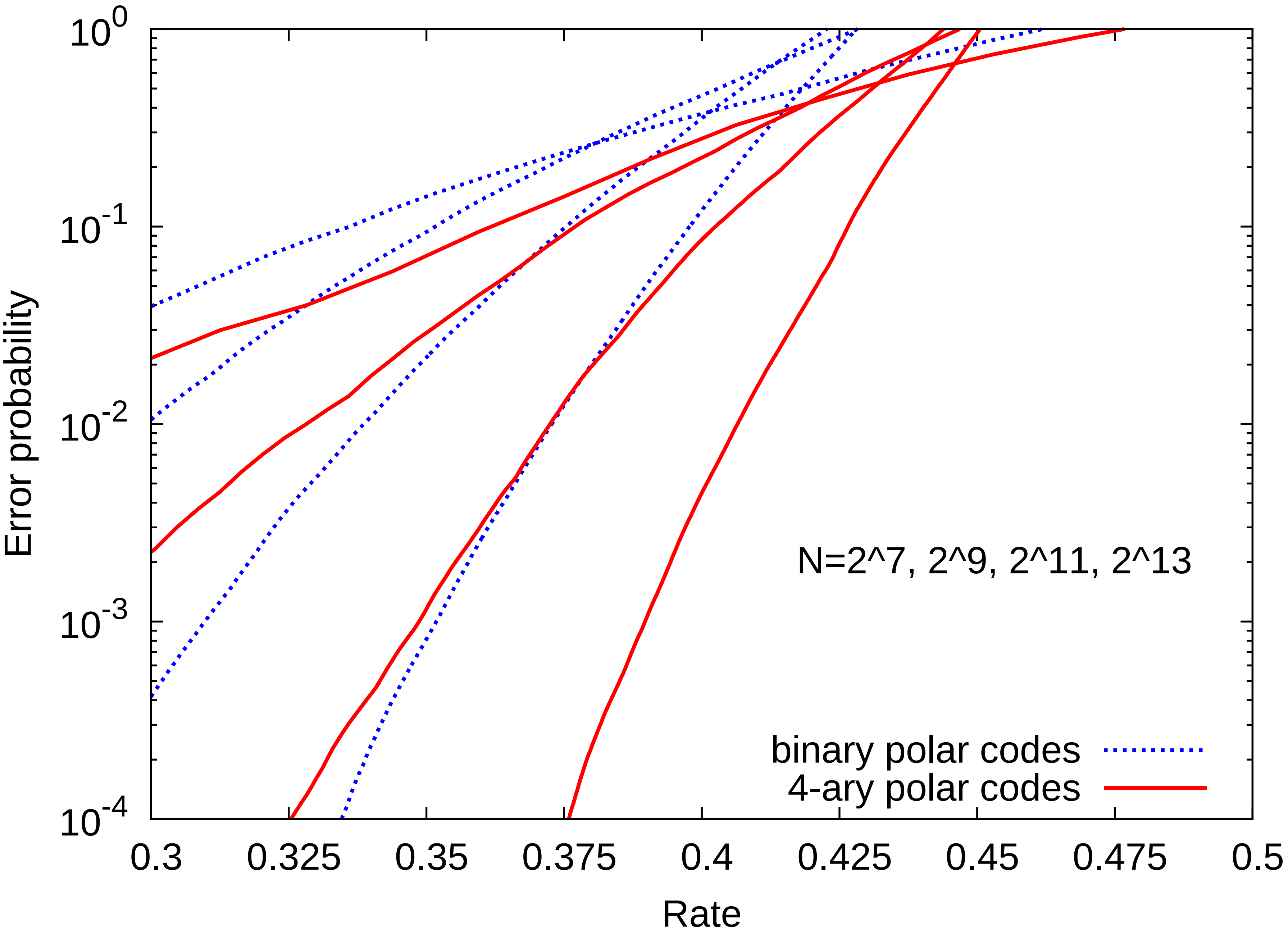
$$\lim_{q\to\infty} E(G_{\mathsf{RS}}(q)) = 1$$

The exponent of binary matrix of size smaller than 32 is smaller than 0.55
[Korada, Şaşoğlu, and Urbanke 2009]

Reed-Solomon matrix is useful for obtaining large exponent !

How about the performance for finite blocklength ?

Simulation result on BAWGNC ($I(W) = 0.5$)



Polar codes and Reed-Muller codes: binary case

[Arıkan 2009]

$$X : \quad 1 \quad 0 \qquad\qquad (X_2, X_1) : (1,1)(1,0)(0,1)(0,0)$$

$$\begin{array}{c} X \\ 1 \end{array} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad\qquad \begin{array}{r} X_2X_1 \\ X_2 \\ X_1 \\ 1 \end{array} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array}$$

Polar rule: $\{i \in \{0, \dots, 2^n - 1\} \mid P_e(W^{(i_1)\cdots(i_n)}) < \epsilon\}$

Reed-Muller rule: $\{i \in \{0, \dots, 2^n - 1\} \mid i_1 + \cdots + i_n > k\}$

Binary polar codes using $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and binary Reed-Muller codes are similar.

Reed-Muller rule maximizes the minimum distance.

Polar codes using RS matrix and Reed-Muller codes: q-ary case

$$\begin{array}{r|ccccccccc|l}
(X_2, X_1): & (2,2) & (2,1) & (2,0) & (1,2) & (1,1) & (1,0) & (0,2) & (0,1) & (0,0) & \\
\hline
X_2^2 X_1^2 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 00 \\
X_2^2 X_1 & 2 & 1 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 01 \\
X_2^2 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 02 \\
X_2 X_1^2 & 2 & 2 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 10 \\
X_2 X_1 & 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 11 \\
X_2 & 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 12 \\
X_1^2 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 20 \\
X_1 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 21 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 22
\end{array}$$

Polar rule: $\{i \in \{0, \dots, q^n - 1\} \mid P_e(W^{(i_1)\cdots(i_n)}) < \epsilon\}$

Reed-Muller rule: $\{i \in \{0, \dots, q^n - 1\} \mid i_1 + \cdots + i_n > k\}$

Q-ary polar codes using $G_{\mathrm{RS}}(q)$ and q-ary Reed-Muller codes are also similar.

Hyperbolic rule: $\{i \in \{0, \dots, q^n - 1\} \mid (i_1 + 1) \cdots (i_n + 1) > k\}$

Hyperbolic rule maximizes the minimum distance
(Massey-Costello-Justesen codes, hyperbolic cascaded RS codes).

Contents

- Polar 符号と通信路分極現象 [Arıkan 2008]
- Polar 符号に関する研究紹介 I(polar 符号の性質)
    1. Polar 符号の漸近的誤り確率 [Arıkan and Telatar 2008]
    2. Polar 符号の $\ell \times \ell$ 行列への一般化 [Korada, Şaşoğlu, and Urbanke 2009]
    3. 密度発展法を用いた polar 符号の構成 [Mori and Tanaka 2009]
    4. Polar 符号の compound capacity [Hassani, Korada, and Urbanke 2009]
    5. 多元 (素体) polar 符号 [Şaşoğlu, Telatar, and Arıkan 2009]
    6. 多元 (一般の有限体) polar 符号と Reed-Solmon 行列 [Mori and Tanaka 2010]
    7. Polar 符号のより詳細な漸近的誤り確率 [Tanaka and Mori 2010] [Hassani and Urbanke 2010] [Hassani, Mori, Tanaka, and Urbanke 2011]
    8. Polar 符号の誤り確率のスケーリング [Korada, Montanari, Telatar, and Urbanke 2010] [Hassani, Alishahi, and Urbanke 2010]
    9. Polar 符号の重み分布 [Mori and Urbanke]
- Polar 符号に関する研究紹介 II(復号法とアプリケーション)

Polar 符号のより詳細な漸近的誤り確率

[Tanaka and Mori 2010] [Hassani and Urbanke 2010]
[Hassani, Mori, Tanaka and Urbanke 2011]
For $R \in (0, 1)$,

$$\lim_{n\to\infty} \Pr\left(Z(W_n) \le 2^{-\ell^{nE(G)+\sqrt{nV(G)}Q^{-1}(R/I(W))+f(n)}} \right) = R$$

for any $f(n) = o(\sqrt{n})$ where $\ell^n = N$,

$$Q(x) := \int_x^\infty \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-\frac{1}{2}x^2} \mathrm{d}x$$

$$E(G) := \frac{1}{\ell} \sum_{i=1}^{\ell} \log_\ell D_i(G)$$

$$V(G) := \frac{1}{\ell} \sum_{i=1}^{\ell} \left(\log_\ell D_i(G) - E(G)\right)^2 .$$

通信路に依存するビット の数

[Mori 2010 SITA Newsletter] [Hassani, Mori, Tanaka and Urbanke 2011]

Reed-Muller 符号:

- インデックスの二進展開に 1 の数が多いビット を選ぶ

Polar 符号:

- インデックスの二進展開に従って密度発展法で $P_e(W_N^{(i)})$ を計算し $P_e(W_N^{(i)})$ が小さいものから順に選ぶ

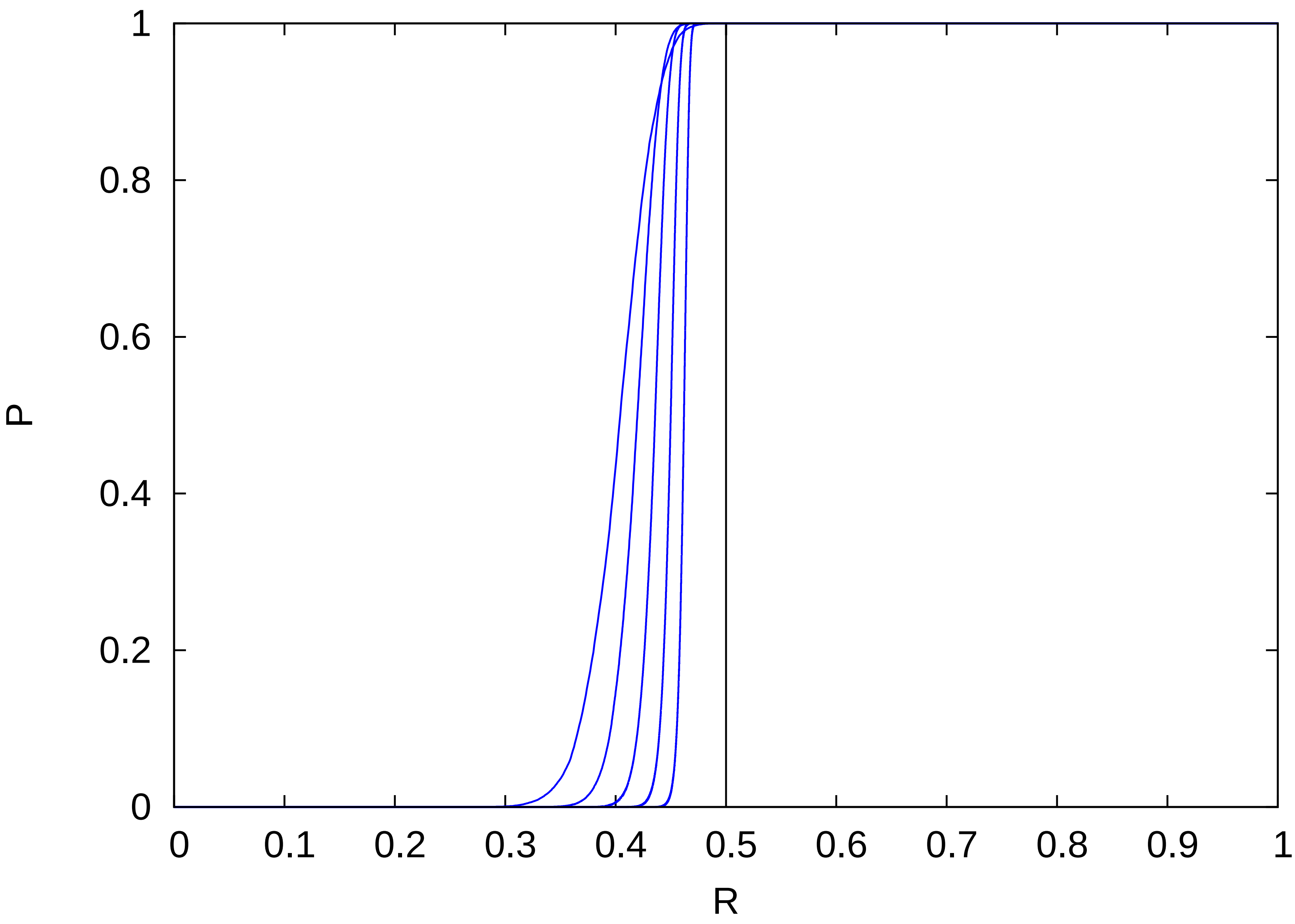
二進展開のうち最初の $\Theta(\log n)$ ビット を通信路に依存して選び、残りの部分を Reed-Muller ルールで選ぶ方法で漸近的に最適な誤り確率が得られる $(2^n = N)$

この手法を繰り返し適用すれば、二進展開のうち最初の $\Theta(\log \log \log \ldots \log n)$ ビット だけが通信路に依存する構成法で漸近的に最適な polar 符号が得られる ！

Contents

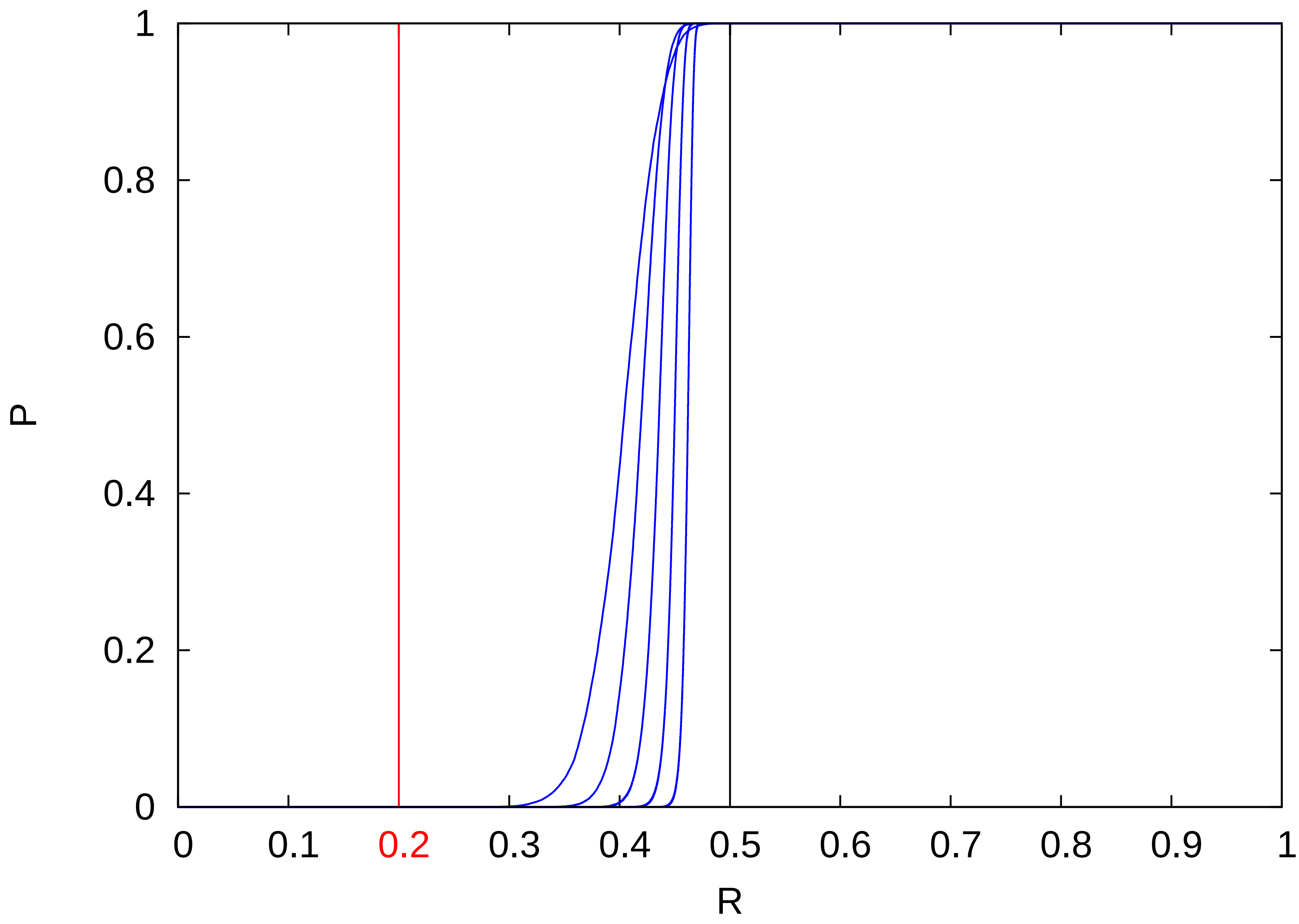
- Polar 符号と通信路分極現象 [Arıkan 2008]
- Polar 符号に関する研究紹介 I(polar 符号の性質)
  1. Polar 符号の漸近的誤り確率 [Arıkan and Telatar 2008]
  2. Polar 符号の $\ell \times \ell$ 行列への一般化 [Korada, Şaşoğlu, and Urbanke 2009]
  3. 密度発展法を用いた polar 符号の構成 [Mori and Tanaka 2009]
  4. Polar 符号の compound capacity [Hassani, Korada, and Urbanke 2009]
  5. 多元 (素体) polar 符号 [Şaşoğlu, Telatar, and Arıkan 2009]
  6. 多元 (一般の有限体) polar 符号と Reed-Solmon 行列 [Mori and Tanaka 2010]
  7. Polar 符号のより詳細な漸近的誤り確率 [Tanaka and Mori 2010] [Hassani and Urbanke 2010] [Hassani, Mori, Tanaka, and Urbanke 2011]
  8. Polar 符号の誤り確率のスケーリング [Korada, Montanari, Telatar, and Urbanke 2010] [Hassani, Alishahi, and Urbanke 2010]
  9. Polar 符号の重み分布 [Mori and Urbanke]
- Polar 符号に関する研究紹介 II(復号法とアプリケーション)

Polar 符号の誤り確率 BEC($\epsilon = 0.5$)



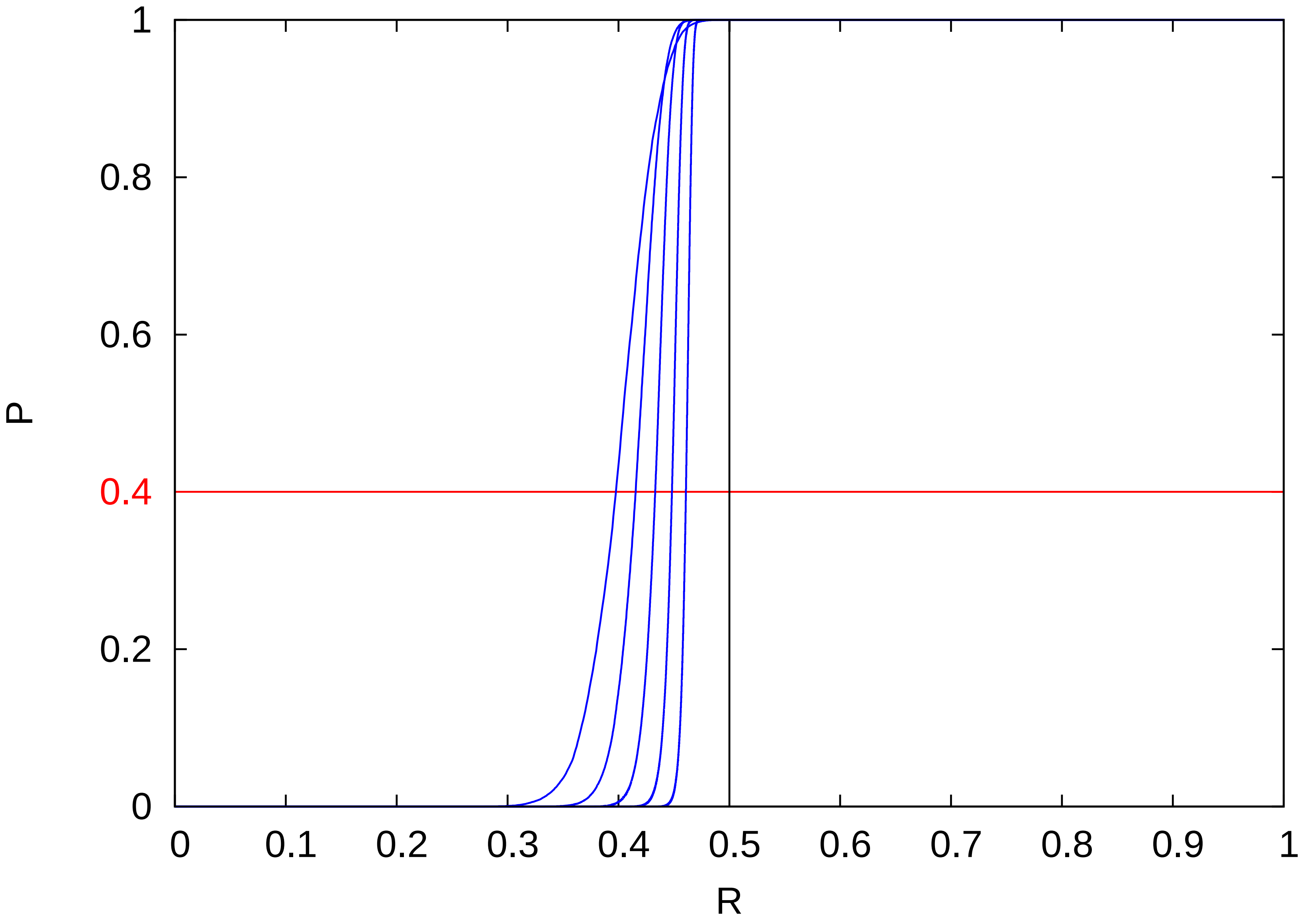
$N = \mathbf{2^{10}, 2^{12}, 2^{14}, 2^{16}, 2^{18}}$

Polar 符号の誤り確率 BEC($\epsilon = 0.5$)



レートを止めて符号長を大きくしたときにどれくらいの
速さで誤り確率が減少するか $\Longleftrightarrow$ Gallager Type の解析

Polar 符号の誤り確率 BEC($\epsilon = 0.5$)



誤り確率を止めて符号長を大きくしたときにどれくらいの
速さでレートがキャパシティに近づくか $\Longleftrightarrow$ Strassen Type の解析

Polar 符号の誤り確率のスケーリング

[Korada, Montanari, Telatar, and Urbanke 2010]
[Hassani, Alishahi, and Urbanke 2010]

ある固定した $a \in (0, 1)$ について

$$F_N(\epsilon) := \Pr(\epsilon \le Z(W_n) \le a)$$

Scaling Asumption:
ある $\mu > 0$ が存在して、任意の $\epsilon \in (0, a]$ について

$$F(\epsilon) := \lim_{N\to\infty} N^{\frac{1}{\mu}} F_N(\epsilon)$$

が存在する (μ: スケーリングパラメータ)

このとき、

$$F^{-1}(N^{\frac{1}{\mu}}(I(W) - R)) \le P_e$$

Polar 符号のスケーリングパラメータ

[Korada, Montanari, Telatar, and Urbanke 2010]
[Hassani, Alishahi, and Urbanke 2010]

$$P_\mathrm{e} \geq F^{-1}(N^{\frac{1}{\mu}}(I(W) - R))$$

$$NR \leq NI(W) - N^{1-\frac{1}{\mu}} F(P_\mathrm{e})$$

これは Strassen 型の評価

Scaling Assumption より $F_N(\epsilon) = \Theta(N^{-\frac{1}{\mu}})$.

$$-\frac{1}{\mu} = \lim_{n\to\infty} \frac{1}{n} \log \Pr(a \leq Z(W_n) \leq b)$$

通信路が BEC のときには評価可能で $1/\mu \approx 0.2757$.
AWGC 通信路の場合ガウス近似を使って評価すると $1/\mu \approx 0.2497$.
ランダム符号や LDPC 符号は $1/\mu = 0.5$.

Contents

- Polar 符号と通信路分極現象 [Arıkan 2008]
- Polar 符号に関する研究紹介 I(polar 符号の性質)
    1. Polar 符号の漸近的誤り確率 [Arıkan and Telatar 2008]
    2. Polar 符号の $\ell \times \ell$ 行列への一般化 [Korada, Şaşoğlu, and Urbanke 2009]
    3. 密度発展法を用いた polar 符号の構成 [Mori and Tanaka 2009]
    4. Polar 符号の compound capacity [Hassani, Korada, and Urbanke 2009]
    5. 多元 (素体) polar 符号 [Şaşoğlu, Telatar, and Arıkan 2009]
    6. 多元 (一般の有限体) polar 符号と Reed-Solmon 行列 [Mori and Tanaka 2010]
    7. Polar 符号のより詳細な漸近的誤り確率 [Tanaka and Mori 2010] [Hassani and Urbanke 2010] [Hassani, Mori, Tanaka, and Urbanke 2011]
    8. Polar 符号の誤り確率のスケーリング [Korada, Montanari, Telatar, and Urbanke 2010] [Hassani, Alishahi, and Urbanke 2010]
    9. Polar 符号の重み分布 [Mori and Urbanke]
- Polar 符号に関する研究紹介 II(復号法とアプリケーション)

Polar 符号の重み分布

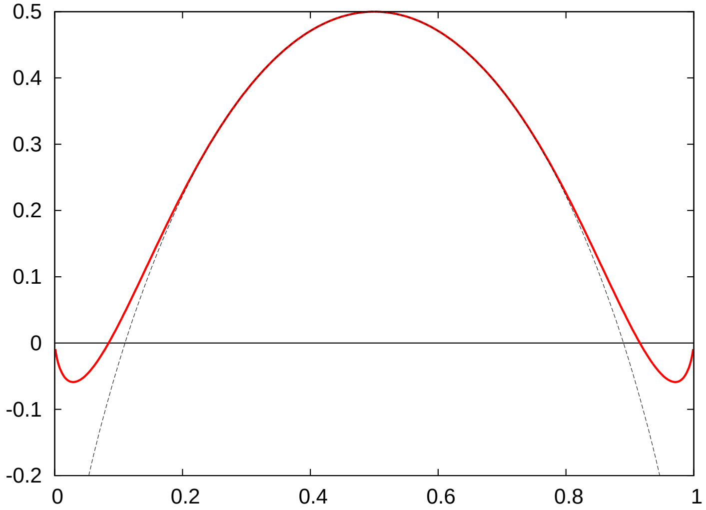
2010 年 10 月 10 日から 10 月 30 日まで EPFL の Urbanke 教授の研究室に滞在

$M(N, w)$: 符号列 $\{\mathcal{C}_N\}_{N\in\mathbb{N}}$ について、符号長 N の符号 $\mathcal{C}_N$ に含まれる重み w の符号語の数

Growth rate $G(\omega)$:

$$G(\omega) := \lim_{N\to\infty} \frac{1}{N} \log M(N, \lfloor N\omega \rfloor)$$

for $\omega \in [0, 1]$ (極限の存在は仮定する).

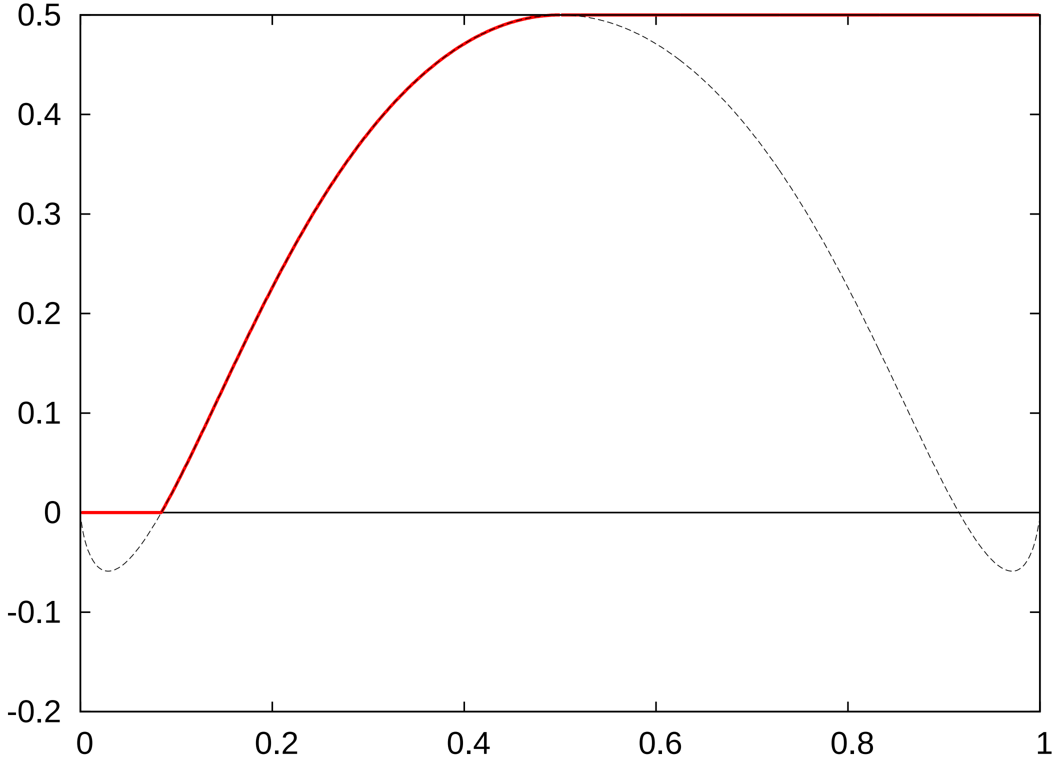


Polar 符号の重み分布

Cumulative growth rate $G(\omega)$ [Mori and Urbanke]:

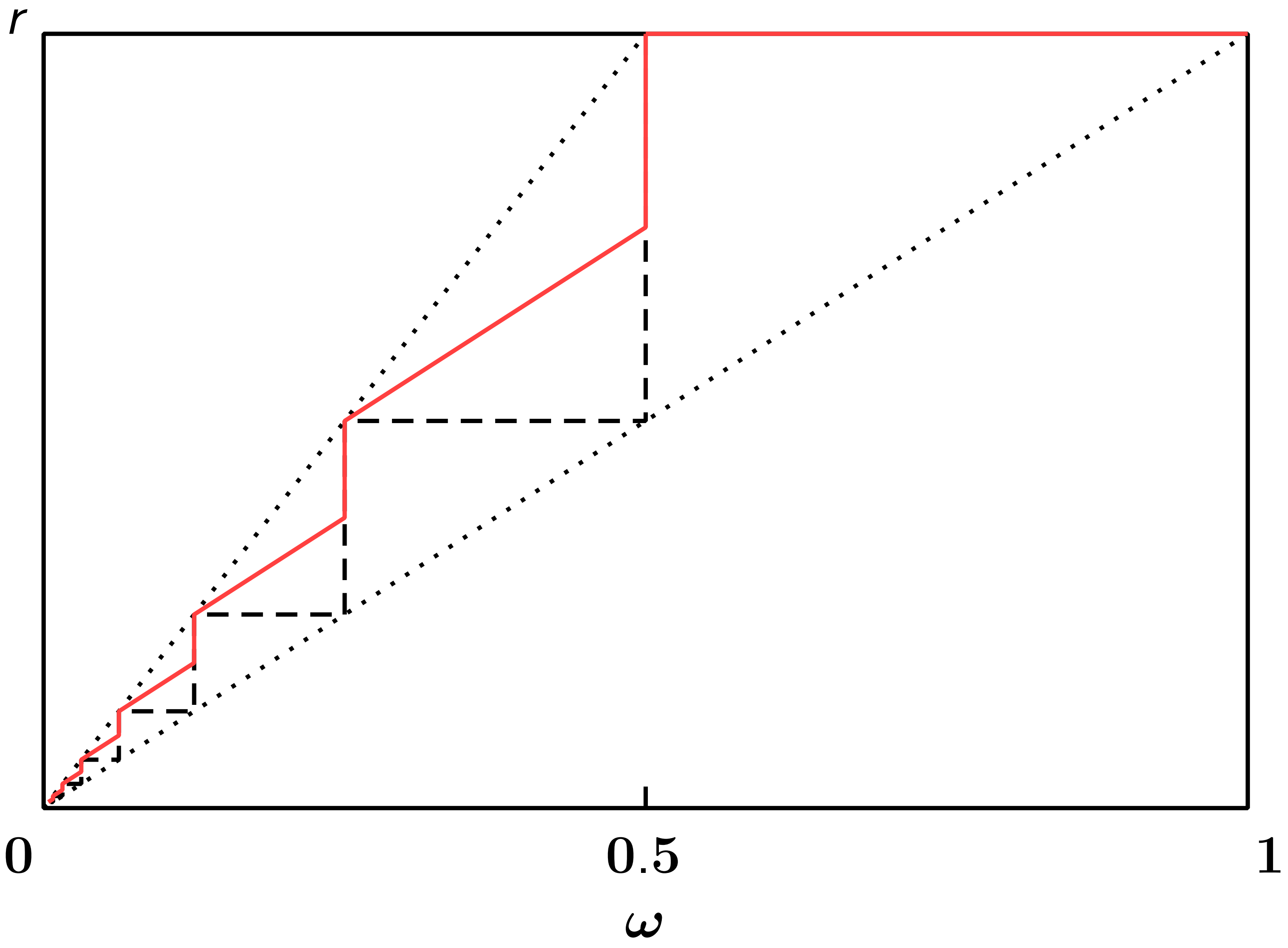
$$G(\omega) := \liminf_{N\to\infty} \frac{1}{N} \log \sum_{i=0}^{\lfloor N\omega \rfloor} M(N,i)$$

for $\omega \in [0, 1]$.



Polar 符号と Reed-Muller 符号の cumulative growth rate の下界

[Mori and Urbanke]



Contents

- Polar 符号と通信路分極現象 [Arıkan 2008]
- Polar 符号に関する研究紹介 I(polar 符号の性質)
    1. Polar 符号の漸近的誤り確率 [Arıkan and Telatar 2008]
    2. Polar 符号の $\ell \times \ell$ 行列への一般化 [Korada, Şaşoğlu, and Urbanke 2009]
    3. 密度発展法を用いた polar 符号の構成 [Mori and Tanaka 2009]
    4. Polar 符号の compound capacity [Hassani, Korada, and Urbanke 2009]
    5. 多元 (素体) polar 符号 [Şaşoğlu, Telatar, and Arıkan 2009]
    6. 多元 (一般の有限体) polar 符号と Reed-Solmon 行列 [Mori and Tanaka 2010]
    7. Polar 符号のより詳細な漸近的誤り確率 [Tanaka and Mori 2010] [Hassani and Urbanke 2010] [Hassani, Mori, Tanaka, and Urbanke 2011]
    8. Polar 符号の誤り確率のスケーリング [Korada, Montanari, Telatar, and Urbanke 2010] [Hassani, Alishahi, and Urbanke 2010]
    9. Polar 符号の重み分布 [Mori and Urbanke]
- Polar 符号に関する研究紹介 II(復号法とアプリケーション)

Contents

- Polar 符号と通信路分極現象 [Arıkan 2008]
- Polar 符号に関する研究紹介 I(polar 符号の性質)
- Polar 符号に関する研究紹介 II(復号法とアプリケーション)
  1. 歪み有り圧縮と Wyner-Ziv, Gelfand-Pinsker 問題 [Korada and Urbanke 2009]
  2. 歪み無し圧縮と情報源分極 [Arıkan 2010]
  3. Wiretap 通信路 [Mahdavifar and Vardy 2010] [Hof and Shamai 2010] [Koyluoglu and El Gamal 2010]
  4. 2-user MAC [Şaşoğlu, Telatar, and Yeh 2010], m-user MAC [Abbe and Telatar 2010]
  5. Compressed sensing [Pilani, Arıkan, Arıkan 2010]
  6. Relay 通信路 (compress-and-forward) [Blasco-Serrano, Thobaben, Rathi, and Skoglund 2010]
  7. Polar 符号の構成法 [Tal and Vardy 2010] [Pedarsani, Hassani, Tal, and Telatar 2011]
  8. 量子通信路 [Wilde and Guha 2011] [Renes, Dupuis, and Renner 2011]
  9. Markov 情報源 [Şaşoğlu 2011]
  10. リスト復号 [Tal and Vardy 2011]