

非対称通信路の通信路容量を達成する 符号化法に関する最近の進展

東京大学 大学院新領域創成科学研究科
複雑理工学専攻 講師
本多 淳也

情報理論研究会 2018/5/18

概要

- 非対称通信路の符号化
- polar符号を用いる方式
- 無歪み圧縮を用いた符号化法の一般的な枠組み
 - Miyake-Muramatsuの方式
 - 連鎖構造に基づく方式
- 無歪み圧縮の逆操作について

通信路符号化

- ノイズを含む通信路を用いて情報を伝送したい
- m ビットのメッセージを $n > m$ ビットに冗長化して送信

$$(X_1, X_2, \dots, X_n)$$

//



$$P_{Y|X}(y|x) = W(y|x)$$

- 達成可能な符号化率 $R = m/n$ の上限: 通信路容量

$$C(W) = \max_{P_X} I(X; Y) = \max_{P_X} \{H(X) - H(X|Y)\}$$

対称通信路の符号化

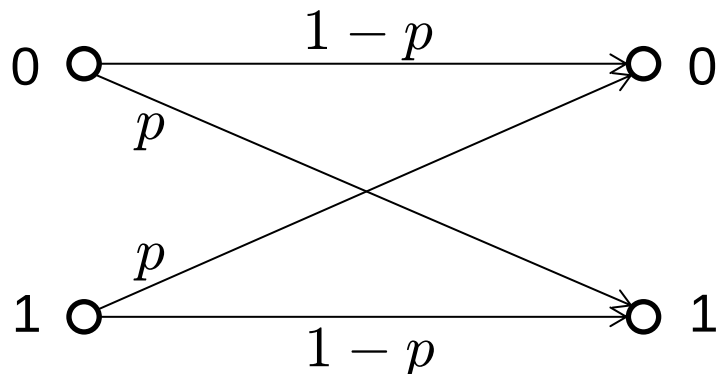
$$\text{通信路容量: } C(W) = \max_{P_X} I(X; Y)$$

- 符号語の各シンボルの頻度分布は P_X に近い必要がある
- 通信路が対称な場合: P_X は一様分布 $\rightarrow$ 線形符号で OK

$$\mathcal{C} = \{x^n \in \{0, 1\}^n : x_1^n H = 0\}, |\mathcal{C}| = 2^m$$

$$n \times (n - m) \text{ 行列, } m/n \approx C(W)$$

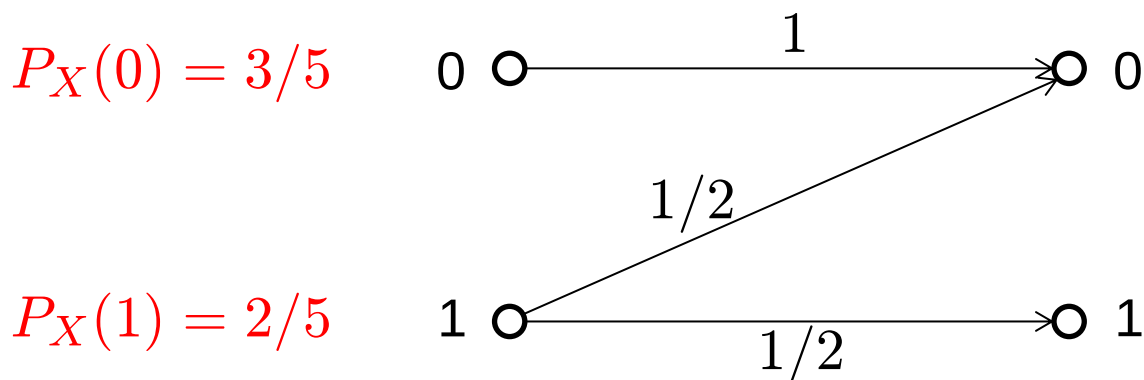
- H のとり方: ランダム行列・LDPC 行列・polar 符号……



非対称通信路の符号化

- 最適な入力分布は一般に非一様
- 通信路容量を達成するには一様分布にしたがうメッセージを頻度分布の偏った符号語に変換する必要がある
- 一様入力で達成できる符号化率は

$$I_s(W) = \frac{1}{2} \sum_{x,y} W(y|x) \log \frac{2W(y|x)}{W(y|0) + W(y|1)} \leq C(W)$$



Gallager の方法

- 入力分布を $(P_X(0), P_X(1)) = (2/3, 1/3)$ としたい場合:

1) 3 元線形符号 $\{\tilde{x}^n \in \{0, 1, 2\}^n : \tilde{x}^n H = 0\}$ の
符号語を生成する

2) 2 元の符号語に写像する

$$x_i := \begin{cases} 0, & \tilde{x}_i = 0, 1 \\ 1, & \tilde{x}_i = 2 \end{cases}$$

- アルファベットサイズは計算量に関わるので大きくしにくい
 - m -user MAC を用いて $P_X(x) = i/2^m$ の形の分布を表現する方法も一応ある [Abbe-Telatar, 2012]
- 場合によっては誤り率や平均歪みも悪くなる

概要

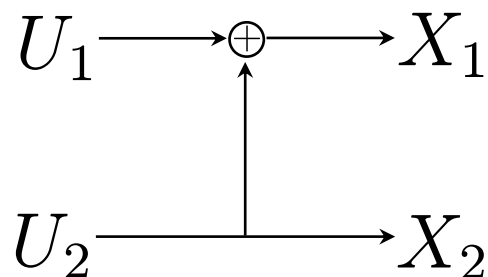
- 非対称通信路の符号化
- polar符号を用いる方式
- 無歪み圧縮を用いた符号化法の一般的な枠組み
 - Miyake-Muramatsuの方式
 - 連鎖構造に基づく方式
- 無歪み圧縮の逆操作について

Polar 符号

- 通信路分極を利用した符号
- 2元対称通信路に対して通信路容量を達成 [Arikan, 2008]
- 一般の通信路に対しても拡張可能
 - 多元通信路 [Sasoglu+, 2009, Mori-Tanaka, 2010]
 - 非対称通信路 [Honda-Yamamoto, 2012]
 - マルコフ通信路 [Sasoglu, 2011][Wang+, 2015][Sasoglu-Tal, 2016]
- 無歪み圧縮や有歪み圧縮等の他の問題にも適用可能
- 動的計画法により符号長 n に対して計算量 $O(n \log n)$, 誤り確率 $2^{-O(\sqrt{n})}$ を達成

エントロピーの分極

- $X_1, X_2 \in \{0, 1\}$: 分布 P_X に独立にしたがう確率変数
- $(U_1, U_2) = (X_1 \oplus X_2, X_2)$

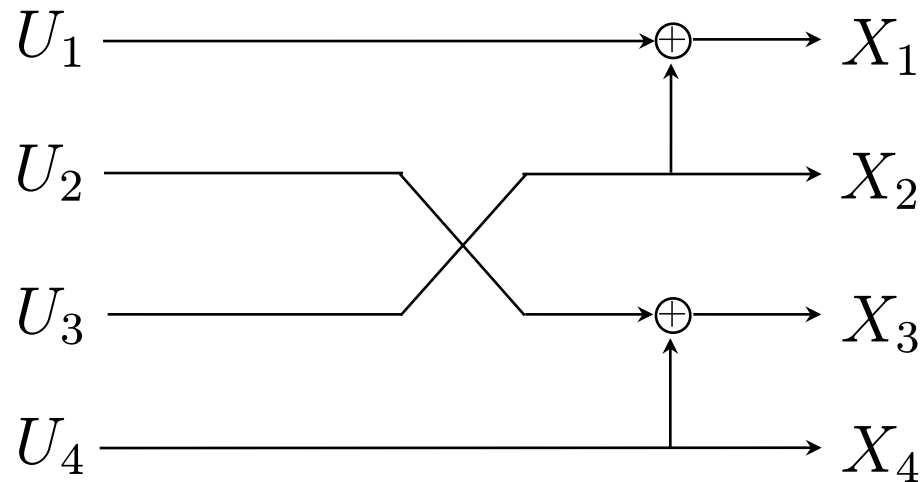


- $H(X_1, X_2) = H(U_1, U_2)$
 $= H(U_1) + H(U_2|U_1)$
 $\quad \quad \quad \uparrow \quad \quad \quad \uparrow$
 $\quad \quad \quad H_1^{(1)} > H_2^{(1)}$

- エントロピーが大きいものと小さいものに分離

エントロピーの分極

- 同じ回路をコピー



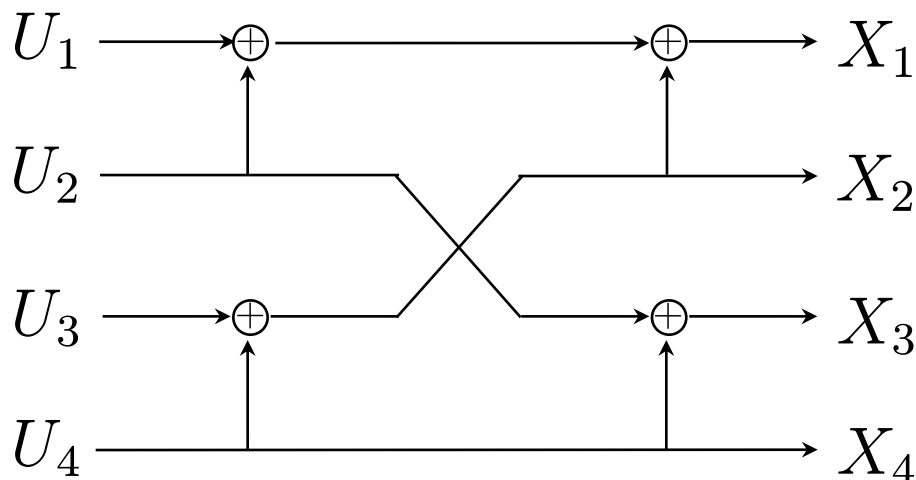
- お互いの回路は交わっていないので

$$H(U_1) = H_1^{(1)} = H(U_2|U_1),$$

$$H(U_3|U_1^2) = H_2^{(1)} = H(U_4|U_1^3)$$

エントロピーの分極

- 同等なビット同士を結合



- 対称性が崩れて

$$H(U_1) > H_1^{(2)} > H(U_2|U_1),$$

$$H(U_3|U_1^2) > H_2^{(2)} > H(U_4|U_1^3)$$

- エントロピーの総和は結合前と同じ

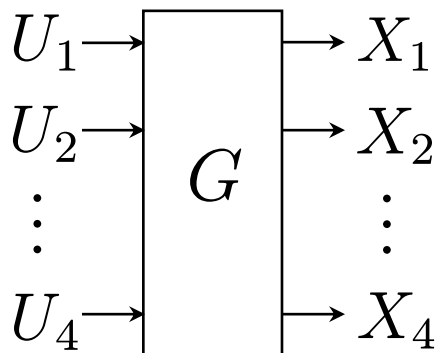
エントロピーの分極

- 以下 1,2 の操作を再帰的に繰り返す
 1. 同じ回路を2個にコピーする
 2. それぞれの回路で同等な位置のビットを

 の回路で結合する
 - エントロピーの和は結合前後で変わらない
 - 結合後はエントロピーが大小に分離
- マルチンゲールの収束定理より, 最終的に $U_1^n = GX_1^n$ のうち
 - $H(U_i|U_1^{i-1}) \approx 1 : nH(X)$ 個
 - $H(U_i|U_1^{i-1}) \approx 0 : n(1 - H(X))$ 個

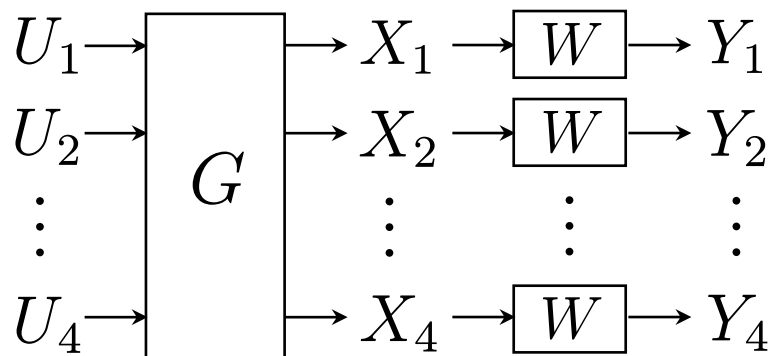
Polar 符号による固定長無歪み圧縮

- 偏りのある系列 X_1^n を, かわりに $U_1^n = GX_1^n$ で表現する
- $H(U_i|U_1^{i-1}) \approx 0$: 凍結ビット
 U_i の情報は U_1^{i-1} を見ればほぼ一意に定まる
- $H(U_i|U_1^{i-1}) \approx 1$: 情報ビット
 U_i の情報は U_1^{i-1} を見ても全く分からない(一様ランダム)
- 情報ビットの値だけを送信すれば受信者は U_1^n 全体を復元可能
 $\rightarrow X_1^n = G^{-1}U_1^n = GU_1^n$ も復元可能



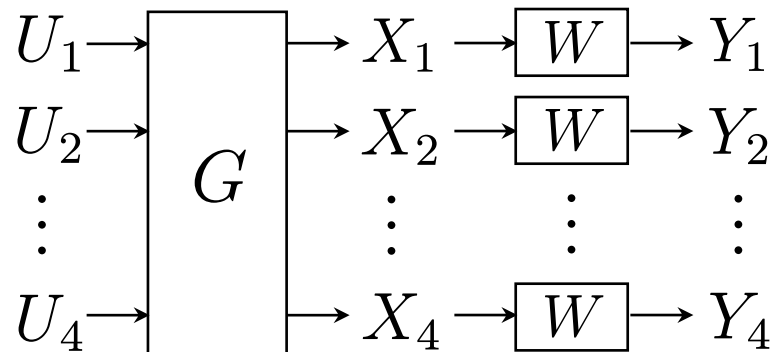
Polar 符号による対称通信路符号化

- 一様分布にしがたう系列 X_1^n を送信して Y_1^n を受信
- $H(U_i | U_1^{i-1}, Y_1^n) \approx 0$: 情報ビット
 U_i の情報は U_1^{i-1} と Y_1^n を見ればほぼ一意に定まる
- $H(U_i | U_1^{i-1}, Y_1^n) \approx 1$: 凍結ビット
 U_i の情報は U_1^{i-1} と Y_1^n を見ても全く分からない
- 凍結ビットの情報を事前に固定しておけば, 受信者は情報ビットに割り振られたメッセージを復元可能



非対称通信路の場合

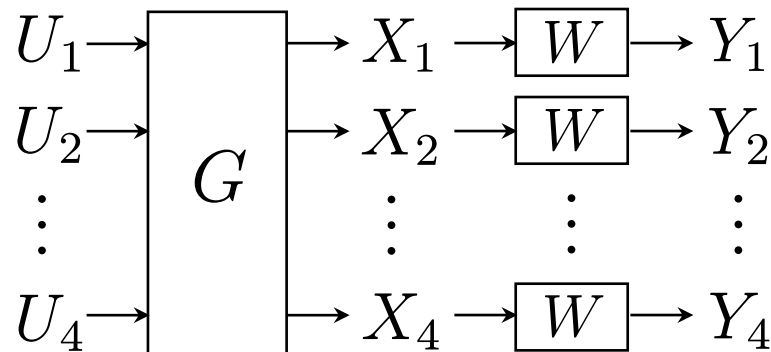
- 通信路容量を達成するためには通信路への入力系列 X_1^n が一様でない分布 P_X に従っていなければならない
 - 凍結ビットの値を固定すると線形符号になってしまうので非一様な入力分布を構成できない
 - エントロピーの分極を用いて非一様な系列を生成すればよい



多段階の分極

- X_1^n が一様でない場合には $H(U_i|U_1^{i-1})$ と $H(U_i|U_1^{i-1}, Y_1^n)$ の両方について分極が生じる

	$H(U_i U_1^{i-1}) \approx 0$	$H(U_i U_1^{i-1}) \approx 1$
$H(U_i U_1^{i-1}, Y_1^n) \approx 0$	$n(1 - H(X))$ bits	$nC(W)$ bits
$H(U_i U_1^{i-1}, Y_1^n) \approx 1$	0 bits	$nH(X Y)$ bits

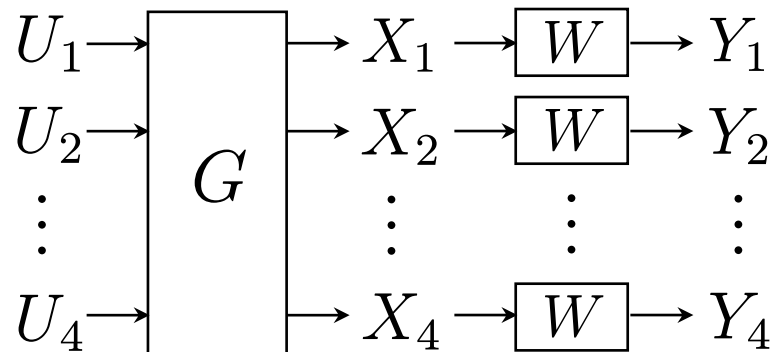


多段階の分極

- X_1^n が一様でない場合には $H(U_i|U_1^{i-1})$ と $H(U_i|U_1^{i-1}, Y_1^n)$ の両方について分極が生じる

	$H(U_i U_1^{i-1}) \approx 0$	$H(U_i U_1^{i-1}) \approx 1$
$H(U_i U_1^{i-1}, Y_1^n) \approx 0$	$n(1 - H(X))$ bits	$nC(W)$ bits
$H(U_i U_1^{i-1}, Y_1^n) \approx 1$	0 bits	$nH(X Y)$ bits

U_1^{i-1} から一意に定める必要あり(メッセージ割り当て不可)

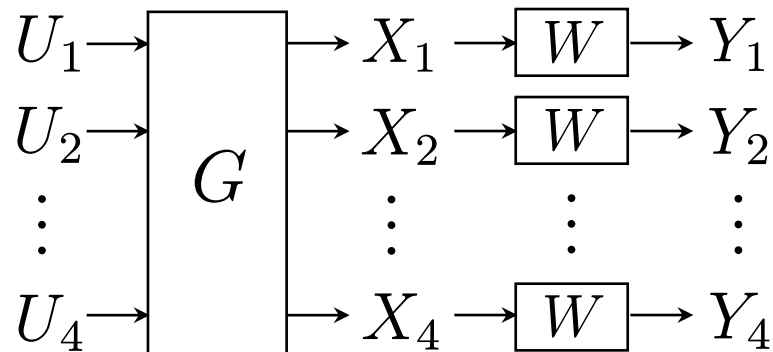


多段階の分極

- X_1^n が一様でない場合には $H(U_i|U_1^{i-1})$ と $H(U_i|U_1^{i-1}, Y_1^n)$ の両方について分極が生じる

	$H(U_i U_1^{i-1}) \approx 0$	$H(U_i U_1^{i-1}) \approx 1$
$H(U_i U_1^{i-1}, Y_1^n) \approx 0$	$n(1 - H(X))$ bits	$nC(W)$ bits
$H(U_i U_1^{i-1}, Y_1^n) \approx 1$	0 bits	$nH(X Y)$ bits

Y_1^n を見ても復元できない

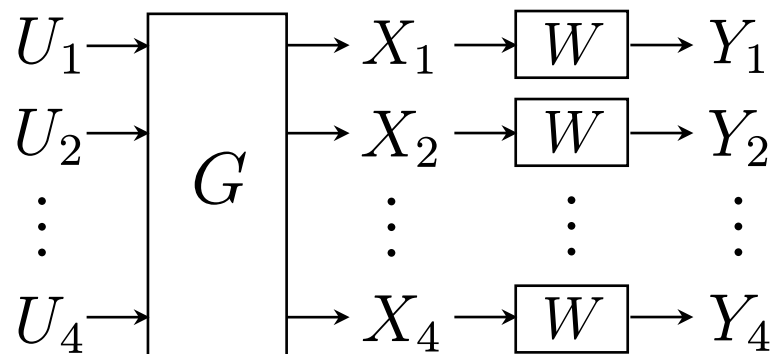


多段階の分極

- X_1^n が一様でない場合には $H(U_i|U_1^{i-1})$ と $H(U_i|U_1^{i-1}, Y_1^n)$ の両方について分極が生じる

	$H(U_i U_1^{i-1}) \approx 0$	$H(U_i U_1^{i-1}) \approx 1$
$H(U_i U_1^{i-1}, Y_1^n) \approx 0$	$n(1 - H(X))$ bits	$nC(W)$ bits
$H(U_i U_1^{i-1}, Y_1^n) \approx 1$	0 bits	$nH(X Y)$ bits

一様分布にしたがうメッセージを割り当てておけば
 Y_1^n を見て復元可能

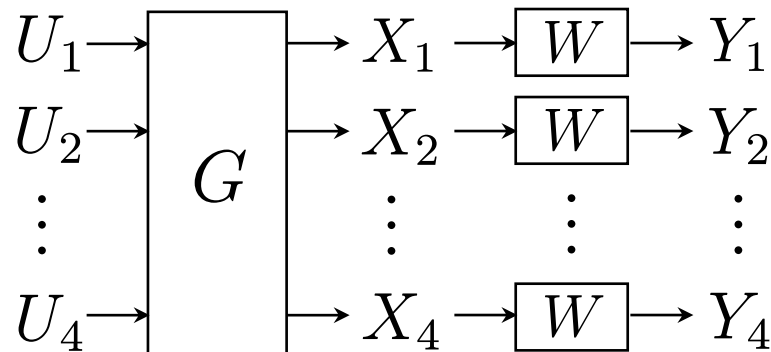


多段階の分極

- X_1^n が一様でない場合には $H(U_i|U_1^{i-1})$ と $H(U_i|U_1^{i-1}, Y_1^n)$ の両方について分極が生じる

	$H(U_i U_1^{i-1}) \approx 0$	$H(U_i U_1^{i-1}) \approx 1$
$H(U_i U_1^{i-1}, Y_1^n) \approx 0$	$n(1 - H(X))$ bits	$nC(W)$ bits
$H(U_i U_1^{i-1}, Y_1^n) \approx 1$	0 bits	$nH(X Y)$ bits

- それぞれのビットの値を適切に定めることで通信路容量を達成
[Honda-Yamamoto, 2012]



概要

- 非対称通信路の符号化
- polar符号を用いる方式
- 無歪み圧縮を用いた符号化法の一般的な枠組み
 - Miyake-Muramatsuの方式
 - 連鎖構造に基づく方式
- 無歪み圧縮の逆操作について

無歪み圧縮

- 出現分布の偏った系列 x^n をほぼ一様な短い系列 u^m に変換
 - 符号化と復号を入れ替えることで一様な系列を偏った系列に変換できる → 通信路符号化のための符号語を生成可能(?)
- 可変長無歪み圧縮 (ハフマン符号・算術符号……):
 - 出現確率が高い系列は短い符号語に, 小さい系列は長い符号語に符号化
 - 実用上よく用いられる
- 固定長無歪み圧縮 (LDPC符号・polar符号……):
 - 復号に失敗する場合がある
 - 他の目的の符号の構成要素として使いやすい

線形符号による固定長無歪み圧縮

- 情報源: $x^n \in \{0, 1\}^n$, 各要素は独立に
分布 $(P_X(0), P_X(1)) = (1 - p, p)$ にしたがう
- 符号化: $u^m := x^n H$, $H : n \times m$ 行列
- 復号: $\hat{x}^n := \operatorname{argmax}_{x^n: x^n H = u^m} P_{X^n}(x^n)$

復号誤り確率の解析:

- x^n は 2^n 通りあるが, それらのうち $2^{nH(X)}$ 個がほとんどの確率を占める
- $x^n \mapsto x^n H$ はほぼ「ランダムな」写像なので, $x^n \neq \tilde{x}^n$ で $x^n H = \tilde{x}^n H$ となる確率は 2^{-m} 程度
- $m > nH(p)$ ならば1に近い確率で正しく復号可能

概要

- 非対称通信路の符号化
- polar符号を用いる方式
- 無歪み圧縮を用いた符号化法の一般的な枠組み
 - Miyake-Muramatsuの方式
 - 連鎖構造に基づく方式
- 無歪み圧縮の逆操作について

Miyake-Muramatsu の方法による 非対称通信路の符号化

- Miyake-Muramatsu (2009, 固定長), Honda (2013, 可変長)
- 符号化:

- 無歪み圧縮の復号操作によりメッセージ u^m を確率分布

$$P_{\tilde{X}^n}(\tilde{x}^n) = \begin{cases} \frac{1}{C} \prod_{i=1}^n P_X(\tilde{x}_i), & \tilde{x}^n H = 0, \\ 0, & \tilde{x}^n H \neq 0, \end{cases}$$

にしたがう系列 $\tilde{x}^n$ に変換して送信 ($H : n \times k$ 行列)

- 復号:

- $\hat{x}^n := \operatorname{argmax}_{x^n: x^n H=0} P_{X^n|Y^n}(x^n|y^n)$ を計算

- 無歪み圧縮の符号化操作により $\hat{x}^n$ から $\hat{u}^m$ を復号

符号の解析

- 確率分布 $P_{\tilde{X}^n}(\tilde{x}^n)$ にしたがう系列は実質的に $2^{nH(X)-k}$ 通り
 - 無歪み圧縮の逆操作が可能な条件: $m < nH(X) - k$
- 受信系列 y^n が出現しうるような x^n は実質的に $2^{nH(X|Y)}$ 通り
 - $\tilde{x}^n$ の復号が可能な条件: $nH(X|Y) < k$
- $m < n(H(X) - H(X|Y))$ ならば y^n から u^m の復号が可能
→ 通信路容量 $C(W) = H(X) - H(X|Y)$ を達成

無歪み圧縮と線形符号を用いた 通信路符号の特徴

- 利点

- 2元符号のまま扱える
- 理論上は復号誤り確率を小さくしやすい

- 欠点

- 確率分布 $P_{\tilde{X}^n}(\tilde{x}^n) = \begin{cases} \frac{1}{C} \prod_{i=1}^n P_X(\tilde{x}_i), & \tilde{x}^n H = 0, \\ 0, & \tilde{x}^n H \neq 0, \end{cases}$

にしたがう系列を無歪み圧縮の逆操作により作る必要がある
(通常の無歪み圧縮は単に

$$P_{X^n}(x^n) = \prod_{i=1}^n P_X(x_i)$$

にしたがう系列を符号化できればいいのでそれより複雑)

Polar 符号による符号構成の別解釈

- Polar 符号による Honda-Yamamoto (2012) の方式は線形符号による通信路符号化と無歪み圧縮の両方に polar 符号を用いたものと解釈できる
 - 無歪み圧縮に polar 符号を用いる必然性はない
- 無歪み圧縮部分に可変長の homophonic 符号を用いることでも通信路容量を達成可能
 - 無歪み圧縮に関する分極が必要ないため(2次の)誤り指数が改善 (有歪み圧縮の場合の結果:

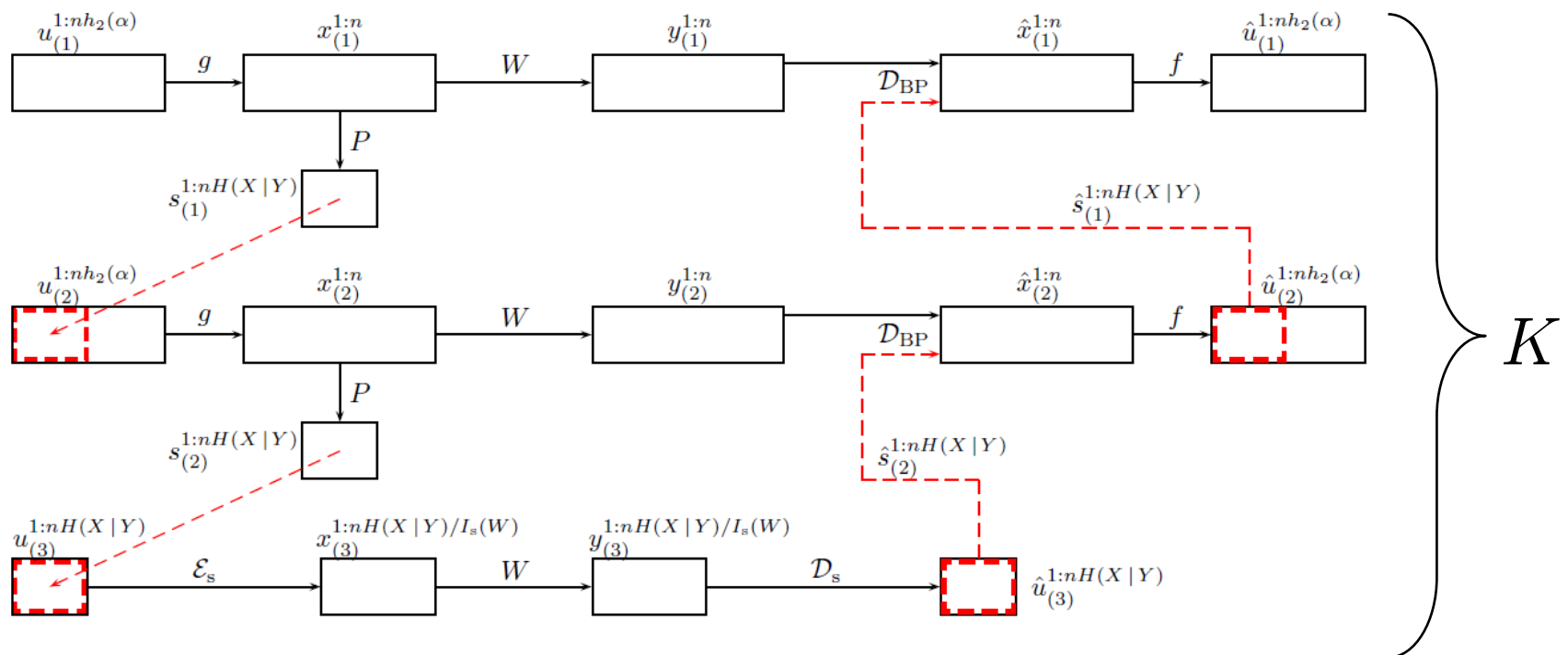
[Wang-Honda-Yamamoto-Rongke, 2015]]

概要

- 非対称通信路の符号化
- polar符号を用いる方式
- 無歪み圧縮を用いた符号化法の一般的な枠組み
 - Miyake-Muramatsuの方式
 - 連鎖構造に基づく方式
- 無歪み圧縮の逆操作について

連鎖構造を用いた通信路符号

- 符号語全体は部分符号語 K ブロックからなる
- 第 $i - 1$ ブロックの符号語を復号するための「手がかり」を第 i ブロックで送信



(図はMondelli-Hassani-Urbanke (2014) より)

符号化アルゴリズム

- $1, 2, \dots, K$ ブロックの順で部分符号語を構成
 - a. 第1ブロック: 無歪み圧縮の復号操作によりメッセージ $u_{(1)}^m$ を確率分布 P_{X^n} にしたがう系列 $x_{(1)}^n$ に変換
 - b. 第 $i = 2, \dots, K - 1$ ブロック:
 1. 前ブロックの符号語 $x_{(i-1)}^n$ から $s_{(i-1)}^k = x_{(i-1)}^n H$ を計算
 2. $m - k$ ビットのメッセージ $\tilde{u}_{(i)}^{m-k}$ と合わせた系列 $u_{(i)}^m = (s_{(i-1)}^k, \tilde{u}_{(i)}^{m-k})$ を分布 P_{X^n} にしたがう系列 $x_{(i)}^n$ に変換
 - c. 第 K ブロック: $s_{(K-1)}^k = x_{(K-1)}^n H$ を頻度分布が一様な符号語 $n' = k/I_s(W)$ ビットに符号化

復号アルゴリズム

- $K, K - 1, \dots, 1$ ブロックの順で部分符号語を推定
 - a. 第 K ブロック: 受信系列 $y_{(K)}^{n'}$ から $\hat{s}_{(K-1)}^k$ を復号
 - b. 第 $i = K - 1, \dots, 1$ ブロック:
 1. $x_{(i)}^n$ を $\hat{x}_{(i)}^n := \operatorname{argmax}_{x^n: x^n H = \hat{s}_{(i)}^k} P_{X^n}(x^n)$ により推定
 2. 無歪み圧縮の符号化により $\hat{x}_{(i)}^n$ から $\hat{u}_{(i)}^m$ を計算
- 復号可能な条件:
 - 無歪み圧縮の逆操作が可能: $m < nH(X)$
 - 第 $K - 1, \dots, 1$ ブロックの復号が可能: $nH(X|Y) < k$

符号長の解析

- 送信できる情報:
 - 第1ブロック: $m < nH(X)$ ビット
 - 第2, 3, $\dots$, $K - 1$ ブロック: $m - k < nC(W)$ ビット
 - 第 K ブロック: 0 ビット
- 符号長:
 - 第1, 2, $\dots$, $K - 1$ ブロック: n ビット
 - 第 K ブロック: $k/I_s(W) > nH(X|Y)/I_s(W)$ ビット
- 符号化率は $R < C(W) \cdot \frac{1 + \frac{H(X|Y)}{(K-1)C(W)}}{1 + \frac{H(X|Y)}{(K-1)I_s(W)}}$
 - $K \rightarrow \infty$ で通信路容量を達成

歴史

- Bocherer-Mathar (ITW2011): ガウス通信路に対して提案
 - 通信寄りの研究で理論寄りのコミュニティーには注目されず
- Sasoglu-Vardy (ISIT2013): 盗聴通信路への手法として提案
- Hassani-Urbanke (ISIT2014): ユニバーサル符号への応用
- Mondelli-Hassani-Sason-Urbanke (IEEE IT2015):
放送通信路への応用
- Mondelli-Hassani-Urbanke (IEEE IT2018):
通信路符号として改めて整理

性質

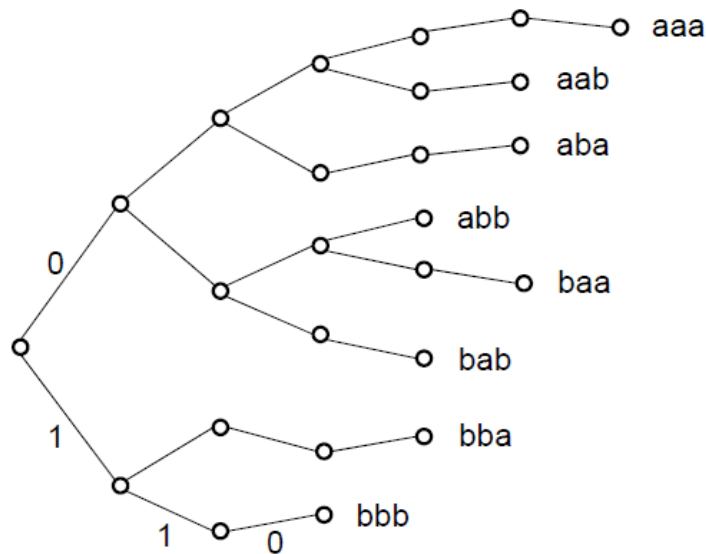
- 利点：
 - 無歪み圧縮に対応する操作で単にi.i.d.確率分布 P_{X^n} にしたがう系列を生成すればいい
 - 非対称通信路に限らず極めて多くの符号化問題に適用可能
- 欠点：
 - 部分符号語長 n だけでなくブロック数 K も大きい必要がある
 - 遅延が大きい・ブロック間で復号誤りが伝播
 - 可変長符号にやや適用しにくい

概要

- 通信路符号化と通信路容量
- Gallager の方法による非対称通信路符号化
- 無歪み圧縮を用いた非対称通信路符号化
 - Miyake-Muramatsu の方式
 - 連鎖構造に基づく方式
- 無歪み圧縮の逆操作について

無歪み圧縮の逆操作について

- 線形符号を用いた固定長無歪み圧縮は実際には性能が悪い
- 算術符号は適用不可(符号木が完全木でないため)



- Homophonic 符号化 (distribution matching) を用いる
 - 所望の確率分布 P_{X^n} をもつ系列 x^n を一様系列 u^n から生成
 - x^n から u^n を一意に復元可能

Homophonic 符号化法の例

- 区間アルゴリズムによるFV符号 [Hoshi-Han, 2001]
 - 非i.i.d.でも可, 理論的に非常に扱いやすい
 - 誤り伝播が生じる
- タイプ集合の数え上げに基づくFF符号 [Schulte-Bocherer, 2016]
 - FF符号なので実用上最も扱いやすい
 - 冗長度 $(\log n)/n$, 非i.i.d.の場合はほぼ使用不能
- 1シンボル復号遅延を許すVF符号 [Honda-Yamamoto, 2017]
 - 非i.i.d.の場合にも適用可能
 - 理論解析に細かい制約が入る

まとめ

- 通信路符号化ではまず対称通信路において通信路容量を達成する方法が考えられた
- 非対称通信路において容量を達成する通信を行うためには頻度分布が一様でない符号語を生成する必要がある
- 古くから知られていた Gallager の方法は実用上ほぼ動かない
- 無歪み圧縮に基づいた方式 (Miyake-Muramatsuの方式, 連鎖構造に基づく方式) が有望
- 無歪み圧縮の逆操作を実用的な性能で実現するには homophonic符号化 / distribution matching が必要