北海道大学
Hokkaido University

情報エレクトロニクス学科共通科目・2年次・夏ターム〔必修科目〕

講義「情報理論」

第10回

第7章 通信路符号化の限界(1)

通信路符号化の基礎概念
情報速度と冗長度
最尤復号法
通信路容量(前半)

通信路の統計的表現[復習]

- 通信路
  - 各時点において、一つの記号が入力され、一つの記号が出力される
  - 出力は入力から一意的に定まるのではなく、確率的に決まる

入力アルファベット $A=\{a_1,a_2,\ldots,a_r\}$の元	$\xrightarrow{X_t}$	通信路 Communication channel	$\xrightarrow{Y_t}$	出力アルファベット $B=\{b_1,b_2,\ldots,b_s\}$の元

$A=B$ かつ$|A|=r$のとき、r元通信路(r-ary channel)という

通信路の統計的性質は、任意の長さの入力系列$X_0 X_1 \ldots,X_{n-1}$とそれに対応する出力系列$Y_0 Y_1 \ldots Y_{n-1}$の確率分布が与えられれば完全に定まる。

$$P_{Y_0Y_1\ldots Y_{n-1}|X_0X_1\ldots X_{n-1}}(y_0, y_1, \ldots, y_{n-1} \mid x_0, x_1, \ldots, x_{n-1})$$

=〔$X_0 = x_0, X_1 = x_1, \ldots, X_{n-1}= x_{n-1}$ であるとき、$Y_0 = y_0, Y_1 = y_1, \ldots, Y_{n-1}= y_{n-1}$ となる確率 〕

記憶のない定常通信路[復習]

記憶のない通信路(memoryless channel)とは

各時点の出力の現れ方が、その時点の入力には関係するが、
それ以外の時点の入力・出力とは独立であるような通信路

$$P_{Y_0\cdots Y_{n-1}|X_0\cdots X_{n-1}}(y_0,\cdots,y_{n-1}|x_0,\cdots,x_{n-1}) = \prod_{i=0}^{n-1} P_{Y_i|X_i}(y_i|x_i)$$

定常通信路とは

時間をずらしても統計的性質が変わらない通信路

$$P_{Y_t\cdots Y_{t+n-1}|X_t\cdots X_{t+n-1}}(y_0,\cdots,y_{n-1}|x_0,\cdots,x_{n-1}) = P_{Y_0\cdots Y_{n-1}|X_0\cdots X_{n-1}}(y_0,\cdots,y_{n-1}|x_0,\cdots,x_{n-1})$$

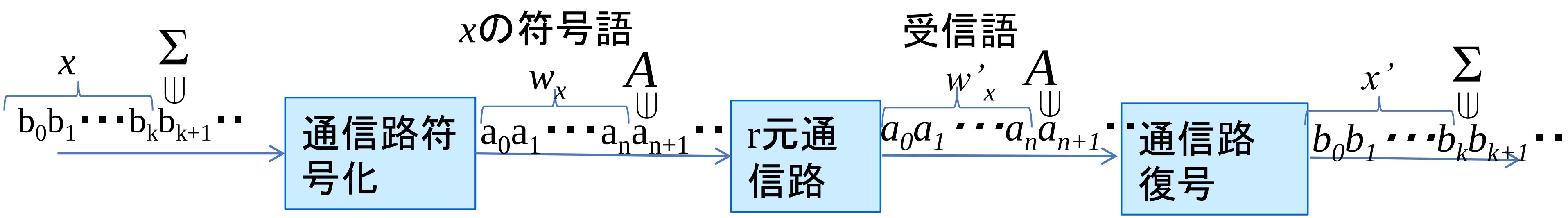
for all $t, n = 1,2,\cdots$

記憶のない定常通信路は

各時点において、入力Xが与えられたときの出力Yの条件付確率 $P_{Y|X}(y|x)$が同一

$$P_{Y_0\cdots Y_{n-1}|X_0\cdots X_{n-1}}(y_0,\cdots,y_{n-1}|x_0,\cdots,x_{n-1}) = \prod_{i=0}^{n-1} P_{Y|X}(y_i|x_i)$$

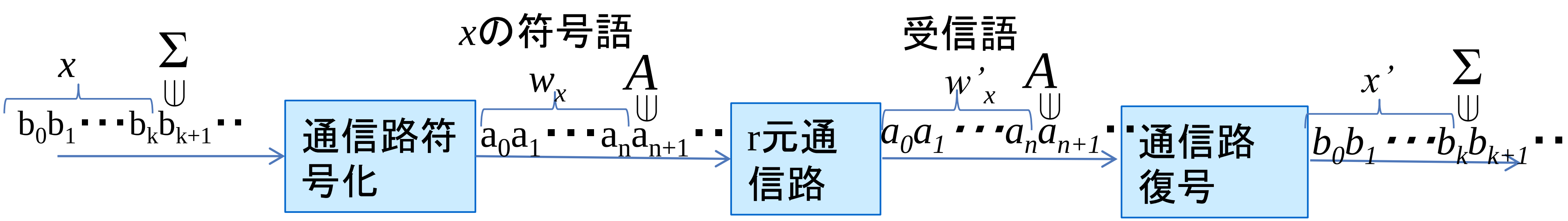
通信路符号の基礎概念(1)



Σ:q元アルファベット　　A:r元アルファベット

- 通信路符号化の目的: 信頼性の向上　そのために→冗長性を付加
- 長さkのブロック$\mathbf{x}\in\Sigma^k$を長さnの符号語$\mathbf{w_x}\in A^n$に符号化
- $q^k < r^n$: 符号語としてA^nの一部のみ使用 (冗長性の付加)

通信路符号の基礎概念(2)



Σ:q元アルファベット　　A:r元アルファベット

[例]$\Sigma=\{0,1\}$, $k=1$,$A=\{0,1\}$,$n=3$ とすれば、

$$A^3=\{000, 001, 010, 011, 100, 101, 110, 111\}$$

この内、000 と 111 の二つだけを符号語として用いる

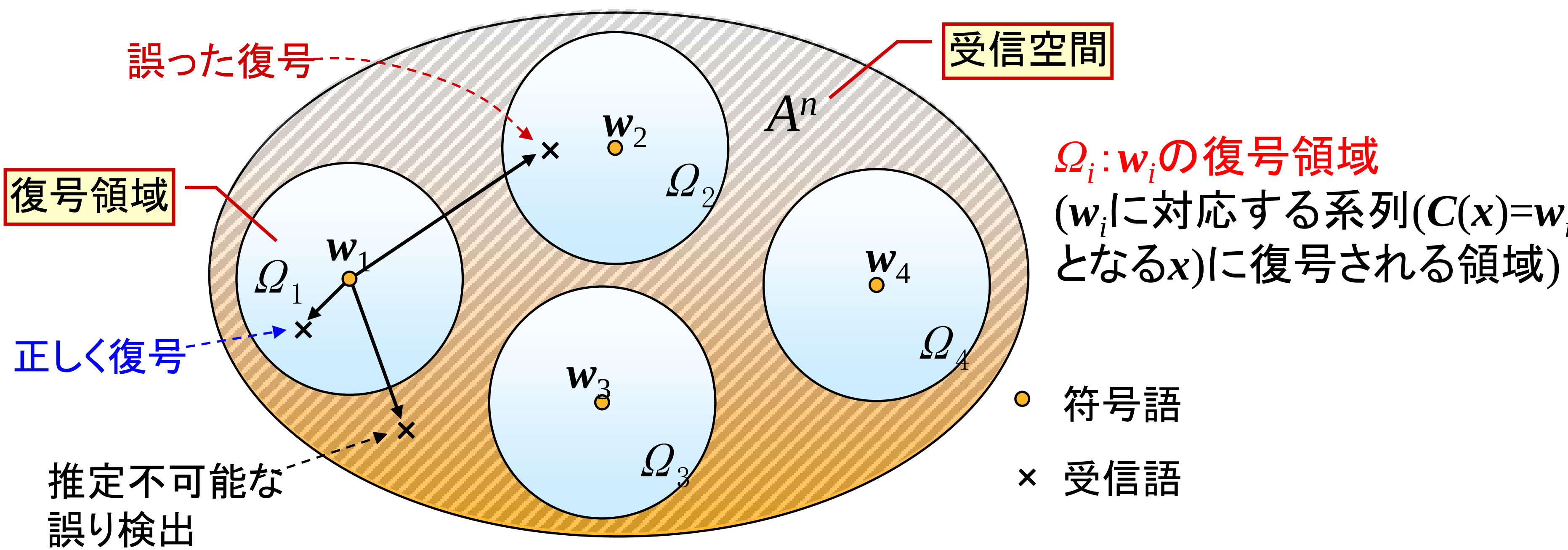
$$0 \rightarrow 000, \qquad 1 \rightarrow 111$$

このとき、送った符号語w_xに1ビット誤りが生じた受信語w'_xを受け取っても、w'_x内の3ビットの多数決により訂正可能

$$001, 010, 100 \rightarrow 0, \qquad 110, 101, 011 \rightarrow 1$$

通信路符号の基礎概念(3)

- **通信路符号**(または**符号**):A^n の中から選ばれた系列の集合 C
- 図は通信路符号による誤り訂正の概念図



図(通信路符号の)復号の概念図

情報速度と冗長度

- 符号$C(\subseteq A^n)$に含まれる符号語の数を$M(=q^k)$とする。
- 符号Cの情報(伝送)速度 R:

符号Cを用いて伝達可能な1記号あたりの最大平均情報量

$$R = \frac{\log_2 M}{n} \quad \text{（ビット／記号）}$$

(符号語を受け取ることにより得られる最大平均情報量$\log_2 M$を符号語の長さnで割った値)

- A^n に含まれる r^n 個の系列すべてを符号語とすれば、情報速度は最大値

$$R_{\max} = (\log_2 r^n) / n = \log_2 r$$

となる。$R < R_{\max}$ とすることで、誤りの訂正や検出が可能となる。

すべての系列を使うと誤りを検知できない

- 情報速度Rの符号Cの効率 (符号化率（code rate）) η と 冗長度ρ:

$$\eta = R / R_{\max}, \quad \rho = 1 - \eta$$

$0 \leqq \eta \leqq 1$, $0 \leqq \rho \leqq 1$ が成り立つ。

冗長度≒信頼性
冗長度と効率はTrade-off

最尤復号法(1)

$\boldsymbol{\Omega}_1, \boldsymbol{\Omega}_2, \ldots, \boldsymbol{\Omega}_M$: 符号語 $\boldsymbol{w}_1, \boldsymbol{w}_2, \ldots, \boldsymbol{w}_M$ の復号領域

正しく復号される確率を最大にする復号領域の求め方は？

⇒(符号語の発生確率が等確率の場合は)最尤復号法!

$P(\boldsymbol{y} \mid \boldsymbol{w}_i)$: $\boldsymbol{w}_i$ を送ったとき $\boldsymbol{y}$ が受信される確率

最尤復号法

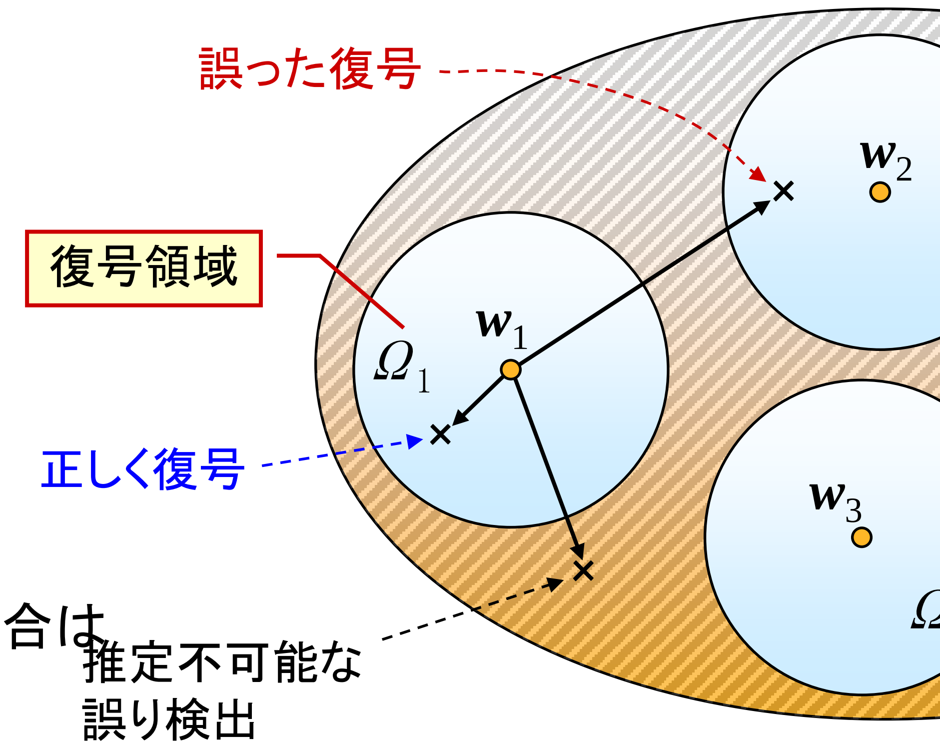
$\boldsymbol{y}$ が受信されたとき、

$P(\boldsymbol{y} \mid \boldsymbol{w}_i)$が最大の$\boldsymbol{w}_i$に復号

最尤復号法の復号領域

$$\boldsymbol{\Omega}_i = \{\boldsymbol{y} \mid i = \mathrm{argmax}_j\, P(\boldsymbol{y} \mid \boldsymbol{w}_j)\}$$

※ $\mathrm{argmax}_j\, P(\boldsymbol{y} \mid \boldsymbol{w}_j)$が複数存在する場合は、
その内の1つに固定する。



最尤復号法は正しく復号される確率が最大

正しく復号される確率を最大にする復号法における符号語 $w_1, w_2, \cdots, w_M$の復号領域を$\Omega_1, \Omega_2, \cdots, \Omega_M$とすれば

$$\Omega_i \cap \Omega_j = \phi, \cup_{i=1}^{M} \Omega_i = A^n$$

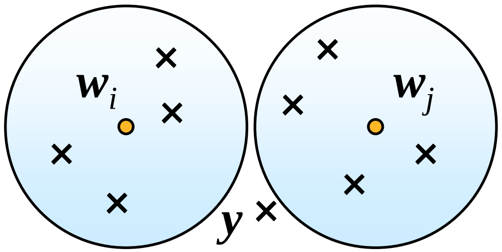
が成り立つと仮定してよい。この時、各々の受信語yはただ1つの符号語w_iの復号領域Ω_iに含まれるので、yに対応するw_iを$\omega(y)$とおく。符号語が等確率で発生するとき正しく復号される確率をP_cとすれば

$$P_c = \frac{1}{M}\sum_{i=1}^{M}\sum_{y\in\Omega_i} P(y|w_i) = \frac{1}{M}\sum_{y\in A^n} P(y|\omega(y))$$

これを最大にするには各yに対して$P(y|\omega(y))$が最大となるように$\omega(y)$を選べば良い、つまり

$$\omega(y) = \underset{w_i}{\operatorname{argmax}}\, P(y|w_i)$$

と復号すればよく、これは最尤復号法に他ならない。



- w_i をyの分布のパラメータだとみなせば$P(y|w_i)$ はw_iの尤度である。
  尤度を最大化する復号法⇒最尤復号法（maximum likelihood decoding）
- すべての符号語w_i に対し、$P(y|w_i)$を計算し比較しなければならず、符号語数 M が大きい場合には、実用的ではない。

ちょっと休憩

通信路容量(1/5)

通信路の**通信路容量**:

通信路ごとに定まる、

その通信路を介して伝送できる情報速度の限界値

つまり、その通信路を介して、

送ることができる1記号あたりの平均情報量の上限

通信路容量の定義(2/5)

入力アルファベット $\boldsymbol{A}=\{a_1,a_2,\ldots,a_r\}$の元 $\xrightarrow{X}$ 定常通信路 $\xrightarrow{Y}$ 出力アルファベット $\boldsymbol{B}=\{b_1,b_2,\ldots,b_s\}$の元

$P_{Y|X}$

定常通信路のモデル

$P_{Y|X}$: 定常通信路の定常条件付き確率分布

- 1記号Xを送ると1記号Yが受信される
  ⇒平均的には1記号あたり相互情報量$I(X;Y)$だけ情報が送られる
- 入力Xの分布は自由に変えることができるが、Xの分布P_Xが定まればYの分布はP_Xと$P_{Y|X}$から定まる

この通信路を介しておくることができる1記号あたりの平均情報量の上限は

$$\max_{P_X} I(X;Y)$$

通信路容量の定義(3/5)

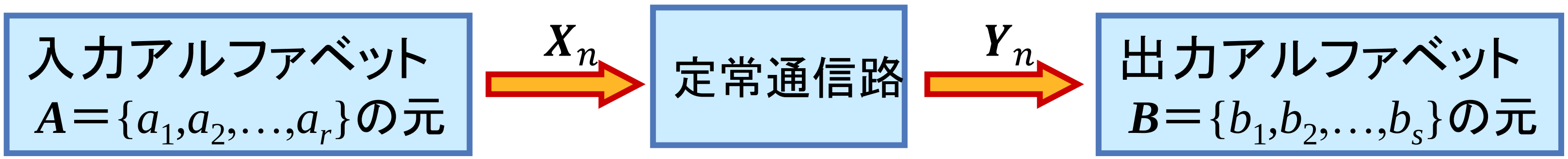
以上の考察から通信路容量Cの定義は

$$C = \max_{P_X} I(X;Y)\ ?$$

無記憶通信路の場合はYES。記憶のある通信路の場合はNO。

記憶のある通信路の場合$n(>1)$記号ごとみると
もっと多くの情報を送れる!

通信路容量の定義(4/5)



$P_{\boldsymbol{Y}_n|\boldsymbol{X}_n}$

定常通信路のモデル

$P_{\boldsymbol{Y}_n|\boldsymbol{X}_n}$: 定常通信路の定常条件付き確率分布

- n記号$\boldsymbol{X}_n$を送るとn記号$\boldsymbol{Y}_n$が受信される
  ⇒平均的には1記号あたり相互情報量$I(\boldsymbol{X}_n;\boldsymbol{Y}_n)/n$だけ情報が送られる
- 入力$\boldsymbol{X}_n$の分布は自由に変えることができるが、$\boldsymbol{X}_n$の分布$P_{\boldsymbol{X}_n}$が定まれば$\boldsymbol{Y}_n$の分布は$P_{\boldsymbol{X}_n}$と$P_{\boldsymbol{Y}_n|\boldsymbol{X}_n}$から定まる

この通信路を介しておくることができる1記号あたりの平均情報量の上限は

$$\max_{P_{\boldsymbol{X}_n}} I(\boldsymbol{X}_n;\boldsymbol{Y}_n)/n$$

式を入力

通信路容量の定義(5/5)

[定義7.1]長さnの入力系列$\boldsymbol{X}_n$に対する通信路の出力系列$\boldsymbol{Y}_n$に対し

$$C = \lim_{n\to\infty} \max_{P_{X_n}} \frac{I(\boldsymbol{X}_n;\boldsymbol{Y}_n)}{n}$$

で定義されるCを通信路容量(channel capacity)と呼ぶ。

通信路容量の単位:

ビット(またはナット、ハートレー)あるいはビット/通信路記号

記憶のない定常通信路の通信路容量

[定理7.1]入力記号Xに対し記号Yが出力される記憶のない通信路の通信路容量は

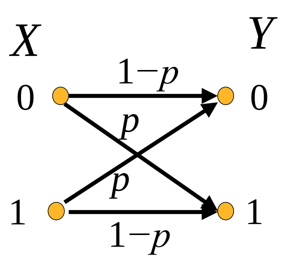
$$C = \max_{P_X} I(X;Y)$$

で計算できる。

証明は意外と煩雑なので省略(興味のある人は教科書7.5節参照)

2元対称通信路の通信路容量(1/2)

2元対称通信路（binary symmetric channel; BSC）



通信路の統計的性質:

$$P_{Y|X}(0|1) = P_{Y|X}(1|0) = p$$
$$P_{Y|X}(0|0) = P_{Y|X}(1|1) = 1 - p$$

この通信路の通信路容量 $C = \max_{P_X} I(X;Y)$を求める

$I(X;Y) = H(Y) - H(Y|X)$である。

$$\begin{aligned} H(Y|X) &= P_X(0)\,H(Y|X=0) + P_X(1)\,H(Y|X=1) \\ &= P_X(0)\mathcal{H}(p) + P_X(1)\mathcal{H}(p) = \mathcal{H}(p) \end{aligned}$$
$$H(Y) = \mathcal{H}(P_Y(1))$$

である。ただし、$\mathcal{H}(x) = -x\log_2 x - (1-x)\log_2(1-x)$ (エントロピー関数)。

$q = P_X(1)$とおくと

$$P_Y(1) = (1-q)p + q(1-p) = p + q - 2pq$$

よって

$$I(X;Y) = \mathcal{H}(p + q - 2pq) - \mathcal{H}(p)$$

2元対称通信路の通信路容量(2/2)

$$C = \max_{P_X} I(X;Y) = \max_{q}(\mathcal{H}(p+q-2pq) - \mathcal{H}(p))$$

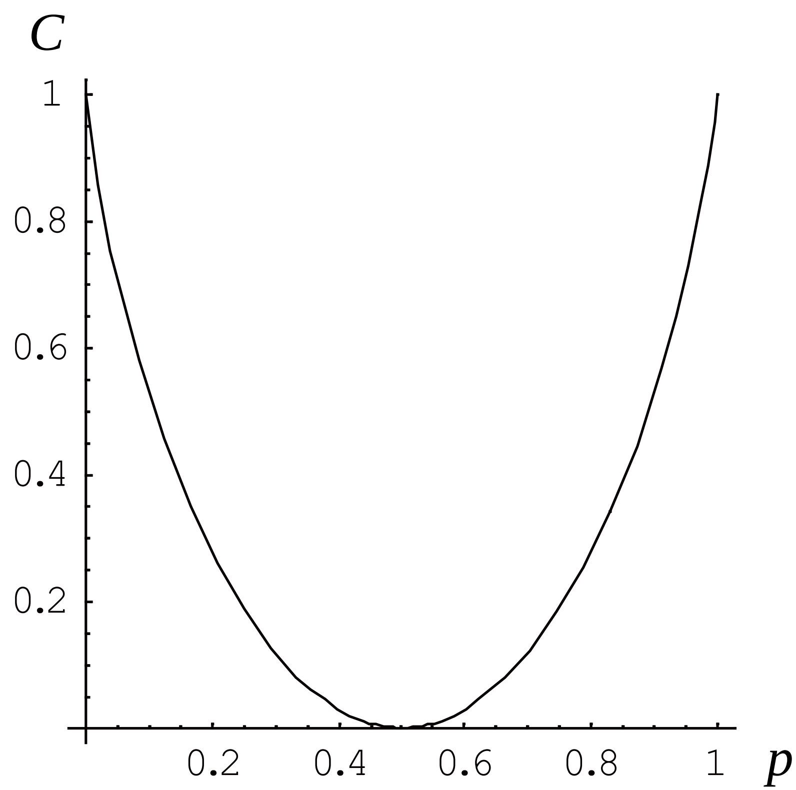
$q = 1/2$のとき、$p + q - 2pq = 1/2$となり$\mathcal{H}(p+q-2pq)$は最大値1をとるから

$$C = 1 - \mathcal{H}(p)$$

$p=0 \Rightarrow C=1$(ビット/記号)
(誤りを生じない場合⇒情報は完全に伝わる)

$p=0.5 \Rightarrow C=0$(ビット/記号)
(出力が入力と独立な場合
⇒情報は全く伝わらない)

$p=1 \Rightarrow C=1$(ビット/記号)
(常に誤る場合⇒情報は完全に伝わる)



2元対称通信路の通信路容量