応用数学５ 2010 年 6 月 8 日

Shannon の通信路符号化定理

講師: 安永憲司

1 通信モデル

ここでは，Shannon が 1948 年に発表した論文 “A mathematical theory of communication” で提起した通信の問題を考える．Shannon は通信の根本的な問題は「ある地点で選ばれたメッセージを別のある地点で正確にまたは近似的に再生すること」であると考えた．その地点同士は，空間的に離れているかもしれないし，時間的に離れているかもしれない．そこで，その離れた地点同士は，通信路を通してつながっていると考える．工学的な視点に立てば，この通信の問題をいかに効率的に解くかが問題となる．

通信路では雑音が加わることも考えられる．

- **雑音なしの場合:** 通信において誤りは発生しない．情報源の冗長性が問題となる．データ圧縮もしくは情報源符号化と呼ばれる操作を行うことで対処する．
- **雑音ありの場合:** 通信において誤りが発生するかもしれない．誤りの発生によって元の情報が取り出せないことが問題となる．通信路符号化という操作で冗長性を加えることで対処する．

通信のモデル化のひとつとして以下のようなものが考えられる．

[**情報源**] → [**情報源符号化**] → [**通信路符号化**] → [**通信路**] → [**通信路復号**] → [**情報源復号**] → [**目的地**]

Shannon は，情報源のエントロピーが通信路の容量よりも小さいならば，上手に符号化を行うことで，信頼ある通信が可能なことを示した．さらに，符号化は情報源符号化と通信路符号化に分けて考えてよいことも示した．本講義では，通信路符号化の問題だけを扱う．

2 通信路の例

Shannon は，通信路として確率的な通信路を考えた．いくつかの例を紹介する．

1. **二元対称通信路 (Binary Symmetric Channel):** 入出力アルファベットは $\{0,1\}$ であり，確率 $p, 0 \le p \le 1/2$ で値が反転する．BSC_p で反転確率 p の二元対称通信路を表す．
2. **q 元対称通信路 (q-ary Symmetric Channel):** 入出力アルファベットはサイズが q であり，確率 $p, 0 \le p \le 1 - 1/q$ で値が他のアルファベットになる．つまり，x を送信したとき，x を受信する確率が $1-p$，x 以外のアルファベットを受信する確率はそれぞれ $p/(q-1)$ である．
3. **二元消失通信路 (Binary Erasure Channel):** 入力アルファベットは $\{0,1\}$ であり，出力アルファベットは $\{0,1,?\}$．入力値は，確率 $\alpha, 0 \le \alpha \le 1$ で ? になる．BEC_α で消失確率 α の二元消失通信路を表す．
4. **二値入力加法的白色ガウス雑音通信路 (Binary Input Additive White Gaussian Noise Channel):** 入力アルファベットは $\{1,-1\}$ で，出力アルファベットは $\mathbb{R}$．入力 x が通信路を通ると出力は $y = x + z$ であり，z は平均 0 で分散 σ^2 の正規分布に従う．つまり，x を送信したときに y を受信する確率密度関

数は，

$$\Pr[y|x] = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{(y-x)^2}{2\sigma^2}\right).$$

3 Shannon の通信路符号化定理

定理 1 (二元対称通信路に対する Shannon の通信路符号化定理) 任意の実数 $0 < p < 1/2$ と $0 < \epsilon < 1/2 - p$ に対して，n が十分に大きいとき，以下が成り立つ．

- **(順定理)** $k \leq \lfloor (1 - H(p+\epsilon))n \rfloor$ のとき，ある実数 $\delta > 0$，符号化関数 $E : \{0,1\}^k \to \{0,1\}^n$ と復号関数 $D : \{0,1\}^n \to \{0,1\}^k$ が存在し，すべての $m \in \{0,1\}^k$ について，

$$\Pr_{e:\mathrm{BSC}_p\text{の雑音}}[D(E(m)+e) \neq m] \leq 2^{-\delta n}.$$

- **(逆定理)** $k \geq \lfloor (1 - H(p) + \epsilon)n \rfloor$ のとき，任意の符号化関数 $E : \{0,1\}^k \to \{0,1\}^n$ と復号関数 $D : \{0,1\}^n \to \{0,1\}^k$ に対して，ある $m \in \{0,1\}^k$ が存在し，

$$\Pr_{e:\mathrm{BSC}_p\text{の雑音}}[D(E(m)+e) \neq m] \geq \frac{1}{2}.$$

補足 2 上記の定理から，BSC_p の通信路容量は $1 - H(p)$ であることがわかる．また，BEC_α の通信路容量は，$1 - \alpha$ であると示すことができる．

4 Shannon の通信路符号化逆定理の証明

補題 3 (Chernoff 限界) $X_1, X_2, \ldots, X_n$ が，$\Pr[X_i = 1] = p$ であるような，$\{0,1\}$ 上の値をとる独立同分布確率変数とする．このとき，任意の $0 < \epsilon < 1$ に対し，n が十分大きいとき，

$$\Pr\left[\sum_{i=1}^{n} X_i \geq (p+\epsilon)n\right] \leq 2^{-\epsilon^2 n/3},$$

$$\Pr\left[\sum_{i=1}^{n} X_i \leq (p-\epsilon)n\right] \leq 2^{-\epsilon^2 n/3}.$$

補題 4 十分大きな n，$0 \leq p \leq 1/2$ に対して，

$$2^{(H(p)-\mathrm{o}(1))n} \leq \mathrm{Vol}(n, pn) \leq 2^{H(p)n}.$$

まず，直感的な証明を与える．逆定理では，任意に誤り率を小さくするには，レートが $1-H(p)$ 以下でなければならないことを示唆している．Chernoff 限界から，BSC_p を通すと，発生する誤りの数は高い確率で $(p - \mathrm{o}(1))n$ と $(p + \mathrm{o}(1))n$ の間であることがわかる．このことから，符号語 c を送ったとき，高い確率で受信語となる系列は，おおよそ $2^{H(p)n}$ 個となる．符号語 c を正しく復号するには，復号関数 D はこれらの系列を c へと復号する必要がある．つまり，各符号語 $c \in C$ に対して，$|D^{-1}(c)| \approx 2^{H(p)n}$ でなければならない．したがって，符号語数の上界として $|C| \leq 2^{(1-H(p)-\mathrm{o}(1))n}$ が導かれる．

証明 (Shannon の通信路符号化逆定理):

符号化関数を $E : \{0,1\}^k \to \{0,1\}^n$, 復号関数を $D : \{0,1\}^n \to \{0,1\}^k$ とする．矛盾を導くため，任意の $m \in \{0,1\}^k$ に対して

$$\Pr_{e:\mathrm{BSC}_p\text{の雑音}}[D(E(m)+e) \neq m] < \frac{1}{2}$$

であると仮定する．

任意にメッセージ $m \in \{0,1\}^k$ を固定する．メッセージ m に復号する受信語集合 D_m を次のように定義する;

$$D_m = \{y \in \{0,1\}^n : D(y) = m\}.$$

仮定より，以下が成り立つ:

$$\Pr_{e:\mathrm{BSC}_p\text{の雑音}}[E(m)+e \notin D_m] < \frac{1}{2}. \tag{1}$$

点 $E(m)$ を中心とした半径 $(1+\gamma)pn$ のハミング球から，半径 $(1-\gamma)pn$ のハミング球をくり抜いたものを S_m とする．つまり，

$$S_m = B(E(m),(1+\gamma)pn) \setminus B(E(m),(1-\gamma)pn).$$

このとき，Chernoff 限界より，

$$\Pr_{e:\mathrm{BSC}_p\text{の雑音}}[E(m)+e \notin S_m] \leq 2^{-\Omega(\gamma^2 n)}. \tag{2}$$

式 (1), (2) より，

$$\begin{aligned}
&\Pr_{e:\mathrm{BSC}_p\text{の雑音}}[E(m)+e \in D_m \cap S_m] \\
&= 1 - \Pr_{e:\mathrm{BSC}_p\text{の雑音}}[E(m)+e \notin D_m \cap S_m] \\
&\geq 1 - \left(\Pr_{e:\mathrm{BSC}_p\text{の雑音}}[E(m)+e \notin D_m] + \Pr_{e:\mathrm{BSC}_p\text{の雑音}}[E(m)+e \notin S_m] \right) \\
&\geq 1 - \left(\frac{1}{2} + 2^{-\Omega(\gamma^2 n)} \right) \\
&\geq \frac{1}{4}.
\end{aligned} \tag{3}$$

ただし，最後の不等式は，n が十分大きいときに成り立つ．

また，次式が成り立つことがわかる．

$$\Pr_{e:\mathrm{BSC}_p\text{の雑音}}[E(m)+e \in D_m \cap S_m] \leq |D_m \cap S_m| \cdot p_{\max},$$

ここで，

$$p_{\max} = \max_{y \in S_m} \Pr[E(m)+e=y] = \max_{d \in [(1-\gamma)pn,(1+\gamma)pn]} p^d (1-p)^{n-d}.$$

式 $p^d(1-p)^{n-d}$ は，$p \leq 1/2$ の範囲で， d に関して減少関数であることがわかるので，

$$\begin{aligned}
p_{\max} &= p^{(1-\gamma)pn}(1-p)^{n-(1-\gamma)pn} \\
&= \left(\frac{1-p}{p}\right)^{\gamma pn} p^{pn}(1-p)^{(1-p)n} \\
&= \left(\frac{1-p}{p}\right)^{\gamma pn} 2^{-H(p)n}.
\end{aligned}$$

したがって，

$$\Pr_{e:\mathrm{BSC}_p\text{の雑音}}[E(m)+e\in D_m\cap S_m]\le |D_m\cap S_m|\left(\frac{1-p}{p}\right)^{\gamma pn}2^{-H(p)n}. \tag{4}$$

式 (3), (4) より，

$$|D_m\cap S_m|\ge \frac{1}{4}\left(\frac{1-p}{p}\right)^{-\gamma pn}2^{H(p)n}. \tag{5}$$

このとき，次の不等式が成り立つ．

$$\begin{aligned}
2^n &= \sum_{m\in\{0,1\}^k}|D_m| && \because m_1\neq m_2 \text{ に対して } D_{m_1}\cap D_{m_2}=\emptyset\\
&\ge \sum_{m\in\{0,1\}^k}|D_m\cap S_m| &&\\
&\ge \frac{1}{4}\left(\frac{1-p}{p}\right)^{-\gamma pn}2^{H(p)n}\cdot 2^k && \text{式 (5) より}\\
&= 2^{k-2}2^{H(p)n-\gamma pn\log_2(1/p-1)} &&\\
&> 2^{k+H(p)n-\epsilon n} && \gamma=\frac{\epsilon}{2p\log_2(1/p-1)}.
\end{aligned}$$

最後の不等式は，n が十分大きいときに成り立つ．この不等式より，$k<(1-H(p)+\epsilon)n$ となるが，これは仮定に矛盾する．■

5 Shannon の通信路符号化定理の証明

はじめに，証明のための直感的なアイディアを述べる．Chernoff 限界より，高い確率で pn 個程度の誤りが発生することがわかる．これらの誤りを訂正するために，各符号語の距離を $2pn$ 以上離せば十分である．しかし，各符号語に対し，他の符号語がすべて距離 $2pn$ 以上離れるようにする必要はない．約 pn 個の誤りが発生するとして，そのような誤りパターンの多くに対して，復号するときに符号語が一意に特定できれば十分である．言い換えると，約 $2^{(1-H(p))n}$ 個のほぼ重ならない半径 pn のハミング球を $\{0,1\}^n$ 上に配置することができればよいのである．

証明 (Shannon の通信路符号化定理): $\ell=k+1$ とする．符号化関数 $E:\{0,1\}^\ell\to\{0,1\}^n$ は，すべての可能な関数の中から一様ランダムに選ばれるとする．つまり，各メッセージ $m\in\{0,1\}^\ell$ に対して，$E(m)$ は $\{0,1\}^n$ から一様ランダムに選ばれる．十分小さい定数として $\gamma>0$ を選ぶ．復号関数 $D:\{0,1\}^n\to\{0,1\}^\ell$ は次のように定義する．

$$D(y)=\begin{cases} m & d(y,E(m))\le (p+\gamma)n \text{ である } E(m) \text{ が唯一存在するとき}\\ \text{失敗} & \text{上記以外の場合.}\end{cases}$$

また，BSC_p を通して雑音 $e\in\{0,1\}^n$ が発生する確率を $\mathrm{pr}(e)$ とする．すると，$\mathrm{pr}(e)=p^{\mathrm{wt}(e)}(1-p)^{n-\mathrm{wt}(e)}$.

ある固定したメッセージ m に対して，BSC_p を通したとき，復号した結果が m にならない確率を見積もると，

$$\begin{aligned}
\Pr_{e:\mathrm{BSC}_p\text{の雑音}}[D(E(m)+e)\neq m] &\le \Pr_{e:\mathrm{BSC}_p\text{の雑音}}[\mathrm{wt}(e)>(p+\gamma)n]+\sum_{e\in B(0,(p+\gamma)n)}\mathrm{pr}(e)\mathbf{1}(D(E(m)+e)\neq m)\\
&\le 2^{-\Omega(\gamma^2 n)}+\sum_{e\in B(0,(p+\gamma)n)}\mathrm{pr}(e)\sum_{m\neq m'}\mathbf{1}(d(E(m)+e,E(m'))\le (p+\gamma)n)
\end{aligned}$$

ここで，$\mathbf{1}(\cdot)$ は指示関数 (つまり，$\mathbf{1}(\mathrm{Ev})$ は事象 Ev が真なら 1，それ以外は 0) である．最後の不等式の一つ目の項は， Chernoff 限界を利用している．二つ目の項は，$(p+\gamma)n$ 個以内の誤りが発生したときに復号に失敗する確率を見積もっており，これは，別のメッセージ m' が距離 $(p+\gamma)n$ 以内にあるときである．

一様ランダムに選ぶ符号化関数 E に対して，この確率を見積もる．固定した e と $m \neq m'$ に対して，

$$\begin{aligned}\mathop{\mathbb{E}}_{\text{ランダムな } E}[\mathbf{1}(d(E(m)+e, E(m')) \leq (p+\gamma)n)] &\leq \mathop{\Pr}_{\text{ランダムな } E}[d(E(m)+e, E(m')) \leq (p+\gamma)n] \\ &= \frac{\mathrm{Vol}(n, (p+\gamma)n)}{2^n} \\ &\leq 2^{-(1-H(p+\gamma))n}.\end{aligned}$$

すると，期待値の線形性より，

$$\begin{aligned}\mathop{\mathbb{E}}_{\text{ランダムな } E}\Big[\mathop{\Pr}_{e:\mathrm{BSC}_p\text{の雑音}}[D(E(m)+e) \neq m]\Big] &\leq 2^{-\Omega(\gamma^2 n)} + \sum_{e \in B(0,(p+\gamma)n)} \mathrm{pr}(e) 2^{\ell} 2^{-(1-H(p+\gamma))n} \\ &\leq 2^{-\Omega(\gamma^2 n)} + 2^{\ell} 2^{-(1-H(p+\gamma))n} \\ &\leq 2^{-\Omega(\gamma^2 n)} + 2^{(1-H(p+\epsilon))n+1} 2^{-(1-H(p+\gamma))n} \\ &= 2^{-\Omega(\gamma^2 n)} + 2 \cdot 2^{-(H(p+\epsilon)-H(p+\gamma))n} \\ &< \frac{1}{2} \cdot 2^{-\delta n}.\end{aligned}$$

ただし，最後の不等式は，γ が十分小さいときに，ある $\delta > 0$ に対して成り立つ．上の不等式は，ある固定した m に対して，復号を誤る確率が小さいことを示している．定理では，すべてのメッセージに対して，誤り確率が小さいことを示さなければならない．メッセージは 2^{ℓ} 個あるので，単純に和集合上界をとると，誤り確率を小さく抑えることができない．そこで，以下のような方法を考える．

固定したメッセージ m に対して，$\mathbb{E}_{\text{ランダムな } E}[\Pr_{e:\mathrm{BSC}_p\text{の雑音}}[D(E(m)+e) \neq m]] < 2^{-1-\delta n}$ であるので，メッセージをランダムに選んだときに平均的に成り立つはずである．つまり，

$$\mathop{\mathbb{E}}_{\text{ランダムな } m}\Big[\mathop{\mathbb{E}}_{\text{ランダムな } E}\Big[\mathop{\Pr}_{e:\mathrm{BSC}_p\text{の雑音}}[D(E(m)+e) \neq m]\Big]\Big] < 2^{-1-\delta n}.$$

平均の順番を取り替えると，

$$\mathop{\mathbb{E}}_{\text{ランダムな } E}\Big[\mathop{\mathbb{E}}_{\text{ランダムな } m}\Big[\mathop{\Pr}_{e:\mathrm{BSC}_p\text{の雑音}}[D(E(m)+e) \neq m]\Big]\Big] < 2^{-1-\delta n}.$$

上記不等式より，ある符号化関数 E^* が存在して，

$$\mathop{\mathbb{E}}_{\text{ランダムな } m}\Big[\mathop{\Pr}_{e:\mathrm{BSC}_p\text{の雑音}}[D(E^*(m)+e) \neq m]\Big] < 2^{-1-\delta n}.$$

平均化原理より，メッセージ $m \in \{0,1\}^{\ell}$ の半分以下に対しては，$\Pr_{e:\mathrm{BSC}_p\text{の雑音}}[D(E^*(m)+e) \neq m] \geq 2^{-\delta n}$ である．これらのメッセージを削除することで，ある符号化関数 $E' : \{0,1\}^k \to \{0,1\}^n$ と復号関数 D' が存在し，すべての $m \in \{0,1\}^k$ に対して，$\Pr_{e:\mathrm{BSC}_p\text{の雑音}}[D'(E'(m)+e) \neq m] < 2^{-\delta n}$ であることがわかる．■

6 Hamming vs Shannon

Hamming	Shannon
符号化や復号には触れず，符号語自体に注目	符号化関数と復号関数を定めている
構成的な方法	非構成的な方法
レートと距離の間のトレードオフ	レートと誤り確率の間のトレードオフ
最悪ケース誤り (誤り数に制限)	確率的な誤り