1　2元対称通信路

$A = B = \{1, -1\}$, $1 > q > 1/2$ とし, 2 元対称通信路 $Q = \begin{pmatrix} q & 1-q \\ 1-q & q \end{pmatrix}$ に対する通信路符号化定理を見る.

この通信路の通信容量は記号 $h(q) := -q\log_2 q - (1-q)\log_2(1-q)$ を用いて

$$C := 1 - h(q) \text{ [bit]}$$

である.

1.1　準備

n と $\mathcal{C} \subset \{0,1\}^n$ が与えられたとき, 次のような決定則, 決定則と入出力を考える事にする. これによって通信路符号化定理は良い n と $\mathcal{C}$ を選べると言いなおすことができる.

1.1.1　ハミング距離と決定則

$\boldsymbol{x}, \boldsymbol{y} \in \{0,1\}^n$ に対し

$$d(\boldsymbol{x}, \boldsymbol{y}) := \frac{1}{n}\#\{i \le n \mid x_i \neq y_i\}$$

とおく.

$\mathcal{C} \subset \{0,1\}^n$ について決定則 $\Delta^{\mathcal{C}}$ は $\boldsymbol{y} \in \{0,1\}^n$

$$d(\Delta^{\mathcal{C}}(\boldsymbol{y}), \boldsymbol{y}) = \min_{\boldsymbol{x}\in\mathcal{C}} d(\boldsymbol{x}, \boldsymbol{y}) \quad \text{for any } \boldsymbol{y} \in \{0,1\}^n$$

を満たすものとする,

1.1.2　確率空間と入出力

$\mathbf{X}$ は $\mathcal{C}$ 上の均等分布とし, $\mathbf{Z} = (Z_k)_{k=1}^n$ を分布

$$P(Z_k = 0) = q, \quad P(Z_k = 0) = 1 - q$$

に従う独立同分布過程で $\mathbf{X}$ とも独立なものとする. 更に $\mathbf{Y} = (Y_k)_{k=1}^n$ を

$$Y_k := X_k + Z_k$$

とおく. ただしこの時の加法は $\mathbb{Z}/2\mathbb{Z}$ におけるものとする. このとき $p^{\mathcal{C}}_{(\boldsymbol{x},\boldsymbol{y})} := P(\mathbf{X} = \boldsymbol{x}, \mathbf{Y} = \boldsymbol{y})$ とおけば $\mathbf{Y}$ の定義と $\mathbf{X}$ と $\mathbf{Z}$ の独立性から

$$p^{\mathcal{C}}_{(\boldsymbol{x},\boldsymbol{y})} := P(\mathbf{X} = \boldsymbol{x}, \mathbf{Y} = \boldsymbol{y}) = P(\mathbf{X} = \boldsymbol{x}, \mathbf{Z} = \boldsymbol{y} - \boldsymbol{x}) = P(\mathbf{X} = \boldsymbol{x})P(\mathbf{Z} = \boldsymbol{y} - \boldsymbol{x}).$$

また $\mathbf{Z}$ の定義から

$$P(\mathbf{Z} = \boldsymbol{y} - \boldsymbol{x}) = q^{(1-d(\mathbf{0},\boldsymbol{y}-\boldsymbol{x}))n}(1-q)^{d(\mathbf{0},\boldsymbol{y}-\boldsymbol{x})n} = q^{(1-d(\boldsymbol{x},\boldsymbol{y}))n}(1-q)^{d(\boldsymbol{x},\boldsymbol{y})n} = q_{\boldsymbol{x},\boldsymbol{y}}$$

であるので

$$P(\mathbf{X} = \boldsymbol{x}, \mathbf{Y} = \boldsymbol{y}) \quad = \quad P(\mathbf{X} = \boldsymbol{x})q_{\boldsymbol{x},\boldsymbol{y}}$$

であり, $\mathbf{X}$, $\mathbf{Y}$ は入出力である.

1.2 定理

特に $\mathbf{X}$ が $\mathcal{C}$ 上の均等分布である事から

$$H(\mathbf{X}) = \log_2 \#\mathcal{C}$$

また間違い率は

$$P(\mathbf{X} \neq \Delta^{\mathcal{C}}(\mathbf{Y})) = \sum_{(\boldsymbol{x},\boldsymbol{y}):\boldsymbol{x}\neq\Delta^{\mathcal{C}}(\boldsymbol{y})} P(\mathbf{X}=\boldsymbol{x}.\mathbf{Y}=\boldsymbol{y}) = \sum_{(\boldsymbol{x},\boldsymbol{y}):\boldsymbol{x}\neq\Delta^{\mathcal{C}}(\boldsymbol{y})} P^{\mathcal{C}}_{\boldsymbol{x},\boldsymbol{y}}$$

であるから通信路符号化定理の通信速度と間違い率に関する評価

$$\frac{1}{n}H(\mathbf{X}) \geq \alpha, \qquad P(\mathbf{X} \neq \Delta^{\mathcal{C}}(\mathbf{Y})) \leq \varepsilon$$

は次の様に言いなおせる:

Theorem 1. 任意の $\alpha < C$, $\varepsilon > 0$ について十分大きな n で

$$\frac{1}{n}\log_2 \#\mathcal{C} \geq \alpha, \qquad \sum_{(\boldsymbol{x},\boldsymbol{y}):\boldsymbol{x}\neq\Delta^{\mathcal{C}}(\boldsymbol{y})} P^{\mathcal{C}}_{\boldsymbol{x},\boldsymbol{y}} \leq \varepsilon$$

なる $\mathcal{C} \in \{0,1\}^n$ が存在する.

1.3 証明

$\boldsymbol{x} \neq \Delta^{\mathcal{C}}(\boldsymbol{y})$ であれば, 任意の $\rho > 0$ に関して, $d(\boldsymbol{x},\boldsymbol{y}) > \rho$ であるか或いはより $\boldsymbol{y}$ に近い (少なくても距離が ρ 以下の) 符号語 $\boldsymbol{c}$ が存在するので誤り率は上から

$$\sum_{(\boldsymbol{x},\boldsymbol{y}):\boldsymbol{x}\neq\Delta^{\mathcal{C}}(\boldsymbol{y})} p^{\mathcal{C}}_{(\boldsymbol{x},\boldsymbol{y})} \leq \sum_{(\boldsymbol{x},\boldsymbol{y}):d(\boldsymbol{x},\boldsymbol{y})>\rho} p^{\mathcal{C}}_{(\boldsymbol{x},\boldsymbol{y})} + \sum_{\boldsymbol{x}\in\mathcal{C}} \sum_{\boldsymbol{c}\in\mathcal{C}\setminus\{\boldsymbol{x}\}} \sum_{d(\boldsymbol{c},\boldsymbol{y})\leq\rho} p^{\mathcal{C}}_{(\boldsymbol{x},\boldsymbol{y})}$$

と評価できる. 以下

$$P_I(n,\mathcal{C}) := \sum_{(\boldsymbol{x},\boldsymbol{y}):d(\boldsymbol{x},\boldsymbol{y})>\rho} p^{\mathcal{C}}_{(\boldsymbol{x},\boldsymbol{y})}, \qquad P_{II}(n,\mathcal{C}) := \sum_{\boldsymbol{x}\in\mathcal{C}} \sum_{\boldsymbol{c}\in\mathcal{C}\setminus\{\boldsymbol{x}\}} \sum_{d(\boldsymbol{c},\boldsymbol{y})\leq\rho} p^{\mathcal{C}}_{(\boldsymbol{x},\boldsymbol{y})}$$

と表す.

$\alpha + h(1-q) < C + h(1-q) = 1 - h(q) + h(1-q) = 1$ と $x \mapsto h(x)$ の連続性, $q > \frac{1}{2}$ から

$$\alpha + h(\rho) < 1, \qquad \frac{1}{2} > \rho > 1 - q$$

を同時に満たす ρ が存在する. 故に次の 2 つの lemma により証明が完結する.

1.4 補題

Lemma 1. $\rho > 1 - q$ であれば十分大きな n で

$$\sup_{\mathcal{C}} P_I(n,\mathcal{C}) \leq \varepsilon$$

Proof.

$$P_I(n,\mathcal{C}) = \sum_{\boldsymbol{x}\in\mathcal{C}} \sum_{\boldsymbol{y}:d(\boldsymbol{x},\boldsymbol{y})>\rho} P(\mathbf{X}=\boldsymbol{x})P(\mathbf{Z}=\boldsymbol{y}-\boldsymbol{x}) = \sum_{\boldsymbol{x}\in\mathcal{C}} P(\mathbf{X}=\boldsymbol{x}) \sum_{\boldsymbol{z}:d(\boldsymbol{0},\boldsymbol{z})>\rho} P(\mathbf{Z}=\boldsymbol{z}) = P(\frac{1}{n}\sum_{k=1}^{n} Z_k > \rho)$$

Z_k は確率 q, $1-q$ で各々0, 1 をとる独立同分布列であったことに注意せよ. $E[Z_k] = 1 - q < \rho$ であったので, 大数の弱法則により $n \to \infty$ のとき右辺は 0 に向かう. □

Lemma 2. $\alpha + h(\rho) < 1$, $\frac{1}{2} > \rho$ であれば十分大きな n と $\#\hat{\mathcal{C}} \geq 2^{\alpha n}$ なる $\hat{\mathcal{C}} \subset \{1,-1\}^n$ で

$$P_{II}(n, \hat{\mathcal{C}}) \leq \varepsilon$$

を満たすものが存在する.

Proof. $M := [2^{\alpha n}] + 1$ とおく. 特に $\mathbf{X}$ が $\mathcal{C}$ 上の均等分布である事から

$$p^{\mathcal{C}}_{(\boldsymbol{x},\boldsymbol{y})} = \begin{cases} \frac{1}{\#\mathcal{C}} P(\mathbf{Z} = \boldsymbol{x} - \boldsymbol{y}) & \text{if } \boldsymbol{x} \in \mathcal{C} \\ 0 & \text{otherwise} \end{cases}$$

$\mathcal{C}$ を動かした時の誤差の総和を評価し, その中に良い $\mathcal{C}$ が存在することを示す.

$$\begin{aligned}
\sum_{\mathcal{C}:\#\mathcal{C}=M} P_{II}(n,\mathcal{C}) &= \sum_{\mathcal{C}:\#\mathcal{C}=M} \sum_{\boldsymbol{x}\in\mathcal{C}} \sum_{\boldsymbol{c}\in\mathcal{C}\setminus\{\boldsymbol{x}\}} \sum_{d(\boldsymbol{c},\boldsymbol{y})\leq\rho} p^{\mathcal{C}}_{(\boldsymbol{x},\boldsymbol{y})} \\
&= \sum_{\mathcal{C}:\#\mathcal{C}=M} \sum_{\boldsymbol{x}\in\mathcal{C}} \sum_{\boldsymbol{c}\in\mathcal{C}\setminus\{\boldsymbol{x}\}} \sum_{d(\boldsymbol{c},\boldsymbol{y})\leq\rho} \frac{1}{M} P(\mathbf{Z} = \boldsymbol{x} - \boldsymbol{y}) \\
&= \frac{1}{M} \sum_{\boldsymbol{c}\in A^n} \sum_{\boldsymbol{x}\in A^n\setminus\{\boldsymbol{c}\}} \sum_{d(\boldsymbol{c},\boldsymbol{y})\leq\rho} P(\mathbf{Z} = \boldsymbol{x} - \boldsymbol{y}) \sum_{\mathcal{C}:\#\mathcal{C}=M, \boldsymbol{x},\boldsymbol{c}\in\mathcal{C}} 1 \\
&= \frac{1}{M} \sum_{\boldsymbol{c}\in A^n} \sum_{\boldsymbol{x}\in A^n\setminus\{\boldsymbol{c}\}} \sum_{d(\boldsymbol{c},\boldsymbol{y})\leq\rho} P(\mathbf{Z} = \boldsymbol{x} - \boldsymbol{y}) \begin{pmatrix} 2^n - 2 \\ M - 2 \end{pmatrix} \\
&= \frac{1}{M} \begin{pmatrix} 2^n - 2 \\ M - 2 \end{pmatrix} \sum_{\boldsymbol{c}\in A^n} \sum_{\boldsymbol{x}\in A^n\setminus\{\boldsymbol{c}\}} \sum_{d(\boldsymbol{c},\boldsymbol{y})\leq\rho} P(\mathbf{Z} = \boldsymbol{x} - \boldsymbol{y}) \\
&= \frac{1}{M} \begin{pmatrix} 2^n - 2 \\ M - 2 \end{pmatrix} \sum_{\boldsymbol{c}\in A^n} \sum_{d(\boldsymbol{c},\boldsymbol{y})\leq\rho} \sum_{\boldsymbol{x}\in A^n\setminus\{\boldsymbol{c}\}} P(\mathbf{Z} = \boldsymbol{x} - \boldsymbol{y}) \\
&\leq \frac{1}{M} \begin{pmatrix} 2^n - 2 \\ M - 2 \end{pmatrix} \sum_{\boldsymbol{c}\in A^n} \sum_{d(\boldsymbol{c},\boldsymbol{y})\leq\rho} 1 \\
&= \frac{1}{M} \begin{pmatrix} 2^n - 2 \\ M - 2 \end{pmatrix} \sum_{\boldsymbol{c}\in A^n} \sum_{r:r\leq\rho n} \sum_{d(\boldsymbol{c},\boldsymbol{y})=r/n} 1 \\
&= \frac{1}{M} \begin{pmatrix} 2^n - 2 \\ M - 2 \end{pmatrix} 2^n \sum_{r:r\leq\rho n} \begin{pmatrix} n \\ r \end{pmatrix}
\end{aligned}$$

ここで後述する組み合わせに関する評価の lemma を用いて

$$\begin{aligned}
\sum_{\mathcal{C}:\#\mathcal{C}=M} P_{II}(n,\mathcal{C}) &\leq \frac{1}{M} \begin{pmatrix} 2^n - 2 \\ M - 2 \end{pmatrix} 2^n 2^{h(\rho)n} \\
&= \begin{pmatrix} 2^n \\ M \end{pmatrix} \frac{M-1}{2^n - 1} 2^{h(\rho)n} \\
&= \begin{pmatrix} 2^n \\ M \end{pmatrix} \frac{[2^{\alpha n}]}{2^{\alpha n}} \frac{2^n}{2^n - 1} 2^{(\alpha + h(\rho) - 1)n}
\end{aligned}$$

$\alpha + h(\rho) < 1$ なので十分大きな n で

$$\sum_{\mathcal{C}:\#\mathcal{C}=M} P_{II}(n,\mathcal{C}) \leq \begin{pmatrix} 2^n \\ M \end{pmatrix} \varepsilon$$

$\#\mathcal{C} = M$ なる $\mathcal{C}$ は $\begin{pmatrix} 2^n \\ M \end{pmatrix}$ 個あるので少なくとも 1 つの $\hat{\mathcal{C}}$ で $P_{II}(n,\mathcal{C}) < \varepsilon$ □

Lemma 3. $\frac{1}{2} > \rho$ であれば

$$2^{nh(\rho)} \geq \sum_{r:r\leq \rho n} \left(\begin{array}{c} n \\ r \end{array} \right)$$

Proof.

$$2^{nh(\rho)} = 2^{n(-\rho\log\rho-(1-\rho)\log(1-\rho))} = \rho^{-n\rho}(1-\rho)^{n-n\rho}$$

なる事に気をつければ

$$\begin{aligned} 1 = ((1-\rho)+\rho)^n &= \sum_r \left(\begin{array}{c} n \\ r \end{array} \right) \rho^r (1-\rho)^{n-r} \\ &\geq \sum_{r:r\leq\rho n} \left(\begin{array}{c} n \\ r \end{array} \right) \rho^r (1-\rho)^{n-r} \\ &= \sum_{r:r\leq\rho n} \left(\begin{array}{c} n \\ r \end{array} \right) 2^{-nh(\rho)} \left(\frac{\rho}{1-\rho}\right)^{r-n\rho} \geq \sum_{r:r\leq\rho n} \left(\begin{array}{c} n \\ r \end{array} \right) 2^{-nh(\rho)} \end{aligned}$$

$\frac{1}{2} > \rho$ より $\frac{\rho}{1-\rho} > 1$ であるので

$$1 \geq \sum_{r:r\leq\rho n} \left(\begin{array}{c} n \\ r \end{array} \right) 2^{-nh(\rho)} \left(\frac{\rho}{1-\rho}\right)^{r-n\rho} \geq \sum_{r:r\leq\rho n} \left(\begin{array}{c} n \\ r \end{array} \right) 2^{-nh(\rho)}$$

□