

以下 Q は入力アルファベット A と出力アルファベット $B(A \subset B$ を仮定する) を持つ通信路であるとする。

1 通信路を使った通信, 無記憶通信

行列 $Q = (q_{ab})$ は「入力 $a \in A$ を与えられた時に出力が $b \in B$ になる確率」を表現していた事を思い出そう。

通常, 通信は単一の符号を送って終わりではなく, 複数の符号を記号を送る事が多い。そこで, 自然な拡張として, 「入力として符号列 $\mathbf{a} = (a_1, \dots, a_n) \in A^n$ を与えられた時に出力が符号列 $\mathbf{b} = (b_1, \dots, b_n) \in B^n$ になる確率」は

$$q_{\mathbf{a}\mathbf{b}} = q_{a_1 b_1} q_{a_2 b_2} \cdots q_{a_n b_n}$$

であるとする。これは, つまり, 各通信が独立に行なわれる, 或いはそれでの通信が次の通信に影響されない事を仮定すると言う事であり, 「無記憶通信」等と表現される。¹

Definition 1. A^n -値確率変数 $\mathbf{X}$ と B^n -値確率変数 $\mathbf{Y}$ の組 $(\mathbf{X}, \mathbf{Y})$ が, 長さ n の (無記憶) 通信路 Q の入出力であるとは, 任意の $\mathbf{a} \in A^n, \mathbf{b} \in B^n$ について

$$P(\mathbf{X} = \mathbf{a}, \mathbf{Y} = \mathbf{b}) = P(\mathbf{X} = \mathbf{a})q_{\mathbf{a}\mathbf{b}}$$

が成り立つときに言う。

2 誤り訂正符号

入力アルファベット A と出力アルファベット $B(A \subset B$ を仮定する) を持つ雑音のある通信路 Q を利用する為の符号について考察する。

情報源アルファベットを Σ とする。符号

$$\varphi: \Sigma \rightarrow A^+$$

は符号語全体の成す言語

$$\mathcal{C} := \varphi(\Sigma) \subset A^+$$

を定める。 φ に十分な復号化可能性があったとしても雑音による変化があるため単純に φ の逆操作によって復号化するだけでは最適でない。 Q の誤りの傾向に沿った復号化により誤りを (確率的に) 訂正する事により効率化が可能である。

以下, 話を簡単にする為に等長符号, 即ち $\varphi: \Sigma \rightarrow A^n$, 言い換えると

$$\mathcal{C} \subset A^n$$

なる場合のみを考える。²

$\mathcal{C}$ の語は雑音の乗った通信路によって $\mathcal{V} := B^n$ の語に変化する ($\mathcal{C} \subset A^n \subset \mathcal{V}$)。そこで受信者は送られてきた情報 Σ の元を知る為に $\mathcal{V}$ からの写像

$$\psi: \mathcal{V} \rightarrow \Sigma$$

を必要とする。素朴に考えるなら, この組 (φ, ψ) を誤り訂正符号と呼ぶべきであろう。

誤り訂正符号 (φ, ψ) , 情報源 $(\Sigma, (p_\sigma))$ が与えられているとき, $(\mathbf{a}, \mathbf{b}) \in \mathcal{C} \times \mathcal{V} = \{\varphi(\sigma) \in A^n \mid \sigma \in \Sigma\} \times B^n =: \Omega$ に対し

$$P_{(\mathbf{a}, \mathbf{b})} = P_{(\varphi(\sigma), \mathbf{b})} := p_\sigma Q_{\mathbf{a}, \mathbf{b}} = p_{\varphi^{-1}(\mathbf{a})} Q_{\mathbf{a}, \mathbf{b}}$$

で確率を定める事ができる。この時

$$\mathbf{X}: \Omega \ni (\mathbf{a}, \mathbf{b}) \mapsto \mathbf{a} \in A^n, \quad \mathbf{Y}: \Omega \ni (\mathbf{a}, \mathbf{b}) \mapsto \mathbf{b} \in B^n$$

¹例えば高速な通信などは, 直前の通信の影響を受けることがある。つまり, 無記憶でない通信なども考えられる。その様な通信に関する議論も存在するが, その場合「通信路」に関する定義から拡張していく必要があり, この授業では割愛する。

²実際後に通信路符号化定理で存在が証明される十分に効率的な符号も等長符号である

は Q の入出力となっていて $\Delta := \varphi \circ \psi$ とおけば

$$\begin{aligned}
P(\text{正しい通信が行なわれなかった}) &= \sum_{\sigma} P(\sigma \text{ が起き, 通信の結果が } \sigma \text{ でなかった}) \\
&= \sum_{\sigma} P(\text{入力が } \varphi(\sigma) \text{ で出力を復号化すると } \sigma \text{ でなかった}) \\
&= \sum_{\sigma} P(\varphi(\sigma) = \mathbf{X}, \psi(\mathbf{Y}) \neq \sigma) \\
&= \sum_{\sigma} P(\varphi^{-1}(\mathbf{X}) = \sigma \neq \psi(\mathbf{Y})) \\
&= P(\varphi^{-1}(\mathbf{X}) \neq \psi(\mathbf{Y})) \\
&= P(\mathbf{X} \neq \Delta(\mathbf{Y})) \\
&= \sum_{(\mathbf{a}, \mathbf{b}) : \Delta(\mathbf{b}) \neq \mathbf{a}} P_{(\mathbf{a}, \mathbf{b})}.
\end{aligned}$$

この最後の値を、情報源 $(\Sigma, (p_{\sigma}))$ の情報を誤り訂正符号 (φ, ψ) を用いて通信路 Q を通して送った時の誤り率という。

ただし、 φ が復号化可能のとき Σ と $\mathcal{C}$ の間には 1 対 1 対応が存在するので $\Delta : \mathcal{V} \rightarrow \mathcal{C}$ によって $\psi = \varphi^{-1} \circ \Delta$ が自然に定まる。故に、しばしば、 (φ, ψ) の代わりに $(\mathcal{C}, \Delta)$ をもって誤り訂正符号と呼ぶ。 Δ は**決定則**と呼ばれる。このときは、 $P(\mathbf{X} \in \mathcal{C}) = 1$ なる入出力 $(\mathbf{X}, \mathbf{Y})$ について³

$$P(\mathbf{X} \neq \Delta(\mathbf{Y}))$$

を誤り訂正符号 $(\mathcal{C}, \Delta)$ を用いて通信路 Q を通して送った時の入力 $\mathbf{X}$ に対する誤り率という。

3 通信路符号化定理

Theorem 1. Q を通信容量 C の通信路とする。任意の $\varepsilon_e > 0, \varepsilon_q > 0$ について、誤り訂正符号 $(\mathcal{C}, \Delta)$ と入力 (の分布) $(\mathcal{C}, (p_c))$ で「誤り率が ε_e で、単位符号あたりの通信量が $C - \varepsilon_q$ 以上」即ち

$$P(\mathbf{X} \neq \Delta(\mathbf{Y})) \leq \varepsilon_e, \quad \left| \frac{1}{n} I(\mathbf{X}, \mathbf{Y}) - C \right| \leq \varepsilon_q$$

を満たすものが存在する。

$$Q\mathbf{x} = \mathbf{h} \text{ とすると } h_a = \sum_b a_{ab} x_b$$

$$\begin{aligned}
I(\mathbf{X}, \mathbf{Y}) &= H(\mathbf{X}) + H(\mathbf{Y}) - H(\mathbf{X}, \mathbf{Y}) \\
&= H(\mathbf{X}) + H(\mathbf{Y}) - \sum_{\mathbf{a}} \sum_{\mathbf{b}} p_{\mathbf{a}} q_{\mathbf{ab}} \log \frac{1}{p_{\mathbf{a}} q_{\mathbf{ab}}} \\
&= H(\mathbf{Y}) - \sum_{\mathbf{a}} p_{\mathbf{a}} \sum_{\mathbf{b}} q_{\mathbf{ab}} \log \frac{1}{q_{\mathbf{ab}}} \\
&= H(\mathbf{Y}) - \sum_{a_1, \dots, a_n} p_{\mathbf{a}} \sum_{b_1, \dots, b_n} \prod_i q_{a_i b_i} \log \frac{1}{\prod_j q_{a_j b_j}} \\
&= H(\mathbf{Y}) - \sum_{a_1, \dots, a_n} p_{\mathbf{a}} \sum_j \sum_{b_1, \dots, b_n} \prod_i q_{a_i b_i} \log \frac{1}{q_{a_j b_j}} \\
&= H(\mathbf{Y}) - \sum_{a_1, \dots, a_n} p_{\mathbf{a}} \sum_j \sum_{b_j} q_{a_j b_j} \log \frac{1}{q_{a_j b_j}} \\
&= H(\mathbf{Y}) - \sum_{a_1, \dots, a_n} p_{\mathbf{a}} \sum_j h_{a_j} \\
&= H(\mathbf{Y}) - \sum_{\mathbf{a}} p_{\mathbf{a}} h_{\mathbf{a}} \\
&= H(\mathbf{r}) - (\mathbf{r}, \mathbf{x})
\end{aligned}$$

³実は $\mathcal{C}$ 上の分布が一つ与えられれば Q の入出力 $(\mathbf{X}, \mathbf{Y})$ の分布が特定され、誤り率が決まる。

