Coding and Information Theory
Chapter 4
Information Channels - B

Xuejun Liang

Fall 2022

4.2 The Binary Symmetric Channel

- Binary symmetric channel (BSC)
  - $\mathrm{A} = \mathrm{B} = Z_2 = \{0, 1\}$.
  - the channel matrix has the form

$$M = \begin{pmatrix} P_{00} & P_{01} \\ P_{10} & P_{11} \end{pmatrix} = \begin{pmatrix} P & \overline{P} \\ \overline{P} & P \end{pmatrix}$$

    for some P where $0 \leq P \leq 1$

  - The input probabilities have the form

$$p_0 = \Pr(a = 0) = p,$$

$$p_1 = \Pr(a = 1) = \overline{p},$$

    for some p such that $0 \leq p \leq 1$

- The channel relationships for BSC = ?

$$q_0 = \Pr(b=0) = pP + \overline{p}\overline{P},$$
$$q_1 = \Pr(b=1) = p\overline{P} + \overline{p}P;$$

$$\sum_{i=1}^{r} p_i P_{ij} = q_j$$

writing $q_0 = q$ and $q_1 = \overline{q}$ we then have

$$(q, \overline{q}) = (p, \overline{p}) \begin{pmatrix} P & \overline{P} \\ \overline{P} & P \end{pmatrix}$$

- Bayes' formula for BSC = ?

$$Q_{00} = \frac{pP}{pP + \overline{p}\overline{P}}, \quad Q_{10} = \frac{\overline{p}\overline{P}}{pP + \overline{p}\overline{P}}$$

$$Q_{01} = \frac{p\overline{P}}{p\overline{P} + \overline{p}P}, \quad Q_{11} = \frac{\overline{p}P}{p\overline{P} + \overline{p}P}$$

$$Q_{ij} = \frac{p_i P_{ij}}{\sum_{k=1}^{r} p_k P_{kj}}$$

- Example 4.4
  - Let the input A be defined by putting $p = 1/2$
  - Probabilities of the output symbols: q_0 = ? And q_1 = ?
  - The backward probabilities: Q_{00}, Q_{01}, Q_{10}, Q_{11}, = ?

$$q_0 = pP + \overline{p}\overline{P}$$

$$q_1 = p\overline{P} + \overline{p}P$$

$$Q_{00} = \frac{pP}{pP + \overline{p}\overline{P}} \quad Q_{11} = \frac{\overline{p}P}{p\overline{P} + \overline{p}P} \quad Q_{10} = \frac{\overline{p}\overline{P}}{pP + \overline{p}\overline{P}} \quad Q_{01} = \frac{p\overline{P}}{p\overline{P} + \overline{p}P}$$

$$Q_{ij} = \frac{p_i}{q_j} P_{ij}$$

- Example 4.5
  - Suppose that P = 0.8 and p = 0.9
  - Probabilities of the output symbols: q_0 = ? And q_1 = ?

$$q_0 = pP + \overline{p}\overline{P}$$

$$q_1 = p\overline{P} + \overline{p}P$$

  - The backward probabilities: Q_{00}, Q_{01}, Q_{10}, Q_{11} = ?

$$Q_{00} = \frac{p_0 P_{00}}{q_0}$$

$$Q_{10} = \frac{p_1 P_{10}}{q_0}$$

$$Q_{01} = \frac{p_0 P_{01}}{q_1}$$

$$Q_{11} = \frac{p_1 P_{11}}{q_1}$$

- Example 4.5 (Cont.)
  - Necessary and sufficient conditions on p and P for

$$Q_{00} > Q_{10} \text{ and } Q_{01} > Q_{11}$$

$$Q_{00} = \frac{p_0 P_{00}}{q_0} \qquad Q_{10} = \frac{p_1 P_{10}}{q_0} \qquad Q_{01} = \frac{p_0 P_{01}}{q_1} \qquad Q_{11} = \frac{p_1 P_{11}}{q_1}$$

4.3 System Entropies

- The input A and the output B of a channel Γ
  - the input entropy $H(\mathcal{A}) = \sum_i p_i \log \frac{1}{p_i}$
  - the output entropy $H(\mathcal{B}) = \sum_j q_j \log \frac{1}{q_j}$
  - If $b = b_j$ is received, then uncertainty about A is the conditional entropy

$$H(\mathcal{A} \mid b_j) = \sum_i \Pr(a_i \mid b_j) \log \frac{1}{\Pr(a_i \mid b_j)} = \sum_i Q_{ij} \log \frac{1}{Q_{ij}}$$

  - the equivocation of A with respect to B

$$H(\mathcal{A} \mid \mathcal{B}) = \sum_j q_j H(\mathcal{A} \mid b_j) = \sum_j q_j \Big(\sum_i Q_{ij} \log \frac{1}{Q_{ij}} \Big) = \sum_i \sum_j R_{ij} \log \frac{1}{Q_{ij}}$$

System Entropies (Cont.)

- Similarly, if a_i is sent, then the uncertainty about B is the conditional entropy

$$H(\mathcal{B} \mid a_i) = \sum_j \Pr(b_j \mid a_i) \log \frac{1}{\Pr(b_j \mid a_i)} = \sum_j P_{ij} \log \frac{1}{P_{ij}}$$

- the equivocation of B with respect to A

$$H(\mathcal{B} \mid \mathcal{A}) = \sum_i p_i H(\mathcal{B} \mid a_i) = \sum_i p_i \Big(\sum_j P_{ij} \log \frac{1}{P_{ij}} \Big) = \sum_i \sum_j R_{ij} \log \frac{1}{P_{ij}}$$

- the joint entropy

$$H(\mathcal{A}, \mathcal{B}) = \sum_i \sum_j \Pr(a_i, b_j) \log \frac{1}{\Pr(a_i, b_j)} = \sum_i \sum_j R_{ij} \log \frac{1}{R_{ij}}$$

System Entropies (Cont.)

- If A and B are statistically independent, i.e. $R_{ij} = p_i q_j$, then

$$H(\mathcal{A}, \mathcal{B}) = H(\mathcal{A}) + H(\mathcal{B}) \qquad (4.5)$$

- In general, A and B are related, rather than independent, then

$$H(\mathcal{A}, \mathcal{B}) = H(\mathcal{A}) + H(\mathcal{B} \mid \mathcal{A}) \qquad (4.6)$$

$$H(\mathcal{A}, \mathcal{B}) = H(\mathcal{B}) + H(\mathcal{A} \mid \mathcal{B}) \qquad (4.7)$$

- We call $H(\mathrm{A}), H(\mathrm{B}), H(\mathrm{A}|\mathrm{B}), H(\mathrm{B}|\mathrm{A}), and\ H(\mathrm{A}, \mathrm{B})$ the system entropies.

4.4 System Entropies for the Binary Symmetric Channel

- The input and output entropies for BSC are

$$H(\mathcal{A}) = -p \log p - \overline{p} \log \overline{p} = H(p),$$
$$H(\mathcal{B}) = -q \log q - \bar{q} \log \overline{q} = H(q),$$

  where $q = pP + \bar{p}\bar{P}$.

- Definition: A function f: [0,1] $\rightarrow$ R is strictly convex, if for $a, b \in [0,1]$ and $x = \lambda a + \bar{\lambda} b$ $with$ $0 \leq \lambda \leq 1$,

$$f(x) \geq \lambda f(a) + \overline{\lambda} f(b),$$

  with equality if and only if x = a or b, that is, $a = b$ or $\lambda = 0$ or 1.

System Entropies for BSC (Cont.)

- Lemma 4.6
  - If a function f : [0,1] $\rightarrow R$ is continuous on the interval [0,1] and twice differentiable on (0,1) , with f''(x) < 0 for all $x \in$ (0,1), then f is strictly convex.
- Corollary 4.7
  - The entropy function $H(p)$ is strictly convex on [0,1].

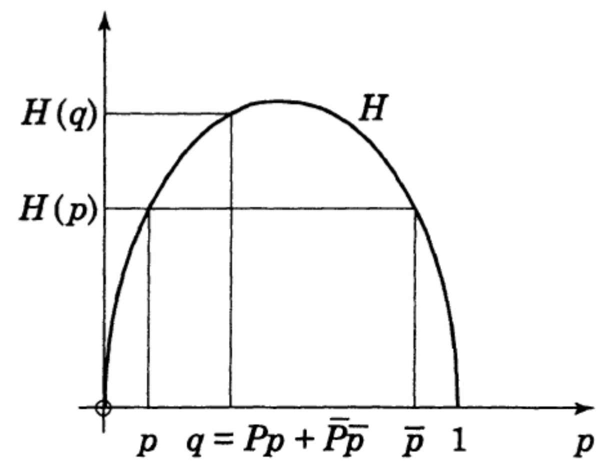
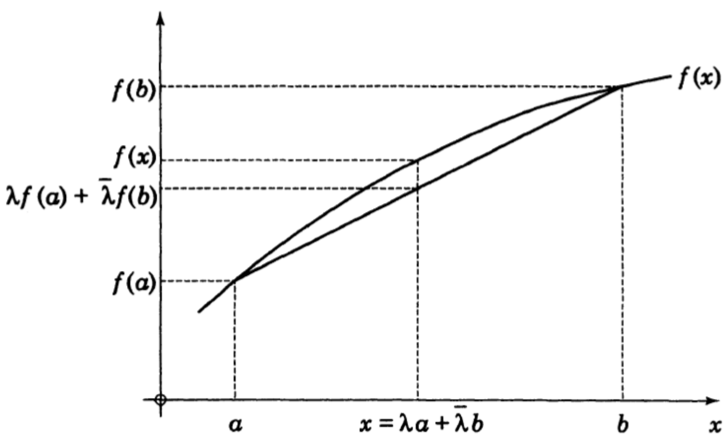


Figure 4.5



$$H(pP + \bar{p}\bar{P}) \geq PH(p) + \bar{P}H(\bar{p})$$

$$H(pP + \bar{p}\bar{P}) \geq pH(P) + \bar{p}H(\bar{P})$$

$$\mathrm{f}\big(\lambda a + \bar{\lambda} b\big) \geq \lambda f(a) + \bar{\lambda} f(b)$$

System Entropies for BSC (Cont.)

- The BSC satisfies

  $$H(\mathcal{B}) \geq H(\mathcal{A}), \qquad (4.8)$$

  with equality if and only if $p = 1/2$ or the channel is totally unreliable (P = 0) or reliable (P = 1)

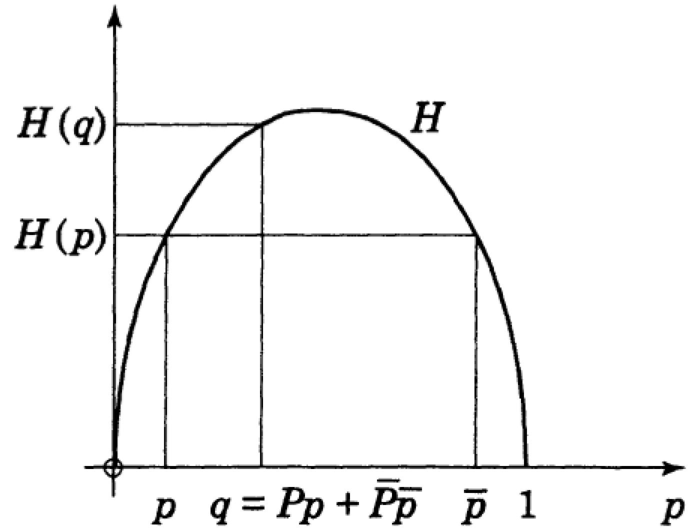


Figure 4.5

Transmission through the BSC generally increases uncertainty

$$H(pP + \bar{p}\bar{P}) \geq PH(p) + \bar{P}H(\bar{p})$$

Note in BSC, $q = pP + \bar{p}\bar{P}$