Information Theory

Shi Yu
2023K8009926030

University of Chinese Academy of Sciences

Contents

§ 1 Entropy,Relative Entropy and Matual information

1.1 Entropy

Setting $X \sim P$ discrete random variable

"P" is the probability massfunction(PMF) of X.

$P_X(X=x) = P_r[X=x] \qquad P_X(x) \longleftrightarrow p(x)$

Definition 1.1.1. ***Entropy:***

$$H(X) = -\sum_{x\in X} p(x)\log p(x) \qquad (log_2 : bit \quad log_e : nat)$$

Convention: $0log0 = 0$

Actually,$H(X) = H[P]$

Accordingly,$\bar{X} = \sum_{x\in X} p(x)x \sim \mathop{\mathbf{E}}_{X\sim p(x)} X$

$$H(X) \sim \mathop{\mathbf{E}}_{X\sim p(x)} log\frac{1}{p(x)}$$

Example 1.1.1. ***Binary Entropy Function:***

$$h(p) = \mathop{H}_{x\in\{0,1\}}(X) = -plog_2p - (1-p)log_2(1-p)$$

Here,$p = P(X=0)$

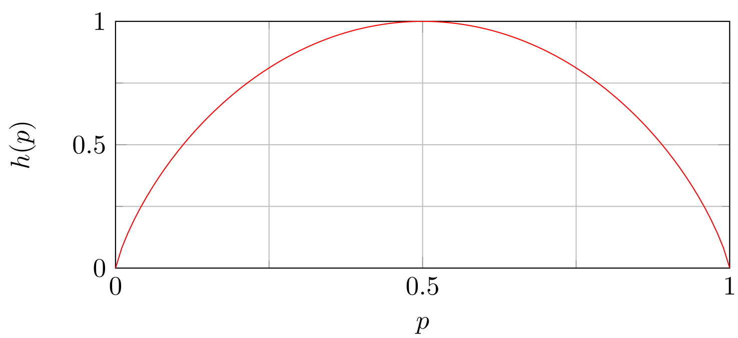


Figure 1: Binary Entropy Function

Each point on the curve represents one distribution of X.

H property:

1. $H[P] \geq 0$
2. $H_b(X) = log_b a H_a(X) \qquad$ nat,when a = e

1.2 Joint Entropy and Conditional Entropy

Definition 1.2.1. ***Joint Entropy:*** $\qquad (X,Y) \sim p_{X,Y}(X=x, Y=y)$

$$H[p_{X,Y}] = -\sum_{x\in\mathfrak{X},y\in\mathfrak{Y}} p_{X,Y}(x,y)\log p_{X,Y}(x,y)$$

Definition 1.2.2. ***Conditional Entropy:*** $p_{X|Y}(X=x|Y=y)$

$$H[X|Y] = -\sum_{x\in\mathfrak{X},y\in\mathfrak{Y}} \underset{\substack{\uparrow\\ \textit{joint}}}{p_{X,Y}(x,y)} \log \underset{\substack{\uparrow\\ \textit{conditional}}}{p_{X|Y}(x|y)}$$

Chain Rule: $P(x,y) = P_Y(y)P_{X|Y}(x|y)$

Theorem 1.2.1. $H(X,Y) = H(Y) + H(X|Y)$

Proof.

$$\begin{aligned}
H(X,Y) &= -\mathop{\mathbf{E}}_{X,Y\sim p_{X,Y}} \log p_{X,Y}(x,y)\\
&= -\mathop{\mathbf{E}}_{X,Y\sim p_{X,Y}} \log(p_{X|Y}(x|y)p_Y(y))\\
&= -\mathop{\mathbf{E}}_{X,Y\sim p_{X,Y}} \log p_{X|Y}(x|y) - \mathop{\mathbf{E}}_{X,Y\sim p_{X,Y}} \log p_Y(y)\\
&= H(X|Y) + H(Y)
\end{aligned}$$

□

1.3 Mutual Information

$$X,Y \sim p_{X,Y}(x,y)$$

Definition 1.3.1. ***Mutual Information:***

$$\begin{aligned}
I(X;Y) &\overset{def}{=} \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p_X(x)p_Y(y)}\\
&= H(X) - H(X|Y)\\
&= H(Y) - H(Y|X)\\
&= H(X) + H(Y) - H(X,Y)
\end{aligned}$$

Property:if $X \perp Y \Leftrightarrow I(X,Y) = 0$
$I(X,Y) \geq 0$
$[I(X,Y)]_{max} = min\{H(X),H(Y)\}$

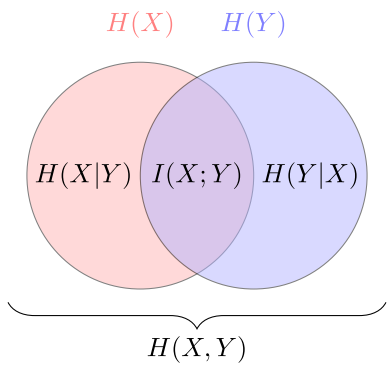


Figure 2: Mutual Information

1.4 KL-Divergence

$$X \sim p_X(x) \qquad X \sim q_X(x)$$

Definition 1.4.1. ***KL-Divergence(Relative Entropy):***
Kullback-Leiblar Divergence between two PMF $p(x)$ and $q(x)$ is defined as:

$$D[p \parallel q] \stackrel{def}{=} \sum_{x \in \mathfrak{X}_p} p(x) \log \frac{p(x)}{q(x)} \in [0, +\infty]$$

KL-Divergence is used to measure the difference between two PMF.

Convention:

1. $0 \log 0 = 0$
2. $0 \log \frac{0}{\tilde{q}} = 0$
3. $\tilde{p} \log \frac{\tilde{p}}{0} = +\infty$

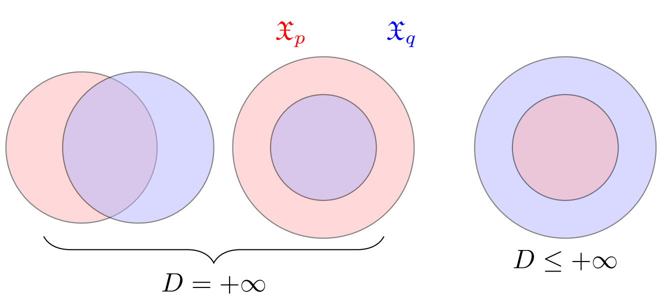


Figure 3: Value selection of KL-Divergence

Property: if $\exists x \in \mathfrak{X}$,st $p(x) > 0$ while $q(x) = 0$ then $D[p \parallel q] = +\infty$.

Definition 1.4.2. ***Conditional Relative Entropy:***

The Conditional Relative Entropy between $p(x, y)$ and $q(x, y)$ is defined as the average KL-Divergence between $p(y|x)$ and $q(y|x)$ by $p(x)$:

$$\begin{aligned} D[p(y|x) \parallel q(y|x)] &= \sum_x p(x) \sum_y p(y|x) \log \frac{p(y|x)}{q(y|x)} \\ &= \sum_{x,y} p(x, y) \log \frac{p(y|x)}{q(y|x)} \end{aligned}$$

1.5 Chain Rule

- $p(x_1, x_2) = p(x_1)p(x_2|x_1)$
  $p(x_1, x_2, \ldots, x_n) = p(x_1)p(x_2|x_1)p(x_3|x_1, x_2) \ldots p(x_n|x_1, x_2, \ldots, x_{n-1})$
- $H(X_1, X_2, \ldots, X_n) = H(X_1) + H(X_2|X_1) + \ldots + H(X_n|X_1, X_2, \ldots, X_{n-1})$
- Conditional Mutual Information:

  $$I(X; Y|Z) = \sum_{X,Y,Z} p(x, y, z) \log \frac{p(x, y|z)}{p(x|z)p(y|z)}$$

  means the information of X and Y given Z.
- $I(X_1, \ldots, X_n; Y) = I(X_1; Y) + I(X_2; Y|X_1) + \ldots + I(X_n; Y|X_1, \ldots, X_{n-1})$
- Chain Rule for KL-Divergence:
  $D[p(x, y)||q(x, y)] = D[p(x)||q(x)] + D[p(y|x)||q(y|x)]$

  Proof.

  $$\begin{aligned} D[p(x, y)||q(x, y)] &\overset{def}{=} \sum_{x,y} p(x, y) \log \frac{p(x, y)}{q(x, y)} \\ &= \sum_{x,y} p(x, y) \log \frac{p(x)p(y|x)}{q(x)q(y|x)} \\ &= \sum_{x,y} p(x, y) \log \frac{p(x)}{q(x)} + \sum_{x,y} p(x, y) \log \frac{p(y|x)}{q(y|x)} \\ &= \sum_{x,y} p(x) \log \frac{p(x)}{q(x)} + \sum_{x,y} p(x, y) \log \frac{p(y|x)}{q(y|x)} \\ &= D[p(x)||q(x)] + D[p(y|x)||q(y|x)] \end{aligned}$$

  □

1.6 Jensen Inequality

Definition 1.6.1. ***Convex Function:***

A function $f(x)$ is convex over (a,b),if $\forall x_1, x_2 \in (a, b)$, $f(\lambda x_1 + (1-\lambda)x_2) \leq \lambda f(x_1) + (1-\lambda)f(x_2)$, *where* $\lambda \in [0, 1]$.

Example 1.6.1. ***Common Convex and Concave Functions:***

Convex Functions: $f(x) = x^2, e^x \quad \leftrightarrow \quad f^{(2)}(x) \geq 0$

Concave Functions: $f(x) = \log x \quad \leftrightarrow \quad f^{(2)}(x) \leq 0$

Theorem 1.6.1. ***Jensen Inequality:***

For a random variable$x \in \mathfrak{X}$,*if* $f(x)$ *is convex, then:*

$$f(\mathbf{E}X) \leq \mathbf{E}f(X) \sim \sum_x p(x)f(x) \geq f(\sum_x p(x)x) \tag{1}$$

Proof. Suppose (1) holds for $|X| \leq K-1$

$$\begin{aligned}
\sum_{i=1}^{K} p(x_i)f(x_i) &= p(x_K)f(x_K) + \sum_{i=1}^{K-1} p(x_i)f(x_i) \\
&= (1-p(x_K))\sum_{i=1}^{K-1} \frac{p(x_i)}{1-p(x_K)} f(x_i) + p(x_K)f(x_K) \\
&\geq (1-p(x_K))f(\sum_{i=1}^{K-1} \frac{p(x_i)}{1-p(x_K)} x_i) + p(x_K)f(x_K) \\
&= f(\sum_{i=1}^{K} p(x_i)x_i)
\end{aligned}$$

□

Theorem 1.6.2. ***Information Inequality:***

$$D[p \parallel q] \geq 0 \quad \textit{with equality iff} \quad p(x) = q(x)$$

Proof.

$$\begin{aligned}
D[p \parallel q] &= \sum_x p(x) \log \frac{p(x)}{q(x)} \\
&= -\sum_x p(x) \log \frac{q(x)}{p(x)} \\
\because -logx &\text{ is convex} \\
\therefore D[p \parallel q] &\geq -\log \sum_x p(x) \frac{q(x)}{p(x)} \\
&= -\log \sum_x q(x) \\
&=0
\end{aligned}$$

Here, the equality holds iff $-log\frac{q(x)}{p(x)} = const \Rightarrow q(x) = p(x)$ □

Corollary 1.6.1.

$$I[X;Y] = D[p(x,y) \parallel p(x)p(y)] \geq 0$$

Corollary 1.6.2.

$$D(p(X|Y) \parallel q(X|Y)) \geq 0$$

Corollary 1.6.3.

$$I(X;Y|Z) \geq 0$$

Theorem 1.6.3.

$$x \in X \qquad H(X) \leq \log |X|$$

Proof.

$$\begin{aligned} u(x) =& \frac{1}{|X|} \\ D[p \parallel u] =& \sum_x p(x) \log \frac{p(x)}{u(x)} \geq 0 \\ =& \sum_x p(x) \log |X| + \sum_x p(x) log \frac{1}{u(x)} \\ =& \log |X| - H(X) \geq 0 \\ \Rightarrow H(X) \leq& \log |X| \end{aligned}$$

□

Theorem 1.6.4.

$$H(X) \geq H(X|Y)$$

Proof.

$$\begin{aligned} H(X) &= I(X;Y) + H(X|Y) \\ \because I(X;Y) &\geq 0 \\ \therefore H(X) &\geq H(X|Y) \end{aligned}$$

□

Example 1.6.2. *P(X,Y) is defined as follows:*

X \ Y	1	2
1	0	$\frac{3}{4}$
2	$\frac{1}{8}$	$\frac{1}{8}$

$$\begin{aligned}H(X) &= -\sum_x p(x)\log p(x)\\ &= -(\frac{1}{8}\log\frac{1}{8}+\frac{7}{8}\log\frac{7}{8})\\ &\approx 0.544(bit)\end{aligned}$$

$$\begin{aligned}H(X|Y) &= -\sum_{x,y} p(x,y)\log p(x|y)\\ &= 0-\frac{3}{4}\log 1-\frac{1}{8}\log\frac{1}{2}-\frac{1}{8}\log\frac{1}{2}\\ &= 0.25(bit)\end{aligned}$$

1.7 log-sum Inequality and convexity of D, H, I

Theorem 1.7.1. ***log-sum Inequality:***

$$\sum_{i=1}^n a_i\log\frac{a_i}{b_i} \geq (\sum_{i=1}^n a_i)\log\frac{\sum\limits_{i=1}^n a_i}{\sum\limits_{i=1}^n b_i} \quad \textit{with equality iff} \quad \frac{a_i}{b_i} = const$$

Proof. Define $f(x) = x\log x$,then $f^{(2)}(x) = \frac{1}{x} > 0$,so $f(x)$ is convex.

$$\begin{aligned}\sum_i a_i\log\frac{a_i}{b_i} =& (\sum_j b_j)\sum_i \frac{b_i}{\sum\limits_j b_j}\frac{a_i}{b_i}\log\frac{a_i}{b_i}\\ \geq& (\sum_j b_j)(\sum_i \frac{b_i}{\sum\limits_j b_j}\frac{a_i}{b_i})\log(\sum_i \frac{b_i}{\sum\limits_j b_j}\frac{a_i}{b_i})\\ =& \sum_i a_i\log\frac{\sum\limits_{i=1}^n a_i}{\sum\limits_{i=1}^n b_i}\end{aligned}$$

□

Theorem 1.7.2. ***KL-Divergence is a convex function.***

For two pair of PMF (p_1,q_1) and (p_2,q_2),we have:

$$D[\lambda p_1+(1-\lambda)p_2 \parallel \lambda q_1+(1-\lambda)q_2] \leq \lambda D[p_1 \parallel q_1]+(1-\lambda)D[p_2 \parallel q_2]$$

Also can be noted as:

$$(D(\lambda\begin{bmatrix}p_1\\p_2\end{bmatrix}+(1-\lambda)\begin{bmatrix}p_2\\q_2\end{bmatrix}) \leq \lambda D(\begin{bmatrix}p_1\\q_1\end{bmatrix})+(1-\lambda)D(\begin{bmatrix}p_2\\q_2\end{bmatrix}))$$

Proof.

$$
\begin{aligned}
left =& \sum_x (\lambda p_1 + (1-\lambda)p_2) \log \frac{\lambda p_1 + (1-\lambda)p_2}{\lambda q_1 + (1-\lambda)q_2} \\
=& \sum_x (\sum_{l=1}^{2} \lambda_l p_l) \log \frac{\sum\limits_{l=1}^{2} \lambda_l p_l}{\sum\limits_{l=1}^{2} \lambda_l q_l} \quad (\lambda_1 = \lambda, \lambda_2 = 1-\lambda) \\
\leq& \sum_x \sum_{l=1}^{2} \lambda_l p_l \log \frac{\lambda_l p_l}{\lambda_l q_l} \\
=& \lambda \sum_x p_1 \log \frac{p_1}{q_1} + (1-\lambda) \sum_x p_2 \log \frac{p_2}{q_2} \\
=& \lambda D[p_1 \parallel q_1] + (1-\lambda) D[p_2 \parallel q_2] = right
\end{aligned}
$$

$$\therefore D[\lambda p_1 + (1-\lambda)p_2 \parallel \lambda q_1 + (1-\lambda)q_2] \leq \lambda D[p_1 \parallel q_1] + (1-\lambda) D[p_2 \parallel q_2]$$

□

Theorem 1.7.3. ***Concavity of Entropy:***

$$H(\lambda p_1 + (1-\lambda)p_2) \geq \lambda H(p_1) + (1-\lambda) H(p_2)$$

Proof.

$$H[p] = -\sum_x p(x) \log p(x) \qquad u(x) = \frac{1}{M} \quad M = |\mathfrak{X}|$$

$$
\begin{aligned}
D[p \parallel u] =& \sum_x p(x) \log \frac{p(x)}{u(x)} = \sum_x p(x) \log p(x) - \sum_x p(x) \log u(x) \\
=& -H[p] - \log M = -H[p] - \log |\mathfrak{X}| \\
&\because D \text{ is a convex function} \\
&\therefore H \text{ is a concave function} \\
&\therefore H(\lambda p_1 + (1-\lambda)p_2) \geq \lambda H(p_1) + (1-\lambda) H(p_2)
\end{aligned}
$$

□

Alternative proof:

Proof.

$$1.\text{Generate an R.V: } \theta = \begin{cases} 1 & \text{with probability: } \lambda \\ 2 & \text{with probability: } 1-\lambda \end{cases}$$

$$2.\text{Generate an R.V: } X \sim \begin{cases} p_1 & \text{if } \theta = 1 \\ p_2 & \text{if } \theta = 2 \end{cases}$$

$$\begin{aligned} \Rightarrow p(x) &= \sum_{\theta} p(x,\theta) = \sum_{\theta=1}^{2} p(x|\theta)p(\theta) \\ &= \lambda p_1(x) + (1-\lambda)p_2(x) \end{aligned}$$

$$\Rightarrow H[\lambda p_1 + (1-\lambda)p_2]$$

$$\begin{aligned} = H(X) \geq H(X|\theta) &= -\sum_{x,\theta} p(x,\theta)\log p(x|\theta) \\ &= -\sum_{x}\sum_{\theta=1}^{2} p(x|\theta)p(\theta)\log p(x|\theta) \\ &= -\lambda\sum_{x} p_1\log p_1 - (1-\lambda)\sum_{x} p_2\log p_2 \\ &= \lambda H(p_1) + (1-\lambda)H(p_2) \end{aligned}$$

$$\therefore H(\lambda p_1 + (1-\lambda)p_2) \geq \lambda H(p_1) + (1-\lambda)H(p_2)$$

□

Theorem 1.7.4. ***Convexity of Mutual Information:***

Let $(X,Y) \sim p(x,y) = p(x)p(y|x)$. The mutual information $I(X;Y)$ is a concave function of $p(x)$ for fixed $p(y|x)$ and a convex function of $p(y|x)$ for fixed $p(x)$.

$$I(X;Y) \begin{cases} \textit{concave of } \; p(x), \textit{for fixed } \; p(y|x) \\ \textit{convex of } \; p(y|x), \textit{for fixed } \; p(x) \end{cases}$$

Proof.

$$\begin{aligned} I(X;Y) = &\sum_{x,y} p(x,y)\log\frac{p(x,y)}{p(x)p(y)} \\ &= H(Y) - H(Y|X) = H(Y) - \sum_{x} p(x)H(Y|X=x) \end{aligned}$$

If $p(y|x)$ is fixed, then $p(y) = \int p(x)p(y|x)dx$ is a linear function of $p(x)$. Because $H(Y)$ is a concave function of $p(y)$, so H(Y) is a concave function of $p(x)$. The latter term $p(x)H(Y|X=x)$ is a linear function of $p(x)$, so $I(X;Y)$ is a concave function of $p(x)$.

Fix $p(x)$, set two CPMF $p_1(y|x), p_2(y|x)$

$$\begin{aligned}
p_\lambda(y|x) =& \lambda p_1(y|x) + (1-\lambda)p_2(y|x) \\
p_\lambda(x,y) =& p(x)p_\lambda(y|x) = \lambda p_1(x,y) + (1-\lambda)p_2(x,y) \\
p_\lambda(y) =& \int p_\lambda(x,y)dx = \lambda p_1(y) + (1-\lambda)p_2(y) \\
&\text{Set } \ q_\lambda(x,y) = p(x)p_\lambda(y) \\
q_\lambda(x,y) =& \lambda q_1(x,y) + (1-\lambda)q_2(x,y) \\
I(X;Y) =& \sum_{x,y} p_\lambda(x,y)\log\frac{p_\lambda(x,y)}{p(x)p_\lambda(y)} = D[p_\lambda \parallel q_\lambda] \\
\because D[p_\lambda \parallel q_\lambda] \ & \text{ is a convex function of } p_\lambda \\
& p_\lambda(x,y) = p(x)p_\lambda(y|x) \text{ is a linear function of } p_\lambda(y|x) \\
\therefore I(X;Y) \ & \text{ is a convex function of } \ p(y|x)
\end{aligned}$$

□

1.8 Data Processing Inequality

Definition 1.8.1. ***Markov Chain:***
R.V X,Y,Z form a MC: $X \to Y \to Z$ *if* $p(x,y,z) = p(x)p(y|x)p(z|y)$, *which also means* $p(x,z|y) = p(x|y)p(z|y)$.

If any part of a process only depends on the previous part,then any three continuous parts of the process form a Markov Chain.

Example 1.8.1. *If a Checker is placed on a chessboard,and the probability of next move is:*

$$P(X) = \begin{cases} p_1, X = up \\ p_2, X = down \\ p_3, X = left \\ p_4, X = right \end{cases}$$

any three continuous moves form a Markov Chain.

Theorem 1.8.1. ***Data Processing Inequality:***
If $X \to Y \to Z$ *form a Markov Chain,then* $I(X;Y) \geq I(X;Z)$.

Proof.

$$\begin{aligned}
I(X;Y,Z) =& I(X;Z) + I(X;Y|Z) \\
=& I(X;Y) + I(X;Z|Y) \\
\because X|Y \perp Z|Y \Rightarrow X \perp Z|Y \Rightarrow & I(X;Z|Y) = 0 \\
\therefore I(X;Y,Z) = I(X;Y) = & I(X;Z) + I(X;Y|Z) \\
\because I(X;Y|Z) \geq 0 & \\
\therefore I(X;Y) \geq & I(X;Z)
\end{aligned}$$

□

Corollary 1.8.1. *If* $Z = f(Y) \Rightarrow I(X;Y) \geq I(X;f(Y))$

1.9 Fano's Inequality

We want to estimate an unknown R.V X with a distribution $p(x)$. We observe an R.V Y that is related to X by the conditional distribution $p(y|x)$. From Y,we caculate a function $f(Y) = \hat{X}$. $X, Y, \hat{X}$ form a MC $X \to Y \to \hat{X}$.

Define the probability of error:

$$P_e = P(\hat{X} \neq X) \qquad Y \sim P(Y|X)$$

We can set the R.V E:

$$E = \begin{cases} 1 & \text{if } \hat{X} \neq X \\ 0 & \text{if } \hat{X} = X \end{cases} \qquad P_e = P(E = 1)$$

Theorem 1.9.1. ***Fano's Inequality:***

$$\begin{aligned} &H(P_e) + P_e \log|\mathfrak{X}| \geq H(X|\hat{X}) \geq H(X|Y) \\ \Rightarrow &1 + P_e \log|\mathfrak{X}| \geq H(X|Y) \\ \Rightarrow &P_e \geq \frac{H(X|Y) - 1}{\log|\mathfrak{X}|} \end{aligned}$$

Proof.

$$\begin{aligned} H(E, X|\hat{X}) =& H(X|\hat{X}) + H(E|X, \hat{X}) \\ =& H(E|\hat{X}) + H(X|E, \hat{X}) \end{aligned}$$

If $X, \hat{X}$ is fixed,then E is also fixed, so

$$H(E|X, \hat{X}) = 0 \Rightarrow H(E, X|\hat{X}) = H(X|\hat{X})$$

Since conditioning reduces entropy, we have:

$$H(E|\hat{X}) \leq H(E) = H(P_e)$$

It is easy to see that E is a binary-valued R.V, so $H(X|E, \hat{X})$ can be bounded as:

$$H(X|E, \hat{X}) = P_r(E = 0)H(X|\hat{X}, E = 0) + P_r(E = 1)H(X|\hat{X}, E = 1)$$

Since $E = 0$ means $\hat{X} = X$, so $H(X|\hat{X}, E = 0) = 0$.
Since the upper bound of H is $\log|\mathfrak{X}|$, so: $H(X|E, \hat{X}) \leq P_e \log|\mathfrak{X}|$
Combine the above results, we have:

$$H(E|\hat{X}) + H(X|E, \hat{X}) \leq H(E) + (1 - P_e)0 + P_e \log|\mathfrak{X}|$$

$$\Rightarrow H(X|\hat{X}) \leq H(P_e) + P_e \log|\mathfrak{X}|$$

□

§ 2 AEP(Asymptotic Equipartition Property)

2.1 AEP

Review:Law of large numbers:

For $X_1, X_2, \ldots, X_n$ i.i.d $\sim P \rightarrow$ note as $\underline{X}_n$:

$$\frac{1}{n}\sum_i X_i \overset{n\to\infty}{\underset{p.}{\rightarrow}} \mathbf{E}X = \sum_x xp(x)$$

Theorem 2.1.1. ***AEP:***

$$\frac{1}{n}\log\frac{1}{p(\underline{X}_n)} = \frac{1}{n}\sum_{i=1}^{n}\log\frac{1}{p(X_i)} \overset{n\to\infty}{\underset{p.}{\rightarrow}} \mathbf{E}\log\frac{1}{p(x)} = H(X)$$

Definition 2.1.1. ***Typical Set:***

$A_\epsilon^{(n)}$ is a set of sequences $(x_1, x_2, \ldots, x_n) \in X^{(n)}$ with the property that:

$$2^{-n(H(X)+\epsilon)} \leq p(x_1, x_2, \ldots, x_n) \leq 2^{-n(H(X)-\epsilon)}$$

1. $\left|A_\epsilon^{(n)}\right| = 2^{nH(X)}$

2. $(1-\epsilon)2^{nH(X)} \leq P(A_\epsilon^{(n)}) \rightarrow 1$

Example 2.1.1.

$$X_i \sim Bernollip = \begin{cases} 1 & \text{with probability: } p = 0.9 \\ 0 & \text{with probability: } p = 0.1 \end{cases}$$

Now we sample $n = 100$ times,then we have:

$$(1, 1, 1, \ldots, 1, 1) \text{with 100 "1"}$$

$$(1, 0, 1, 1, 0, \ldots, 0, 1) \text{with 90 "1" and 10 "0"}$$

Obviously, the second one is more likely to happen.

Theorem 2.1.2. ***Property of the typical set:***

(1) If $(x_1, \ldots, x_n) \in A_\epsilon^{(n)}$ then

$$H(X) - \varepsilon \leq -\frac{1}{n}\log p(x_1, \ldots, x_n) \leq H(X) + \varepsilon$$

(2) $P_r(X_1, \ldots, X_n) \in A_\epsilon^{(n)} \geq 1 - \varepsilon$ for n sufficiently large.

(3) $\left|A_\epsilon^{(n)}\right| \leq 2^{n(H(X)+\varepsilon)}$

(4) $\left|A_\epsilon^{(n)}\right| \geq 2^{n(H(X)-\varepsilon)}$

From (3) and (4),we have:

$$\left|A_\epsilon^{(n)}\right| \approx 2^{nH(X)}$$

Proof. (2) From AEP, $-\frac{1}{n}\log p(x_1,\ldots,x_n) \xrightarrow{p.} H(X)$

$\therefore$ For any $\delta > 0, \varepsilon > 0, \exists n_0, \forall n \geq n_0$:

$$P_r\{\left|-\frac{1}{n}\log p(x_1,\ldots,x_n) - H(X)\right| < \varepsilon\} \geq 1-\delta$$

set $\delta = \varepsilon$,then: $P_r\{A_\varepsilon^{(n)}\} \geq 1-\varepsilon$

(3)

$$1 = \sum_{\underline{x}_n \in X^{(n)}} P(x) \geq P_r\{A_\varepsilon^{(n)}\} = \sum_{\underline{x}_n \in A_\varepsilon^{(n)}} P(x) \geq \sum_{\underline{x}_n \in A_\varepsilon^{(n)}} 2^{-n(H(X)+\varepsilon)}$$

$$= \left|A_\epsilon^{(n)}\right| 2^{-n(H(X)+\varepsilon)}$$

$\Rightarrow \left|A_\epsilon^{(n)}\right| \leq 2^{n(H(X)+\varepsilon)}$

(4)

$$1-\varepsilon \leq P_r\{\left|A_\epsilon^{(n)}\right|\} \leq \sum_{\underline{x}_n \in A_\varepsilon^{(n)}} 2^{-n(H(X)-\varepsilon)} = \left|A_\epsilon^{(n)}\right| 2^{-n(H(X)-\varepsilon)}$$

$\Rightarrow \left|A_\epsilon^{(n)}\right| \geq (1-\varepsilon)2^{n(H(X)-\varepsilon)}$

$\square$

2.2 Consequences of AEP:Data Compression

Compression Scheme:

1. If $\underline{x}_n = (x_1,\ldots,x_n) \in A_\varepsilon^{(n)}$,we use $\lceil n(H(X)+\varepsilon)\rceil$ to encode $\underline{x}_n$;
2. If $\underline{x}_n \notin A_\varepsilon^{(n)}$,we use $\lceil n\log|X|\rceil$ to encode $\underline{x}_n$;
3. Use extra 1 bit to identify whether $\underline{x}_n \in A_\varepsilon^{(n)}$ or not.

$$\underline{x}_n \to b_1 b_2 \cdots b_{l(\underline{x}_n)}$$

Here, b_1=1 or 0, $l(\underline{x}_n) \leq \begin{cases} n(H(X)+\varepsilon)+2 & (1) \\ n\log|X|+2 & (2) \end{cases}$

Theorem 2.2.1.

$$\mathbf{E}[\frac{1}{n}l(\underline{x}_n)] \leq H(X)+\varepsilon$$

Proof.

$$
\begin{aligned}
\mathbf{E}[\frac{1}{n}l(\underline{x}_n)] &= \sum_{\underline{x}_n} p(\underline{x}_n)\cdot\frac{1}{n}l(\underline{x}_n) \\
&= \sum_{\underline{x}_n\in A_\varepsilon^{(n)}} p(\underline{x}_n)\cdot\frac{1}{n}l(\underline{x}_n) + \sum_{\underline{x}_n\notin A_\varepsilon^{(n)}} p(\underline{x}_n)\cdot\frac{1}{n}l(\underline{x}_n) \\
&\le \sum_{\underline{x}_n\in A_\varepsilon^{(n)}} p(\underline{x}_n)\cdot\frac{1}{n}(n(H(X)+\varepsilon)+2) + \sum_{\underline{x}_n\notin A_\varepsilon^{(n)}} p(\underline{x}_n)\cdot\frac{1}{n}(n\log|X|+2) \\
&= P_r\{A_\varepsilon^{(n)}\}\cdot\frac{1}{n}(n(H(X)+\varepsilon)+2) + (1-P_r\{A_\varepsilon^{(n)}\})\cdot\frac{1}{n}(n\log|X|+2) \\
&\le \frac{1}{n}(n(H(X)+\varepsilon)+2) + \varepsilon\frac{1}{n}(n\log|X|+2) \\
&= H(X)+\varepsilon+\frac{2}{n}+\frac{\varepsilon}{n}\log|X|+\frac{2\varepsilon}{n} \\
&= H(X)+\varepsilon' \qquad \text{Here,we set } \varepsilon' = \varepsilon+\frac{2}{n}+\frac{\varepsilon}{n}\log|X|+\frac{2\varepsilon}{n}
\end{aligned}
$$

□

§ 3 Data Compreession

3.1 Code

Definition 3.1.1. ***Source Code:***

(1) For a R.V. X is a map

$$C : X \to D^* \qquad x \mapsto d_1 d_2 \cdots d_{l(x)} = c(x)$$

*(2) $c(x)$ is called **codeword** of x.*

*(3) $l(x)$ is called **length** of the codeword,$l(x) \leq \infty$.*

Example 3.1.1. $\mathcal{X} = \{1, 2, 3, 4\}$

x	$p(x)$	Codeword(*)	Codeword(Native)
1	$\frac{1}{2}$	0	00
2	$\frac{1}{4}$	10	01
3	$\frac{1}{8}$	110	10
4	$\frac{1}{8}$	111	11

$$\bar{l}(x) = H(X) = -\frac{1}{2}\log\frac{1}{2} - \frac{1}{4}\log\frac{1}{4} - \frac{1}{8}\log\frac{1}{8} - \frac{1}{8}\log\frac{1}{8} = 1.75 \ bit$$

Definition 3.1.2. ***Nonsigular Code:***
A code C is nonsigualr, if $\forall x \neq x'$ then $C(x) \neq C(x')$.

Definition 3.1.3. ***Extension of Code:***
For a code:

$$C : x \longmapsto C(x)$$

The extension of code is defined as:

$$C^* : x_1 x_2 \cdots x_n \longmapsto C(x_1)C(x_2)\cdots C(x_n)$$

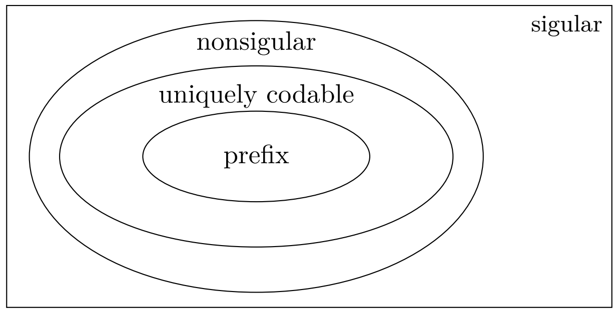
Definition 3.1.4. ***Uniquely Codable:***
A code is uniquely codable if C^* is nonsigular.

Example 3.1.2. *Here are some examples of codes:*

x	singular	nonsigualr	uniquely codable but no prefix	prefix
1	0	0	10	0
2	0	010	00	10
3	1	01	11	110
4	1	10	110	111
$C^*(324)$	101	0101010	1100110	11010111

Obviously, the nonsigular code 0101010 *can be decoded as* 324 *or* 3331*.*

Definition 3.1.5. ***Prefix Code/Instantaneous Code:***
A code is a prefix code if no codeword is a prefix of any other code.



3.2 Kraft Inequality

Theorem 3.2.1. ***Kraft Inequality:***

1) For any prefix code over an alphabet of size D. The code length $l_1, l_2, \ldots, l_m$ must satisfy:

$$\sum_{i=1}^{m} D^{-l_i} \leq 1$$

2) Conversely, given a set of word length $\{l_1, \ldots, l_m\}$ then there exists a prefix code with those lengths, if the set satisfies the Kraft inequality.

3.3 Optimal Codes

Here we will show some inferences:

$$x \in \{x_1, \dots, x_m\} \quad p(x) = p_1, \dots, p_m$$
$$C(x_1), \dots, C(x_m) \quad l(x_1), \dots, l(x_m) \quad \bar{l} = \sum_{i=1}^{m} p_i l(x_i)$$
$$\text{We want to find:} \min_{l_i} \bar{l} = \sum_{i=1}^{m} p_i l(x_i) \quad s.t. \sum_i D^{-l_i} \le 1$$
$$l_i \in \mathbf{Z}^* \Rightarrow l_i \in \mathbf{R}^*$$
$$J = \sum_i p_i l_i + \lambda(\sum_i D^{-l_i} - 1)$$
$$\frac{\partial J}{\partial l_j} = p_j - \lambda D^{-l_j} \ln D = 0 \Rightarrow D^{-l_j} = \frac{p_j}{\lambda \ln D}$$
$$\frac{\partial J}{\partial lambda} = \sum_i D^{-l_i} - 1 = 0 \Rightarrow \frac{\sum_i p_i}{\lambda \ln D} = 1 \Rightarrow \lambda = \frac{1}{\ln D}$$
$$D^{-l_j} = \frac{p_j}{\lambda \ln D} = p_j \Rightarrow l_j^* = -\log_D p_j$$
$$\bar{l}^* = \sum_i p_i l_i^* = \sum_i p_i(-\log_D p_i) = -\sum_i p_i \log_D p_i = H_D[X]$$

Theorem 3.3.1. *The expected length L of any prefix D-adic code satisfies:*

$$L \ge H_D[X]$$

3.4 Upper bound on the optimal code length

Theorem 3.4.1.
$$H_D[X] \le \bar{l}^* \le H_D[X] + 1$$

Proof.

$$l_i^* \in \mathbf{R}^* \Rightarrow l_i = \lceil l_i^* \rceil \in \mathbf{Z}^*$$
$$\sum_i D^{-l_i} \le \sum_i D^{-l_i^*} = 1 \quad \text{Kraft Inequality holds}$$
$$\sum_i p_i \lceil l_i^* \rceil \le \sum_i p_i(l_i^* + 1) = \sum_i p_i l_i^* + \sum_i p_i = H_D[X] + 1$$

□

***Wrong Code:**If we use anothor distribution $q(x)$ instead of the true $p(x)$, then we will get:

Theorem 3.4.2. ***Wrong Code:***

$$l(x) = \left\lceil \log \frac{1}{q(x)} \right\rceil$$

$$\bar{l} = \mathbf{E}l(x) = \sum_i p(x_i)l(x_i) = \sum_i p(x_i) \left\lceil \log \frac{1}{q(x)} \right\rceil$$

$$\begin{aligned}
\sum_i p(x_i) \left\lceil \log \frac{1}{q(x)} \right\rceil <& \sum_i p(x_i)(\log \frac{1}{q(x)} + 1) \\
=& \sum_i p(x_i) \log \frac{p(x_i)}{q(x_i)} - \sum_i p(x_i) \log p(x_i) + \sum_i p(x_i) \\
=& D(p \parallel q) + H[p] + 1 \\
\sum_i p(x_i) \left\lceil \log \frac{1}{q(x)} \right\rceil >& D(p \parallel q) + H[p]
\end{aligned}$$

We call $D(p \parallel q)$ the puhishment of wrong code.

3.5 Huffman Code

Observation:

1. Smaller probability $\Rightarrow$ longer codeword.
2. The two longest codewords must have the same length.
3. Two longest codewords merges to one single source symbol, with the probability being the sum of the replaced two symbols.

Here we have the Huffman algorithm:

Input:$\{(x_i, p_i) | i = 1, 2, \cdots, n\}$
Output: $\{C(x_i)\}$ A tree representing Huffman code.
Algorithm:

```
Initialize Q as the PriorityQueue ({p_i,x_i,N_i})//N_i is the tree node
While Q.size()>1:
    p_1,x_1,N_1 = Q.pop()
    p_2,x_2,N_2 = Q.pop()
    N_3 = NewTreeNode(N_1,N_2)
    Q.push(p_1+p_2,Null,N_3)
return Q.pop()
```

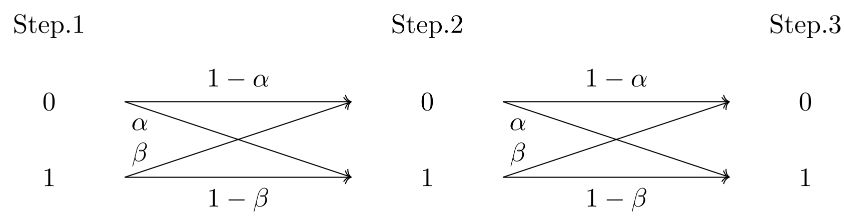
§ 4 Entropy Rate of a stochastic process

$X \leftarrow H[X]$
$X_1, X_2, \ldots, X_n i.i.d \sim p(x) \leftarrow H[X_1, X_2, \ldots, X_n] = nH[X]$
Normally, $X_1, \ldots, X_n, X_i \not\perp X_j, H[X_1, \ldots, X_n] =? \propto n \cdot h$
Here, h is called the entropy rate of the process.

4.1 Markove Chain

$$P(X_n|X_1, X_2, \ldots, X_{n-1}) = P(X_n|X_{n-1})$$

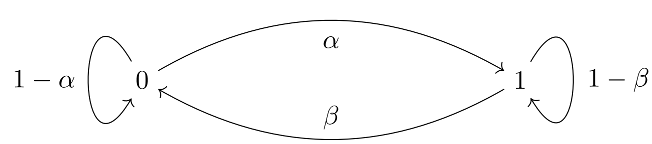
Example 4.1.1. $x \in \{0, 1\}$



This is a Markov Chain with 3 steps.
To describe a Markov Chain, we need:

1. $P_0(X_0)$
2. $P(X_{n+1}|X_n) = \begin{bmatrix} P(0|0) = 1-\alpha & P(1|0) = \alpha \\ P(0|1) = \beta & P(1|1) = 1-\beta \end{bmatrix}$

We can also use a map to describe a Markov Chain:



Definition 4.1.1. ***Time invariant Markov Chain:***
A Markov Chain is time invariant if the transition probability does not depend on time:

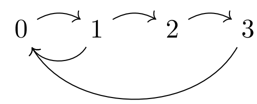
$$P_{k+1}(X_{k+1}|X_k) = P_k(X_k|X_{k-1})$$

Notions of Markov Chain:

1. **State:**X_i is a state of the Markov Chain, X_0 is the initial state.

2. **Irreducable:**$\forall i, j, \exists n, s.t. P(X_n = j | X_i = i) > 0$
3. **Aperiodic:**The largest common factoer of the length of paths from a state to itself is 1.

   Example 4.1.2. *Here is a Markov Chain with 4 states:*

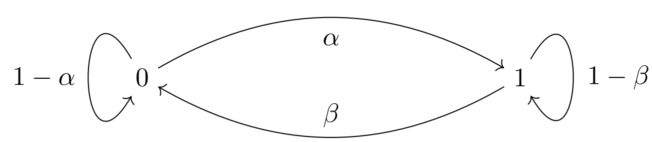
   Length of path 1 is 2, length of path 2 is 4, the largest common factor is 2.

   This Markov Chain is not aperiodic.

4. **Probability trainsition matrix:**$p_{ij} = P(X_{n+1} = X_j | X_n = X_i)$

   $P = [p_{ij}] \qquad P(X_{n+1}) = \sum_{X_n} P(X_{n+1}, X_n) = [P(X_1) \dots P(X_n)]P$

   Example 4.1.3. $P(X_{n+1}|X_n) = \begin{bmatrix} P(0|0) = 1-\alpha & P(1|0) = \alpha \\ P(0|1) = \beta & P(1|1) = 1-\beta \end{bmatrix}$

$$V_n = \begin{matrix} P(X_n = 0) \\ P(X_n = 1) \end{matrix} = \begin{matrix} 0.1 \\ 0.9 \end{matrix} \qquad V_{n+1} = V_n^T P \qquad V_\infty = ?$$

$$V_\infty = V_\infty P \Rightarrow \begin{cases} (1-\alpha)V_1 + \beta V_2 = V_1 \\ \alpha V_1 + (1-\beta)V_2 = V_2 \\ V_1 + V_2 = 1 \end{cases} \Rightarrow \begin{cases} (1-\alpha)V_1 + \beta V_2 = V_1 \\ V_1 + V_2 = 1 \end{cases}$$

$$\Rightarrow \frac{V_1}{V_2} = \frac{\beta}{\alpha}$$

4.2 Entropy Rate

Definition 4.2.1. ***Entropy Rate:***

1) The entropy rate of a stochastic process $\{X_i\}$ is defined as:

$$H[\mathcal{X}] = \lim_{n\to\infty} \frac{1}{n} H[X_1, \dots, X_n]$$

2) Conditional entropy rate:

$$H'[\mathcal{X}] = \lim_{n\to\infty} H[X_n|X_1, \dots, X_{n-1}]$$

Definition 4.2.2. ***Stationary stochastic process:***
A stochastic process $\{X_i\}$ is stationary if the joint distribution of $X_1, \dots, X_n$ does not depend on n:

$$P(X_{l+1}, \dots, X_{l+n}) = P(X_{l+2}, \dots, X_{l+n+1})$$

Theorem 4.2.1. *For a stationary stochastic process:*

$$\begin{aligned} &H[X_n|X_1, \dots, X_{n-1}] \geq H[X_{n+1}|X_1, \dots, X_n] \\ \Rightarrow &H'[\mathcal{X}] \textit{ exists a limit} \end{aligned}$$

Proof.

$$H[X_n|X_1, \dots, X_{n-1}] = H[X_{n+1}|X_1, \dots, X_n] \geq H[X_{n+1}|X_1, \dots, X_n]$$

□

Theorem 4.2.2. ***Cesáro mean:***
If $a \to a_n, b_n = \frac{1}{n}\sum\limits_{i=1}^{n} a_i$, then $b_n \to a$

Based on the above theorem, we can get:

$$\begin{aligned} H[\mathcal{X}] &= \lim_{n\to\infty} \frac{1}{n} H[X_1, \dots, X_n] \\ &= \lim_{n\to\infty} (H[X_1] + H[X_2|X_1] + \dots + H[X_n|X_1, \dots, X_{n-1}]) \end{aligned}$$

$$H[X_n|X_1, \dots, X_{n-1}] \stackrel{def}{=} b_n$$

$$H[\mathcal{X}] = \lim_{n\to\infty} \frac{1}{n} \sum_{m=1}^{n} b_m = \lim_{n\to\infty} b_n = H'[\mathcal{X}]$$

Theorem 4.2.3. ***Entropy rate of a Markov Chain:***
Obviously, the entropy rate only depends on the transition probability matrix:

$$H[\mathcal{X}] = F(P)$$

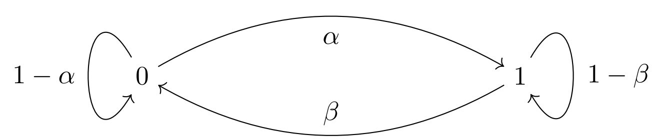
$$\begin{aligned} H[\mathcal{X}] = H'[\mathcal{X}] &= \lim_{n\to\infty} H[X_n|X_1, \dots, X_{n-1}] = \lim_{n\to\infty} H[X_n|X_{n-1}] \\ &= H[X_2|X_1] \qquad X \sim V_\infty \qquad V_\infty = V_\infty P \\ &= -\sum_{X_1} V_\infty P(X_2|X_1) \log P(X_2|X_1) \end{aligned}$$

Theorem 4.2.4. *Let u and P be the stationary distribution and transition probability matrix respectively, then the entropy rate:*

$$H[\mathcal{X}] = -\sum_{i,j} u_i P_{ij} \log P_{ij}$$

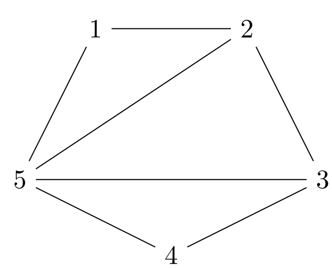
where $u_j = \sum_i u_i p_{ij}$

Example 4.2.1. *For the Markov Chain:*



$$\begin{aligned}
H[\mathcal{X}] =& H[X_2|X_1] \\
=& -\frac{\beta}{\alpha+\beta}((1-\alpha)\log(1-\alpha) + \alpha\log\alpha) - \frac{\alpha}{\alpha+\beta}((1-\beta)\log(1-\beta) + \beta\log\beta) \\
=& \frac{\beta}{\alpha+\beta}H[X_1] + \frac{\alpha}{\alpha+\beta}H[X_2]
\end{aligned}$$

Example 4.2.2. ***Random walk on a graph:***



$$
\begin{aligned}
&X_k \in \{1,2,3,4,5\} \quad k=0,1,2 \quad X_0 = l\\
&P(X_{k+1}=j|X_k=i) = \frac{A_{ij}}{d_i} \quad A_{ij} = \begin{cases} 1 & \textit{if } (i,j) \in E \\ 0 & \textit{otherwise} \end{cases}\\
&P_0(X_0) = \begin{cases} 1 & \textit{if } X_0 = l \\ 0 & \textit{otherwise} \end{cases} \quad v^* = v^* P \quad v^* = [v_1, v_2, \ldots, v_5]\\
&v^*P = [v_1\frac{A_{11}}{d_1} + v_2\frac{A_{21}}{d_2} + v_3\frac{A_{31}}{d_3} + v_4\frac{A_{41}}{d_4} + v_5\frac{A_{51}}{d_5}, \ldots]\\
&\Rightarrow v_i^* = \frac{d_i}{2D} \quad D = |E|\\
H[\mathcal{X}] &= -\sum_{i,j} v_i^* p_{ij} \log p_{ij} = -\sum_{i,j} \frac{d_i}{2D}\frac{A_{ij}}{d_i} \log\frac{A_{ij}}{d_i} = -\sum_{i,j}\frac{A_{ij}}{2D}\log(\frac{A_{ij}}{2D}\frac{2D}{d_i})\\
&= -\sum_{i,j}\frac{A_{ij}}{2D}\log\frac{A_{ij}}{2D} - \sum_{i,j}\frac{A_{ij}}{2D}\log\frac{2D}{d_i}\\
&= -\sum_{i,j}\frac{A_{ij}}{2D}\log\frac{A_{ij}}{2D} + \sum_{i}\frac{d_i}{2D}\log\frac{d_i}{2D}\\
&= log(2D) - H[v^*]
\end{aligned}
$$

§ 5 Mutual Information Estimation

5.1 Fenchel-Legendre Transform

Definition 5.1.1. ***F-L transform***
For a given $f(u)$, Fenchel-Legredre transform of f is defined by:

$$f^*(t) = \sup_u \{ut - f(u)\}$$

Corollary 5.1.1. *If f is convex, the $ut - f(u)$ is concave.*

$$u^* : \frac{d(ut - f(u))}{du} = 0 \Rightarrow t = f'(u^*) \Rightarrow u^* = f'^{-1}(t)$$

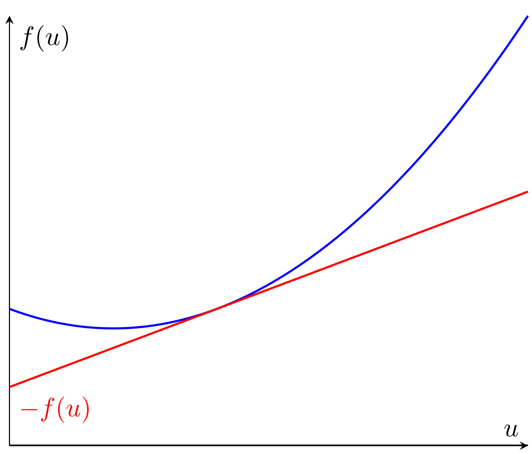
therefore, $f^*(t) = u^*t - f(u^*), u^* = f'^{-1}(t)$

Definition 5.1.2. ***Inverse FL transform***

$$f^{**}(u) = (f^*)^* = \sup_t \{ut - f^*(t)\}$$

Example 5.1.1. *Obviously, the tangent line of $f(u)$ at u^* is:*

$$g(u) = ut^* - f(u^*)$$



Each t corresponds to a tangent line of $f(u)$.

Theorem 5.1.1. ***F-L transform for a convex***
If $f(u)$ is strictly convex, then $f^{**} = f$.

Proof.

$$\begin{aligned}
f^*(t) &= u^*t - f(u^*) \quad \text{where } t = f'(u^*) \\
f^{**}(u) &= (f^*(t))^* = \sup_t \{ut - u^*t + f(u^*)\} \\
&= \sup_{u^*} \{uf'(u^*) - u^*f'(u^*) + f(u^*)\} \\
\frac{d[f'(u^*)(u-u^*) + f(u^*)]}{du^*} &= f''(u^*)(u-u^*) - f'(u^*) + f'(u^*) \\
&= f''(u^*)(u-u^*) = 0 \\
\because f \text{ is strictly convex} &\Rightarrow f''(u^*) > 0 \Rightarrow u = u^* \\
\therefore f^{**}(u) &= \sup_t \{ut - u^*t + f(u^*)\} = f(u)
\end{aligned}$$

□

5.2 Estimate Mutual Information/K-L Divergence via maximizing lower bound

- **Setting:**Suppose we have a set of observed data:

$$\{(Y_1, Z_1), (Y_2, Z_2), \ldots, (Y_m, Z_m)\} = D \quad (Y_i, Z_i) \sim P(Y, Z) \to \text{Unkown}$$

- **Task:**The objective is to estimate:

$$I[Y; Z] = \sum_{Y,Z} p(Y, Z) \log \frac{p(Y, Z)}{p(Y)p(Z)} = D[p(Y, Z) \parallel (p(Y)p(Z))]$$

Example 5.2.1.

$$Y \in \{0, 1\} \qquad Z \in \{0, 1\}$$

i	Y	Z
1	0	1
2	0	0
3	1	1
4	0	0
5	0	1
6	1	1
7	0	0
8	1	0

$$P(Y, Z) = \frac{\#(Y, Z)}{\#total}$$

When the dimension of observed data is too large, it is hard to estimate the distribution by the frequency.

Theorem 5.2.1. ***Nguyen 2010:***

$$D[P(X) \parallel Q(X)] = \mathop{\mathbf{E}}_{X\sim P} \log \frac{P(X)}{Q(X)} \geq \sup_{T\in\mathcal{T}} \{ \mathop{\mathbf{E}}_{X\sim P} T(X) - \mathop{\mathbf{E}}_{X\sim Q} e^{T(X)-1} \}$$

Through this theorem, we can estimate the mutual information by machine learning.

Proof.

$$\begin{aligned} D[P(X) \parallel Q(X)] &= \sum_X P(X) \log \frac{P(X)}{Q(X)} = \sum_X Q(X) \frac{P(X)}{Q(X)} \log \frac{P(X)}{Q(X)} \\ &= \sum_X Q(X) f(u) \quad \begin{cases} u = \frac{P(X)}{Q(X)} \\ f(u) = u \log u \end{cases} \end{aligned}$$

$$f'(u) = \log u + 1 \quad f'(u^*) = t = \log u^* + 1 \Rightarrow u^* = e^{t-1}$$

$$f^*(t) = u^* t - f(u^*) = te^{t-1} - f(e^{t-1}) = e^{t-1}$$

$$\begin{aligned} \therefore \sum_X Q(X) f(u) &= \sum_X Q(X) (f^*)^* = \sum_X Q(X) \sup_t \{ut - f^*(t)\} \\ &= \sum_X Q(X) \sup_t \{ \frac{P(X)}{Q(X)} t - f^*(t) \} \end{aligned}$$

$$\because f = u \log u \text{ is convex} \Rightarrow f^* \text{ is concave} \Rightarrow f^{**} \text{ is convex}$$

$$\begin{aligned} \therefore \sum_X Q(X) f(u) &\geq \sup_t \{ \sum_X Q(X) [\frac{P(X)}{Q(X)} t - f^*(t)] \} \\ &= \sup_t \{ \sum_X P(X) t - \sum_X Q(X) f^*(t) \} \\ &= \sup_X \{ \mathop{\mathbf{E}}_{X\sim P} t_X - \mathop{\mathbf{E}}_{X\sim Q} f^*(t) \} \\ &= \sup_X \{ \mathop{\mathbf{E}}_{X\sim P} t_X - \mathop{\mathbf{E}}_{X\sim Q} e^{t_X - 1} \} \end{aligned}$$

□

5.3 Implement the estimation of I using lower bound

Let $X = (Y, Z) \quad P(X) = P(Y, Z) \quad Q(X) = P(Y)P(Z)$

Critic function $T_\theta(X)$: Define a neural network $T_\theta(X)$ with parameter $\theta = \{\omega_1, \omega_2\}$.$T_\theta = f(\omega_2 f(\omega_1 X))$ while f is a non-linear function.

$$\max_\theta \{ \sum_{Y,Z} P(Y, Z) T_\theta(Y, Z) - \sum_{Y,Z} P(Y)P(Z) e^{T_\theta(Y,Z)-1} \}$$

$$\approx \max_\theta \{ \frac{1}{N} \sum_{i=1}^N T_\theta(Y_i, Z_i) - \frac{1}{N^2} \sum_{i=1}^N \sum_{j=1}^N e^{T_\theta(Y_i, Z_j)-1} \}$$

$$\approx \max_\theta \{ \frac{1}{N} \sum_{i=1}^N T_\theta(Y_i, Z_i) - \frac{1}{M} \sum_{k=1}^M e^{T_\theta(Y_{i_k} Z_{j_k})-1} \} \quad i_k, j_k \quad i.i.d. \sim (1, \dots, N)$$

§ 6 Information Theory and Statistics

6.1 Method of type

Definition 6.1.1. ***Type:***

$$P_x = \frac{\textit{Number of } X_i \textit{ equal to } a}{\textit{Total number of sample } \underline{x}_n} = P_x(a)$$

Example 6.1.1.

$$\mathcal{X} = \{1,2,3\} \qquad \underline{x}_n = [1,1,3,2,1] \qquad n = 5$$

$$P_x(a=1) = \frac{3}{5} \qquad P_x(a=2) = \frac{1}{5} \qquad P_x(a=3) = \frac{1}{5}$$

Definition 6.1.2. *The probability simplex in* $\mathbf{R}^m$ *is the set of points* $\mathbf{x} = (x_1, x_2, \ldots, x_m) \in \mathbf{R}^m$ *such that:*$x_i \geq 0, \sum\limits_{i=1}^{m} x_i = 1$

Definition 6.1.3. $\mathcal{P}_n$ *denotes the set of all empirial distributions with number of samples n.*

Example 6.1.2. $\mathcal{X} = \{0,1\}$, $\mathcal{P}_n$ *is:*

$$\mathcal{P} = \{(P(0), P(1)) : (\frac{0}{n}, \frac{n}{n}), (\frac{1}{n}, \frac{n-1}{n}), \ldots, (\frac{n}{n}, \frac{0}{n})\}$$

Definition 6.1.4. ***Type class:***

$$T(P) = \{x \in \mathcal{X}^n : P_x = P\}$$

Example 6.1.3.

$$\mathcal{X} = \{1,2,3\} \qquad P = \{\frac{3}{5}, \frac{1}{5}, \frac{1}{5}\}$$

$$|T(P)| = \frac{5!}{3!1!1!} = 20$$

Theorem 6.1.1.

$$|\mathcal{P}_n| \leq (n+1)^{|\mathcal{X}|}$$

Proof.

$$P_x(a) = \frac{n_a}{n} \qquad n_a = 0, 1, \ldots, n$$

$\because a$ has $|\mathcal{X}|$ possible values.

The elements in $\mathcal{P}_n$ are like $(P(a_1), \ldots, P(a_{|\mathcal{X}|}))$

$\therefore |\mathcal{P}_n| \leq (n+1)^{|\mathcal{X}|}$

Actually, $\sum P_x(a) = 1$,when we fix $a_1, \ldots, a_{|\mathcal{X}|-1}$,the $a_{|\mathcal{X}|}$ is fixed.Therefore, $|\mathcal{P}_n| \leq (n+1)^{|\mathcal{X}|-1}$ ☐

Theorem 6.1.2. *Let* $x_1, x_2, \dots, x_n \overset{i.i.d}{\sim} Q(x)$

$$Q(\underline{x}_n) = 2^{-n(H[P_x]+D[P_x\|Q])}$$

Proof.

$$\begin{aligned}
Q(\underline{\mathrm{x}}_n) &= Q(x_1)\dots Q(x_n) = \prod_{i=1}^{n} Q(x_i) = \prod_{k=1}^{|\mathcal{X}|} Q(a_k)^{n_k} \qquad n_k = \#(x = a_k) \\
&= 2^{\sum_{k=1}^{|\mathcal{X}|} n_k \log Q(a_k)} = 2^{n\sum_{k=1}^{|\mathcal{X}|} \frac{n_k}{n} \log Q(a_k)} = 2^{n\sum_{k=1}^{|\mathcal{X}|} P_x(a_k)\log Q(a_k)} \\
&= 2^{n\sum_{k=1}^{|\mathcal{X}|} P_x(a_k)\log \frac{Q(a_k)}{P_x(a_k)} + n\sum_{k=1}^{|\mathcal{X}|} P_x(a_k)\log P_x(a_k)} \\
&= 2^{-n(H[P_x]+D[P_x\|Q])}
\end{aligned}$$

□

Theorem 6.1.3. ***Size of a type class:***$T(P)$*,* $P \in \mathcal{P}_n$*:*

$$\frac{1}{(n+1)^{|\mathcal{X}|}} 2^{nH(P)} \le |T(P)| \le 2^{nH(P)}$$

Proof. Here, we only prove the upper bound.

$$1 \ge P[\underline{\mathrm{x}}_n \in T(P)] = \sum_{\underline{\mathrm{x}}_n \in T(P)} P^n(\underline{\mathrm{x}}_n)$$

$$\begin{aligned}
P^n(\underline{\mathrm{x}}_n) &= \prod_{i=1}^{n} P(x_i) = 2^{\sum_{i=1}^{n} \log P(x_i)} = 2^{\sum_{a\in\mathcal{X}} n_a \log P(a)} \\
&= 2^{n\sum P(a \log P(a))} = 2^{-nH(P)} \\
\therefore 1 &\ge \sum_{\underline{\mathrm{x}}_n \in T(P)} 2^{-nH(P)} = |T(P)|\, 2^{-nH(P)} \\
\therefore |T(P)| &\le 2^{nH(P)}
\end{aligned}$$

□

Example 6.1.4.

Theorem 6.1.4. ***Probability of type class:***
For any $P \in \mathcal{P}_n$*, and any distribution* Q*:*

$$\frac{1}{(n+1)^{|\mathcal{X}|}} 2^{-nD[P\|Q]} \le Q[\underline{x}_n \in T(P)] \le 2^{-nD[P\|Q]}$$

Proof. Theorem 6.1.2 multiplies Theorem 6.1.3. □

6.2 Law of large numbers

For $X_1, \dots, X_n \sim^{i.i.d} Q$

- $\frac{1}{n} \sum\limits_{i=1}^{n} X_i \xrightarrow{p.} \underset{X \sim Q}{\mathbf{E}} X$
- $\frac{1}{n} \sum\limits_{i=1}^{n} f(X_i) \xrightarrow{p.} \underset{X \sim Q}{\mathbf{E}} f(X)$
- $P_x(X = a) = \frac{n_a}{n} \overset{n \to \infty}{\to} Q(a)$

Theorem 6.2.1. *Formally, for any* $\epsilon > 0$*:* $\lim\limits_{n \to \infty} PrD(P_x \parallel Q) > \epsilon = 0$

Proof.

$$PrD(P_x \parallel Q) > \epsilon = \sum_{P: D(P \| Q) > \epsilon} Q(\underline{\mathrm{x}}_n \in P) \leq 2^{-nD[P \| Q]}$$
$$\leq (n+1)^{|\mathcal{X}|} 2^{-n\epsilon} = 2^{-n(\epsilon - \frac{|\mathcal{X}|}{n+1})} \to 0$$

□

6.3 Universal source coding

Definition 6.3.1. ***Universal source coding:***

1) A fix-rate block code of rate R *for a source* $X_1, \dots, X_n \overset{i.i.d.}{\sim} Q$*:*

$$f_n : \quad \mathcal{X}^n \longrightarrow \{1, 2, \dots, 2^{-nR}\} \quad \textit{encode}$$
$$\phi_n : \quad \{1, 2, \dots, 2^{-nR}\} \longrightarrow \mathcal{X}^n \quad \textit{decode}$$

2) R *is called the rate of the code.*

3) The prob of error for the code is defined as:

$$P_e^(n) = Q^n(\phi_n(f_n(x^n)) \neq x^n)$$

Theorem 6.3.1. *There exist a sequence of* $(2^{-nR}, n)$ *universal source code, such that for every source* Q*, satisfying* $H(Q) < R$*,* $P_e^{(n)} \to 0$*.*

Proof. Let $R_n = R - |\mathcal{X}| \frac{\log(n+1)}{n}$

Consoder the set of sequence:

$$A_n = \{x^n \in \mathcal{X}^n | H(P_x) \leq R_n\}$$

$$|A_n| = \sum_{P: H(P) \leq R_n} |T(P)| \leq \sum_{P: H(P) \leq R_n} 2^{nR_n}$$

$$\leq (n+1)^{|\mathcal{X}|} 2^{nR_n} = 2^{|\mathcal{X}|\log(n+1) + nR - n|\mathcal{X}|\frac{\log(n+1)}{n}}$$
$$= 2^{nR}$$

Any sequence $x^n \notin A_n$ will result in an error, hence the probability of error is:

$$P_e^{(n)} = \sum_{P:H(P>R_n)} Q^n(T(P)) \leq (n+1)^{|\mathcal{X}|} \max_{P:H(P)>R_n} Q^n(T(P))$$

Due to the Theorem 6.1.4:$Q^n(T(P)) \leq 2^{-nD(P\|Q)}$

$$P_e^{(n)} \leq (n+1)^{|\mathcal{X}|} 2^{-n \min_{P:H(P)>R_n} D(P\|Q)}$$
$$\lim_{n\to\infty} (n+1)^{|\mathcal{X}|} 2^{-n \min_{P:H(P)>R_n} D(P\|Q)} = 0$$
$$\therefore P_e^{(n)} \to 0$$

□

6.3.1 Fisher Information and Cramér-Rao Lower Bound

For $\underline{\mathrm{X}}_n = X_1, X_2, \ldots, X_n \overset{i.i.d}{\sim} P_\theta$:

$$\{\underline{\mathrm{X}}_n\} \overset{estimate}{\longrightarrow} parameter : \theta$$

The error of the estimate T is:

$$\mathbf{E}[T(\underline{\mathrm{X}}_n) - \theta]^2 \qquad MSE$$

$$\mathbf{E}[T(\underline{\mathrm{X}}_n) - \theta] = 0 \qquad unbias$$

Theorem 6.3.2. ***Cramér-Rao Lower Bound:***
The MSE of any unbias estimator $T(X)$ of the parameter θ is lower bounded by:

$$var(T) \geq \frac{1}{J(\theta)} \qquad where\ J(\theta) \overset{def}{=} \mathbf{E}_X[\frac{\partial}{\partial\theta} \ln f(X,\theta)]^2$$

Here, $f(X,\theta)$ is the probability density function of X, $J(\theta)$ is called the Fisher information.

Proof.

$$v \overset{def}{=} \frac{\partial \ln f(X,\theta)}{\partial\theta} = \frac{\frac{\partial}{\partial\theta} f(X,\theta)}{f(X,\theta)}$$
$$\mathbf{E}[v] = \int v f(X,\theta) dX = \int \frac{\partial}{\partial\theta} f(X,\theta) dX$$
$$= \frac{\partial}{\partial\theta} \int f(X,\theta) dX = \frac{\partial}{\partial\theta} 1 = 0$$
$$\therefore J(\theta) = \mathbf{E}_X[v^2]$$

Due to the Cauchy-Schwarz inequality:

$$
\begin{aligned}
[\mathbf{E}(v-\mathbf{E}v)(T-\mathbf{E}T)]^2 \leq \mathbf{E}(v-\mathbf{E}v)^2\mathbf{E}(T-\mathbf{E}T)^2 &= \mathbf{E}[v^2]var(T) \\
\Rightarrow [\mathbf{E}(vT)]^2 &\leq J(\theta)var(T) \\
\mathbf{E}(vT) = \int vTf(X,\theta)dX &= \int \frac{\partial}{\partial\theta}f(X,\theta)TdX \\
&= \frac{\partial}{\partial\theta}\int f(X,\theta)TdX = \frac{\partial}{\partial\theta}\mathbf{E}[T] = \frac{\partial}{\partial\theta}\theta = 1 \\
&\Rightarrow J(\theta)var(T) \geq 1 \Rightarrow var(T) \geq \frac{1}{J(\theta)}
\end{aligned}
$$

□

Example 6.3.1. *Let $X_1, X_2, \ldots, X_n \overset{i.i.d}{\sim} N(\theta, \sigma^2)$ with a known σ^2.*

$$
\begin{aligned}
&T_1 = \frac{1}{n}\sum_{i=1}^{n} X_i \quad T_2 = X_1 \quad f(X,\theta) = \frac{1}{\sqrt{2\pi}\sigma}e^{-\frac{(X-\theta)^2}{2\sigma^2}} \\
&\frac{\partial}{\partial\theta}\ln f(X,\theta) = \frac{\partial}{\partial\theta}[-\frac{(X-\theta)^2}{2\sigma^2} - \ln(\sqrt{2\pi}\sigma)] = -\frac{x-\theta}{\sigma^2} \\
&T_2 : MSE = \mathbf{E}(T_2-\theta)^2 = \mathbf{E}(X-\theta)^2 = \sigma^2 \\
&J(\theta) = \mathbf{E}(v^2) = \mathbf{E}(\frac{(X-\theta)^2}{\sigma^4}) = \frac{\sigma^2}{\sigma^4} = \frac{1}{\sigma^2}
\end{aligned}
$$

Here, T_2 is not an unbias estimator, but reaches the lower bound.

§ 7 Maximum Entropy Principle

For a r.v. X:

1. $\mu = \mathbf{E}X$;
2. $\sigma^2 = var(X) = \mathbf{E}(X-\mu)^2$;
3. $X \in \mathbf{R}/X \in \{0,1,2,\ldots\}$.

Objective: Given a set of constants, the aim to get the distribution via MEP.

Example 7.0.1.

$$\max_{p(x)} H[p(x)] \quad s.t. \begin{cases} \sum\limits_x r_j(x)p(x) = \mu_j \quad j = 1,2,\ldots,m \\ \sum\limits_x p(x) = 1 \\ p(x) \geq 0 \quad \forall x \in \mathcal{X} \end{cases}$$

$$L[\{p(x)\},\{\lambda_j\}] = -\sum_x p(x)\log p(x) + \sum_j \lambda_j(\sum_x r_j(x)p(x) - \mu_j) + \lambda_0(\sum_x p(x) - 1)$$

$$\frac{\partial L}{\partial p(x_i)} = -(\log p(x_i) + 1) + \sum_j \lambda_j r_j(x_i) + \lambda_0 = 0 \Rightarrow p(x_i) = e^{-1+\lambda_0+\sum\limits_j \lambda_j r_j(x_i)}$$

$$= \frac{1}{Z}e^{\sum\limits_j \lambda_j r_j(x_i)} \qquad Z = e^{\lambda_0 - 1} \quad p_i \textit{ is called Bolzmann distribution}$$

$$\frac{\partial L}{\partial \lambda_0} = \sum_x p(x) - 1 = 0 \Rightarrow Z = \sum_x e^{\sum\limits_j \lambda_j r_j(x)}$$

$$\frac{\partial L}{\partial \lambda_j} = \sum_x r_j(x)p(x) - \mu_j = 0 \Rightarrow \lambda_j$$

1. $\mathbf{E}X = 0 \quad var(X) = \sigma^2 \quad X \in \mathbf{R}$

   $p(x) = \frac{1}{Z}e^{\lambda_1 x^2 + \lambda_2 x} = \frac{1}{\sqrt{2\pi}\sigma}e^{-\frac{x^2}{2\sigma^2}}$

2. $\mathbf{E}X = \mu \quad X \in [0,+\infty)$

   $p(x) = \frac{1}{Z}e^{-|\lambda_1|x}$

3. $\mathbf{E}X = \mu \quad X \in \mathbf{R}$

   $p(x) = unknown$

4. $X \in [a,b]$

   $p(x) = \frac{1}{b-a}$

Theorem 7.0.1. *Let* $f^*(x) = e^{\lambda_0 + \sum\limits_j \lambda_j r_j(x)}$, $\lambda_0, \lambda_1 \ldots, \lambda_m$ *are chosen s.t.* $\begin{cases} \int f(x)dx = 1 \\ \int r_j(x)f(x)dx = \alpha_j \quad j = 1,2,\ldots,m \\ f(x) \geq 0 \end{cases}$. f^* *uniquely maximize the entropy* $H[f]$ *over all possible* f *satisfies the constraints.*

Proof. For any $g(x)$ satisfies the constraints, we have:

$$
\begin{aligned}
H[g] - H[f^*] &= -\int g(x) \log g(x) dx + \int f^*(x) \log f^*(x) dx \\
&= -\int g(x) \log \frac{g(x)}{f^*(x)} dx - \int g(x) \log f^*(x) dx + \int f^*(x) \log f^*(x) dx \\
&= -D[g \parallel f^*] - \int g(x) \log f^*(x) dx + \int f^*(x) \log f^*(x) dx \\
\int f^*(x) \log f^*(x) dx &= \int f^*(x) [\lambda_0 + \sum_j \lambda_j r_j(x)] dx \\
&= \lambda_0 + \sum_j \lambda_j \alpha_j \\
\int g(x) \log f^*(x) dx &= \int g(x) [\lambda_0 + \sum_j \lambda_j r_j(x)] dx \\
&= \lambda_0 + \sum_j \lambda_j \alpha_j \\
\therefore H[g] - H[f^*] &= -D[g \parallel f^*] \leq 0 \\
\therefore H[f^*] &\geq H[g] \quad \forall g \text{ satisfies the constraints} \\
\text{i.i.f } g &= f^*, H[g] = H[f^*]
\end{aligned}
$$

$\square$

§ 8 Channel Coding

$$\underset{message}{W} \xrightarrow[f(W)]{encoder} \underline{X}^n \xrightarrow[P(\underline{Y}^n|\underline{X}^n)]{channel} \underline{Y}^n \xrightarrow[g(\underline{Y}^n)]{decoder} \underset{\text{estimate of message}}{\hat{W}}$$

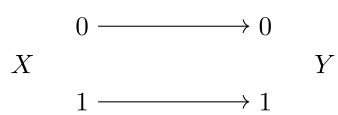
8.1 Information Channel Capacity

Definition 8.1.1. ***Information channel capacity:***

$$C \overset{def}{=} \max_{p(x)} I[X;Y] = \max_{p(x)} \sum p(x,y) \log \frac{p(x,y)}{p(x)p(y)} = \max_{p(x)} \sum p(x)p(y|x) \log \frac{p(y|x)}{p(y)}$$

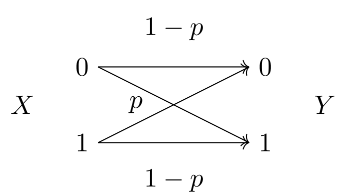
Here, $p(y|x)$ is given by the channel, $p(y) = \sum p(x)p(y|x)$.Hence, the only variable is $p(x)$, which is given by the encoder.

Example 8.1.1. ***Noiseless channel:***



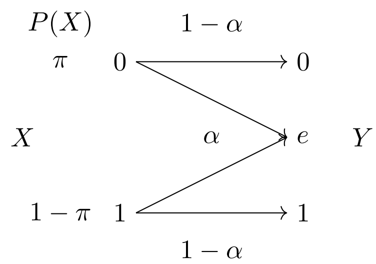
$$\begin{aligned} C &= \max_{p(x)} I(X;Y) = \max_{p(x)} H(X) - H(X|Y) \\ &= \max_{p(x)} H(X) = 1 \end{aligned}$$

Example 8.1.2. ***Binary symetric channel:***



$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) = H(Y) - \sum_x p(X=x)H(Y|X=x) \\ &= H(Y) - \sum_x p(X=x)h(p) \qquad h(p) = -p\log p - (1-p)\log(1-p) \\ &= H(Y) - h(p) \\ C &= \max_{p(x)} I(X;Y) = \max_{p(x)} H(Y) - h(p) = 1 - h(p) \end{aligned}$$

Example 8.1.3. ***Binary erasure channel:***



If follow the method of Exmaple 8.1.2:

$$I(X;Y) = H(Y) - h(\alpha) \qquad C = 1 - h(\alpha)$$

Set $E = even(Y = e)$

$$\begin{aligned} H(Y) &= H(Y,E) - H(E|Y) \quad H(E|Y) = 0 \\ &= H(E) + H(Y|E) \\ &= h(\alpha) + \sum_e P(E=e)H(Y|E=e) \\ &= h(\alpha) + (1-\alpha)h(\pi) \\ \therefore \quad C &= \max H(Y) - h(\alpha) = (1-\alpha)\max_\pi h(\pi) \end{aligned}$$

8.2 Channel Code

1. An (M, n) code for the channel $\{X, Y, P(Y|X)\}$ includes:
   (a) An index set $\{1, 2, \ldots, M\}$
   (b) An encoder: $\{1, 2, \ldots, M\} \to \underline{X}^n, X \in \{0, 1\}$
   (c) A decoder: $\underline{Y}^n \to \{1, 2, \ldots, M\}$
2. The rate of a code (M, n) is $R = \frac{\log_2 M}{n}$, for a no-error transmission:

$$R \leq C$$

   Here, C is the channel capacity.

8.3 Hamming Code

Set a matrix H as follows:

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

For this matrix, the Null space(kernel) is $Null(H)$, the $Rank(H) = 3$

For all $x \in Null(H)$, we have:

$$Hx = 0 \qquad |Null(H)| = 2^4 = 16$$

Now we can encode a message using the $x \in Null(H)$, it is easy to find that any two different codes $x_1, x_2 \in Null(H)$ satisfy:

$$d(x_1, x_2) = |x_1 - x_2| \geq 3$$

So when we transmit a code $x \in Null(H)$ with one bit error, we have:

$$x \to x + e = y \qquad e = \begin{bmatrix} 0 \\ \dots \\ 0 \\ 1 \\ 0 \\ \dots \\ 0 \end{bmatrix}$$

To find the index of the error bit, we can use the following method:

$$Hy = Hx + He = He$$

The index of the error bit is the index of the column in H with the same value as He.

In this example, we can find the rate of the code is:

$$R = \frac{\log_2 2^4}{7} = \frac{4}{7}$$

8.4 Joint Typical Set and Joint AEP

Definition 8.4.1. ***Joint typical set:***

$$A_\epsilon^n = \{(\underline{X}^n, \underline{Y}^n) | \begin{cases} \left|-\frac{1}{n}\log P(\underline{X}^n) - H(X)\right| < \epsilon \\ \left|-\frac{1}{n}\log P(\underline{Y}^n) - H(Y)\right| < \epsilon \\ \left|-\frac{1}{n}\log P(\underline{X}^n, \underline{Y}^n) - H(X,Y)\right| < \epsilon \end{cases} \}$$

1. $|A_\epsilon^n| = 2^{n(H(X,Y)+\epsilon)}$;
2. $P(A_\epsilon^n) \to 1$, as $n \to \infty$;
3. If $\underline{X}^n, \underline{Y}^n \sim P(\underline{X}^n)P(\underline{Y}^n)$, which means $\underline{X}^n \perp \underline{Y}^n$, then:

$$P(A_\epsilon^n) \leq 2^{-n(I(X;Y)-3\epsilon)}$$

Proof.

$$\begin{aligned}
P[(\underline{X}^n, \underline{Y}^n) \in A_\epsilon^n] &= \sum_{(\underline{X}^n, \underline{Y}^n) \in A_\epsilon^n} P(\underline{x}^n) P(\underline{y}^n) \\
&\leq \sum_{(\underline{X}^n, \underline{Y}^n) \in A_\epsilon^n} 2^{-n(H(X)+\epsilon)} 2^{-n(H(Y)+\epsilon)} \\
&\leq |A_\epsilon^n| \, 2^{-n(H(X)+H(Y)+2\epsilon)} \\
&= 2^{n(H(X,Y)+\epsilon)} 2^{-n(H(X)+H(Y)+2\epsilon)} \\
&= 2^{-n(I(X;Y)-3\epsilon)}
\end{aligned}$$

□

8.5 Channel Coding Theorem

Definition 8.5.1. ***Decode Error:***
Here, we have three types of decode error:

1. $\lambda_i = Pr\{g(Y^n) \neq i | X^n(i)\}$;
2. $\bar{\lambda}_i = \frac{1}{m} \sum_{i=1}^{m} \lambda_i$;
3. $\lambda_{max} = \max\{\lambda_i\}$

Theorem 8.5.1. ***Channel coding theorem:***

1. *For every rate $R < C$, there exists a sequence $(M = 2^{nR}, n)$ code with $\lambda_{max}^{(n)} \to 0$.*
2. *Conversely, any sequence $(2^{nR}, n)$ code with $\lambda_{max}^{(n)} \to 0$, must have $R \leq C$.*

Proof.

1. $W \in \{1, 2, \ldots, M = 2^{nR}\} \sim$ uniform distribution.
2. Channel Code: $C : \{1, 2, \ldots, M\} \to \underline{X}^n = (x_1, x_2, \ldots, x_n), x_i \in \{0, 1\}$

$$C = \begin{bmatrix} X_1(1) & \ldots & X_n(1) \\ \ldots & & \ldots \\ X_1(M) & \ldots & X_n(M) \end{bmatrix}_{M \times n}$$

3. Channel: $P(Y^n | X^n(w)) = \prod_{i=1}^{n} P(y_i | x_i(w))$ (Memoryless)
4. Decode(Jointly typical decoder):

   From recieved $\underline{Y}^n$, estimate $\hat{W}(\underline{Y}^n)$ based on the joint typical set $A_\epsilon^{(n)}$:

$$\hat{W}(\underline{Y}^n) = \begin{cases} \hat{w} & \text{if } \exists \text{ unique } \hat{w} \text{ s.t. } (X^n(\hat{w}), Y^n) \in A_\epsilon^{(n)} \\ 0 & otherwise \end{cases}$$

5. The probability of decode error is:
   - $P_e^n(C) = Pr\{W \neq \hat{W}(\underline{Y}^n)\}$ for any given random code C.
   - $\bar{P}_e^n = \sum_C Pr(C)P_e^n(C)$

We will prove if $R < I(X;Y) - 3\epsilon$, then $\bar{P}_e^n < 2\epsilon$.If $R > C - \epsilon$ holds, then we have those corollaries:

1. Choose $P(X)$ to maximize $I(X;Y)$, then we have $R < C - 2\epsilon$;
2. There exists one code C^* s.t. $\bar{P}_e^n(C^*) = \frac{1}{2^{nR}} \sum \lambda_i < 2\epsilon$;
3. There are at least $\frac{2^{nR}}{2}$ codes with decode error $\lambda_i \leq 4\epsilon$.

Due to corollary 3, if we just use the $\frac{2^{nR}}{2}$ codes, the code rate is $R - \frac{1}{n} \to R$, and the maximum decode error is $\lambda_{max} \leq 4\epsilon$.

WLOG, we just discuss the error rate of code "1" in all random codes:

$$\begin{aligned}
E_i &= \{(\underline{X}^n(i), \underline{Y}^n) \in A_\epsilon^{(n)} | W = i\} \\
P_{e,1} &= \sum_C Pr(C)\lambda_1 = Pr[E_1^C \cup E_2 \cup \ldots \cup E_M] \\
&\leq Pr[E_1^C] + Pr[E_2 \cup \ldots \cup E_M]
\end{aligned}$$

We have two results:

1. $Pr[E_1^C] \leq \epsilon$ due to AEP Theorem;
2. $P(\underline{X}^n(i), \underline{Y}^n) = P(\underline{X}^n(i))P(\underline{Y}^n), i \neq 1$ due to the random code C.

If the recieved $\underline{Y}^n$ is not transmitted from $\underline{X}^n(1)$, then $\underline{Y}^n \perp \underline{X}^n(1)$.

$$\begin{aligned}
Pr[E_2 \cup \ldots \cup E_M] &\leq \epsilon + 2^{-n(I(X;Y)-3\epsilon)} P(\underline{X}^n(2), \underline{Y}^n(\underline{X}^n(1))) \\
&\leq 2^{-n(I(X;Y)-3\epsilon)} P(\underline{X}^n(2)) P(\underline{Y}^n(\underline{X}^n(1)))
\end{aligned}$$

There are 2^{nR} codes, the average error rate is:

$$Pr[E_1^C] + 2^{nR} Pr[E_2 \cup \ldots \cup E_M] \leq \epsilon + 2^{-n(I(X;Y)-3\epsilon-R)} P(\underline{X}^n(2)) P(\underline{Y}^n(\underline{X}^n(1)))$$

If $R < I(X;Y) - 3\epsilon$, then we have:

$$2^{nR} Pr[E_2 \cup \ldots \cup E_M] \to 0, n \to \infty$$

$$\therefore \quad P_{e,1} \leq \epsilon$$

□

§ 9 Differential Entropy

9.1 Definition

1. continuous random variable X;
2. C.D.F : $F(x) = Pr(X \leq x)$
3. P.D.F : $f(x) = \frac{dF(x)}{dx}$

Definition 9.1.1. ***Differential entropy:***

$$h(X) = -\int f(x) \log f(x) dx = \mathbf{E} \log \frac{1}{f(x)}$$

Example 9.1.1. $X \sim U[0, a] \qquad f(x) = \frac{1}{a}$

$$h(X) = -\int_0^a \frac{1}{a} \log \frac{1}{a} dx = \log a$$

If $a < 1$, then $h(X) < 0$.

- $Y = X + C, h(Y) = h(X + C) = h(X), C = const$
- $h(aX) = h(X) + \log |a|, a = const$

9.2 Mutual Information, Joint Entropy and Conditional Entropy

- $I(X; Y) = \mathbf{E} \log \frac{f(X)f(Y)}{f(X,Y)}$;
- $h(X, Y) = \mathbf{E} \log \frac{1}{f(X,Y)}$;
- $h(X|Y) = \mathbf{E} \log \frac{1}{f(X|Y)}$.

9.3 K-L Divergence

$$X \sim f \qquad X \sim g$$

$$D[f \parallel g] = \mathop{\mathbf{E}}_{f(x)} \log \frac{f(x)}{g(x)} = \int f(x) \log \frac{f(x)}{g(x)} dx$$

Theorem 9.3.1.

$$D[f \parallel g] \geq 0$$

Proof.

$$
\begin{aligned}
-D[f \parallel g] &= -\int f(x) \log \frac{f(x)}{g(x)} dx \\
&= \int f(x) \log \frac{g(x)}{f(x)} dx \\
&\leq \log\left(\mathop{\mathbf{E}}_{x \sim f(x)} \frac{g(x)}{f(x)} \right) \\
&= \log \int g(x) dx = \log 1 = 0 \\
\therefore \quad & D[f \parallel g] \geq 0
\end{aligned}
$$

□