Shannon’s Theory

Dr. Odelu Vanga
Computer Science and Engineering
Indian Institute of Information Technology Sri City
odelu.vanga@iiits.in

Conditional Entropy:

Suppose X & Y are two r.v.

Then for any fixed y of Y, we get a conditional probability distribution on X,

$$H(X|y) = -\sum_{x} \Pr[x|y] \log \Pr[x|y].$$

$$\underline{H(X|Y)} = -\sum_{y} \sum_{x} \Pr[y] \Pr[x|y] \log_2 \Pr[x|y].$$

<u>Note</u>: Measures the average amount of information about X that is revealed by Y.

Ex: Consider cryptosystem

$\mathcal{P} = \{a, b, c\}$

$\mathcal{K} = \{k_1, k_2, k_3\}$

$\mathcal{C} = \{1, 2, 3, 4\}$

Encryption

$E_k(x)$	a	b	c
k_1	1	2	3
k_2	2	3	4
k_3	3	4	1

$Pr[a] = 1/2$, $Pr[b] = 1/3$

$Pr[c] = 1/6$

$Pr[k_1] = Pr[k_2] = Pr[k_3] = 1/3$.

Q: $H(\mathcal{P})$

$H(\mathcal{K})$

$H(\mathcal{C})$

$H(\mathcal{K} | C)$ - Key Equivocation

Sol:

$$H(X) = -\sum_{x} pr[x] \log_2 pr[x]$$

$$H(P) = -\left(pr[a] \log_2 pr[a] + pr[b] \log_2 pr[b] + pr[c] \log_2 pr[c] \right)$$

$$= -\left(\frac{1}{2} \log \frac{1}{2} + \frac{1}{3} \log \frac{1}{3} + \frac{1}{6} \log \frac{1}{6} \right)$$

$$= \frac{1}{2} \log 2 + \frac{1}{3} \log 3 + \frac{1}{6} \log 6$$

$$= 1.45915$$

$$H(\mathcal{K}) = -\left(pr[k_1] \log pr[k_1] + pr[k_2] \log pr[k_2] + pr[k_3] \log pr[k_3] \right)$$

$$= -\left(\frac{1}{3} \log \frac{1}{3} + \frac{1}{3} \log \frac{1}{3} + \frac{1}{3} \log \frac{1}{3} \right)$$

$$= \log 3$$

$$= 1.58496$$

$$H(C) = -\sum_{y \in C} pr[y] \log pr[y]$$

we have to find $pr[1]$, $pr[2]$, $pr[3]$, $pr[4]$

$$\boxed{pr[y] = \sum_{\{k \,:\, y \in c(k)\}} pr[k]\, pr[x = D_k(y)]}$$

$$pr[2] = 5/18$$

$$pr[3] = 1/3$$

$$pr[4] = 1/6$$

$$H(C) =$$

$$pr[1] = \sum_{\{k \,:\, 1 \in C(k)\}} pr[k] \cdot pr[x = D_k(1)]$$

$$c(k_1) = \{1, 2, 3\}$$

$$c(k_2) = \{2, 3, 4\}$$

$$c(k_3) = \{3, 4, 1\}$$

$$pr[1] = pr[k_1]\, pr[x = a] + pr[k_3]\, pr[c]$$

$$= \frac{1}{3} \times \frac{1}{2} + \frac{1}{3} \times \frac{1}{6}$$

$$= \frac{2}{9}$$

$$H(e) = -\Big(pr[1] \log pr[1] + pr[2] \log pr[2] + pr[3] \log pr[3] + pr(4) \log pr[4] \Big)$$

$$= -\left(\frac{2}{9} \log \frac{2}{9} + \frac{5}{18} \log 5/18 + \frac{1}{3} \log \frac{1}{3} + \frac{1}{6} \log \frac{1}{6} \right)$$

$$= \frac{2}{9} \log \frac{9}{2} + \frac{5}{18} \log \frac{18}{5} + \frac{1}{3} \log 3 + \frac{1}{6} \log 6$$

$$= 1.95469$$

$$H(\mathcal{K}|\mathcal{C}) = -\sum_{y}\sum_{k} pr[y]\, pr[k|y] \log pr[k|y]$$

$$pr[k|y] = \frac{pr[k]\, pr[y|k]}{pr[y]}$$

$$pr[k_1|1] = \frac{pr[k_1]\, pr[1|k_1]}{pr[1]}$$

$$pr[\mathcal{Y}=y \mid \mathcal{K}=k]$$

$$= pr[E_k(x)=y \mid \mathcal{K}=k]$$

$$= pr[E_k(x)=y]$$

$$= pr[x = D_k(y)]$$

$$(y, k) \to x$$

$$E_k(x)=y$$

$$x = D_k(y)$$

State: For given y and K in any cryptosystem,

$\exists$ only one x with condition $x = D_K(y)$.

proof: Suppose $\exists$ $x_0 \neq x_1$ $\ni$

$$y = E_K(x_0), \quad \underline{y = E_K(x_1)}$$

$$x_0 = D_K(E_K(x_0)) = D_K(y) = D_K(E_K(x_1)) = x_1$$

$$\Rightarrow x_0 = x_1$$

$$\rightarrow \leftarrow$$

our assumption wrong.

$$\therefore x_0 = x_1$$