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,

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

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

Note: 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: $H(\mathcal{P})$ ✓

$H(\mathcal{K})$ ✓

$H(\mathcal{C})$ ✓

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

$$\boxed{Pr[Y = y \mid K = k] = Pr[x = D_k(y)]}$$

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

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

y	1	2	3	4
$Pr[y]$	$2/9$	$5/8$	$1/3$	$1/6$

$$Pr[k_1|1] = \frac{Pr[k_1]\,Pr[1|k_1]}{Pr[1]} = \frac{\frac{1}{3}\cdot\frac{1}{2}}{2/9} = \frac{3}{4}$$

$$Pr[k_1|2] =$$

$$Pr[k_1|3] =$$

$$Pr[k_1|4] =$$

$Pr[k|y]$

K \ y	1	2	3	4
k_1	$3/4$	$2/5$	$1/6$	0
k_2	0	$3/5$	$1/3$	$1/3$
k_3	$1/4$	0	$1/2$	$2/3$

$$\boxed{H(K|C) = 1.08942}$$

$$H(K|C) = -\sum_y \sum_k Pr[y]\,Pr[k|y] \log Pr[k|y]$$

$$\Rightarrow \boxed{H(K|C) = H(K) + H(P) - H(C)}$$

Ex:

$\mathcal{P} = \{a, b\}$ $Pr[a] = 1/4$, $Pr[b] = 3/4$

$\mathcal{K} = \{k_1, k_2, k_3\}$ $Pr[k_1] = 1/2$, $Pr[k_2] = Pr[k_3] = 1/4$

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

	a	b
k_1	1	2
k_2	2	3
k_3	3	4

Q) $H(\mathcal{K} \mid \mathcal{C}) = ?$

Home work

practice ?!