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 detoids an

m×1

$$H(x|y) = -\frac{2}{3} \sum_{x} Pr[y] Pr[x|y] \log_2 Pr[x|y].$$

Note: Measures the average amount
of information and x that is revealed by Y.

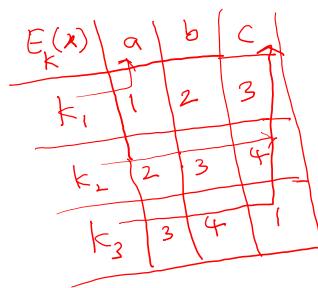
Ex: Consider cryptosyslain

P={a,b,c}

$$P = \{a_1b_1c_5$$

 $K = \{k_1, k_2, k_3\}$
 $E = \{1, 2, 3, 4\}$

Encoyption



pr[a] = ½, pr[b] = 3

pr(c) = 1/6

pr[k] = pr[k] = Pr[k]=3=3

$$H(x) = - \sum_{\alpha} P(\alpha) \log_{\alpha} P(\alpha)$$

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

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

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

We have to find pr[1], pr[2], pr[3], pr[4]

$$Pr(y) = \sum Pr(k) Pr(x = D_k(y))$$

$$\{k : y \in c(k)\}$$

$$PY(2) = \frac{5}{18}$$
 $PY(3) = \frac{1}{3}$
 $PY(4) = \frac{1}{6}$
 $P(4) = \frac{1}{6}$

$$P^{*}[1] = S P^{*}[1] \cdot P^{*}[x]$$

$$(k: 1 \in C(k))$$

$$C(k) = \{1, 2, 3\}$$

$$C(k_{2}) = \{2, 3, 4\}$$

$$C(k_{3}) = \{3, 4, 1\}$$

$$P^{*}[1] = P^{*}[k_{1}] P^{*}[x = q]$$

$$+ P^{*}[k_{2}] P^{*}[c]$$

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

$$= \frac{2}{q}$$

$$H(e) = -\left(\frac{pr(1) \log pr(1)}{pr(2) \log pr(2)} + \frac{pr(2) \log pr(2)}{pr(4)} \right)$$

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

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

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

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

$$= 1.95469$$

$$H(x|z) = -\sum_{y} \sum_{k} pr(y) pr(k|y) \log pr(k|y)$$

$$(pr(y) = \sum_{y} \sum_{k} pr(y) pr(y) \log pr(k|y)$$

$$Pr(k|y) = \frac{pr(k) pr(y|k)}{pr(k)}$$

$$Pr(k|y) = \frac{pr(k) pr(y|k)}{pr(y)}$$

$$Pr(Y=y|X=k)$$

$$= Pr(E_k(x)=y|X=k)$$

$$= Pr(X=D_k(y))$$

$$= Pr(X=D_k(y))$$

$$= D_k(y)$$

State: For giveer y and k en any cryptosystem, I only one or with condition $x = D_k(y)$. Suppose 3 2, +2, 7 $y = E_k(x_0), y = E_k(n_0)$ $\mathcal{X}_{o} = \mathcal{D}_{k}(E_{k}(x_{o})) = \mathcal{D}_{k}(y) = \mathcal{D}_{k}(E_{k}(x_{o})) = \mathcal{X}_{l}$ ⇒ 20 - 21 our assumpt an word. :. x = 1