$$H(X) = -\sum_{i=1}^{K} p_i \log p_i = -\sum_{x\in\mathcal{X}} p(x) \log p(x)$$

X è una v.a. su un insieme (finito) $\mathcal{X}$ di simboli, con d.d.p. $p = (p_1, p_2, \dots, p_K) \in \mathbb{R}^K$

$(K = |\mathcal{X}|)$

$$H_b(X) = -\sum_i p_i \log_b p_i \qquad \log_b z = \frac{\log_a z}{\log_a b} \Rightarrow H_b(X) = \frac{H_a(X)}{\log_a b}$$

$H(X)$ è una misura dell'incertezza residua (informazione mancante) nella v.a. X

Esempio. $\mathcal{X} = \{1, 2, \dots, 32\}$ e $p = \left(\frac{1}{32}, \frac{1}{32}, \dots, \frac{1}{32}\right)$

Allora $H(X) = -\sum_{i=1}^{32} \frac{1}{32} \log \frac{1}{32} = +\sum_{i=1}^{32} \frac{1}{32} \overbrace{\log 32}^{=5} = 5$ bit

1 : 00000 32 : 11111

2 : 00001

- - - -

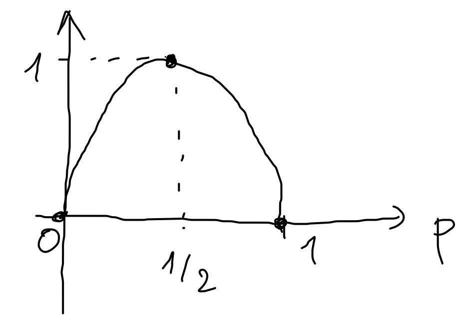
Se invece $\mathcal{X} = \{1, \dots, 30\}$?

$H(X) \simeq \underline{4.906}$

Esempio. $\mathcal{X} = \{0,1\}$ $\quad X = \begin{cases} 0 & \text{con prob. } p \\ 1 & \text{con prob. } 1-p \end{cases}$ (per qualche $\underline{p \in [0,1]}$)

$$H(X) = -p \log p - (1-p)\log(1-p) \triangleq h_2(p)$$ funzione entropia binaria

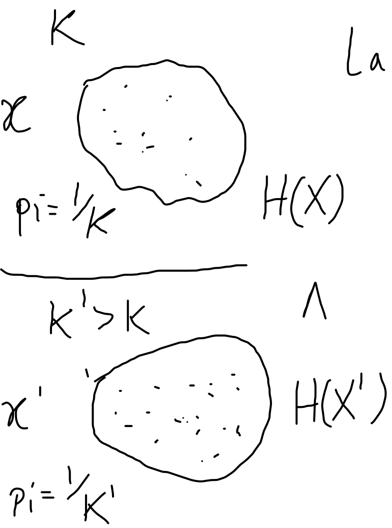
(≥ 0)



Se $p=0$: $-\cancel{0 \log 0} - \cancel{1 \log 1} = 0 = H(X)$

Se $p=1$: $H(X)=0$

Se $p=1/2$: $-\frac{1}{2}\log\frac{1}{2} - \frac{1}{2}\log\frac{1}{2} = \underline{1}$ bit



La formula per l'entropia si può derivare a partire da alcuni assiomi naturali:

→ ① Continuità : $H(X)$ deve essere $\underline{\text{continua}}$ nel vettore $p = (p_1, \dots, p_K)$

→ ② Monotonia : Se X e X' sono v.a. con distr. uniforme su $\mathcal{X}$, $\mathcal{X}'$ rispettivam. e $|\mathcal{X}| < |\mathcal{X}'|$, allora $H(X) < H(X')$.

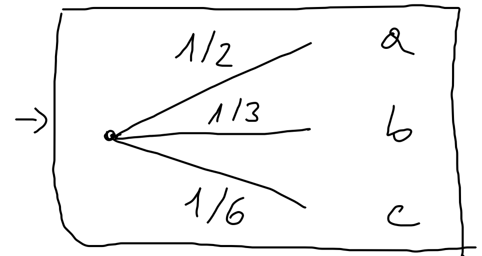
→ ③ Diramazione

③ Diramazione

$H(X)$ posso scriverla anche come $H(p_X)$

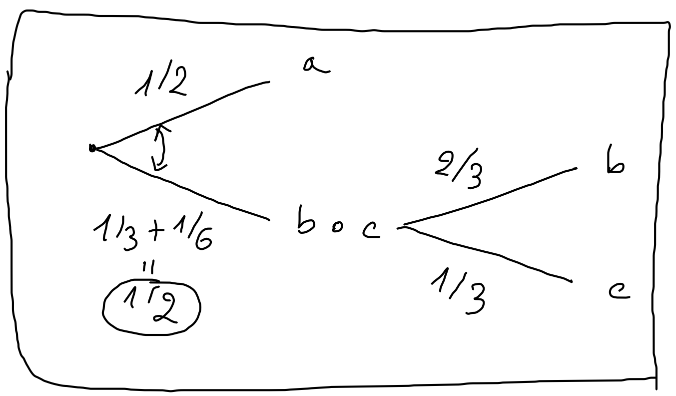
x_i	a	b	c
p_i	$1/2$	$1/3$	$1/6$

$H(X)$



Esempio delle proprietà di diramazione

$$H\left(\left(\frac{1}{2}, \frac{1}{3}, \frac{1}{6}\right)\right) = H\left(\left(\frac{1}{2}, \frac{1}{2}\right)\right) + \frac{1}{2} H\left(\left(\frac{2}{3}, \frac{1}{3}\right)\right)$$



Si può dimostrare che l'unica funzione (a meno di un fattore costante) H che soddisfa gli assiomi ①, ②, ③ è proprio l'entropia di Shannon $H(X) = -\sum_i p_i \log p_i$

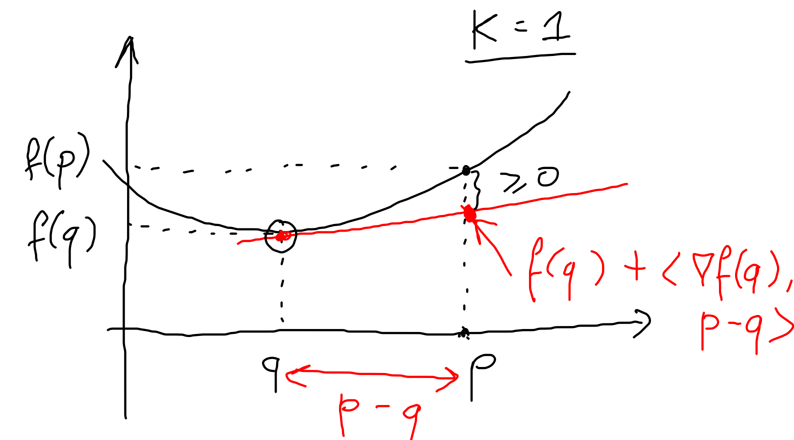
$$D(p\|q) \triangleq \sum_{i=1}^{K} p_i \log p_i/q_i$$

$$I(X;Y) \triangleq D(p_{XY} \| p_X \cdot p_Y) = \sum_{x\in\mathcal{X},\, y\in\mathcal{Y}} p(x,y) \log \frac{p(x,y)}{p(x)\,p(y)}$$

$$H(X) \triangleq I(X;X) = -\sum_i p_i \log p_i$$

$H(p)$

Divergenza di Bregman per una funzione f (derivabile) : $\mathbb{R}^K \to \mathbb{R}$



$$D_f(p\|q) = f(p) - f(q) - \langle \nabla f(q),\, p-q \rangle$$

$$f(p) \approx f(q) + f'(q)(p-q)$$

Quando f è convessa : $D_f(p\|q) \geq 0$ (per la convessità della f)

Scelgo :

$x \log x$

$$\boxed{f(x) = \sum_{i=1}^{K} x_i \log x_i}$$

(entropia negativa)

Scelgo:

$$\boxed{f(x) = \sum_{i=1}^{k} x_i \log x_i}$$

(convessa)

$$(x \log x)' = 1 + \log x$$

$$\nabla f(q) = (1+\log q_1, 1+\log q_2, \dots, 1+\log q_k)$$

$$\in \mathbb{R}^k$$

?

Allora $D_f(p\|q) = f(p) - f(q) - \langle \nabla f(q), p-q \rangle$

$$= \sum_i p_i \log p_i - \sum_i q_i \log q_i - \sum_i (1+\log q_i)(p_i - q_i)$$

$$= \sum_i p_i \log p_i - \cancel{\sum_i q_i \log q_i} - \underbrace{\cancel{\sum_i (p_i - q_i)}}_{0} - \sum_i (p_i - \cancel{q_i}) \log q_i$$

$$= \sum_i p_i \log p_i - \sum_i p_i \log q_i = \sum_i p_i \log \frac{p_i}{q_i} = D(p\|q).$$

Divergenza informazionale

Esercizio. Lancio una moneta (onesta) finché non esce testa

Sia X = numero di lanci $\in \{1, 2, 3, \ldots\}$

Quanto vale $H(X)$?

(Si usi il fatto $\sum_{n=0}^{\infty} n \cdot r^n = \dfrac{r}{(1-r)^2}$ per qualunque $r \in [0,1)$)

$$H(X) = - \sum_{x \in \mathcal{X}} p(x) \log p(x)$$

$$= - \sum_{k=1}^{\infty} \frac{1}{2^k} \log \frac{1}{2^k} =$$

$$= + \sum_{k=1}^{\infty} \frac{1}{2^k} \boxed{\log 2^k}$$

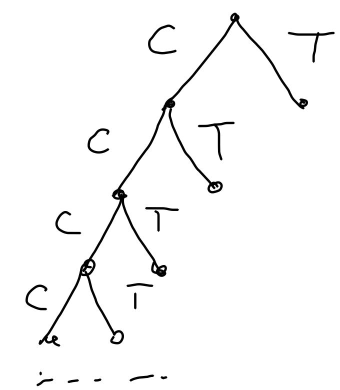
$= k$ (base 2)

$$= \sum_{k=1}^{\infty} k/2^k = \sum_{k=0}^{\infty} k/2^k$$

Uso con $r = 1/2$

$$= \frac{1/2}{(1 - 1/2)^2} = \frac{1/2}{(1/2)^2} = 2 \text{ bit.}$$

# lanci (x)	p(x)
1	1/2
2	1/4
3	1/8
$\vdots$	$\vdots$
k	$1/2^k$

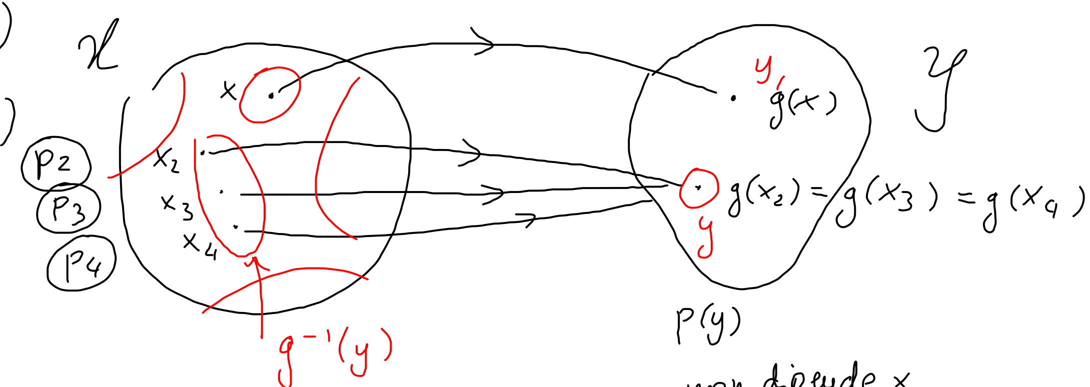


Es. Sia X una v.a. con valori su un sottoinsieme $\mathcal{X}$ finito di $\mathbb{R}$

Che relazione c'è tra $H(X)$ e $H(Y)$ quando:

→ (a) $Y = 2^X$? $H(Y) = H(X)$

→ (b) $Y = \cos(X)$? $H(Y) \le H(X)$



$y = g(x)$, $g : \mathcal{X} \to \mathcal{Y}$

$\mathcal{X} = \{x_1, \dots, x_k\}$

$$\Pr[Y=y] = p(y) = \sum_{x : g(x) = y} p(x) \implies \sum_{x : g(x)=y} p(x) \log p(x) \le \sum_{x : g(x) = y} p(x) \overbrace{\log p(y)}^{\text{non dipende } x} = (\log p(y)) \cdot p(y)$$

$$\implies H(X) = -\sum_{\underline{x \in \mathcal{X}}} p(x) \log p(x) = -\sum_{y \in \mathcal{Y}} \sum_{x : g(x) = y} p(x) \log p(x) \ge -\sum_{y \in \mathcal{Y}} p(y) \log p(y) = H(Y)$$

In generale (sia nel caso (a) che nel caso (b)) ho $H(Y) \le H(X)$; se g è biettiva tra $\mathcal{X}$ e $\mathcal{Y}$, allora $H(Y) = H(X)$.