(1) Mostrare che $H(Y|X)=0$,

$\iff$ per ogni x con $\underbrace{p(x)>0}$ esiste uno e un solo y tale che $p(y|x)=1$.

(Y è una funzione della X) (Generalizza: $H(Y)=0 \iff Y$ è costante)

Dim. $H(Y|X)=0 \iff \sum_{x\in\mathcal{X}} \underbrace{p(x)}_{\geq 0}\ \underbrace{H(Y|X=x)}_{\geq 0} = 0$

$\iff \forall x\in\mathcal{X}: \ p(x)\, H(Y|X=x)=0$

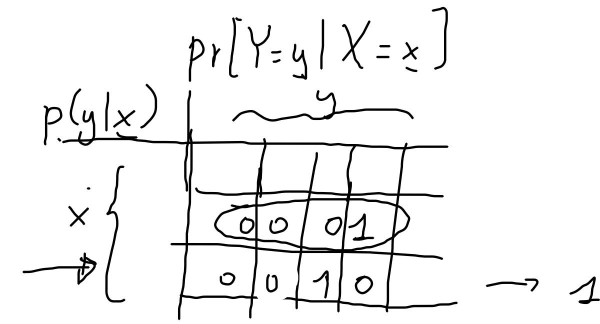
$\iff \forall x: p(x)>0 \quad H(Y|X=x)=0$

$\iff \forall x: p(x)>0 \quad -\sum_{y\in\mathcal{Y}} \underbrace{p(y|x)}_{\geq 0}\ \underbrace{\log p(y|x)}_{\leq 0} = 0$

$\iff \forall x: p(x)>0 \ \ \forall y\in\mathcal{Y} \quad p(y|x)=0 \ \vee \ p(y|x)=1$

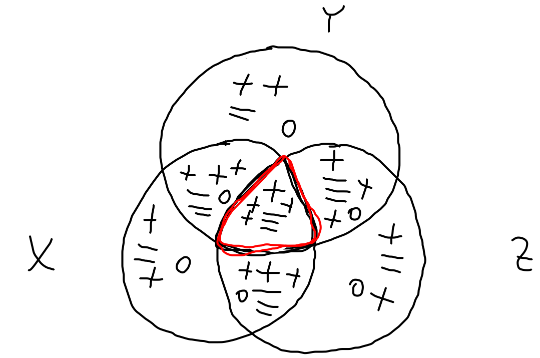
$\iff \forall x: p(x)>0 \quad \exists$ uno e un solo y : $p(y|x)=1$

(tutti gli altri y : $p(y|x)=0$)



② Mutua informaz. "multivariate"

(più di 2 v.a.)



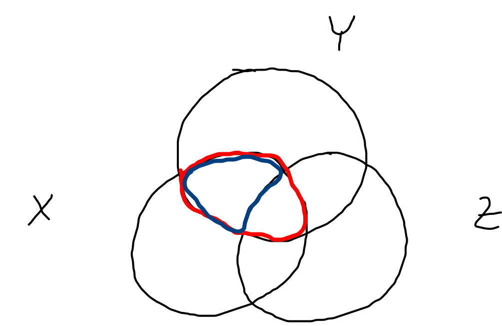
$$I(X;Y;Z) \overset{def}{=} H(X,Y,Z) - H(X,Y) - H(X,Z) - H(Y,Z) + H(X) + H(Y) + H(Z).$$

$$\downarrow$$

$$\mu(X \cap Y \cap Z) = \mu(X \cup Y \cup Z) - \mu(X \cup Y) - \mu(X \cup Z) - \mu(Y \cup Z) + \mu(X) + \mu(Y) + \mu(Z).$$

⚠ Attenzione $I(X;Y;Z)$ non è una divergenza informazionale!

Non è necessariamente positiva! $X \cap Y$ $(X \cap Y) \setminus Z$



Si può verificare: $I(X;Y;Z) = \underbrace{I(X;Y)}_{\geq 0} - \underbrace{I(X;Y|Z)}_{\geq 0}$

(2a) Esempio in cui $I(X;Y)=0$ e $I(X;Y|Z)>0$ $\quad (\Rightarrow I(X;Y;Z)<0)$

Siano X, Y, Z v.a. binarie con X e Y indipendenti e distribuite uniformemente

$\rightarrow I(X;Y)=0 \qquad \rightarrow \boxed{Z = X \oplus Y} \qquad (X+Y \bmod 2)$

$\hookrightarrow X = Z \ominus Y = Z \oplus Y \qquad (Z+Y \bmod 2)$

X è una funzione della coppia (Y,Z)

$$I(X;Y|Z) = H(X|Z) - \overbrace{H(X|Y,Z)}^{=0}$$

$$= \sum_{z\in Z} p(z)\, \underbrace{H(X|Z=z)}$$

P_{XY}	$Y=0$	$Y=1$
$X=0$	1/4	1/4
$X=1$	1/4	1/4

$Z=1$ (Pr. $1/2$)

$Z=0$ (Pr. $1/2$)

P_{XZ}	$Z=0$	$Z=1$
$X=0$	1/4	1/4
$X=1$	1/4	1/4
$p(z)$	1/2	1/2

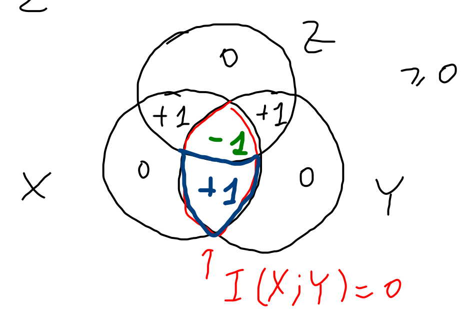
$p(x\|z)$, $P_{X\|Z=z}$	$Z=0$	$Z=1$
$X=0$	1/2	1/2
$X=1$	1/2	1/2

$$p(x|z) = \frac{p(x,z)}{p(z)}$$

$H(X|Z=0) = h(1/2) = 1$

$H(X|Z=1) = 1 \quad \longrightarrow \quad \boxed{I(X;Y|Z)} = \frac{1}{2}\cdot 1 + \frac{1}{2}\cdot 1 = 1 > 0$

$$\overset{|Z}{I(X;Y)} = \overset{|Z}{H(X)} - H(X|\overset{|Z}{Y})$$



2b Esempio in cui $I(X;Y) > 0$ e $I(X;Y|Z) = 0$

Consideriamo tre v.a. X, Y, Z in catena di Markov $X \to Z \to Y$ con X e Y non indipendenti.

$$\Downarrow \qquad\qquad \Downarrow$$

$$I(X;Y) > 0 \qquad\qquad I(X;Y|Z) = 0$$

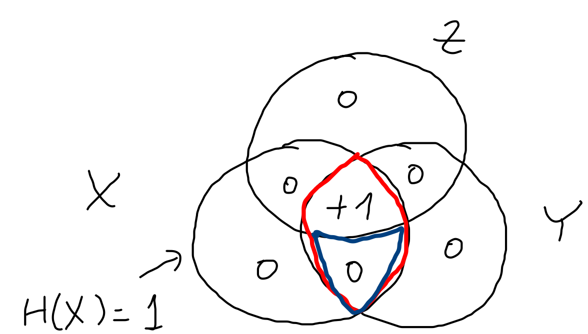
Concretamente, $X \in \{0,1\}$ con distribuz. uniforme

$$Z = X$$

$$Y = Z = X$$

$$I(X;Y) = I(X;X) = H(X) = 1 > 0$$

$$I(X;Y|Z) = \underbrace{H(X|Z) - H(X|Y,Z) = 0}_{\text{per Markovianità}}$$



$I(X;Y)$

$I(X;Y|Z)$

$(X \cap Y) \setminus Z$

(3) Teorema della segretezza perfetta (Shannon 1949)

X, Y, Z v.a.

X : testo in chiaro

Y : testo cifrato

Z : chiave

Uno schema di cifratura desiderabile:

✓ - decifrabile : $\underline{H(X \mid Y, Z) = 0}$ (X è funz. della coppia (Y, Z))

✓ - a segretezza perfetta : $\underline{I(X ; Y) = 0}$

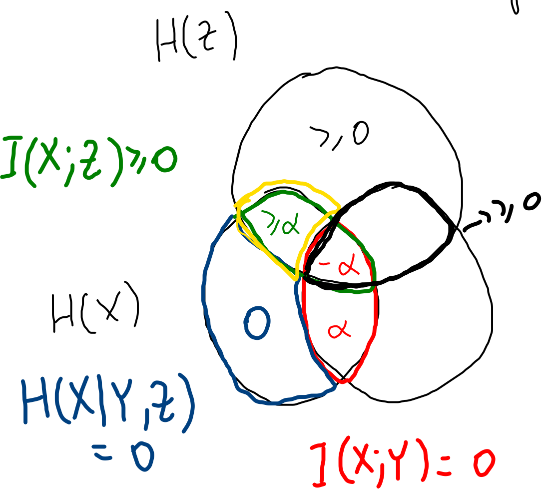
Teorema: Per ogni schema decifrabile e a segretezza perfetta: $\boxed{H(Z) \geq H(X)}$.

(→ informaz. contenuta nella chiave $\geq$ informaz. contenuta nel testo in chiaro)

la chiave deve essere lunga almeno quanto il testo in chiaro

One-time pad:

$H(Z) = H(X)$



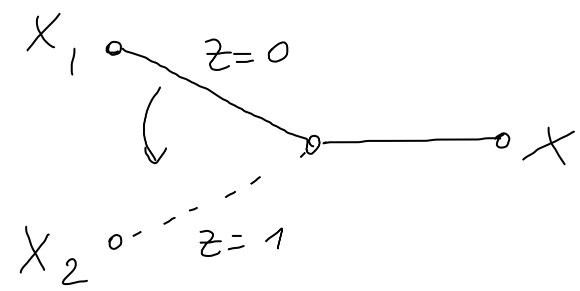
$H(X) = \boxed{I(X; Z \mid Y)} \leq$ $H(Z) = \square + \square + \geq 0 \geq \square$

$H(Y)$

$\alpha \geq 0$ $I(X; Y \mid Z) \geq 0$

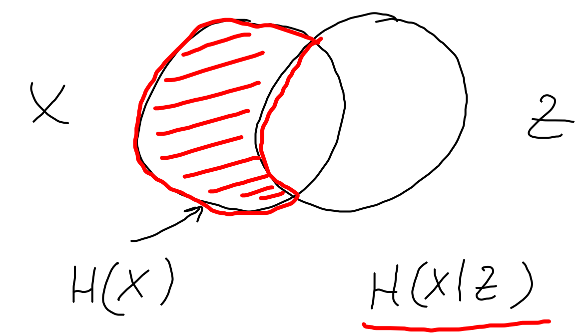
(4) Consideriamo due v.a. X_1, X_2. Definiamo una terza v.a. $X = \begin{cases} X_1 & \text{con prob. } \lambda \\ X_2 & \text{con prob. } 1-\lambda \end{cases}$ $(\lambda \in (0,1))$

Dimostrare che $\underline{H(X)} \geq \lambda H(X_1) + (1-\lambda) H(X_2)$.



Sia $Z = \begin{cases} 0 & \text{con prob. } \underline{\lambda} \\ 1 & \text{con prob. } 1-\lambda \end{cases}$ $\qquad X = \begin{cases} X_1 & \text{se } Z=0 \\ X_2 & \text{se } Z=1 \end{cases}$

$$\underline{H(X)} \geq H(X|Z) = \overset{\lambda}{\Pr[Z=0]} \cdot H(X|Z=0) +$$
$$+ \overset{1-\lambda}{\Pr[Z=1]} \cdot H(X|Z=1).$$
$$= \lambda \underbrace{H(X|Z=0)}_{H(X_1)} + (1-\lambda) \underbrace{H(X|Z=1)}_{H(X_2)}$$
$$= \underline{\lambda H(X_1) + (1-\lambda) H(X_2)}.$$



⑤ Consideriamo due v.a. X, Y.

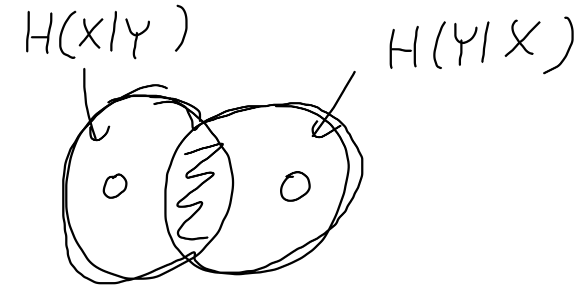
Sia $\rho = \dfrac{I(X;Y)}{H(X,Y)}$.

$(H(X,Y) \neq 0)$

(a) Mostrare che $0 \leq \rho \leq 1$

(b) Quand'è che $\rho = 0$?

(c) Quand'è che $\rho = 1$?



(a) $I(X;Y) \geq 0$, $H(X,Y) > 0 \implies \rho \geq 0$

$I(X;Y) \leq H(X,Y) \implies \rho \leq 1$

(b) $\rho = 0 \iff X$ e Y sono v.a. indipendenti

(c) $\rho = 1 \iff \underline{I(X;Y) = H(X,Y)}$

$\iff H(X|Y) = 0$ e $H(Y|X) = 0$

$\iff X$ è funz. di Y e Y è funz. di X

$\iff X$ e Y sono

in corrispondenza biunivoca.