⓪ SIGSALY

$\underbrace{X \oplus Y}_{Z} \oplus Y = X$

$$\begin{tikzcd} X \arrow[r] & \oplus \arrow[r] & Z \arrow[r] & \approx \arrow[r] & Z \arrow[r] & \oplus \arrow[r] & X \\ & Y \arrow[u] & & & & Y \arrow[u] & \end{tikzcd}$$

(a) $p_X = (\overbrace{\alpha}^{X=0}, \overbrace{1-\alpha}^{X=1})$

$p_Y = (1/2, 1/2)$ $\Longrightarrow$ $I(X;Z) = 0$

$I(X;Z|Y) > 0$

(b) $p_X = (\alpha, 1-\alpha)$

$p_Y = (1/4, 3/4)$ $\Longrightarrow$ Cosa cambia?

X e Z sono v.a. indipendenti? NO $\Longrightarrow$ $I(X;Z) > 0$

NON può essere

?

$p_X \cdot p_Y = p_{XY}$

p_{XY}	$Y = 0$	$Y = 1$
$X = 0$	$\alpha/4$	$3\alpha/4$
$X = 1$	$(1-\alpha)/4$	$3(1-\alpha)/4$

$Z=1$

$Z=0$

p_{XZ}	$Z = 0$	$Z = 1$
$X = 0$	$\alpha/4$	$3\alpha/4$
$X = 1$	$3(1-\alpha)/4$	$(1-\alpha)/4$

$p_{XZ} = p_X \cdot p_Z$

	$(1/4$	$3/4)$
α	$\alpha/4$	$3\alpha/4$
$1-\alpha$	$(1-\alpha)/4$	

contraddizione

① Mostrare $H(Y|X)=0 \iff$ per ogni $x\in\mathcal{X}$ con $p(x)>0$

esiste uno e un solo y tale che $p(y|x)=1$

(in altre parole, Y è funzione di X).

(Generalizza il fatto che $H(Y)=0 \iff Y$ è una costante)

Dim. $H(Y|X)=0 \iff \sum_{x\in\mathcal{X}} \underbrace{p(x)}_{\geq 0}\,\underbrace{H(Y|X=x)}_{\geq 0} = 0$ $\quad(\mathbb{E}_{x}[H(Y|X=x)])$

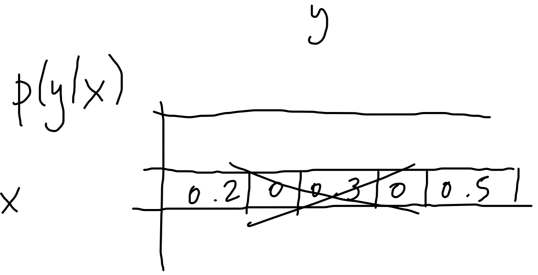
$$\iff \sum_{x\in\mathcal{X}:p(x)>0} \overset{>0}{p(x)}\,\overbrace{H(Y|X=x)}^{\geq 0} = 0$$

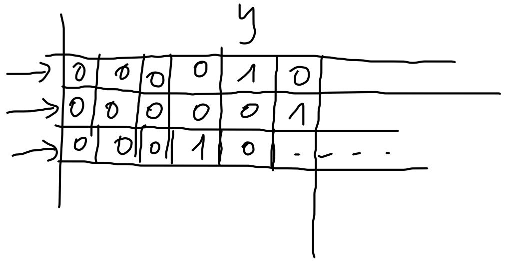
$$\iff \forall x: p(x)>0 \text{ ho } H(Y|X=x)=0$$

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

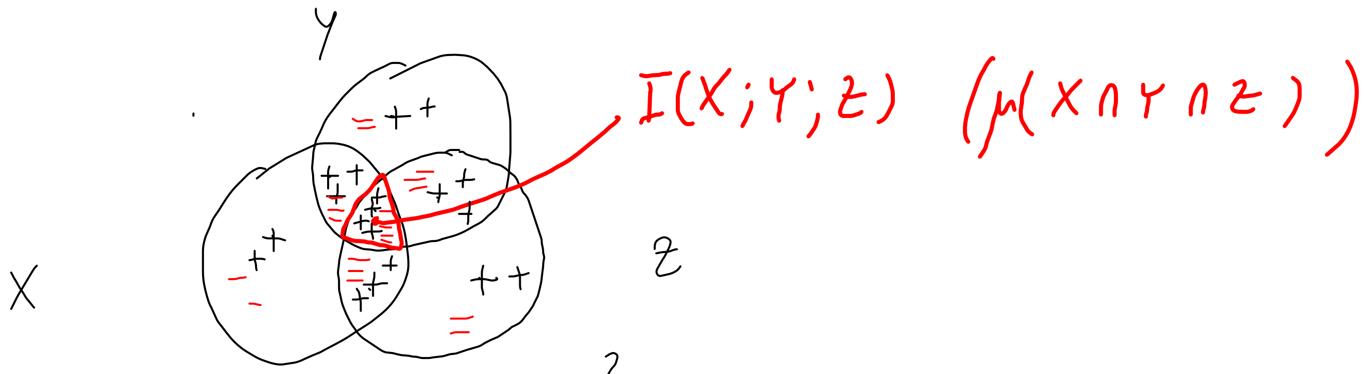
$$\iff \forall x: \underline{p(x)>0} \quad \forall y\in\mathcal{Y} \text{ ho } p(y|x)=0 \text{ oppure } p(y|x)=1$$

$\iff Y$ è funzione di X.





② "Mutua informazione" tra 3 v.a.



Come definisco $I(X;Y;Z)$?

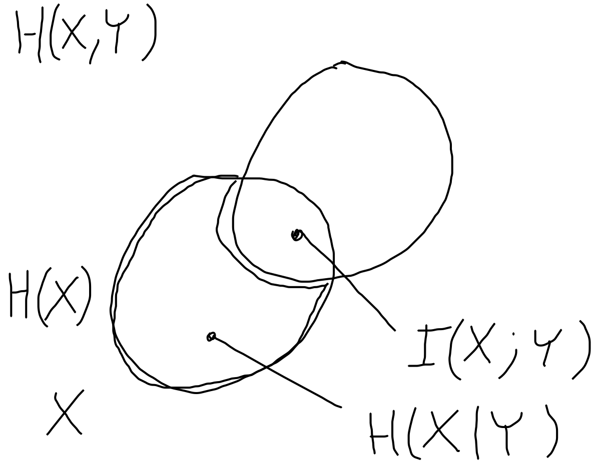
Una possibilità è la seguente:

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

Attenzione: $I(X;Y;Z)$ NON è una divergenza informazionale

$$\mu(X\cap Y\cap Z) + \mu(X\cup Y) + \mu(X\cup Z) + \mu(Y\cup Z) \overset{\checkmark}{=} \mu(X\cup Y\cup Z) + \mu(X) + \mu(Y) + \mu(Z)$$

$$\left(I(X;Y) \overset{def}{=} D(p_{XY} \| p_X \cdot p_Y) \geq 0 \right)$$



$; \longrightarrow \cap$

$| \longrightarrow \setminus$

$, \longrightarrow \cup$

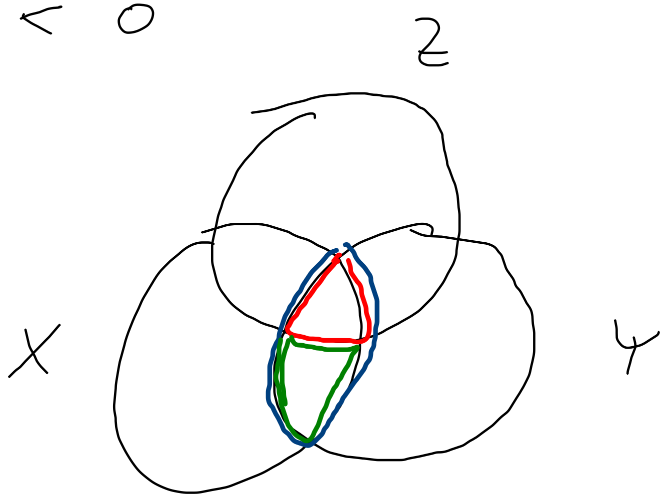
μ

$\mu(S_X) = H(X) \geq 0$

$\mu(S_X \cap S_Y) = I(X;Y) \geq 0$

$$\rightarrow \quad \underline{I(X;Y;Z)} = \underbrace{I(X;Y)}_{\uparrow\, = 0} - \underbrace{I(X;Y|Z)}_{\nearrow\, > 0} < 0$$

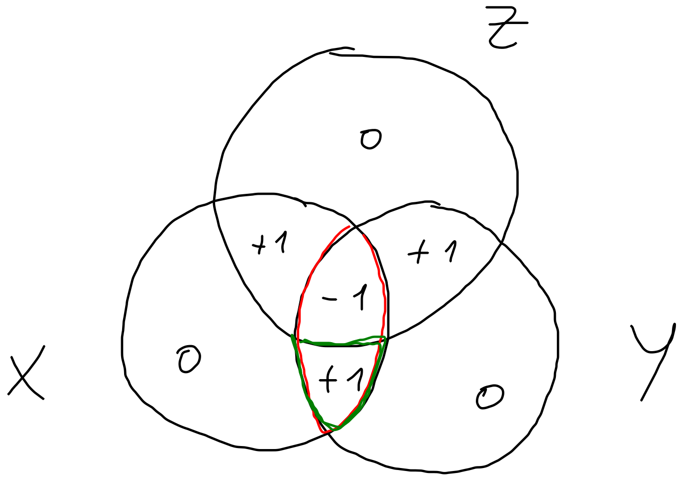
si può avere simultaneamente



Esempio : X uniforme su $\{0,1\}$

Z uniforme su $\{0,1\}$

$Y = X \oplus Z$



$H(X) = 1$

$I(X;Y) = 0$ $\qquad I(X;Y|Z) = 1$

$I(X;Y;Z) = -1$

③ Esempio di 3 v.a. X, Y, Z con $I(X;Y)>0$ e $I(X;Y|Z)=0$.

Consideriamo 3 v.a. X, Y, Z in catena di Markov $X \to Z \to Y$

con X e Y non indipendenti

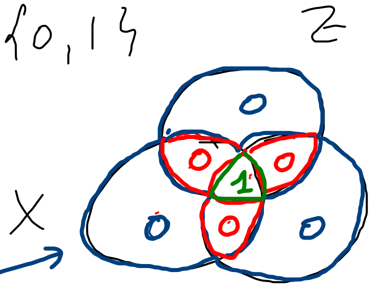
Allora, X e Y non indipendenti → $I(X;Y)>0$

D'altra parte per Markovianità, $I(X;Y|Z)=0$

→ Scenario concreto: Prendo X con distribuzione uniforme su $\{0,1\}$

Prendo $Z = X$

Prendo $Y = Z = X$



$H(Y|X,Z)=0$

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

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

$H(Z)=H(X)=H(Y)=1$

→ Vale la catena $X \to Z \to Y$.

→ $I(X;Y;Z)=1$

④ Teorema della segretezza perfetta (Shannon 1949)

X, Y, Z v.a.

X : testo in chiaro

Y : testo cifrato

Z : chiave di cifratura

Uno schema di cifratura "ideale" dovrebbe avere queste proprietà:

(1) Decifrabilità : $H(X \mid Y, Z) = 0$ (X è funzione della coppia (Y, Z))

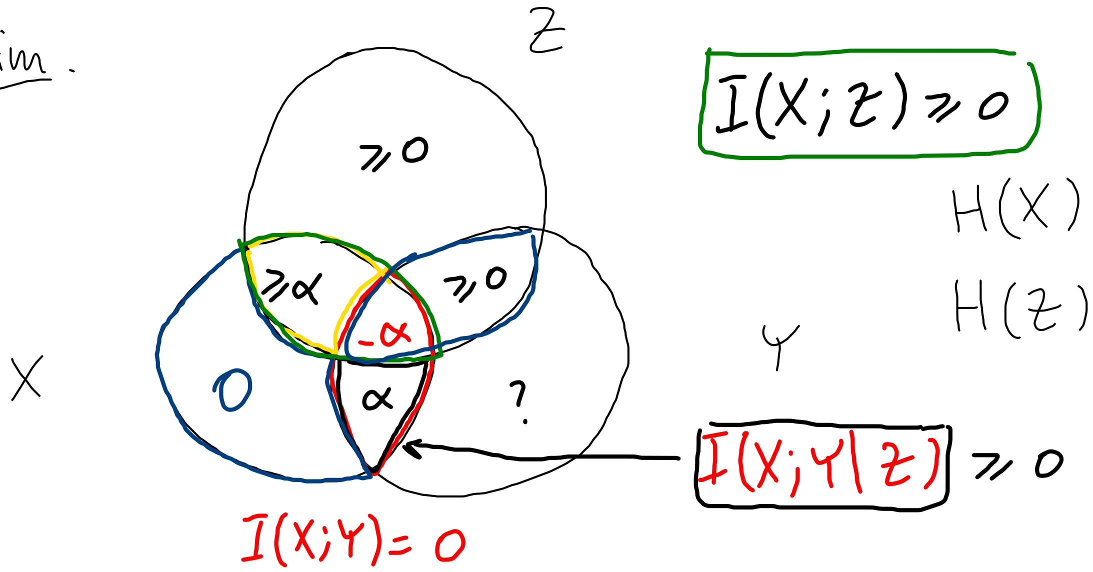
(2) Segretezza perfetta : $I(X ; Y) = 0$

Teorema : Per qualunque schema di cifratura con le proprietà (1) e (2), si ha:

$$H(Z) \geq H(X).$$

(in pratica: la chiave deve essere lunga quanto il testo in chiaro)

Dim.



$I(Y;Z) \geq 0$

$$H(X) = 0 + \alpha - \alpha + \overset{\geq \alpha}{\bullet}$$

$$H(Z) = \geq 0 + \bullet + \geq 0$$

(Nota. Nel one-time pad, si ha $H(Z) = H(X)$)

$\rightarrow H(Z) \geq H(X)$

QED.

Sia $\lambda \in (0,1)$

⑤ Consideriamo due v.a. X_1 e X_2

Definiamo una terza v.a. X, come $X = \begin{cases} X_1 & \text{con prob. } \lambda \\ X_2 & \text{con prob. } 1-\lambda \end{cases}$

Dimostrare che

$$H(X) \geq \lambda H(X_1) + (1-\lambda) H(X_2)$$