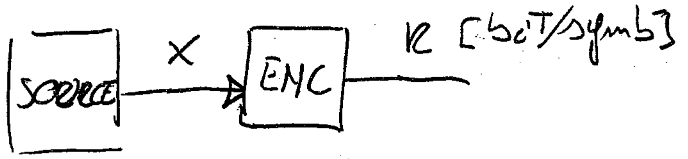
# Codifica di Sorgente Distribuita

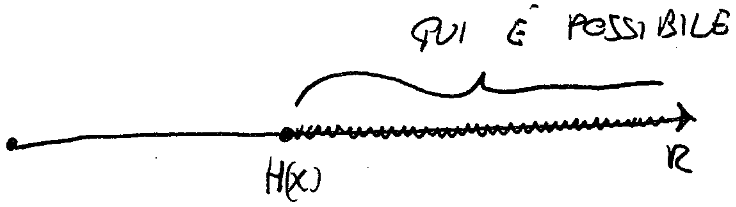
Data una sorgente $X \sim p(x)$ $x \in \mathcal{X}$ posso effettuare codifica "lossless", senza perdite, di $X$ e, raggruppando n per volta ottenere una lunghezza media di descrizione di $X$ pari a

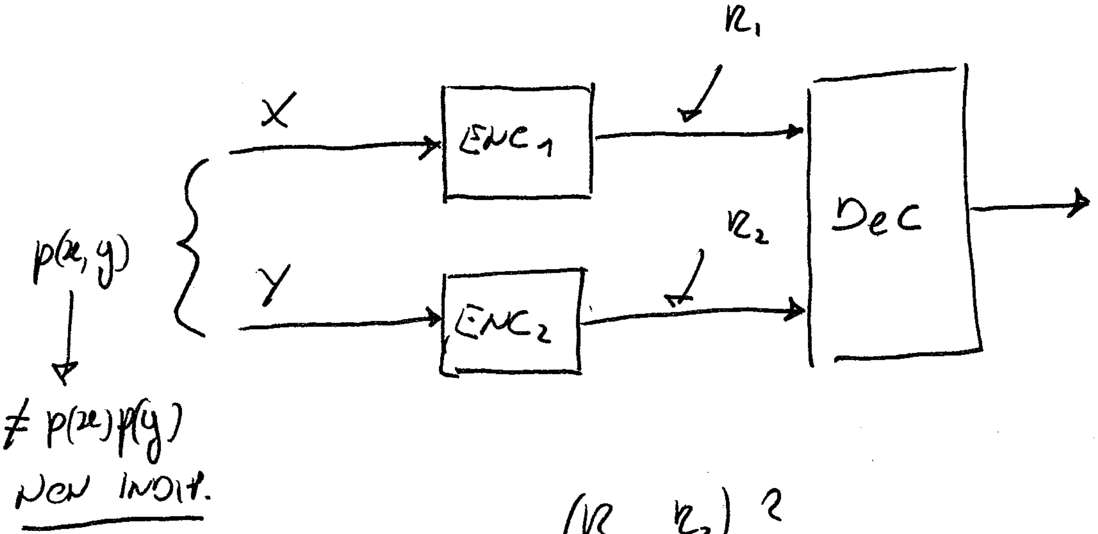
$$H(X) \; [\text{bit}]$$




$$R \geq H(X)$$

Cosa è consentito, possibile, e cosa no?

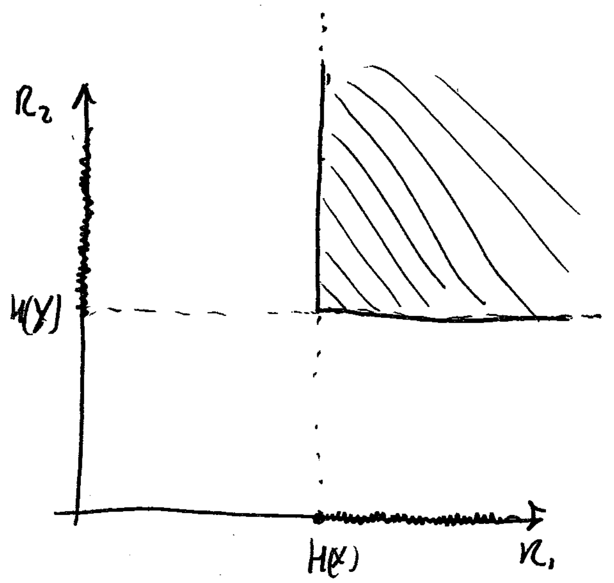


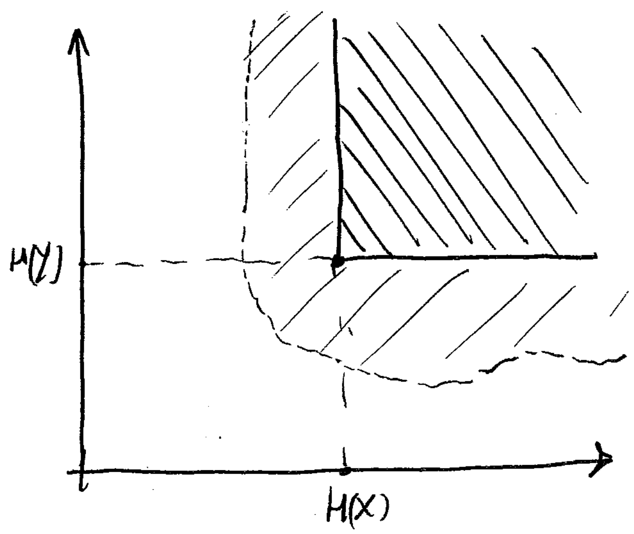

$$(R_1, R_2) \; ?$$

Codifico X e Y separatamente.

Potrei usare un codice ottimo per X e un ottimo per Y



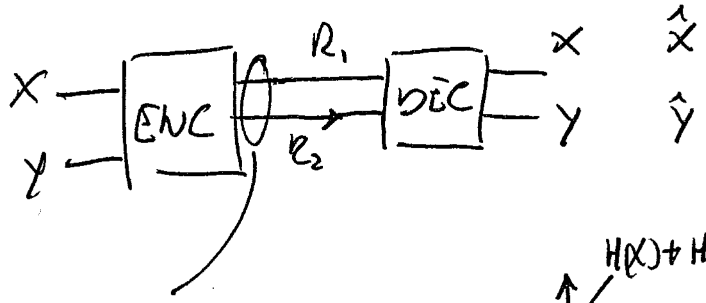

Posso fare meglio?



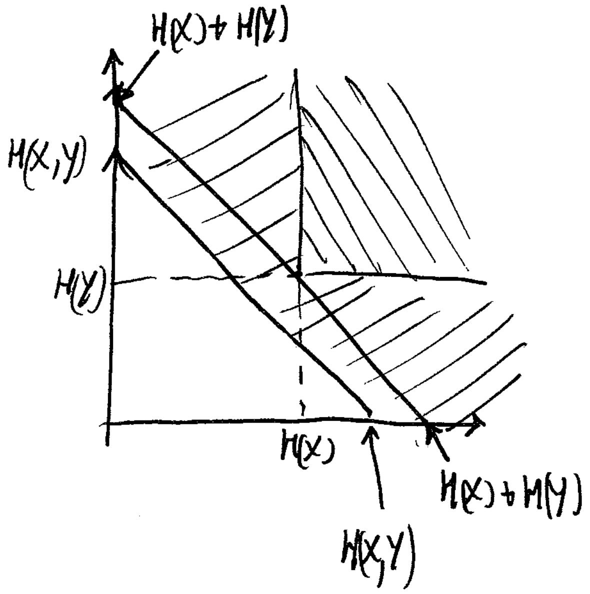

Qual'è il limite? Qual'è la parte di piano che comprende tutti gli insiemi che posso dimostrare raggiungibili?

# Outer bounds intuitivi

Con un codificatore unico che opera su entrambi $(X,Y)$ NON POSSO CHE FAR MEGLIO O UGUALE rispetto a due cod. separati




rate $R = R_1 + R_2$

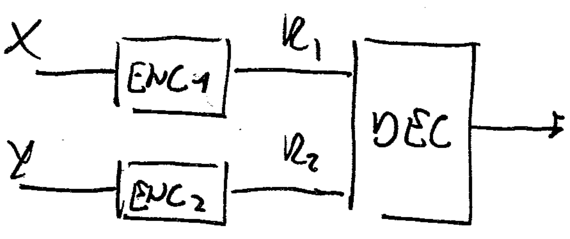



Perciò

$$R_1 + R_2 \geq H(X;Y)$$

è un outer bound

Se codifico separatamente




non posso ripartire i tassi in modo arbitrario:

$R_1 = H(X;Y)$ $\quad R_2 = 0$ $\quad$ verifica $\quad R_1 + R_2 = H(X;Y)$

ma vorrebbe dire che descrivo $(X,Y)$ sulla base del solo $X$ !!!

C'è una parte di Y che non è nota, ma è <u>prevedibile</u> sulla base del solo X.

Intuitivamente essa è L'INCERTEZZA SU Y NOTO X

ovvero

$$H(Y|X)$$

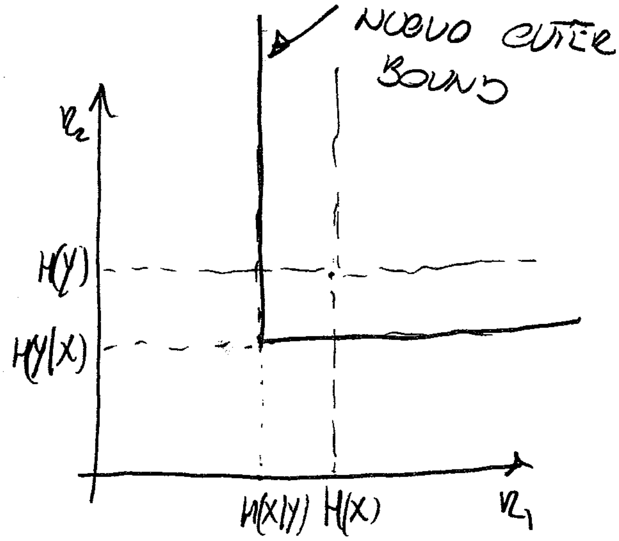
Quindi se $R_2 < H(Y|X)$ sto tentando di incorporare in $R_1$ una parte dell'informazione su Y che NON È CONTENUTA IN X

Perciò deve essere

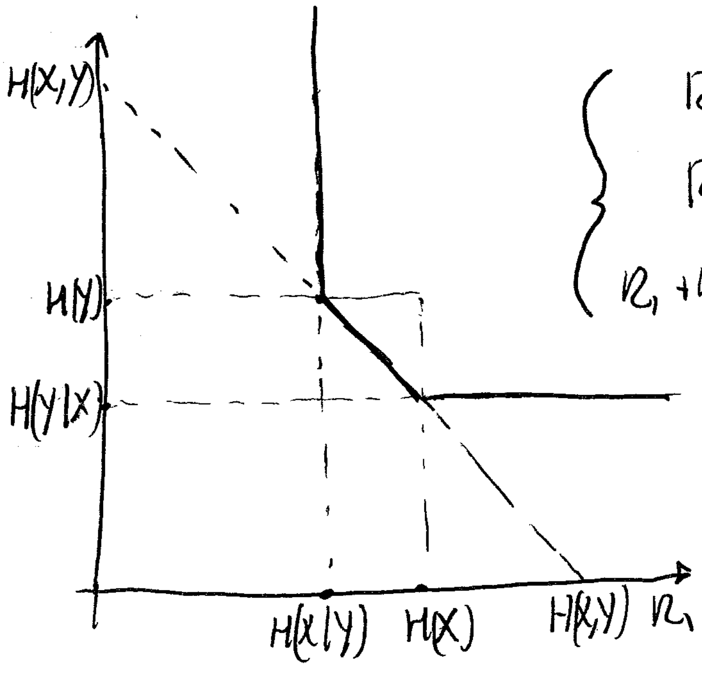
$$R_2 \geq H(Y|X)$$

e, analogamente

$$R_1 \geq H(X|Y)$$




combinando:




$$\begin{cases} R_1 \geq H(X|Y) \\ R_2 \geq H(Y|X) \\ R_1 + R_2 \geq H(X,Y) \end{cases}$$

Definizione: un codice $((2^{nR_1}, 2^{nR_2}), n)$ per la codifica distribuita di una coppia $(X, Y)$ di sorgenti è data da 2 funzioni (o mappe) di codifica

$$f_1 : \mathcal{X}^n \longrightarrow \{1, \dots, 2^{nR_1}\}$$

$$f_2 : \mathcal{Y}^n \longrightarrow \{1, \dots, 2^{nR_2}\}$$

e da una corrispondente funzione (o mappa) di decodifica

$$g : \{1, \dots, 2^{nR_1}\} \times \{1, \dots, 2^{nR_2}\} \longrightarrow \mathcal{X}^n \times \mathcal{Y}^n$$

Quindi: si mappano vettori $\underline{x} \in \mathcal{X}^n$ e $\underline{y} \in \mathcal{Y}^n$ in <u>indici interi</u> (rapp. risp. con $nR_1$ e $nR_2$ bit)

In generale, per avere compressione

$$2^{nR_1} < |\mathcal{X}|^n \qquad \text{e} \qquad 2^{nR_2} < |\mathcal{Y}|^n$$

non tutti i vettori $(\underline{x}, \underline{y})$ possono essere rappresentati!

Un siffatto codice è LOSSY. (in una accezione particolare: vediamo:)

Ammettiamo una prob. di errore $> 0$ sui vettori decodificati:

$$g(f_1(\underline{X}), f_2(\underline{Y})) = (\hat{\underline{X}}, \hat{\underline{Y}}) \qquad \text{(stime)}$$

La probabilità di errore $P_e^{(n)}$ di un DSC con parole lunghe n è data da

$$P_e^{(n)} = P_r\left\{ g\left(f_1(\underline{X}), f_2(\underline{Y})\right) \neq (\underline{X}, \underline{Y}) \right\}$$

Una coppia di tassi $(R_1, R_2)$ si dice raggiungibile (achievable) se $\exists$ una sequenza di codici

$\left(\left(2^{nR_1}, 2^{nR_2}\right), n\right)$ per cui $\lim_{n \to \infty} P_e^{(n)} = 0$

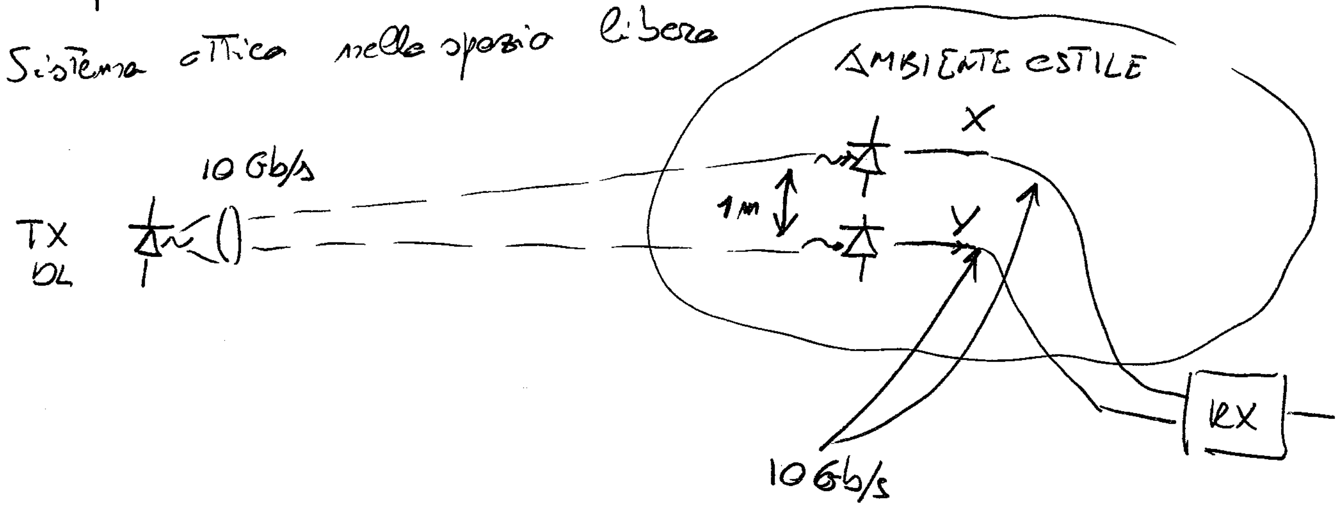
La regione dei tassi raggiungibili è la chiusura dell'insieme di tutti gli $(R_1, R_2)$ raggiungibili.

Teorema (Slepian e Wolf 1973)
La regione dei tassi raggiungibili mediante DSC di una coppia di sorgenti $(X, Y)$ i.i.d. $(X, Y) \sim p(x, y)$ è data da

$$\begin{cases} R_1 \geq H(X|Y) \\ R_2 \geq H(Y|X) \\ R_1 + R_2 \geq H(X,Y) \end{cases}$$

Esempio:

Sistema ottico nello spazio libero




X e Y 10 Gb/s ma saranno quasi sempre uguali!

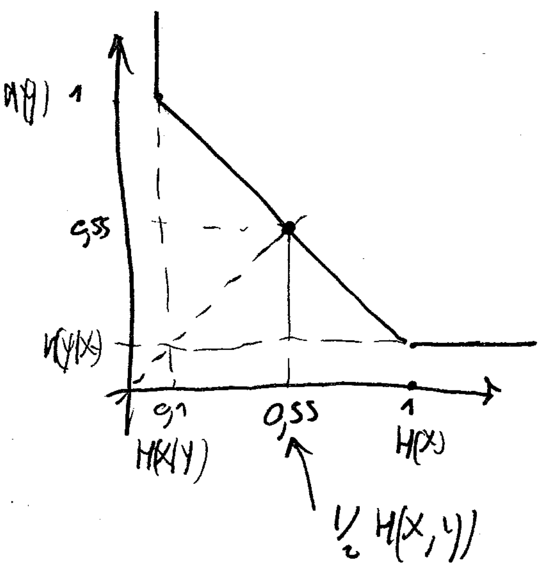
$p(x,y)$

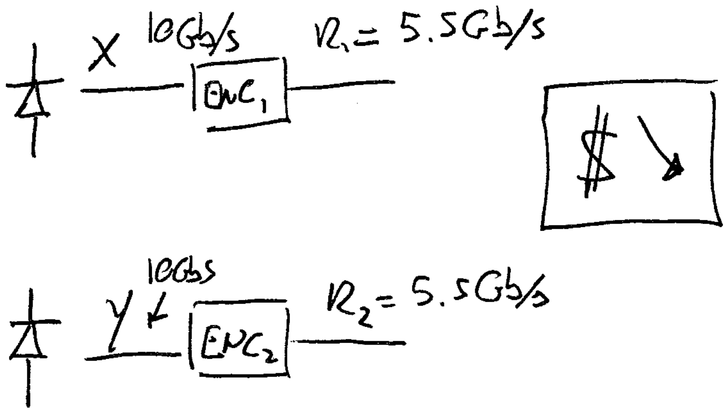
| X \ Y | 0 | 1 |
|---|---|---|
| 0 | 0,4935 | 0,0065 |
| 1 | 0,0065 | 0,4935 |

$$P\{X=0\} = P\{X=1\} = P\{Y=0\} = P\{Y=1\} = \frac{1}{2}$$

$$P\{X=Y\} = p = 0,987$$

$$H(X;Y) = H(X) + H(Y|X) = H(X) + h(p) = 1 + 0.1 = 1.1$$



$(U,V) \sim p(u,v) \qquad (u,v) \in \{0,1\}\times\{0,1\}$

$p(u,v)$

$$\begin{array}{c|cc} u \backslash v & 0 & 1 \\ \hline 0 & 1/3 & 1/3 \\ 1 & 0 & 1/3 \end{array}$$

$H(U) = h(1/3) = 0{,}918$ bit

$H(V) = H(U)$

$H(U,V) = -\log \frac{1}{3} = 1{,}585$ bit

$H(U|V) = \frac{2}{3} = H(V|U)$

Senza codifica: 2 bit per coppia di simboli

Codifica entropica standard: $2 \times 0{,}918 = 1{,}836$ bit "

DSC S-W : $1.585$ bit "

# Tecnica per dimostrare la raggiungibilità

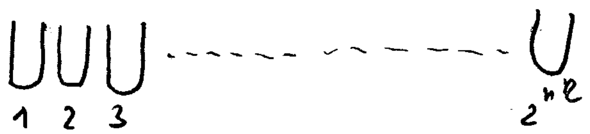
## RANDOM BINNING

Codifica di Sorgente mediante R.B.

• Singola sorgente $X \sim p(x)$ $\quad x \in \mathcal{X}$

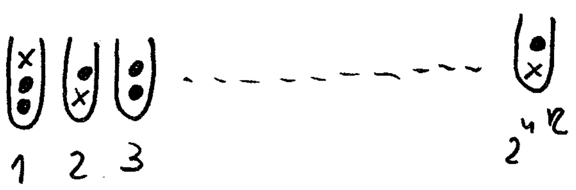
1) fisso $n$ lunghezza della sequenza da cod.
   fisso $R$ tasso della codifica (del codice)

2) Predispongo $2^{nR}$ contenitori (bins) numerati




3) Genero tutte le possibili sequenze $\underline{x} \in \mathcal{X}^n$ e pongo ogni sequenza in un bin di indice $I \sim$ unif. $\{1, \dots, 2^{nR}\}$
(Un bin può contenere più sequenze)

Considero $A_\varepsilon^{(n)}$ e rappresento con una $\times$ le sequenze tipiche e con $\bullet$ tutte le altre




Se $R > H(X)$ e $n$ è grande con elevata prob. ogni bin conterrà al più $1$ $\underline{x} \in A_\varepsilon^{(n)}$

(S)

Codifica:

$$f: \mathcal{X}^n \to \{1, \dots, 2^{nR}\} \qquad f(\underline{x}) = \text{indice del bin corrispondente a } \underline{x}$$

Decodifica: $g(\cdot)$

ricevo $i$: se nell'i-esimo bin c'è solo una $\underline{x}^* \in A_\varepsilon^{(n)}$

emetto $\underline{x}^*$ altrimenti dichiara errore

$$\underline{g(i) = \underline{x}^*} \qquad \underline{g(i) = e}$$

↖ simbolo speciale

$$P_e^{(n)} = P_r\{g(f(\underline{X})) \neq \underline{X}\} = P_r\{g(f(\underline{X})) = e\}$$

$$= P_r\Big\{\{\underline{X} \notin A_\varepsilon^{(n)}\} \cup \bigcup_{\substack{\underline{x}' \neq \underline{X} \\ \underline{x}' \in A_\varepsilon^{(n)}}} \{f(\underline{x}') = f(\underline{X})\}\Big\}$$

ATTENZIONE! $f$ è random!

$$\leq P_r\{\underline{X} \in A_\varepsilon^{(n)}\} + P_r\Big\{\bigcup \{f(\underline{x}') = f(\underline{X})\}\Big\}$$

$$= P_r\{\underline{X} \in A_\varepsilon^{(n)}\} + \sum_{\underline{x}} P_r\{\underline{X} = \underline{x}\}\, P_r\Big\{\bigcup_{\substack{\underline{x}' \in A_\varepsilon^{(n)} \\ \underline{x}' \neq \underline{x}}} \{f(\underline{x}') = f(\underline{x})\}\Big\}$$

$$\leq \varepsilon + \sum_{\underline{x}} p(\underline{x}) \sum_{\substack{\underline{x}' \in A_\varepsilon^{(n)} \\ \underline{x}' \neq \underline{x}}} \underbrace{P_r\{f(\underline{x}') = f(\underline{x})\}}_{2^{-nR}}$$

$$\leq \varepsilon + \sum_{\underline{x}} p(\underline{x}) \sum_{A_\varepsilon^{(n)}} 2^{-nR}$$

$$\leq \varepsilon + 2^{-nR}\, 2^{n(H(X)+\varepsilon)} \qquad \sum_{\underline{x}} p(\underline{x}) = 1$$

se $R > H(X) + \varepsilon$ e $n > \frac{\lg \varepsilon}{R - H(X) - \varepsilon}$ $\Longrightarrow$ $\boxed{P_e^{(n)} \leq 2\varepsilon}$

OVVERO
$P_e^{(n)}$ piccola a piacere per ogni $R > H(X)$

Dim: del Teorema di S. e W.

1. $\forall (R_1, R_2)$ con
$$\begin{cases} R_1 > H(X|Y) \\ R_2 > H(Y|X) \\ R_1 + R_2 > H(X,Y) \end{cases}$$

$\exists$ una sequenza di codici DSC |

$$\lim_{n\to\infty} P_e^{(n)} = 0$$

2. Data una sequenza di DSC $((2^{nR_1}, 2^{nR_2}), n)$

allora
$$R_1 \geq H(X|Y)$$
$$R_2 \geq H(Y|X)$$
$$R_1 + R_2 \geq H(X,Y).$$

Dim 1

Costruiamo una sequenza di codici usando il random binning.

1) Ad ogni $\underline{x} \in \mathcal{X}^n$ assegnare un bin a caso fra $2^{nR_1}$ possibili $f_1 : \mathcal{X}^n \to \{1, \dots, 2^{nR_1}\}$ $f_1(\underline{x}) \rightsquigarrow i$ indice del bin corrisp.

Ad ogni $\underline{y} \in \mathcal{Y}^n$ " " " " " " "
$2^{nR_2}$ possibili $f_2 : \mathcal{Y}^n \to \{1, \dots, 2^{nR_2}\}$ $f_2(\underline{x}) \rightsquigarrow j$

2) le $f_1(\cdot)$ e $f_2(\cdot)$ vengono rivelate agli ENC e al DECOD.

3) $ENC_1$ osserva $\underline{X}$ ed emette $I = f_1(\underline{X})$

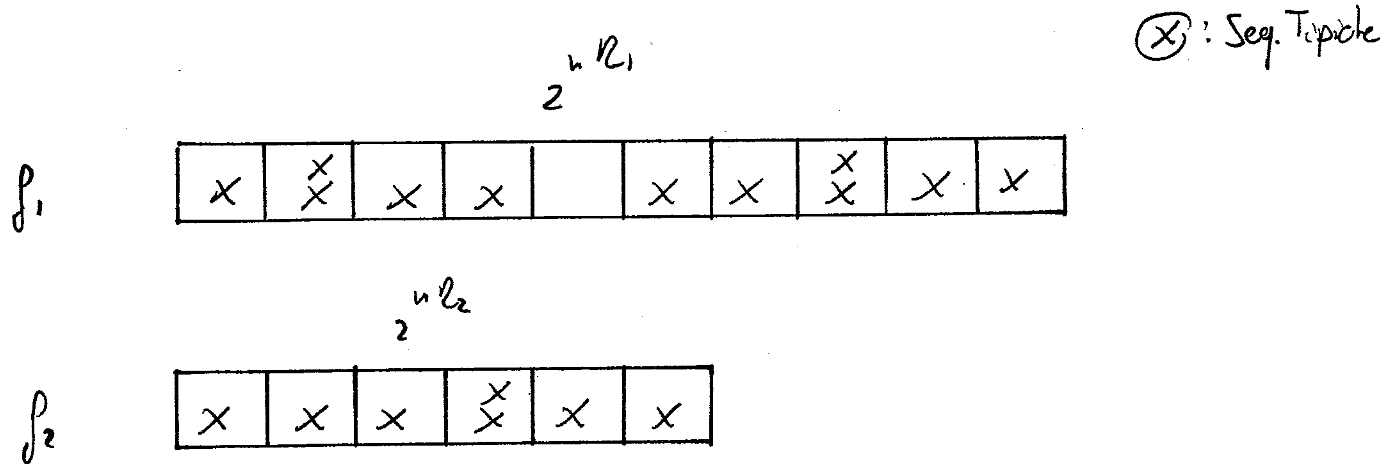
$ENC_2$ osserva $\underline{Y}$ ed emette $J = f_2(\underline{Y})$

4) il DECOD emette $g(I, J) = (\hat{\underline{X}}, \hat{\underline{Y}})$

dove $g(\cdot,\cdot)$

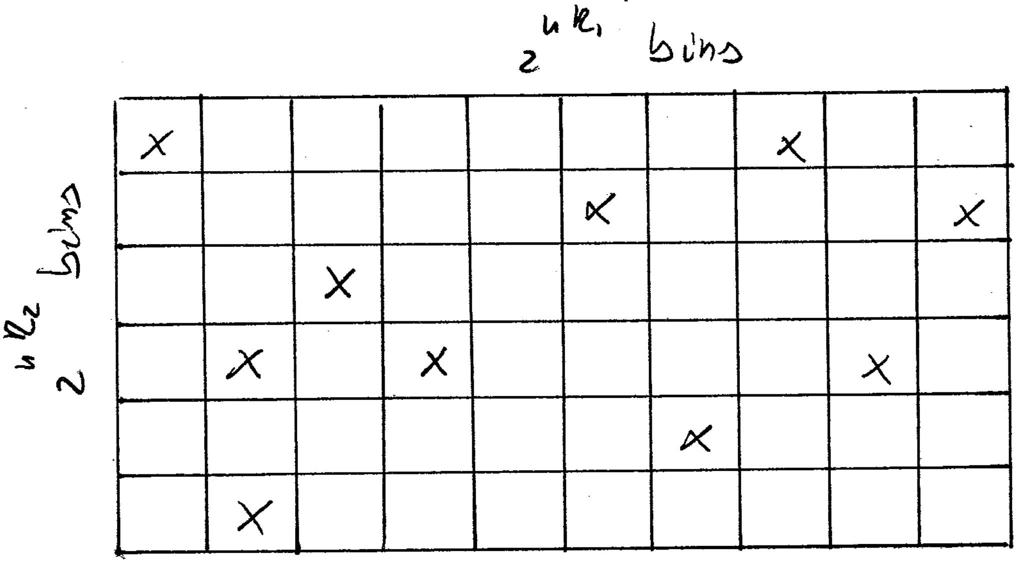
$$g(i,j) = \begin{cases} (\underline{x}^*, \underline{y}^*) & \text{se } \exists! (\underline{x}^*, \underline{y}^*) \in A_\varepsilon^{(n)} \text{ con } (f_1(\underline{x}^*), f_2(\underline{y}^*)) = (i,j) \\ e & \text{altrimenti (error)} \end{cases}$$

Se ci limitiamo alle sequenze cong. Tipiche sbagliamo con $P_e^{(n)}$ piccola a piacere. Basta che in nessun bin ci sia più di una crocetta!




In una visione mono dimensionale (visione di ogni singolo enc)

si vorrebbe $R_1 > H(X)$ $R_2 > H(Y)$ per non avere crocette multiple. Ma al DECOD la visione è bidim




ⓧ Seq. cong. Tipiche (da non confondersi)

non c'è una rel semplice fra queste crocette e quelle sopra

Qui il numero di spazi deve essere $> 2^{nH(X,Y)}$

Anclisi della $P_e^{(n)}$

$$E_0 = \{ (\underline{X}, \underline{Y}) \notin A_\varepsilon^{(n)} \}$$

$$E_1 = \bigcup_{\substack{\underline{x}' \neq \underline{X} \\ (\underline{x}', \underline{Y}) \in A_\varepsilon^{(n)}}} \{ f_1(\underline{x}') = f_1(\underline{X}) \}$$

$$E_2 = \bigcup_{\substack{\underline{y}' \neq \underline{Y} \\ (\underline{X}, \underline{y}') \in A_\varepsilon^{(n)}}} \{ f_2(\underline{y}') = f_2(\underline{Y}) \}$$

$$E_{12} = \bigcup_{\substack{(\underline{x}', \underline{y}') \neq (\underline{X}, \underline{Y}) \\ (\underline{x}', \underline{y}') \in A_\varepsilon^{(n)}}} \{ (f_1(\underline{x}'), f_2(\underline{y}')) = (f_1(\underline{X}), f_2(\underline{Y})) \}$$

$$P_e^{(n)} = P_r(E_0 \cup E_1 \cup E_2 \cup E_{12})$$

$$\leq \underbrace{P_r(E_0)}_{< \varepsilon} + P_r(E_1) + P_r(E_2) + P_r(E_{12})$$

Prendiamo ad esempio $P(E_1)$

$$P(E_1) = P_r\left( \bigcup_{\substack{\underline{x}' \neq \underline{X} \\ (\underline{x}', \underline{Y}) \in A_\varepsilon^{(n)}}} \{ f_1(\underline{x}') = f_1(\underline{X}) \} \right)$$

$$= \sum_{(\underline{x}, \underline{y})} p(\underline{x}, \underline{y}) \, P_r\left( \bigcup_{\substack{\underline{x}' \neq \underline{x} \\ (\underline{x}', \underline{y}) \in A_\varepsilon^{(n)}}} \{ f_1(\underline{x}') = f_1(\underline{x}) \} \,\middle|\, \underline{X} = \underline{x}, \underline{Y} = \underline{y} \right)$$

INDIP

$$\leq \sum_{(\underline{x},\underline{y})} p(\underline{x},\underline{y}) \sum_{\substack{\underline{x}'\neq\underline{x} \\ (\underline{x}',\underline{y})\in A_\varepsilon^{(n)}}} 2^{-nR_1}$$

$$= \sum_{(\underline{x},\underline{y})} p(\underline{x},\underline{y})\, 2^{-nR_1} \underbrace{\sum_{\substack{\underline{x}'\neq\underline{x} \\ (\underline{x}',\underline{y})\in A_\varepsilon^{(n)}}} 1}$$

n° di sequenze cong Tipiche a y $\leq 2^{n(H(X|Y)+2\varepsilon)}$

$$\leq 2^{-nR_1}\, 2^{n(H(X|Y)+2\varepsilon)} \sum_{(\underline{x},\underline{y})} p(\underline{x},\underline{y})$$

$$= 2^{-n(R_1 - H(X|Y)+2\varepsilon)}$$

$$\rightarrow \quad R_1 > H(X|Y) \quad \Rightarrow \quad P(E_1) \to 0$$

Analogamente

$$R_2 > H(Y|X) \quad \Rightarrow \quad P(E_2) \to 0$$

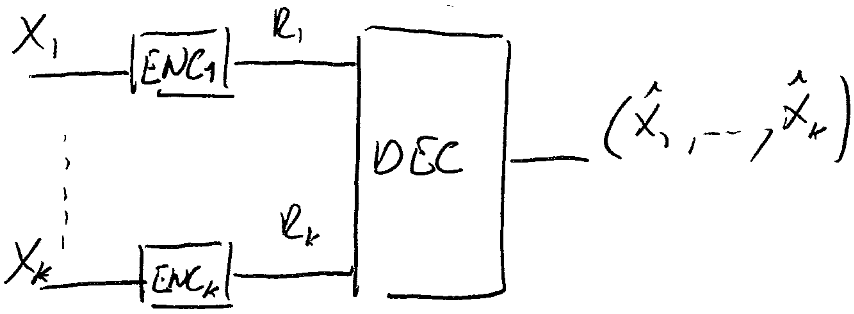
$$R_1+R_2 > H(X,Y) \quad \Rightarrow \quad P(E_{12}) \to 0$$

Ovvero $\forall \varepsilon>0 \quad \forall (R_1, R_2)$
$$\begin{aligned} R_1 &> H(X|Y) \\ R_2 &> H(Y|X) \\ R_1+R_2 &> H(X,Y) \end{aligned}$$

$$\exists n^* \mid \forall n > n^* \quad P_e^{(n)} < 2\varepsilon$$

$\blacksquare$

# Numero arbitrario di sorgenti




$$R_1 \geq H(X_1 \mid X_2, \dots, X_k)$$

$$R_2 \geq H(X_2 \mid X_1, X_3, \dots, X_k)$$

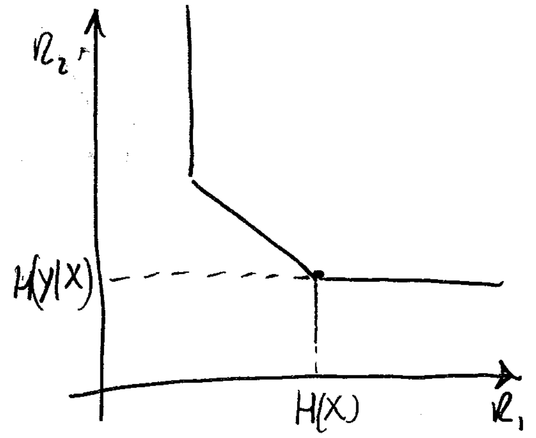
$$\vdots$$

$$R_i + R_j \geq H(X_i X_j \mid \{X_1, \dots, X_k\} \setminus \{X_i, X_j\})$$

$$\vdots$$

$$R_1 + \dots + R_k \geq H(X_1, \dots, X_k)$$

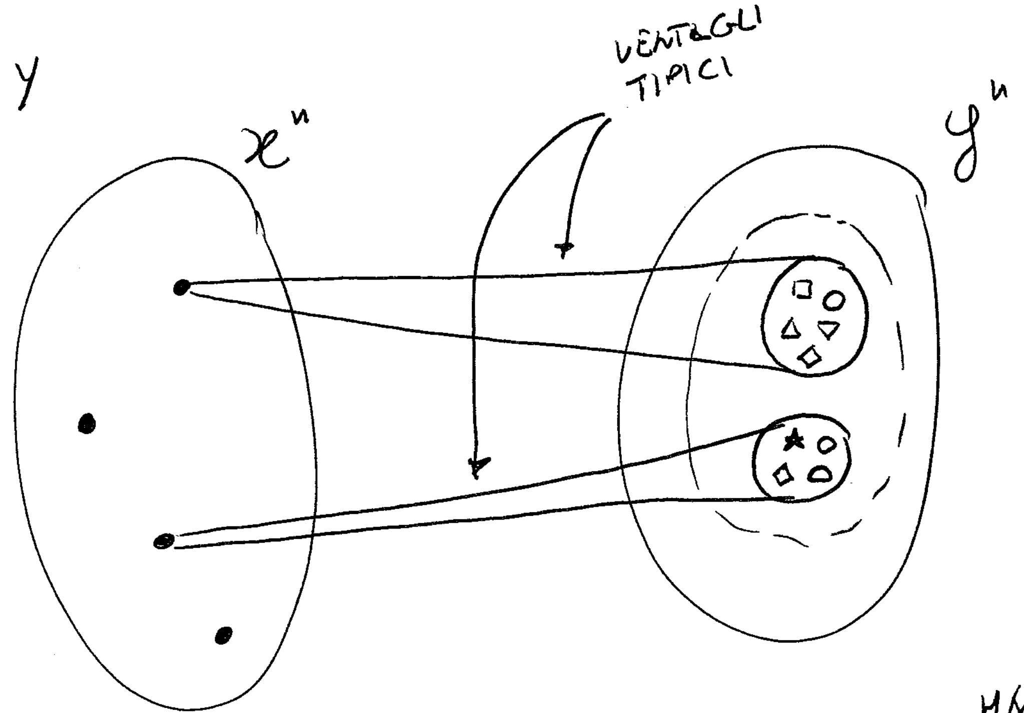
Codifica di S-W con il metodo della colorazione




$R_1 = H(X)$ $\qquad R_2 = H(Y|X)$

per X uso Tecniche note

Per Y

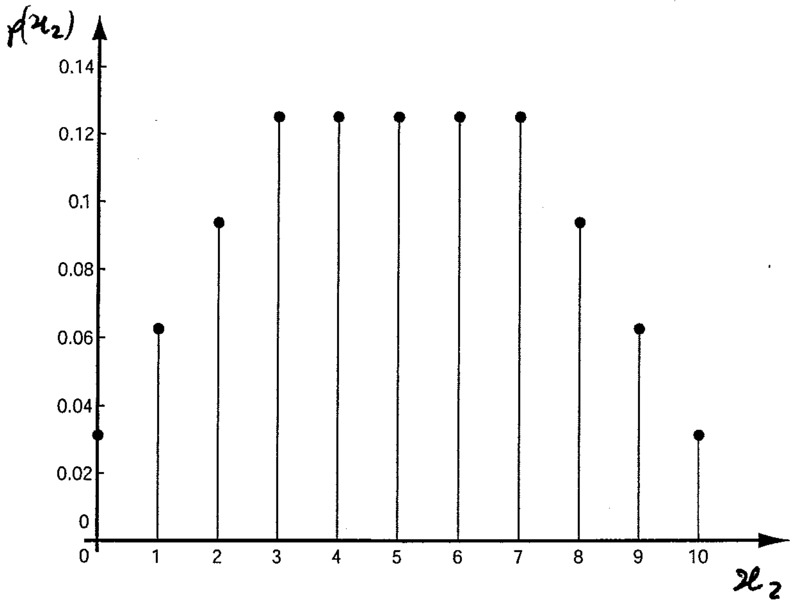


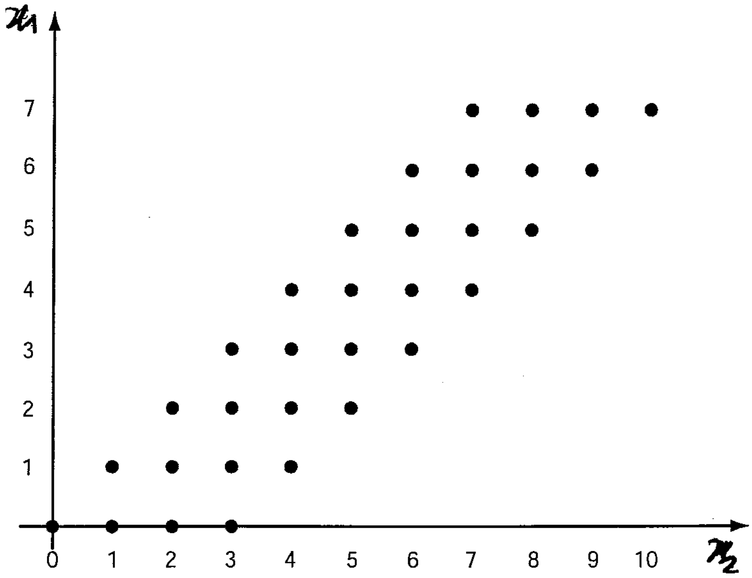

Ad ogni sequenza $\underline{x}$ sono associate $\simeq 2^{nH(Y|X)}$ sequenze $\underline{y}$ tipiche (congiunt. con $\underline{x}$) se coloro con un numero di colori $2^{nR_2} > 2^{nH(Y|X)}$ tutte le sequenze $\underline{y}$ in modo casuale in ogni ventaglio non compariranno 2 parole con il medesimo colore (con alta prob.) $\Rightarrow$ RICOSTRUISCO $\underline{y}$ dal colore e da $X$

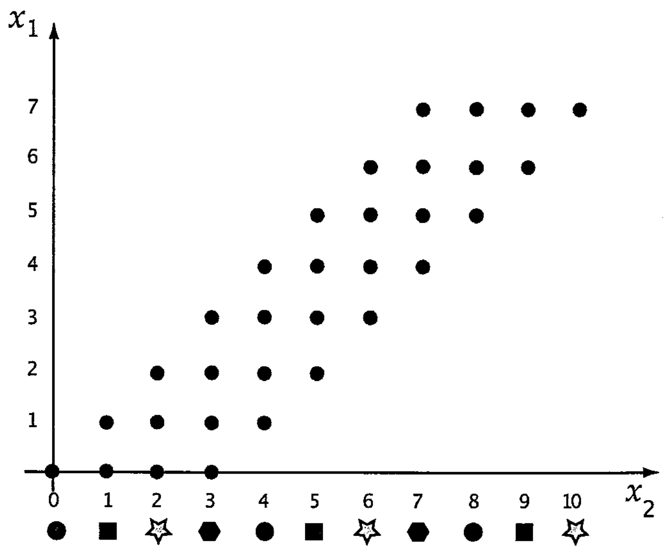
$X_1 \in \{0, \dots, 7\}$ unif. $\qquad Z \sim \text{unif}\,\{0, \dots, 3\}$

$X_2 = X_1 + Z \quad \in \{0, \dots, 10\}$

$p(x_2)$



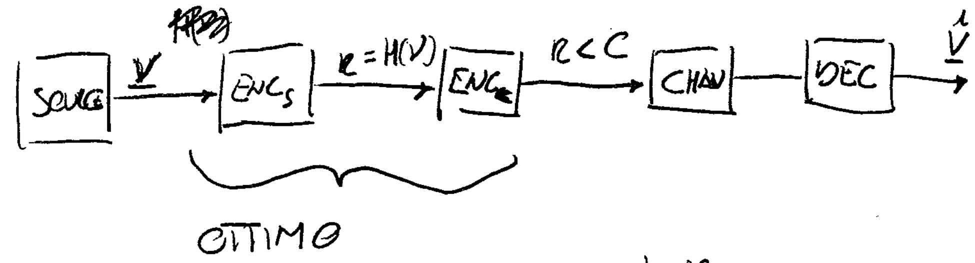






TX $x_1$ così com'è e codifico $x_2$ con un colore

ENC$_2$ NON CONOSCE $X_1$ MA LA RICOSTRUZIONE È IMMEDIATA

# Separabilità fra codifica di sorgente e di canale 

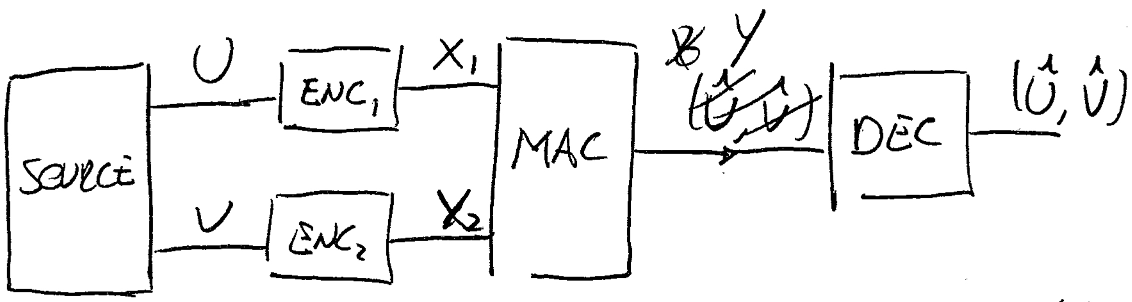



per $H(V) < C$ è sempre possibile spezzare la codifica in SORGENTE/CANALE con cod di sorgente ottima seguita da cod di canale ottima.

Consideriamo

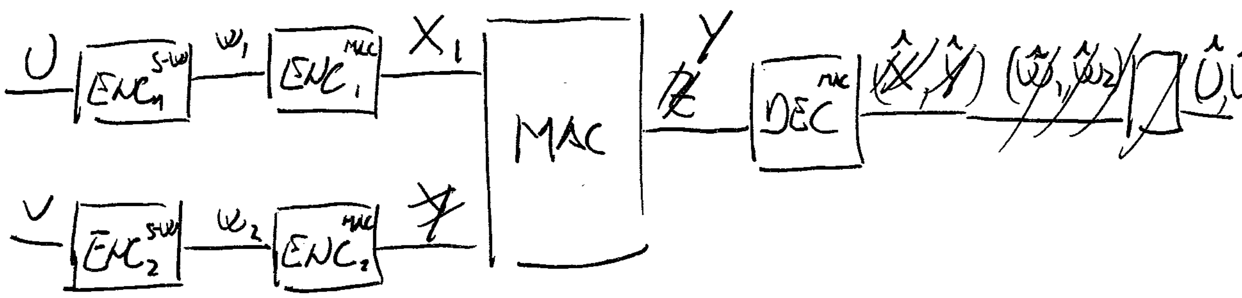
$(U, V)$ $\quad p(u,v)$

| | 1 | 0 |
|---|---|---|
| 0 | ~~1/3~~ | ~~1/3~~ |
| 1 | ~~0~~ | ~~1/3~~ |




Quali sono i limiti in termini di $H(U)$ $H(V)$ e $H(U,V)$ ai quali si può effettuare TX affidabile?

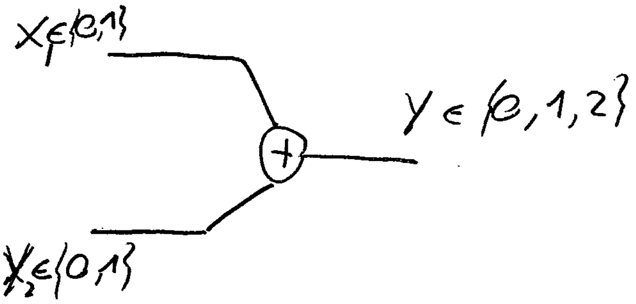
Vale ancora come sol. ottima?



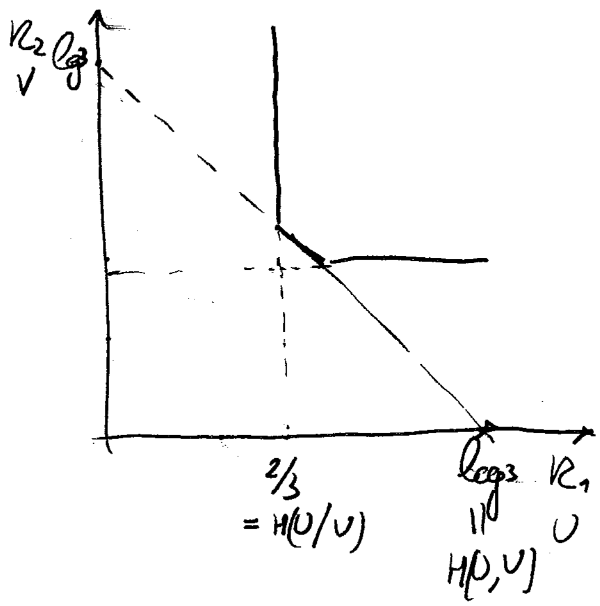
$p(u,v)$

| $u \backslash v$ | 0 | 1 |
|---|---|---|
| 0 | 1/3 | 1/3 |
| 1 | 0 | 1/3 |

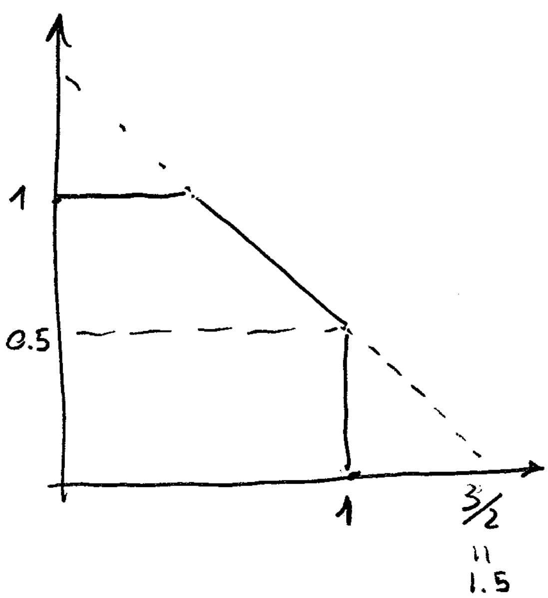
BE-MAC



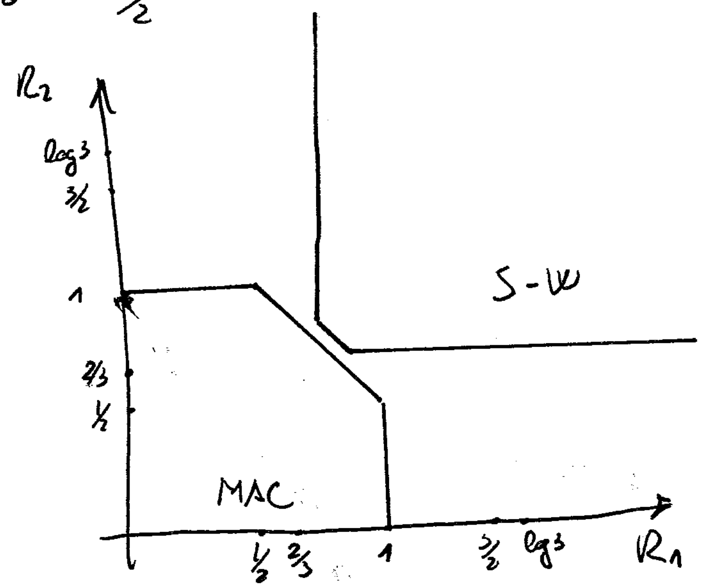

S - W




BE - MAC

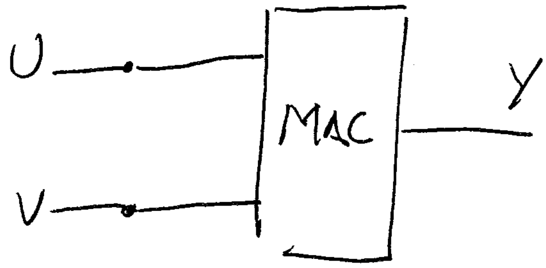


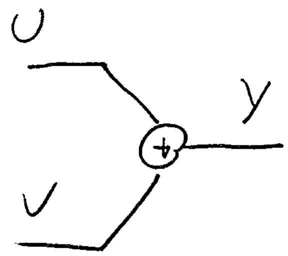

$\log 3 = 1.58 \qquad 3/2 = 1.5$




SEMBRA IMPOSSIBILE . . .

... EPPURE




$Y$

| U \ V | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 2 |

$p(U,V)$

| U \ V | 0 | 1 |
|---|---|---|
| 0 | $\frac{1}{3}$ | $\frac{1}{3}$ |
| 1 | 0 | $\frac{1}{3}$ |

RICEVO $0 \rightarrow \hat{U}=0 \quad \hat{V}=0$

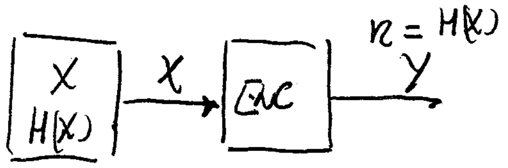
" $2 \rightarrow \hat{U}=1 \quad \hat{V}=1$

" $1 \ldots \rightarrow \hat{U}=0 \quad \hat{V}=1 \quad \left(p(U=1, V=0 \mid Y=1)=0\right)$

SI PUÒ !

(SPIEGAZIONE: MAC prevede ingressi indip.
per questo rende $I(X_1,X_2;Y)$ non può
essere max da ingressi indipendenti...)

# Cenni sull'entropia di sequenze compresse




Come appare la sequenza $\{Y_i\}$ ?

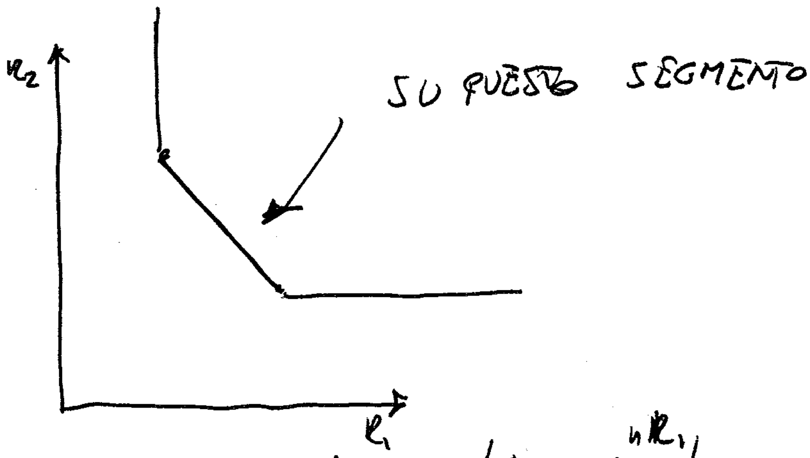
- Sicuramente non può essere ulteriormente compressa

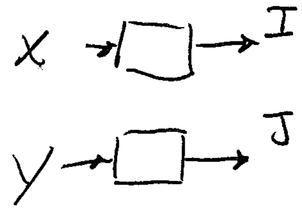
$x \in \mathcal{X} \qquad y \in \mathcal{Y} = \{y_1, \dots, y_D\}$

$Y$ deve essere $\sim$ Unif. $\{y_1, \dots, y_D\}$ altrimenti $H(Y) < \log D$ ed è comprimibile

$\{Y_i\}$ devono essere i.i.d. altrimenti $H(\mathcal{Y}) < \log D$

Nel caso DSC

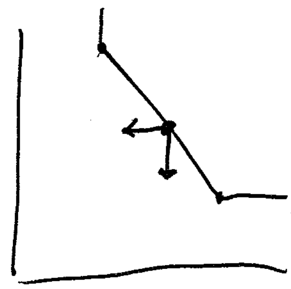



$I$ e $J$ unif. su $\{1, \dots, 2^{nR_1}\}$ e $\{1, \dots, 2^{nR_2}\}$ risp

e i.i.d.

altrimenti, comprimendo



Ex

Si discuta la relazione di dipendenza fra

$\{I_k\}$ e $\{J_k\}$ .