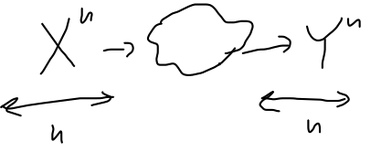
TEOREMA DELLA CODIFICA DI CANALE (PARTE DIRETTA): (informale)

→ { - Sorgente S binaria con entropia $H(S) = 1$
  - Canale binario simmetrico $BSC(\varepsilon)$

→ Per ogni $\delta > 0$ e per ogni valore del tasso $R < C$

esistono dei codici con probabilità di errore $< \delta$

BSC(ε)

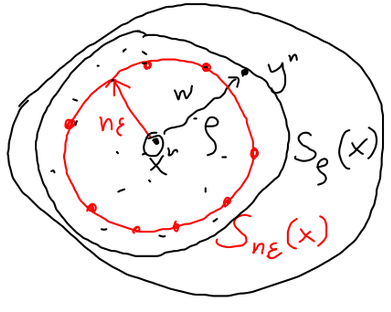


w = # posizioni i $(1 \le i \le n)$ tali che $x_i \neq y_i$

$E w = n \cdot \varepsilon$ $\qquad Var(w) = n\varepsilon(1-\varepsilon)$

Disuguaglianza di Chebyshev:

$$Pr[w > \underbrace{Ew + \alpha}_{\text{soglia}}] \le \frac{Var(w)}{\alpha^2} \qquad \text{per ogni } \alpha > 0$$



A^n

δ = target di prob. di errore

Scelgo $\alpha = \sqrt{\frac{n\varepsilon(1-\varepsilon)}{\delta/2}}$ $\longrightarrow$ $Pr[w > \underbrace{Ew + \alpha}_{n\varepsilon + \alpha}] \le \frac{n\varepsilon(1-\varepsilon)}{n\varepsilon(1-\varepsilon)} \frac{\delta}{2}$

→ Sfera di raggio $\boxed{\rho = \lfloor n\varepsilon + \alpha \rfloor}$

Sia $\mathcal{C}$ il dizionario del codice (insieme delle parole di codice)

Decodifica: quando riceviamo la seq. y, se $x_i \in \mathcal{C}$ è l'unica parola di codice tale che $d_H(y, x_i) \leq \rho$, allora decodifico in x_i.

Altrimenti restituisco errore di decodifica.

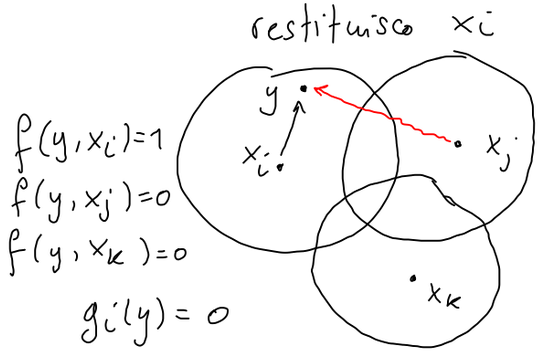
Per due n-ple $u, v \in A^n$:

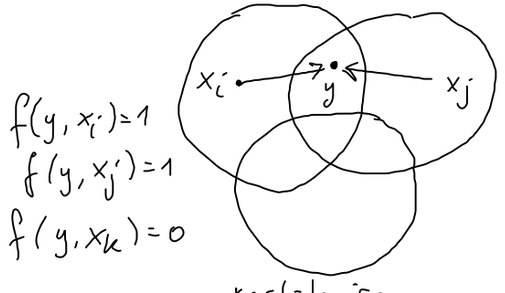
$$f(u,v) \stackrel{def}{=} \begin{cases} 1 & \text{se } d_H(u,v) \leq \rho \\ 0 & \text{se } d_H(u,v) > \rho \end{cases}$$

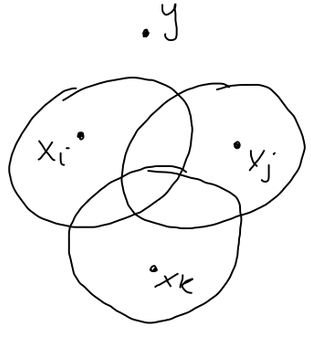
Se $x_i \in \mathcal{C}$, e $y \in A^n$, poniamo:

$$g_i(y) \stackrel{def}{=} 1 - f(y, x_i) + \sum_{j \neq i} f(y, x_j)$$

Se x_i è l'<u>unica</u> parola di codice a distanza $\leq \rho$ da y, allora $g_i(y) = 1 - 1 + \sum 0 = 0$; altrimenti $g_i(y) \geq 1$.







Sia $P^*(M, n, \varepsilon)$ = il minimo della prob. di errore su tutti i possibili codici in funzione di M, n, ε

- M: # parole di codice
- n: lunghezza delle parole di codice
- ε: parametro del canale BSC(ε)

Teorema (4.2) (Teorema diretto di Shannon di codifica di canale).
Se il tasso R è minore della capacità C del canale, allora $P^*(M, n, \varepsilon) \longrightarrow 0$ quando $n \to \infty$.

$(M = 2^{nR})$

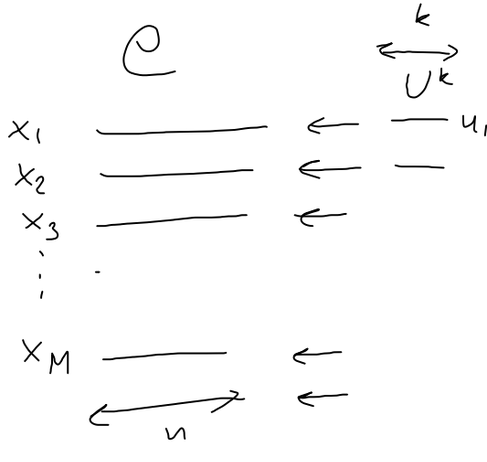
$\left(R = \frac{\log_2 M}{n}\right)$

Dim. Quando viene trasmessa la parola di codice x_i la prob. di errore $P_e(i)$ è al più:

$$P_e(i) \leq \sum_{y \in A^n} p(y|x_i) \cdot g_i(y)$$

$$= \sum_{y \in A^n} p(y|x_i) \left[1 - f(y, x_i) + \sum_{j \neq i} f(y, x_j) \right]$$

$$= \underbrace{\sum_{y \in A^n} p(y|x_i)\left(1 - f(y, x_i)\right)}_{= \sum_{y \notin S_\delta(x_i)} p(y|x_i) \leq \delta/2} + \sum_{y \in A^n} p(y|x_i) \sum_{j \neq i} f(y, x_j)$$



$$P_e(i) \leq \delta/2 + \sum_{y \in A^n} p(y|x_i) \sum_{j \neq i} f(y, x_j)$$

Mediando su tutte le possibili parole di codice $x_1, x_2, \ldots, x_M$,
la prob. di errore (media)

$$P_e = \frac{1}{M} \sum_{i=1}^{M} P_e(i) = \delta/2 + \frac{1}{M} \sum_{i=1}^{M} \sum_{y \in A^n} p(y|x_i) \sum_{j \neq i} f(y, x_j)$$

Considero un codice scelto uniformemente a caso tra tutti i possibili codici con M parole di lunghezza n.

Valutiamo $E[P_e]$

$$P^*(M, n, \varepsilon) \leq E[P_e] \leq \delta/2 + \frac{1}{M} \sum_{i=1}^{M} \sum_{y \in A^n} E[p(y|x_i)] \sum_{j \neq i} E[f(y, x_j)]$$

minimo è ≤ valore atteso

$$= \delta/2 + \frac{1}{M} \sum_{i=1}^{M} \sum_{y \in A^n} \sum_{j \neq i} E[p(y|x_i)] E[f(y, x_j)]$$

$$E[p(y|x_i)] = \sum_{z\in A^n} p(y|z)\,\underbrace{Pr[x_i = z]}_{1/2^n} = \frac{1}{2^n}\sum_{z\in A^n} p(y|z)$$

($A=\{0,1\}$)

$$E[f(y,x_j)] = \sum_{z\in A^n} f(y,z)\,\underbrace{Pr[x_j = z]}_{1/2^n} = \frac{1}{2^n}\sum_{z\in A^n} f(y,z) \le \frac{1}{2^n}\,|S_\rho^{(60000)}|$$

$\sum_{z\in A^n} f(y,z)$ = "numero di elementi della sfera $S_\rho(y)$"

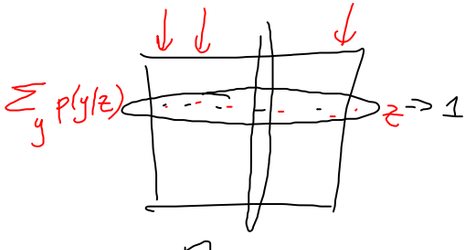
$|S_\rho^{(60000)}|$ = "

$|S_\rho| = |S_\rho|\cdot\frac{1}{2^n}\sum_{z\in A^n} 1$

$|S_\rho(y)| \le 2^{n h_2(\rho/n)}$

$$p^*(M,n,\varepsilon) \le \frac{\delta}{2} + \frac{1}{M}\sum_{i=1}^{M}\sum_{y\in A^n}\sum_{j\neq i}\left[\frac{1}{2^n}\sum_{z\in A^n} p(y|z)\right]\left[\frac{1}{2^n}\sum_{z\in A^n}|S_\rho|\right]$$

$$= \frac{\delta}{2} + \frac{1}{M}\sum_{i=1}^{M} \frac{1}{2^n}|S_\rho|\sum_{j\neq i}\frac{1}{2^n}\sum_{z\in A^n}\underbrace{\sum_{y\in A^n} p(y|z)}_{=1}$$



$$= \frac{\delta}{2} + \frac{1}{M}\frac{1}{2^n}\sum_{i=1}^{M}|S_\rho|\underbrace{\sum_{j\neq i}}_{M-1}\cancel{1}\,\frac{1}{\cancel{2^n}}\underbrace{\sum_{z\in A^n}}_{\cancel{2^n}}\cancel{1} = \frac{\delta}{2} + \frac{1}{2^n M}\sum_{i=1}^{M}|S_\rho|(M-1)$$

$$= \frac{\delta}{2} + \frac{|S_\rho|}{2^n}(M-1)\cdot 1$$

$$p^*(M,n,\varepsilon) \leq \underbrace{\delta/2 + \frac{|S_\rho|}{2^n}}(M-1)$$

$M = 2^{nR}$

$M - 1 < M \qquad \log(M-1) < nR$

$$\log\left(p^*(M,n,\varepsilon) - \delta/2\right) \leq \log|S_\rho| - n + \log(M-1)$$
$$< \log|S_\rho| - n + nR$$
$$\leq n\,h_2(\rho/n) - n + nR$$

$|S_\rho| \leq 2^{n h_2(\rho/n)}$

$\log|S_\rho| \leq n\,h_2(\rho/n)$

$\rho = \lfloor \varepsilon n + \alpha \rfloor$

$$\frac{1}{n}\log\left(p^*(M,n,\varepsilon) - \delta/2\right) \leq h_2(\rho/n) - 1 + R$$

Ho $\rho = \lfloor \varepsilon n + \alpha \rfloor \Rightarrow \rho/n = \frac{\lfloor \varepsilon n + \alpha \rfloor}{n} \xrightarrow{n\to\infty} \varepsilon$

Quindi $h_2(\rho/n)$ è approssimabile con $h_2(\varepsilon)$ per $n \to \infty$ (n suff. grande)

$h_2(\varepsilon) - 1 = -C$

$1 - h_2(\varepsilon) = C$

↑ capacità del canale BSC(ε) !

$$\frac{1}{n}\log\left(p^*(M,n,\varepsilon) - \delta/2\right) \leq \underbrace{R - C}_{\text{costante negativa}} + \xi_n$$

$h_2(\rho/n) = h_2(\varepsilon) + \xi_n$ ← infinitesimo

Per n suff. grande,

$\leq -\beta$ ← $\beta > 0$ costante

$$\frac{1}{n} \log \left(P^*(M, u, \varepsilon) - \delta/2 \right) \leq -\beta$$

$$P^*(M, u, \varepsilon) \leq \delta/2 + \underbrace{2^{-\beta n}}$$

(per ogni n suff. grande)

può essere reso piccolo a piacere scegliendo n suff. grande;

$$\Rightarrow \leq \delta/2 + \delta/2 = \delta.$$

in particolare scelgo n tale che $2^{-\beta n} < \delta/2$

$\Rightarrow$ la prob. di errore può essere reso piccola a piacere.