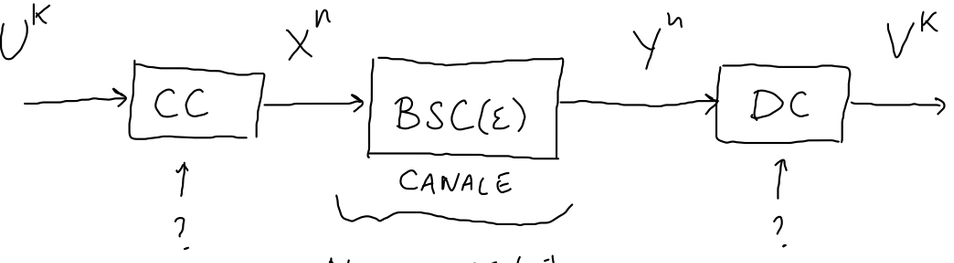
TEOREMA DELLA CODIFICA DI CANALE (PARTE DIRETTA): (informale)

Per ogni $\delta > 0$ e per ogni valore del tasso $R < C$ (capacità del canale), esiste almeno un codice con tasso R e probabilità d'errore $< \delta$.



Numero di bit errati atteso: $n \cdot \varepsilon$

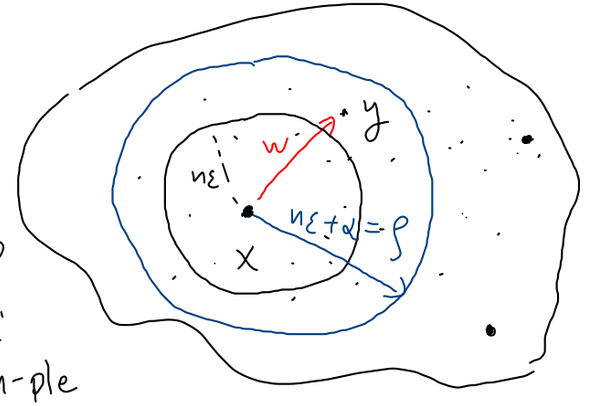
$W \triangleq$ v.a. che indica il numero di bit di Y^n diversi da i corrispondenti bit di X^n

$E[W] = n\varepsilon$

$\rightarrow Pr[\, W > E[W] + \alpha \,] \leq \delta/2$ $\qquad \alpha \triangleq \sqrt{\frac{n\varepsilon(1-\varepsilon)}{\delta/2}}$

prob. che $y \notin S_{\lfloor n\varepsilon + \alpha \rfloor}(x) = S_\rho(x)$

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

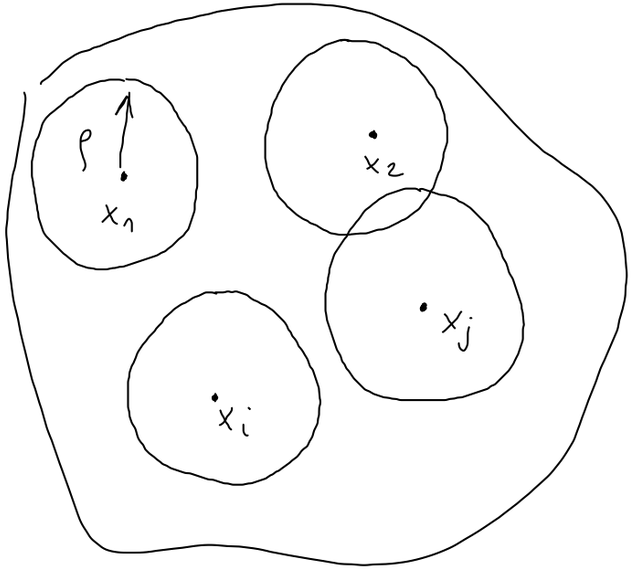


Insieme di tutte le n-ple sull'alfabeto del codice

Sia $\mathcal{C}$ il dizionario del codice (insieme delle parole di codice); lo definiamo più avanti.

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

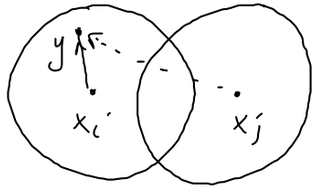
Altrimenti restituisco errore.



Per due n-ple u, v:

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

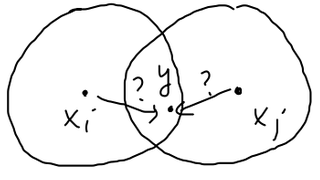
Esempio:



→ Decodifico y come x_i.

$f(y, x_i) = 1$, $f(y, x_j) = 0$

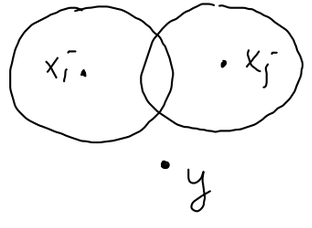
Esempio:



→ Restituisco errore di decodifica

$f(y, x_i) = 1$, $f(y, x_j) = 1$

Esempio:



→ Restituisco errore di decodifica

$f(y, x_i) = 0$, $f(y, x_j) = 0$

Se $x_i \in \mathcal{C}$ e y è una qualunque n-pla, poniamo:

$$g_i(y) \triangleq 1 - f(y, x_i) + \sum_{j : j \neq i} f(y, x_j)$$

→ Se x_i è l'unica parola di codice con $d_H(y, x_i) \leq \rho$,

allora $g_i(y) = 1 - 1 + 0 = 0$

Altrimenti $g_i(y) \geq 1$.

Sia $P^*(M, n, \varepsilon)$ = minimo delle probabilità di errore P_e su tutti i codici con M parole di codice, lunghezza n, sul canale $BSC(\varepsilon)$

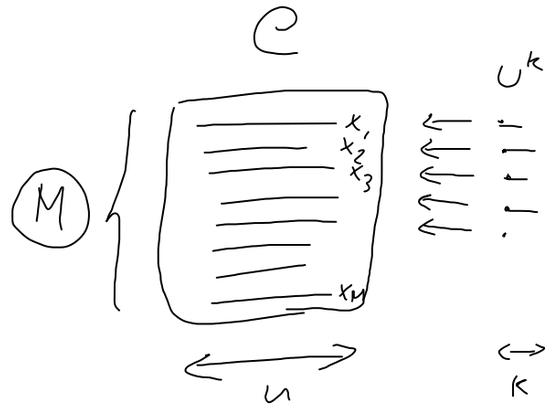
- M: Numero delle parole di codice ($M = |\mathcal{C}|$)
- n: Lunghezza delle parole di codice
- ε: Parametro di errore del canale $BSC(\varepsilon)$

Teorema (4.2) (Teorema diretto di Shannon di codifica di canale).

Se il tasso R è $< C = 1 - h_2(\varepsilon)$, e $M = 2^{nR}$ $\left(R = \frac{\log_q M}{n}\right)$

allora $P^*(M, n, \varepsilon) \to 0$ quando $n \to \infty$.

Dim. Quando viene trasmessa sul canale la parola di codice x_i,
la probabilità d'errore $P_e(i)$ è al più:



$$P_e(i) \le \sum_{y \in 2^n} Pr[y|x_i] \cdot g_i(y) =$$

(tutte le possibili n-ple binarie)

$$= \sum_{y \in 2^n} Pr[y|x_i] \left(1 - f(y, x_i) + \sum_{j \neq i} f(y, x_j)\right)$$

$$= \underbrace{\sum_{y \in 2^n} Pr[y|x_i] \left(1 - f(y, x_i)\right)}_{\text{Prob. che } y \notin S_\delta(x_i) \le \delta/2} + \sum_{y \in 2^n} Pr[y|x_i] \sum_{j \neq i} f(y, x_j)$$

Mediando $P_e(i)$ su tutte le parole di codice x_i (ciascuna delle quali ha probabilità $1/M$)

$$P_e = \frac{1}{M} \sum_i P_e(i) \le \underbrace{\frac{1}{M} \sum_{i=1}^{M} \frac{\delta}{2}}_{\frac{1}{M} \cdot M \cdot \delta/2} + \frac{1}{M} \sum_{i=1}^{M} \sum_{y \in 2^n} Pr[y|x_i] \sum_{j \neq i} f(y, x_j)$$

P_e: Prob di errore media

Ripetiamo il ragionamento per tutti i codici possibili e, per un codice scelto a caso, valutiamo $E[P_e]$

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

$$E[Pr[y|x_i]] = \sum_{z\in 2^n} Pr[y|z]\cdot \underbrace{Pr[x_i=z]}_{1/2^n} = \frac{1}{2^n}\sum_{z\in 2^n} Pr[y|z]$$

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

$\to$ $|S_\rho(y)|$ non dipende da y!

$$\to P^*(M,n,\varepsilon) \le \frac{\delta}{2} + \frac{1}{M}\sum_{i=1}^{M}\sum_{y\in 2^n}\sum_{j\neq i} \frac{|S_\rho(000\ldots0)|}{2^n}\cdot\frac{1}{2^n}\sum_{z\in 2^n} Pr[y|z]$$

$$\sum_{z\in 2^n}\sum_{y\in 2^n} Pr[y|z] = 2^n \quad (\text{ogni } z \text{ contribuisce } 1)$$

$$= \frac{\delta}{2} + \frac{1}{M}\sum_{i=1}^{M}\sum_{j\neq i}\frac{|S_\rho(000\ldots0)|}{2^n} = \frac{\delta}{2} + \frac{1}{M}\,M\,(M-1)\,\frac{|S_\rho|}{2^n}$$

$M \quad M-1$

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

← tutte le sfere di raggio ρ hanno la stessa cardinalità

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

$$\leq \frac{1}{n}\log M - 1 + h_2(\rho/n)$$

$$= \underbrace{\frac{1}{n}\log M}_{R \text{ (tasso)}} - \underbrace{(1 - h_2(\rho/n))}$$

↖ $|S_\rho| \leq 2^{n h_2(\rho/n)}$

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

$C = 1 - h_2(\varepsilon)$

Quando $n \to \infty$ ho $\rho/n = \frac{\lfloor n\varepsilon + \alpha \rfloor}{n} \to \varepsilon$ e quindi $1 - h_2(\rho/n) \to 1 - h_2(\varepsilon) = C$

Quindi per n sufficientemente grande,

$$\frac{1}{n}\log\left(P^*(M,n,\varepsilon) - \delta/2\right) < \underbrace{R - C}_{\text{Per ipotesi, } R<C} + \underbrace{\xi_n}_{\text{infinitesimo}} < \underbrace{-\beta}_{\text{costante}} < 0 \Rightarrow P^*(M,n,\varepsilon) < \frac{\delta}{2} + 2^{-\beta n}$$

↑ può essere resa arbitrariamente piccola, scegliendo δ piccolo, n grande

→ QED