TEOREMA DELLA CODIFICA DI SORGENTE

CODICI <u>B - LV</u> ; Quando <u>$n = 1$</u>

$\mathcal{S}$ $X_1 X_2 X_3 \dots \longrightarrow \varphi(X_1), \varphi(X_2), \dots$

$\qquad\qquad\qquad\qquad\qquad\;\; \overset{\Uparrow}{w} \qquad\; \overset{\Uparrow}{w}$

Tasso : $R = \dfrac{\mathbb{E}[L]}{n}$; $n = 1 \rightarrow R = \mathbb{E}[L]$

1) Per <u>ogni codifica</u> , $\mathbb{E}[L] \geq H_D(\mathcal{S})$ $\longrightarrow$ $H_D(\mathcal{S}) = H_D(X_1)$
D-aria

2) <u>Esiste una</u> codifica (Shannon-Fano) D-aria tale che : $\mathbb{E}[L] \leq H_D(\mathcal{S}) + 1$

Codifica con blocchi di lunghezza $n \geq 1$

Alfabeto : $\mathcal{A}^n$ Sorgente "estesa" : $\mathcal{S}^n$ (1 simbolo di $\mathcal{S}^n$ corrisponde a n simboli di $\mathcal{S}$)

← lunghezza della codifica di 1 simbolo di $\mathcal{S}^n$

1) Per ogni codifica D-aria , $\mathbb{E}[L^{(n)}] \geq H_D(\mathcal{S}^n) = H_D(X_1, X_2, X_3, \dots, X_n)$

$$= n \cdot H_D(X_1) = n\, H_D(\mathcal{S})$$

$$\Longrightarrow \quad \frac{\mathbb{E}[L^{(n)}]}{n} \geq H_D(\mathcal{S}) \quad \longrightarrow \quad \text{Per ogni codifica, il tasso } R \text{ è} \geq H_D(\mathcal{S})$$

Tasso R

2) Esiste una codifica tale che : $\mathbb{E}[L^{(n)}] \leq H_D(S^n) + 1 = n H_D(S) + 1$

$$\rightarrow R = \frac{\mathbb{E}[L^{(n)}]}{n} \leq H_D(S) + \frac{1}{n}$$

In particolare, per una codifica ottimale (= a tasso minimo), ho:

$$H_D(S) \leq R \leq H_D(S) + 1/n$$

$\rightarrow$ Il tasso di una codifica ottimale tende a $H_D(S)$ quando $n \to \infty$

Codici B-B

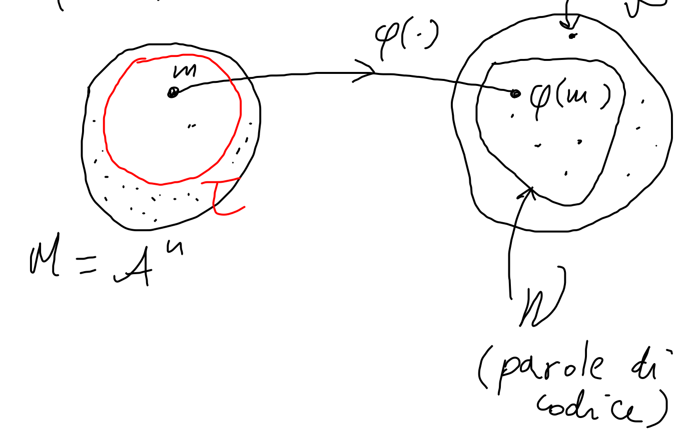
$\mathcal{A} = \{a_1, \ldots, a_K\}$ blocchi di lungh. n

$\mathcal{B} = \{b_1, \ldots, b_D\}$ blocchi di lungh. ℓ

$\varphi : \mathcal{M} = \mathcal{A}^n \longrightarrow \mathcal{B}^\ell$

$\mathcal{W} = \varphi(\mathcal{M}) \subseteq \mathcal{B}^\ell$

seq. che non è una parola di codice



Per avere u.d. della codifica, φ deve essere iniettiva; quindi serve che

$$|\mathcal{B}^\ell| \geq |\mathcal{A}^n|$$

$$D^\ell \geq K^n \iff \ell \geq \log_D(K^n) = n \log_D K$$

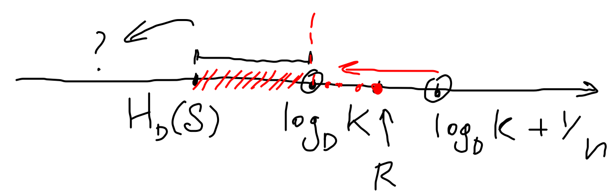
Inoltre ℓ deve essere un intero; $\iff \ell \geq \lceil n \log_D K \rceil$

Per qualunque codice, il tasso è

$$R \geq \frac{\lceil n \log_D K \rceil}{n}$$; Se $\ell = \lceil n \log_D K \rceil$, ho

$$\frac{n \log_D K}{n} \leq R = \frac{\lceil n \log_D K \rceil}{n} \leq \frac{n \log_D K + 1}{n} = \log_D K + \frac{1}{n}$$

$$H_D(S) \leq \underline{\log_D} K \leq R \leq \underline{\log_D} K + 1/n$$



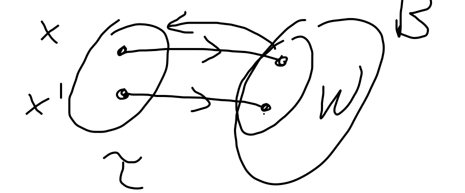
Codifica : $\varphi : \mathcal{M} \to \mathcal{B}^\ell$ Decodifica : $\psi : \mathcal{B}^\ell \to \mathcal{M}$

Ho un errore di decodifica quando $\psi(\varphi(m)) \neq m$

$$P_{err} := \Pr_X[\psi(\varphi(X)) \neq X]$$

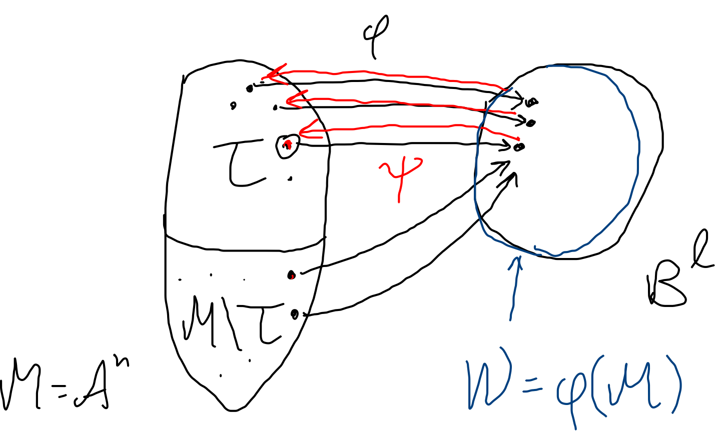
X ← v.a. che indica il blocco generato dalla sorgente (blocco di lunghezza n)

$$\mathcal{T} := \{x \in \mathcal{A}^n : \psi(\varphi(x)) = x\}$$



Tutte le n-ple in $\mathcal{T}$ hanno associate parole di codice distinte

Quindi $|\mathcal{T}| \leq |\mathcal{B}^\ell|$



$$P_{err} = 1 - \Pr[\psi(\varphi(X)) = X]$$
$$= 1 - \Pr[X \in \mathcal{T}]$$

Vorrei : $\mathcal{T}$ con cardinalità $\leq |\mathcal{B}^\ell|$

$\mathcal{T}$ deve raccogliere una alta probabilità :

$$\Pr[X \in \mathcal{T}] \approx 1$$

(in modo tale che $P_{err} \approx 0$)

Tasso del codice : $R = \frac{\mathbb{E}[L]}{n} = \frac{l}{n}$; $l = \lceil \log_D |\mathcal{T}| \rceil$

$\rightarrow R = \frac{\lceil \log_D |\mathcal{T}| \rceil}{n}$ (per questo motivo vorrei $|\mathcal{T}|$ piccola)

Scelgo $\mathcal{T} = \mathcal{T}^{(u,\delta)}$ (insieme delle sequenze (u,δ)-tipiche) per qualche $\delta > 0$

$= \left\{ x \in \mathcal{A}^n : \left| \frac{1}{n} \mathcal{I}(x) - H_D(\mathcal{S}) \right| \leq \delta \right\}$

Avevamo dimostrato che $\Pr[X \in \mathcal{T}^{(u,\delta)}] = \underline{1 - \varepsilon}$ con $\varepsilon = \varepsilon(u,\delta) \xrightarrow{n \to \infty} 0$

Inoltre $(1-\varepsilon) 2^{n(H_2(\mathcal{S}) - \delta)} \leq |\mathcal{T}^{(u,\delta)}| \leq 2^{n(H_2(\mathcal{S}) + \delta)}$

$2^{H_2(\mathcal{S})} = (2^{\log_2 D})^{H_D(\mathcal{S})} =$

$= D^{H_D(\mathcal{S})}$

$\rightarrow (1-\varepsilon) D^{n(H_D(\mathcal{S}) - \delta')} \leq |\mathcal{T}^{(u,\delta)}| \leq D^{n(H_D(\mathcal{S}) + \delta')}$

$\delta' = (\log_2 D)\, \delta$

$\delta > 0$

$\delta' > 0$

Per essere sicuri che $\mathcal{B}^l$ riesca a contenere $|\mathcal{T}^{(u,\delta)}|$ elementi,

prendiamo l : $D^l \geq D^{n(H_D(\mathcal{S}) + \delta')}$ $\rightarrow l = \lceil n(H_D(\mathcal{S}) + \delta') \rceil$

Per quanto mostrato sopra, prob. di errore è $P_{err} = 1 - P_r[X \in T]$

$$= 1 - (1 - \varepsilon) = \varepsilon \xrightarrow[n \to \infty]{} 0$$

Il tasso del codice è

$$R = \frac{\ell}{n} = \frac{\lceil n H_D(S) + \delta' \rceil}{n} < \frac{n H_D(S) + \delta' + 1}{n} = H_D(S) + \frac{\delta' + 1}{n}$$

Esiste una codifica B-B D-aria con prob. di errore P_{err} infinitesima e tasso $R \xrightarrow[n \to \infty]{} H_D(S)$

Se invece volessimo: $R \leq H_D(S) - 2\delta'$:

$$R = \frac{\ell}{n} \leq H_D(S) - 2\delta' \rightarrow \ell \leq n(H_D(S) - 2\delta') \longrightarrow D^{\ell} \leq D^{n(H_D(S) - 2\delta')}$$

Allora $P_r[X \in T^{(n,\delta)}$ e X viene correttamente decodificata$] \leq$ (Prob. max di 1 messaggio in $T^{(n,\delta)}$) $\times$

$\times$ (numero di messaggi correttamente decodificati)

$$= \underbrace{D^{-n(H_D(S)-\delta')}}_{\substack{\text{prob. max di 1} \\ \text{messaggio in } \mathcal{T}^{(n,\delta)}}} \cdot D^{n(H_D(S)-2\delta')} =$$

$$= \cancel{D^{-nH}}\, \cancel{D^{+nH}}\; D^{n\delta'}\, D^{n(-2\delta')} = D^{-n\delta'}$$ esponenzialmente piccolo

$$Pr(\text{corretta decodifica}) \leq \underbrace{Pr(\text{corr. decodifica e } X \in \mathcal{T}^{(n,\delta)})}_{D^{-n\delta'}} + \underbrace{Pr(\text{corr. decodifica e } X \notin \mathcal{T}^{(n,\delta)})}_{\varepsilon = \varepsilon(n,\delta)}$$

$$\leq D^{-n\delta'} + \varepsilon = \varepsilon(n,\delta)$$

$\longrightarrow 0$ quando $n \to \infty$

Analisi asintotica; cosa succede per n finito?