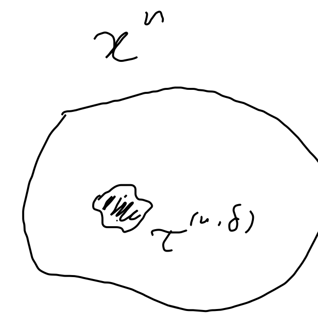
SEQUENZE TIPICHE IN PROBABILITÀ

δ $\quad \vec{x} \in \mathcal{X}^n$ $\quad p(\vec{x})$ $\quad \geq 1-\varepsilon$



Def.:

$\vec{x} \in \mathcal{X}^n$ è (n,δ)-tipica in probabilità se $\left| \frac{1}{n} \underbrace{\mathcal{I}(\vec{x})}_{}^{-\log p(\vec{x})} - H(\vec{p}) \right| \leq \delta$.

Autoinformazione di $\vec{x}$ è $\mathcal{I}(\vec{x}) \overset{def}{=} -\log p(\vec{x})$
$= -\log \Pr[X^n = \vec{x}]$

L'insieme delle sequenze (n,δ)-tipiche è denotato $\mathcal{T}^{(n,\delta)} \subseteq \mathcal{X}^n$

Teo 3.5. Consideriamo $\mathcal{T}^{(n,\delta)}$. Allora:

(a) Probabilità di una sequenza tipica: $\forall \vec{x} \in \mathcal{T}^{(n,\delta)}$: $\quad 2^{-n[H(\vec{p})+\delta]} \leq p(\vec{x}) \leq 2^{-n[H(\vec{p})-\delta]}$

(b) Numerosità delle sequenze tipiche: $(1-\varepsilon) 2^{n[H(\vec{p})-\delta]} \leq |\mathcal{T}^{(n,\delta)}| \leq 2^{n[H(\vec{p})+\delta]}$

(a) $\vec{x}$ è (n,δ)-tipica $\iff$ $\delta \geq -\frac{1}{n} \log p(\vec{x}) - H(\vec{p}) \geq -\delta$

$$H(\vec{p}) + \delta \geq -\frac{1}{n} \log p(\vec{x}) \geq H(\vec{p}) - \delta$$

$a \leq b$
$\Downarrow$
$2^a \leq 2^b$

$p(\vec{x}) \approx 2^{-nH(\vec{p})}$

$$-n[H(\vec{p})+\delta] \leq \log p(\vec{x}) \leq -n[H(\vec{p})-\delta]$$

$$2^{-n[H(\vec{p})+\delta]} \leq p(\vec{x}) \leq 2^{-n[H(\vec{p})-\delta]}.$$

(b) Limitaz. superiore

$$1 \geq \sum_{\vec{x} \in \tau^{(n,\delta)}} p(\vec{x}) \geq |\tau^{(n,\delta)}| \overbrace{\min_{\vec{y} \in \tau^{(n,\delta)}} p(\vec{y})}^{p(\vec{x}) \geq} \overset{(a)}{\geq} |\tau^{(n,\delta)}| \cdot \underbrace{2^{-n[H(\vec{p})+\delta]}}$$

$$\Leftrightarrow \quad |\tau^{(n,\delta)}| \leq 2^{+n[H(\vec{p})+\delta]}$$

$H(\vec{p}) \leq \log K$
$=$ sse $\vec{p}$ è uniforme

Limitaz. inferiore

$$1-\varepsilon \leq \sum_{\vec{x} \in \tau^{(n,\delta)}} p(\vec{x}) \leq |\tau^{(n,\delta)}| \cdot \max_{\vec{y} \in \tau^{(n,\delta)}} p(\vec{y}) \overset{(a)}{\leq} |\tau^{(n,\delta)}| \cdot 2^{-n[H(\vec{p})-\delta]}$$

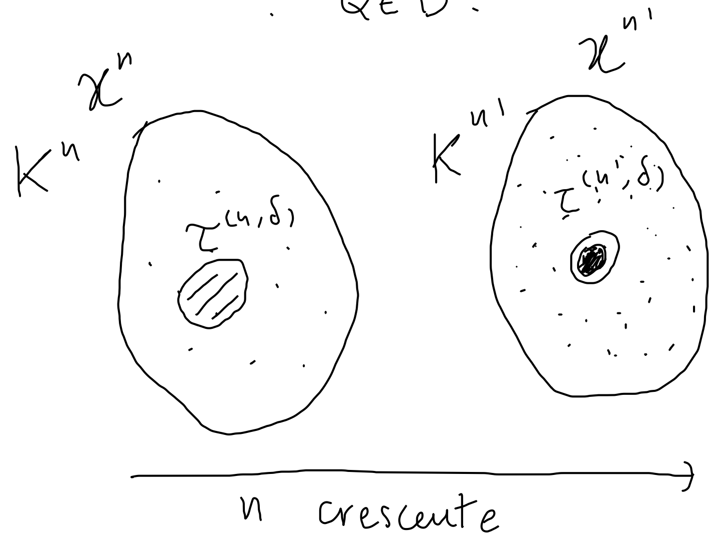
$$\Leftrightarrow \quad |\tau^{(n,\delta)}| \geq (1-\varepsilon)\, 2^{+n[H(\vec{p})-\delta]} \quad .$$ QED.

$\log K > H(\vec{p})+\delta$

$$|\tau^{(n,\delta)}| \approx 2^{nH(\vec{p})}$$

$$\underbrace{p(\vec{x}) \approx 2^{-nH(\vec{p})}}$$

$$[\, 2^{-nH-\delta} \,,\; 2^{-nH+\delta} \,]$$



$n' > n$

$$\frac{|\tau^{(n,\delta)}|}{K^n} \leq \frac{2^{n[H(\vec{p})+\delta]}}{2^{n \log K}} =$$

$$= 2^{-n[\underbrace{\log K - H(\vec{p}) - \delta}_{>0}]} \xrightarrow[n\to\infty]{} 0$$

Per n grande, una sorgente stazionaria senza memoria emette quasi esclusivamente solo sequenze tipiche (principio di equipartizione asintotica)

Esempio. $n = 100$, $K = 2$

$-0.89 \log 0.89 - 0.11 \log 0.11$

$\vec{p} = (p_0, p_1) = (0.89, 0.11)$ $\quad H(\vec{p}) = 0.499\ldots \simeq 0.5$

$E[\text{peso}(\vec{x})] = n \cdot p_1$

$= 100 \cdot 0.11$

$= \underline{11}$

Fissiamo $\delta = 0.061 \rightarrow \mathcal{T}^{(n,\delta)} = \mathcal{T}^{(100,\, 0.061)}$

$\vec{x} \in \{0,1\}^{100}$ $\quad 2^{-100[0.5+0.061]} \leq p(\vec{x}) \leq 2^{-100[0.5-0.061]}$

$$\boxed{1.295 \cdot 10^{-17} \leq p(\vec{x}) \leq 6.029 \cdot 10^{-14}}$$

dove $\vec{x}$ ha esattamente j "1"

$$\boxed{p(\vec{x}) = 0.89^{n-j} \cdot 0.11^{j}}$$

dove j è il numero di "1" in $\vec{x}$ (peso di $\vec{x}$)

Ci sono $\binom{n}{j}$ tali sequenze. Calcolando $p(\vec{x})$ per $j = 0, 1, \ldots, 100$

$j = 8$: $p(\vec{x}) \simeq 4.73 \cdot 10^{-13}$: troppo grande

$j = 9$: $p(\vec{x}) \simeq 5 \cdot 10^{-14}$: OK

$\vdots$

$j = 13$: $p(\vec{x}) \simeq 1.3 \cdot 10^{-17}$: OK

$j = 14$: $p(\vec{x}) \simeq 1.5 \cdot 10^{-18}$: troppo piccola

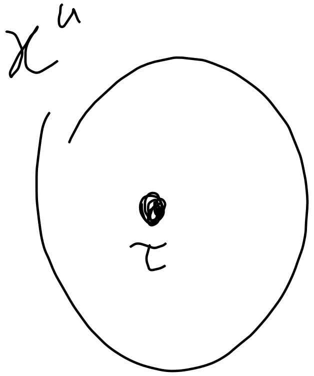
$\mathcal{T}^{(n,\delta)}$ consiste di tutte le sequenze lunghe 100 di peso compreso tra $\underline{9}$ e $\underline{13}$

La prob. totale $\Pr[X^n \in \mathcal{T}^{(n,\delta)}] = \sum_{\vec{x} \in \mathcal{T}} p(\vec{x}) = \sum_{j=9}^{13} \binom{n}{j} 0.89^{n-j}\, 0.11^{j}$

$$\simeq \boxed{0.576}$$

$$\frac{|\mathcal{T}^{(n,\delta)}|}{K^n} = \frac{\sum_{j=9}^{13}\binom{n}{j}}{2^n} \simeq \frac{8.32 \cdot 10^{15}}{2^{100}} \cong \frac{8.32 \cdot 10^{15}}{10^{30}} \approx 10^{-15}$$

$$2^{10} = 1024 \cong 10^3$$



TIPICITÀ IN COMPOSIZIONE (più stringente)

Basata sul "tipo" di una sequenza:

$$(\underset{\substack{\uparrow \\ \#\text{ di } x_1}}{n_1}, \underset{\substack{\uparrow \\ \#\text{ di } x_2}}{n_2}, n_3, \dots, \underset{\substack{\uparrow \\ \#\text{ di } x_K}}{n_K}) \text{ è il tipo di } \vec{x}$$

\# di sequenze di tipo $(n_1, \dots, n_K)$ sono $\displaystyle\binom{n}{n_1, n_2, \dots, n_K} = \frac{n!}{n_1!\, n_2! \cdots n_K!}$

$$n_1 + n_2 + \dots + n_K = n$$

CODIFICA DI SORGENTE

Alfabeto della sorgente (primario)

$\mathcal{A} = \{a_1, \dots, a_K\}$

$\mathcal{A}^+$: insieme delle sequenze finite di simboli di $\mathcal{A}$

$\xrightarrow{\text{codifica}}$

Alfabeto del canale (secondario)

$\mathcal{B} = \{b_1, \dots, b_D\}$

(Spesso $D=2$ e $K > D$)

$\mathcal{B}^+$: ins. delle sequenze finite di simboli di $\mathcal{B}$

- Per non perdere informaz., il codice dev'essere univocamente decodificabile (u.d.):

  la codifica deve essere invertibile

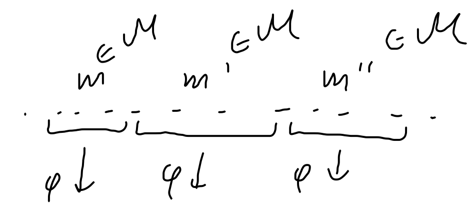
- Possibilmente, il rapporto tra la lungh. (media) delle seq. secondarie e la lunghezza (media) delle seq. primarie deve essere piccolo (per efficienza)

Concatenazione di sequenze $*$ $\qquad \alpha_1, \alpha_2 \in \mathcal{A}^+ \Rightarrow \alpha_1 * \alpha_2 \in \mathcal{A}^+$

Codice astratto: funzione $\varphi : A^+ \to B^+$ che sia un omomorfismo:

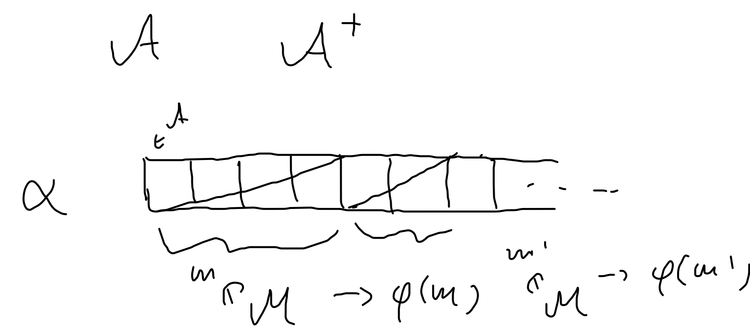
$$\varphi(\alpha_1 * \alpha_2) = \varphi(\alpha_1) * \varphi(\alpha_2)$$

(La codifica di una concatenaz. è la concatenaz. delle codifiche)



Insieme finito $\mathcal{M} = \{m_1, \ldots m_T\} \subseteq A^+$ di <u>messaggi</u>

(se $\mathcal{M} = A$, i messaggi sono singole lettere dell'alfabeto)



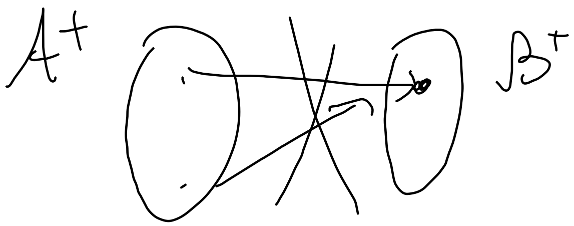
Insieme di parole di codice $\mathcal{W} = \{\varphi(m_1), \ldots, \varphi(m_T)\} \subseteq B^+$

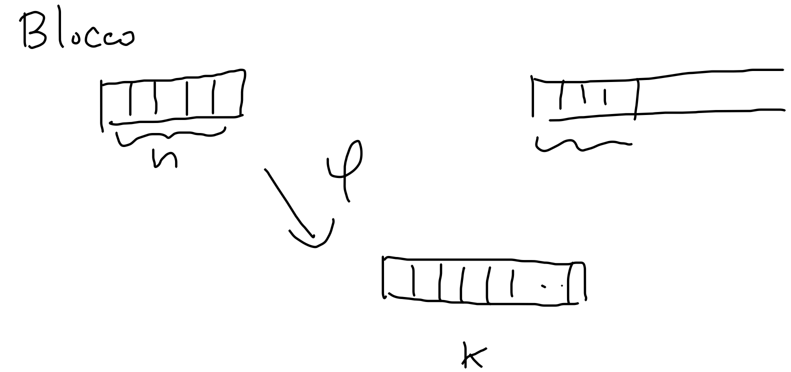
(dizionario delle parole di codice)

Un codice è una terna $C = (\mathcal{M}, \varphi, \mathcal{W})$.

Def. Un insieme di messaggi $\mathcal{M}$ è esauriente se per ogni sequenza α semi-infinita a destra costruita su A, esiste almeno un prefisso di α che appartiene a $\mathcal{M}$.

Def. Il codice $\mathcal{C} = (\mathcal{M}, \varphi, \mathcal{W})$ è detto univocamente decodificabile (u.d.) quando φ è iniettiva: $\alpha \neq \beta \Rightarrow \varphi(\alpha) \neq \varphi(\beta) \quad \forall \alpha, \beta \in \mathcal{A}^+$.





Tipi di codici di sorgente

* - Blocco-blocco (B-B): $\mathcal{M} = \mathcal{A}^n$, per qualche $n \geq 1$ (tutti i messaggi sono blocchi a lunghezza costante n)

  Anche le parole di codice (elementi di $\mathcal{W}$) hanno lunghezza costante (l'esaurienza è garantita)

* - Blocco - lunghezza variabile (B-LV): $\mathcal{M} = \mathcal{A}^n$

  Le parole di codice hanno lunghezza variabile (l'esaurienza garantita)

- LV - B
- LV - LV