TEOREMA DELLA CODIFICA DI SORGENTE PER CODICI BLOCCO-BLOCCO (B-B)

Sia $\delta' > 0$. Sorgente (s.s.m.) $\mathcal{S}$

Parte diretta: Se fissiamo il tasso $R \geq H_D(\mathcal{S}) + \delta'$, allora esiste una famiglia di codici (B-B) per $\mathcal{S}^n$, $\underbrace{C^1, C^2, \ldots, C^n, \ldots}$, con una probabilità $P_{err}^{(n)}$ tale che $\lim_{n \to \infty} P_{err}^{(n)} = 0$

Parte inversa: Se $R \leq H_D(\mathcal{S}) - 2\delta'$, allora per qualunque famiglia di codici B-B per $\mathcal{S}^n$, la prob. $P_{err}^{(n)}$ è tale che $\lim_{n \to \infty} P_{err}^{(n)} = 1$.

Cosa succede per n finito?

CODICI DI SORGENTE (Cap. 5)

Codici B-LV. (simbolici) ($n=1$) $\qquad \mathcal{A} = \{a_1, \dots, a_K\}$ $\qquad \mathcal{B} = \{b_1, \dots, b_D\}$ $\qquad$ Lunghezze delle $\{w_i\}$

$$p = (p_1, \dots, p_K) \qquad \mathcal{W} = \{w_1, \dots, w_K\} \qquad \mathcal{L} = \{\ell_1, \dots, \ell_k\}$$

Codice $\mathcal{C}$ $\to$ il tasso $R(\mathcal{C}) = \dfrac{\mathbb{E}[L]}{1} = \mathbb{E}[L]$.

Esempio: Codifica di Shannon-Fano: associa ad ogni a_i una parola di codice di lunghezza $\ell_i = \lceil -\log_D p_i \rceil$.

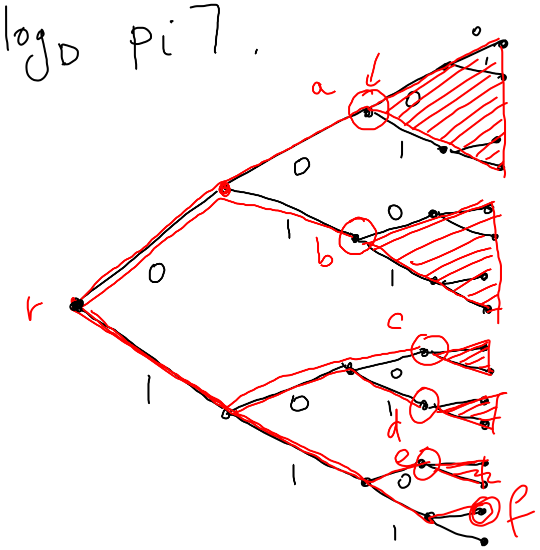
Esempio.

- $\mathcal{A} = \{a, b, c, d, e, f\}$
- $p = (4/16,\ 4/16,\ 3/16,\ 2/16,\ 2/16,\ 1/16)$

$D = 2 \quad (\mathcal{B} = \{0, 1\})$

$\varphi : \mathcal{M} \to \mathcal{B}^+$, $\quad \mathcal{M} \equiv \mathcal{A}$

$$\ell_a = \lceil -\log 4/16 \rceil = \lceil \log 4 \rceil = 2 \qquad \ell_d = 3$$
$$\ell_b = 2 \qquad \ell_e = 3$$
$$\ell_c = 3 \qquad \ell_f = 4$$



a	00
b	01
c	100
d	101
e	110
f	1110 $\to$ 111

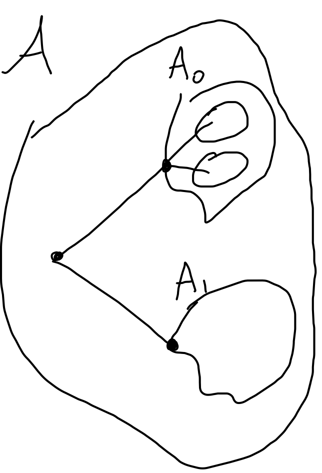
$$\mathbb{E}[L] = \tfrac{4}{16}\cdot 2 + \tfrac{4}{16}\cdot 2 + \tfrac{3}{16}\cdot 3 + \tfrac{2}{16}\cdot 3 + \tfrac{2}{16}\cdot 3 + \tfrac{1}{16}\cdot 4$$
$$= \tfrac{41}{16}.$$

In questo esempio, la codifica di Shannon-Fano non è <u>ottima</u>.

(Codice C^* è ottimo <u>in una classe di codici</u>

se $R(C^*) \leq R(C)$ per ogni codice C nella classe).

Se modifico la codifica di f : $\varphi(f) = 111$, ottengo $\mathbb{E}[L] = 40/16 < 41/16$.



Codifica di Fano. Partizioniamo A in due sottoinsiemi A_0 e A_1 : $A_0 \cup A_1 = A$, $A_0 \cap A_1 = \emptyset$

in modo tale da minimizzare $\left| \sum_{i \in A_0} p_i - \sum_{i \in A_1} p_i \right|$

Continuo: partiziono $A_0 = A_{00} \cup A_{01}$ sempre con lo stesso criterio

$A_1 = A_{10} \cup A_{11}$

finché tutti gli insiemi non contengono un singolo elemento.

Esempio. Stessa sorgente di prima; sei simboli, $p = \left(\frac{4,\ 4,\ 3,\ 2,\ 2,\ 1}{16}\right)$

Passo 1

4	a	A_0: 8	0	00 (A_{00})	$\boxed{00}$
4	b		0	01 (A_{01})	$\boxed{01}$
3	c	A_1: 8	1	10 (A_{10})	$\boxed{100}$ (A_{100})
2	d		1	11 (A_{11})	$\boxed{110}$
2	e		1	11	$\boxed{111}$
1	f		1	10 (A_{10})	$\boxed{101}$

$$\mathbb{E}[L] = 2 \cdot 8/16 + 3 \cdot 8/16 = 40/16$$

In questo caso, la codifica di Fano ha una lungh. attesa inferiore della codifica di Shannon-Fano.

Però, in generale, la codifica di Fano non è ottima.

Lemma (5.1). Sia (senza perdita di generalità) $p_1 \geq p_2 \geq \dots \geq p_K$ (altrimenti riordino)

Allora esiste un codice ottimo C^* (nella classe dei codici u.d.) ~~a prefisso~~ tale che:

→ (1) Se $p_j > p_K$ si ha $l_j \leq l_K$ (e dunque $l_1 \leq l_2 \leq \dots \leq l_K$)

→ (2) Se $l_K = |w_K|$ è la lunghezza massima, esiste un'altra parola di codice w_j di lunghezza l_K, e che differisce da w_K solo per l'ultimo simbolo

Dim. Consideriamo un qualunque codice C^* ottimo.

Costruiamo un altro codice C' scambiando w_j con w_K.

	C^*	C'
a_1	w_1	w_1
a_2	w_2	w_2
$\vdots$	$\vdots$	$\vdots$
a_j	w_j	w_K
$\vdots$	$\vdots$	$\vdots$
a_K	w_K	w_j

Allora $0 \leq \mathbb{E}[L'] - \mathbb{E}[L^*] = \sum_i p_i l_i' - \sum_i p_i l_i =$

per ipotesi, C^* è ottimo $\mathbb{E}[L^*] \leq \mathbb{E}[L']$

$$= p_j l_K + p_K l_j - (p_j l_j + p_K l_K)$$

$$= p_j (l_K - l_j) - p_K (l_K - l_j) =$$

$$= \underbrace{(p_j - p_K)}_{\substack{>0 \\ \text{per ipotesi}}} (l_K - l_j)$$

$(l_K - l_j)$ Deve essere $\geq 0 \implies l_K \geq l_j$

$\left.\begin{array}{l} 01001 \\ 01000 \end{array}\right\}$ quelle

Essendo C^* u.d., esso soddisfa la disuguaglianza di McMillan-Kraft.

Quindi esiste un codice a prefisso con le stesse lunghezze di C^*.

Se non esistesse w_j con $|w_j| = |w_K|$,

si potrebbe elidere l'ultimo di w_K, senza violare la proprietà del prefisso.

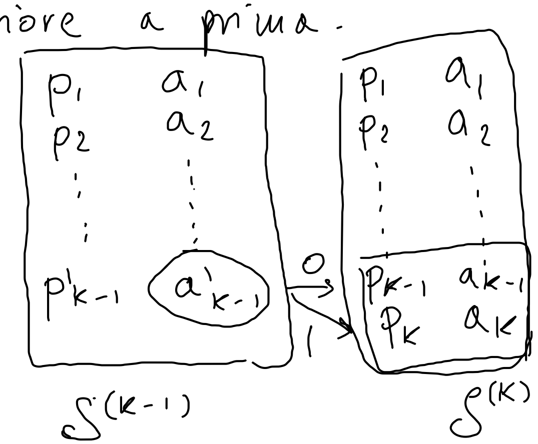
Ma il codice sarebbe a lunghezza attesa inferiore a prima.

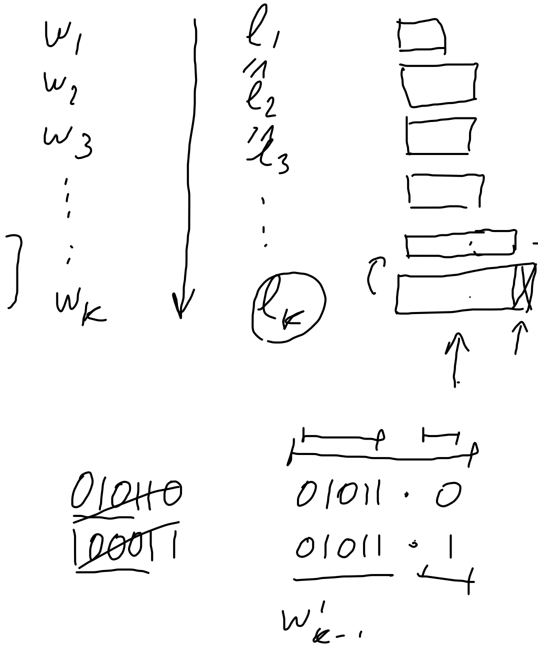
Quindi esiste w_{K-1} con $|w_{K-1}| = |w_K|$.

Costruisco una sorgente "ridotta" $S^{(K-1)}$

aggregando i due simboli a_K e a_{K-1} di

probabilità minima.





Posso ottenere un codice a prefisso per $S^{(K)}$

partendo da un codice a prefisso per $S^{(K-1)}$;

Sia w'_{K-1} la parola di codice per a'_{K-1}; ottengo $w_{K-1} = w'_{K-1} \cdot 0$, $w_K = w'_{K-1} \cdot 1$

Teorema 5.1. Se il codice a prefisso $\mathcal{C}^{(k-1)}$ è ottimo per la sorgente ridotta $\mathcal{S}^{(k-1)}$, allora il codice $\mathcal{C}^{(k)}$ descritto come sopra è ottimo per la sorgente $\mathcal{S}^{(k)}$.

Dim. Se il codice a prefisso $\mathcal{C}^{(k-1)}$ è ottimo per $\mathcal{S}^{(k-1)}$

$l_{k-1} = l_k$

$$R(\mathcal{C}^{(k)}) = \mathbb{E}[L(\mathcal{S}^{(k)})] = \sum_{i=1}^{k} p_i l_i = \sum_{i=1}^{k-2} p_i l_i + (p_{k-1} l_{k-1}) + (p_k l_k)$$

$$= \sum_{i=1}^{k-2} p_i l_i + \underbrace{(p_{k-1} + p_k)}_{p'_{k-1}} l_k$$

p'_{k-1} prob. del simbolo aggregato

$$= \sum_{i=1}^{k-2} p_i l_i + p'_{k-1} \cdot (l'_{k-1} + 1)$$

$$= \underbrace{\sum_{i=1}^{k-2} p_i l_i + p'_{k-1} l'_{k-1}}_{\mathbb{E}[L(\mathcal{S}^{(k-1)})] \,=\, R(\mathcal{C}^{(k-1)})} + p'_{k-1}$$

non dipende da come scelgo il codice $\mathcal{C}^{(k-1)}$

$\Rightarrow$ minimizzare $R(\mathcal{C}^{(k)})$ è equivalente

a " $R(\mathcal{C}^{(k-1)})$

Algoritmo di Huffman. (caso binario)

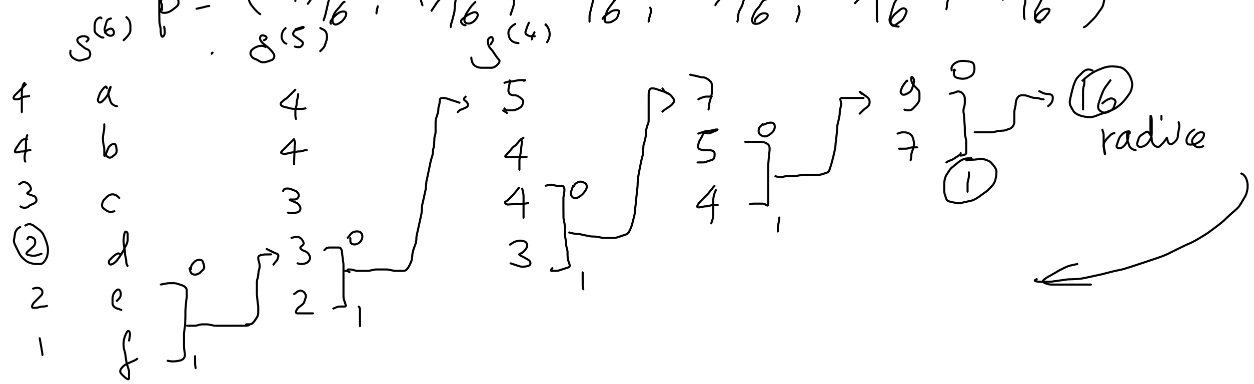
- Ordina i simboli per probabilità non crescenti
- Accorpa i 2 simboli meno probabili
- Trova ricorsivamente un codice (ottimo) per $S^{(k-1)}$
- Estendi il codice $S^{(k-1)}$ apponendo '0'/'1' per distinguere i simboli a_{k-1} e a_k alla parole di codice per il simbolo aggregato.

(La codifica di Huffman è ottima nella classe dei codici u.d.:

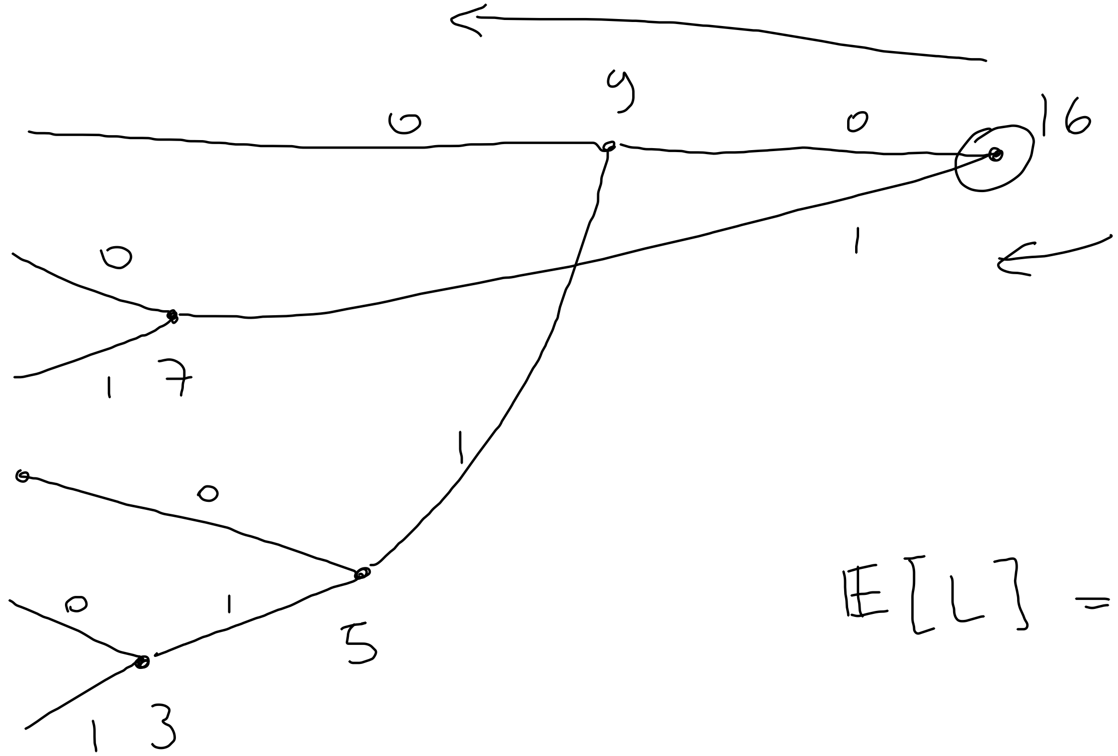
$$R(C^{Huff.}) \le R(C) \quad \forall C \text{ u.d.}$$

Esempio. $\mathcal{A} = \{a, b, c, d, e, f\}$

$$p = \left(4/16,\ 4/16,\ 3/16,\ 2/16,\ 2/16,\ 1/16 \right)$$



00	a	4
10	b	4
11	c	3
010	d	2
0110	e	2
0111	f	1



$E[L] = 40/16$