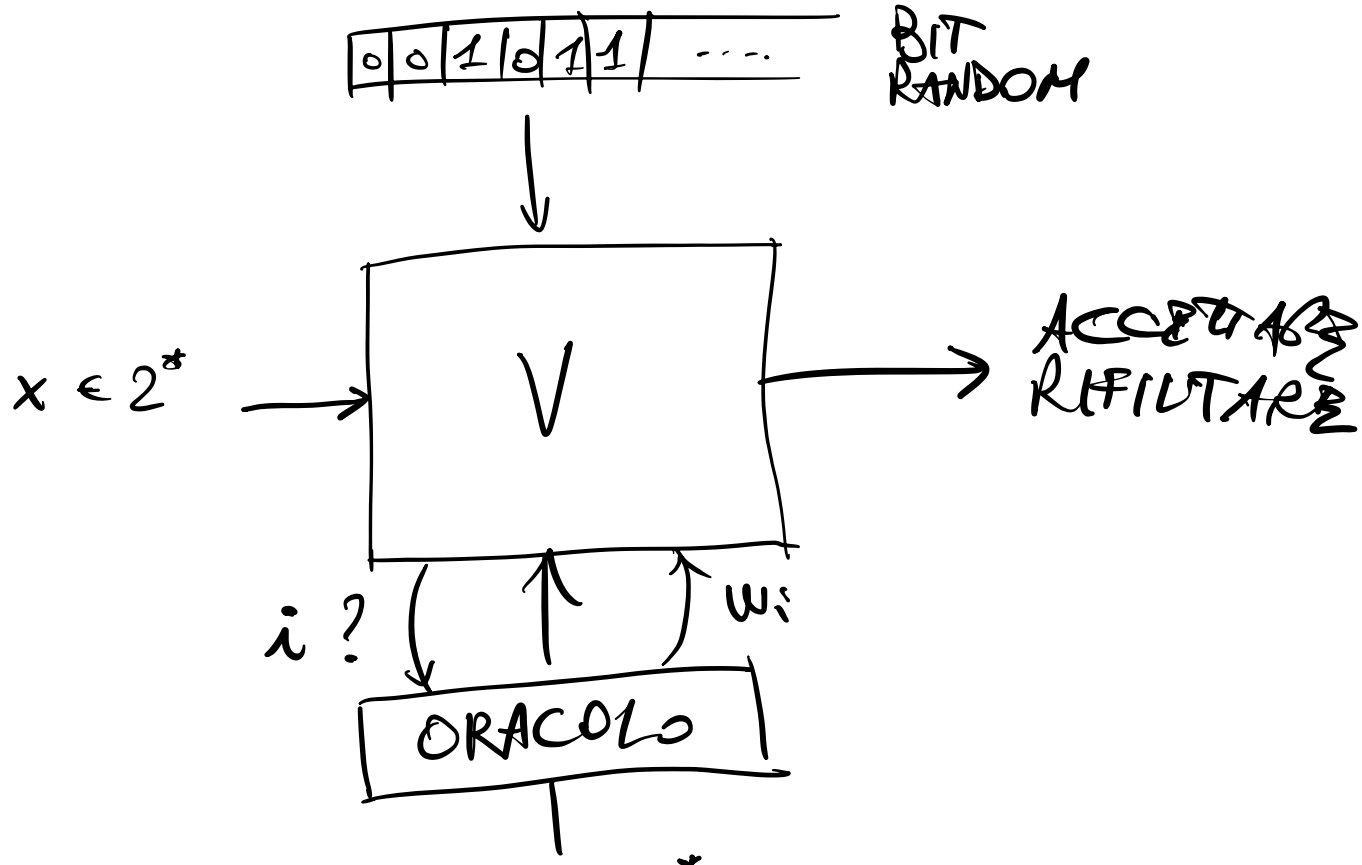
VERIFICATORE PROBABILISTICO



Un linguaggio $L \subseteq 2^*$ è accettato da V sse

1) $\forall x \in L \quad \exists w \in 2^*$
t.c. $P[V \text{ accetti } x, \text{ avendo come testimone } w] = 1$

2) $\forall x \notin L \quad \forall w \in 2^*$
$P[V \text{ accetti } x, \text{ avendo come testimone } w] < \frac{1}{2}$

Fissate due funzioni $r(n)$, $q(n)$ chiamiamo

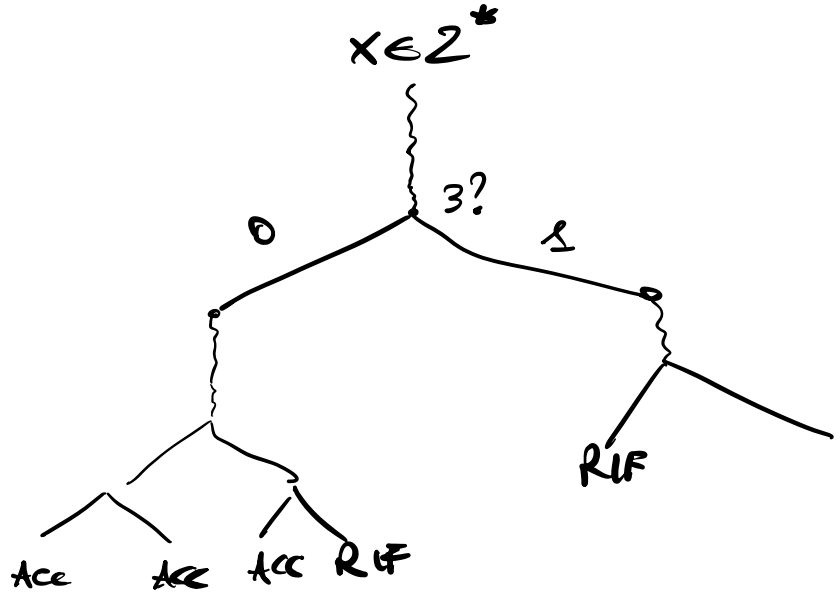
$PcP[r,q] = L \subseteq 2^*$ t.c. esiste un verificatore probabilistico

dove

1) V in tempo polinomiale
2) accetta L
3) su input di lungh. n fa al più $r(n)$ query e estrae al più $r(n)$ bit ciascuna

$$PCP[0,0] = P$$

$$PCP[0, Poly] = \bigcup_{Q(n) \in Poly} PCP[0, Q] = NP$$



Teorema: (Arora + Safra, 1998)

$$NP = PCP[O(\log n), O(1)]$$

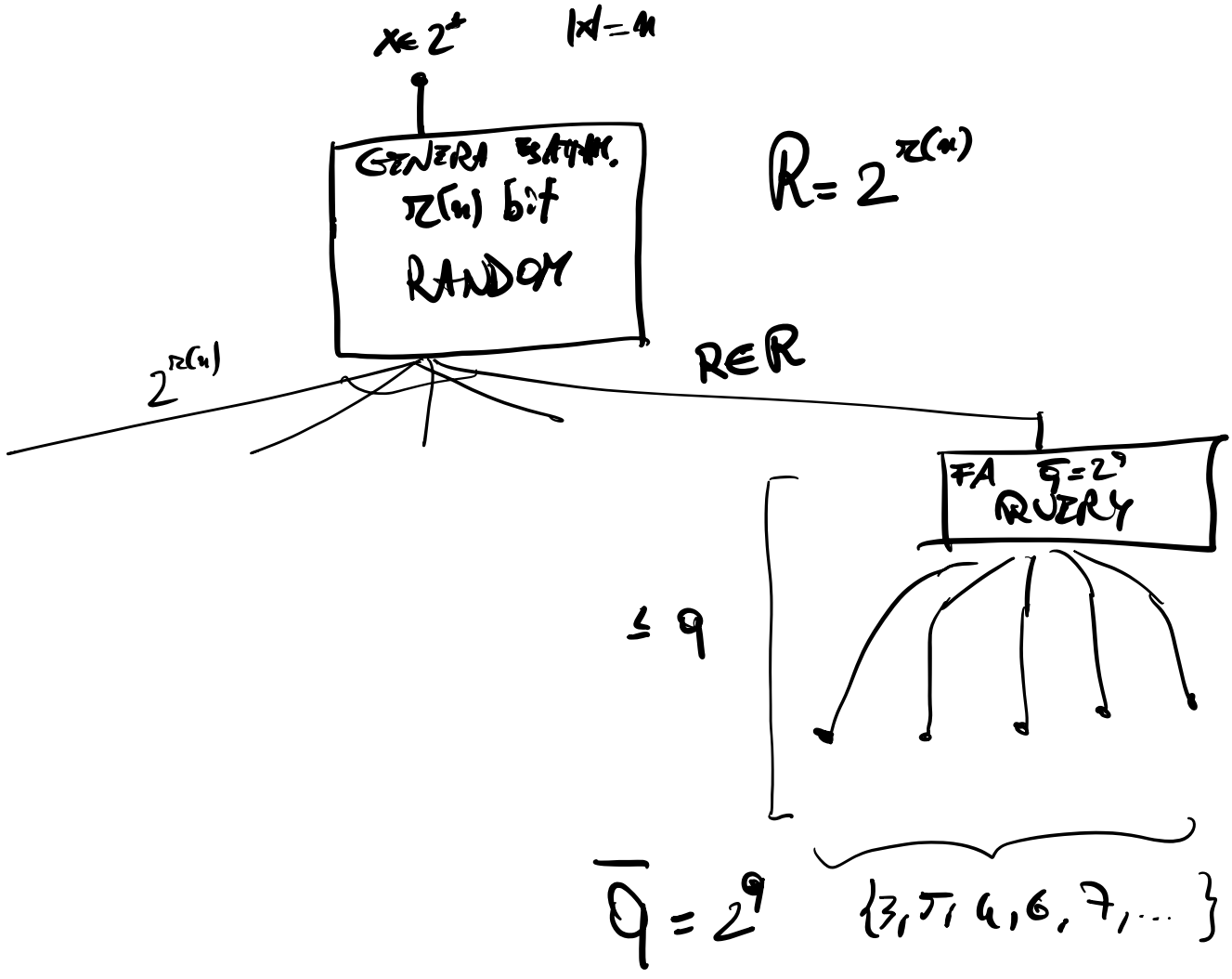
Contr. $NP = PCP[0, Poly]$

VERIFICATORI CANONICI

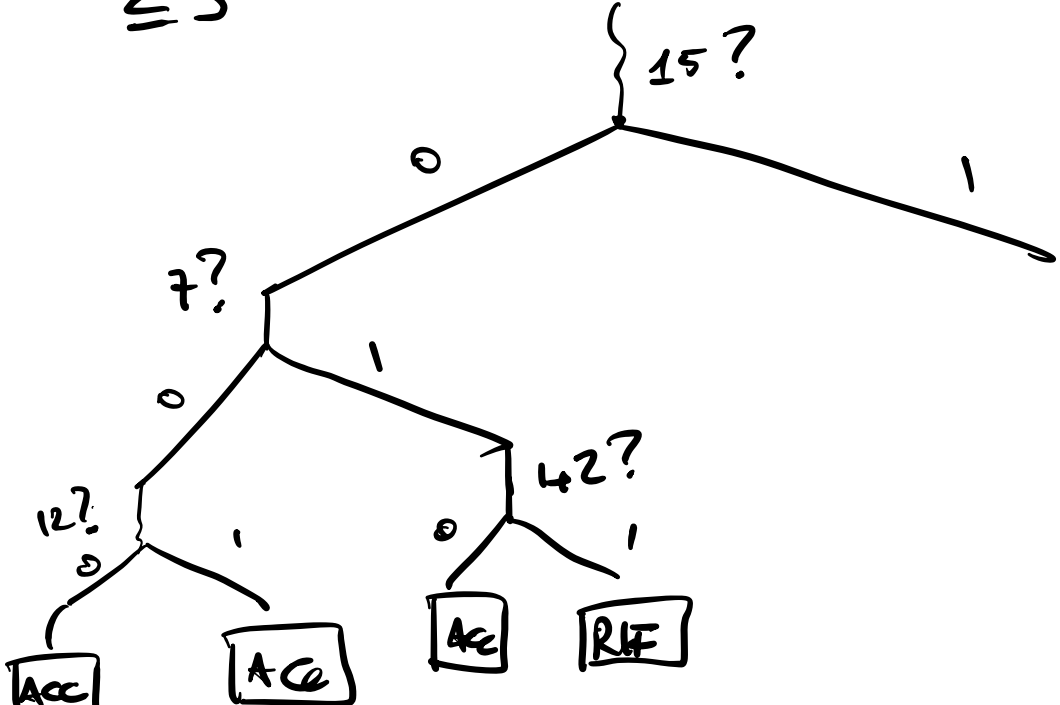
$PCP[r(n), q]$

$r(n) \in O(\log n)$

$q \in \mathbb{N}$



≤ 3



$L \in NP = PCP[r(n), q]$ $\quad r(n) \in O(\log n)$, $q \in \mathbb{N}$

Verificatore canonico

Su input $z \in 2^*$

$R = 2^{r(|z|)} \qquad R \in \mathcal{R}$

$f^{z,R}(w_{i_1}^{z,R}, \dots, w_{i_q}^{z,R}) = \begin{cases} acc. \\ rif. \end{cases}$

Possiamo scrivere una CNF φ_z^R soddisf. sse (z,R) viene accettata

in cui le variabili $x_1, x_2, x_3, \dots$ rappresentano i valori di w nelle varie posizioni,

$x_i = false$ sse $w_i = 0$

$x_i = true$ sse $w_i = 1$

$x_{i_1^{z,R}}, x_{i_2^{z,R}}, \dots, x_{i_q^{z,R}}$

$z = 010010$ $\quad r(6) = 3$ $\quad q = 3$

$R = \{000, 001, 010, \boxed{011}, \dots 111\}$

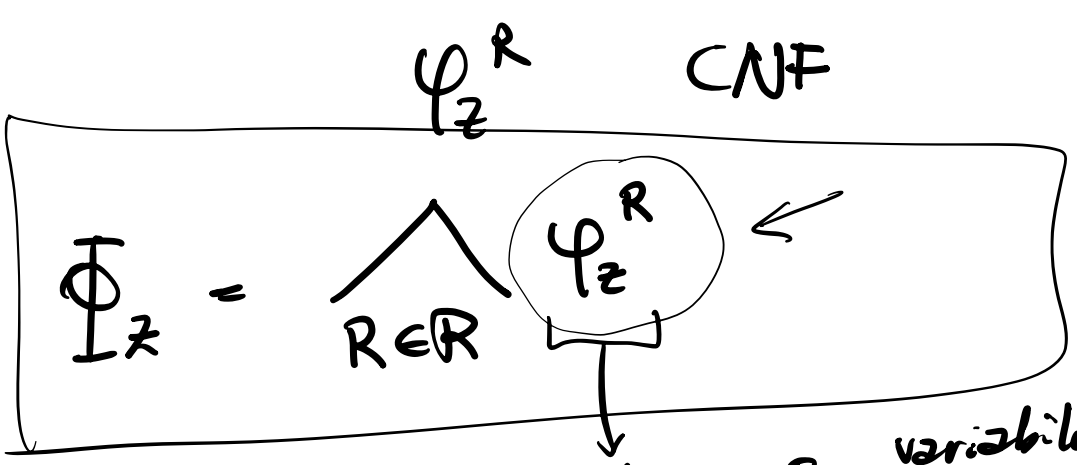
R

$z = 010010$ $\quad R = 011$

75? —
12? —
24? —

75?	12?	24?	ACCETTI
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
0	0	0	0
0	0	1	0
1	1	0	0
1	1	1	1
1			

$$\varphi_2^R = \left(\overline{x_{75}} \wedge x_{12} \wedge x_{24}\right) \vee \left(x_{75} \wedge x_{12} \wedge x_{24}\right)$$



CNF contiene 9 variabili

$\Rightarrow 2^{29}$ clausole

$z \in L$

$\exists w$ che fa accettare con prob. 1

Φ_z è soddisfacibile

$\Rightarrow$ Possiamo rendere vere **$|R| 2^{29}$** clausole

$z \notin L$

$\forall w$ accettiamo con probabilità $< \frac{1}{2}$

$\Rightarrow$ #clausole soddisfatte

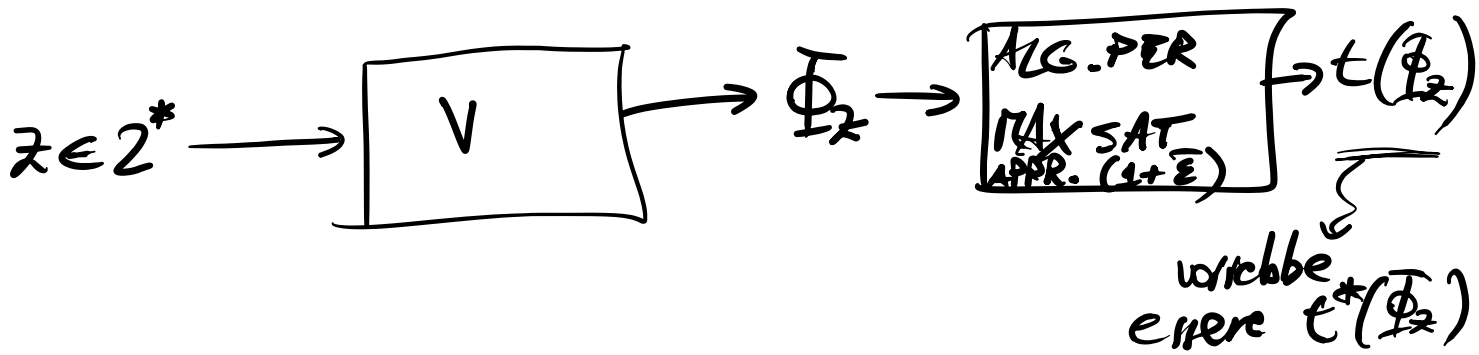
$$< \frac{|R|}{2} 2^{29} + \frac{|R|}{2}\left(2^{29} - 1\right)$$

Teorema: Esiste $\bar{\varepsilon} > 0$ t.c. MAX SAT non è $(1+\bar{\varepsilon})$-approssimabile

Dim: Sia $L \in NPC$, $L = PCP[r(n), q]$ con $r(n) \in O(n)$, $q \in \mathbb{N}$

V

$$\bar{\varepsilon} = \frac{1}{2^{29+1}}.$$



$$z \in L \Rightarrow t^*(\Phi_z) = |R| 2^{29}$$

$$z \notin L \Rightarrow t^*(\Phi_z) \leq \frac{|R|}{2} 2^{29} + \frac{|R|}{2}(2^{29}-1) =$$

$$= 2^{29}|R| - \frac{|R|}{2}$$

$$t(\Phi_z) \geq \frac{t^*(\Phi_z)}{1+\bar{\varepsilon}} = \frac{t^*(\Phi_z)}{1 + \frac{1}{2^{29+1}}}$$

Se $z \in L$

$$t(\Phi_z) \geq \frac{|R| 2^{29}}{1 + \frac{1}{2^{29+1}}} \triangleq A$$

Se $z \notin L$

$$t(\Phi_z) \leq t^*(\Phi_z) \leq 2^{29}|R| - \frac{|R|}{2} \triangleq B$$

$$A - B = \frac{|R|\,2^{29}}{1+\frac{1}{2^{29+1}}} - 2^{29}|R| + \frac{|R|}{2} =$$

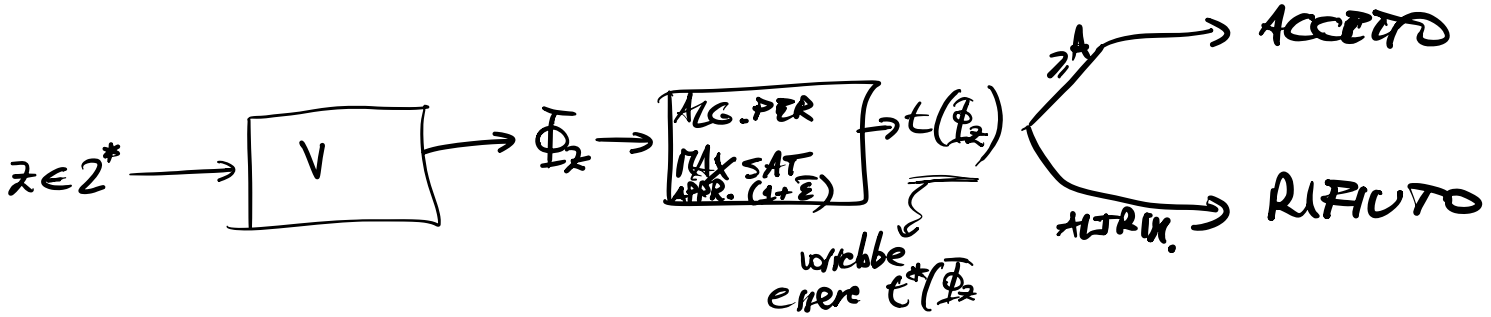
$$= |R| \; \frac{2^{29+1} - 2^{29+1}\left(1+\frac{1}{2^{29+1}}\right) + \left(1+\frac{1}{2^{29+1}}\right)}{2\left(1+\frac{1}{2^{29+1}}\right)} =$$

$$= |R| \; \frac{2^{29+1} - 2^{29+1} - 1 + 1 + \frac{1}{2^{29+1}}}{2\left(1+\frac{1}{2^{29+1}}\right)} > 0$$

$$A > B$$

Se $z \in L$, $t(\Phi_z) \geq A$

Se $z \notin L$, $t(\Phi_z) \leq B$



Polinom.

DECIDO EL . □