CLASSE $PCP[r, q]$

$r, q: \mathbb{N} \to \mathbb{N}$

$PCP[r, q]$ è la classe dei linguaggi $L \subseteq 2^*$ t.c. esiste un probabilistic checker V

1) V lavora in tempo polinomiale in $|x|$
2) V effettua al più $q(|x|)$ query
3) V estrae al più $r(|x|)$ bit random
4) Sia $x \in 2^*$
   - se $x \in L$ $\exists w \in 2^*$ t.c. $P[V(x,w) = YES] = 1$
   - se $x \notin L$ $\forall w \in 2^*$ $P[V(x,w) = YES] \leq \frac{1}{2}$

NOTE

- $PCP[0, 0] = P$
- $PCP[0, Poly] = NP$

Teorema: (Arora, Safra 1998)

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

$L \in NP$

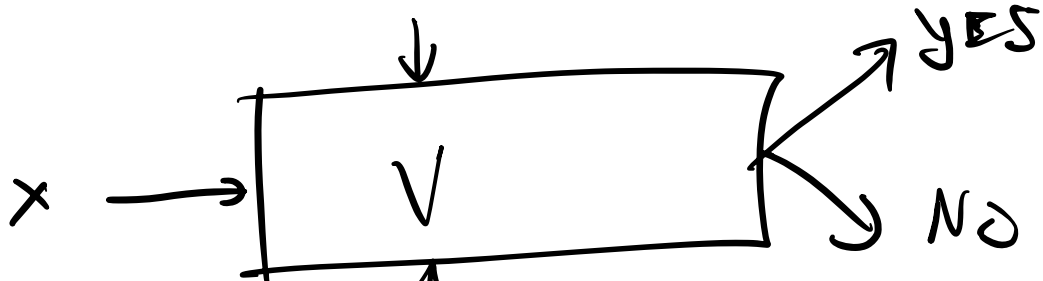
$\exists q \in \mathbb{N}$ $\exists r(n) \in O(\log n)$

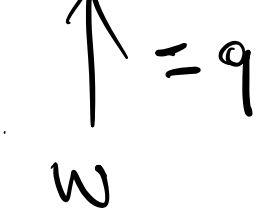
t.c. L è in $PCP[r(n), q]$

VERIFICATORI IN FORMA NORMALE

L è in $PCP[r(n), q]$

$R \in 2^{r(n)}$

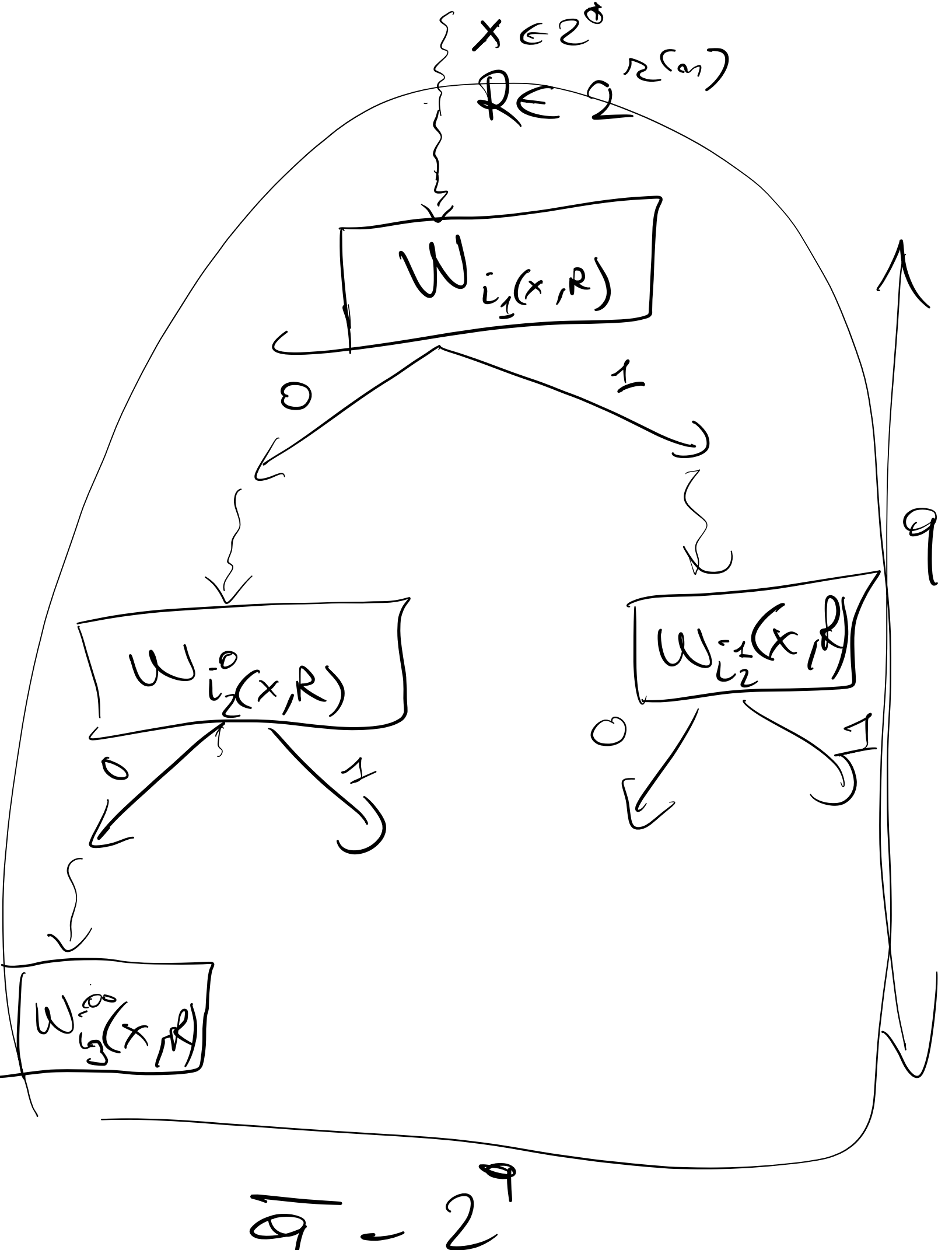


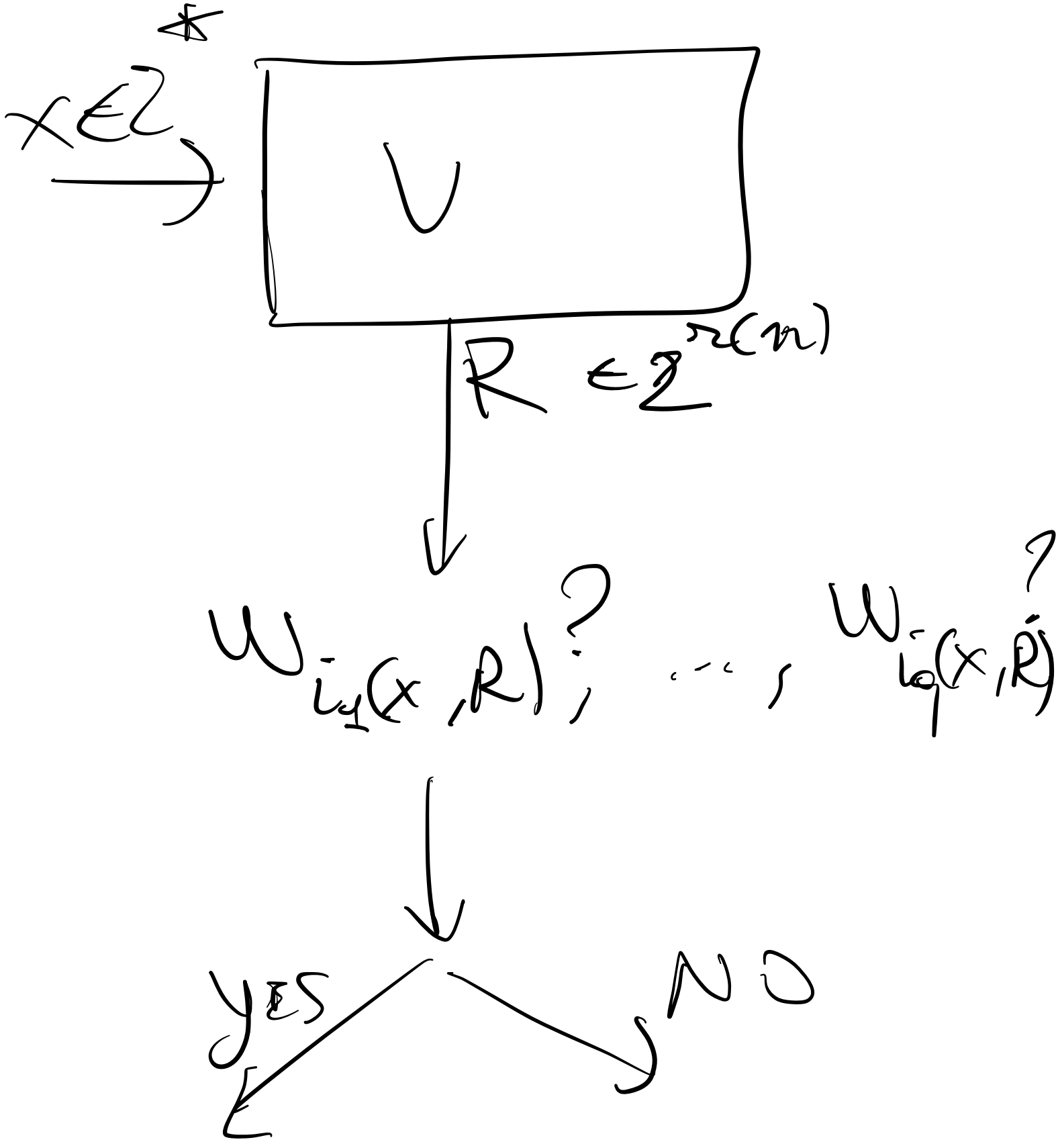


1) posso assumere che V legga esattamente q bit di w e estragga esattamente r(n) bit random

2) posso assumere che tutti i bit random siano estratti all'inizio

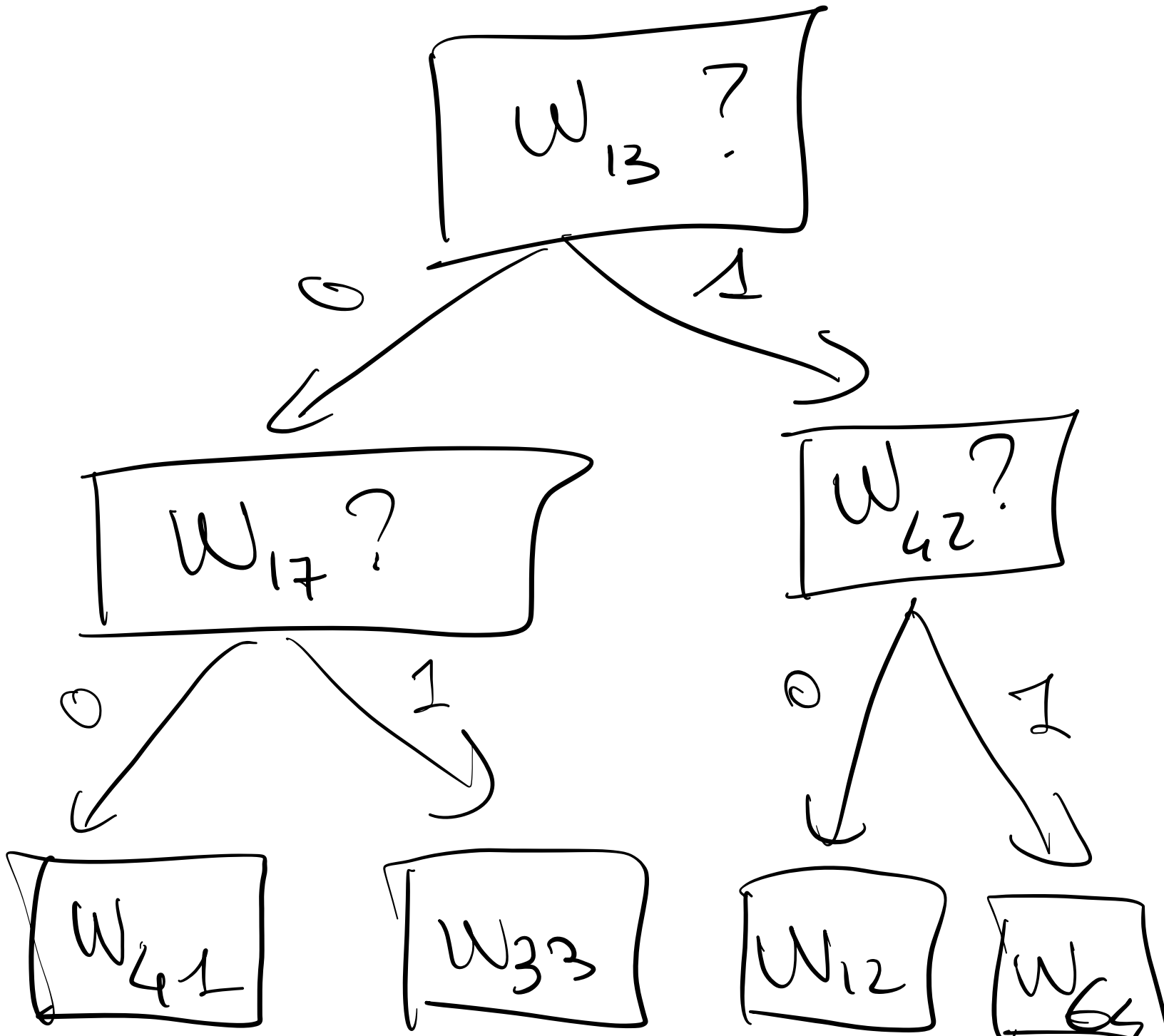
3) posso assumere che le q posizioni di w che vengono lette siano fisse e dipendenti solo da x e da R


$x \in 2^{\phi}$
$R \in 2^{r(n)}$
$W_{i_1}(x,R)$
0
1
$W_{i_2}^{0}(x,R)$
$W_{i_2}^{1}(x,R)$
0
1
0
1
$W_{i_3}^{00}(x,R)$
q
$q = 2^{q}$


$x \in \Sigma^*$
U
$R \in \Sigma^{r(n)}$
$W_{i_1}(x,R)$? , ... , $W_{i_q}(x,R)$?
YES
NO

$q = 3$

x, R



$\{12, 13, 17, 33, 42, 41, 64\}$

INAPPROSSIMABILITÀ DI MAXE3SAT MEDIANTE PCP

Lemma: Sia

$$f: 2^{\{x_1,\dots,x_k\}} \longrightarrow 2$$

una funzione booleana. Allora f si può scrivere come una CNF con al più 2^k clausole, ognuna con esattamente k letterali.

x_1	x_2	x_3	f
0	0	0	1
0	0	1	0 ←

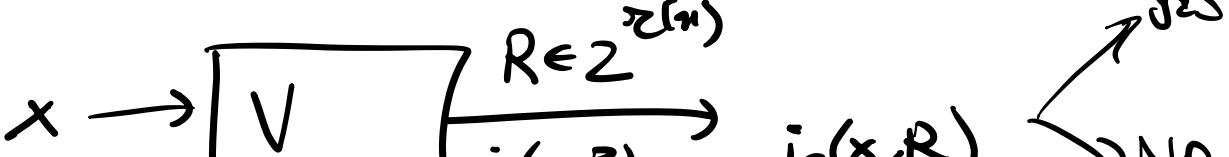
k

$x_1 = 0$	$x_2 = 1$	$x_3 = 0$	1	2^3
$x_1 = 0$	$x_2 = 1$	$x_3 = 1$	1	
⋮	⋮	⋮	⋮	

$$(x_1 \vee x_2 \vee \neg x_3) \wedge \dots \wedge$$

Teorema: Esiste un $\bar{\varepsilon} > 0$ t.c. MAXCNFSAT non è $(1+\bar{\varepsilon})$-approssimabile in tempo polinomiale, a meno che $P = NP$)

Dim: Sia $L \in NP$-completo.
Quindi $L \in NP = PCP[r(n), q]$ per qualche $r(n) \in O(\log n)$ e $q \in \mathbb{N}$. Sia V un verificatore in forma normale per L.



$i_1(x,R), \ldots, i_q(x,R)$? ?

V è descrivibile come segue:

1) fissato l'input $x \in 2^*$

2) fissata $R \in 2^{r(|x|)}$

interroga l'oracolo w in q posizioni

$$i_1(x,R), \ldots, i_q(x,R)$$

e accetta/rifiuta

$$f(w_{i_1(x,R)}, \ldots, w_{i_q(x,R)}) \in 2$$

$\Downarrow$ (Lemma)

descrivibile come una formula CNF $\varphi_{x,R}$ nelle variabili $w_{i_1(x,R)}, \ldots, w_{i_q(x,R)}$ con $\leq 2^q$ clausole di q letterali.

E.g. $(w_3 \vee w_7 \vee \neg w_8) \wedge (w_3 \vee \neg w_2 \vee w_8)$

Chiaramente

$$\Phi = \bigwedge_{R \in 2^{r(|x|)}} \varphi_{x,R}$$

Φ_x $R \in 2^{r(|x|)}$

1) Φ_x è fatta da clausole con q letterali

2) Φ_x contiene ~~esattamente~~ ciascuna esattamente

$2^q 2^{r(|x|)} = 2^{q + r(|x|)} = 2^{q + O(\log |x|)} = p(|x|) \in Poly$

clausole

- Se $x \in L$, V deve essere tale che esiste un w che fa decidere con prob. 1

$\Rightarrow$ Φ_x è soddisfacibile

$\Rightarrow$ esiste un assegnamento che soddisfa

fatte le $p(|x|)$
chiamate di Φ_x

- $\forall x \notin L$, V deve essere tale che qualunque sia w accetta con prob. $< \frac{1}{2}$

$\Rightarrow$ per $\geq \frac{2^{p(|x|)}}{2}$ stringhe R

Φ deve essere

non sodd distacchi

$$\overline{\varphi_{x,R_1}} \wedge \overline{\varphi_{x,R_2}} \wedge \dots \wedge \overline{\varphi_{x,R_t}}$$

$$t = 2^{r(|x|)}$$

$$\forall w \quad \sum_{i=1}^{t} |q_i| \, \varphi_{x,R_i} = \frac{1}{2}$$

$$< \frac{\epsilon}{2} = \frac{2^{-r(|x|)}}{2} =$$

$$= \frac{P(|x|)}{2^{q+1}}$$

$$P(|x|) = 2^{q + r(|x|)}$$

$$2^{r(|x|)} = P(|x|)$$

2^q

di φ_{x,R_i}

$\forall w$ non soddisfa

$\geq t - \frac{P(|x|)}{2^{q+1}}$

di φ_{x,R_i}

$\forall w$ non soddisfa

$\geq \left(t - \frac{P(|x|)}{2^{q+1}}\right)$

$$\left(2^{q}-1\right)$$

classe

Hw non scaricata

$$\geq \left(2^{r(|x|)} - \frac{P(|x|)}{2^{q+r}}\right)$$

$$\left(2^{q}-1\right) =$$

$$\left(P(|x|) - \frac{P(|x|)}{}\right)$$

$$\left(\frac{}{2^{q}} \qquad \frac{}{2^{q+1}}\right)$$

$$\left(2^{q}-1\right) =$$

$$\frac{P(|x|)}{2^{q+1}} \left(2^{q}-1\right)$$

$$\varepsilon = \frac{1}{2^{q+}}$$