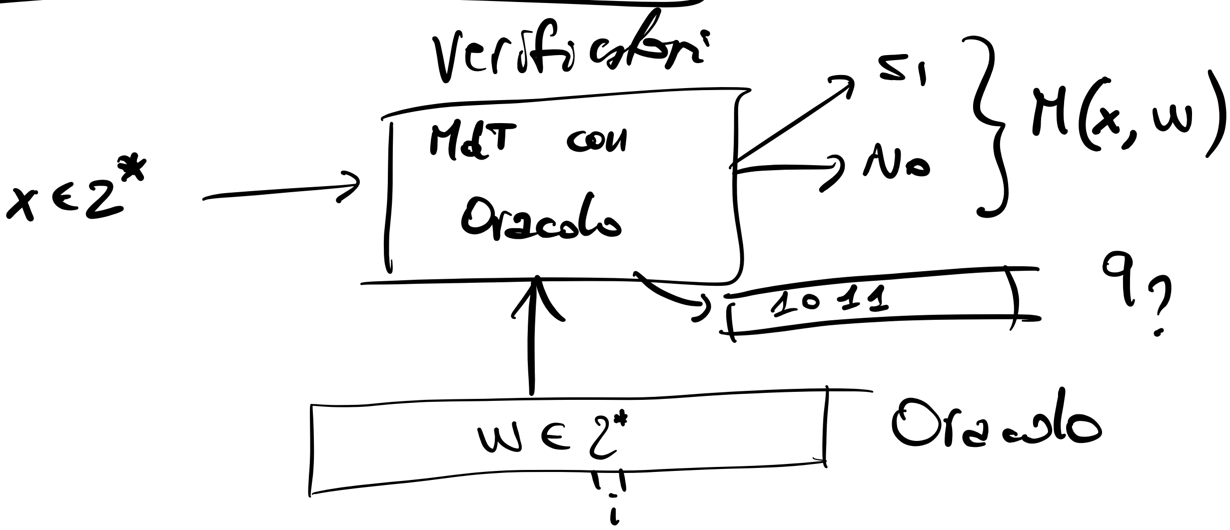
TEOREMA PCP

$L \subseteq \Sigma^*$

$\boxed{\text{MdT CON ORACOLO}}$ = VERIFICATORI



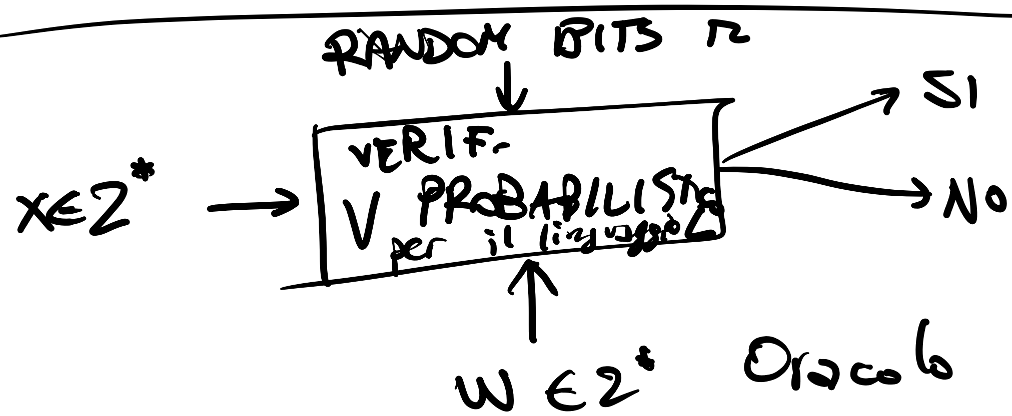
NASTRO DELLE QUERY

i

Teorema: $L \subseteq \Sigma^*$ sta in NP, esiste una MdT V con oracolo t.c.

1) $V(x,w)$ lavora in tempo polinomiale in $|x|$
2) $\forall x \in \Sigma^*$ $\exists w \in \Sigma^*$ t.c. $V(x,w) = SI$ <u>sse</u> $x \in L$

VERIFICATORI PROBABILISTICI



1) V lavora in tempo polinomiale
$|x|$

2) . se $x \in L$, $\exists w \in \Sigma^*$ t.c.
$V(x, w)$ accetta con probabilità 1

. se $x \notin L$, $\forall w \in \Sigma^*$
$V(x, w)$ rifiuta con probabilità $\geq \frac{1}{2}$

Date due funzioni $r, q : \mathbb{N} \to \mathbb{N}$

$PCP[r, q]$

la classe dei linguaggi accettati da un verificatore probabilistico che su input x faccia

$\leq q(|x|)$ query all'oracolo

$\leq r(|x|)$ bit random

$PCP[0, 0] = P$

$PCP[0, Poly] = NP$

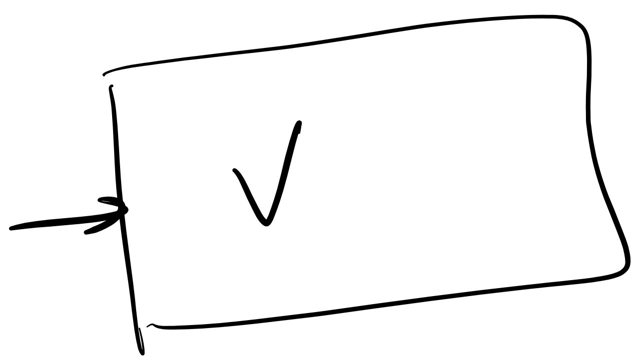
<u>Teorema</u> PCP [Arora, Safra 1998]

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

$$SAT \in PCP[O(\log n), O(1)]$$

$$\Rightarrow SAT \in PCP[5 \log n + 7 \log \log n + 12, 157]$$

$x \in \Sigma^*$



$O(1)$

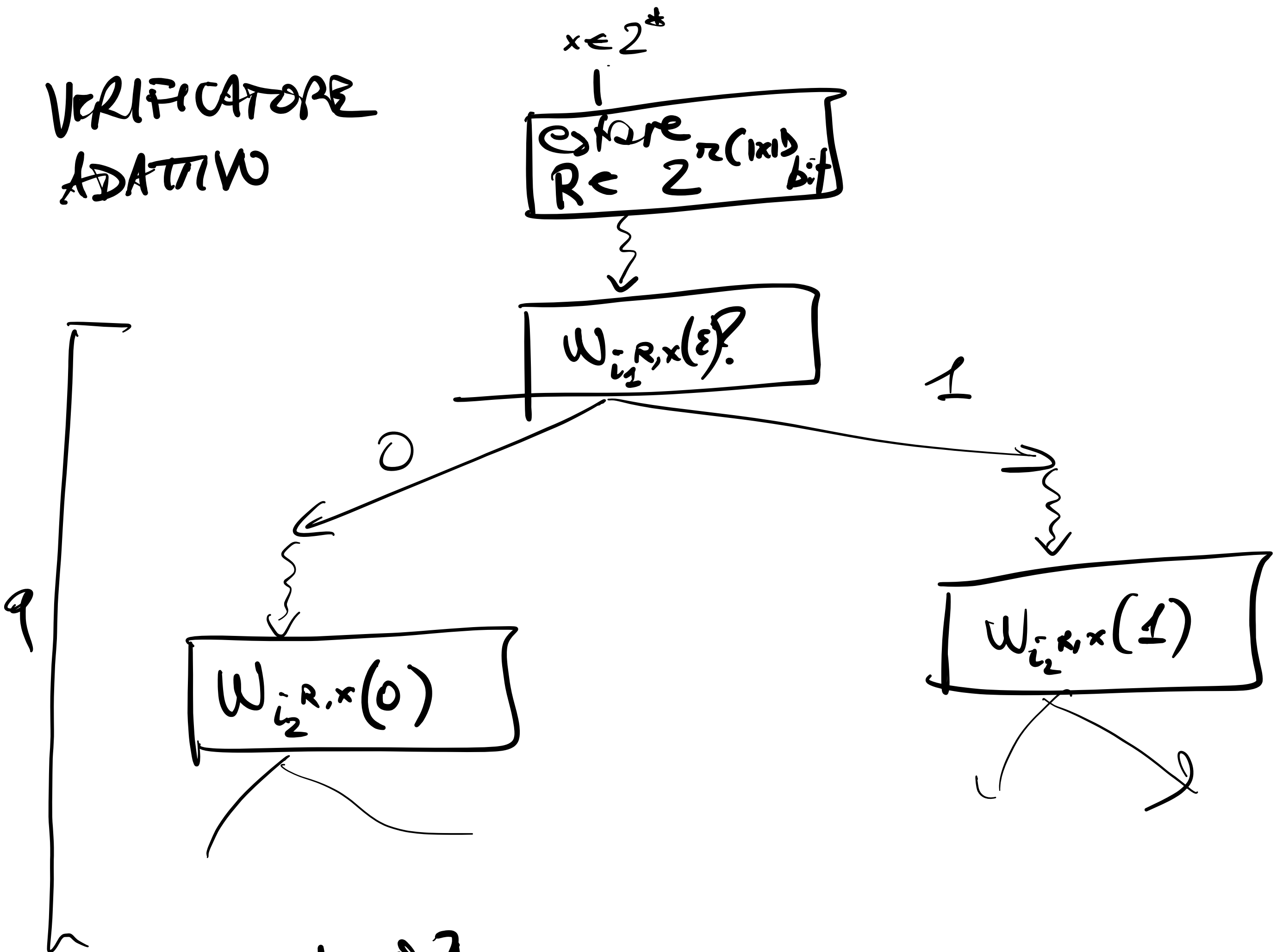
$V \in PCP[r, q]$ su input $x \in \Sigma^*$

1) faccia esattamente $q(|x|)$ query
2) estraggo esattamente $r(|x|)$ bit random

VERIFICATORE

$$V \in PCP[\underbrace{r(n)}_{O(\log n)}, \underbrace{q}_{\in \mathbb{N}}]$$

VERIFICATORE ADATTIVO



$$\bar{q} = 2^{q-1} + 2^{q-2} + \dots + 1$$

$\Rightarrow$ NON ADATTIVO

$$V \in PCP[r(n), q]$$

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

1) legge una stringa

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

di bit random

2) effettua q di query

$$\{ i_1^{R,x}, \dots, i_q^{R,x} \}$$

3) comportamento puramente deterministico

$$x, R, \underbrace{w_{i_1}, \dots, w_{i_q}}_{\text{risposte}}$$

$q=3$

x, R