PROBLEMA MAX E_kSAT

letterali

$$\underbrace{\underbrace{(x_1 \vee x_3 \vee \neg x_4)}_{\text{clausola}} \wedge (x_4 \vee \underbrace{\neg x_5 \vee \neg x_1)}} \wedge (x_1 \vee \neg x_2 \vee \neg x_3)}_{t}$$

Teorema: MAXE_kSAT è NPO-completo per ogni $k \geq 3$.

Teorema (1). Un assegnamento casuale soddisfa in media

$$E[T] = \frac{2^k - 1}{2^k} t$$

clausole.

- $x_1, \ldots, x_n$: variabili che compaiono nella formula
- $c_1, \ldots, c_t$: clausole

1) $X_i \sim Unif\{0,1\}$ (è il valore assegnato alla variabile x_i)

2) C_i

$$C_i = \begin{cases} 1 & \text{se } c_i \text{ è soddisfatta} \\ 0 & \text{altrimenti} \end{cases}$$

3) T il numero di clausole soddisfatte

$$E[T] = \sum_{b_1\in Z}\cdots\sum_{b_n\in Z} E[T \mid \overbrace{X_1=b_1,\dots,X_n=b_n}^{\mathcal{E}_i}]\; P[X_1=b_1,\dots,X_n=b_n] =$$

$$\boxed{\begin{array}{l}\text{Legge del valore atteso totale}\\ E[X] = \displaystyle\sum_{i=1}^{k} E[X \mid \mathcal{E}_i]\,P[\mathcal{E}_i]\\ \text{dove } \mathcal{E}_i \text{ sono eventi disgiunti}\\ \text{la cui unione è l'universo}\end{array}}$$

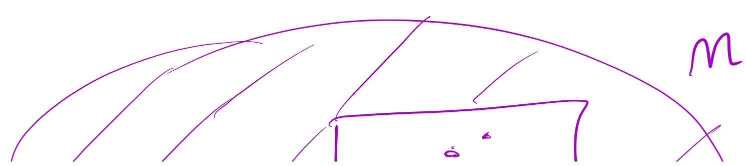
$$= \sum_{b_1\in Z}\cdots\sum_{b_n\in Z} E[T \mid X_1=b_1,\dots,X_n=b_n]\; \underbrace{P[X_1=b_1]}_{\frac{1}{2}}\, P[X_2=b_2]\cdots P[X_n=b_n] =$$

$$= \frac{1}{2^n}\sum_{b_1\in Z}\cdots\sum_{b_n\in Z} E[\underbrace{T}_{T=C_1+\dots+C_t} \mid X_1=b_1,\dots,X_n=b_n] =$$

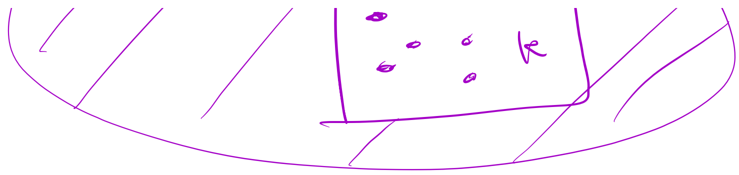
$$= \frac{1}{2^n}\sum_{j=1}^{t}\left(\sum_{b_1\in Z}\cdots\sum_{b_n\in Z} E[C_j \mid X_1=b_1,\dots,X_n=b_n]\right)$$

$b_1=0,\ b_2=1,\ b_3=1,\ b_4=0,\ b_5=1$

$C_j = x_1 \lor \neg x_2 \lor x_5$



2^n = # assegnazioni possibili



2^{n-k} = rendono falsa la clausola

$\boxed{2^n - 2^{n-k}}$ = rendono vera la clausola

$$= \frac{1}{2^n} \sum_{j=1}^{t} \left(2^n - 2^{n-k}\right) =$$

$$= \frac{2^n - 2^{n-k}}{2^n}\, t = \frac{2^k - 1}{2^k}\, t$$

Abbiamo dimostrato che

$$E[T] = \frac{2^k - 1}{2^k}\, t.$$

DERANDOMIZZAZIONE

Teorema (2): Per ogni $j = 0, \dots, n$ esistono $b_1, \dots, b_j \in 2$ t.c.

$$E[T \mid X_1 = b_1, \dots, X_j = b_j] \geq \frac{2^k - 1}{2^k}\, t$$

Dim: (Per induzione su j)

Il caso $j = 0$ è Teorema (1).

$$\frac{2^k - 1}{2^k}\, t \overset{\text{IP. IND.}}{\leq} E[T \mid X_1 = b_1, \dots, X_{j-1} = b_{j-1}] =$$

Legge del valore atteso totale

$$= E[T \mid X_1=b_1, \dots, X_{j-1}=b_{j-1}, X_j=0]\, P[X_j=0]$$
$$+ E[T \mid X_1=b_1, \dots, X_{j-1}=b_{j-1}, X_j=1]\, P[X_j=1] =$$

$$= \frac{1}{2} \underbrace{E[T \mid X_1=b_1, \dots, X_{j-1}=b_{j-1}, X_j=0]}_{\alpha_0}$$
$$+ \frac{1}{2} \underbrace{E[T \mid X_1=b_1, \dots, X_{j-1}=b_{j-1}, X_j=1]}_{\alpha_1} =$$

$$= \boxed{\frac{1}{2}\alpha_0 + \frac{1}{2}\alpha_1} \Rightarrow \alpha_0 \text{ o } \alpha_1 \text{ devono essere } \geq \frac{2^k-1}{2^k} t$$

Per assurdo, supponiamo α_0 e $\alpha_1 < \frac{2^k-1}{2^k} t$

$$< \frac{1}{2} \frac{2^k-1}{2^k} t + \frac{1}{2} \frac{2^k-1}{2^k} t = \frac{2^k-1}{2^k} t \qquad \square$$

Corollario:

Esistono $b_1, \dots, b_n \in 2$ t.c.

$$\underbrace{E[T \mid X_1=b_1, \dots, X_n=b_n]}_{\substack{\#\text{clausole soddisfatte} \\ \text{se } X_1=b_1, \dots, X_n=b_n}} \geq \frac{2^k-1}{2^k} t$$

ALGORITMO DERANDOMIZZATO

$D \leftarrow \emptyset$ // Indici delle clausole già determinate

for $i = 1, \dots, n$

$\Delta_0 \leftarrow 0$ $\Delta D_0 \leftarrow \emptyset$

$\Delta_1 \leftarrow 0$ $\Delta D_1 \leftarrow \emptyset$

for $j = 1, \dots, t$

if $j \in D$ **continue**

if x_i non compare in c_j **continue**

$h \leftarrow$ numero di variabili di indice $\geq i$ che compaiono in c_j

if x_i compare positiva in c_j

$\Delta_0 \leftarrow \Delta_0 - \frac{1}{2^h}$

$\Delta_1 \leftarrow \Delta_1 + \frac{1}{2^h}$

$\Delta D_1 \leftarrow \Delta D_1 \cup \{j\}$

else

$\Delta_0 \leftarrow \Delta_0 + \frac{1}{2^h}$

$\Delta_1 \leftarrow \Delta_1 - \frac{1}{2^h}$

$\Delta D_0 \leftarrow \Delta D_0 \cup \{j\}$

$u = \operatorname{argmax} \{\Delta_0, \Delta_1\}$

$x[i] = u$

$D \leftarrow D \cup \Delta D_u$

Teorema: L'algoritmo trova un assegnamento che soddisfa

$$\frac{2^k-1}{2^k}\, t$$

clausole.

L'algoritmo garantisce che quando assegna la variabile i-esima

$$\underbrace{E[T \mid X_1 = x[1], \dots, X_{i-1} = x[i-1]]}\geq \frac{2^k-1}{2^k}\, t$$

Per $i=0$, vero per il Teorema (1).

Passo induttivo:

$$E[T \mid X_1 = x[1], \dots, X_{i-1} = x[i-1]] \geq \frac{2^k-1}{2^k}\, t$$

$X_i = ?$

$$C_j \quad [\; x_{..} \;\; \vee \; \overbrace{x_i \vee \; \neg x_{...} \;\; x_{..}}^{h} \;]$$

clausola ...

con $\boxed{\dfrac{2^h-1}{2^h}}$ assegnamenti rendono la clausola vera

$\boxed{X_i = 1}$ con 1

$$\Delta E[T] = 1 - \frac{2^h - 1}{2^h} = \frac{2^h - 2^h + 1}{2^h} = \boxed{\frac{1}{2^h}}$$

$\boxed{X_i = 0}$ $\rightsquigarrow$ $\frac{2^{h-1} - 1}{2^{h-1}}$

$$\Delta E[T] = \frac{2^{h-1} - 1}{2^{h-1}} - \frac{2^h - 1}{2^h} = \frac{2^h - 2 - 2^h + 1}{2^h} =$$

$$= \boxed{-\frac{1}{2^h}}$$

Corollario

L'algoritmo fornisce una $\frac{2^k}{2^k - 1}$-appross. per MaxEkSat.

<u>Dim</u>: Sia t^* il numero di clausole ottimo: $t^* \leq t$

$$\frac{t^*}{t_{ALG}} \leq \frac{t}{t_{ALG}} \leq \frac{t}{\frac{2^k - 1}{2^k} t} = \frac{2^k}{2^k - 1}$$

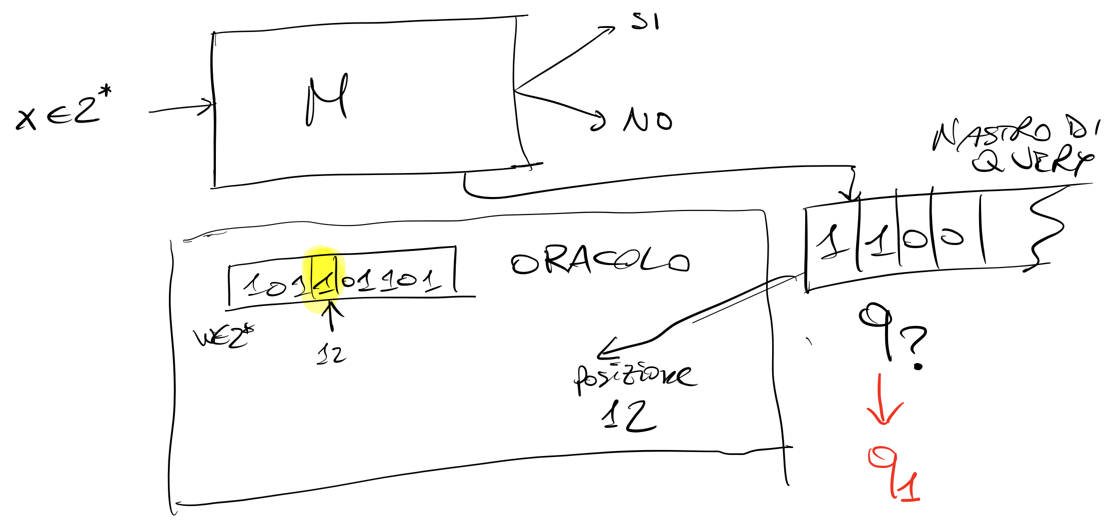
$\square$

P.es.

k	APPROSS.
3	8/7
4	16/15

MdT CON ORACOLO

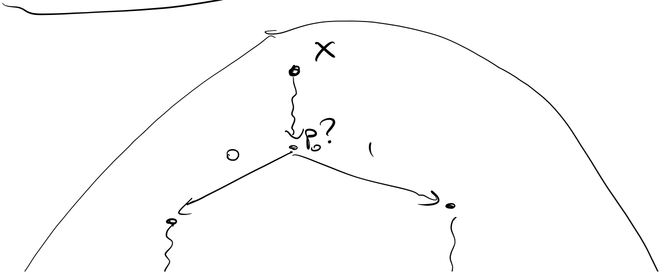
$M(x, w) \begin{cases} SI \\ NO \end{cases}$



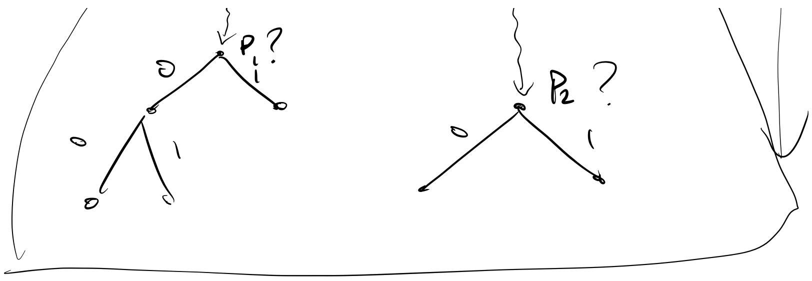
Teorema: Un linguaggio $L \subseteq \Sigma^*$ appartiene a NP sse esiste una MdT con oracolo V ("verificatore")

1) $V(x, w)$ termina in tempo pol. nella $|x|$
2) $\forall x \in \Sigma^*$

$$\boxed{\exists w \in \Sigma^* \text{ t.c. } V(x,w) = SI \iff x \in L}$$

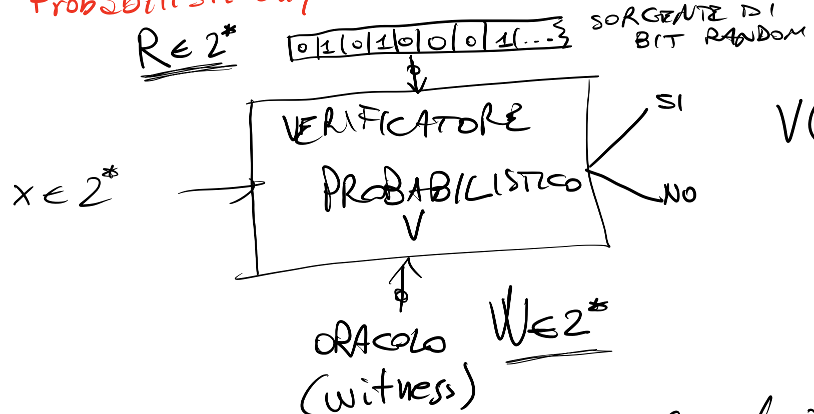


$V(x, -)$



PROBABILISTIC CHECKERS

(PCP = Probabilistically Checkable Proofs)



$V(x, r, w)$

$PCP[r, q]$ ⟵ classe dei verificatori che leggono $\leq r$ bit random e effettuano $\leq q$ query all'oracolo

⟵ classe dei linguaggi accettati

$L \in \boxed{PCP[r, q]}$ sse esiste un verif. probabilistico V

1) $V(x, R, W)$ funziona in tempo polinomiale in $|x|$

2) $V(x, R, W)$ effettua al massimo $q(|x|)$ query

3) $V(x, R, W)$ legge al massimo $r(|x|)$ bit random

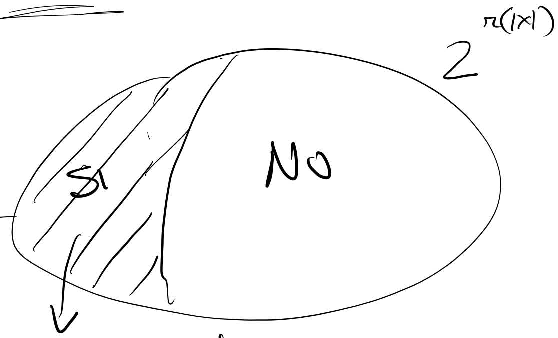
4) • se $x \in L$, $\exists W \in 2^*$ t.c. V accetta x con prob. 1

V accetta

(cioè $V(x, -, W) = $ SI)

- se $x \notin L$, V rifiuta ogni W con prob. $\geq \frac{1}{2}$

$V(\underline{x}, \_, \underline{W})$



PROBABILITÀ = #sequenze / $2^{p(|x|)}$

$PCP[0, 0] = P$

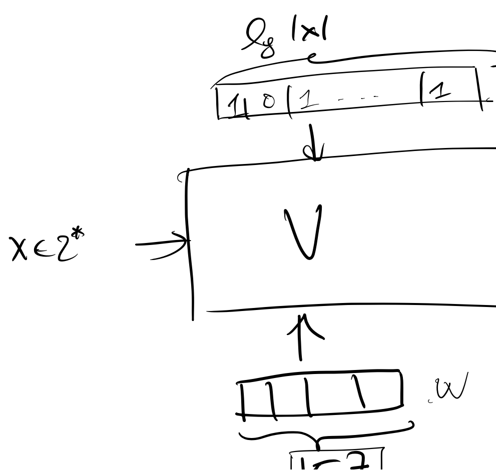
$PCP[0, Poly] = \bigcup_{p \in Polynomial}$

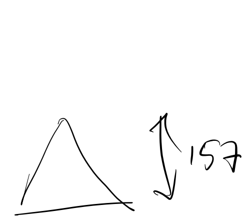
$PCP[0, P] = NP$

Teorema (Arora, Safra 1998)

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

$L \in NP$





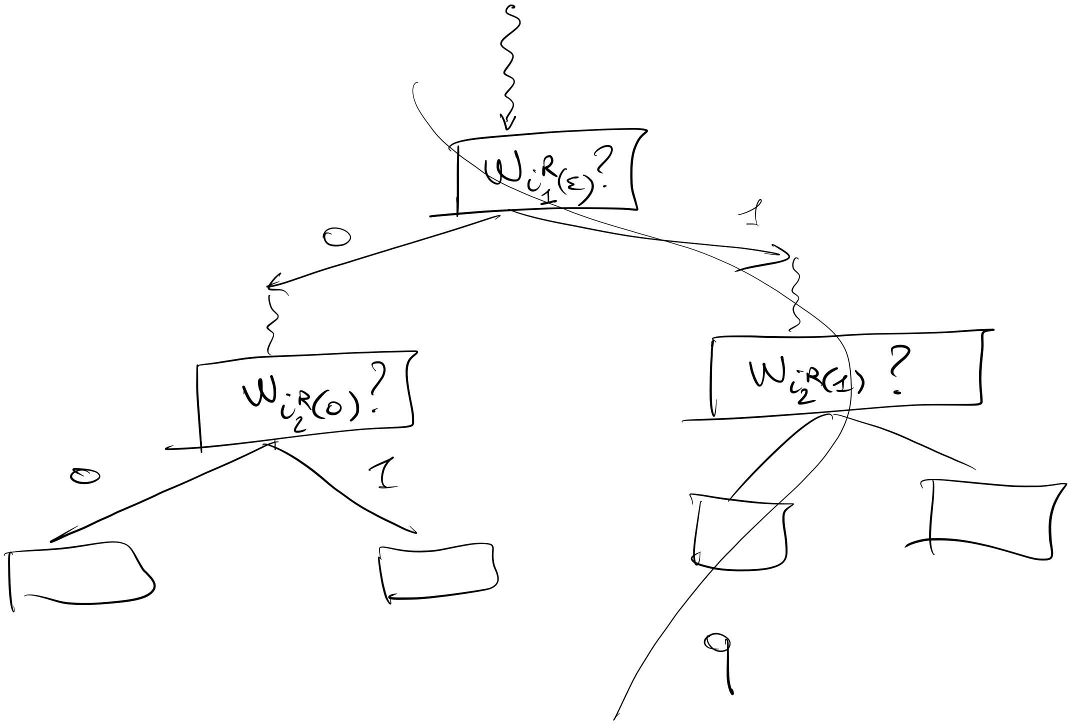
$V \in PCP[r(n), q]$ $\quad r(n) \in O(\log n)$

$q \in \mathbb{N}$

1) V usi esattamente $r(|x|)$ bit random
2) V effettui esattamente q query all'oracolo
3) V estrae tutti gli $r(|x|)$ bit random all'inizio
4) V subito dopo aver estratto i bit random effettua tutte le q query all'oracolo

VERIF. IN FORMA NORMALE

$$
\left[\begin{array}{rcl}
 & \text{input } |x| & \\
R \in \mathbb{Z}^* & \Big\downarrow & \text{estrae gli } r(|x|) \text{ bit random} \\
\underbrace{w_{i_1}, w_{i_2}, \dots, w_{i_q}}_{\text{Risultati delle } q \text{ query}} \in \mathbb{Z} & \Big\downarrow & \text{effettua le } q \text{ query} \\
 & \rightsquigarrow & \text{MdT deterministica "standard"}
\end{array}\right.
$$



$$\boxed{\bar{q} = 2^{q}}$$