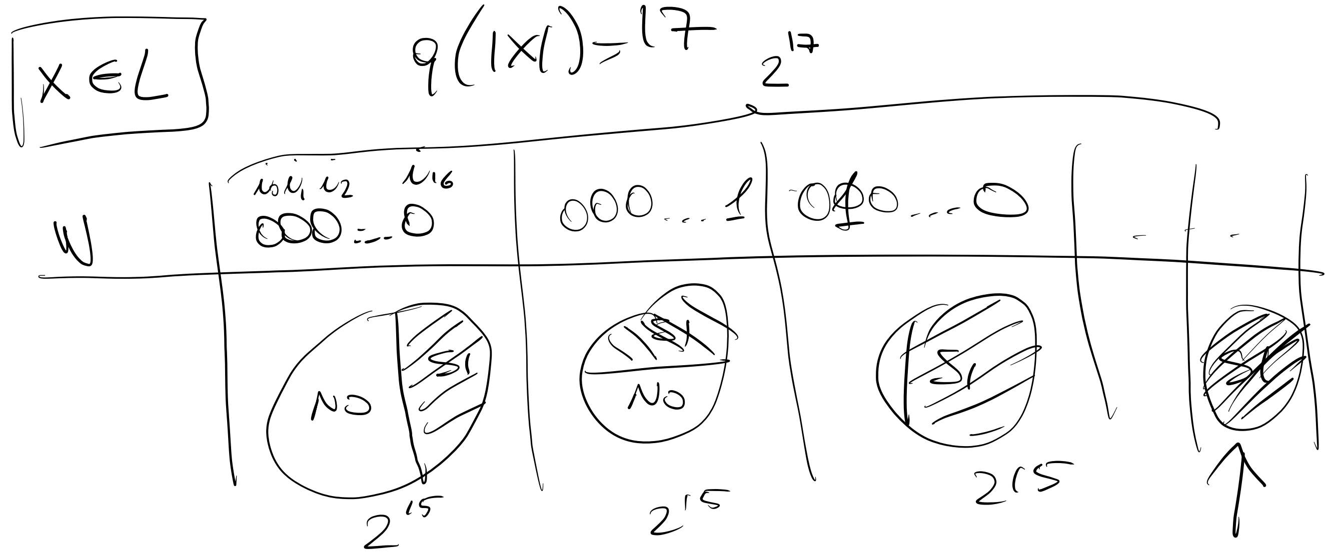
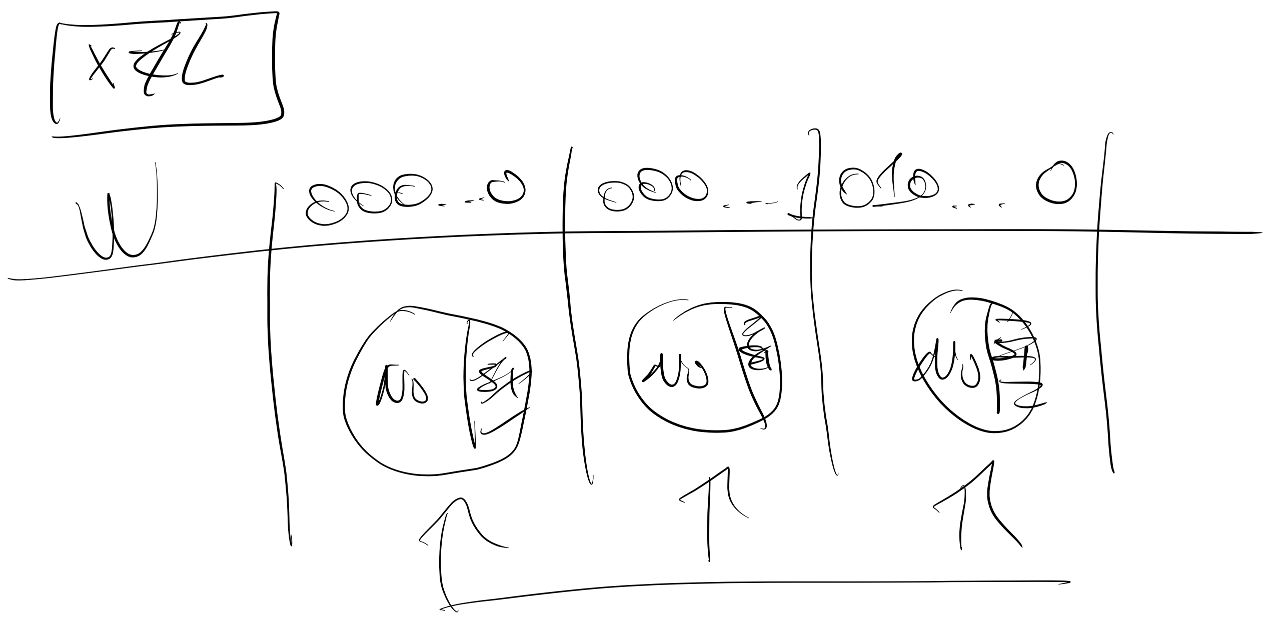
$L \in PCP[r(n), q(n)]$

$r(|x|) = 15$

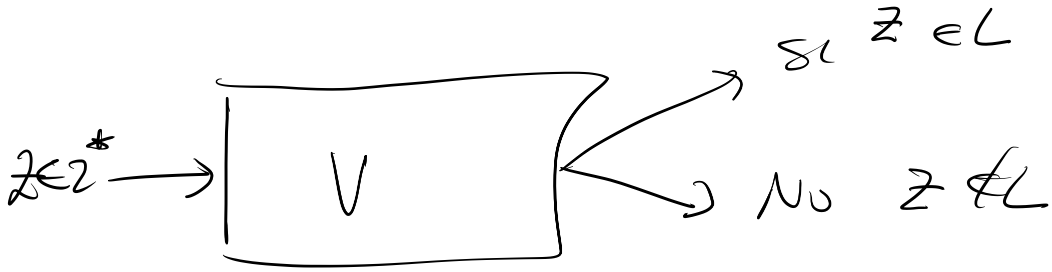




APPLICAZIONE DEL PCP ALL'INAPPROSSIMABILITÀ DI MAXE_3SAT

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

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



$z \in 2^*$ INPUT

- $\mathcal{R} = 2^{r(|z|)}$ spazio probabilistico (su input z)

$R \in \mathcal{R}$

$$\begin{array}{cccc} i_1^R, & i_2^R, & \dots, & i_q^R\ ? \\ \downarrow & \downarrow & & \downarrow \\ 0 & 1 & & 0 \end{array}$$

⊛ $f^R(w_{i_1^R}, w_{i_2^R}, \dots, w_{i_q^R}) =$ SI oppure NO

$x_1, x_2, x_3, \dots$ variabili che rappresentano i bit da cui w è composto

⊛ si può descrivere con una formula logica in CNF

$$\varphi_z^R \begin{cases} (x_1=1 \vee x_2=0 \vee x_3=1 \vee x_7=1) \wedge \\ (x_1=1 \vee x_4=1 \vee x_8=0 \vee x_9=1) \wedge \\ \dots \end{cases}$$

$\Downarrow$

clausole con q letterali

$\wedge$

$$\boxed{\Phi_z = \bigwedge_{R \in \mathcal{R}} \boxed{\varphi_z^R}}$$

1) CNF $\leq \underbrace{|\mathcal{R}|\, 2^q}_{\text{CLAUSOLE}} = 2^{r(|z|)}\, 2^q =$

$$= 2^{r(|z|)+q} = 2^{O(\log |z|)+q} = O(|z|)$$

2) se $z \in L$, V deve accettare con prob. 1 per un qualche $\overline{w}$, $\overline{w}$ deve soddisfare ogni $\varphi_z^R \Rightarrow \Phi_z$ è soddisfacibile

3) se $z \notin L$, $\forall w$, soddisfo meno di $\boxed{\frac{|\mathcal{R}|}{2}}$ delle φ_z^R

$$\overbrace{\underbrace{\wedge \ \wedge \ \wedge}_{\varphi_z^{000\ldots0}}}^{\text{SI}} \ \bigwedge \ \overbrace{\underbrace{\wedge \ \wedge \ \ldots \wedge}_{\varphi_z^{000\ldots1}}}^{\text{NO}} \ \bigwedge \ \overbrace{\underbrace{\wedge \ \wedge \ \wedge \ \wedge}_{\varphi_z^{010\ldots1}}}^{\text{SI}}$$

Φ_z

Delle $|R|2^q$ clausole di cui Φ_z è costituita, ogni w rende vere

$$\le \frac{|R|}{2} 2^q + \frac{|R|}{2}(2^q-1)$$

CLAUSOLE

<u>Teorema</u>: Esiste $\varepsilon > 0$ t.c. MAX SAT non è $(1+\varepsilon)$-appross. in tempo polinomiale, a meno che $P=NP$.

<u>Dim</u>: Sia $L \in NP$-completo. Esisterà $r(n) \in O(\log n)$ <u>specifica</u> e un $q \in \mathbb{N}$

<u>specifico</u> t.c. $L \in PCP(\log n, q)$.

$\overline{\varepsilon} \triangleq \dfrac{1}{2^{q+1}}$, e

immaginiamo che MAXSAT

sia $(1+\overline{\varepsilon})$-approssimabile.

$$z \in \Sigma^* \longrightarrow \boxed{\text{COSTR. SOPRA}} \longrightarrow \Phi_z \longrightarrow \underset{\text{MAXSAT}}{\boxed{A}} \longrightarrow \underline{t(\Phi_z)}$$

$z \in L \Rightarrow \Phi_z$ è soddisfacibile

$$\Rightarrow t^*(\Phi_z) = \underbrace{|R|\,2^q}$$ (*)

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

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

$z \in L$ $$t(\Phi_z) \geq \frac{t^*(\Phi_z)}{1+\overline{\varepsilon}} \overset{(*)}{=} \frac{2^q|R|}{1+\frac{1}{2^{q+1}}} \triangleq \underline{A}$$

$z \notin L$

$$t(\Phi_2) \le t^*(\Phi_2) \le 2^q|R| - \frac{|R|}{2} \triangleq B$$

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

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

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

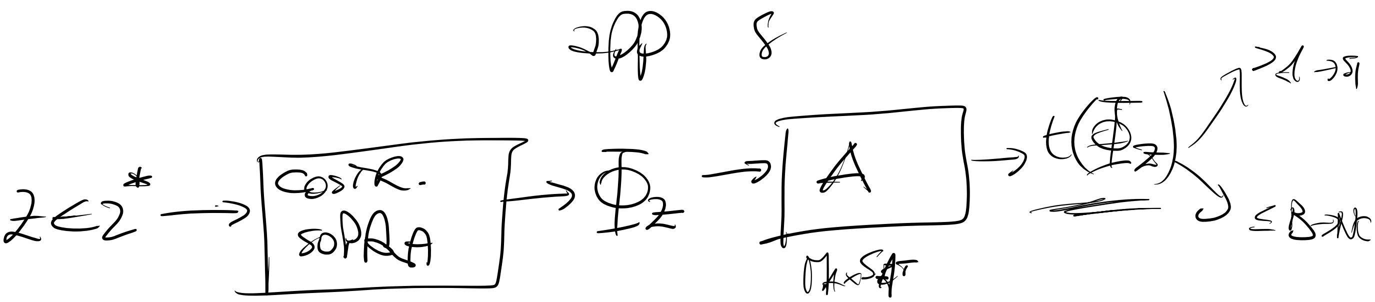
$$= |R| \frac{\frac{1}{2^{q+1}}}{2\left(1 + \frac{1}{2^{q+1}}\right)} > 0$$

$$\Rightarrow \quad A > B$$

$t(\Phi_z) \geq A$ $\quad>\quad$ $B \geq t(\Phi_z)$

$\Updownarrow$ $\qquad\qquad$ $\Updownarrow$

$z \in L$ $\qquad\qquad$ $z \notin L$



Decide L in tempo polinomiale.

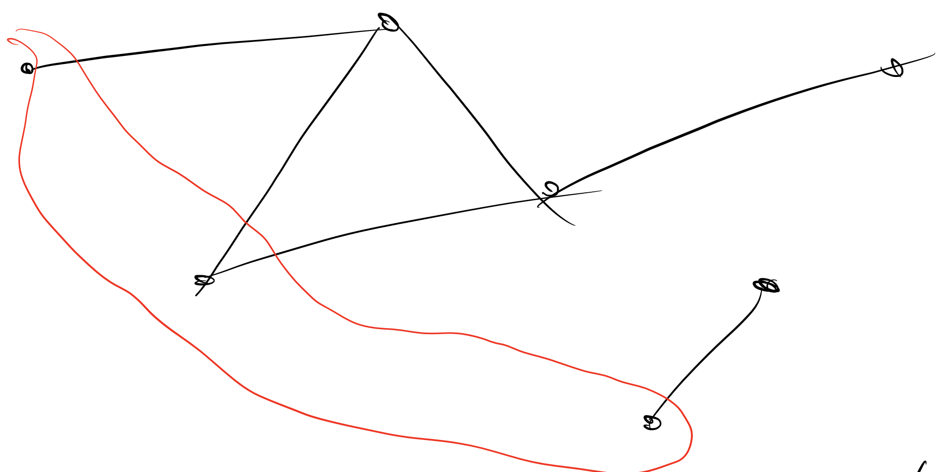
Assurdo. $\square$

Teorema: MAX E_3SAT non è $\left(\frac{8}{7}+\varepsilon\right)$-appross. per qualche $\varepsilon > 0$

Dim: OMESSA

Corollario: L'algoritmo derandomizzato per MAXE3SAT è ottimo.

PROBLEMA DELL' INDEPENDENT SET E SUA INAPPROSSIMABILITÀ (ATTRAVERSO PCP)



INPUT : $G=(V,E)$ non orientato

OUTPUT : $X \subseteq V$ insieme indip. (cioè, t.c. $\forall i,j \in X \quad ij \notin E$)

FUNZ. OB. : $|X|$

TIPO : MAX

Teorema: Per ogni $\varepsilon > 0$,

INDEPENDENTSET non è $(2-\varepsilon)$-approssimabile in tempo polinomiale (se $P \neq NP$).

Dim: $L \in NP$-completo

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

$z \in 2^*$ $\quad R_z = 2^{r(|z|)}$ seq. bit random

$Q_z^R = 2^q$ risposte dell'oracolo

$$\underbrace{\mathcal{C}_z = \bigcup_{R \in R_z} \{R\} \times Q_z^R}$$ SI / NO

$\boxed{\mathcal{A}_z} \subseteq \mathcal{C}_z$ configurazioni accettanti

$\cup$

$$c = (R, \langle i_1^R : 0,\ i_2^R : 0,\ i_3 : 1, \ldots, i_q : 1 \rangle)$$

seq. di bit random

query effettuate e le risposte ottenute

$$(\Phi_z, \text{incompatib.}) = G_z$$

$$\boxed{(R, \langle i_1^R : v_1, \ldots, i_q^R : v_q \rangle)}$$

incompatib. $\iff R = R' \vee \exists k, k' \in \{1, .., q\}$ t.c. $i_k^R = i_{k'}^{R'}$ e $v_k \neq v_{k'}$

$$\boxed{(R', \langle i_1^{R'} : v_1', \ldots, i_q^{R'} : v_q' \rangle)}$$

Fatto 1: Se $z \in L$, G_z ha un insieme indipendente di cardinalità $\geq 2^{r(|z|)}$.

Dim: $\exists \overline{w}$ che fa accett. con prob. 1 (*) $\forall R \in \mathbb{R}$

$\mathcal{A}_2$

$\left(R, \underbrace{<15:0 \ \_ \ \_ \ \_ \ \_ >}_{\text{compatib. } \overline{w}}\right)$

$(R', < \_ \ \_ \ \_ \ \_ >)$

$(R'', < \_ \ \_ \ \_ \ \_ >)$

Insieme indip. $\geq |\mathbb{R}| = 2^{\pi(|Z|)}$

(*) $\mathcal{A}_2^{\overline{w}} = \{ (R, < i_1^R : v_1, \ldots, i_q^R : v_q >) \mid \overline{w}_{i_1^R} = v_1, \ldots, \overline{w}_{i_q^R} = v_q \} \subseteq \mathcal{A}_2$

$R \in \mathbb{R}$

$\mathcal{A}_2^{\overline{w}}$

000

0001

0010

⋮

$|\mathbb{R}| = 2^{\pi(|Z|)}$