Significato di $P = NP$

Per il teorema di Cook-Levin:

Dati $x \in NT_M$:

$$E_M(x) = H \wedge S^0 \wedge (G^0 \wedge M_1^0) \wedge S^1 \wedge (G^1 \wedge M_1^1) \wedge \ldots \wedge S^{p(|x|)} \wedge M_1^{p(|x|)}$$

Calcolabile mediante un algoritmo deterministico

Se $P = NP$ vuol dire che trovo T_{SAT} che opera in tempo polinomiale

$\Rightarrow \forall \Gamma \in NP \; \exists T_M$ che decide Γ in tempo polinomiale

Potrei risolvere $E(x)$ in tempo polinomiale

Definire un problema NP-completo

Teorema

Se $\Gamma_1 \in NP \wedge \exists \Gamma_2 \in NP\text{-completo} \wedge \Gamma_2 \propto \Gamma_1$

$\Rightarrow \Gamma_1 \in NP\text{-completo}$

Dim

Diamo per scontato che $\exists \gamma$

x istanza sì

1) Se $\Gamma_2 \propto \Gamma_1 \Rightarrow \exists f_{21} : \mathcal{I}_{\Gamma_2} \to \mathcal{I}_{\Gamma_1} : x \in \mathcal{I}_2 \Leftrightarrow f(x) \in \mathcal{I}_1 \wedge \exists T_{21}, k \in \mathbb{N} : \forall x \in \mathcal{I}_{\Gamma_2} \left[dTIME(T_{21}, x) \in O(|x|^k) \right]$

2) $\forall \Gamma_3 \in NP \left[\exists T_{32}, h \in \mathbb{N} : \forall z \in \mathcal{I}_{\Gamma_3} \left[z \in \mathcal{I}_{\Gamma_3} \Leftrightarrow T_{32}(z) \in \mathcal{I}_2 \wedge dTIME(T_{32}, z) \in O(|z|^h) \right] \right]$

3) COSTRUISCO T_{31} CON INPUT $z \in \Gamma_{31}^1$

FASE 1) : SIMULA $T_{32}(z) = X$

FASE 2) : SIMULA $T_{21}(X) = Y$

RETURN Y

4) $z \in \Gamma_3^1 \Longleftrightarrow X \in \Gamma_2^1 \Longleftrightarrow Y \in \Gamma_1^1$

5) CALCOLIAMO LA COMPLESSITA'

$$dTIME(T_{31}, z) = dTIME(T_{32}, z) + dTIME(T_{21}, x) = O(|z^h|) + O(|x|^k)$$

SAPPIAMO CHE X OCCUPA SPAZIO $O(|z|^h)$

QUINDI $dTIME(T_{31}, z) \in O(|z|^{h+k})$

6) $\forall \Gamma_3^1 \in NP \Rightarrow$

$\Gamma_3^1 \propto \Gamma_2^1$ E $\Gamma_2^1 \propto \Gamma_1^1$ ALLORA $\Gamma_3^1 \propto \Gamma_1^1 \Rightarrow \Gamma_1^1 \in NP$-COMPLETO

NP-COMPLETEZZA DI 3-SAT

$$\mathcal{I}_{3\text{-}SAT} = \{ \langle f, X \rangle : f = C_1 \wedge \ldots \wedge C_m, \forall i = 1 \ldots m \; |C_i| = 3, \; X = x_1, \ldots, x_n \text{ LETTERALI} \}$$

$$\mathcal{I}_{SAT} = \{ \langle g, Y \rangle : g = d_1 \wedge \ldots \wedge d_r, \; Y = y_1, \ldots y_q \text{ LETTERALI} \}$$

SAT $\propto$ 3-SAT

$f: \mathcal{I}_{SAT} \to \mathcal{I}_{3\text{-}SAT}$ → TRASFORMIAMO OGNI d_i IN C_i

$\forall d_i \in g$ ABBIAMO DIVERSE CASISTICHE:

1) $|d_i| = 1 \Rightarrow d_i = l_j$

d_i VERA $\iff$ l_j E' VERA

$$d_i = (l_j \vee z_{i_1} \vee z_{i_2}) \wedge (l_j \vee \bar{z}_{i_1} \vee z_{i_2}) \wedge (l_j \vee z_{i_1} \vee \bar{z}_{i_2})$$

CLAUSOLE AGGIUNTIVE

2) $|d_i| = 2 \Rightarrow d_i = l_{j_1} \vee l_{j_2}$

$$d_i = (l_{j_1} \vee l_{j_2} \vee z_{i_1}) \wedge (l_{j_1} \vee l_{j_2} \vee \bar{z}_{i_1})$$

3) $|d_i| = 3 \Rightarrow d_i = l_{j_1} \vee l_{j_2} \vee l_{j_3}$ → OK

4) $|d_i| = 4 \Rightarrow d_i = l_{j_1} \vee l_{j_2} \vee l_{j_3} \vee l_{j_4}$

DIVIDIAMO d_i IN 2 PARTI:

$l_{j_1} \vee l_{j_2}$

$l_{j_3} \vee l_{j_4}$

E LI COLLEGHIAMO CON UNA VARIABILE AGGIUNTIVA

$$d_i = (l_{j_1} \vee l_{j_2} \vee z_{i_1}) \wedge (\bar{z}_{i_1} \vee l_{j_3} \vee l_{j_4})$$

COSTRUITA IN QUESTO MODO

$\exists$ UN'ASSEGNAZIONE DI x_i CHE RENDE VERA $d_i \iff$ E' VERA $l_{j_1} \vee l_{j_2} \vee l_{j_3} \vee l_{j_4}$

5) $|d_i| = 5 \Rightarrow d_i = l_{j_1} \vee l_{j_2} \vee l_{j_3} \vee l_{j_4} \vee l_{j_5}$

PRENDIAMO LA COPPIA INIZIALE, LA COPPIA FINALE E SINGOLARMENTE LE VARIABILI CENTRALI

$$d_i = (l_{j_1} \vee l_{j_2} \vee z_{i_1}) \wedge (\bar{z}_{i_1} \vee l_{j_3} \vee z_{i_2}) \wedge (\bar{z}_{i_2} \vee l_{j_4} \vee l_{j_5})$$

8) $|d_i| = 5 \Rightarrow d_i = l_{j_1} \vee l_{j_2} \vee l_{j_3} \vee l_{j_4} \vee l_{j_5} \vee l_{j_6} \vee l_{j_7} \vee l_{j_8}$

$$d_i = (l_{j_1} \vee l_{j_2} \vee z_{i_1}) \wedge (\bar{z}_{i_1} \vee l_{j_3} \vee z_{i_2}) \wedge (\bar{z}_{i_2} \vee l_{j_4} \vee z_{i_3}) \wedge (\bar{z}_{i_3} \vee l_{j_5} \vee z_{i_4}) \wedge$$

$$\wedge (\bar{z}_{i_4} \vee l_{j_6} \vee z_{i_5}) \wedge (\bar{z}_{i_5} \vee l_{j_7} \vee l_{j_8})$$

CALCOLO $f = r \cdot \max_{i=1 \dots r} \{|d_i|\}$

COSTANTI PER $h \leq 3$

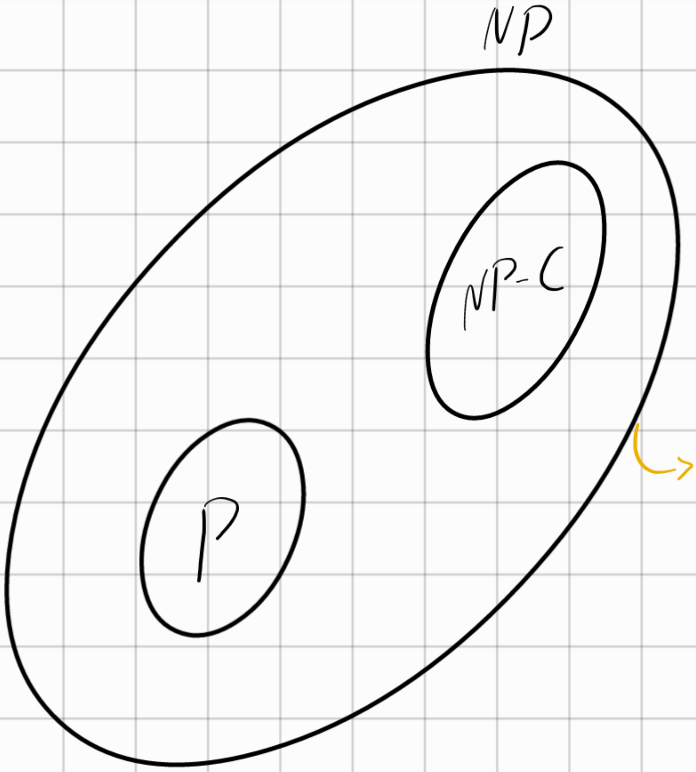
$|d_i| = h \rightarrow d_i$: $h-2$ CLAUSOLE PER $h \geq 4$

NUMERO DI CLAUSOLE DI SAT

$f(x) \in O(r \cdot |Y|) \rightarrow f(x) \in O(|g|\,|X|)$

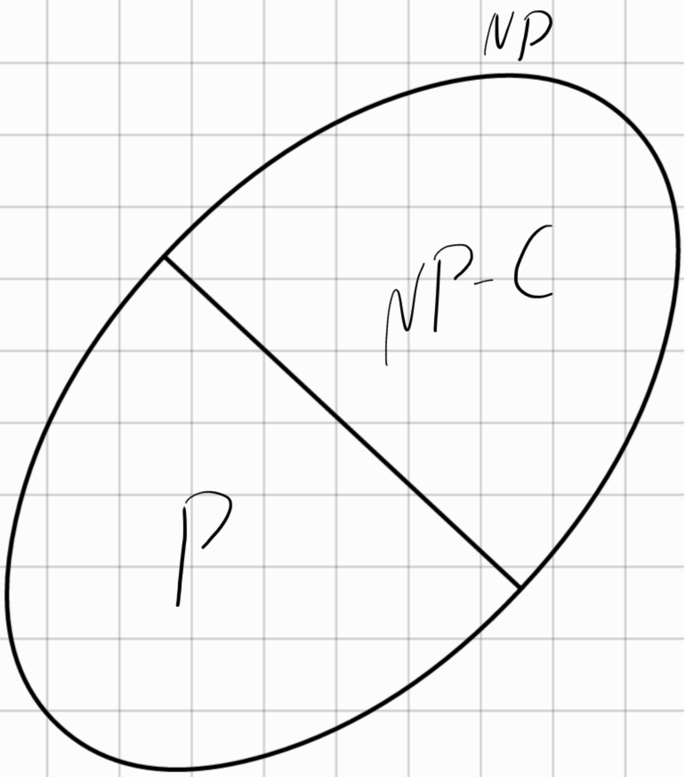
AL MASSIMO UNA CLAUSOLA d_i PUO' AVERE $|Y|$ CLAUSOLE

Struttura di NP



Fino ad ora abbiamo visto NP in questo modo

$\Downarrow$

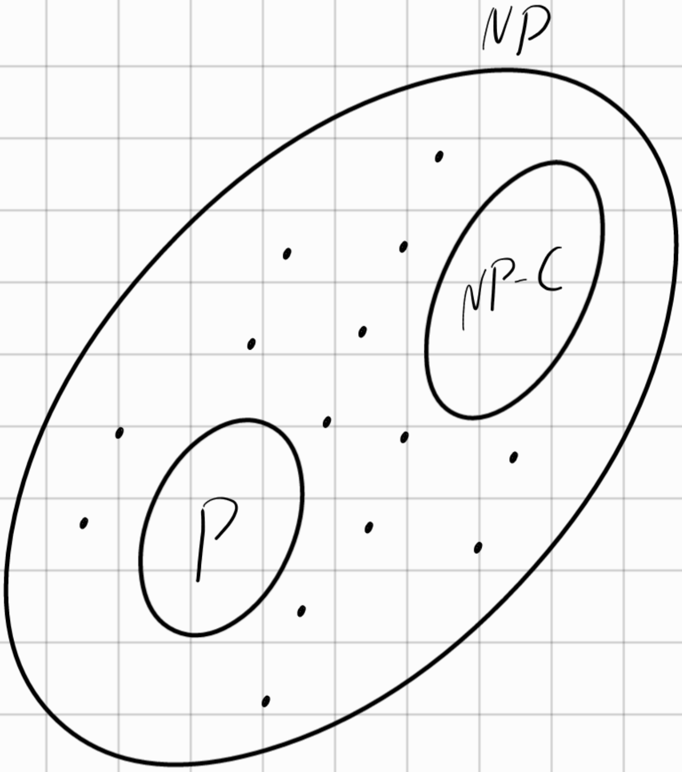


Potrebbe essere così?

Teorema di Ladner

Se $P \neq NP \Rightarrow \exists\, \Pi \in NP : \Pi \notin P \wedge \Pi \notin NP\text{-completo}$

Quindi



I problemi $\Pi \notin P \wedge \Pi \notin NP\text{-C}$ si dicono NP intermedi

↳ Mai dire che un problema sia NP-intermedio

Equivale a dire che $P \neq NP$

Quindi