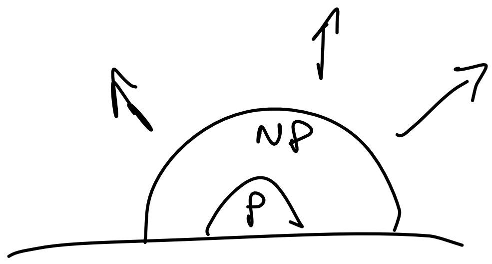
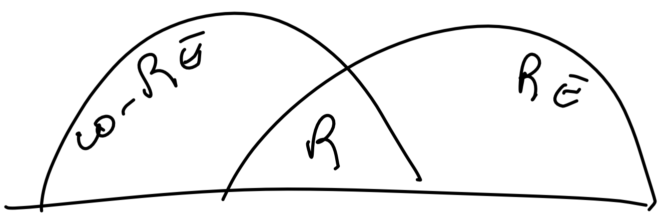
UNSAT = { ϕ / ϕ è una formula in CNF <u>non</u> soddisfacibile }

TAUT = { ϕ / ϕ in CNF che sono tautologie }

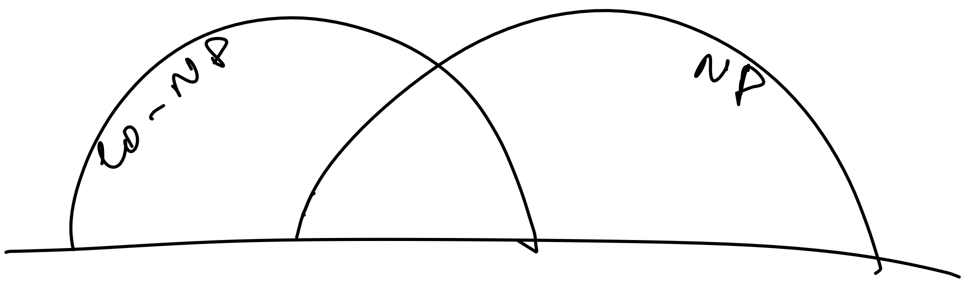
$\overline{\text{TAUT}}$

$$\text{CO-NP} = \{ L \mid \overline{L} \in NP \}$$





$$\text{co-NP} \stackrel{?}{=} NP$$

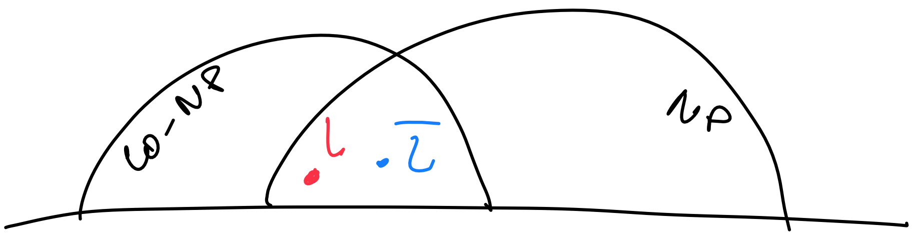


TEOREMA: NP = co-NP $\iff$ esiste un linguaggio L NP-completo t.c. $L \in$ co-NP

$\Rightarrow$) NP = co-NP $\Rightarrow$ esiste un linguaggio NP-completo in co-NP.

$\Leftarrow$) esiste un linguaggio L NP-completo che sia in coNP $\Rightarrow$ NP = coNP

- L è NP-completo $\Rightarrow$ $L \in NP$ $\Rightarrow$ $\overline{L} \in co\text{-}NP$
- $L \in coNP$ $\Rightarrow$ $\overline{L} \in NP$



- NP $\subseteq$ coNP

Sia $L' \in NP$ un linguaggio qualsiasi, mostriamo che $L' \in coNP$, e ciò lo mostriamo facendo vedere che $\overline{L'} \in NP$

→ siccome $L' \in NP$ ed inoltre L è NP-completo abbiamo che $L' \leq_p L$

→ esiste una funzione $f: \Sigma^* \to \Sigma^*$ t.c.

$\forall w \quad w \in L' \iff f(w) \in L$

→ $\forall w \quad w \notin L' \iff f(w) \notin L$

→ $\forall w \quad w \in \overline{L'} \iff f(w) \in \overline{L}$

$\Rightarrow \quad \overline{L'} \leq_p \overline{L}$

NOI ABBIAMO CHE $\overline{L} \in NP$

ABBIAMO CHE $\overline{L'} \leq_p \overline{L}$ DA CUI $\underline{\overline{L'} \in NP}$

$\Uparrow$

NP

- $coNP \subseteq NP$

SIA $L' \in coNP$ UN LINGUAGGIO ARBITRARIO

MOSTRIAMO CHE $L' \in NP$

→ $L' \in coNP \Rightarrow \overline{L'} \in NP$

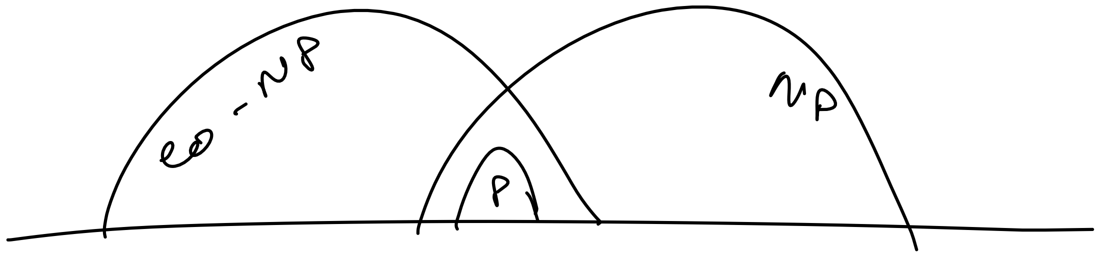
→ POICHÉ L È NP-COMPLETO, E INOLTRE $\overline{L'} \in NP$

ABBIAMO CHE $\overline{L'} \leq_p L$

→ $L' \leq_p \overline{L}$

→ ABBIAMO CHE $\overline{L} \in NP$

→ DA CUI $L' \in NP$



THEOREM: $P \subseteq NP \cap coNP$

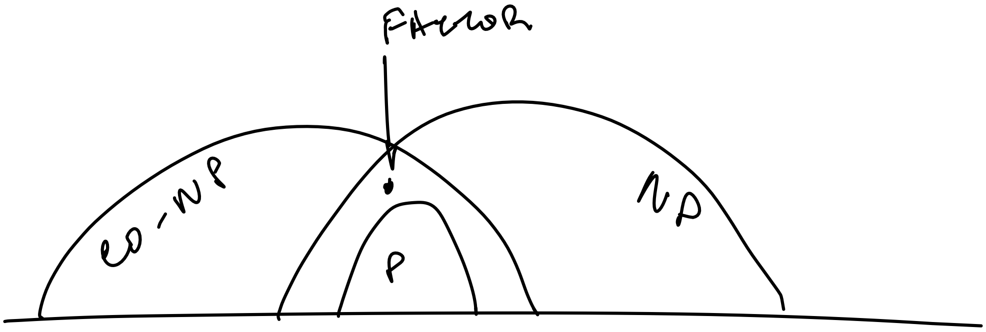
SIA L UN LINGUAGGIO GENERICO DI P.

POICHÉ $L \in P$ E $P \subseteq NP$, ALLORA $L \in NP$

CONSIDERIAMO $\overline{L}$. $\overline{L} \in P$

DA $\overline{L} \in P$ ~~SE~~ SEGUE CHE $\overline{L} \in NP$

E QUINDI $L \in coNP$



FACTOR = $\{ \langle n, k \rangle \mid$ n è un intero naturale che ha almeno un fattore primo $p \leq k \}$

$175 = 5 \cdot 5 \cdot 7$

$\langle 175, 6 \rangle \in$ FACTOR

$\langle 175, 4 \rangle \notin$ FACTOR

THEOREM: FACTOR $\in$ NP $\cap$ coNP

- FACTOR $\in$ NP

  GUESS un fattore primo $p \leq k$

  CHECK che p sia primo, e che p divida n

- FACTOR $\in$ coNP

  $\overline{\text{FACTOR}} \in$ NP

  $\overline{\text{FACTOR}} = \{ \langle n, k \rangle \mid$ n è un naturale i cui fattori primi sono tutti più grandi di $k \}$

$\overline{\text{FACTOR}} \overset{?}{\in}$ NP : GUESS della fattorizzazione di n $(p_1, p_2, \dots, p_m)$

$$EXP = \bigcup_{c \geq 1} DTIME(2^{n^c})$$

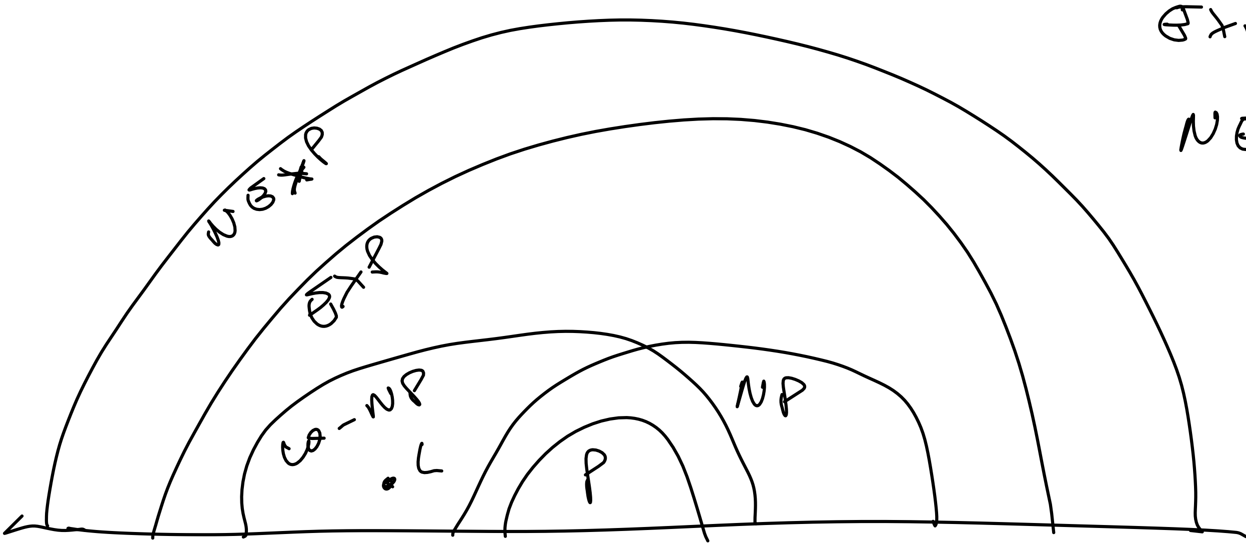
$EXP \neq P$

$EXP \overset{?}{=} NP$

$EXP \overset{?}{=} NEXP$

$NEXP \neq NP$

$$P \subseteq NP \subseteq EXP$$



- $L \in coNP \Rightarrow \bar{L} \in NP$
- $\bar{L} \in NP \Rightarrow \bar{L} \in EXP$
- $\bar{L} \in EXP \Rightarrow L \in EXP$ perché EXP è chiuso sotto complemento

$$NEXP = \bigcup_{c \geq 1} NTIME(2^{n^c})$$