

I PROBLEMI DI CLAUSE NP SONO VARI I PROBLEMI PER IL QUALE ESISTERE UN ALGORITMO DI VERIFICA POLINOMIALE.

ESEMPIO

$\Phi ::= \dots$

$$\Phi ::= x \mid \overline{x} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid \exists x. \Phi \mid \forall x. \Phi$$

↑
VARIABLE BORIANA GENERICA
FORMULA GENERICA

↑
VALORE SOLO SE ENTROGLI VENI
ESISTE ALMENO UN X TALE CHE LA FORMULA Φ SIA VERA

↑
PER OGNI X VALORE

In particolare, le formule in forma Normale Congiuntiva (CNF) e le formule Quantificate sono definite in questo modo:

$$L ::= x \mid \overline{x} \quad \text{LEMMALE}$$

$$C ::= L_1 \vee \dots \vee L_m \quad \text{CLASOLO}$$

$$\Phi_{\text{CNF}} ::= c_1 \wedge \dots \wedge c_m \quad \boxed{\text{FORMULA IN CNF}}$$

$$\Phi_Q ::= \Phi_{\text{CNF}} \mid \exists x. \Phi_Q \mid \forall x. \Phi_Q \quad \boxed{\text{FORMULA QUANTIFICATA}}$$

IMPORTANTI PER RISOLVERE PROBLEMI

PROBLEMA SAT: DATA UNA FORMULA IN FORMA NORMALE CONGIUNTIVA, DETERMINARE SE ESISTE UNA LEGGE DI VALORE DI VERA' AGLI VARIAZIONI, CHE LA rende VERA.

ESEMPIO

DATI LA PRECEDENTE DEFINIZIONE, DETERMINARE SE LA SEGUENTE FORMULA E' VERA:

$$\Phi = (x \vee y \vee \overline{z}) \wedge (\overline{x} \vee \overline{y} \vee z) \wedge y$$

$$\Phi \text{ E' VERA} \quad \text{Dunque} \quad \begin{cases} x = T \\ y = T \\ z = T \end{cases} \quad \text{INFATTI AVEMMO: } (T \vee T \vee F) \wedge (F \vee F \vee T) \wedge T = T \wedge T \wedge T = T$$

TUTTAVIA PER RISOLVERLA BISOGNA USARE UN ALGORITMO, CHE ESISTERE GIA' DIVERO IC BUTTERFLY, POSSO TUTTI LE COMBINAZIONI FINITE NON MI RESTANO TUTTE, TUTTAVIA QUESTA CRESCE IN MODO ESPONENZIALE, NON APPARTEGA SE ESISTERE UNA SOLUZIONE CHE LO RISOLVA IN TEMPO POLINOMIALE.

OGLI ALGORITMI POLINOMIALI L'ALGORITMO E' PIUTTORE EFFICIENTE ANCHE SU GRANDI INPUT, PER ESEMPIO 12 MIESSI SONO

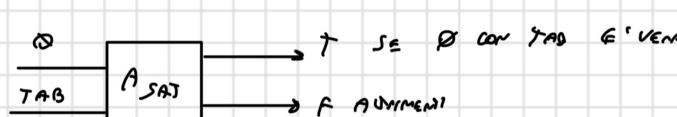
NON IMPORTA SE LA SEQUENZA E' DI 3 ELEMENTI O 3000, L'ALGORITMO E' POLINOMIALE PERCHÉ C'È UNO

SUPERAMENTE DI UNA FUNZIONE POLINOMIALE.

TORNANDO ALL'ESEMPIO DI PRIMA, IL PROBLEMA E' APERTO, INFATTI:

• LIMITI SUPERIORI: ALGORITMO ESPONENZIALE

• LIMITI INFERIORI: $\Omega(m)$ DOVE m E' LA CONGREGA DELLA FORMULA



Φ : FORMULA, TAB: TABLEAU DI VERSO'

QUESTO DIMOSTRA CHE SPESO UN ALGORITMO AI DECISIONE DENGHI UN CERTO FRAGO CHE AVERA LA VERA/DELE PROPRIETA' DA VERIFICARE, NELL'ESSEMPO DI PRIMA SOTTOVIA DI TAB.

SE \emptyset NON E' SOBVISITANTE, QUINDI $SAT(\emptyset) = F$, SIGNIFICA CHE PER TUTTE LE MAGGIA DI VERITA' CHE SONO DIFFERENTI DA 0.

SE \emptyset E' SOBVISITANTE, QUINDI $SAT(\emptyset) = T$, SIGNIFICA CHE $\exists TAB$ TALE CHE $A^{SAT}(\emptyset, TAB) = T$

ESEMPIO: CICLO HAMILTONIANO, ABBRACCIO UN GRAPPO ORIENTATO E VOGLIAMO SCOPRIRE SE ESISTE UN CAMMINO CHE TUTTI I NODI VADA SU UNA SOLO VOLTA:

- ESISTE UN ALGORITMO BRUTE FORCE, PROVA I TUTTI POSSIBILI CAMMINI
- NON SI SA SE ESISTE UN ALGORITMO POLINOMIALE CHE LO RISOLVE
- ESISTE UN ALGORITMO DI VERIFICA POLINOMIALE, DUREVO UN CERTO FRAGO = CICLO

DEFINIZIONE: UN ALGORITMO DI VERIFICA PER UN PROBLEMA (ASSIGNATO) $P \subseteq I$ E' UN ALGORITMO

$A: I \times C \rightarrow \{T, F\}$ DOVE C E' UN INSIEME DI CERTIFICATI, E $A(x, y) = T$ PER QUALCHE y SE E' SODDISFATTO $x \in P$.

NEL CASO DEI PROBLEMI CONNETTI, SI HA $I = C = \{\emptyset, 1\}^*$. QUINDI UN ALGORITMO VERIFICA UN PROBLEMA

SE PER OGNI ISTANZA CON RISPOSTA POSITIVA ESISTE UN CERTIFICATO VERSO, E' NON ESISTE PER STRATEGIE CATE NON VI APPARTENGONO.

DEFINIZIONE: UN PROBLEMA P E' NELLA CLASSE NP SE E' SODDISFATTO UN ALGORITMO DI VERIFICA

POLINOMIALE A E UNA COSTANTE $k > 0$ TAL CHE: $P = \{x \mid \exists y. A(x, y) = T, |y| = O(|x|^k)\}$

COME SI GEDE?

IL PROBLEMA P E' DEFINITO COME L'INSIEME DI TUTTI GLI INPUT X TAL CHE, ESISTE ALMENO UN CERTIFICATO y PER CUI VALE TALE $A(x, y) = T$ OVVERO: L'ALGORITMO DI VERIFICA A , CONTROLLANDO L'INPUT X INSIEME AL CERTIFICATO y , RESTITUISCE TRUE. INOLTRÉ, LA LUNGHEZZA DEL CERTIFICATO y E' POLINOMIALE RISPETTO ALLA LUNGHEZZA DEL INPUT X .

NOTA BENE: SI PUO' ANCHE DEFINIRE NP COME LA CLASSE DEI PROBLEMI PER CUI ESISTE UN ALGORITMO POLINOMIALE CHE DETERMINISCE CHE LI RISOLVE, TALE CHE' CHE SE LA RISPOSTA E' POSITIVA ESISTE UN NUMERO UNA POSSIBILE CONVERGENCE CHE E' LA RISPOSTA POSITIVA.

LEGAME CON LA VERIFICA IN TEMPO POLINOMIALE: UN ALGORITMO NON DETERMINISTICO PUO' SEMPRE ESSERE VISTO COME COMPOSTO IN 2 FASI:

- UNA PRIMA FASE NON DETERMINISTICA, CHE COSTRUISCE UN CERTIFICATO
- UNA SECONDA FASE DETERMINISTICA CHE CONTROLLA SE QUESTO CERTIFICATO E' VERSO

ALGORITMO DETERMINISTICO: DATO UN INPUT PRODUCE SEMPRE LO STESSO OUTPUT E SECONDO SEMPRE LA STESSA SQUISITTA DI INTRAZIONI PER OGNI INPUT

ALGORITMO NON DETERMINISTICO: DATA UN INPUT PROBLEMA (O PROBLEMA PROBLEMA) DIVERSE OUTPUT E PUÒ HANNE SCHEMI CASUALI
NON DETERMINISTICI DURANTE L'ESECUZIONE.

E' FACILE VERIFICARE CHE $P \subseteq NP$ PERCHÉ UN ALGORITMO DETERMINISTICO È UN CASO PARZIALE DI ALGORITMO
NON DETERMINISTICO OPPURE E GUARAVIENEMENTE A' UN CASO PARZIALE DI ALGORITMO DI VENDETTA IN CUI SI TROVA
IL CENTRALINO.