DEFINIZIONE ALTERNATIVA DI NP

REMINDER → DEFINIZIONE INFORMALE

DATO M: $TL_M(z, S_M(z)) = \exists y \in S_M(z) : \eta_M(y, z) = \text{VERO}$

$\eta(x, y)$ è' VERIFICABILE IN TEMPO DETERMINISTICO POLINOMIALE $\wedge$ y è' COSTRUITO IN TEMPO NON DETERMINISTICO POLINOMIALE $\Rightarrow [M \in NP]$

CONDIZIONE NECESSARIA

TEOREMA

$L_M(\pi) \in NP$

$\Longleftrightarrow$

$\exists\, T_V(N\bar{T}), k \in \mathbb{N}:$

SPIEGATO BENE DURANTE LA DIMOSTRAZIONE

$$\forall x \in \Sigma^*, x \in L_M(\pi) \Leftrightarrow \left[\exists y_x \in \{0,1\}^* : |y_x| \leq |x|^k \wedge T_V(N\bar{T})(x, y_x) = q_A \wedge dTIME\left(T_V(\bar{TN}), x, y_x\right) \in O(|x|^k)\right]$$

DIM

$\Rightarrow$

- DATA π CODIFICA RAGIONEVOLE t.c. $\pi : \mathcal{J}_M \to L_M(\pi)$
- $L_M(\pi) \in NP \Rightarrow \exists N\bar{T}, k : \forall x \in L_M(\pi)\left[N\bar{T}(x) = q_A \wedge hTIME(N\bar{T}, x) \in O(|x|^k)\right]$
  $\forall x \notin L_M(\pi)\left[N\bar{T}(x) \neq q_A\right]$

- SCRIVIAMO UN ALGORITMO CHE SIA EQUIVALENTE AD NT

INPUT: $x \in \{0,1\}^*$ → INSIEME DI QUINTUPLE

COSTANTI: $P = \{P_1, \dots, P_m\}, q_0, q_A$

$q \leftarrow q_0$, $Y_x \leftarrow \emptyset$

FOR $(i \leftarrow 1;\ i \leq |x|^{ic};\ i{+}{+})$ DO

  SCEGLI $P_j \in P$

  $Y_x \leftarrow Y_x \oplus P_j$ → CONCATENAZIONE

END

VERIFICA CHE Y_x SIA UNA COMPUTAZIONE ACCETTANTE DI x

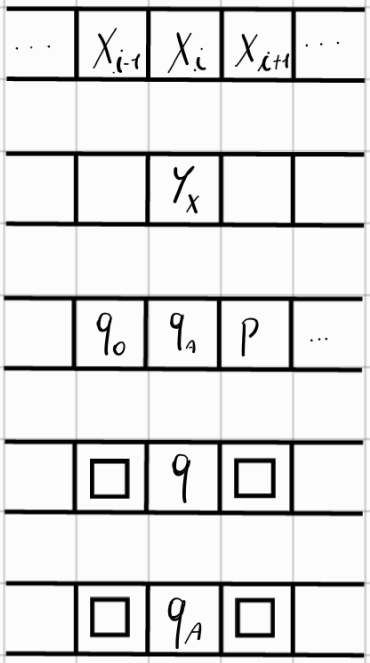
RETURN q

- LA VERIFICA VIENE ESEGUITA DA UNA MACCHINA T_V → VERIFICATORE

- COSTRUIAMO $T_V(NT)$:

  INPUT: x, Y_x, q_0, q_A, P

ESEGUE UNA SERIE DI CONTROLLI



→ CI SI SCRIVE LA STRINGA IN INPUT

→ SCRIVIAMO LA SEQUENZA DI QUINTUPLE DA ESEGUIRE

→ SCRIVIAMO LE COSTANTI

→ SCRIVIAMO LO STATO CORRENTE

→ STATO D'ACCETTAZIONE

- LA MACCHINA $T_V(NT)(x, Y_x)$ ESEGUE LA COMPUTAZIONE Y_x SU x E VERIFICA CHE PORTI IN q_A → CERTIFICATO

- $T_V(NT)$ VIENE ESEGUITA IN $O(|x|^k)$ IN QUANTO → CONDIZIONE DEL FOR
  Y_x È LA CONCATENAZIONE AL MASSIMO DI $|x|^k$ QUINTUPLE

- QUINDI SE
  $$L(\pi) \in NP \Rightarrow \exists T_V(NT)(x,y), k \in \mathbb{N} :$$

$$\forall x \in \Sigma^* \; x \in L(\pi) \iff \left[\exists Y_x : |Y_x| \leq |x|^k \wedge T_V(NT)(x, Y_x) = q_A \wedge dTIME\left(T_V(NT), x, Y_x\right) \in O(|x|^k)\right]$$

$Y_x \in \{0,1\}^*$

- PER SEMPLICITÀ POSSIAMO CODIFICARE Y_x COME UNA STRINGA $\in \{0,1\}^*$

⇐

- DOBBIAMO CREARE UNA NT CHE ACCETTI L CONOSCENDO T_V, k

- CREIAMO UNA MACCHINA $NT_{CALCOLA}$

```
INPUT : x
B ← T_S(|x|)        → FUNZIONE TIME COSTRUCTIBLE CHE CALCOLA LA LUNGHEZZA DI Y_x
                      → |x|^k
FOR(i←1; i≤B; i←i+1) DO BEGIN
    SCEGLI SE Y_x,i ← 1 OR Y_x,i ← 0
    Y_x ← Y_x ⊕ Y_x,i
END
RETUR Y_x
```

- $NT_{CALCOLA}$ VIENE ESEGUITA IN $O(|x|^k)$

- CREIAMO ORA NT CHE ACCETTA $L(\pi)$

  INPUT: $x \in \{0,1\}^*$

  $y_x \leftarrow NT_{CALCOLA}(x) \longrightarrow O(|x|^{ic})$

  $q \leftarrow T_v(NT)(x, y_x) \longrightarrow O(|x|^{ic})$

  ↳ DATA DALLE IPOTESI

  RETURN q

- SE $x \in L(\pi) \Rightarrow \exists y_x \dots T_v(NT)(x, y_x) = q_A \Rightarrow NT = q_A$

- SE $x \notin L(\pi) \Rightarrow \forall y_x \in \{0,1\}^* \dots T_v(NT)(x, y_x) = q_R \Rightarrow NT \neq q_A$

OSS

SE ANALIZIAMO BENE L'ENUNCIATO DEL PROBLEMA POSSIAMO NOTARE CHE:

1) y_x È IL NOSTRO CERTIFICATO CALCOLATO IN TEMPO NON DETERMINISTICO $O(|x|^{ic})$

2) T_v È IL NOSTRO VERIFICATORE CHE AGISCE IN TEMPO DETERMINISTICO $O(|x|^{ic})$

INOLTRE IL TEOREMA CI STA DICENDO CHE UN PROBLEMA STA IN NP SE E SOLO SE AMMETTE UN CERTIFICATO E UN VERIFICATORE