ALCUNI ESEMPI E OSSERVAZIONI SU $\exists$SO E FO(LFP)

$\boxed{\exists SO}$

- COSA OFFRE, IN TERMINI DI ESPRESSIVITÀ, LA QUANTIFICAZIONE AL SECOND'ORDINE ESISTENZIALE?
- PERCHÉ $\exists SO \supsetneq FO$
- COSTRUIAMO UN ESEMPIO DI FORMULA F IN $\exists$SO TALE CHE NESSUNA FORMULA G IN FO SIA TALE PER CUI $\text{struct}(G) = \text{struct}(F)$
- COME È POSSIBILE, AD ESEMPIO, CATTURARE IL PROBLEMA PARITY?

$$\mathcal{L} = \{ s \in \{0,1\}^* \mid \#_1(s) \text{ È PARI} \}$$

DOVE $\#_b(s)$ STA PER IL NUMERO DI OCCORRENZE DEL BIT b NELLA STRINGA s

- POSSIAMO PROCEDERE NEL MODO SEGUENTE

$$F \equiv \exists X^1 . X^1(0) \wedge \Big(\forall x . \Big[x < \max \rightarrow$$
$$(X^1(x) \wedge S(x) \rightarrow \neg X^1(x+1)) \wedge$$
$$(\neg X^1(x) \wedge S(x) \rightarrow X^1(x+1)) \wedge$$
$$(X^1(x) \wedge \neg S(x) \rightarrow X^1(x+1)) \wedge$$

$\left(\neg X^1(x) \wedge \neg S(x) \longrightarrow \neg X^1(x+1)\right)\Big]\Big) \wedge X^1(max)\Big)$

INTUITIVAMENTE, QUESTA FORMULA CORRISPONDE ALL'ALGORITMO SEGUENTE

```
fun Parity(S: string): boolean
    var X: array
    X[0] ← True
    for i ← 0 to |S|-1 do
        if X[i] ∧ S[i] then
            X[i+1] ← False
        if ¬X[i] ∧ S[i] then
            X[i+1] ← True
        if X[i] ∧ ¬S[i] then
            X[i+2] ← True
        if ¬X[i] ∧ ¬S[i] then
            X[i+1] → False
    return X[|S|]
```

$\boxed{\text{FO(LFP)}}$

- RICORDIAMO CHE:
  - → IN FO(LFP) POSSIAMO PRENDERE IL MINIMO PUNTO FISSO DI FORMULE X^{un}-POSITIVE, CIOÈ DI FORMULE AL PRIM'ORDINE CHE FACCIANO RIFERI-

MENTO A X^m, IN CUI LE VARIABILI $x_1, \dots x_m$ OCCORRONO LIBERE E IN CUI OGNI OCCORRENZA DI X^m SIA POSITIVA, OVVERO SIA NELLO SCOPE DI UN NUMERO PARI DI NEGAZIONI.

$$X^2(x_1, x_2) \quad \checkmark$$

$$\neg X^2(x_1, x_2) \quad \times$$

$$\underbrace{X^2}(x_1, 0) \longrightarrow X^2(x_2, 0) \quad \times$$

$$S(x_1) \longrightarrow X^2(x_1, x_2) \quad \checkmark$$

$$\neg\neg X^2(X_1, X_2) \quad \checkmark$$

- DI CIASCUNA TRA TALI FORMULE POSSIAMO CONSIDERARE IL MINIMO PUNTO FISSO

$$LFP(X^m, x_1, \dots, x_m, F)$$

IL QUALE DIVENTA UN PREDICATO m-ARIO NELLA NOSTRA LOGICA.

- SAPPIAMO CHE QUESTO NUOVO PREDICATO È INTERPRETATO COME IL MINIMO PUNTO FISSO DI UN FUNZIONALE

A_n È L'UNIVERSO

$A_n^m = A_n \times A_n \dots \times A_n$

$$F^I : \mathcal{P}(A_n^m) \longrightarrow \mathcal{P}(A_n^m)$$

INSIEME DELLE PARTI

$$D \overset{F^I}{\longmapsto} \{(a_1, \dots, a_m) \in A_n^m \mid (A_n, I), \xi \models F, \text{ DOVE } \xi(X^m) = D \quad \xi(x_i) = a_i\}$$

- CONSIDERIAMO UN ESEMPIO DI FORMULA CHE IN UN CERTO SENSO CHE VEDREMO, CATTURI PARITY

$$F \equiv (x_1 = 0 \wedge x_2 = 0) \vee$$

$$\Big(\exists y . (1 + y = x_1) \wedge$$

$$\Big[(X^2(y,1) \wedge S(x_1) \wedge x_2 = 0) \vee$$
$$(X^2(y,1) \wedge \neg S(x_1) \wedge x_2 = 1) \vee$$
$$(X^2(y,0) \wedge S(x_1) \wedge x_2 = 1) \vee$$
$$(X^2(y,0) \wedge \neg S(x_1) \wedge x_2 = 0) \Big] \Big)$$

TUTTE OCCORRENZE POSITIVE

SE PRENDIAMO $LFP(X^2, x_1, x_2, F)$

OTTENIAMO PROPRIO IL PREDICATO CHE CI SERVE.

> TEOREMA (COROLLARIO DEI TEOREMI DI KNASTER-TARSKI E KLEENE)
>
> IL FUNZIONALE F^I, OGNIQUALVOLTA F È X^m-POSITIVA HA UN MINIMO PUNTO FISSO $\mu^I X^m(x_1, \dots x_m).F$.
>
> INOLTRE,
>
> $$\mu^I X^m(x_1, \dots, x_m).F = \bigcup_{n \in \mathbb{N}} (F^I)^n(\emptyset)$$

CALCOLIAMO ALCUNI VALORI DI $(F^I)^n$ NEL NOSTRO ESEMPIO, SUPPONENDO CHE S SIA INTERPRETATA COME LA STRINGA 1010, OSSIA CHE S^I CONTENGA I VALORI 1 E 3

$$(F^I)^0(\emptyset) = \emptyset$$

$$(F^I)^1(\emptyset) = F^I(\emptyset) = \{(0,0)\}$$

$$(F^I)^2(\emptyset) = F^I(\{(0,0)\}) = \{(0,0),(1,1)\}$$

$$(F^I)^3(\emptyset) = \{(0,0),(1,1),(2,0)\}$$

DIMOSTRAZIONE DEL TEOREMA DI FAGIN - PRIMA PARTE

$\boxed{\text{TEOREMA. } \exists SO = NP}$

$\exists SO = \{ struct(F) \mid F$ È FORMULA AL SECOND'ORDINE ESISTENZIALE $\}$

$\exists SO \subseteq NP$

- IN QUEST'INCLUSIONE CI OCCUPIAMO DI DIMOSTRARE CHE OGNI FORMULA F ESISTENZIALE AL SECOND'ORDINE È TALE PER CUI ESISTE UNA MdT NONDETERMINISTICA E POLYTIME M_F CHE DECIDE PROPRIO $struct(F)$
- ABBIAMO BISOGNO DI UN PAIO DI LEMMI AUSILIARI

LEMMA 1

- OGNIQUALVOLTA ESISTA ALMENO UN SIMBOLO PREDICATIVO DI ARIETÀ ALMENO PARI AD 1, VALE CHE

$$|bin^n(I)| \geq n$$

DIMOSTRIAMOLO

- SE ESISTE COME PER IPOTESI, UN SIMBOLO PREDICATIVO P_j DI ARIETÀ ALMENO PARI AD 1, ALLORA AVREMO CHE

$$|bin^n(I)| = |bin^n(P_1) \dots bin^n(P_m) \; bin^n(f_1) \dots bin^n(f_k)|$$

$$\geq |bin^n(P_j)| = n^{ar(P_j)} \geq n$$

$\boxtimes$

$\boxed{\text{LEMMA 2}}$

$$FO \subseteq P$$

DIMOSTRIAMOLO

- DIMOSTRARE $FO \subseteq P$ SIGNIFICA DIMOSTRARE CHE PER OGNI F CHIUSA NELLA LOGICA AL PRIMORDINE, $struct(F) \subseteq P$
- NON POSSIAMO PROCEDERE QUINDI PER INDUZIONE PERCHÉ F POTREBBE AVERE SOTTOFORMULE APERTE, ALLE QUALI NON SI PUÒ APPLICARE L'IPOTESI INDUTTIVA.
- OCCORRE QUINDI DIMOSTRARE UN RISULTATO LEGGERMENTE PIÙ FORTE, OVVERO IL SEGUENTE:

  PER OGNI F CON VARIABILI LIBERE $x_1, \dots, x_m$ ESISTE UN ALGORITMO $\mathcal{A}_F$ POLYTIME TALE CHE SU INPUT $S, i_1, \dots, i_m$ DETERMINA SE $S = bin^n(I)$ DOVE

$$(A_n, I), \xi \models F$$

DOVE $\xi(x_j) = i_j$

QUESTO È EFFETTIVAMENTE UNO STATEMENT CHE POSSIAMO DIMOSTRARE PER INDUZIONE SULLA STRUTTURA DI F:

- SE $F: P(t_1, \dots, t_p)$ ALLORA A_F PROCEDERÀ NEL MODO SEGUENTE:
  - PRIMA DI TUTTO CALCOLANDO $[\![t_i]\!]_\xi$ DOVE ξ È L'AMBIENTE CHE ASSEGNA i_j AD x_j
  - POI, CONTROLLA CHE L'INTERPRETAZIONE DI P, RICAVABILE DA S SIA TALE PER CUI $([\![t_1]\!]_\xi, \dots [\![t_p]\!]_\xi)$ APPARTIENE A TALE INTERPRETAZIONE.

  OSSERVIAMO CHE IN QUESTO MODO A_F DETERMINA CORRETTAMENTE SE

$$(A_n, I), \xi \models F.$$

- SE $F = F_1 \wedge F_2$, ALLORA A_F LO COSTRUIRÒ A PARTIRE DA A_{F_1} E A_{F_2}, I QUALI ESISTONO PER IPOTESI INDUTTIVA. IN PARTICOLARE A_F RITORNERÀ IL VALORE 1 SSE A_{F_1} E A_{F_2} RITORNANO IL VALORE 1
- SE $F = F_1 \vee F_2$ O $F = \neg F_1$, ALLORA

SI PROCEDE ESATTAMENTE COME NEL CASO PRECEDENTE

- SE $F = \exists x. G$ ALLORA PROCEDIAMO USANDO L'IPOTESI INDUTTIVA E IL LEMMA 1. PER L'IPOTESI INDUTTIVA, INFATTI, A_G ESISTE POLYTIME. INOLTRE A_G SI ASPETTA ANCHE UN INPUT i_q RELATIVO PROPRIO ALLA VARIABILE x. CIÒ CHE FARÀ A_F È CHIAMARE A_G PIÙ VOLTE, UNA PER OGNI VALORE POSSIBILE DI i_q. POICHÉ IL NUMERO DI TALI VALORI POSSIBILI È n E PER IL LEMMA 1, $|bin^n(I)| \geq n$ A_F PRENDERÀ TEMPO POLINOMIALE. IL RISULTATO RESTITUITO DA A_F SARÀ INFINE 1 SSE A_G RITORNA 1 ALMENO UNA VOLTA.
- SE $F = \forall x. G$, ALLORA POSSIAMO PROCEDERE ANALOGAMENTE AL CASO PRECEDENTE

$\boxtimes$