24/4/2008

FO(LFP) = FIRST ORDER + LEAST FIXED POINT

<u>ES.</u>: CHIUSURA TRANSITIVA E^* DI $E \subset V$ SODDISFA A UN'EQ. DI P. FISSO:

$E^*(x,y) \Leftrightarrow x=y \vee \exists z[E(x,z) \wedge E^*(z,y)]$ (GRAFO $G=(V,E)$)

<u>NOTAZIONI</u>: $E^* = LFP_{\varphi,R,x,y}$, $\varphi \equiv [x=y \vee \exists z(E(x,z) \wedge R(z,y))]$

$f: \mathcal{P}(V^2) \longrightarrow \mathcal{P}(V^2)$, $f(R)=R'$: $R'(x,y) \Leftrightarrow [x=y \vee \exists z: E(x,z) \wedge R(z,y)]$

E' CRESCENTE, QUINDI: $\emptyset \subset f(\emptyset) \subset \_\ \_\ \_ \subset f^k(\emptyset) = \underbrace{f^{k+1}(\emptyset)}_{"E^*}$, $k \leq n^2$, $n=|V|$

VOGLIAMO DIMOSTRARE: $FO_{\leq}(LFP) = PTIME$

σ LINGUAGGIO I ORDINE, $S \subset \{\sigma\text{-STRUTTURE}\}$; DATA A S-STRUTTURA $\overset{\text{ORDINATA}}{\downarrow}$, SI PUÒ CODIFICARE CON UNA STRINGA BINARIA, $bin(A)$:

$Dom(A) = n$ $(\{0, \ldots, n-1\})$; $R \subset n^2$; $R \in 2^{n^2}$ $(c \in n = 2^{\log n})$

ALLORA, AD OGNI $\varphi \in FO(LFP)$ ASSOCIO UNA $T \in PTIME$ (E VICEVERSA) T.C. $A \models \varphi \Leftrightarrow T(bin\ A)\downarrow$.

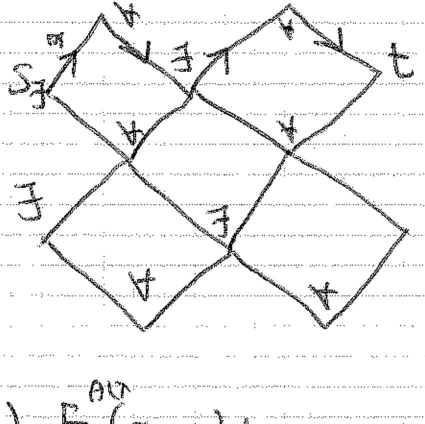
GRAFO ALTERNANTE

PROBLEMA <u>REACH</u>: $\sigma = (E^2, s, t)$, $G=(V,E,s,t) \in REACH \Leftrightarrow$

$\Leftrightarrow E^*(s,t)$, DOVE $E^* = LFP_{\varphi,R,x,y} \in FO(LFP)$; OSSIA, REACH =

= $Mod(\varphi)$, PER QUALCHE $\varphi \in FO(LFP)$. CIÒ CATTURA IL CONCETTO DI

NON DETERMINISMO. VEDIAMO IL CONCETTO DI ALTERNANZA.



; $REACH_{ALT} \subset \sigma$-STRUTTURE, CON

$\sigma = (E^2, s, t, G^1_\forall, G^1_\exists)$.

DEFINIAMO LA CHIUSURA ALTERNANTE:

E^{ALT} ~~(x,y)~~ È LA PIÙ PICCOLA RELAZIONE T.C.

1) $E^{ALT}(x,x)$;

2) $G_\exists(x) \wedge \exists z$ T.C. $(E(x,z) \wedge E^{ALT}(z,y)) \Rightarrow E^{ALT}(x,y)$;

3) $G_\forall(x) \wedge \forall z(E(x,z) \rightarrow E^{ALT}(z,y)) \Rightarrow E^{ALT}(x,y)$

$[\wedge \exists z: E(x,z)])$ (PER NON QUANTIFICARE A VUOTO)

ALLORA, $REACH^{ALT} \iff E^{ALT}(s,t)$. È DEFINIBILE IN FO(LFP)?

$E^{ALT}(x,y) \iff x=y \vee [\exists z(E(x,z) \wedge E^{ALT}(z,y))] \wedge G_{\forall}(x) \to \forall z$ $[E(x,z) \to E^{ALT}(z,y))]]$. CONSIDERO ORA LA FORMULA:

$R'(x,y)$: $R' = \varphi(R,x,y) \iff \{x=y \vee [\exists z(E(x,z) \wedge R(z,y))) \wedge$
$\wedge G_{\forall}(x) \to \forall z(E(x,z) \to R(z,y))]]\}^{=\varphi}$: DÀ UNA FUNZIONE:

$f: P(V^2) \to P(V^2)$, $f(R) = R'$ MONOTONA ⟹ HA PUNTO FISSO. PERCIÒ:

$LFP_{\varphi,R,x,y} = E^{ALT} \in FO(LFP)$.

OSS.: φ PUÒ ANCHE NON ESSERE DEL PRIMO ORDINE: E SI PUÒ OTTENERE COME LFP DI QUALCOS'ALTRO, OSSIA SI PUÒ ITERARE IL PUNTO FISSO.

ORA DIMOSTRIAMO CHE $PTIME = FO(LFP)$

AD OGNI T CORRISPONDE φ

OSSIA, $\forall$ T.C. $T(bin A) \iff A \models \varphi$ (φ σ-FORMULA CON $\leq$, $+$, $\cdot$, BIT)

$\subseteq$: IDEA: $REACH^{ALT}$ È PTIME-COMPLETO

($S \leq_p S'$ SE $\exists f \in PTIME$ T.C. $w \in S \iff f(w) \in S'$)

E QUI SI PUÒ PORRE $S' = REACH^{ALT}$.

INOLTRE, $REACH^{ALT}$ È PTIME-COMPLETO PER FO-RIDUZIONI.

$\supseteq$: IDEA: IL LFP SI CALCOLA ITERANDO UNA f CRESCENTE, $f: P(A^k) \to P(A^k)$ AL MASSIMO n^k VOLTE, $n=|A|$, QUINDI POLINOMIAL

INOLTRE OSSERVIAMO CHE PTIME = A LOG SPACE, CHE CI SERVE PER DIMOSTRARE REACH ∈ PTIME.

DETTAGLI: $FO \subset NL (\subset AL = PTIME)$; OSSIA, $\forall \varphi \in FO$, $\exists T_\varphi \in PTIME$ T.C. $T_\varphi(bin A) \iff A \models \varphi$.

CASO BASE: $\sigma = (E^2, s, t)$, $\varphi \equiv E(s,t)$;

$A(V,E,s,t)$: $E \subseteq V^2$; ALLORA $bin(A) = \overset{n^2}{bin(E)}\,\overset{\log n}{bin(s)}\,\overset{\log n}{bin(t)}$, DOVE

$bin(E) \in 2^{n^2}$ $(n \in \mathbb{N})$

$\langle b_0, \dots, b_{n^2-1} \rangle$ ED $E(a,b) \Leftrightarrow b_{a\cdot n+b} = 1$

DATA $\varphi \in E(s,t)$, VOGLIO UNA $T \in$ PTIME T.C. $\forall A$ σ-STRUTTURA, $A = (V, E, s, t)$

$A \models \varphi \Leftrightarrow T(bin(A))\downarrow$. IN REALTÀ, ADDIRITTURA SI TROVA $T \in$ LOGSPACE

$\Updownarrow$ (DATI $\overset{a,b}{}$, MI SPOSTO DI $a\cdot n+b$ E VERIFICO SE IL BIT È 1...)

$E^A(s^A, t^A)$

POI, SE HO UNA COMB. BOOLEANA DI PEZZI ELEMENTARI, COSTRUISCO LE LORO T E POI LE METTO INSIEME. LA COSA COMPLICATA SONO I QUANTIFICATORI:

$\varphi = \exists x\, \vartheta(x)$, $\sigma = \langle E^2, s, t \rangle$

VOGLIO T_φ. INNANZITUTTO, SO COSTRUIRE $T_{\vartheta(c)}$ SU UN LINGUAGGIO

$\sigma' = \langle E^2, s, t, c \rangle$. LO FACCIO IN LOGSPACE $\subset$ PTIME.

INPUT: $\overset{|A|=n}{bin(A)} = bin(E, s, t)$; CICLO SU TUTTI I VALORI DI $x \in A$, QUINDI x È UNA STRINGA BINARIA LUNGA $\log n$. AD OGNI PASSO CHIAMO $T_{\vartheta(c)}$ SU INPUT $bin(A)^\frown x = bin(B)$ (CON $B \in \sigma'$).

SE $T_{\vartheta(c)}(bin(A)^\frown x)\downarrow$ ALLORA $T_{\exists x \vartheta x}(bin(A))\downarrow$, ALTRIMENTI PASSO A $x+1$ (BINARIO).

IDEM PER $\forall x\, \vartheta x$. CIÒ DIMOSTRA: FO $\subset$ LOGSPACE $\subset$ PTIME

~~ORA~~ VEDREMO: FO(LFP) $\subset$ PTIME, CIOÈ:

: DATA $\varphi \in$ FO(LFP), TROVARE $T_\varphi \in$ PTIME T.C. $\forall A \in \sigma$,

$A \models \varphi \Leftrightarrow T_\varphi(bin(A))\downarrow$.

ES.: $\sigma = \langle E, s, t \rangle$; PRENDIAMO $\varphi = E(s,t)$, MA COSÌ $\varphi \in$ FO.

SE $\varphi = E^*(s,t)$, SAPPIAMO CHE PER PASSARE DA E A E^* DEFINIAMO:

SE $E^* = E^r$ (DOVE $f^r(\emptyset) = f^{r+1}(\emptyset)$), $E^r(x,y) \Leftrightarrow$ (VADO DA x A y IN MENO DI n PASSI).

28/4/2008

HIERARCHY THEOREM

$TIME(f(n)) \subsetneq TIME((f(n))^3)$

DA QUESTO SI PUÒ DIMOSTRARE: $P \subset EXP$.

MdT A PIÙ STRINGHE: (K, Σ, δ, s)

K = STATI;

Σ = ALFABETO;

$\underset{\uparrow \text{PROGRAMMA}}{\delta}: K \times \Sigma^n \longrightarrow (K \cup \{h, \text{"SÌ"}, \text{"NO"}\}) \times (\Sigma \times \{\leftarrow, -, \rightarrow\})^n$, s = STATO INIZIALE
h = STATO FINALE

COME SI SIMULA UNA MdT A PIÙ NASTRI CON UNA MdT A UN NASTRO?
[F.C. HENNIE, R.E. STEARNS, "TWO-TAPE SIMULATIONS OF MULTITAPE TURING MACHINES", J. ACM 13.4, PP. 533-546, 1966]

IN REALTÀ IL LIMITE È: $TIME(f(n)) \subsetneq TIME(f(n)\,g(n))$ CON $g(n) > \log(n)$

$M(X) \Rightarrow M': \underset{\uparrow \text{INIZIO NASTRO}}{\triangleright} x \underset{\downarrow \text{FINE NASTRO}}{\triangleleft} \underbrace{\triangleright \triangleleft \overset{\triangleright\triangleleft}{\blacktriangleleft} \ldots \triangleright \triangleleft}_{K \text{ BLOCCHI}} \underset{\uparrow \text{FINE DESCRIZIONE}}{\triangleleft}$ (K = NUM. NASTRI)

CI SONO K BLOCCHI CIASCUNO AL PIÙ $n+2$, $+1$: LA LUNGH. DELLA RAPPRESENTAZIONE È $K(n+2)+1$, AL PIÙ

ALFABETO DI M': $\Sigma' = \Sigma \cup \underline{\Sigma} \cup \{\triangleright, \triangleleft, \triangleleft', \sqcup\}$

QUESTO PORTA A UN TEMPO $T = 4(K(f(n)+2)+1) + K(2K(f(n)+2)+1)$ RISPETTO ALL'INPUT SU UN SINGOLO ~~NASTRO~~ PASSO OSSIA $T \cdot f(n)$ ~~SU M NASTRI~~ IN TOTALE.

CIÒ DÀ UN TEMPO $\simeq 2K^2 f^2(n)$, CHE PERÒ SI PUÒ CONSIDERARE $O(f(n))$.

LINEAR SPEED-UP: SE HO UNA MACCHINA M DI TEMPO $f(n)$, SI PUÒ EMULARE CON UNA M' DI TEMPO $\varepsilon f(n) + n + 2 + \lceil \frac{\varepsilon}{6} \rceil n$ $(\forall \varepsilon > 0)$.

(SCRITTURA: $n+2$; SPOSTAMENTI E LETTURE: TUTTO IL RESTO)

IN REALTÀ, CIÒ CHE SI DIMOSTRA È: $TIME(f(n)) \subsetneq TIME((f(2n+1))^3)$.

<u>LEMMA 1</u>: $H_f \notin TIME(f(\lfloor \frac{n}{2} \rfloor))$.

<u>LEMMA 2</u>: $H_f \in TIME((f(n))^3)$.

H_f È UNA DESC. MODIFICATA DEL LINGUAGGIO HALTING H:

$H = \{(M; x) : M$ TERMINA SU INPUT x ACCETTANDO$\}$.

[illegible] $D(M) = \neg H(M,M)$; $D(D) \Leftrightarrow \neg H(D,D) \Leftrightarrow \neg D(D)\downarrow$, ASSURDO.

$H_f = \{ (M, x) :$ M(x) TERMINA ACCETTANDO IN TEMPO $f(n) \}$. DA CUI:
$n = |M| + |x|$

H NON E' CALCOLABILE, H_f SI'.

DIM. LEMMA 1: COME SOPRA, SE $D(M) = \neg H_f(M,M)$, ALLORA

$D(D) \Leftrightarrow \neg H_f(D,D) \Leftrightarrow D(D)\downarrow_f$; ASSURDO. $\boxed{OK}$

DIM. LEMMA 2: COSTRUIAMO UNA MdT UNIVERSALE

INPUT: (M, x) ; OUTPUT: $M(x)$ SE SI ARRESTA IN MENO DI $f(n)$.

LA MACCHINA HA 4 NASTRI:

$\triangleright \ulcorner M \urcorner, \ulcorner x \urcorner \rightarrow$ CODIFICA DI

$\triangleright S, \alpha_1, \dots, \alpha_K$

$\triangleright \ulcorner M \urcorner$

$\triangleright \sqcup f(\ulcorner x \urcorner)$

A OGNI PASSO SCANDISCE L'INPUT AVANTI E INDIETRO E RIPORTA LE INFORMAZIONI SU x. POI SCANDISCE M IN CERCA DI REGOLE CHE CORRISPONDANO ALLA POSIZIONE INIZIALE E DOPO OGNI PASSO CANCELLA UNO DEI SIMBOLI DELL'ULTIMO ~~[illegible]~~ NASTRO

IN TOTALE, OGNI PASSO SI SIMULA IN: $l_M K_M^2 f(|x|) \leq l_M K_M^2 f(n) \leq$

$(l_M =$ LUNGH. CODIFICA DI UNO STATO$)$

$\leq (\log(n))^3 f(n) \leq O(f^2(n))$ E QUINDI IL TOTALE DEI PASSI SI SIMULA IN $O(f^3(n))$. $\boxed{OK}$

ORA, $TIME(f(n)) \not\ni H_{f(2n+1)}$ MA $H_{f(2n+1)} \in TIME((f(2n+1))^3)$ E QUESTO DA' SUBITO LO HIERARCHY THEOREM. $\boxed{OK}$

COROLL.: $TIME(2^n) \supseteq P$

$\not\cap$

$TIME((2^{2n+1})^3) = TIME(2^{6n+3}) \subseteq EXP$; DA CUI, $P \subsetneq EXP$.

PER LO SPAZIO, VALE: $SPACE(n) \subset SPACE(f(n) \log f(n))$

PSPACE $\subset$ EXPTIME NON SI SA SE STRETTA.

2/5/2008

TEOR.: PTIME = FO(LFP)

DATA σ SEGNATURA (= LINGUAGGIO DEL 1° ORDINE, = SIMBOLI DI REL. E COSTANTE), UNA σ-STRUTTURA A; SE $N \in PTIME$: MACCHINA DI TURING; $\exists \varphi \in FO(LFP)_\sigma$ T.C. $N(bin(A))\downarrow \iff A \models \varphi$ E VICEVERSA.

DIM.: AVEVAMO DIMOSTRATO CHE $FO \subset P$ (IN REALTÀ, $FO \subset \overset{L}{LOGSPACE} \subset P$), OSSIA, DATO σ E DATA $\overset{\text{CHIUSA}}{\varphi} \in FO$, $\exists N \in L\text{-}TM$ T.C. $N(bin\,A)\downarrow \iff A \models \varphi$.

ORA DIMOSTRIAMO CHE $FO(LFP) \subset P$: FISSATA σ, DATA $\varphi \in FO(LFP)_\sigma$, $\exists M \in P\text{-}MT$ T.C. $\forall$ σ-STRUTTURA A, $A \models \varphi \iff M(bin\,A)\downarrow$.
$M = M_\varphi$ E VERRÀ COSTRUITA PER INDUZIONE SU φ. IL CASO INTERESSANTE È QUANDO $\varphi = LFP_{R,\vec{x},\varphi}(\vec{s})$.

ES.: $E^*(x,y) \iff x=y \vee \exists z\,[E(x,z) \wedge E^*(z,y)]$; ESISTE COMUNQUE LA MINIMA RELAZIONE CHE SODDISFA QUESTA CONDIZIONE.
SE $\varphi \equiv [x=y \vee \exists z[E(x,z) \wedge R(z,y)]] = \varphi(R,x,y)$,
$E^* = LFP_{R,x,y,\varphi}$; NON È UNA FORMULA.

FISSATA σ-STRUTTURA A (AD ES. $A = (|A|, E)$) E DATA $R \subset A^2$, HA SENSO CALCOLARE $R' \subset A^2$. $R_0 = \emptyset$, $R_{i+1} = R'_i$; $\exists r$ T.C. $R_r = R_{r+1} =$ $= LFP_{R,x,y}\,A$ (DOVE $R' = \varphi(R,x,y)$) $r \leq n^k$, K = ARITÀ DI R.

(RIFERIMENTI: FOCL: IMMERMAN PAG. 46; $FO(LFP) \subset P$: IMMERMAN PAG. 60)

SUPPONIAMO DI AVERE UN LINGUAGGIO CON COSTANTI;
$\varphi = LFP_{R,\vec{x},\varphi}(\vec{s})$; COSTRUIAMO M_φ: $M_\varphi(bin\,A)\downarrow \iff A \models \varphi$.
NEL CASO E^*, ~~$M(bin(E, s_0, s_1$~~ $A = (|A|, E, s_0, s_1)$;
$bin(A) = bin(E)\ bin(s_0)\ bin(s_1)$; $M(bin\,A)\downarrow \iff A \models LFP_{R,\vec{x},\varphi}(\vec{s}) \iff$
(LUNGHEZZE → n^2 $\quad \log n \quad \log n$)

$\iff E^*(s_0, s_1)$.

SUL NASTRO DI INPUT ABBIAMO bin(A); SUL NASTRO DI LAVORO, ALL'INIZIO ABBIAMO bin(∅); AD OGNI PASSAGGIO ABBIAMO bin(R), $R \subset n^k$, QUINDI $R \in 2^{n^k}$. SU UN ALTRO NASTRO, CALCOLIAMO bin(R'), CON $R'(\vec{x}) = \varphi(\vec{R}, \vec{x})$. COME LO CALCOLIAMO? SUPPONIAMO PER SEMPLICITÀ $K=2$ ($R \in 2^{n^2}$), QUINDI $bin(R)_{an+b} = 1 \iff R(a,b)$.

ALLORA $R'(x,y) \iff \varphi(R,x,y)$. VOGLIAMO CHE $\mathrm{bin}(R')_{an+b} \iff R(a,b)$.
PER INDUZIONE, $\exists T_\varphi$ CON $\varphi \in \sigma'$-FORMULA, $\sigma' = \sigma \cup \{c_0, c_1, R\}$
E SI HA $\mathrm{bin}(R')_{an+b} = 1 \iff T_\varphi(\mathrm{bin}\,R, \mathrm{bin}\,A, \mathrm{bin}\,b)$. CICLIAMO SU TUTTE LE COPPIE (a,b) (SONO n^2), SCRIVIAMO $\mathrm{bin}\,R$, $\mathrm{bin}\,A$, $\mathrm{bin}\,b$ E CONTROLLIAMO R'. ABBIAMO COSÌ UNA FUNZIONE $R \to R'$. CANCELLIAMO R SIMETTIAMO R' E ITERIAMO FINCHÉ NON TROVIAMO UN PUNTO FISSO.
ALLA FINE CONTROLLIAMO SE R VALE PER $\{c_0, c_1\}$ E SI FA ANDANDO A CONTROLLARE ~~TE POSTI~~ SE ~~MEMORIZZATO NEL~~ IL BIT AL POSTO $c_0 n + c_1$ È 0 O 1 E ABBIAMO FINITO. $\boxed{\text{OK}}$ $\boxed{P \subset FO(LFP)}$

ORA DIMOSTRIAMO $FO(LFP) \subset P$. SI FA IN DUE PASSAGGI:
$P \leq_{FO} REACH_{ALT} \in FO(LFP)$ E $REACH_{ALT}$ È P-COMPLETO.
SFRUTTIAMO IL FATTO CHE $P = ALOGSPACE = \bigcup_c ASPACE(c \log n)$.
$REACH_{ALT}$: (IMMERMAN PAG. 53):

$$G = (V, E^{(2)}, \underset{G_\forall, G_\exists}{\overset{\shortparallel}{A^{(1)}_{IN}}}, s, t). \quad REACH_{ALT} = LFP_{R,x,y,\varphi} : \varphi(R,x,y) \iff$$

$$\iff x = y \lor [G_\exists(x) \land \exists z (E(x,z) \land R(z,y))] \lor [G_\forall(x) \land \forall z (E(x,z) \to R(z,y)) \land \underbrace{\exists z\, E(x,z)}_{\downarrow \text{NON SI QUANTIFICA A VUOTO.}}]$$

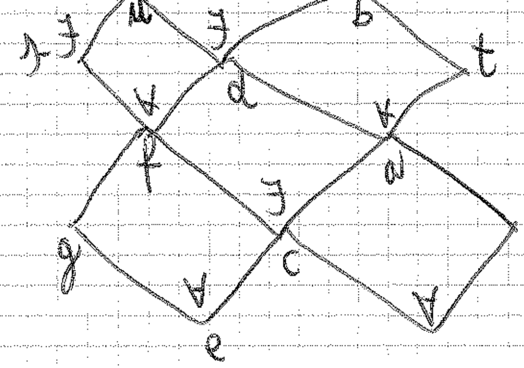
QUINDI $REACH_{ALT}(x,y) \iff \varphi(REACH_{ALT}(x,y))$.

<u>OSS</u>: $REACH_{ALT} \in P$; ANZI, $REACH_{ALT}$ È LINEARE.
[$REACH_{ALT} \in P$: $\exists M \in PTIME$: $M(\mathrm{bin}\,G)\downarrow \iff REACH_{ALT}(s,t)$]

ALGORITMO (IMMERMAN PAG. 54): LAVORIAMO CON UNA QUEUE = CODA. INPUT: G.

```
CODA := $\emptyset$, MARK(t)
INSERT(t)
WHILE CODA $\neq \emptyset$ DO
    { RIMUOVI IL PRIMO ELEMENTO $x$ DELLA CODA,
      FOR $y$: $E(y,x)$ DO   [E $y$ NON MARCATO]
        { RIMUOVI IL LATO $(y,x)$
          IF $G_\exists(y)$ $\lor$ $y$ NON HA ARCHI USCENTI, THEN {MARK($y$),
              INSERT $y$ } } }
IF s È MARCATO, THEN ACCETTA, (ELSE RIFIUTA). END.
```

Ⓒ :



{ a NON SI INSERISCE PERCHE' NON SUPERA IL TEST: b SI'. }

b ~~t~~ b VIENE MARCATO

d ~~b~~ (d E' ∃, QUINDI SUPERA IL TEST ED E' MARCATO)

u ~~d~~ (u PASSA IL TEST ED E' MARCATO, f NO)

s ~~u~~

~~s~~ (FINE)

I NODI $\overset{x}{\text{MARCATI}}$ SONO TUTTI E SOLI QUELLI $\overset{\text{TALI}}{\text{x CHE}}$ (REACH (x,t))

Ⓓ : FACILE; Ⓔ : UN PO' MENO, MA SI FA.

5/5/2008

$SO(LFP) = EXPTIME$

LINGUAGGIO $L = \{ c_1, \dots, c_r, E_1^{n_1}, \dots, E_j^{n_j} \}$ (COSTANTI)

VARIABILI RELAZIONI R_1^k; HANNO UNA ARITA' FISSATA E POSSONO ESSERE QUANTIFICATE: $\forall R_1^k (\dots)$.

ES.: DEFINIZIONE SUI NUMERI NATURALI DEL PRINCIPIO D'INDUZIONE:

$$\forall R^1 \{ R^1(0) \wedge \forall x (R^1(x) \rightarrow R^1(Sx)) \rightarrow \forall x R^1(x) \}.$$

ES.: $REACH_{s} \in SO$ [OSS.: $FO(LFP) \subset SO$] DA CUI: $P \subset SO$

$L = \{ E^2_1, s, t \}$ (RELAZIONI DEFINENTI IL GRAFO)

$$\forall R^2 [(\forall x, y, t \ (R(x,y) \wedge R(y,t) \rightarrow R(x,t)) \wedge \forall x, y \ E(x,y) \Rightarrow R(x,y)) \rightarrow R(s,t)] \Leftrightarrow E^*(s,t)$$ (CHIUSURA TRANSITIVA DI E)

POSSIAMO ORA DEFINIRE $LFP_{\varphi, x, R}(\vec{t})$, CON R VARIABILE RELAZIONALE:

$$LFP_{\varphi, x, R}(\vec{t}) \Leftrightarrow \forall S (\varphi(S) = S \wedge S(\vec{t}))$$

OSS.: $SO = PH = \bigcup_{k,l} ATIME\text{-}ALT(n^k, l)$ (l = NUM. FISSATO DI ALTERNANZE DI QUANTIFICATORI).

OSS.:
$FO(LFP) = P \subseteq PH = SO \subset SO(LFP) = EXPTIME$

OSS.: $NP = \exists SO$; $NP^{MON} = \exists R^1 (SO)$ (I GRAFI SCONNESSI STANNO IN NP^{MON} MA NON IN $co\text{-}NP^{MON}$)

$\neq$

$co\text{-}NP^{MON} = \forall R^1 (SO)$.

E' APERTO IL PROBLEMA SE $NP = co\,NP$; SE FOSSERO DIVERSI, AVREMMO $P \neq NP$.

COSTRUIAMO ORA L'LFP PER IL 2° ORDINE:

$LFP^2_{\varphi, x, y, R, G}$

DOVE $G^l(R_1, R_2, \dots, x_1, x_2, \dots, x_j)$ = RELAZIONE FRA RELAZIONI.

ES.: CONTENIMENTO FRA RELAZIONI:

$$\subseteq (R_1, R_2) \Leftrightarrow \forall \vec{x} (R_1(\vec{x}) \rightarrow R_2(\vec{x}))$$

$(R_1^k = R_2^k) \vee (\exists R_3^k$ T.C. $\varphi(R_1^k, R_3^k) \wedge G(R_3^k, R_2^k))$,

ES: SIA $\varphi(R_1^k, R_2^k, G) \Leftrightarrow$;

VOGLIAMO TROVARE IL MINIMO G PER CUI CIO' ACCADE; QUESTO SARA' $LFP_{\varphi, R_1, R_2, G}$

$\boxed{SO(LFP) \subset EXPTIME}$: SE HO UNA φ DEL 2° ORDINE, VOGLIO COSTRUIRE UNA MACCHINA CHE DICA SE E' VERA.

φ PUO' ESSERE:

$\varphi_1 \wedge \varphi_2$, $\varphi_1 \vee \varphi_2$, $\neg \varphi_1$, $\exists x \varphi_1(x)$, $\forall x \varphi_1(x)$.

SI PROCEDE PER INDUZIONE: SUPPONIAMO DI AVERE M_φ CHE VERIFICA φ IN UN LINGUAGGIO ESTESO $L' = L \cup \{c\}$ IN CUI x E' UNA COSTANTE. CICLIAMO SU n VALORI.

SE $\varphi = \exists R_1^k \varphi_1(R_1^k)$, ANCHE QUI SUPPONIAMO DI AVERE M_φ IN $L' = \{R^k\} \cup L$ E CICLIAMO SU 2^{n^k} VALORI. LA PARTE DELICATA E' LFP.

$\varphi = LFP_{\varphi, \vec{R}, \vec{x}, G}(\vec{P}, \vec{C})$, CON $\vec{P}, \vec{C}$ COSTANTI DI RELAZIONE.

SUPPONIAMO PER COMODITA' $G = G(R_1^k, \dots, R_l^k)$; $|\mathrm{bin}\, G| = 2^{n^k l}$.
OGNI VOLTA CHE UNA PARTICOLARE l-UPLA DI RELAZIONI VERIFICA G, METTIAMO "1" NEL BIT CORRISPONDENTE. SE OGNI R_i VIENE RAPPRESENTATA DA UN NUMERO $0 \leq n_i < 2^{n^k}$, IL CORRISPONDENTE BIT E'

$n_1 + n_2 2^{n^k} + n_3 2^{2n^k} + \dots + n_l 2^{(l-1)n^k}$.

LAVORIAMO IN $L' = L \cup \{F^l\}$; CALCOLIAMO $\varphi(\vec{x}, \vec{R}, G)$;

QUANTO CI VUOLE A ENUMERARE TUTTE LE FUNZIONI $\varphi(\vec{x}, \vec{R}, F^l) \to F^{l'}$? PER CALCOLARNE UNA IMPIEGHIAMO 2^{n^k}. PER CALCOLARE LFP, OGNI VOLTA CHE CALCOLIAMO UN'ITERAZIONE LA CONFRONTIAMO CON LA VECCHIA; SE E' UGUALE, CI FERMIAMO. POICHE' LA STRINGA E' LUNGA 2^{ln^k}, AL MASSIMO IMPIEGHIAMO TEMPO $2^{2^{ln^k}}$. RESTANO LE FORMULE ATOMICHE:
PRESE $R_i = R_i(c_1, \dots, c_k)$ CON SOLO COSTANTI, $G(R_1, \dots, R_l)$ SI CALCOLA ANCORA IN EXPTIME COME SOPRA (SI RAPPRESENTANO COME $2^{n^k}, 2^{2n^k}, \dots, 2^{(l-1)n^k}$). QUINDI $M_\varphi \in EXPTIME$.

$\boxed{SO(LFP) \supseteq EXPTIME}$ SFRUTTIAMO IL FATTO CHE EXPTIME = APSPACE.

SE $M \in ASPACE(n^k)$, USA UN NASTRO LUNGO AL PIÙ n^K, QUINDI LE SUE CONFIGURAZIONI SONO $2^{n^k} \cdot \#STATI \cdot \underset{\downarrow}{n^k} \cong 2^{n^{k+1}}$. AL SECONDO ORDINE

POSIZIONE DELLA TESTINA

LO SI PUÒ ESPRIMERE COME RELAZIONE: UNO STATO DELLA MACCHINA È UNA RELAZIONE $(K+1)$-ARIA. VOGLIAMO COSTRUIRE UNA φ CHE CI DICA CHE

K+1 NON MOLTO GRANDE

$C_1 \vdash^M C_2$. C_1 RAPPRESENTA LA POSIZIONE $n_1 + n_2 \cdot n + \dots + n_K \cdot n^{K-1}$.

$C_1(n_1, \dots, n_k, J, q, p, p')$: ~~CON CONTENUTO~~ POSIZIONE DEL NASTRO, SIMBOLO IN QUELLA POSIZIONE, STATO, POSIZIONE DELLE TESTINE SUI NASTRI DI INPUT E DI LAVORO. $J \in \{0,1\}$, $q \in \{0, \dots, \#STATI\}$, $0 \leq p, p' \leq$ [illegible] n^K.

A QUESTO PUNTO, SCRIVENDO LA RELAZIONE DI PASSAGGIO $\vdash^M$, SAPPIAMO SE SI PUÒ PASSARE DA C_i A C_j, $\forall i, j$:

ALLORA, $\varphi(C_1^{2k}, C_2^{2k}, G) \iff C_1 = C_2 \vee (q_\forall(C_1) \wedge \forall C_3^{2K}(C_1 \vdash^M C_3 \rightarrow G(C_3, C_2)))$ $\vee (q_\exists(C_1) \wedge \exists C_3^{2k}(C_1 \vdash^M C_3 \wedge G(C_3, C_2)))$.

G COMPARE POSITIVAMENTE $\Rightarrow$ POSSIAMO FARNE L' $LFP_{\varphi, C_1, C_2, G}(C_1', C_2')$.

A QUESTO PUNTO, M ACCETTA $\iff LFP_{\varphi, C_1, C_2, G}(C_0, C_F)$, E SIAMO ARRIVA

A DIRE CHE $\forall M \exists \varphi \forall A \; M(bin A) \iff A \models \varphi$.

DEFINIZIONE DI $\vdash^M$: $C_1 \vdash^M C_2$ SE $\bigvee$ [illegible] DI CASI:

$\circ \; \delta: (\underset{\substack{\uparrow \\ INPUT}}{w}, \underset{\substack{\uparrow \\ LAVORO}}{b}, \underset{\substack{\uparrow \\ STATO}}{q}) \longrightarrow (q', (SX, DX), b')$ $\circ$ — — ALTRI CASI.

3/2008

FINE <u>DIM.</u> $P = FO(LFP)$

<u>TEOR.</u> FAGIN: $SO\exists = NP$

<u>TEOR.</u>: $NP^{MON} \neq CO\text{-}NP^{MON}$

<u>DIM.</u> $P \subset FO(LFP)$: 1) – $P = ALOGSPACE = ASPACE(\log n)$;
2) – $REACH_{ALT} \in P$ (IMMERMAN PAG. 54);
3) – $REACH_{ALT} \in FO(LFP)$; (IMMERMAN PAG. 59)
4) – $P \leq_{FO} REACH_{ALT}$. (QUESTO VA FATTO) (IMMERMAN PAG. 51) O QUASI

3): $$\varphi(R,x,y) \equiv x=y \vee [G_\exists(x) \wedge \exists z[E(x,z)\wedge R(z,y)]]$$
$$\vee [G_\forall(x) \wedge \forall z[E(x,z) \wedge R(z,y)]$$
$$\vee \exists z\, E(x,z)]];$$

VOGLIAMO LA MINIMA R T.C. $R(x,y) \Leftrightarrow \varphi(R,x,y)$. ALLORA $R = E_{ALT}$.
$R = LFP(\varphi_{R,x,y})$. QUINDI, $\underset{\underset{G}{\shortparallel}}{LFP}_{\varphi,R,x,y}(s,t) \in FO(LFP)$.

4): NELL'IMMERMAN SI DIMOSTRA $NL \leq_{FO} REACH$, CON DIMOSTRAZIONE ESSENZIALMENTE UGUALE.
SI SFRUTTA IL FATTO CHE $P = ALOGSPACE$. SIA $N \in ASPACE(c \cdot \log n)$
FISSO $\sigma = \langle R_1^{a_1}, \dots, R_r^{a_r}, c_1, \dots, c_s \rangle$; ALLORA VOGLIAMO DIRE CHE
$\forall$ σ-STRUTTURA A, $N(bin\, A)\downarrow \Leftrightarrow I(A) \in REACH_{ALT}$, CON
$I(A) = G(V, G^1_\forall, G^1_\exists, E^2, s, t)$; PONIAMO

$V = A^{1+a+c}$, DOVE c = COSTANTE CHE COMPARE IN "$c \log n$",
$a = \max_i \{a_i\}$. ALLORA L'IDEA E' CHE $I(A)$ = GRAFO DELLE
CONFIGURAZIONI DI N SU INPUT $bin\, A$ E SICCOME N E' ALT, SARA' UN GRAFO ALTERNANTE. SUPPONIAMO CHE $|A| = n$ E $A = \{0, \dots, n-1\}$
UNA ID (ISTANTANEOUS DESCRIPTION) E' UNA $(1+a+c)$-UPLA
$I = \langle p, r_1, \dots, r_a, w_1, \dots, w_c \rangle \in V$ DOVE:
$\vec{w} = (w_1, \dots, w_c) \in n^c = 2^{c \log n}$ CODIFICA IL CONTENUTO DEL NASTRO DI LAVORO DI N.
$R_i \subset n^{a}$ E QUINDI $R_i \in 2^{n^a}$ $\forall i$; $\vec{r} \in n^a$ E QUINDI $2^{a \log n}$.

<u>OSS</u>: NON SI PUO' CODIFICARE L'INPUT, PERCHE' E' TROPPO LUNGO ($n > \log n$): SE $r=1$, CODIFICHIAMO LA POSIZIONE DELLA TESTINA SULL'INPUT, POICHE' $R \subset n^a \Rightarrow R \in 2^{n^a}$. IN QUESTO CASO SPECIALE,
$|bin R| = n^a$

L'INPUT E' UNA STRINGA $\leq 2^{n^a}$, MA LA POSIZIONE E' UN NUMERO DI LUNGHEZZA $n^a = 2^{a \log n}$. ORA, PONIAMO $p = \langle i, \text{STATO}, \text{POS. NASTRO LAVORO}, \forall / \exists \rangle$

CON $i \leq r$ INDICA SU QUALE R_i STA LA TESTINA DI INPUT

p CODIFICA: QUALE R_i STIAMO LEGGENDO, LO STATO DI N, LA POSIZIONE DELLA TESTINA SUL NASTRO DI LAVORO (CHE HA LUNGHEZZA LOGARITMICA: $c \log n \leq n$) E SE LO STATO E' $\forall$ O $\exists$.

$\boxed{E}$ SIA LA FUNZIONE DI TRANSIZIONE DI N; $E(ID, ID') \Leftrightarrow ID \vdash_{N} ID'$

$G_\exists(ID) = G_\exists(\langle p_1, p_2, p_3, p_4, \vec{r}, \vec{w} \rangle) \Leftrightarrow (p_4 = 0)$;

$G_\forall(ID) = G_\forall \qquad \Leftrightarrow (p_4 \neq 0)$.

s = CONFIG. INIZIALE SU INPUT (bin A): $\vec{p} = \vec{r} = \vec{w} = 0$;

t = CONFIG. FINALE: $\vec{p} = \vec{r} = \vec{w} = MAX$.

<u>OSS.</u>: $E(ID, ID')$ DIPENDE DA N MA NON DA A.

<u>ES.</u>: $\sigma = \langle R^2 \rangle$; $N: \langle q, \underset{\substack{\uparrow \\ \text{INPUT} \\ 0,1}}{b}, \underset{\substack{\uparrow \\ \text{LAVORO} \\ 0,1}}{v} \rangle \xrightarrow{\rho} q', v', \underset{\substack{\uparrow \\ \text{SPOST.} \\ \text{INPUT}}}{x}, \underset{\substack{\uparrow \\ \text{SPOST.} \\ \text{LAVORO}}}{y'}$.

$\underset{=}{\langle p, r_1, r_2, \vec{w} \rangle} \qquad \underset{=}{\langle p', r_1', r_2', \vec{w}' \rangle}$

ALLORA, $ID \vdash_\rho ID'$ QUANDO? IL PROBLEMA E': COME SI CONOSCE L'INPUT, NON ESSENDO CODIFICATO?

$bin(A) = bin(R) \in 2^{n^2}$; $|bin(R)| = n^2$; $(bin(R))_{an+b} = 1 \Leftrightarrow R(a, b)$

ALLORA SI PASSA DA ID A ID' QUANDO ρ E' APPLICABILE, CIOE' $(b = 0 \wedge \neg R(r_1, r_2)) \vee (b = 1 \wedge R(r_1, r_2))$. DOVREMMO AVER DIMOSTRATO (MODULO DETTAGLI) CHE: <u>TEOR.</u>: DATA $N \in ASPACE(c \log n)$, DATO

$\sigma = \langle R_1^{a_1}, \ldots, R_r^{a_r}, c_1, \ldots, c_s \rangle$, PONENDO $K = 1 + a + c$, $\exists$ UNA QUERY K-ARIA I (OSSIA $\exists$ FORMULE $\langle E, G_\forall, G_\exists, \alpha, \omega \rangle = I$, CON $E(ID, ID') = E(x_1, \ldots, x_k, y_1, \ldots, y_k)$, $\alpha(x_1, \ldots, x_k)$, IDEM ω) T.C. DATA A, QUESTE FORMULE DEFINISCONO $I(A) = \langle A^k, E^A, G_\forall^A, G_\exists^A, \alpha^A, \omega^A \rangle$ E $I(A) \in REACH_{ALT} \Leftrightarrow N(bin(A))\downarrow$. $\boxed{OK}$

SI DA' PER ACQUISITO CHE $A \mapsto I(A)$ E' POLINOMIALE (SI BASA SU $FO \subset L \subset P$). QUINDI, <u>$P = FO(LFP)$</u>. $\boxed{OK}$

TEOR. FAGIN: $NP = SO\exists$, IN PARTICOLARE, $FO(LH) \subseteq SO\exists$.

ESEMPI: $SAT \in SO\exists$; $3\text{-COL} \in SO\exists$:

$\Gamma = \langle E^{(2)} \rangle$ LINGUAGGIO DEI GRAFI; VOGLIAMO $\varphi \in SO\exists$ T.C.

$A \models \varphi \Leftrightarrow A \in 3\text{-COL}$.

$\varphi = \exists R^1, Y^1, B^1 : \forall x$

$$[Rx \vee Yx \vee Bx] \wedge \forall y [E(x,y) \rightarrow \neg(Rx \wedge Ry) \wedge$$

$\wedge \neg(Yx \wedge Yy) \wedge \neg(Bx \wedge By)]$. OSS: MANCA L'IPOTESI CHE OGNI VERTICE ABBIA UN UNICO COLORE, MA CIÒ NON ALTERA LA SITUAZIONE.

PER QUANTO RIGUARDA SAT: SUPPONIAMO DI AVERE FORME NORMALI CONGIUNTIVE E CHE IL NUM. DI VARIABILI SIA UGUALE AL NUM. DELLE CLAUSOLE.

$A = (n, P^2, N^2)$ DOVE $P(a,b)$ = LA VAR. b COMPARE POSITIVAMENTE NELLA CLAUSOLA a; $N(a,b)$ NEGATIVAMENTE.

$A \in SAT \Leftrightarrow \exists S^{(1)} [\forall x \exists y ((P(x,y) \wedge S(y)) \vee (N(x,y) \wedge \neg S(y))]$.

(OSSIA: $A \models \varphi$, $\varphi \in SO\exists$) (x = CLAUSOLA, y = VARIABILE)

CLIQUE: $(G,K) \in$ CLIQUE $\Leftrightarrow$ G HA UN SOTTOGRAFO COMPLETO DI CARD. K. (ESERCIZIO: CLIQUE $\in SO\exists$). $G = (V,E)$.

OSSIA: $\exists$ PERMUTAZIONE T.C. I PRIMI K VERTICI SONO UNA CLIQUE.

$\exists f$ (BIEZ. f) $\wedge \forall i,j < K \; E(f(i), f(j))$.

$P = FO(LFP)$ / 5/ 2008

$\cap$

$NP = SO\text{-}\exists$

COROLL.: $REACH \in \exists\text{-}SO$

DIM.: E' FACILE VEDERE CHE $REACH \in \forall\text{-}SO$:

SE E^* = CH. TRANS. DI $E \Rightarrow E^*(s,t) \Leftrightarrow \underline{\underline{\forall}} R \supseteq E$ TRANS. $R(s,t)$;

CON L'$\exists$, SI PUO' DIRE: (POSTO $G = (V, E, s, t)$)

$E^*(a,b) \Leftrightarrow$

$\Leftrightarrow \exists R^2, S^1$ [R ORDINE LINEARE SU $S \wedge S(a) \wedge S(b) \wedge \forall x ($

$(Sx \rightarrow E(x, succ^R(x)))]$ DOVE SUCC E':

$y = succ^R(x) \Leftrightarrow R(x,y) \wedge \forall z \neg (R(x,z) \wedge R(z,y))$. $\boxed{OK}$

PROBLEMA APERTO: $\exists SO = \forall SO$? SE $P = NP$, SAREBBE VERO

(E' EQUIVALENTE A $NP = CO\text{-}NP$).

E' PERO' VERA: $\exists SO^{MON} = \forall SO^{MON}$.

LA DIMOSTRAZIONE NON FUNZIONA PER GRAFI INFINITI.

TEOR. FAGIN: $\exists\text{-}SO = NP$ (IMMERMAN PAG 115).

DIM.: LA PARTE FACILE E' $\exists\text{-}SO \subseteq NP$. SFRUTTIAMO IL FATTO GIA' NOTO

CHE $FO \subseteq LOGSPACE \subseteq P$.

SIA $\Phi = \exists R_1^{r_1} \ldots R_k^{r_k} \, \Psi \in \exists\text{-}SO$ IN $\sigma = (S_1, \ldots, S_l, c_1, \ldots, c$

DEVO COSTRUIRE UNA MdT $N \in NTIME(p(n))$ T.C.

$\downarrow$ POLINOMIO

$\forall A$ σ-STRUTTURA, $N(bin(A))\downarrow \Leftrightarrow A \models \Phi$.

SIA $card(A) = n$; N NON DET. SCRIVE K STRINGHE BINARIE DI

LUNGHEZZA $n^{r_1}, \ldots, n^{r_k}$, CIOE' $bin(R_1), \ldots, bin(R_k)$.

POI SCRIVENDO CONSECUTIVAMENTE $bin(A)\, bin(R_1) \ldots bin(R_k) = bin(B)$

DOVE $B = (A, R_1, \ldots, R_k)$ E' UNA σ'-STRUTTURA, CON

$\sigma' = \sigma \cup \{R_1, \ldots, R_k\}$. QUESTA STRUTTURA LA DA' IN PASTO AD UNA

MACCHINA LOGSPACE. BISOGNA ORA VERIFICARE SE $b \models \Psi$, SE SI' ACCETTA,

SE NO, RIFIUTA RISPETTO A QUELLA SUCC. NON DETERMINISTICA.

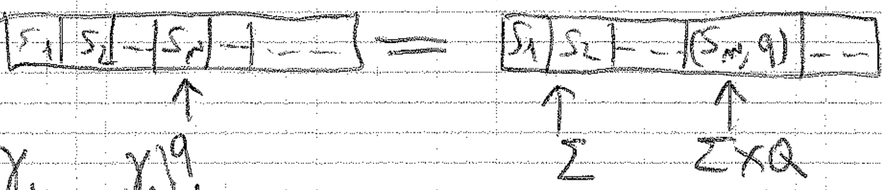
CHIARAMENTE, $A \models \Phi \Leftrightarrow \exists B$ STRUTTURA CHE VERIFICA $\Psi \Leftrightarrow$ QUALCHE

COMPUTAZIONE NON DETERMINISTICA LE SCRIVE.

$NP \subset \exists$-SO: SIA $N \in NTIME(n^k - 1)$; VOGLIAMO $\Phi \in \exists$-SO T.C. $\forall A$ σ-STRUTTURA $N(bin(A))\downarrow \Leftrightarrow A \models \Phi$.

SARA' $\Phi = \exists$ (COMPUTAZIONE ACCETTANTE).

UTILIZZIAMO UN TRUCCO:



SIA $\Gamma = \Sigma \cup (\Sigma \times Q) = \{\gamma_1, \dots, \gamma_g\}$.

$\Phi_N = (\exists C_1^{2k} \dots C_g^{2k}\, \Delta^{k})\, \varphi$. CI SONO $g+1$ QUANTIFICATORI $\exists$.

$(C_1, \dots, C_g, \Delta)$ CODIFICA UNA COMPUTAZIONE NEL MODO SEGUENTE: $C_i(s_1, \dots, s_k, t_1, \dots, t_k) \Leftrightarrow$ LA CELLA $s_1 + s_2 n + \dots + s_k n^{k-1}$ AL TEMPO $t_1 + t_2 n + \dots + t_k \underset{\vec{t}}{\underset{\parallel}{n^{k-1}}}$ CONTIENE IL SIMBOLO γ_i. SUPPONIAMO ORA CHE N FACCIA AL PIU' SCELTE BINARIE; ALLORA, $\Delta(t_1, \dots, t_k) \Leftrightarrow$ AL TEMPO $\vec{t}$ HO SCELTO "0".

CALCOLO DI φ: φ ESPRIME IL FATTO CHE $(\vec{C}, \Delta)$ E' UNA N-COMPUTAZIONE LECITA.

$\sigma = (E^{(2)}, R^{(1)})$, $A = (n, E^A, R^A)$; $bin(A) = bin(E)\, bin(R)$ CON $E \subset n^2$ (OSSIA $E \in 2^{n^2}$); $(bin\,E)_{an+b} = 1 \Leftrightarrow E(a,b)$.

φ DICE:

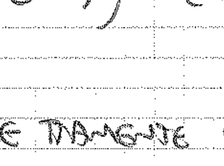
- L'INPUT E' CORRETTAMENTE CODIFICATO, OSSIA: AL TEMPO "0" SUL NASTRO DI INPUT C'E' LA STRINGA CORRETTA.

ES.: $E(2,3)\, R(5) \Rightarrow C_1(2,3,0,\vec{0}) \wedge C_1(5,0,1,\vec{0})$, OSSIA IN POS. $2+3n$ C'E' SCRITTO "1", IDEM IN POS. 5 DI bin(R). (n^2+5)

IN GENERALE, $\forall a,b,c$, $E(a,b)\, R(c) \Rightarrow C_1(a,b,0,\vec{0}) \wedge C_1(c,0,1,\vec{0})$.

- $(C_1, \dots, C_k, \Delta)$ E' UNA COMPUTAZIONE CORRETTA.

$\langle a_{-1}, a_0, a_1, \delta \rangle \xrightarrow{N} b$, CON $a_i, b \in \Gamma$, $\delta \in \{0,1\}$ SIGNIFICA:



SE N SI TROVA IN, FACENDO LA SCELTA NON DET. δ, ANDRA' IN ALTRIMENTI DETTO: $\forall t \forall s$,

$$\bigwedge_{\langle a_{-1}, a_0, a_1, \delta \rangle \xrightarrow{N} b} \left(\neg^{\delta} \Delta(\vec{t}) \vee \neg C_{a_{-1}}(\vec{s}-1, \vec{t}) \vee \neg C_{a_0}(\vec{s}, \vec{t}) \vee \neg C_{a_1}(\vec{s}+1, \vec{t}) \vee C_b(\vec{s}, \vec{t}+1)\right),$$

DOVE:

$\neg^{\circ} := \begin{cases} 1 & \text{SE } \delta=0 \\ \text{NON ESISTE SE } \delta=1 \end{cases}$ E $\vec{S}-1$ = "SPAZIO PRECEDENTE A $\vec{S}$"

POI: $\neg A \lor \neg B \lor \neg C \lor D$ È EQUIVALENTE A $(A \land B \land C) \rightarrow D$, QUINDI LA SCRITTURA DI CELLA b È IMPLICATA DA a_{-1}, a_0, a_1. STESSA COSA CON Δ: UNA VOLTA SCELTO δ, LA SCELTA È DETERMINISTICA.

- L'OUTPUT È ACCETTANTE: $C_{\langle q_{FINALE}, 1\rangle}(\vec{0}, \overrightarrow{MAX})$ (NELLO STATO FINALE C'È IL SIMBOLO DI ACCETTAZIONE).

A QUESTO PUNTO, TUTTO FUNZIONA: SE $\Phi = \exists C_1, \dots, C_g \Delta \psi$,
$\forall A$, $\forall C_1^A, \dots, C_g^A, \Delta$ SU A, $(C_1, \dots, C_g, \Delta) \models \psi \iff$
$(C_1, \dots, C_g, \Delta)$ CODIFICA UNA COMPUTAZIONE ~~ACCETTANTE~~ DI N (b,w,A). $\boxed{\text{OK}}$

COROLL.: $P \subset \exists$SO-HORN, DOVE "HORN" È UNA DISGIUNZIONE DI LETTERALI DI CUI AL MASSIMO UNO NON NEGATO. (HORN: $A \land B \land C \rightarrow D$; NON-HORN: $A \land B \land C \rightarrow D \lor E$)

OSS.: $\exists$SO È CHIUSO PER QUANTIFICAZIONI DEL I ORDINE:
$\forall x \exists R \varphi$ SI PUÒ ROVESCIARE FACENDO $\exists$(SO).
INOLTRE, $NP \subset (\exists \vec{R} \forall x \land$(COSE SENZA QUANTIFICATORI)).

ESERC.: $\forall x \exists R^{(2)} \varphi(R, x)$; RISCRIVERLA COL QUANTIFICATORE $\exists$ ALL'ESTERNO.

ASSIOMA DELLA SCELTA: $(\forall x \exists y R(x,y)) \iff \exists f \forall x R(x, f(x))$.

SI INTRODUCE UNA Q^3 T.C. $Q(x,y,z) = R_x(x,z)$
QUINDI, $\exists Q \forall x \varphi(Q(x,\cdot,\cdot), x)$.

TEOREMA DI TRAKHTENBROT 12/5/200

FINSAT NON E' RICORSIVO.

CON LA STESSA TECNICA, SI PUO' DIMOSTRARE: SAT E' NP-COMPLETO.

MdT: S (STATI); A (ALFABETO FINITO); $S \ni \overline{s}$ (INIZIALE); $* \notin A$ (SPAZIO VUOTO); $A_* = A \cup \{*\}$;

MdT $\delta: S \times A_* \dashrightarrow S \times A_* \times \{-1; 0; 1\}$ (F. PARZIALE)

$f: \mathbb{N}^k \dashrightarrow \mathbb{N}$ E' <u>CALCOLATA</u> DA δ SE $\vec{n} \in \mathbb{N}^k$ VIENE ACCETTATO DA δ COME INPUT, IL CALCOLO HA TERMINE E IN OUTPUT C'E' $f(\vec{n})$.

ESSENDO S, A_* FINITI, SI PUO' PENSARE $S, A_* \subset \mathbb{N}$ E QUINDI ASSOCIARE A δ UN NATURALE: $\varphi^{(k)}_{\delta}$. IL TEOR. DICE: $U(x,y) = \varphi^{(1)}_x(y)$ E' CALCOLABILE.

OSSIA: $\exists U$ MdT UNIVERSALE CHE PRENDE UNA MdT x E UN INPUT y E CALCOLA $\varphi^{(1)}_x(y)$.

DEF.: $A \subset \mathbb{N}$ E' DECIDIBILE (O RICORSIVO) SE $\chi_A: \mathbb{N} \to \mathbb{N}$ E' CALCOLABILE; SEMIDECIDIBILE (RIC. ENUMERABILE) SE A E' IL DOMINIO DI $\varphi: \mathbb{N} \to \mathbb{N}$ PARZIALE CALCOLABILE.

TEOR.: A DECIDIBILE $\Leftrightarrow$ A E $\mathbb{N} \setminus A$ SEMIDECIDIBILI (POST).

$K = \{e \in \mathbb{N} : \varphi^{(1)}_e(e)\downarrow\}$ E' RIC. ENUM. MA NON RICORSIVO; INFATTI $K = \mathrm{Dom}\, \tilde{U}$, $\tilde{U}(x) = U(x,x)$ E $\mathbb{N} \setminus K$ NON E' SEMIDECIDIBILE, PERCHE' SE ESISTESSE φ: $\mathbb{N} \setminus K = \mathrm{dom}\, \varphi_e$, $e \in \mathbb{N} \setminus K \Leftrightarrow \varphi_e(e)\downarrow \Leftrightarrow e \in K$.

SI HA: $RE \supseteq RIC \subseteq CO\text{-}RE$

DEF.: $A \leq_m B$ SE $\exists f: \mathbb{N} \to \mathbb{N}$ CALC. T.C. $f^{-1}(B) = A$;

$A \leq_m B$: B RIC. $\Rightarrow$ A RIC.; B RE $\Rightarrow$ A RE; $A \leq_m B \Leftrightarrow {}^cA \leq_m {}^cB$.

OSS.: $A \nleq_m {}^cA$.

$\Leftrightarrow \varphi_{s(x)}(s(x))\downarrow \Leftrightarrow s(x) \in K$.

A RE $\Rightarrow$ $A = \mathrm{dom}\, \varphi^{(1)}_e$, $x \in A \Leftrightarrow \varphi^{(1)}_e(x)\downarrow$, COSTRUIAMO $\varphi^{(1)}_{s(x)}(x) = f(x,y) = \varphi^{(1)}_e(x)$. QUINDI K E' RE-COMPLETO.

OSS.: TRAKHTENBROT $\Leftrightarrow$ $K \leq_m$ FINSAT.

DIM: $M_\delta (M_\delta)\downarrow \iff \varphi_\delta \in$ FINSAT, È EQUIVALENTE ALL'ENUNCIATO DEL TEOREMA

SIA $L = \{<^{(2)}, Q_s^{(1)}, P^{(2)}, M_\omega^{(2)}\}$; GLI ASSIOMI SONO:

$A_{x_<}$: È UN ORDINE STRETTO TOTALE; Ax_Q: $\bigwedge_{s\in S}\left(Q_s(x) \to \bigwedge_{s'\in S\setminus\{s\}} \neg Q_{s'}(x)\right)$

DOVE $Q_s(x)$ = AL TEMPO x C'È LO STATO S;

$Q(x) = \bigvee_{s\in S} Q_s(x)$ (X È UN ISTANTE DI TEMPO);

INOLTRE, $(Q(x) \wedge Q(y) \wedge x<z<y) \to Q(z)$.

$P(x,y)$: AL TEMPO x LA TESTINA È IN POSIZIONE y;

A_{x_P}: $P(x,y) \to Q(x)$, $Q(x) \to \exists y\,(P(x,y) \wedge \forall z\,(P(x,z) \to z=y))$.

$M_\omega(x,y)$: AL TEMPO x IN POS. y C'È ω; $M_*(x,y) = \bigwedge_{\omega\in A} \neg M_\omega(x,y)$.

A_{x_M}: $\bigvee_{\omega\in A} M_\omega(x,y) \to Q(x)$; $\bigwedge_{\omega\in A}\left(M_\omega(x,y) \to \bigwedge_{b\in A\setminus\{\omega\}} \neg M_b(x,y)\right)$.

DEFINIAMO ORA UNA PRECONDIZIONE DI δ:

$$PRE_\delta: \bigwedge_{(s,\omega,s',\omega',d)\in\delta} \Big(C(x,y) \wedge P(x,z) \wedge P(y,w) \wedge Q_s(x) \wedge M_\omega(x,z) \to \big(M_{\omega'}(y,z) \wedge$$

$$\wedge\, Q_{s'}(y) \wedge C_d(z,w) \wedge \big(\overset{v\neq z \Rightarrow}{\bigwedge_{b\in A_*}} (M_b(x,v) \to M_b(y,v))\big)\big)\Big),$$

DOVE: $C(x,y) = x<y \wedge \neg(\exists z : x<z<y)$;

$$C_d(x,y) = \begin{cases} C(x,y) & \text{SE } d=1 \\ x=y & \text{SE } d=0 \\ C(y,x) & \text{SE } d=-1 \end{cases}.$$

DEFINIAMO ORA: $\min_Q(x) \equiv Q(x) \wedge \forall y\,(y<x \to \neg Q(y))$;

$\max_Q$ = (IDEM); ALLORA:

$\min_Q(x) \to Q_{\bar{s}}(x)$;

$$\bigwedge_{(s,a)\in \mathrm{dom}\,\delta} \neg\left(\max_Q(x) \wedge Q_s(x) \wedge P(x,y) \wedge M_a(x,y)\right)$$

INOLTRE, SE $STR_t(x)$ = AL TEMPO x C'È LA STRINGA t, SI HA:
$\min_Q(x) \to STR_t(x)$; $MAX_Q(x) \to BINSTR(x)$ (DOVE BINSTR È UN ALTRO ASSIOMA DA DEFINIRE). QUINDI ABBIAMO GARANTITO UN MODELLO FINITO T.C.

SE TERMINA $\iff$

DIM. SAT È NP-COMPLETO: L LINGUAGGIO, C COSTANTI (FINITE); TRASFORMIAMO I QUANTIFICATORI IN $\bigvee$ E $\bigwedge$.

FUNZIONE L-FORMULE $\longrightarrow$ LUC-FORMULE T.C.:

$$\varphi \mapsto \varphi^*$$

$\varphi^* = \varphi$ SE φ È ATOMICO; $(\neg\varphi)^* = \neg(\varphi^*)$;

$(\forall x \varphi(x))^* = \bigwedge_{c \in C} (\varphi(c))^*$; $(\exists x \varphi(x))^* = \bigvee_{c \in C} (\varphi(c))^*$. INOLTRE,

$\forall x \left(\bigvee_{c \in C} x = c \right) \vdash \varphi \Leftrightarrow \varphi^*$.

ALTRA FUNZIONE: LUC-FORMULE SENZA QUANTIFICATORI $\longrightarrow$ FORMULE PROPOSIZIONALI T.C.

$R^{(k)}(c_1, \dots, c_k) \mapsto X_{R, c_1, \dots, c_k}$; "$c_1 = c_2$" $\mapsto \begin{cases} \text{TAUTOLOGIA SE } c_1 = c_2 \\ \text{CONTRADDIZIONE SE } c_1 \neq c_2 \end{cases}$

L-ENUNCIATI $\rightarrow$ FORMULE PROP. T.C. φ HA UN MODELLO DI CARD. $|C| \Leftrightarrow$

$$\varphi \mapsto \varphi^c$$

$\Leftrightarrow \varphi$ HA UN MODELLO PROPOSIZIONALE.

<u>es</u>: $\forall x \forall y R(x,y) \rightarrow (X_{R,0,0} \vee X_{0,1}) \wedge (X_{1,0} \vee X_{1,1})$.
$C = \{0,1\}$;

SIA ORA $W \subseteq \mathbb{N}$ NP, OSSIA, $\exists \delta$ MdT E POLINOMIO P T.C. $\forall n$

$n \in W \Leftrightarrow (\exists s)(|s| < p(|n|)) \wedge \varphi_\delta^{(2)}(n, s)\downarrow_{\leq p(|n|)} = 1$.

~~[illegible]~~: $\overset{\text{DATA}}{\forall}$ COMP$_\delta$ (QUELLA DEFINITA NELLA DIM. PRECEDENTE, ESTESA A COPPIE (δ, INPUT)) : $^\delta$ TRASFORMIAMO L'INPUT IN UNA FORMULA PROP.

$n \mapsto (\text{COMP}_\delta \wedge \text{INPUT}(n, \text{BINARIA}) \wedge \text{OUTPUT}_1)^{C_n}$ CON $|C_n| = p(|n|)$.

$\boxed{\text{Ok}}$

<u>OSS</u>: SI DIMOSTRA CHE ANCHE NEL LINGUAGGIO DEI GRAFI FINSAT È INDECIDIBILE.

15/5/2008

ABBIAMO VISTO: $NP = \exists SO$

QUINDI: $CO\text{-}NP = \forall SO$

ES 1: GRAFI 3-COLORABILI (V,E) = MODELLI $\left(\overset{\exists A^1, B^1, C^1}{ECC.}\right)$. $\in$

NOTIAMO CHE $P = NP \Rightarrow NP = CO\text{-}NP$, DA CUI, $NP \neq CO\text{-}NP \Rightarrow P \neq NP$.

DIMOSTREREMO CHE $NP^{MON} \neq CO\text{-}NP^{MON}$, DOVE

$NP^{MON} = (\exists^{M}$ PREDICATI UNARI$)$ FO.

ES 2: {GRAFI SCONNESSI} SI PUO' VEDERE COME MODELLI $(\exists A^1, B^1$:

$(\forall x\, Ax \underset{\overset{\uparrow}{XOR}}{\vee} Bx)(\exists x Ax \wedge \exists x Bx)(\forall x y\, Ax \wedge By \rightarrow \neg E(x,y)))$; STA IN NP^{MON}

PER CERTO $P = CO\text{-}NP$ E $P \subset NP \Rightarrow P \subset (NP \cap CO\text{-}NP)$.

INVECE, $P \not\subset NP^{MON} \cap CO\text{-}NP^{MON}$.

{GRAFI CONNESSI} $\in FO(LFP) = P \subset NP\, (\forall x, y, E^*(x,y))$; SICCOME (FAGIN) $NP = \exists SO$, SI PUO' ESPRIMERE COME $\exists$.....

UN GRAFO E' CONNESSO SE ESISTE UNO SPANNING TREE CHE COPRE TUTTI I VERTICI, OSSIA UN ORDINE PARZIALE:

~~$\forall$~~ $\exists R^{(2)}$ ORD. PARZ. STRETTO CON UNICO MINIMO: $\forall x y\; R(x,y) \wedge \neg \exists z (R(x,z) \wedge R(z,y)) \Rightarrow$

$\rightarrow E(x,y))$ ~~[illegible]~~.

GIOCHI DI EHRENFEUCHT-FRAÏSSÉ

TEOR: FISSATO UN VOCABOLARIO τ $A \equiv_m B \; (\overset{DEF}{\Leftrightarrow} \forall \varphi \in FO$, RANGO$(\varphi) \leq m$, $A \models \varphi \Leftrightarrow B \models \varphi) \Leftrightarrow$

$\Leftrightarrow A \sim_m B$ (CIOE' IL GIOCATORE "$\exists$" VINCE IL GIOCO A m MOSSE).

COME SI DIMOSTRA CHE {GRAFI CONNESSI} $\notin \exists SO^{MON}$?

PER ASSURDO, SIA $Mod(\exists P_1^1, \ldots, P_n^1 . \varphi)$ = {GRAFI CONNESSI}, DOVE $\varphi \in FO$; PER UN TEOREMA, SI POSSONO PORTARE ALL'INIZIO TUTTI I QUANTIFICATORI DEL 2° ORDINE. COSTRUIAMO 2 STRUTTURE A, B IN $\tau' = \{E^{(2)}, P_1, \ldots, P_n\}$ PENSABILI COME GRAFI COLORATI CON 2^n COLORI. SIA m = RANGO(φ);

L'IDEA E' TROVARE A CONNESSO, B SCONNESSO MA $A \equiv_m B$.

INFATTI: $\mathcal{A} = (A, E^A, P_1^A, \ldots, P_n^A)$, $\mathcal{B} = (B, E^B, P_1^B, \ldots, P_n^B)$;

(A, E^A) CONNESSO E $(A, E^A) \models \exists P_1, \ldots, P_n, \varphi$; SCELGO $P_i^A \subset A$: $(A, E^A, P_1^A, \ldots, P_n^A) \models \varphi$; COSTRUIAMO UNA NUOVA STRUTTURA

$(B, E^B, P_1^B, \dots, P_n^B) \equiv_m (A, E^A, P_1^A, \dots, P_n^A)$ MA SCONNESSA. ALLORA $(B, E^B, P_i^B) \models \varphi \Rightarrow (B, E) \models \exists P_i, \varphi$ MA QUESTO E' IL MODELLO DEI GRAFI CONNESSI, QUINDI SI HA UN ASSURDO.

A POSSIAMO SCEGLIERLO NOI; [illegible]

SIA $l \gg m$; (A, E^A) GRAFO CICLICO CON $l+1$ NODI (OSSIA: $E(i, i+1)$ PER $0 \leq i \leq l-1$ E $E(l, 0)$); SIA $(B,E) \models \exists P_1, \dots, P_n \varphi$; QUINDI $\exists\, P_1^A, \dots, P_n^A \subset A : (A, E^A, P_i^A) \models \varphi$.

PER $x \in A$, $d \in \mathbb{N}$, DEFINIAMO LA PALLA DI CENTRO x E RAGGIO d: $B_d(x) \subset A$.

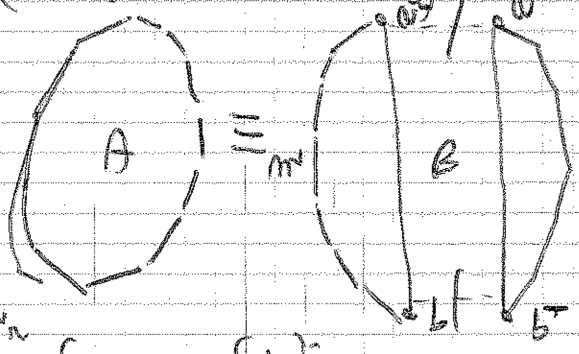
SE C'E' UN'ALTRA STRUTTURA B, E^B, P_i^B, $y \in B$, ANALOGAMENTE SI CONSIDERA $B_d(y) \subset B$. DICIAMO CHE $A,x \sim_d B,y \underset{DEF}{\Leftrightarrow} \exists$ ISOMORFISMO FRA $B_d(x) \rightarrow B_d(y)$: $x \mapsto y$.

SE $l \gg m$, ESISTONO $a, b \in A$: $B_m(a) \simeq B_m(b)$ E $B_m(a) \cap B_m(b) = \emptyset$

INFATTI: $|B_m(a)| = 2m+1$ E ABBIAMO AL PIU' $2^{n(2m+1)}$ COLORAZIONI DISTINTE SU DI ESSA; PER l ABB. GRANDE, NE TROVO DUE ISOMORFE.

"SPEZZIAMO" A IN CORRISPONDENZA DI a E b:

$B = (B, E^B)$: $|B| = |A|$, $E^B = \left(E^A \setminus \{(a^-, a), (b^-, b)\}\right) \cup$
$\cup \{(a^-, b), (b^-, a)\}$.



DEF: A τ-STRUTTURA, $\tau = (R_1^{m_1}, \dots, R_r^{m_r}, C_1, \dots, C_s)$;

IL GRAFO ASSOCIATO E' $G_A = (|A|, E^A)$ DEFINITO COSI': (GRAFO DI GAIFMAN)

$E^A = \{(a, b), a \neq b : \exists R_i^{m_i} \exists\, d_1, \dots, d_{m_i} : R(d_1, \dots, d_{m_i}) \in a, b \in \{d_1, \dots, d_{m_i}$

G_A E' NON ORIENTATO (E E' SIMMETRICO).

$A = (V, R^2)$ CON R: $R(a,b) \Leftrightarrow R(b,a) \wedge \neg R(a,a) \Rightarrow G_A = A$.

DATI $x \in A$, $d \in \mathbb{N}$, $N_d(x) = \{y \in A : d_{G_A}(x,y) \leq d\} \subset G_A$.

B τ-STRUTTURA, $y \in B$, $N_d(y)^B \cong N_d(x)^A$ CON UN ISOM. RISPET

SI DICE CHE x E y HANNO LO STESSO d-TIPO DI GAIFMAN: $A, x \underset{d}{\sim} B, y$.

TEOR. (HAUF, IMMERMAN PAG. 100): COND. SUFF PERCHE' $A \equiv_r B$ E' CHE $\forall$ ~~[illegible]~~ 2^r-TIPO DI GAIFMAN t, A, B HANNO LO STESSO NUMERO DI ELEMENTI DI TIPO t.

DIM.: LA STRATEGIA PER IL SECONDO GIOCATORE ("∃") E' DI MANTENERE IL SEGUENTE INVARIANTE: DOPO LA MOSSA m-ESIMA, $(A, a_1, \dots, a_m), (B, b_1, \dots, b_m)$, "∀" SCEGLIE AD ES. a_{m+1} DA A; "∃" CERCA UN $b_{m+1} \in B$ T.C. $(A, a_1, \dots, a_{m+1})$ E $(B, b_1, \dots, b_{m+1})$ ABBIANO LO STESSO NUM. DI ELEM. DI TIPO DI GAIFMAN 2^{r-m}.
b_{m+1} E' SCELTO DELLO STESSO 2^{r-m}-TIPO DI a_{m+1} RISP. A $(B, \{b_1, \dots, b_m\}), (A, a_1, \dots, a_m)$. ~~QUESTO E' VERO~~ PER IPOTESI INDUTTIVA $(A, a_1, \dots, a_m) \overset{2^{r-m}}{\sim} (B, b_1, \dots, b_m)$; BISOGNA DIMOSTRARE $(A, a_1, \dots, a_{m+1}) \overset{2^{r-m-1}}{\sim} (B, b_1, \dots, b_{m+1})$. SE v E' UN EL. A DISTANZA 2^{r-m-1} DA a_{m+1}, $N_{2^{r-m-1}}(v) \subset N_{2^{r-m}}(a_{m+1})$; PER ISOMORFISMO, SU $B(b_1, \dots, b_m)$, QUESTA PALLA PICCOLA CORRISPONDE A UNA ANALOGA IN B. AGGIUNGENDO a_{m+1} E b_{m+1} AL LINGUAGGI, BISOGNA DIMOSTRARE CHE C'E' UN ISOMORFISMO CHE CONSERVA I TIPI E T.C. $a_{m+1} \mapsto b_{m+1}$. LO VEDIAMO DOMANI.

DIM. DIVERSA (FLUM). 16/5/2008

INVECE DI RAGGIO 2^m, SI CONSIDERANO INTORNI DI RAGGIO 3^m. $\underbrace{}$ *

RICORDIAMO: DIMOSTRARE {GRAFI CONNESSI} ≠ MODELLI $(\exists P_1, \dots, P_n, \varphi)$, P_i RELAZIONI UNARIE, φ 1° ORDINE IN $\tau = \{E^2, P_1, \dots, P_n\}$.

PER ASSURDO, VALGA L'UGUAGLIANZA.

SIA $m = \text{rango}(\varphi)$, $\ell \gg m$; $G_\ell = (V_\ell, E_\ell)$, CICLICO DI LUNGH. $\ell+1$: $V_\ell = \{0, \dots, \ell\}$, $\underset{0 \le i \le \ell-1}{E_\ell(i, i+1)}$, $E_\ell(\ell, 0)$, T.C. $G_\ell \models \exists P_1, \dots, P_n, \varphi$; QUINDI $\exists P_1^A, \dots, P_n^A \subset V_\ell$: $A := (V_\ell, E_\ell, P_1^A, \dots, P_n^A) \models \varphi$.

DEFINIAMO $B := (V_\ell, E^B, P_1^B, \dots, P_n^B)$, CON $P_i^B = P_i^A$ $\forall i$.

DEFINIREMO E T.C. B SIA SCONNESSO.

PER $d \in \mathbb{N}$, $V_\ell \supseteq N_d(x)^A$ = I VERTICI ~~R~~ A DISTANZA $\le d$ DA x.

$\text{CARD}(N_d(x)^A) = 2d+1$ SE $\varepsilon' < \ell$. ANALOGAMENTE, $N_d(x)^B$.

VOGLIAMO DEFINIRE E^B T.C. $A \equiv_m B$. A QUEL PUNTO $B \models \varphi \Rightarrow$ $\Rightarrow (V_\ell, E_\ell) \models *$; ASSURDO.

SCEGLIAMO ℓ: $\exists a \neq b$ IN A: $N_{3^m}(a)^A \cong N_{3^m}(b)^A$ E $N_{3^m}(a)^A \cap N_{3^m}(b)^A = \emptyset$. (QUI A È UN QUALSIASI $(\ell+1)$-CICLO CON 2^n COLORI). POI FISSIAMO IL GRAFO (G_ℓ, E_ℓ) E POI SI COLORA (IN QUANTO $(G_\ell, E_\ell) \models \exists P_1, \dots, P_n \varphi$).

SCELTI a, b, DEFINIAMO $E^B := (E_\ell \setminus \{(a^-, a), (b^-, b)\}) \cup$ $\cup \{(a^-, b), (b^-, a)\}$.

$\forall$ TIPO t DI ISOMORFISMO DI PALLE DI RAGGIO 3^m COLORATE CON 2^n COLORI, CI SONO LO STESSO NUMERO DI ELEMENTI DI TIPO t IN A E IN B

OSSIA: $A \overset{G}{\underset{m}{\sim}} B$ ("m" VUOL DIRE" RAGGIO 3^m"). $n < m \Rightarrow A \overset{G}{\underset{n}{\sim}} B$.

ORA, $A, a_1, \dots, a_k \overset{G}{\underset{n}{\sim}} B, b_1, \dots, b_k \underset{\text{DEF}}{\Longleftrightarrow}$:

$\boxed{K=0!}$ VEDI SOPRA;

K GENERICO: 1) $\exists$ ISOMORFISMO f: $N_{3^m}(a_1)^A \cup \dots \cup N_{3^m}(a_k)^A \mapsto$

$\mapsto N_{3^m}(b_1)^B \cup \dots \cup N_{3^m}(b_k)^B \}$ T.C. $a_i \mapsto b_i \ \forall i$;

2) $A \overset{G}{\underset{m}{\simeq}} B$. DIMOSTRIAMO $\overset{G}{\underset{m}{\simeq}} \Rightarrow \equiv_m$ (PROPRIETA' DEL "VA' E VIENI"). E' SUFFICIENTE DIMOSTRARE CHE $\overset{G}{\underset{m}{\simeq}}$ GODE DELLA PROPRIETA'.

LEMMA: $A, a_1, \dots, a_k \overset{G}{\underset{m+1}{\simeq}} B, b_1, \dots, b_k \Rightarrow \forall a \in A, \exists b \in B$:

$A, a_1, \dots, a_k, a \overset{G}{\underset{m}{\simeq}} B, b_1, \dots, b_k, b$ E $\forall b \in B, \exists a \in A$: IDEM.

COROLL.: $\overset{G}{\underset{m}{\simeq}} \Rightarrow \equiv_m$.

E SICCOME PER K=0 VALEVA $A \overset{G}{\underset{m}{\simeq}} B$, ABBIAMO $A \equiv_m B$.

LEMMA $\Rightarrow$ COROLL.: E' UN VECCHIO TEOREMA DEI GIOCHI DI E-F.

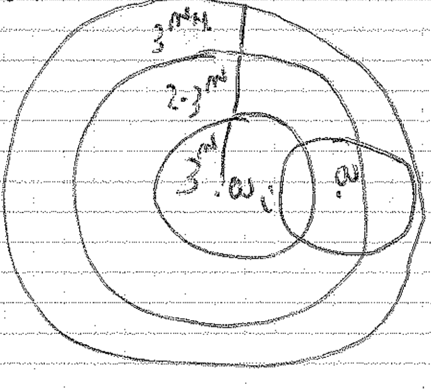
OSS.: $A, a_1, \dots, a_k \overset{G}{\underset{0}{\simeq}} B, b_1, \dots, b_k \Rightarrow \{a_1, \dots, a_k\} \simeq \{b_1, \dots, b_k\}$.

DIM. LEMMA: DATO $a \in A$, SCEGLIAMO $b \in B$.

CASO 1: $a \in N_{2\cdot 3^m}(a_i)$ PER QUALCHE i. ALLORA

$N_{3^m}(a) \subset \bigcup_{i \leq k} N_{3^{m+1}}(a_i)$.

$N_{3^m}(a) \subset \mathrm{dom}(f)$; ALLORA SI PRENDE $b = f(a)$ E IL NUOVO ISOMORFISMO E' LA RESTRIZIONE DEL VECCHIO.



CASO 2: $a \notin \bigcup_{i \leq k} N_{2\cdot 3^m}(a_i) \}$. ALLORA

$N_{3^m}(a)$ E' DISGIUNTA DA $N_{3^m}(a_i) \ \forall i$. SE t E' UN TIPO DI 3^m-PALLA, NOTIAMO CHE CI SONO LO STESSO NUMERO DI EL. DI TIPO t IN $\bigcup_i N_{2\cdot 3^m}(a_i)^A$ E $\bigcup_i N_{2\cdot 3^m}(b_i)^B$. VISTO CHE $a \notin \bigcup_i N_{2\cdot 3^m}(a_i)^A$ DEVE ESISTERE $b \in B$ CON $N_{3^m}(b)^B \overset{g}{\cong} N_{3^m}(a)^A$,

$b \notin \bigcup_i N_{2\cdot 3^m}(b_i)^B$. ALLORA $A, a_1, \dots, a_k, a \overset{G}{\underset{m}{\simeq}} B, b_1, \dots, b_k, b$:

$\mathrm{dom} f \cap \mathrm{dom}\, g \neq \emptyset$, MA $\mathrm{dom} f_{|3^m} \cap \mathrm{dom}\, g = \emptyset$, QUINDI SI

POSSONO UNIRE f E g PER CREARE IL NUOVO ISOMORFISMO. $\boxed{\text{OK}}$

OSS.: IMPLICITAMENTE NOI ABBIAMO DIMOSTRATO ANCHE IL TEOR. DI ~~GAIFMAN~~ HANF:

GENERALIZZANDO IL CONCETTO DI DISTANZA A STRUTTURE QUALSIASI,

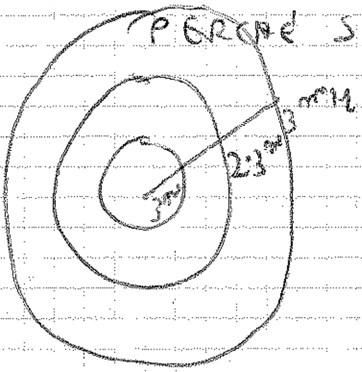
$A, a_1, \dots, a_k \overset{G}{\underset{m}{\sim}} B, b_1, \dots, b_k$ GODE DEL "VA' E VIENI".

(2.4.1 FLUM) τ LINGUAGGIO RELAZIONALE, A, B τ-STRUTTURE, $m \in \mathbb{N}$; PER OGNI TIPO t DI 3^m-PALLA A, B HANNO LO STESSO NUMERO DI ELEMENTI DI TIPO $t \Rightarrow A \equiv_m B$ (L'IPOTESI SI PUÒ INDEBOLIRE IN: A E B HANNO UN NUM. DI TIPI $\geq m \cdot e$, e = MAX. CARD. DI UNA 3^m-PALLA).

SAPPIAMO CHE $\text{NSPACE}(f(n)) \subset \text{ASPACE}(f(n)) \subset \text{DSPACE}(f(n)^2) \subset$
$\subset \text{CO-NSPACE}(f(n)^2)$. SI PUÒ DIMOSTRARE IL TEOR. DI IMMERMAN:
NSPACE = CO-NSPACE.
$\shortparallel$
FO(CH. TRANSITIVA) $\subset$ FO(LFP)

GRAFI CONNESSI NON SONO ESPRIMIBILI COME MONADICI DEL II ORDINE: EBBINGHAUS, PROP. 2.4.5 PAG. 29. 22/5/2008

PERCHÉ SERVONO PALLE DI RAGGIO 3^{n+1}?



UNA PALLA DI RAGGIO 3^n O STA IN UNA PALLA DI RAGGIO 3^{n+1} O È DISGIUNTA DA QUELLA DI RAGGIO 3^n. A SECONDA DEI CASI, IL SECONDO GIOCATORE HA MODO DI PRESERVARE LE RELAZIONI.

RIPASSO GENERALE

GIOCHI DI EHRENFEUCHT-FRAÏSSÉ

τ VOCABOLARIO $= \underbrace{\{\text{RELAZIONI, FUNZIONI, COSTANTI}\}}_{\text{(SIMBOLI)}}$

$A \equiv B$ (τ-STRUTTURE)

SE $\forall$ τ-FORMULA CHIUSA φ, $A \models \varphi \Leftrightarrow B \models \varphi$. ($A \equiv_\varphi B$).

ES.: $\mathbb{Z} = (\mathbb{Z}, <)$; $\mathbb{Z} + \mathbb{Z} = (\mathbb{Z} \times \{0\} \cup \mathbb{Z} \times \{1\}, \overset{\text{lex inverso}}{<}$ $((z,0) < (z',1)\ \forall z, z')$. ALLORA $\mathbb{Z} \equiv \mathbb{Z} + \mathbb{Z}$ (MA NON SONO ISOMORFE).

OSS.: $A \equiv B \Leftrightarrow \forall n$ $A \equiv_n B$, DOVE $A \equiv_n B$ SIGNIFICA $\forall$ φ FORMULA DI RANGO $\leq n$, $A \equiv_\varphi B$.

TEOR. E.F.: $A \equiv_n B \Leftrightarrow A \sim_n B$.

OSS.: $(\Leftarrow)$ FUNZIONA ANCHE SE τ È UN LINGUAGGIO CON FUNZIONI, $(\Rightarrow)$ NO.

DEF.: $A, a_1, \dots, a_n \sim_0 B, b_1, \dots, b_n$ SE $\langle a_1, \dots, a_n \rangle^A \cong \langle b_1, \dots, b_n \rangle^B$ E L'ISOMORFISMO MANDA a_i IN b_i.

SE CI SONO SOLO RELAZIONI IN τ, $\langle a_1, \dots, a_n \rangle^A = \{a_1, \dots, a_n\}$.

L'ISOMORFISMO, SE ESISTE, È UNICO.

$A, a_1, \dots, a_n \sim_{K+1} B, b_1, \dots, b_n$ SE $\forall a \in A$, $\exists b \in B$:

$A, a_1, \dots, a_n, a \sim_K B, b_1, \dots, b_n, b$ E $\forall b \in B, \exists a \in A$: (IDEM).

QUINDI, IL CASO K CON n PARAMETRI È EQUIVALENTE A $K-1$ CON $n+1$ PARAMETRI ___ FINO ALLA 0-EQUIVALENZA CON $K+n$ PARAMETRI.

DIMOSTRIAMO CHE $A \underset{K}{\sim} B \Rightarrow A \equiv_K B$ (O IDEM CON PARAMETRI).

SIA $\varphi(x_1, \dots, x_n)$ DI RANGO $\leq K$; SI PUÒ PENSARE COME FORMULA IN τ E VARIABILI x_i O IN $\tau' = \tau \cup \{x_1, \dots, x_n\}$ SENZA VARIABILI.

SUPPONIAMO CHE $A, a_1, \dots, a_n \sim_K B, b_1, \dots, b_n$.

<u>K=0</u>: $\langle a_i \rangle^A \cong \langle b_i \rangle^B$; ~~UN ISOMORFISMO~~ $\forall R(x_i) \in \tau$ FORMULA ATOMICA (O RELAZIONE), $R^A(a_i) \Leftrightarrow R^B(b_i)$ ECC. CHE ~~VUOL DIRE~~ IMPLICA PRESERVARE LE FORMULE DI RANGO 0.

<u>K>0</u>: INDUZIONE. K-EQUIVALENZA: $\forall a \in A \; \exists b \in B \; (\forall b \in B, \exists a \in A)$:

$A, a_1, \dots, a_n, a \underset{K-1}{\sim} B, b_1, \dots, b_n, b \overset{(\text{IP. INDUT.})}{\Longrightarrow}$ VERIFICANO LE STESSE FORMULE DI RANGO $\leq K-1$. SIA $\varphi(x_1, \dots, x_n)$ DI RANGO K.

CASO DIFFICILE: $\varphi(x_i) = \exists y \, \theta(x_i, y)$. SIANO $A, a_i \models \exists y \, \theta(x_i, y)$

$\Rightarrow$ ~~OSSIA~~ $A \models \exists y \, \theta(a_i, y) \Rightarrow \exists a \in A : A \models \theta(a_i, a)$; ALLORA $\exists b$:

$A, a_i, a \underset{K-1}{\sim} B, b_i, b$; PER IP. IND. SONO ANCHE $\equiv_{K-1}$ E POICHÉ

$A, a_i, a \models \theta(a_i, y)$, ALLORA $B \models \theta(b_i, b)$, CIOÈ $B \models \exists y \, \theta(b_i, y)$. $\boxed{\text{OK}}$

(I CASI $\varphi_1 \wedge \varphi_2$, $\varphi_1 \vee \varphi_2$, $\neg \varphi_1$, È FACILE PER INDUZIONE SUI CONNETTIVI)

<u>OSS.</u>: NON ABBIAMO USATO TUTTE LE PROPRIETÀ DELLE STRUTTURE;

VALE ANCHE $\overset{*}{\underset{K}{\sim}} \Rightarrow \equiv_K$, DOVE $\overset{*}{\underset{K}{\sim}}$ VERIFICA:

1) $\overset{K}{\underset{0}{\sim}} \Rightarrow$ ISOMORFISMO ; 2) $A, \vec{a} \underset{K+1}{\sim} B, \vec{b} \Rightarrow (\forall a \exists b, \forall b \exists a)$:

$A, \vec{a}, a \overset{*}{\underset{K}{\sim}} B, \vec{b}, b$ (PROPRIETÀ DEL VA-E-VIENI)

(3) $\overset{*}{\underset{K}{\sim}} \Rightarrow \overset{*}{\underset{0}{\sim}}$ }: È AUTOMATICO?). DA CUI:

<u>TEOR.</u>: SE $\exists \left(\overset{*}{\underset{K}{\sim}}\right)_K$ CHE GODE DI 1, 2, ALLORA $A \overset{*}{\underset{K}{\sim}} B \Rightarrow A \equiv_K B$.

POI VEDIAMO: $A \underset{K}{\equiv} B \Rightarrow A \underset{K}{\sim} B \not\Rightarrow A \overset{*}{\underset{K}{\sim}} B$ (CON ~~B~~ $\overset{*}{\underset{K}{\sim}}$ ~~B~~ $= \underset{K}{\sim}$)

<u>OSS.</u>: $\overset{*}{\underset{K}{\sim}} \Rightarrow$ IL 2° GIOCATORE HA UNA STRATEGIA PER RESISTERE K MOSSE.

<u>DEF.</u>: $A, \vec{a} \overset{*}{\underset{\infty}{\sim}} B, \vec{b}$ SE $\forall a \in A \; \exists b \in B$ (E VICEVERSA): $A, \vec{a}, a \overset{*}{\underset{\infty}{\sim}} B, \vec{b}, b$

$A \sim B \Leftrightarrow A \sim B \; \forall K$

SI PUÒ DEFINIRE: $A \underset{\infty}{\sim} B$ SE $A \underset{\alpha}{\sim} B$ $\forall \alpha$ ORDINALE.

ESERC.: E' EFFETTIVAMENTE UNA ∞-EQUIVALENZA

D'ORA IN POI, τ È UN LINGUAGGIO SENZA FUNZIONI. $C(K,n)$

TEOR.: FISSATI K ED n, CI SONO UN NUMERO FINITO DI CLASSI DI EQUIVALENZA DI FORMULE CON n VARIABILI E RANGO $\leq K$.

$\left(\varphi(x_i) \Leftrightarrow \psi(x_i) \text{ SE } \forall \text{ [illegible] } A, \vec{a}_i, \text{ [illegible] } : A \models \varphi(\vec{a}) \Leftrightarrow A \models \psi(\vec{a}) \right)$

STIMA: $C(K+1,n) \leq 2^{C(K,n+1)}$; INOLTRE, $C(0,n) < \aleph_0$.

$C = [A, a_1, \ldots, a_n]_{K,n} = \{ B, b_1, \ldots, b_n : B, b_i \equiv_n A, a_i \}$

$C(K,n) = | \text{CLASSI}_{K,n} |$ (CLASSI DI <u>STRUTTURE</u>).

DATA UNA CLASSE C, (ES. $C = [A, \vec{a}_n]_K$), $\exists\, \varphi_C(\vec{x}_i)$:

$B, \vec{b}_i \models \varphi_C \Leftrightarrow B, \vec{b}_i \in C$.

DIM.: DATA C, VOGLIAMO φ_C. OSSERVIAMO: $B, \vec{b} \in C \Leftrightarrow B, \vec{b} \equiv_K A, \vec{a}$.

$$K=0: \varphi_C(\vec{x}) = \bigwedge_{\substack{\varphi \text{ ATOMICA} \\ A, \vec{a} \models \varphi(\vec{x})}} \varphi(\vec{x}) \wedge \bigwedge_{\substack{\psi \text{ ATOMICA} \\ A, \vec{a} \not\models \psi(\vec{x})}} \neg \psi(\vec{x}) . \quad B, \vec{b} \models \varphi_C \Leftrightarrow B, \vec{b} \equiv_0 A, \vec{a}.$$

DA CUI: $C(0,n) \leq 2^{\#\{\text{ATOMICHE CON } n \text{ VARIABILI}\}}$.

$K>0$: $\forall\, b \in B, \exists\, a \in A$ ---- SI FA DOMANI.

BISOGNA VERIFICARE CHE LE $\sim_K$ SONO IN NUM. FINITO. 23/5/2008

$(A, \vec{a}) \overset{K}{\sim} (B, \vec{b})$; $C = [A, \vec{a}]_{K,n} = [B, \vec{b}]_{K,n} \in C(K, n) < \aleph_0$

INOLTRE, $|C(K+1, n)| \leq 2^{|C(K, n+1)|}$.

ABBIAMO DIMOSTRATO CHE $C(0, n)$ E' FINITO (UNA CLASSE DI EQUIVALENZA E' DETERMINATA DA UN SOTTOINSIEME DELLE FORMULE ATOMICHE).

INOLTRE, DATA $C \in C(K, n)$, $\exists\ \varphi_C(x_1, \dots, x_n)$:

$(B, \vec{b}) \models \varphi_C(\vec{x}) \iff [B, b] \in C$.

- $K=0$: $\varphi_C(\vec{x}) = \bigwedge_{\substack{\varphi \text{ ATOMICA} \\ (A, \vec{a}) \models \varphi}} \varphi(\vec{x}) \wedge \bigwedge_{\substack{\varphi \text{ ATOMICA} \\ (A, \vec{a}) \not\models \varphi}} \neg\varphi(\vec{x})$.

- $K>0$: $B, \vec{b} \sim_K A, \vec{a}$ VUOL DIRE: $\forall a \in A, \exists b \in B$ (E VICEVERSA) T.C. $B, \vec{b}, b \sim_{K-1} A, \vec{a}, a$.

SIA $H = [A, \vec{a}, a] \in SUCC([A, \vec{a}])$ (<u>DEF.</u> DI SUCCESSORE);
SIA $[B, \vec{b}] \in C$; ALLORA $[B, \vec{b}] \models \varphi_C(\vec{x})$.

$\varphi_C(\vec{x}) := \bigwedge_{H \in SUCC(C)} \exists x_{n+1} \varphi_H(\vec{x}, \overset{x_{n+1}}{y}) \wedge \forall x_{n+1} \bigvee_{H \in SUCC(C)} \varphi_H(\vec{x}, x_{n+1})$, CON

$H \in C(K-1, n+1)$ $\forall$ SCELTA DI UN SOTTOINSIEME DI $C(K-1, n+1)$

HO UNA φ_C CANDIDATA; QUINDI HO AL PIU' $2^{C(K-1, n+1)}$; DA CUI:

$|C(K, n)| \leq 2^{|C(K-1, n+1)|}$. $\boxed{OK}$

~~ALLORA~~: SE $\overset{*}{\underset{K}{\sim}}$ GODE DEL VA E VIENI, ALLORA

. $\overset{*}{\underset{K}{\sim}} \Rightarrow \equiv_K$ E $\overset{\text{QUINDI}}{\underset{K}{\sim}} \Rightarrow \equiv_K$. MANCA: $\equiv_K \Rightarrow \sim_K$.

SIANO $A, \vec{a} \equiv_K B, \vec{b}$; SIA $C = [A, \vec{a}]_{\sim_K}$;

ALLORA $A, \vec{a} \models \varphi_C(\vec{x})$ (PERCHE' ESPRIME IL VA E VIENI PER K MOSSE)

QUINDI $B, \vec{b} \models \varphi_C(\vec{x})$ (PERCHE' HA RANGO K), MA ALLORA

$B, \vec{b} \sim_K A, \vec{a}$. $\boxed{OK}$.

<u>OSS.</u>: RESTA DA DIMOSTRARE CHE CI SONO UN NUM. FINITO DI FORMULE DI RANGO $\leq K$ A MENO DI EQUIVALENZA.

DIM.: DATA $\theta(\bar{x})$, $\uparrow$ DI RANGO K $\theta(\bar{x}) \# \Longleftrightarrow \underset{\underset{\varphi_C \Rightarrow \theta}{C \in C(k,m)}}{\bigvee} \varphi_C(\bar{x})$ E QUINDI CI SONO SOLO UN NUM. FINITO DI θ, ~~ESATTAMENTE~~. $\boxed{OK}$

COR.: $K \subset \tau$-STRUTTURE; $K \notin FO \Longleftrightarrow \forall m, \exists A \in K, B \notin K, A \sim_m B$.

(OSSIA: $K \in FO \} \Longleftrightarrow \exists m$: K E' $\sim_m$-CHIUSO).

VALE UN COROLLARIO SIMILE PER NP.

DIM.: $K = Mod(\varphi) \Rightarrow$ K E' $\sim_m$-CHIUSO, $m = RANGO(\varphi)$.

VICEVERSA, K $\sim_m$-CHIUSO $\Rightarrow K \subset \bigcup_{A \in K} Mod(\psi_{[A]_{\sim_m}}) =$

$= Mod(\underbrace{\bigvee_{A \in K} \psi_{[A]_{\sim_m}}}_{=\psi})$ ~~MA PERO~~ DOBBIAMO VERIFICARE CHE $Mod(\bigvee_{A \in K} \psi_{[A]_{\sim_m}}) \subset K$:

$B \models \psi \Rightarrow \exists A \in K : B \models \psi_{[A]_{\sim_m}} \Rightarrow B \sim_m A \in K \Rightarrow B \in K$. $\boxed{OK}$

TEOR.: (8.5 PAG. 127, AJTAI-FAGIN, IMMERMAN) ⊛ $(NP \neq CO\text{-}NP)$

DIM.: CLIQUE E' NP-COMPLETO $\Rightarrow \neg$CLIQUE $\in$ CO-NP E BASTA DIMOSTRARE CHE $\neg$CLIQUE $\notin$ NP.

RICORDIAMO CHE $NP = \exists SO$: $K \in NP \Longleftrightarrow K = Mod(\exists R_i, \varphi)$, $\varphi \in FO$.

$\rightarrow \forall$ SCEGLIE $c, m \in \mathbb{N}$;

$\rightarrow \exists$ SCEGLIE $A \in K$;

$\rightarrow \forall$ SCEGLIE c RELAZIONI UNARIE, C_1^A e $C_c^A \subset A$;

$\rightarrow \exists$ SCEGLIE $B \notin K$ E $C_1^B, \ldots, C_c^B$ UNARIE $\subset B$ E CERCA DI MOSTRARE $(B, C_1^B, \ldots, C_c^B) \sim_m (A, C_1^A, \ldots, C_c^A)$.

$\nwarrow$ IN REALTA' CERCA DI DIMOSTRARE $\equiv_m$, PER POTER UTILIZZARE UNA $\sim_m$.

⊛ **TEOR.**: $K \notin \exists^{MON} SO \Longleftrightarrow \exists$ VINCE.

DIM.: $\Leftarrow$ PER ASSURDO, SIA $K = Mod(R_1, \ldots, R_c, \varphi)$, $RANGO(\varphi) = c$; SUPPONIAMO CHE $\forall$ GIOCHI c, m; ~~ALLA FINE ABBIAMO LE DUE STRUTTURE~~ POI $\exists$ GIOCA $A \in K$ $(A \models \exists R_i; \varphi)$; $\forall$ PUO' GIOCARE $C_i^A \subset A$ T.C. $(A, C_i^A) \models \varphi$; $\exists$ PRODUCE $B, C_i^B \sim_m A, C_i^A$, ALLORA

$B, C_i^B \models \varphi$, MA ALLORA $B \models \exists R_i; \varphi$, QUINDI $B \in K$; ASSURDO.

$\Leftarrow$ OSS.: SE SI DIMOSTRA CHE $\neg SAT \notin NP$, ALLORA $NP \neq CONP$ (E QUINDI $P \neq NP$). ~~MA~~ RIMANDATO.

26/5/2008

SO = PH

MdT ORACOLARI: STATI PARTICOLARI: $q_{ORACOLARE}, q_{SI}, q_{NO}$ NASTRO ORACOLARE $B \subseteq \Sigma^*$

$B : \Sigma^* \longrightarrow \{0, 1\}$

DATI C_1, C_2 CLASSI DI COMPLESSITÀ, $C_2^{C_1} = \bigcup_{B \in C_2} C_1^B \supseteq C_2$

(PUÒ NON ESSERE STRETTA: $NP^P = NP$)

<u>DEF.</u>: PH; $\Sigma_0^P = PTIME$; $\Sigma_{i+1}^P = NP^{\Sigma_i^P}$; $PH = \bigcup_{i \geq 0} \Sigma_i^P$.

Δ; $\Delta_0 = PTIME$; $\Delta_{i+1}^P = P^{\Sigma_i^P}$; $\Delta = \bigcup_i \Delta_i^P$.

Π; $\Pi_0 = PTIME$; $\Pi_{i+1}^P = CO\text{-}NP^{\Sigma_i^P}$ $\Pi = \bigcup_i \Pi_i$.

<u>OSS.</u>: $\Pi_{i+1}^P = CO\text{-}(NP^{\Sigma_i^P}) = CO\text{-}\Sigma_i^P$.

E' EVIDENTE CHE $NP \subseteq PH$: $P \to NP^P = NP \to NP^{NP} = NP$ ...

<u>OSS.</u>: <u>SE</u> ESISTE UN PROBLEMA PH-COMPLETO ALLORA Σ_i^P SI STABILIZZA.

<u>SE</u> $P = NP$ O $NP = CO\text{-}NP$, ALLORA $PH = \Sigma_0^P = P$.

<u>DEF.</u>: $\Sigma_K^{SO} = \{(\exists R_1)(\forall R_2) \ldots (Q_K R_K)\varphi\}$ (K ALTERNANZE FRA $\exists$ E $\forall$)

$\varphi \in FO$

$\exists SO = \Sigma_1^{SO}$.

ATIME-ALT$[n^{O(1)}, k]$ = MdT ALTERNANTI CHE LAVORANO IN TEMPO POLINOMIALE CON MAX. K ALTERNANZE.

<u>TEOR.</u>: τ VOCABOLARIO, $S = \{\tau\text{-STRUTTURE}\}$, $\forall k \geq 1$, SONO EQUIVALENTI:

1) $S = MOD[\Phi]$, $\Phi \in \Sigma_K^{SO}$;

2) $S = \{x : \exists y_1 : |y_1| \leq |x|^c ; \forall y_2 : |y_2| \leq |x|^c \ldots Q_K R_{y_K} |y_K| \leq |x|^c \; R(x, y)\}$;

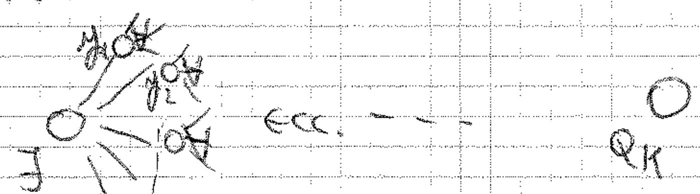
3) $S \in$ ATIME-ALT$[n^{O(1)}, k]$;

4) $S \in \Sigma_K^P$.

DIM.: 1)⇒2): $\exists R_1 \forall R_2 \dots Q_K R_K \underset{\|\Phi}{\psi}$; SIA $A \in S$: $A \models \Phi$;

$^N\gamma_i = \dots$

2)⇒3)



E' UN CAMMINO ALTERNANTE CHE PORTA ALLA SOLUZIONE.

3)⇒1) (FAGIN: NP ⊂ ∃SO)

4.) ⇔ 2): CASO SEMPLICE: SIA $A \in NP^{NP}$, SCRIVIAMO "$x \in A$" IN FORMA "$\exists\forall\psi$": L'IDEA E' CHE FISSATO L'INPUT L'ORACOLO VIENE USATO SOLO UN NUM. FINITO DI VOLTE:

$$(M^B(x))\downarrow \iff \exists f\,(f \subset_{\text{FINITA}} B \wedge M^f(x)\downarrow) \iff$$
$$\iff \exists f \exists c_f\,(f \subset_{\text{FINITO}} B \wedge \psi_A(c,x,f)).$$

$f \subset_{\text{FINITO}} B$ SI RISCRIVE: $\forall u \in \text{dom} f\,(f(u)=0 \Rightarrow \forall w\, M_B(u)\uparrow w) \wedge$
$\wedge (f(u)=1 \Rightarrow \exists z: M_B(u)\downarrow z)$. CI SONO PERO' TROPPI QUANTIFICATORI. SI RISOLVE COSI':

$$\exists (z(u))_{u \in \text{dom} f}: \forall u \forall w\,(f(u)=1 \Rightarrow M_B(w)\downarrow z(u)) \wedge$$
$$\wedge (f(u)=0 \Rightarrow M_B(u)\uparrow z(u)).$$ CONTROLLIAMO LE LUNGHEZZE:

$|u| \le |x|^c$ PERCHE' COMPARE SUL NASTRO ORACOLARE.

TEOR. GENERALE: $L \subseteq \Sigma^*$, $i \ge 1$; $L \in \Sigma_i^p \iff \exists R$
$\{(x,y):(x,y)\in R\} \in \Pi^p_{i-1}$ E $L = \{x : \exists y\,(x,y) \in R\}$.

COROLL.: $L \in \Pi_i^p \iff \overset{\exists R}{\in} \Sigma^p_{i-1}$ E $L = \{x : \forall y\,(x,y) \in R\}$.

DA QUESTO DERIVA 4)⇔2). $\boxed{OK}$

E DA QUESTO DERIVA: SO = PH.

$\underset{\substack{k \\ \| PH}}{\bigcup} ATIME(n^{O(1)},k)\ CATIME(n^{O(1)}) =$
$= DSPACE(n^{O(1)})$.

SO ⊂ PH

DIM. INDUZIONE: $i \Rightarrow i+1$: $NP^{\Sigma^p_{i-1}}$ COSTRUIAMO LA MdT CORRISPONDENTE TRAMITE 2).

PASSO: ~~Σ_i~~ $x \in L$, $L \in NP^{\Sigma^p_{i-1}}$: C'E' UNA MACCHINA M^K CON
$K \in \Sigma^p_{i-1}$, $z \in K \iff \exists w: (z,w) \in S$, S E' TUTTO POLINOMIALE (Π^p_{i-1}). $\boxed{OK}$

29/5/2008

$\overset{\vec{a}}{A} \underset{m}{\sim} B, \vec{b}$: $A \models \varphi \Leftrightarrow B \models \varphi$ $rk(\varphi) \leq m$;

$A \overset{k}{\underset{m}{\sim}} B$: $A \models \varphi \Leftrightarrow B \models \varphi$ CON # VARIABILI $(\varphi) \leq K$.

~~NP = ∃~~

FAGIN: $NP = \exists SO = \exists SO_{\leq}$; $P = FO(LFP)$

INCLUSIONI: $P \subset NP \subset A$ E $A \subset P$ CON UN ESPONENZIALE

SAVIC: $ASPACE(s(n)) \subset DSPACE(s(n)^2)$ $(s(n) \geq \log(n))$

(FINE DEL TEOR. DI AJTAI-FAGIN (METHODOLOGY THEOREM, PAG. 127 IMMERMAN))

COSA VUOL DIRE "$FO(LFP) \subset \exists SO$, CON $\leq$"?

DATA $C \subset \tau$-STRUTTURE, $\exists \varphi \in SO$, $C = Mod(\varphi) \Leftrightarrow$

$\Leftrightarrow \{ bin(A)_{\leq} : A \in C \} \in NP$.

SIA DUNQUE $C^* = \{ (A, \leq) : (A, \leq) \models \varphi \}$, $\varphi \in FO_{\leq}(LFP)$.

ALLORA, $(A, \leq) \models \varphi \Leftrightarrow \exists R$ ORDINE T.C. $(A, R) \models \varphi$.

PROBLEMA APERTO: ESPRIMERE ALGORITMI TRAMITE STRUTTURE CHE NON FACCIANO RIFERIMENTO ALL'ORDINE.
($P = FO(LFP)$ RICHIEDE UN ORDINE, MENTRE $NP = \exists SO$ NO)

AJTAI-FAGIN:
$C \subset STRUT(\tau)$; $C \overset{?}{=} Mod(\exists \underbrace{C_1, \dots, C_c}_{UNARI} \underset{FO}{\varphi})$ $\swarrow \exists^{MON} SO$;

$C \notin \exists^{MON} SO \Leftrightarrow$ "$\exists$" VINCE IL SEGUENTE GIOCO DI E.F.:

- (∀) SCEGLIE c, m;
- (∃) SCEGLIE $A \in C$;
- (∀) SCEGLIE $C_1^A, \dots, C_c^A \subset A$;
- (∃) SCEGLIE $B \notin C$, $C_1, \dots, C_c \subset B$ E CERCA DI MOSTRARE CHE $(B, \vec{C}^B) \underset{m}{\sim} (A, \vec{C}^A)$.

ABBIAMO VISTO: (∃) VINCE $\Rightarrow C \notin \exists^{MON} SO$.

VICEVERSA: $C \notin \exists^{MON} SO$;

- (∀) SCEGLIE c, m; SIA $S_{m,c}$ = INSIEME FINITO MASSIMALE DI FORMULE NON EQUIVALENTI DELLA FORMA $\exists C_1, \dots, C_c, \varphi$, CON $rk(\varphi) \leq m$ E φ COMPLETA, OSSIA: $\forall \psi$, $RK(\psi) \leq m$, $\varphi \vdash \psi \vee \varphi \vdash \neg\psi$.

ES.: DATA A, $\exists\, \varphi_{[A]}$ CON $rk(\varphi_{[A]}) \leq m$, T.C. $B \models \varphi(A) \iff B \underset{m}{\simeq} A$; $\varphi_{[A]}$ E' COMPLETA.

SIA $T = \{ \Phi \in S_{m,C} : \forall B \notin C,\ B \models \neg\Phi \}$; $\left(\bigvee_{\Phi \in T} \Phi \right) \in S_{m,C}$;

$\exists A \in C : A \models \neg\left(\bigvee_{\Phi \in T} \Phi \right)$, ALTRIMENTI $\left(\bigvee_{\Phi \in T} \Phi \right)$ ~~ASSIO~~ ASSIOMATIZZEREBBE C: $C = Mod\left(\bigvee_{\Phi \in T} \Phi \right)$. ALLORA $\textcircled{\exists}$ SCEGLIE A;

$\textcircled{\forall}$ SCEGLIE $c_1, \dots, c_c \in A$;

$\textcircled{\exists}$ CONSIDERA $(A, \vec{c}^A) = A'$; ESISTE $\varphi_{[A']}$ CON RANGO $\leq m$;

$A \models \exists \vec{c}\, \varphi_{[A']}$; ALLORA $\left[\exists \vec{c}\, \varphi_{[A']} \notin T \right]$. INFATTI, $\forall \Phi \in T$, $A \models \neg\Phi$.

DUNQUE $\exists B \notin C : B \models \exists \vec{c}\, \varphi_{[A']}$: $\textcircled{\exists}$ SCEGLIE B E $\vec{c}^B$ T.C. $B, \vec{c}^B \models \varphi_{[A']}$. MA ALLORA $B, \vec{c}^B \underset{m}{\simeq} A' = A, \vec{c}^A$. $\boxed{OK}$

TEOR.: SAT E' NP-COMPLETO. $(\Leftarrow$ FAGIN$)$

DIM.: OSSIA, $NP \leq_p SAT$. SIA $M \in$ N-TURING MACHINE, $A = \{ x : M(x)\downarrow \}$; DIMOSTRIAMO $x \in A \iff f(x) \in SAT$, CON $f(x)$ FORMULA DIPENDENTE DA x. (PAG. 119 IMMERMAN)

SIA $\mathfrak{B} \in NP$; PER FAGIN, $\mathfrak{B} = Mod(\Phi)$. $\mathfrak{B} \subset \tau$-STRUTTURE.

NELLA DIM. DI FAGIN, $\Phi = \exists \underbrace{S_1^{a_1}, \dots, S_k^{a_k}}_{\text{2K-ARIE}} \underset{\substack{\uparrow \\ \text{K-ARIA}}}{\Delta^K} \forall x_1, \dots, x_t\ \varphi(\vec{x})$.

DATA A τ-STRUTTURA, $|A| = n$, DOBBIAMO DEFINIRE ~~$\mathfrak{B}$~~ $\gamma(A)$ FORMULA PROPOSIZIONALE T.C. $A \in \mathfrak{B} \iff \gamma(A) \in SAT$.

$\gamma(A)$ HA COME VARIABILI PROPOSIZIONALI: $C_i(e_1, \dots, e_{2k})$, ~~DOVE~~ $\Delta(e_1, \dots, e_k)$, ~~$e_i \in n$~~ $R(\vec{e})$, $e_i \in n$, $R \in \tau$.

DEFINIAMO MEGLIO: $\psi = \bigwedge_{j=1}^{r} \bigvee R_j(\vec{x})$. ORA, $A \in \mathfrak{B} \Rightarrow A \models \exists \vec{C}^{2k}, \Delta^k, \forall \vec{x}\ \bigwedge_j R_j(\vec{x})$. ALLORA $\gamma(A) = \bigwedge_{e_1, \dots, e_t \in n} \bigwedge_j \bigvee R_j(\vec{e})$; PER COSTRUZIONE, OGNI VALUTAZIONE DI γ E' SAT. $\boxed{OK}$

30/5/2008

$ATIME(t(n)) \subset DSPACE(t(n)$;

2) $ATIME(s(n)) \subset DTIME(O(1)^{S(n)})$.

QUAL E' LA COMPLESSITA' DETERMINISTICA DI VARIE FORME DI ALTERNATING REACHABILITY?

GRAFO: $G = (V, E^2; \underset{\substack{\Downarrow \\ \text{VERTICI} \\ \text{UNIVERSALI}}}{A^1}; s; t)$; $\tau = \{E, A, s, t\}$.

$REACH_{ALT} \subset \tau$-STRUTTURE, $REACH_{ALT} = \{G : E_{ALT}(s,t)\}$.

E_{ALT} SI DEFINISCE COSI':

1) $\forall x\, E_{ALT}(x,x)$;

2) $\neg A(x) \wedge \exists z\, ((E(x,z) \wedge E_{ALT}(z,y)) \rightarrow E_{ALT}(x,y))$

3) $A(x) \wedge \forall z((E(x,z) \rightarrow E_{ALT}(z,y)) \rightarrow E_{ALT}(x,y)) \wedge \exists z(E(x,z))$.

PROBLEMA: TROVARE ALGORITMI EFFICIENTI PER DIRE SE G STA IN $REACH_{ALT}$.

TEOR.: $REACH_{ALT} \in DTIME(n)$, $n = |G|$.

DIM.: Q = QUEUE SI PARTE DA t E SI VA A RITROSO

```
$Q := \emptyset$;
MARK(t); INSERISCO t IN Q.
WHILE $Q \neq \emptyset$ DO
    RIMUOVO IL PRIMO EL. $x$ DI Q
    FOR $y$ NON MARCATO T.C. $E(y,x)$
        CANCELLO $(y,x)$
        IF $\neg A(y)$ O $y$ NON HA ARCHI USCENTI
            MARK($y$); INSERISCO $y$ IN Q
        END IF
    END FOR
    SE $s$ E' MARCATO ACCETTO; SE NO, NO.
END WHILE ; END.
```

AFFERMAZIONE: x VIENE MARCATO $\Leftrightarrow E_{ALT}(x,t)$.

ALTRO ALGORITMO: GRAFI CON RAMIFICAZIONE ≤ 2

SI LAVORA CON UNA ~~STACK~~ PILA INVECE CHE UNA CODA.

L'IDEA È CHE SE NELLA PILA C'È UNA CERTA STRINGA, SI È SUL NODO IN CUI SI ARRIVA SEGUENDO I NODI CORRISPONDENTI A QUELLA STRINGA.

INOLTRE SI MANTIENE IN MEMORIA ANCHE UNA RISPOSTA $R \in \{SÌ, NO, ?\}$

$S = (C_1, \dots, \overset{\forall}{C_{n-1}}, C_n)$; $R = NO \Rightarrow$ AGGIORNIAMO COME

$S := (C_1, \dots, C_{n-1})$, $R = NO$.

$S = (C_1, \dots, \overset{\exists}{C_{n-1}}, 0)$, $R = NO \Rightarrow$ AGGIORNIAMO COME

$S = (C_1, \dots, C_{n-1}, 1)$, $R = ?$.

$S = (C_1, \dots, C_{n-1}, 1)$ $R \neq ? \Rightarrow$ AGGIORNIAMO COME

$S = (C_1, \dots, C_{n-1}, 1)$, R IMMUTATA

$S = (C_1, \dots, C_n)$, $R = ? \Rightarrow S := (C_0, \dots, C_n, 0)$, $R = ?$ $\boxed{\text{OK}}$

TEOR.: ATIME$(t(n)) \subset$ DSPACE$(t(n))$.

DIM.: $M \in$ ATIME$(t(n))$; w INPUT, $|w| = n$;

$G_w = (V, E, A, s, t)$; $V \ni ID = <$CONT. NASTRI, STATO, POSIZ. TESTINE$>$; $|ID| = t(n) +$ COSTANTE $+ \log(t(n)) = O(t(n))$.

$\vec{s} = <\vec{w}$, STATO INIZIALE 1$>$. $M(w)\downarrow \iff E_{ALT}^{G_w}(s_w, t)$;

CIÒ SI CONTROLLA CON L'ALGORITMO DELLA PILA.

OSS.: NON SI PUÒ TENERE TUTTO IL GRAFO IN MEMORIA, PERCHÉ LA SUA GRANDEZZA È ESPONENZIALE: $|G_w = O(1)^{t(n)}$.

DIMOSTRIAMO CHE $|STACK| \leq TIME = t(n)$. ALLA FINE PER ESPANDERE CI SI METTE TEMPO $t(n)$, QUINDI SPAZIO $t(n)$. $\boxed{\text{OK}}$

TEOR.: ASPACE$(t(n)) \subset$ DTIME$(O(1)^{t(n)})$.

DIM.: $|STACK| \leq TIME \leq O(1)^{t(n)}$. OSSERVIAMO CHE LA COPPIA $<$STACK, RISPOSTA$>$ NON SI RIPETE ... $\boxed{\text{OK}}$

OSS.: SI SUPPONE SEMPRE $S(n) \geq \log(n)$.

TEOR.: $NSPACE(S(n)) \subset ATIME(S(n)^2) (\subset DSPACE(S(n)^2))$.

DIM.: $M \in NSPACE(S(n))$ - TM; W INPUT, $|W| = n$;

VOGLIAMO SAPERE SE $M(W)\downarrow$ TRAMITE UNA MACCHINA ALTERNANTE.

G_W = GRAFO DELLE COMPUTAZIONI $= (V, E, s, t)$ CON TUTTI I NODI $\exists$.

ROUTINE: $P(d, x, y) \Longleftrightarrow E^*$ (DA X SI RAGGIUNGE y IN MENO DI 2^d PASSI)

x, y = CONFIGURAZIONI <MEMORIA, STATO, POSIZIONE>.

OSS.: $P(d+1, x, y) \Longleftrightarrow \exists z \left(P(d, x, z) \underset{\text{"}\forall\text{"}}{\underbrace{\wedge}} P(d, z, y) \right)$.

UNA ATM PUO' CALCOLARE $P(d+1, x, y)$ COME: SE IN $\exists$, PRENDI z; SE IN $\forall$, SCEGLI LA STRADA DA PRENDERE (OSSIA RIPARTE CON $P(d, x, z)$ O $P(d, z, y)$).

SE $T(d)$ = TEMPO PER CALCOLARE $P(d, x, y)$, ALLORA

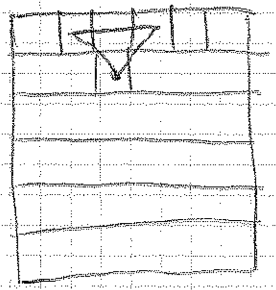
$T(d+1) = O(S(n)) + T(d)$. ALLA FINE, $M(W)\downarrow \Longleftrightarrow P(C \cdot S(n), s_W, t)$

~~QUINDI~~ SI HA $T(d) = d \cdot S(n)$, MA POICHE' SI PARTE DA $d = S(n)$, SI HA $T(S(n)) = S(n)^2$. $\boxed{OK}$

TEOR.: $DTIME(K^{S(n)}) \subset ASPACE(S(n))$.

DIM.: $M \in DTIME(K^{S(n)})$, INPUT W, $|W| = n$;

G_W = MATRICE $K^{S(n)} \times K^{S(n)}$, DOVE IN POS. (t, p) C'E' IL SIMBOLO AL TEMPO t IN POSIZIONE p. "SIMBOLO" E' O IL SIMBOLO DEL NASTRO O LA COPPIA <SIMBOLO, STATO> (SE NECESSARIO).



IL CONTENUTO DI UNA CELLA E' DETERMINATO DALLE 3 CELLE CHE LE STANNO "SOPRA".

$C(t, p, a)$ = AL TEMPO t IN POS. p C'E' a;

$C(t+1, p, a) \Longleftrightarrow \exists a_{-1}, a_0, a_1 \left((a_{-1}, a_0, a_1) \xrightarrow[M]{} a \right) \wedge$
$\forall i \in \{-1, 0, 1\}\ C(t, p+i, a_i))$. $C(0, p, a)$ E' FACILE:

$C(0, 1, \langle W_0, q \rangle)$, $C(0, 2, W_1)$ ECC.... ; ALLA FINE PER VERIFICARE SE ACCETTA, BASTA VERIFICARE $C(K^{S(n)}, 1, ACCETTO)$.

$C(t+1, p, w)$ SI CALCOLA CON UNA ATM; $|b| \leq O(S(n))$, $|p| \leq O(S(n))$, w E' UNA COSTANTE. $\boxed{\text{OK}}$

SI SA CHE NPSPACE = APTIME = PSPACE.

SE FOSSE VERA NPSPACE = APSPACE, ESSENDO APSPACE = EXPTIME, SAREBBE PSPACE = EXPTIME, IL CHE SEMBRA DUBBIO.