11 MARZO 2016 - TEMA D'ESAME

ES 3.

Y ALL'INIZIO AVRÀ UN CERTO VALORE NON SPECIFICATO

IL PROGRAMMA SOMMA I NUMERI DISPARI

$$P \left[\begin{array}{l} z := 0;\ x := 0; \qquad A \\ \text{WHILE } y > 0 \text{ DO} \\ \quad \left.\begin{array}{l} \left.x := 2*z + x + 1;\right]C_1 \\ \left.\begin{array}{l} z := z + 1; \\ y := y - 1 \end{array}\right]C_2 \end{array}\right]C \\ \text{ENDWHILE} \end{array}\right.\Bigg]W$$

$$\{ y = k \wedge k > 0 \}\ P\ \{ x = k^2 \}$$

SI PUÒ ANCHE DIRE CHE IL PROGRAMMA CALCOLA Y^2 E LO METTE IN X

CERCHIAMO UN'INVARIANTE PER L'ITERAZIONE, SIMULIAMO L'ESECUZIONE PER TROVARLA

X	0	1	4	9	16
Z	0	1	2	3	4
Y	k	k-1	k-2	k-3	k-4

$y + z = k$ (UGUALE A DIRE $y = k - z$)

ABBIAMO BISOGNO ANCHE X PERCHÉ È NELLA POST CONDIZIONE

$x = z^2$

PENSIAMO ALL'OBIETTIVO, ABBIAMO $x = k^2$ COME POST CONDIZIONE,

CI RICORDIAMO CHE NELLA CONCLUSIONE DEL CICLO (POST CONDIZIONE) AVREMO L'INVARIANTE E LA CONDIZIONE DI CICLO NEGATA OVVERO $y \leq 0$ AGGIUNGIAMO LA ALL'INVARIANTE

QUESTO NON È SUFFICIENTE A DIRE $z = k^2$

POSSIAMO VEDERE CHE Y DECRESCE DI 1, FINO A QUANDO ARRIVA A 0

L'INVARIANTE DI QUESTO È CHE $Y \geq 0$

QUESTE INVARIANTI POSSONO ANCHE ESSERE DIMOSTRATE SEPARATAMENTE SE NON TE NE ACCORGI SUBITO

SCRIVIAMO LA FORMULA DELL'INVARIANTE CON ?, PERCHÉ NON È ANCORA DIMOSTRATA

$$? \{ \underbrace{y + z = k,\ x = z^2,\ y \geq 0}_{\text{INVARIANTE}},\ y > 0 \}\ C\ \{ y + z = k,\ x = z^2,\ y \geq 0 \}$$

SENZA CONDIZIONE DI CICLO

INVE

APPLICHIAMO REGOLA ASSEGNAMENTO E SEQUENZA

CONSIDERIAMO PRIMA C2 (SI PARTE DAL FONDO NEGLI ASSEGNAMENTI) E POI C1 VISTO CHE POTREBBERO NON ESSERE INDIPENDENTI

MC-C2}

APPLICHIAMO LA REGOLA DELL'ASSEGNAMENTO

SEMPLIFICAZIONI

$$\vdash^{ASS}_{SEQ} \underbrace{\{x - \cancel{1} + z - \cancel{1} = k,\ x = \overset{z^2+2z+1}{(z+1)^2},\ y - 1 \geq 0\}}_{\alpha \leftarrow \text{ALPHA}} C_2 \{inv\}$$

SIMBOLO DERIVABILITÀ DIMOSTRABILITÀ

LA REGOLA DELL'ASSEGNAMENTO GARANTISCE CHE QUESTA TRIPLA È CORRETTA.

α DIVENTA POST CONDIZIONE DI C_1, APPLICHIAMO L'ASSEGNAMENTO E POI CONFRONTIAMO LA PRECONDIZIONE TROVATA CON L'OBIETTIVO

SEMPLIFICHIAMO α ALGEBRICAMENTE

SEMPLIFICAZIONI

$$\vdash^{ASS} \{y + z = k,\ \cancel{2z} + x + \cancel{1} = z^2 + \cancel{2z} + \cancel{1},\ y - 1 \geq 0\} C_1 \{\alpha\}$$

IL NOSTRO OBIETTIVO È RICONDURCI ALLA PRE DI "?"

$y - 1 \geq 0$ EQUIVALE A DIRE $y > 0$ → PARTE DELLA PRECONDIZIONE OBIETTIVO

SEMPLIFICHIAMO 2Z E 1

L'UNICA DIFFERENZA È $y \geq 0$ NELLA PRE OBIETTIVO

POSSIAMO USARE LA REGOLA DI IMPLICAZIONE E DIRE CHE LA PRE OBIETTIVO IMPLICA LA PRE TROVATA (PRE OBIETTIVO HA UNA COSA IN PIÙ)

QUESTE L'HO SCRITTO IO NON LUI

$$\{y+z=k,\ x=z^2,\ y \geq 0,\ y>0\} \to \{y+z=k,\ x=z^2,\ y>0\}$$

$$\vdash^{IMPL} \{y+z=k,\ x=z^2,\ y\geq 0,\ y>0\}\ C\ \{y+z=k,\ x=z^2,\ y\geq 0\}$$

REGOLA ITERAZIONE ↓ $\neg B$ ↓

$$\vdash^{ITER} \{inv\}\ W\ \{inv\ \ y \leq 0\}$$

↓ DIVENTA $\{x = k^2\}$ → METTENDO INSIEME INV E $y \leq 0$

OBIETTIVO INIZIALE DELL'ES. ↑

$$?\ \{y = k \wedge k > 0\}\ A\ \{inv\}$$

$$\vdash^{ASS} \{y = k,\ 0 = 0^2,\ y \geq 0\}\ A\ \{inv\}$$

SICCOME $y = k$ POSSIAMO SCRIVERLA COME $k \geq 0$

POI $k \geq 0 \xrightarrow[\text{IMPLICA}]{} k > 0$

$$\vdash^{IMPL} \{y = k \wedge k > 0\}\ A\ \{inv\}$$

PASSIAMO ALLA CORRETTEZZA TOTALE

y È IL VARIANTE CHE CI SERVE VISTO CHE $y = k - z$

HO UN VALORE INIZIALE h A y E DERIVO LA REGOLA DELLA VARIANTE

E SARÀ GARANTITO CHE y DIMINUISCE

(PASSAGGI DA FARE)

IL PUNTO CRUCIALE DI QUESTO ESERCIZIO È LA SCELTA DELL'INVARIANTE IN FUNZIONE DELLA POST CONDIZIONE DELL'OBIETTIVO

MOLTO SPESSO IN ESAME I PROGRAMMI HANNO QUESTA STRUTTURA

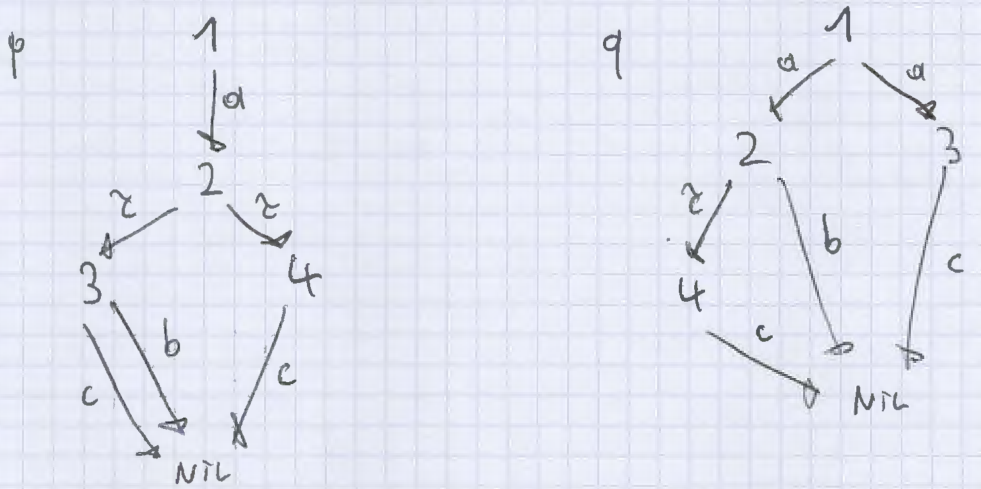
$$\{p\}\ \underbrace{A}_{\text{ASSEGNAMENTO}}\ ;\ \underbrace{W}_{\text{CICLO}}\ ;\ B\ \{q\}$$

SE C'È QUESTA PARTE PRIMA BISOGNA FARE LA PRECONDIZIONE DI B CHE DIVENTERÀ LA POST DI W

ESERCIZIO 1

$$p = a \cdot (\tau \cdot (b \cdot \text{nil} + c \cdot \text{nil}) + \tau \cdot c \cdot \text{nil})$$

$$q = a \cdot (b \cdot \text{nil} + \tau \cdot c \cdot \text{nil}) + a \cdot c \cdot \text{nil}$$



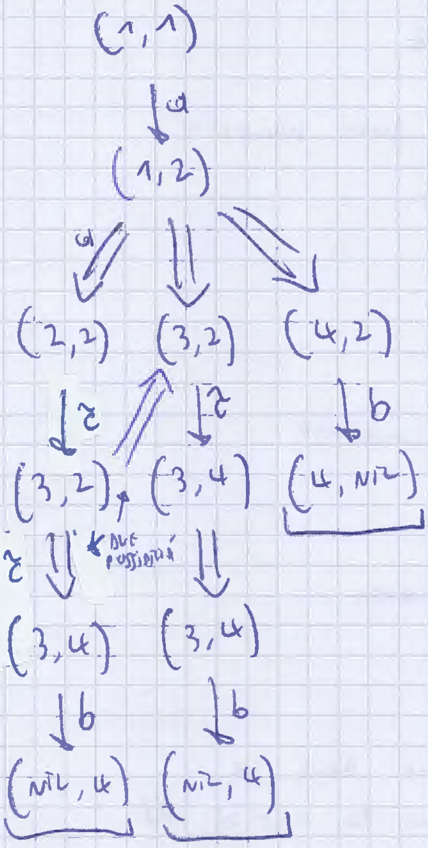
$p_4 \approx q_3 \approx q_4$ È EQUIVALENTE

PER DIMOSTRARE CHE NON SONO BISIMILI L'ATTACCANTE DEVE OTTENERE UNA STRATEGIA

(p_4, q_3) o (p_4, q_4)

M(-123)

IO AVREI FATTO MOSSA $p_1 \xrightarrow{a} p_2$ PER INIZIARE



SI POSSONO ANCHE SCRIVERE I PASSAGGI NORMALMENTE

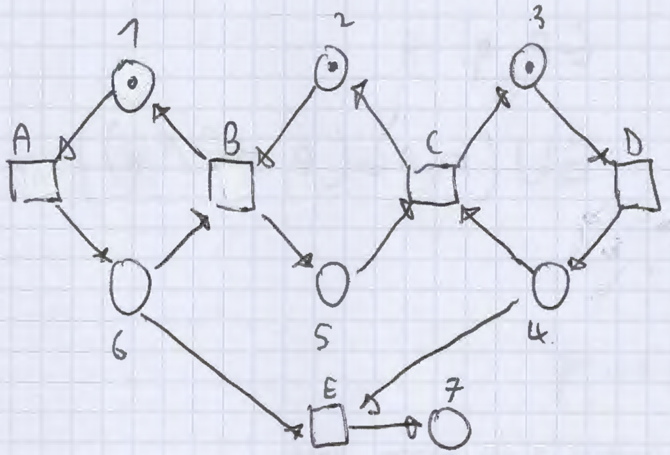
LA DOMANDA DI SCRIVERE LA DEFINIZIONE DI BISIMULAZIONE DEBOLE NON C'È PIÙ MA C'È ALL'ORALE

SE SONO BISIMILI BISOGNA TROVARE UNA STRATEGIA VINCENTE DEL DIFENSORE QUINDI BISOGNA CONSIDERARE TUTTE LE POSSIBILI MOSSE DELL'ATTACCANTE

ALL'ESAME NON SARANNO BISIMILI

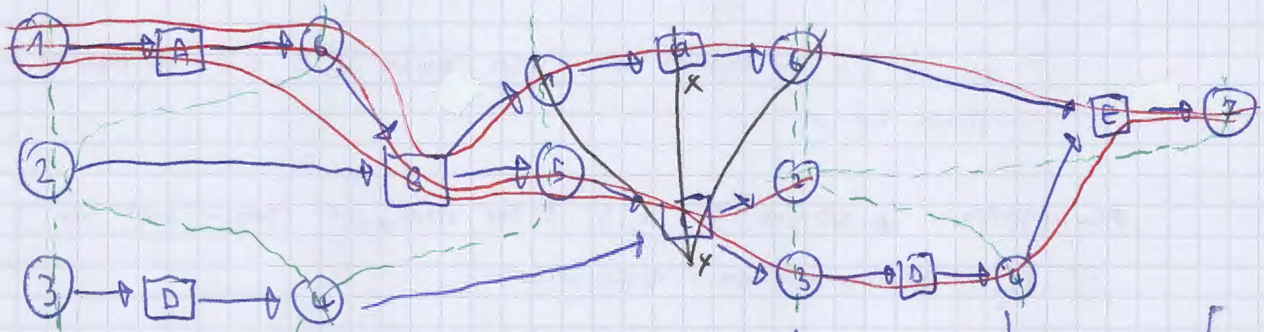
MC-L23

ESERCIZIO 2



ANCHE QUI LA DEFINIZIONE
NON LA CHIEDONO PIÙ

I CONFLITTI SONO SU 6 TRA B ED E E SU 4 TRA C ED E



A E D SONO GLI EVENTI ABILITATI

B NON È ABILITATO

SAME C, E

2, 4, 6 È UN NUOVO TAGLIO AKA CASO RAGGIUNGIBILE

EVENTI ABILITATI: B, E NON SONO INDIPENDENTI, SONO IN CONFLITTO

SE SCATTA E, C NON PUÒ PIÙ SCATTARE QUINDI ROCCIAMO B

1, 4, 5 TAGLIO

EVENTI ABILITATI A, C

TAGLIO 2, 3, 6

TAGLIO 2, 4, 6

TAGLIO FINALE 2, 7

3 POSSIBILI LINEE CON ALMENO UN'OCCORRENZA DI C

PER FARE UN TAGLIO DISCONNESSO DARE UN IDENTIFICATORE ES X, Y ALTRIMENTI

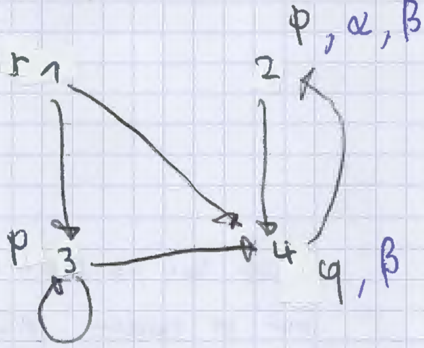
SE DICI A, C A OCCORRE ANCHE PRIMA QUINDI È SBAGLIATO

3 POSSIBILI TAGLI

ALTRIMENTI BASTA FARE LINEE E TAGLI GRADUALMENTE

MC-L23

ESERCIZIO 4



$GF\,q$

$EU(r, AG(p \to AX\,q))$

1 "è sempre vero che prima o poi q"

VALIDA IN UNO STATO SE NEL PRESENTE O NEL FUTURO VALE

RICHIAMOCI UN'IDEA AGLI CAMMINI MASSIMALI

$GF\,q$ vale in 2, 4

in 3 c'è il cammino che rimane sempre in 3 dove la formula non è vera

idem in 1

Per giustificare la risposta in 1, 3 si può mostrare il cammino dove non è valida

in 2, 4 bisogna mostrare il ragionamento

2 per CTL (* no LTL) possiamo partire dall'interno

$AX\,q$ "per ogni cammino nel prossimo stato vale q"

non vale in 1, 3, 4

vale in 2

A questo punto chiamiamo $\alpha = AX\,q$ e la marchiamo come prop. atomica che sappiamo dove vale, aggiungiamola al sistema di transizioni

Ora abbiamo $EU(r, AG(p \to \alpha))$

Ora consideriamo

$\beta = AG(p \to \alpha)$ in 2, quando va in 4 $p \to \alpha$ è vera perché l'antecedente è falso quindi è vera in 2

vale anche nello stato 4

in 3 vale p ma non vale α quindi non vale

in 1 no perché possiamo andare a 3

MC123

$\gamma : E\, U(\Gamma, \beta)$

NELLO STATO 2 VALE

ANCHE 4

IN 3 NO PERCHÉ IN 3 NON VALGONO NÉ Γ NÉ β

IN 1 SÌ PERCHÉ IN 1 VALE Γ ED ESISTE UN CAMMINO CHE VA IN 4 DOVE VALE BETA, DATO CHE C'È E QUESTO BASTA.

$\gamma : 2, 4, 1$