CORRETTEZZA PARZIALE E TOTALE DI PROGRAMMI URM

UN PROGRAMMA P SI DICE PARZIALMENTE CORRETTO RISPETTO A DATE SPECIFICHE DI INPUT $\mathcal{A}$ E DI OUTPUT $\mathcal{B}$ SE

- PER OGNI INPUT $\vec{x}$ SODDISFACENTE LE SPECIFICHE $\mathcal{A}$, SE L'ESECUZIONE DI P SU $\vec{x}$ E' TERMINANTE, ALLORA L'OUTPUT DI P SODDISFA LE SPECIFICHE $\mathcal{B}$

ESEMPI

$\lambda xy.\, x+y$

I_1 $J(3,2,5)$

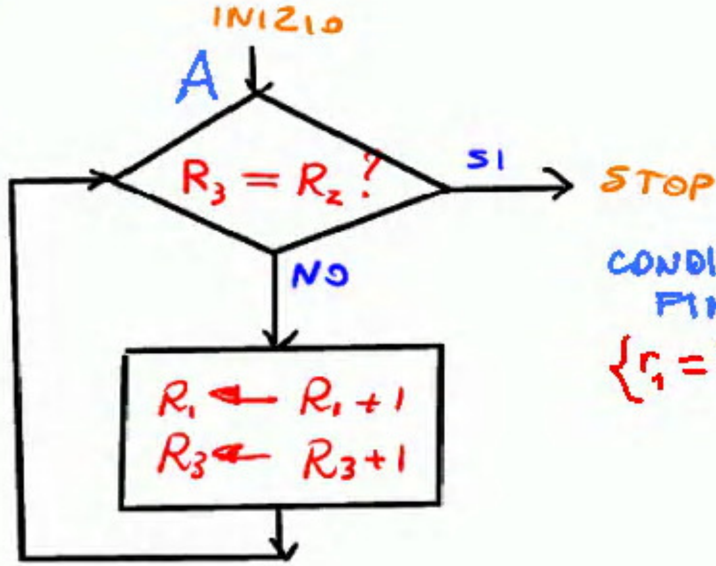
I_2 $S(1)$

I_3 $S(3)$

I_4 $J(1,1,1)$

CONDIZIONI INIZIALI

$$\begin{cases} r_1 = \bar{r}_1 \\ r_2 = \bar{r}_2 \\ r_3 = 0 \end{cases}$$



CONDIZIONE FINALE

$$\{ r_1 = \bar{r}_1 + \bar{r}_2 \}$$

DEBBONO VALERE

CONDIZIONI INIZIALI $\Longrightarrow$ A

$A \wedge r_3 = r_2 \Longrightarrow$ CONDIZIONE FINALE

$$(A \wedge r_3 \neq r_2 \wedge r_1' = r_1 + 1 \wedge r_3' = r_3 + 1 \wedge r_2' = r_2) \longrightarrow A^{r_1\, r_2\, r_3}_{r_1'\, r_2'\, r_3'}$$

ESEMPI

$\lambda xy.\, x+y$

I_1 $J(3,2,5)$

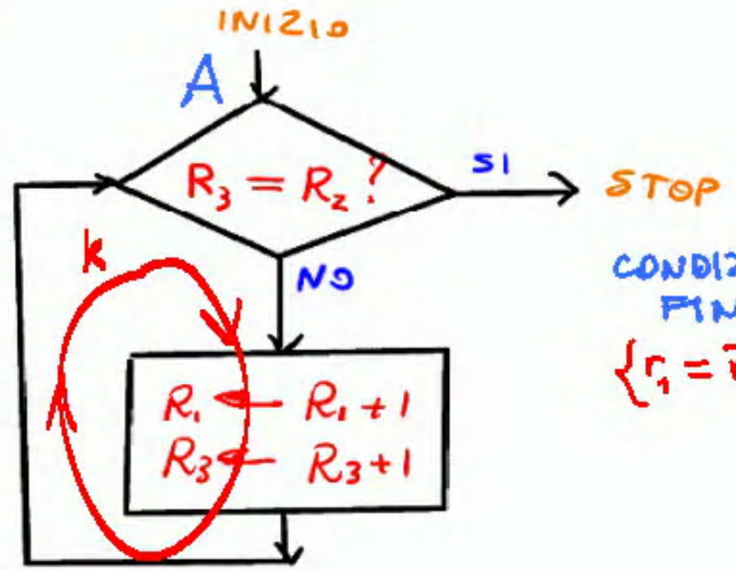
I_2 $S(1)$

I_3 $S(3)$

I_4 $J(1,1,1)$

CONDIZIONI INIZIALI

$$\begin{cases} r_1 = \bar{r}_1 \\ r_2 = \bar{r}_2 \\ r_3 = 0 \end{cases}$$



CONDIZIONE FINALE

$$\{ r_1 = \bar{r}_1 + \bar{r}_2 \}$$

DOPO k CICLI:

$$\left.\begin{array}{l} r_1^{(k)} = \bar{r}_1 + k \\ r_2^{(k)} = \bar{r}_2 \\ r_3^{(k)} = k \end{array}\right\} \Rightarrow \begin{array}{l} r_1^{(k)} = \bar{r}_1 + r_3^{(k)} \\ r_2^{(k)} = \bar{r}_2 \end{array} \Rightarrow A = \begin{cases} r_1 = \bar{r}_1 + r_3 \\ r_2 = \bar{r}_2 \end{cases}$$

CONDIZIONI INIZIALI $\Longrightarrow$ A

$$\begin{cases} r_1 = \bar{r}_1 \\ r_2 = \bar{r}_2 \\ r_3 = 0 \end{cases} \Longrightarrow \begin{cases} r_1 = \bar{r}_1 + r_3 \\ r_2 = \bar{r}_2 \end{cases}$$

INFATTI : $r_1 = \bar{r}_1 = \bar{r}_1 + 0 = \bar{r}_1 + r_3$

$A \wedge r_3 = r_2 \Longrightarrow$ CONDIZIONE FINALE

INFATTI :

$$\begin{cases} r_1 = \bar{r}_1 + r_3 \\ r_2 = \bar{r}_2 \end{cases} \wedge \quad r_3 = r_2 \Longrightarrow r_1 = \bar{r}_1 + r_3 = \bar{r}_1 + r_2 = \bar{r}_1 + \bar{r}_2$$

(CONDIZIONE FINALE)

$$\left(A \wedge r_3 \neq r_2 \wedge r_1' = r_1+1 \wedge r_3' = r_3+1 \wedge r_2' = r_2\right) \longrightarrow A^{r_1 r_2 r_3}_{r_1' r_2' r_3'}$$

INFATTI:

$$\begin{Bmatrix} r_1 = \bar{r}_1 + r_3 \\ r_2 = \bar{r}_2 \end{Bmatrix} \wedge r_3 \neq r_2 \wedge r_1' = r_1+1 \wedge r_3' = r_3+1 \wedge r_2' = r_2$$

$$\rightarrow \begin{Bmatrix} r_1' = r_1 + 1 = \bar{r}_1 + r_3 + 1 = \bar{r}_1 + r_3' \\ r_2' = r_2 = \bar{r}_2 \end{Bmatrix} \equiv \begin{Bmatrix} r_1' = \bar{r}_1 + r_3' \\ r_2' = \bar{r}_2 \end{Bmatrix}$$

$$\equiv A^{r_1 r_2 r_3}_{r_1' r_2' r_3'}$$

PERTANTO IL NOSTRO PROGRAMMA E' PARZIALMENTE CORRETTO, RISPETTO ALLE SPECIFICHE DATE SULLE CONDIZIONI INIZIALI E QUELLE FINALI

PER DIMOSTRARE LA TOTALE CORRETTEZZA, OCCORRE VERIFICARE CHE IL NOSTRO PROGRAMMA SI FERMA SEMPRE (TERMINAZIONE)

E' SUFFICIENTE TROVARE UNA MISURA A VALORI IN UN INSIEME BEN FONDATO CHE DECRESCE STRETTAMENTE AD OGNI ITERAZIONE.

SPESSO COME INSIEME BEN FONDATO SI PUÒ SCEGLIERE $\mathbb{N}$

NEL NOSTRO CASO, C'E' UN'ESPRESSIONE NATURALE DEI NOSTRI REGISTRI CHE DECRESCE STRETTAMENTE AD OGNI ITERAZIONE?

UNA POSSIBILE FUNZIONE MISURA NEL NOSTRO CASO E': $r_2 - r_3$

MA OCCORRERA' VERIFICARE CHE VALGONO SEMPRE

(a) $r_2 - r_3 \in \mathbb{N}$, CIOE' $r_2 - r_3 \geq 0$

(b) $r_2' - r_3' < r_2 - r_3$

A TAL FINE E' UTILE RAFFORZARE L'INVARIANTE:

$$B \equiv A \wedge r_2 - r_3 \geq 0 \equiv \begin{cases} r_1 = \overline{r}_1 + r_3 \\ r_2 = \overline{r}_2 \\ r_2 - r_3 \geq 0 \end{cases}$$

E QUINDI VERIFICARE CHE:

$$\text{CONDIZIONI INIZIALI} \Longrightarrow B$$

$$B \wedge r_3 = r_2 \Longrightarrow \text{CONDIZIONE FINALE}$$

$$(B \wedge r_3 \neq r_2 \wedge r_1' = r_1 + 1 \wedge r_3' = r_3 + 1 \wedge r_2' = r_2) \longrightarrow B^{r_1\, r_2\, r_3}_{r_1'\, r_2'\, r_3'}$$

AD ESEMPIO, VERIFICHIAMO LA CONDIZIONE (b)

$$(B \wedge r_3 \neq r_2 \wedge r_3' = r_3 + 1 \wedge r_1' = r_1 + 1 \wedge r_2' = r_2) \rightarrow (r_2' - r_3' < r_2 - r_3)$$

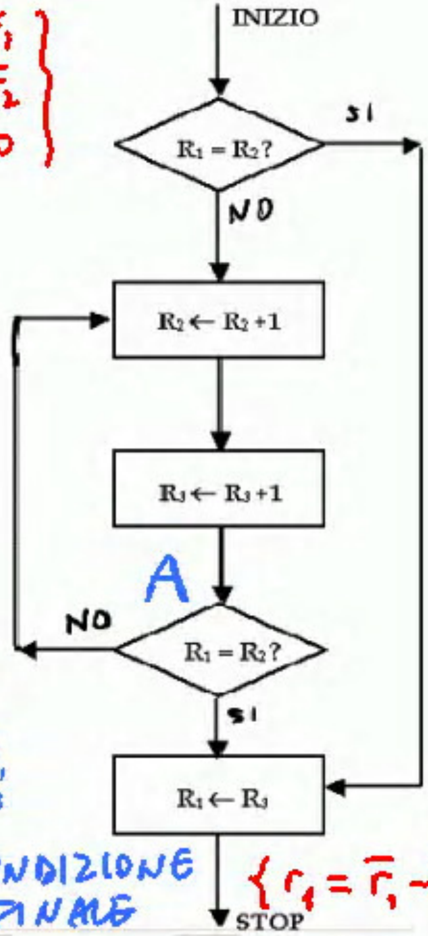
BANALMENTE SI HA:

$$r_2' - r_3' = r_2 - r_3 - 1 < r_2 - r_3$$

ESEMPIO

CONDIZIONI INIZIALI $\begin{cases} r_1 = \bar{r}_1 \\ r_2 = \bar{r}_2 \\ r_3 = 0 \end{cases}$

$I_1 : J(1,2,6)$		**if** $R_1 = R_2$ **then goto** 6
$I_2 : S(2)$	[2]	$R_2 \leftarrow R_2 + 1$
$I_3 : S(3)$		$R_3 \leftarrow R_3 + 1$
$I_4 : J(1,2,6)$		**if** $R_1 = R_2$ **then goto** 6
$I_5 : J(1,1,2)$		**if** $R_1 = R_1$ **then goto** 2
$I_6 : T(3,1)$	[6]	$R_1 \leftarrow R_3$



CONDIZIONE FINALE $\{ r_1 = \bar{r}_1 - \bar{r}_2 \}$

- $(\text{CONDIZIONI INIZIALI} \wedge r_1 = r_2 \wedge r_1' = r_3 \wedge r_2' = r_2 \wedge r_3' = r_3) \rightarrow r_1' = \bar{r}_1 - \bar{r}_2$
- $(\text{CONDIZIONI INIZIALI} \wedge r_1 \neq r_2 \wedge r_1' = r_1 \wedge r_2' = r_2 + 1 \wedge r_3' = r_3 + 1) \rightarrow A^{r_1 r_2 r_3}_{r_1' r_2' r_3'}$
- $(A \wedge r_1 \neq r_2 \wedge r_1' = r_1 \wedge r_2' = r_2 + 1 \wedge r_3' = r_3 + 1) \rightarrow A^{r_1 r_2 r_3}_{r_1' r_2' r_3'}$
- $(A \wedge r_1 = r_2 \wedge r_1' = r_3 \wedge r_2' = r_2 \wedge r_3' = r_3) \rightarrow r_1' = \bar{r}_1 - \bar{r}_2$

• $\left(\text{CONDIZIONI INIZIALI} \wedge r_1 = r_2 \wedge r_1' = r_3 \wedge r_2' = r_2 \wedge r_3' = r_3\right) \rightarrow r_1' = \bar{r}_1 - \bar{r}_2$

$$\left(\begin{Bmatrix} r_1 = \bar{r}_1 \\ r_2 = \bar{r}_2 \\ r_3 = 0 \end{Bmatrix} \wedge r_1 = r_2 \wedge r_1' = r_3 \wedge r_2' = r_2 \wedge r_3' = r_3 \right) \rightarrow$$

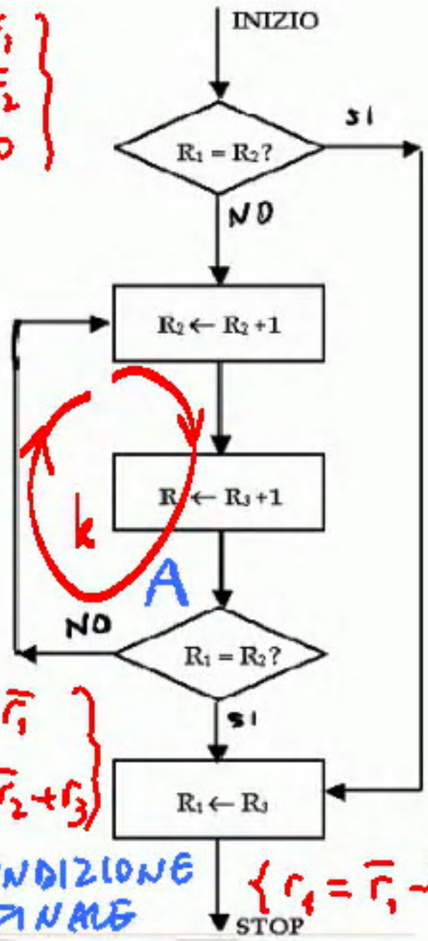
$$r_1' = r_3 = 0 = r_1 - r_2 = \bar{r}_1 - \bar{r}_2$$

$\blacksquare$

ESEMPIO

CONDIZIONI INIZIALI $\begin{cases} r_1 = \bar{r}_1 \\ r_2 = \bar{r}_2 \\ r_3 = 0 \end{cases}$

I_1 : $J(1,2,6)$		**if** $R_1 = R_2$ **then goto** 6
I_2 : $S(2)$	[2]	$R_2 \leftarrow R_2 + 1$
I_3 : $S(3)$		$R_3 \leftarrow R_3 + 1$
I_4 : $J(1,2,6)$		**if** $R_1 = R_2$ **then goto** 6
I_5 : $J(1,1,2)$		**if** $R_1 = R_1$ **then goto** 2
I_6 : $T(3,1)$	[6]	$R_1 \leftarrow R_3$



DOPO k CICLI:

$$\left.\begin{aligned} r_1^{(k)} &= \bar{r}_1 \\ r_2^{(k)} &= \bar{r}_2 + k + 1 \\ r_3^{(k)} &= k + 1 \end{aligned}\right\} \Rightarrow \begin{aligned} r_1^{(k)} &= \bar{r}_1 \\ r_2^{(k)} &= \bar{r}_2 + r_3^{(k)} \end{aligned} \Rightarrow A = \begin{cases} r_1 = \bar{r}_1 \\ r_2 = \bar{r}_2 + r_3 \end{cases}$$

CONDIZIONE FINALE $\{ r_1 = \bar{r}_1 - \bar{r}_2 \}$

$$\left(\text{CONDIZIONI INIZIALI} \wedge r_1 \neq r_2 \wedge r_1' = r_1 \wedge r_2' = r_2 + 1 \wedge r_3' = r_3 + 1\right) \to A^{r_1 r_2 r_3}_{r_1' r_2' r_3'}$$

$$\left(\begin{Bmatrix} r_1 = \bar{r}_1 \\ r_2 = \bar{r}_2 \\ r_3 = 0 \end{Bmatrix} \wedge r_1 \neq r_2 \wedge r_1' = r_1 \wedge r_2' = r_2 + 1 \wedge r_3' = r_3 + 1\right)$$

$$\Longrightarrow \begin{Bmatrix} r_1' = r_1 = \bar{r}_1 \\ r_2' = r_2 + 1 = \bar{r}_2 + 1 = \bar{r}_2 + (r_3 + 1) = \bar{r}_2 + r_3' \end{Bmatrix} \Longrightarrow \begin{Bmatrix} r_1' = \bar{r}_1 \\ r_2' = \bar{r}_2 + r_3' \end{Bmatrix}$$

$$\to A^{r_1 \; r_2 \; r_3}_{r_1' \; r_2' \; r_3'}$$

- $$(A \wedge r_1 \neq r_2 \wedge r_1' = r_1 \wedge r_2' = r_2 + 1 \wedge r_3' = r_3 + 1) \to A^{r_1\, r_2\, r_3}_{r_1'\, r_2'\, r_3'}$$

$$\left(\begin{Bmatrix} r_1 = \bar{r}_1 \\ r_2 = \bar{r}_2 + r_3 \end{Bmatrix} \wedge r_1 \neq r_2 \wedge r_1' = r_1 \wedge r_2' = r_2 + 1 \wedge r_3' = r_3 + 1 \right)$$

$$\Rightarrow \left\{ \begin{array}{l} r_1' = r_1 = \bar{r}_1 \\ r_2' = r_2 + 1 = \bar{r}_2 + r_3 + 1 = \bar{r}_2 + r_3' \end{array} \right\}$$

$$\Rightarrow \left\{ \begin{array}{l} r_1' = \bar{r}_1 \\ r_2' = \bar{r}_2 + r_3' \end{array} \right\} \equiv A^{r_1\, r_2\, r_3}_{r_1'\, r_2'\, r_3'}$$

- $(A \wedge r_1 = r_2 \wedge r_1' = r_3 \wedge r_2' = r_2 \wedge r_3' = r_3) \to r_1' = \bar{r}_1 - \bar{r}_2$

$$\left(\left\{\begin{matrix} r_1 = \bar{r}_1 \\ r_2 = \bar{r}_2 + r_3 \end{matrix}\right\} \wedge r_1 = r_2 \wedge r_1' = r_3 \wedge r_2' = r_2 \wedge r_3' = r_3\right)$$

$$\Rightarrow \quad r_1' = r_3 = r_2 - \bar{r}_2 = r_1 - \bar{r}_2 = \bar{r}_1 - \bar{r}_2$$

$$\Rightarrow \quad r_1' = \bar{r}_1 - \bar{r}_2$$

ESEMPIO

CONDIZIONI INIZIALI $\begin{cases} r_1 = \bar{r}_1 \\ r_2 = \bar{r}_2 \\ r_3 = 0 \end{cases}$

$I_1 : J(1,2,6)$ — if $R_1 = R_2$ then goto 6

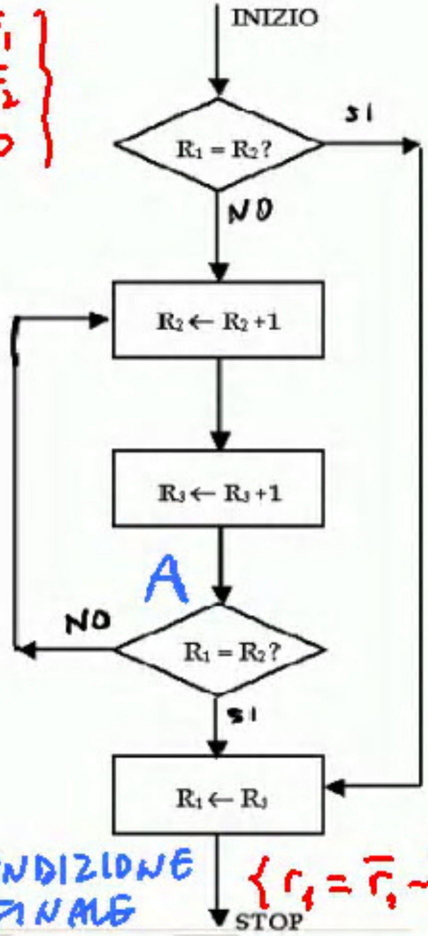
$I_2 : S(2)$ — [2] $R_2 \leftarrow R_2 + 1$

$I_3 : S(3)$ — $R_3 \leftarrow R_3 + 1$

$I_4 : J(1,2,6)$ — if $R_1 = R_2$ then goto 6

$I_5 : J(1,1,2)$ — if $R_1 = R_1$ then goto 2

$I_6 : T(3,1)$ — [6] $R_1 \leftarrow R_3$



CONDIZIONE FINALE $\{ r_1 = \bar{r}_1 - \bar{r}_2 \}$

TERMINAZIONE

CONDIZ. INIZIALI* $\equiv$ CONDIZ. INIZIALI $\wedge$ $\bar{r}_2 \leq \bar{r}_1$

$$A^* \equiv A \wedge r_2 \leq r_1$$

FUNZIONE MISURA $\equiv$ $r_1 - r_2$

CONDIZIONI DI VERIFICA

- $\left(\text{CONDIZIONI INIZIALI}^* \wedge r_1 = r_2 \wedge r_1' = r_3 \wedge r_2' = r_2 \wedge r_3' = r_3\right) \rightarrow r_1' = \bar{r}_1 - \bar{r}_2$
- $\left(\text{CONDIZIONI INIZIALI}^* \wedge r_1 \neq r_2 \wedge r_1' = r_1 \wedge r_2' = r_2 + 1 \wedge r_3' = r_3 + 1\right) \rightarrow A^{*\,r_1\, r_2\, r_3}_{\;\;r_1'\, r_2'\, r_3'}$
- $\left(A^* \wedge r_1 \neq r_2 \wedge r_1' = r_1 \wedge r_2' = r_2 + 1 \wedge r_3' = r_3 + 1\right) \rightarrow A^{*\,r_1\, r_2\, r_3}_{\;\;r_1'\, r_2'\, r_3'}$
- $\left(A^* \wedge r_1 = r_2 \wedge r_1' = r_3 \wedge r_2' = r_2 \wedge r_3' = r_3\right) \rightarrow r_1' = \bar{r}_1 - \bar{r}_2$

CONDIZIONE DI TERMINAZIONE

$$\left(A^* \wedge r_1 \neq r_2 \wedge r_1' = r_1 \wedge r_2' = r_2 + 1 \wedge r_3' = r_3 + 1\right) \rightarrow \left(r_1' - r_2' < r_1 - r_2\right)$$

$$\left(A^* \wedge r_1 \neq r_2 \wedge r_1' = r_1 \wedge r_2' = r_2 + 1 \wedge r_3' = r_3 + 1\right)$$

$$\Rightarrow \quad r_1' - r_2' = r_1 - r_2 - 1 < r_1 - r_2$$

PERTANTO IL NOSTRO PROGRAMMA CALCOLA LA FUNZIONE

$$f(x,y) = \begin{cases} x - y & \text{SE } x \geq y \\ ? & \text{ALTRIMENTI} \end{cases}$$

• STUDIAMO LA CONDIZIONE INIZIALE $\bar{r}_1 < \bar{r}_2$

IN TAL CASO POSSIAMO DIMOSTRARE CHE VALE L'INVARIANTE

$$\bar{A} \equiv A \wedge r_1 < r_2$$

E QUINDI IL TEST DELL'ISTRUZIONE $I_4 : J(1,2,6)$ DARÀ IN QUESTO CASO ESITO SEMPRE NEGATIVO E IL SUCCESSIVO CONTROLLO $I_5 : J(1,1,2)$ RIPORTERÀ A 2 IL VALORE DEL CONTATORE DI PROGRAMMA.

NE SEGUE CHE CON CONDIZIONE INIZIALE $\bar{r}_1 < \bar{r}_2$, IL NOSTRO PROGRAMMA NON SI FERMA MAI E QUINDI LA FUNZIONE CALCOLATA È:

$$f(x,y) = \begin{cases} x - y & \text{SE } x \geq y \\ \uparrow & \text{ALTRIMENTI} \end{cases}$$

∎