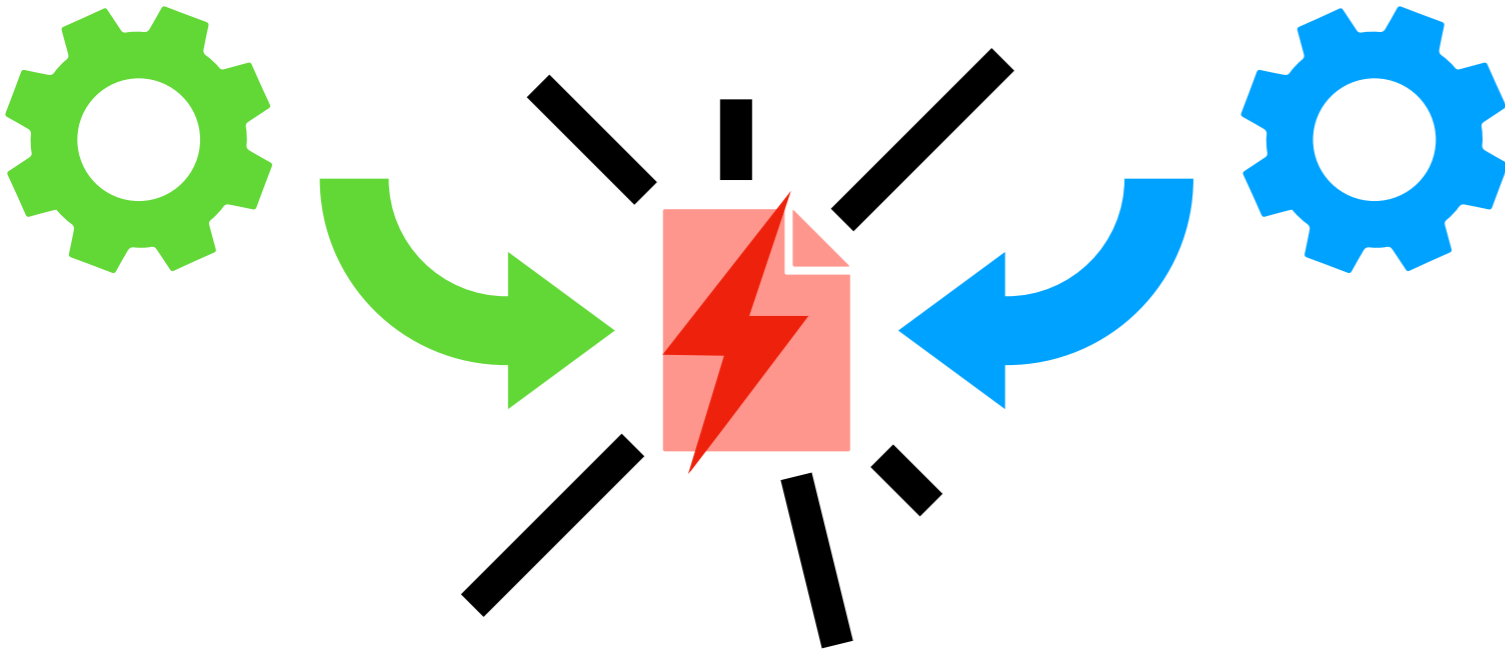


Linguaggi di Programmazione



Roberta Gori

4 - Ancora Induzione

Determinismo via induzione strutturale

Determinismo delle espressioni aritmetiche

$a ::= x \mid n \mid a \text{ op } a$

$x \in \text{Ide} \quad \text{op} \in \{+, \times, -\}$

$n \in \mathbb{Z} \quad \mathbb{M} \triangleq \{\sigma \mid \sigma : \text{Ide} \rightarrow \mathbb{Z}\}$

$$\frac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)} \quad \frac{}{\langle n, \sigma \rangle \longrightarrow n} \quad \frac{\langle a_0, \sigma \rangle \longrightarrow n_0 \quad \langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow n_0 \text{ op } n_1}$$

$$P(a) \triangleq \forall \sigma \in \mathbb{M}. \forall m, m' \in \mathbb{Z}. \langle a, \sigma \rangle \longrightarrow m \wedge \langle a, \sigma \rangle \longrightarrow m' \Rightarrow m = m'$$

$\forall a. P(a) ?$

Principio di induzione strutturale

$$\forall x \in \text{Ide. } P(x)$$

$$\forall n \in \mathbb{Z}. P(n)$$

$$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \text{ op } a_1)$$

$$\forall a. P(a)$$

Caso base

Prendiamo un generico $x \in Ide$

$\forall x \in Ide. P(x)$

Vogliamo provare

$$P(x) \triangleq \forall \sigma, m, m'. \langle x, \sigma \rangle \longrightarrow m \wedge \langle x, \sigma \rangle \longrightarrow m' \Rightarrow m = m'$$

Prendiamo σ, m, m' s.t. $\langle x, \sigma \rangle \longrightarrow m$ e $\langle x, \sigma \rangle \longrightarrow m'$

Vogliamo provare $m = m'$

Prendiamo il goal $\langle x, \sigma \rangle \longrightarrow m$

Solo la regola $\frac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)}$ è applicabile, da cui deriva $m = \sigma(x)$

Analogamente $\langle x, \sigma \rangle \longrightarrow m'$ e per questo possiamo concludere $m' = \sigma(x)$

e perciò possiamo concludere $m = \sigma(x) = m'$.

Caso base

Prendiamo un generico $n \in \mathbf{Z}$

$\forall n \in \mathbf{Z}. P(n)$

Vogliamo provare

$$P(n) \triangleq \forall \sigma, m, m'. \langle n, \sigma \rangle \longrightarrow m \wedge \langle n, \sigma \rangle \longrightarrow m' \Rightarrow m = m'$$

Prendiamo σ, m, m' s.t. $\langle n, \sigma \rangle \longrightarrow m$ e $\langle n, \sigma \rangle \longrightarrow m'$

Vogliamo provare $m = m'$

Consideriamo $\langle n, \sigma \rangle \longrightarrow m$

Solo la regola $\frac{}{\langle n, \sigma \rangle \longrightarrow n}$ è applicabile, da cui deriva $m = n$

Allo stesso modo $\langle n, \sigma \rangle \longrightarrow m'$ deve essere $m' = n$
e perciò possiamo concludere $m = m'$

Caso Induttivo

$\forall a_0, a_1. P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \text{ op } a_1)$ Prendiamo un generico a_0, a_1

Assumiamo **(ipotesi induttiva)**

$$P(a_i) \stackrel{\Delta}{=} \forall \sigma, m_i, m'_i. \langle a_i, \sigma \rangle \longrightarrow m_i \wedge \langle a_i, \sigma \rangle \longrightarrow m'_i \Rightarrow m_i = m'_i$$

Vogliamo provare

$$P(a_0 \text{ op } a_1) \stackrel{\Delta}{=} \forall \sigma, m, m'. \langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow m \wedge \langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow m' \Rightarrow m = m'$$

Prendiamo un generico σ, m, m' tale che $\langle a_0 \text{ op } a_1, \sigma \rangle \rightarrow m$ e $\langle a_0 \text{ op } a_1, \sigma \rangle \rightarrow m'$

Vogliamo provare $m = m'$

Caso induttivo (con.)

Consideriamo il goal $\langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow m$

Solo la regola $\frac{\langle a_0, \sigma \rangle \longrightarrow n_0 \quad \langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow n_0 \text{ op } n_1}$ e' applicabile

per cui $m = n_0 \text{ op } n_1$ con $\langle a_0, \sigma \rangle \rightarrow n_0$ e $\langle a_1, \sigma \rangle \rightarrow n_1$

Dal momento che $\langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow m'$

è necessariamente vero che $m' = n'_0 \text{ op } n'_1$ con $\langle a_0, \sigma \rangle \rightarrow n'_0$ e $\langle a_1, \sigma \rangle \rightarrow n'_1$

Per ipotesi induttiva, $n_0 = n'_0$ e $n_1 = n'_1$

e perciò possiamo concludere che $m = n_0 \text{ op } n_1 = n'_0 \text{ op } n'_1 = m'$

Segnature su multi-sort

Termini su una segnatura con sort

$S = \{s, \dots\}$ un insieme di **sort (tipi)**

$\Sigma = \{\Sigma_{s_1 \dots s_n, s}\}_{s_1, \dots, s_n, s \in S}$ una **segnatura con sort**

$f \in \Sigma_{s_1 \dots s_n, s}$ $f : (s_1 \times \dots \times s_n) \rightarrow s$

$T_{\Sigma, s}$ denota l'insieme dei **termini del sort s**

e' il minimo insieme tale che:

- if $c \in \Sigma_{\epsilon, s}$, then $c \in T_{\Sigma, s}$
- if $f \in \Sigma_{s_1 \dots s_n, s}$ and $\forall i. t_i \in T_{\Sigma, s_i}$, then $f(t_1, \dots, t_n) \in T_{\Sigma, s}$

$T_{\Sigma} = \{T_{\Sigma, s}\}_{s \in S}$ denota l'insieme di tutti i termini che rispettano i sort

Espressioni booleane

$$x \in \text{Ide} \quad n \in \mathbb{Z} \quad \text{op} \in \{+, \times, -\}$$

$$v \in \mathbb{B} \quad \text{bop} \in \{\wedge, \vee\} \quad \text{cmp} \in \{<, \leq, >, \geq, =, \neq\}$$

$$a ::= x \mid n \mid a \text{ op } a$$

$$b ::= v \mid a \text{ cmp } a \mid \neg b \mid b \text{ bop } b$$

$$S \triangleq \{A_{\text{exp}}, B_{\text{exp}}\}$$

$$\Sigma_{\epsilon, A_{\text{exp}}} \triangleq \text{Ide} \cup \mathbb{Z}$$

$$\Sigma_{A_{\text{exp}}A_{\text{exp}}, A_{\text{exp}}} \triangleq \{+, \times, -\}$$

$$\Sigma_{\epsilon, B_{\text{exp}}} \triangleq \mathbb{B}$$

$$\Sigma_{A_{\text{exp}}A_{\text{exp}}, B_{\text{exp}}} \triangleq \{<, \leq, >, \geq, =, \neq\}$$

$$\Sigma_{B_{\text{exp}}, B_{\text{exp}}} \triangleq \{\neg\}$$

$$\Sigma_{B_{\text{exp}}B_{\text{exp}}, B_{\text{exp}}} \triangleq \{\wedge, \vee\}$$

Semantica delle espressioni aritmetiche e booleane

$a ::= x \mid n \mid a \text{ op } a$

$b ::= v \mid a \text{ cmp } a \mid \neg b \mid b \text{ bop } b$

$$\frac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)} \quad \frac{}{\langle n, \sigma \rangle \longrightarrow n} \quad \frac{\langle a_0, \sigma \rangle \longrightarrow n_0 \quad \langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow n_0 \text{ op } n_1}$$

$$\frac{}{\langle v, \sigma \rangle \longrightarrow v} \quad \frac{\langle b, \sigma \rangle \longrightarrow v}{\langle \neg b, \sigma \rangle \longrightarrow \neg v} \quad \frac{\langle a_0, \sigma \rangle \longrightarrow n_0 \quad \langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \text{ cmp } a_1, \sigma \rangle \longrightarrow n_0 \text{ cmp } n_1}$$

$$\frac{\langle b_0, \sigma \rangle \longrightarrow v_0 \quad \langle b_1, \sigma \rangle \longrightarrow v_1}{\langle b_0 \text{ bop } b_1, \sigma \rangle \longrightarrow v_0 \text{ bop } v_1}$$

Sottotermini

$$t_i < f(t_1, \dots, t_n)$$

un sort

a special case:

$S = \{*\}$ a singleton set of **sorts**

Terminazione delle espressioni booleane

Terminazione di espressioni booleane

$a ::= x \mid n \mid a \text{ op } a$

$b ::= v \mid a \text{ cmp } a \mid \neg b \mid b \text{ bop } b$

$$\frac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)} \quad \frac{}{\langle n, \sigma \rangle \longrightarrow n} \quad \frac{\langle a_0, \sigma \rangle \longrightarrow n_0 \quad \langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow n_0 \text{ op } n_1}$$

$$\frac{}{\langle v, \sigma \rangle \longrightarrow v} \quad \frac{\langle b, \sigma \rangle \longrightarrow v}{\langle \neg b, \sigma \rangle \longrightarrow \neg v} \quad \frac{\langle a_0, \sigma \rangle \longrightarrow n_0 \quad \langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \text{ cmp } a_1, \sigma \rangle \longrightarrow n_0 \text{ cmp } n_1}$$

$$\frac{\langle b_0, \sigma \rangle \longrightarrow v_0 \quad \langle b_1, \sigma \rangle \longrightarrow v_1}{\langle b_0 \text{ bop } b_1, \sigma \rangle \longrightarrow v_0 \text{ bop } v_1}$$

$$P(b) \triangleq \forall \sigma \in \mathbb{M}. \exists v \in \mathbb{B}. \langle b, \sigma \rangle \longrightarrow v$$

$$\forall b. P(b) ?$$

Caso base

$\forall v \in \mathbb{B}. P(v)$

Consideriamo un generico $v \in \mathbb{B}$

Vogliamo provare

$$P(v) \triangleq \forall \sigma. \exists u. \langle v, \sigma \rangle \longrightarrow u$$

the only
variable

Consideriamo un generico $\sigma \in \mathbb{M}$ e consideriamo il goal $\langle v, \sigma \rangle \rightarrow u$

Per la regola

$$\frac{}{\langle v, \sigma \rangle \longrightarrow v}$$

abbiamo

$$\langle v, \sigma \rangle \longrightarrow u \xrightarrow{[u=v]} \square$$

e abbiamo finito (considerando $u=v$)

Un caso base sorprendente

$\forall a_0, a_1. P(a_0 \text{ cmp } a_1)$

Consideriamo un generico a_0, a_1

Vogliamo provare $(a_0 \text{ cmp } a_1) \stackrel{\Delta}{=} \forall \sigma. \exists v. \langle a_0 \text{ cmp } a_1, \sigma \rangle \longrightarrow v$

Consideriamo il goal $\langle a_0 \text{ cmp } a_1, \sigma \rangle \longrightarrow v$

Per la regola $\frac{\langle a_0, \sigma \rangle \longrightarrow n_0 \quad \langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \text{ cmp } a_1, \sigma \rangle \longrightarrow n_0 \text{ cmp } n_1}$ abbiamo

$\langle a_0 \text{ cmp } a_1, \sigma \rangle \longrightarrow v \swarrow_{[v=n_0 \text{ cmp } n_1]} \langle a_0, \sigma \rangle \longrightarrow n_0, \langle a_1, \sigma \rangle \longrightarrow n_1$

Per la terminazione delle espressioni aritmetiche, un tale n_0, n_1 esistono

e abbiamo finito (considerando $v = n_0 \text{ cmp } n_1$)

Per finire la prova

provare per esercizio

$$\forall b. P(b) \Rightarrow P(\neg b)$$

$$\forall b_0, b_1. (P(b_0) \wedge P(b_1)) \Rightarrow P(b_0 \text{ bop } b_1)$$

Comandi

Comandi

$a ::= x \mid n \mid a + a \mid \dots$

$b ::= v \mid a \leq a \mid \dots$

$c ::= \mathbf{skip} \mid x := a \mid c; c \mid \mathbf{if } b \mathbf{ then } c \mathbf{ else } c \mid \mathbf{while } b \mathbf{ do } c$

$S \triangleq \{ \text{Aexp}, \text{Bexp}, \text{Com} \}$

$\Sigma_{\epsilon, \text{Aexp}} \triangleq \text{Ide} \cup \mathbb{Z}$

$\Sigma_{\text{AexpAexp}, \text{Aexp}} \triangleq \{ +, \times, - \}$

$\Sigma_{\epsilon, \text{Bexp}} \triangleq \mathbb{B}$

$\Sigma_{\text{AexpAexp}, \text{Bexp}} \triangleq \{ <, \leq, >, \geq, =, \neq \}$

$\Sigma_{\text{Bexp}, \text{Bexp}} \triangleq \{ \neg \}$

$\Sigma_{\text{BexpBexp}, \text{Bexp}} \triangleq \{ \wedge, \vee \}$

$\Sigma_{\epsilon, \text{Com}} \triangleq \{ \mathbf{skip} \}$

$\Sigma_{\text{Aexp}, \text{Com}} \triangleq \{ x := \mid x \in \text{Ide} \}$

$\Sigma_{\text{ComCom}, \text{Com}} \triangleq \{ ; \}$

$\Sigma_{\text{BexpComCom}, \text{Com}} \triangleq \{ \mathbf{if} \}$

$\Sigma_{\text{BexpCom}, \text{Com}} \triangleq \{ \mathbf{while} \}$

Memorie

$$\mathbb{M} \triangleq \{ \sigma : \text{Ide} \rightarrow \mathbb{Z} \mid \sigma \text{ ha un dominio finito} \}$$

$$\{x \in \text{Ide} \mid \sigma(x) \neq 0\} \text{ e' finito}$$

$$(n_1/x_1, \dots, n_k/x_k) : \text{Ide} \rightarrow \mathbb{Z}$$

all different

$$(n_1/x_1, \dots, n_k/x_k)(x) \triangleq \begin{cases} n_i & \text{if } x = x_i \\ 0 & \text{otherwise} \end{cases}$$

$$\sigma_0 \triangleq () \text{ e' una tipica memoria iniziale}$$

Modificare la memoria

$$\sigma[n/y](x) \triangleq \begin{cases} n & \text{if } x = y \\ \sigma(x) & \text{otherwise} \end{cases}$$

$$\forall \sigma, m, n, y. \sigma[m/y][n/y] = \sigma[n/y]$$

$$\sigma[m/y][n/y](x) \triangleq \begin{cases} n & \text{if } x = y \\ \sigma[m/y](x) = \sigma(x) & \text{otherwise} \end{cases}$$

$$\forall \sigma, m, n, y, z. y \neq z \Rightarrow \sigma[n/y][m/z] = \sigma[m/z][n/y]$$

scritto anche come $\sigma[n/y, m/z]$

$$(n_1/x_1, \dots, n_k/x_k) = \sigma_0[n_1/x_1, \dots, n_k/x_k]$$

Semantica dei comandi

$c ::= \text{skip} \mid x := a \mid c; c \mid \text{if } b \text{ then } c \text{ else } c \mid \text{while } b \text{ do } c$

$$\frac{}{\langle \text{skip}, \sigma \rangle \longrightarrow \sigma} \quad \frac{\langle a, \sigma \rangle \longrightarrow n}{\langle x := a, \sigma \rangle \longrightarrow \sigma[n/x]} \quad \frac{\langle c_0, \sigma \rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma'' \rangle \longrightarrow \sigma'}{\langle c_0; c_1, \sigma \rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma \rangle \longrightarrow \text{ff} \quad \langle c_1, \sigma \rangle \longrightarrow \sigma'}{\langle \text{if } b \text{ then } c_0 \text{ else } c_1, \sigma \rangle \longrightarrow \sigma'} \quad \frac{\langle b, \sigma \rangle \longrightarrow \text{tt} \quad \langle c_0, \sigma \rangle \longrightarrow \sigma'}{\langle \text{if } b \text{ then } c_0 \text{ else } c_1, \sigma \rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma \rangle \longrightarrow \text{ff}}{\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma} \quad \frac{\langle b, \sigma \rangle \longrightarrow \text{tt} \quad \langle c, \sigma \rangle \longrightarrow \sigma'' \quad \langle \text{while } b \text{ do } c, \sigma'' \rangle \longrightarrow \sigma'}{\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma'}$$

C'e' una definizione ricorsiva!

una premessa e'
complessa come la
conclusione



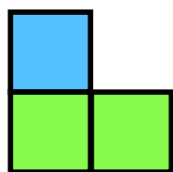
$$\frac{\langle b, \sigma \rangle \longrightarrow \mathbf{tt} \quad \langle c, \sigma \rangle \longrightarrow \sigma'' \quad \langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma'' \rangle \longrightarrow \sigma'}{\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \longrightarrow \sigma'}$$

Numeri triangolari

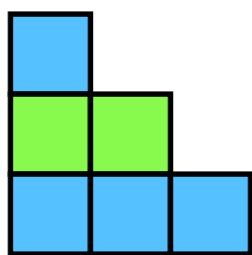
T_1 1



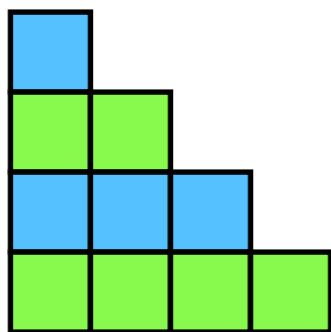
T_2 3



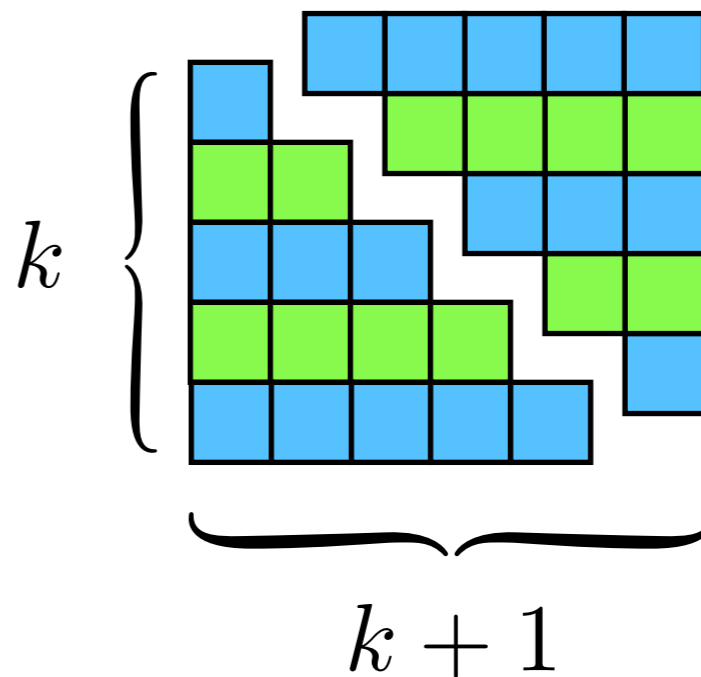
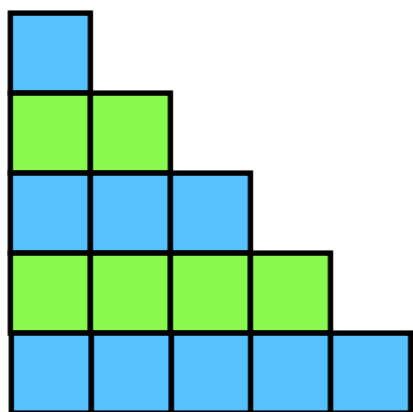
T_3 6



T_4 10



T_5 15



$$T_k \triangleq \sum_{i=1}^k i = \frac{k(k+1)}{2}$$

Calcoliamo T_2 senza div

$$\frac{\langle c_0, \sigma \rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma'' \rangle \longrightarrow \sigma'}{\langle c_0 ; c_1, \sigma \rangle \longrightarrow \sigma'}$$

$$\begin{array}{l}
 c_0 \{ \\
 c_1 \{ \\
 w \{
 \end{array}
 \left. \begin{array}{l}
 t := 0; \\
 i := 1; \quad \overbrace{\quad b \quad} \\
 \mathbf{while} \ i \leq k \ \mathbf{do} \ (\\
 \quad t := t + i; \\
 \quad i := i + 1)
 \end{array} \right\}
 \begin{array}{l}
 c_2 \\
 c_3
 \end{array}
 \left. \vphantom{\begin{array}{l} c_0 \\ c_1 \\ w \end{array}} \right\} c$$

troviamo σ tale che $\langle (c_0; c_1); w, (2/k) \rangle \rightarrow \sigma'$

troviamo σ', σ tali che $\left\{ \begin{array}{l} \langle c_0; c_1, (2/k) \rangle \longrightarrow \sigma' \\ \langle w, \sigma' \rangle \longrightarrow \sigma \end{array} \right.$

Deriviamo

troviamo σ' tale che $\langle c_0; c_1, (2/k) \rangle \longrightarrow \sigma'$

$$\langle c_0; c_1, (2/k) \rangle \longrightarrow \sigma'$$

$$\swarrow \langle t := 0, (2/k) \rangle \longrightarrow \sigma_1, \langle i := 1, \sigma_1 \rangle \longrightarrow \sigma'$$

$$\swarrow_{\sigma_1 = (2/k)[n_1/t]} \langle 0, (2/k) \rangle \longrightarrow n_1, \langle i := 1, (2/k, n_1/t) \rangle \longrightarrow \sigma'$$

$$\swarrow_{n_1=0} \langle i := 1, (2/k, 0/t) \rangle \longrightarrow \sigma'$$

$$\swarrow_{\sigma' = (2/k, 0/t)[n_2/i]} \langle 1, (2/k, 0/t) \rangle \longrightarrow n_2$$

$$\sigma' = (2/k, 0/t, 1/i)$$

$$\swarrow_{n_2=1} \square$$

$$\langle c_0; c_1, (2/k) \rangle \longrightarrow \sigma'$$

$$\swarrow^*_{\sigma' = (2/k, 0/t, 1/i)} \square$$

$c_0 \{ t := 0;$
 $c_1 \{ i := 1; \overbrace{b}^{\text{while } i \leq k \text{ do ($
 $w \{ \quad t := t + i; \quad \} c_2 \}$
 $\quad i := i + 1) \quad \} c_3 \} c$

$$\sigma \triangleq (2/n)$$

$$\frac{\langle a, \sigma \rangle \longrightarrow n}{\langle x := a, \sigma \rangle \longrightarrow \sigma[n/x]}$$

$$\frac{\langle c_0, \sigma \rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma'' \rangle \longrightarrow \sigma'}{\langle c_0; c_1, \sigma \rangle \longrightarrow \sigma'}$$

Deriviamo

$$\frac{\langle b, \sigma \rangle \longrightarrow \mathbf{tt} \quad \langle c, \sigma \rangle \longrightarrow \sigma'' \quad \langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma'' \rangle \longrightarrow \sigma'}{\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma \rangle \longrightarrow \mathbf{ff}}{\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \longrightarrow \sigma}$$

$$\begin{array}{l} c_0 \{ \\ c_1 \{ \\ w \{ \end{array} \left. \begin{array}{l} t := 0; \\ i := 1; \quad b \\ \mathbf{while} \ i \leq k \ \mathbf{do} \ (\\ \quad t := t + i; \\ \quad i := i + 1) \end{array} \right\} \begin{array}{l} c_2 \\ c_3 \end{array} \right\} c$$

troviamo σ tale che $\langle w, (2/k, 0/t, 1/i) \rangle \longrightarrow \sigma$

$$\langle w, (2/k, 0/t, 1/i) \rangle \longrightarrow \sigma$$

$$\swarrow \langle b, (2/k, 0/t, 1/i) \rangle \longrightarrow \mathbf{tt}, \langle c, (2/k, 0/t, 1/i) \rangle \longrightarrow \sigma_1, \langle w, \sigma_1 \rangle \longrightarrow \sigma$$

$$\swarrow^* \langle c, (2/k, 0/t, 1/i) \rangle \longrightarrow \sigma_1, \langle w, \sigma_1 \rangle \longrightarrow \sigma$$

$$\swarrow_{\sigma_1 = (2/k, 0/t, 1/i)[1/t, 2/i]}^* \langle w, (2/k, 1/t, 2/i) \rangle \longrightarrow \sigma$$

$$\swarrow \langle b, (2/k, 1/t, 2/i) \rangle \longrightarrow \mathbf{tt}, \langle c, (2/k, 1/t, 2/i) \rangle \longrightarrow \sigma_2, \langle w, \sigma_2 \rangle \longrightarrow \sigma$$

$$\swarrow^* \langle c, (2/k, 1/t, 2/i) \rangle \longrightarrow \sigma_2, \langle w, \sigma_2 \rangle \longrightarrow \sigma$$

$$\swarrow_{\sigma_2 = (2/k, 1/t, 2/i)[3/t, 3/i]}^* \langle w, (2/k, 3/t, 3/i) \rangle \longrightarrow \sigma$$

$$\swarrow_{\sigma = (2/k, 3/t, 3/i)} \langle b, (2/k, 3/t, 3/i) \rangle \longrightarrow \mathbf{ff}$$

$$\sigma = (2/k, 3/t, 3/i)$$

$\swarrow^* \square$

Divergenza

Terminazione di comandi?

$c ::= \text{skip} \mid x := a \mid c; c \mid \text{if } b \text{ then } c \text{ else } c \mid \text{while } b \text{ do } c$

$$\frac{}{\langle \text{skip}, \sigma \rangle \longrightarrow \sigma} \quad \frac{\langle a, \sigma \rangle \longrightarrow n}{\langle x := a, \sigma \rangle \longrightarrow \sigma[n/x]} \quad \frac{\langle c_0, \sigma \rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma'' \rangle \longrightarrow \sigma'}{\langle c_0; c_1, \sigma \rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma \rangle \longrightarrow \text{ff} \quad \langle c_1, \sigma \rangle \longrightarrow \sigma'}{\langle \text{if } b \text{ then } c_0 \text{ else } c_1, \sigma \rangle \longrightarrow \sigma'} \quad \frac{\langle b, \sigma \rangle \longrightarrow \text{tt} \quad \langle c_0, \sigma \rangle \longrightarrow \sigma'}{\langle \text{if } b \text{ then } c_0 \text{ else } c_1, \sigma \rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma \rangle \longrightarrow \text{ff}}{\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma} \quad \frac{\langle b, \sigma \rangle \longrightarrow \text{tt} \quad \langle c, \sigma \rangle \longrightarrow \sigma'' \quad \langle \text{while } b \text{ do } c, \sigma'' \rangle \longrightarrow \sigma'}{\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma'}$$

$$P(c) \triangleq \forall \sigma \in \mathbb{M}. \exists \sigma' \in \mathbb{M}. \langle c, \sigma \rangle \longrightarrow \sigma'$$

$$\forall c. P(c) ?$$

Terminazione?

$$P(c) \triangleq \forall \sigma. \exists \sigma'. \langle c, \sigma \rangle \longrightarrow \sigma'$$

$$\forall c. P(c) ?$$

take $w \triangleq$ while tt do skip

$$\langle w, \sigma \rangle \longrightarrow \sigma'$$

$$\frac{\langle b, \sigma \rangle \longrightarrow \mathbf{tt} \quad \langle c, \sigma \rangle \longrightarrow \sigma'' \quad \langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma'' \rangle \longrightarrow \sigma'}{\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma \rangle \longrightarrow \mathbf{ff}}{\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \longrightarrow \sigma}$$

$$\swarrow \langle \mathbf{tt}, \sigma \rangle \longrightarrow \mathbf{tt}, \langle \mathbf{skip}, \sigma \rangle \longrightarrow \sigma'', \langle w, \sigma'' \rangle \longrightarrow \sigma'$$

$$\swarrow \langle \mathbf{skip}, \sigma \rangle \longrightarrow \sigma'', \langle w, \sigma'' \rangle \longrightarrow \sigma'$$

$$\swarrow_{\sigma'' = \sigma} \langle w, \sigma \rangle \longrightarrow \sigma'$$

stesso goal dal quale siamo partiti!
nessun'altra opzione: $\langle \mathbf{tt}, \sigma \rangle \not\rightarrow \mathbf{ff}$
nessun modo di completare la derivazione!

$\neg P(w)$ abbiamo trovato un contro esempio alla terminazione

Divergenza

$\langle c, \sigma \rangle \not\rightarrow$ significa $\neg \exists \sigma'. \langle c, \sigma \rangle \rightarrow \sigma'$

e diciamo che c diverge con σ

qualche volta la divergenza e' difficile da
individuare
(bhe... e' indecidibile)

Divergenza

$w \triangleq \text{while } x > 0 \text{ do } x := x + 1$

consideriamo un σ generico

se $\sigma(x) \leq 0$ $\langle w, \sigma \rangle \longrightarrow \sigma' \quad \swarrow_{\sigma'=\sigma} \langle x > 0, \sigma \rangle \longrightarrow \mathbf{ff} \quad \swarrow^* \square$

quindi $\langle w, \sigma \rangle \longrightarrow \sigma$

se $\sigma(x) > 0$ $\langle w, \sigma \rangle \longrightarrow \sigma'$

$\swarrow \langle x > 0, \sigma \rangle \longrightarrow \mathbf{tt}, \langle x := x + 1, \sigma \rangle \longrightarrow \sigma'', \langle w, \sigma'' \rangle \longrightarrow \sigma'$

$\swarrow^* \langle x := x + 1, \sigma \rangle \longrightarrow \sigma'', \langle w, \sigma'' \rangle \longrightarrow \sigma'$

$\swarrow_{\sigma''=\sigma[n/x]} \langle x + 1, \sigma \rangle \longrightarrow n, \langle w, \sigma[n/x] \rangle \longrightarrow \sigma'$

$\swarrow_{n=\sigma(x)+1}^* \langle w, \sigma[\sigma(x) + 1/x] \rangle \longrightarrow \sigma'$

non e' lo stesso goal con il quale siamo partiti!

$$\sigma(x) > 0 \Rightarrow \sigma[\sigma(x) + 1/x](x) = \sigma(x) + 1 > 0$$

Come possiamo provare la divergenza?

Provare la divergenza (se e' possibile)

$$w \triangleq \text{while } b \text{ do } c$$

supponiamo di trovare un insieme di memorie $S \subseteq M$ tale che

- $\forall \sigma \in S. \langle b, \sigma \rangle \longrightarrow \mathbf{tt}$
- $\forall \sigma \in S. \forall \sigma' \in \mathbb{M}. \langle c, \sigma \rangle \longrightarrow \sigma' \Rightarrow \sigma' \in S$

Possiamo concludere $\forall \sigma \in S. \langle w, \sigma \rangle \not\rightarrow$

da notare che se $\langle c, \sigma \rangle \not\rightarrow$, $\langle c, \sigma \rangle \rightarrow \sigma' \in S$ è banalmente verificato

Rivediamo l'esempio

$w \triangleq \mathbf{while} \ x > 0 \ \mathbf{do} \ x := x + 1$ Consideriamo un generico σ

se $\sigma(x) \leq 0 \langle w, \sigma \rangle \longrightarrow \sigma$

Sia $S \triangleq \{\sigma \mid \sigma(x) > 0\}$

• $\forall \sigma \in S. \langle x > 0, \sigma \rangle \longrightarrow \mathbf{tt}$ ✓

• $\forall \sigma \in S. \forall \sigma'. \langle x := x + 1, \sigma \rangle \longrightarrow \sigma' \Rightarrow \sigma' \in S$ ✓

Infatti $\langle x := x + 1, \sigma \rangle \longrightarrow \sigma' \Rightarrow \sigma' = \sigma[\sigma(x) + 1/x]$

$\sigma(x) > 0 \Rightarrow \sigma[\sigma(x) + 1/x](x) = \sigma(x) + 1 > 0$

Perciò se $\sigma(x) > 0$, allora $\langle w, \sigma \rangle \not\rightarrow$

Esercizio

$w \triangleq \mathbf{while} \ x \neq 0 \ \mathbf{do} \ x := x - 2$

trovare tutte e sole le memorie σ tali che $\langle w, \sigma \rangle \not\rightarrow$


$$S_1 \triangleq \{\sigma \mid \sigma(x) < 0\}$$

$$S_2 \triangleq \{\sigma \mid \exists k \in \mathbb{Z}. \sigma(x) = 2k + 1\}$$

- $\forall \sigma \in S. \langle x \neq 0, \sigma \rangle \longrightarrow \mathbf{tt}$
- $\forall \sigma \in S. \forall \sigma'. \langle x := x - 2, \sigma \rangle \longrightarrow \sigma' \Rightarrow \sigma' \in S$
 $\langle x := x - 2, \sigma \rangle \longrightarrow \sigma' \Rightarrow \sigma' = \sigma[\sigma(x) - 2/x]$

Conggettura di Collatz: doppio o triplo piu' uno

$w \triangleq$ while $x > 1$ do (if $x \% 2 = 0$ then $x := x/2$
else $x := (3 \times x) + 1$)

$\forall \sigma. \sigma(x) \leq 1 \Rightarrow \langle w, \sigma \rangle \longrightarrow \sigma$ 

Conggettura aperta: $\forall \sigma. \exists \sigma'. \langle w, \sigma \rangle \longrightarrow \sigma' \equiv \neg(\exists \sigma. \langle w, \sigma \rangle \not\rightarrow)$

piu' precisamente: $\forall \sigma. \sigma(x) > 1 \Rightarrow \langle w, \sigma \rangle \longrightarrow \sigma[1/x]$

Evidenze sperimentali:

fino al 2020, la congettura e' stata verificata per tutti i valori fino a 2^{68} .

Barina, David. "Convergence verification of the Collatz problem".

The Journal of Supercomputing (2020). doi:10.1007/s11227-020-03368-x

Determinismo

Determinismo dei comandi

$c ::= \text{skip} \mid x := a \mid c; c \mid \text{if } b \text{ then } c \text{ else } c \mid \text{while } b \text{ do } c$

$$\frac{}{\langle \text{skip}, \sigma \rangle \longrightarrow \sigma} \quad \frac{\langle a, \sigma \rangle \longrightarrow n}{\langle x := a, \sigma \rangle \longrightarrow \sigma[n/x]} \quad \frac{\langle c_0, \sigma \rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma'' \rangle \longrightarrow \sigma'}{\langle c_0; c_1, \sigma \rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma \rangle \longrightarrow \text{ff} \quad \langle c_1, \sigma \rangle \longrightarrow \sigma'}{\langle \text{if } b \text{ then } c_0 \text{ else } c_1, \sigma \rangle \longrightarrow \sigma'} \quad \frac{\langle b, \sigma \rangle \longrightarrow \text{tt} \quad \langle c_0, \sigma \rangle \longrightarrow \sigma'}{\langle \text{if } b \text{ then } c_0 \text{ else } c_1, \sigma \rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma \rangle \longrightarrow \text{ff}}{\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma} \quad \frac{\langle b, \sigma \rangle \longrightarrow \text{tt} \quad \langle c, \sigma \rangle \longrightarrow \sigma'' \quad \langle \text{while } b \text{ do } c, \sigma'' \rangle \longrightarrow \sigma'}{\langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma'}$$

$$P(c) \stackrel{\Delta}{=} \forall \sigma, \sigma_1, \sigma_2. \langle c, \sigma \rangle \longrightarrow \sigma_1 \wedge \langle c, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2 \quad \forall c. P(c) ?$$

Principio di induzione strutturale

$$\forall x, a. P(x := a) \quad P(\text{skip})$$

$$\forall c_0, c_1. P(c_0) \wedge P(c_1) \Rightarrow P(c_0 ; c_1)$$

$$\forall b, c_0, c_1. P(c_0) \wedge P(c_1) \Rightarrow P(\text{if } b \text{ then } c_0 \text{ else } c_1)$$

$$\forall b, c. P(c) \Rightarrow P(\text{while } b \text{ do } c)$$

$$\forall c \in \text{Com}. P(c)$$

Caso base

$\forall x, a. P(x := a)$

Consideriamo $x \in \text{Ide}, a \in \text{Aexp}$

Vogliamo provare

$P(x := a) \triangleq \forall \sigma, \sigma_1, \sigma_2. \langle x := a, \sigma \rangle \longrightarrow \sigma_1 \wedge \langle x := a, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$

Consideriamo $\sigma, \sigma_1, \sigma_2$ t.c. $\langle x := a, \sigma \rangle \longrightarrow \sigma_1$ e $\langle x := a, \sigma \rangle \longrightarrow \sigma_2$

vogliamo ottenere $\sigma_1 = \sigma_2$

Vogliamo provare $\langle x := a, \sigma \rangle \longrightarrow \sigma_1$

Solo la regola $\frac{\langle a, \sigma \rangle \longrightarrow n}{\langle x := a, \sigma \rangle \longrightarrow \sigma[n/x]}$ e' applicabile, quindi $\sigma_1 = \sigma[n/x]$
con $\langle a, \sigma \rangle \longrightarrow n$

Analogamente, dal momento che $\langle x := a, \sigma \rangle \longrightarrow \sigma_2$ deve essere $\sigma_2 = \sigma[m/x]$
con $\langle a, \sigma \rangle \longrightarrow m$

per il determinismo di Aexp abbiamo $n = m$ e quindi $\sigma_1 = \sigma_2$

Caso Induttivo

$$\forall c_0, c_1. P(c_0) \wedge P(c_1) \Rightarrow P(c_0 ; c_1)$$

Consideriamo c_0, c_1

Assumiamo **(ipotesi induttiva)**

$$P(c_i) \triangleq \forall \sigma, \sigma_1, \sigma_2. \langle c_i, \sigma \rangle \longrightarrow \sigma_1 \wedge \langle c_i, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$$

Vogliamo provare

$$P(c_0 ; c_1) \triangleq \forall \sigma, \sigma_1, \sigma_2. \langle c_0 ; c_1, \sigma \rangle \longrightarrow \sigma_1 \wedge \langle c_0 ; c_1, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$$

Consideriamo $\sigma, \sigma_1, \sigma_2$ t.c. $\langle c_0 ; c_1, \sigma \rangle \rightarrow \sigma_1$ e $\langle c_0 ; c_1, \sigma \rangle \rightarrow \sigma_2$

Vogliamo provare $\sigma_1 = \sigma_2$

Caso induttivo (con.)

Consideriamo il goal $\langle c_0 ; c_1, \sigma \rangle \longrightarrow \sigma_1$

solo la regola
$$\frac{\langle c_0, \sigma \rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma'' \rangle \longrightarrow \sigma'}{\langle c_0 ; c_1, \sigma \rangle \longrightarrow \sigma'}$$
 e' applicabile

quindi $\sigma_1 = \sigma'_1$ con $\langle c_0, \sigma \rangle \rightarrow \sigma''_1$ e $\langle c_1, \sigma'' \rangle \rightarrow \sigma'_1$

Analogamente, $\langle c_0 ; c_1, \sigma \rangle \longrightarrow \sigma_2$

deve essere che $\sigma_2 = \sigma'_2$ con $\langle c_0, \sigma \rangle \rightarrow \sigma''_2$ e $\langle c_1, \sigma'' \rangle \rightarrow \sigma'_2$

Per ipotesi induttiva $P(c_0)$, abbiamo $\sigma''_1 = \sigma''_2$

e perciò $\langle c_1, \sigma''_2 \rangle \rightarrow \sigma'_1$ e $\langle c_1, \sigma'' \rangle \rightarrow \sigma'_2$

Per ipotesi induttiva $P(c_1)$, abbiamo $\sigma'_1 = \sigma'_2$

e possiamo concludere $\sigma_1 = \sigma'_1 = \sigma'_2 = \sigma_2$

Caso Induttivo

$\forall b, c. P(c) \Rightarrow P(\text{while } b \text{ do } c)$ Prendiamo b, c generici

Assumiamo **(ipotesi induttiva)**

$$P(c) \triangleq \forall \sigma, \sigma_1, \sigma_2. \langle c, \sigma \rangle \longrightarrow \sigma_1 \wedge \langle c, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$$

Vogliamo provare

$$P(\text{while } b \text{ do } c) \triangleq \forall \sigma, \sigma_1, \sigma_2. \langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma_1 \wedge \langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma_2 \Rightarrow \sigma_1 = \sigma_2$$

Consideriamo

$$\sigma, \sigma_1, \sigma_2 \quad \text{t.c.} \quad \langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma_1 \quad \text{e} \quad \langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma_2$$

Vogliamo provare $\sigma_1 = \sigma_2$

Per il determinismo delle espressioni booleane, abbiamo due casi

$$\langle b, \sigma \rangle \longrightarrow \mathbf{ff}$$

$$\langle b, \sigma \rangle \longrightarrow \mathbf{tt}$$

Caso induttivo (con.)

se $\langle b, \sigma \rangle \longrightarrow \mathbf{ff}$

Consideriamo il goal $\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \longrightarrow \sigma_1$

solo la regola $\frac{\langle b, \sigma \rangle \longrightarrow \mathbf{ff}}{\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \longrightarrow \sigma}$ è applicabile per cui $\sigma_1 = \sigma$

Analogamente, $\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \longrightarrow \sigma_2$ deve essere $\sigma_2 = \sigma$
e per questo possiamo concludere $\sigma_1 = \sigma = \sigma_2$

Caso induttivo (con.)

se $\langle b, \sigma \rangle \longrightarrow \mathbf{tt}$

Consideriamo il goal $\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \longrightarrow \sigma_1$

solo la regola
$$\frac{\langle b, \sigma \rangle \longrightarrow \mathbf{tt} \quad \langle c, \sigma \rangle \longrightarrow \sigma'' \quad \langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma'' \rangle \longrightarrow \sigma'}{\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \longrightarrow \sigma'}$$
 e' applicabile

per cui $\sigma_1 = \sigma'_1$ con $\langle c, \sigma \rangle \longrightarrow \sigma''_1$ e $\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma''_1 \rangle \longrightarrow \sigma'_1$

Analogamente $\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \longrightarrow \sigma_2$

Deve essere $\sigma_2 = \sigma'_2$ con $\langle c, \sigma \rangle \longrightarrow \sigma''_2$ e $\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma''_2 \rangle \longrightarrow \sigma'_2$

Per ipotesi induttiva $P(c)$, abbiamo $\sigma''_1 = \sigma''_2$

quindi $\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma''_2 \rangle \longrightarrow \sigma'_1$ e $\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma''_2 \rangle \longrightarrow \sigma'_2$

ma non esiste un ipotesi induttiva $P(\mathbf{while} \ b \ \mathbf{do} \ c)$!

Definizione ricorsiva!

la premessa complessa
quanto la conclusione



$$\frac{\langle b, \sigma \rangle \longrightarrow \mathbf{tt} \quad \langle c, \sigma \rangle \longrightarrow \sigma'' \quad \langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma'' \rangle \longrightarrow \sigma'}{\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \longrightarrow \sigma'}$$

per finire la prova di derminismo
dobbiamo usare un giusto principio di induzione:

Induzione sulle regole