Linguaggi di Programmazione

Roberta Gori

4 -Ancora Induzione

Determinismo via induzione strutturale

Determinismo delle espressioni aritmetiche

$$a \ ::= \ x \ | \ n \ | \ a \ \mathsf{op} \ a$$

$$x \in \mathsf{Ide} \qquad \mathsf{op} \in \{+, \times, -\}$$

$$n \in \mathbb{Z} \qquad \mathbb{M} \triangleq \{\sigma \mid \sigma : \mathsf{Ide} \to \mathbb{Z}\}$$

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

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

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

Principio di induzione strutturale

$$\forall x \in \mathsf{Ide}.\ P(x) \qquad\qquad \forall n \in \mathbb{Z}.\ P(n)$$

$$\frac{\forall a_0, a_1.\ P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \ \mathsf{op}\ a_1)}{\forall a.\ P(a)}$$

Caso base

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

Prendiamo un generico $x \in Ide$

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 $\dfrac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)}$ è applicabile, da cui deriva $m = \sigma(x)$

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

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

Caso base

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

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

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 $\dfrac{}{\langle n, \sigma \rangle \longrightarrow n}$ è applicabile, da cui deriva $m = n$

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

Caso Induttivo

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

Prendiamo un generico a_0, a_1

Assumiamo (ipotesi induttiva)

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

Vogliamo provare

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

Prendiamo un generico σ, m, m' tale che $\langle a_0\ op\ a_1, \sigma \rangle \to m$ e $\langle a_0\ op\ a_1, \sigma \rangle \to m'$

Vogliamo provare $m = m'$

Caso induttivo (con.)

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

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

per cui $m = n_0 \; op \; n_1$ con $\langle a_0, \sigma\rangle \rightarrow n_0$ e $\langle a_0, \sigma\rangle \rightarrow n_1$

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

è necessariamente vero che $m' = n_0' \; op \; n_1'$ 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 $m = n_0 \; op \; n_1 = n_0' \; op \; n_1' = m'$

Segnature su multi-sort

Termini su una segnatura con sort

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

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

$f \in \Sigma_{s_1 \ldots s_n, s}$ $\quad f : (s_1 \times \cdots \times s_n) \to s$

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

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

Espressioni booleane

$x \in \mathsf{Ide} \qquad n \in \mathbb{Z} \qquad \mathsf{op} \in \{+, \times, -\}$

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

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

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

$S \triangleq \{\mathsf{Aexp}, \mathsf{Bexp}\}$

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

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

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

$\Sigma_{\mathsf{Aexp}\mathsf{Aexp},\mathsf{Aexp}} \triangleq \{+, \times, -\}$

$\Sigma_{\mathsf{Aexp}\mathsf{Aexp},\mathsf{Bexp}} \triangleq \{<, \leq, >, \geq, =, \neq\}$

$\Sigma_{\mathsf{Bexp}\mathsf{Bexp},\mathsf{Bexp}} \triangleq \{\wedge, \vee\}$

Semantica delle espressioni aritmetiche e booleane

$$a \ ::= \ x \ | \ n \ | \ a \ \mathsf{op} \ a$$

$$b \ ::= \ v \ | \ a \ \mathsf{cmp} \ a \ | \ \neg b \ | \ b \ \mathsf{bop} \ b$$

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

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

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

Sottotermini

$$t_i \prec f(t_1, ..., t_n)$$

un sort

a special case:

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

$$\Sigma_{\underbrace{*\ldots*}_{n},*} \simeq \Sigma_n$$

Terminazione delle espressioni booleane

Terminazione di espressioni booleane

$$a \ ::= \ x \ | \ n \ | \ a \ \mathsf{op} \ a$$
$$b \ ::= \ v \ | \ a \ \mathsf{cmp} \ a \ | \ \neg b \ | \ b \ \mathsf{bop} \ b$$

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

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

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

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

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 $\langle v, \sigma \rangle \to u$

Per la regola $\overline{\langle v, \sigma \rangle \longrightarrow v}$ abbiamo $\langle v, \sigma \rangle \longrightarrow u \nwarrow_{[u=v]} \square$

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 $(a_0 \text{ cmp } a_1) \triangleq \forall \sigma.\ \exists v.\ \langle a_0 \text{ cmp } a_1, \sigma \rangle \longrightarrow v$

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

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

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

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

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

Per finire la prova

provare per esercizio

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

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

Comandi

Comandi

$$a ::= x \mid n \mid a + a \mid \cdots \qquad\qquad b ::= v \mid a \leq a \mid \cdots$$

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

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

$$\Sigma_{\epsilon,\mathsf{Aexp}} \triangleq \mathsf{Ide} \cup \mathbb{Z} \qquad \Sigma_{\mathsf{AexpAexp},\mathsf{Aexp}} \triangleq \{+, \times, -\}$$

$$\Sigma_{\epsilon,\mathsf{Bexp}} \triangleq \mathbb{B} \qquad \Sigma_{\mathsf{AexpAexp},\mathsf{Bexp}} \triangleq \{<, \leq, >, \geq, =, \neq\}$$

$$\Sigma_{\mathsf{Bexp},\mathsf{Bexp}} \triangleq \{\neg\} \qquad \Sigma_{\mathsf{BexpBexp},\mathsf{Bexp}} \triangleq \{\wedge, \vee\}$$

$$\Sigma_{\epsilon,\mathsf{Com}} \triangleq \{\textbf{skip}\} \qquad \Sigma_{\mathsf{Aexp},\mathsf{Com}} \triangleq \{x := \mid x \in \mathsf{Ide}\}$$

$$\Sigma_{\mathsf{ComCom},\mathsf{Com}} \triangleq \{\,;\,\} \qquad \Sigma_{\mathsf{BexpComCom},\mathsf{Com}} \triangleq \{\,\textbf{if}\,\}$$

$$\Sigma_{\mathsf{BexpCom},\mathsf{Com}} \triangleq \{\,\textbf{while}\,\}$$

Memorie

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

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

$$(n_1/x_1, \ldots, n_k/x_k) : \mathsf{Ide} \to \mathbb{Z}$$

all different

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

$\sigma_0 \triangleq ()$ 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 $\sigma[n/y, m/z]$

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

Semantica dei comandi

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

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

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

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

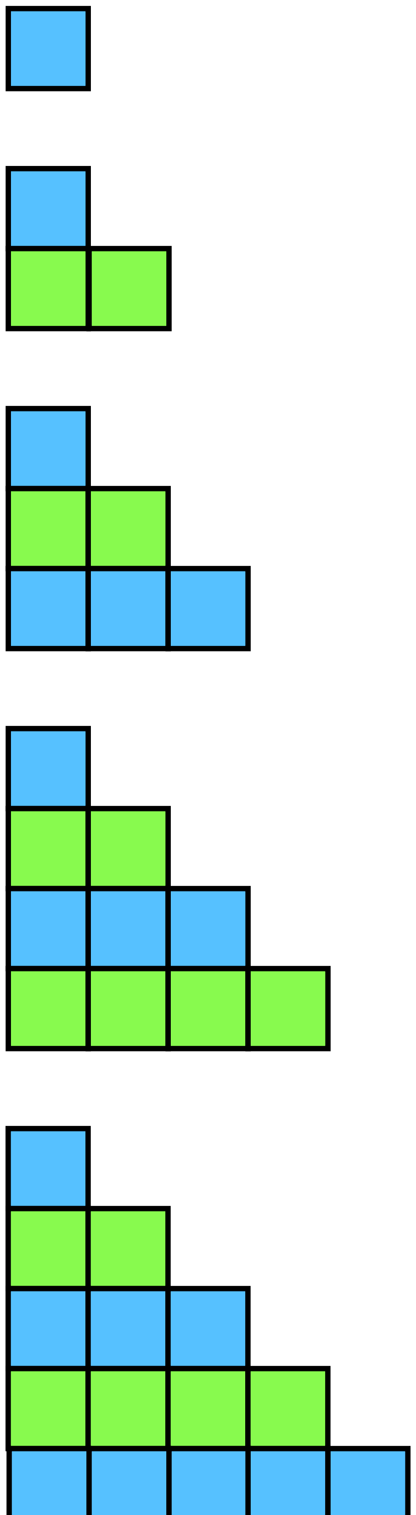
C'e' una definizione ricorsiva!

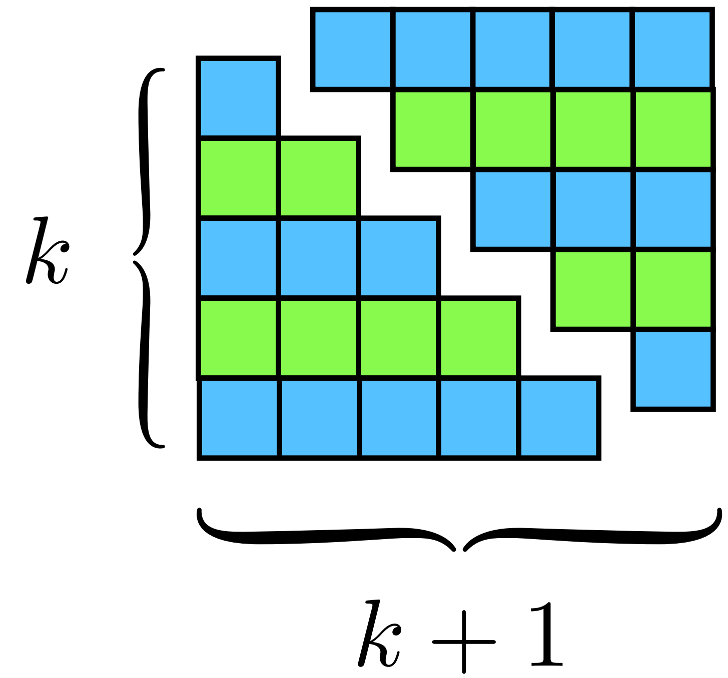
una premessa e' complessa come la conclusione

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

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

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

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

troviamo σ', σ tale 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

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

$\sigma \triangleq (2/n)$

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

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

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

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

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

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

$\nwarrow_{n_2=1} \square$

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

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

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

Deriviamo

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

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

troviamo σ' tale che $\langle w, (2/k, 0/t, 1/i) \rangle \longrightarrow \sigma$

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

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

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

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

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

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

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

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

$\nwarrow^* \square$

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

Divergenza

Terminazione di comandi?

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

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

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

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

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

Terminazione?

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

take $w \triangleq$ **while tt do skip**

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

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

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

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

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

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

Divergenza

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

e diciamo che c diverge con σ

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

Divergenza

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

consideriamo un σ generico

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

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

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

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

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

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

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

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)

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

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 $\forall \sigma \in S.\ \langle w, \sigma \rangle \not\longrightarrow$

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

Revediamo l'esempio

$w \triangleq \textbf{while } x > 0 \textbf{ do } x := x + 1$ 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 $\langle x := x + 1, \sigma \rangle \longrightarrow \sigma' \Rightarrow \sigma' = \sigma[\sigma(x) + 1/x]$

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

Percio' se $\sigma(x) > 0$, allora $\langle w, \sigma \rangle \not\longrightarrow$

Esercizio

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

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

$$S_1 \triangleq \{\sigma \mid \sigma(x) < 0\} \qquad S_2 \triangleq \{\sigma \mid \exists k \in \mathbb{Z}.\ \sigma(x) = 2k + 1\}$$

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

$$\langle x := x - 2, \sigma \rangle \longrightarrow \sigma' \Rightarrow \sigma' = \sigma[\sigma(x) - 2/x]$$

Congettura di Collatz: doppio o triplo piu' uno

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

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

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

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

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

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

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

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

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

Principio di induzione strutturale

$$\frac{\forall x, a.\ P(x := a) \qquad P(\mathbf{skip}) \qquad \forall c_0, c_1.\ P(c_0) \wedge P(c_1) \Rightarrow P(c_0\,;c_1) \qquad \forall b, c_0, c_1.\ P(c_0) \wedge P(c_1) \Rightarrow P(\mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1) \qquad \forall b, c.\ P(c) \Rightarrow P(\mathbf{while}\ b\ \mathbf{do}\ c)}{\forall c \in \mathsf{Com}.\ P(c)}$$

Caso base

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

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

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 $\langle x := a, \sigma \rangle \longrightarrow \sigma_2$

Consideriamo il goal $\sigma_1 = \sigma_2$

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

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

con $\langle a, \sigma \rangle \longrightarrow n$

Analogomente, 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

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

Consideriamo c_0, c_1

Assumiamo (ipotesi induttiva)

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

Vogliamo provare

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

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 $\dfrac{\langle c_0, \sigma\rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma''\rangle \longrightarrow \sigma'}{\langle c_0\, ; c_1, \sigma\rangle \longrightarrow \sigma'}$ e' applicabile

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

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

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

Per ipotesi induttiva $P(c_0)$, abbiamo $\sigma_1'' = \sigma_2''$

e percio' $\langle c_1, \sigma_2''\rangle \to \sigma_1'$ e $\langle c_1, \sigma''\rangle \to \sigma_2'$

Per ipotesi induttiva $P(c_1)$, abbiamo $\sigma_1' = \sigma_2'$

e possiamo concludere $\sigma_1 = \sigma_1' = \sigma_2' = \sigma_2$

Caso Induttivo

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

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

Consideriamo

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

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 $\langle \textbf{while } b \textbf{ do } c, \sigma \rangle \longrightarrow \sigma_1$

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

Analogamente, $\langle \textbf{while } b \textbf{ do } c, \sigma \rangle \longrightarrow \sigma_2$ 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 $\dfrac{\langle b, \sigma \rangle \longrightarrow \mathbf{tt} \quad \langle c, \sigma \rangle \longrightarrow \sigma'' \quad \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma'' \rangle \longrightarrow \sigma'}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma \rangle \longrightarrow \sigma'}$ 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

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

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

Induzione sulle regole