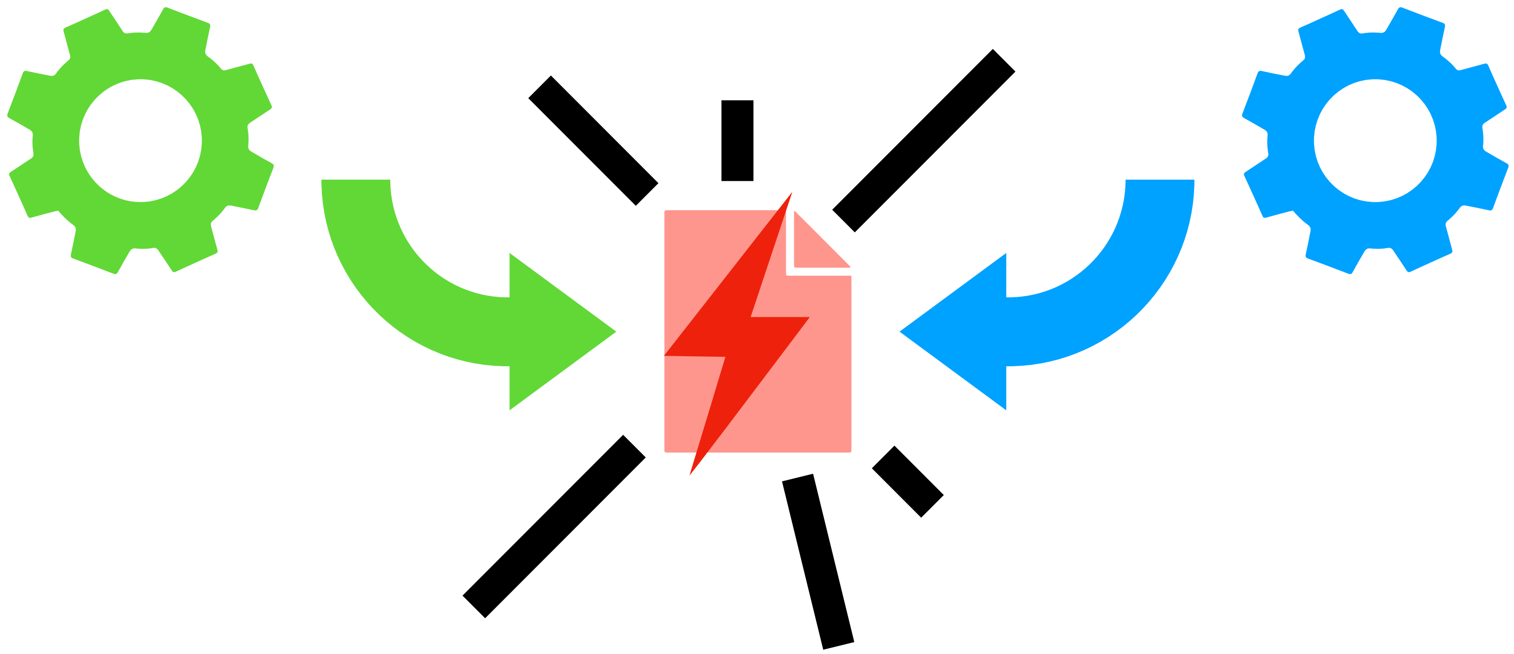
Linguaggi di Programmazione



Roberta Gori

Consistenza e congruenza-6.3

Equivalenza operazionale

Equivalenza operazionale

$$a_1 \sim_{\mathrm{op}} a_2 \quad \text{sse} \quad \forall \sigma, n.\ (\ \langle a_1, \sigma \rangle \rightarrow n \Leftrightarrow \langle a_2, \sigma \rangle \rightarrow n\ )$$

$$b_1 \sim_{\mathrm{op}} b_2 \quad \text{sse} \quad \forall \sigma, v.\ (\ \langle b_1, \sigma \rangle \rightarrow v \Leftrightarrow \langle b_2, \sigma \rangle \rightarrow v\ )$$

$$c_1 \sim_{\mathrm{op}} c_2 \quad \text{sse} \quad \forall \sigma, \sigma'.\ (\ \langle c_1, \sigma \rangle \rightarrow \sigma' \Leftrightarrow \langle c_2, \sigma \rangle \rightarrow \sigma'\ )$$

terminazione and determinismo non hanno importanza:
l'equivalenza operazionale e' sempre ben definita

Congruenza

$$a_1 \sim_{\text{op}} a_2 \quad \text{sse} \quad \forall \sigma, n. \ (\ \langle a_1, \sigma \rangle \to n \Leftrightarrow \langle a_2, \sigma \rangle \to n \ )$$

prendiamo un qls contesto $\mathbb{A}[\cdot]$ p.e. $2 \times ([\cdot] + 5)$

e' vero che $a_1 \sim_{\text{op}} a_2 \Rightarrow \mathbb{A}[a_1] \sim_{\text{op}} \mathbb{A}[a_2]$?

ovvero: possiamo rimpiazzare una sottoespressione con una equivalente senza cambiare il risultato?

Contesti

quali sono i contesti possibili per le espressioni aritmetiche?

$$[\cdot] + 5$$

$$2 \times ([\cdot] + 5)$$

$$2 \times ([\cdot] + 5) \leq 50$$

$$(2 \times ([\cdot] + 5) \leq 50) \wedge x = y$$

$$x := 2 \times ([\cdot] + 5)$$

$$\textbf{while } x \leq 100 \textbf{ do } x := 2 \times ([\cdot] + 5)$$

Contesti

quali sono i contesti possibili per le espressioni aritmetiche?

$$\mathbb{A}[\cdot] \quad ::= \quad [\cdot] \quad | \quad \mathbb{A}[\cdot] \ \mathsf{op}\ a \quad | \quad a\ \mathsf{op}\ \mathbb{A}[\cdot]$$

$$\mathbb{B}[\cdot] \quad ::= \quad \mathbb{A}[\cdot]\ \mathsf{cmp}\ a \quad | \quad a\ \mathsf{cmp}\ \mathbb{A}[\cdot] \quad | \quad \neg\mathbb{B}[\cdot] \quad | \quad \mathbb{B}[\cdot]\ \mathsf{bop}\ b \quad | \quad b\ \mathsf{bop}\ \mathbb{B}[\cdot]$$

$$\mathbb{C}[\cdot] \quad ::= \quad x := \mathbb{A}[\cdot] \quad | \quad \mathbb{C}[\cdot]; c \quad | \quad c; \mathbb{C}[\cdot] \quad | \quad \textbf{if}\ \mathbb{B}[\cdot]\ \textbf{then}\ c\ \textbf{else}\ c \quad | \quad \textbf{if}\ b\ \textbf{then}\ \mathbb{C}[\cdot]\ \textbf{else}\ c \quad | \quad \textbf{if}\ b\ \textbf{then}\ c\ \textbf{else}\ \mathbb{C}[\cdot] \quad | \quad \textbf{while}\ \mathbb{B}[\cdot]\ \textbf{do}\ c \quad | \quad \textbf{while}\ b\ \textbf{do}\ \mathbb{C}[\cdot]$$

Proof obligation

dobbiamo trattare molte proof obligation:

$$\forall a, a_1, a_2.\ (\ a_1 \sim_{\mathrm{op}} a_2 \Rightarrow a_1\ \textsf{op}\ a \sim_{\mathrm{op}} a_2\ \textsf{op}\ a\ )$$

$$\forall a, a_1, a_2.\ (\ a_1 \sim_{\mathrm{op}} a_2 \Rightarrow a\ \textsf{op}\ a_1 \sim_{\mathrm{op}} a\ \textsf{op}\ a_2\ )$$

$$\forall a, a_1, a_2.\ (\ a_1 \sim_{\mathrm{op}} a_2 \Rightarrow a\ \textsf{cmp}\ a_1 \sim_{\mathrm{op}} a\ \textsf{cmp}\ a_2\ )$$

$$\forall a, a_1, a_2.\ (\ a_1 \sim_{\mathrm{op}} a_2 \Rightarrow a_1\ \textsf{cmp}\ a \sim_{\mathrm{op}} a_2\ \textsf{cmp}\ a\ )$$

$$\forall x, a_1, a_2.\ (\ a_1 \sim_{\mathrm{op}} a_2 \Rightarrow x := a_1 \sim_{\mathrm{op}} x := a_2\ )$$

la stessa cosa per espressioni booleane e comandi

Equivalenza denotazionale

Equivalenza denotazionale

$$a_1 \sim_{\text{den}} a_2 \quad \text{sse} \quad \mathcal{A}[\![a_1]\!] = \mathcal{A}[\![a_2]\!]$$

$$b_1 \sim_{\text{den}} b_2 \quad \text{sse} \quad \mathcal{B}[\![b_1]\!] = \mathcal{B}[\![b_2]\!]$$

$$c_1 \sim_{\text{den}} c_2 \quad \text{sse} \quad \mathcal{C}[\![c_1]\!] = \mathcal{C}[\![c_2]\!]$$

(due funzioni sono la stessa se coincidono su tutti gli argomenti)

Principio di Composizionalita'

$$a_1 \sim_{\text{den}} a_2 \quad \text{sse} \quad \mathcal{A}[\![a_1]\!] = \mathcal{A}[\![a_2]\!]$$

prendiamo un qls contesto $\mathbb{A}[\cdot]$

e' vero che $a_1 \sim_{\text{den}} a_2 \Rightarrow \mathbb{A}[a_1] \sim_{\text{den}} \mathbb{A}[a_2]$?

SI, è garantito dal principio di composizionalita' della semantica denotazionale:

il significato di un'espressione composta è unicamente determinato dal significato dei suoi costituenti

Consistenza

se garantiamo la coerenza tra
la semantica operazionale e
la semantica denotazionale
allora la proprietà di congruenza è garantita
anche per la semantica operazionale

$$\forall a_1, a_2.\ (\ a_1 \sim_{\mathrm{op}} a_2 \stackrel{?}{\Leftrightarrow} a_1 \sim_{\mathrm{den}} a_2\ )$$

$$\forall b_1, b_2.\ (\ b_1 \sim_{\mathrm{op}} b_2 \stackrel{?}{\Leftrightarrow} b_1 \sim_{\mathrm{den}} b_2\ )$$

$$\forall c_1, c_2.\ (\ c_1 \sim_{\mathrm{op}} c_2 \stackrel{?}{\Leftrightarrow} c_1 \sim_{\mathrm{den}} c_2\ )$$

Consistenza: espressioni

$$\forall\, a \in Aexp\ \forall \sigma \in \Sigma.\ \langle a, \sigma \rangle \to \mathscr{A}\,[\![a]\!]\,\sigma$$

$$P(a) \stackrel{\text{def}}{=} \forall \sigma \in \Sigma.\ \langle a, \sigma \rangle \to \mathscr{A}\,[\![a]\!]\,\sigma$$

per induzione strutturale

$$\forall\, b \in Bexp\ \forall \sigma \in \Sigma.\ \langle b, \sigma \rangle \to \mathscr{B}\,[\![b]\!]\,\sigma$$

$$P(b) \stackrel{\text{def}}{=} \forall \sigma \in \Sigma.\ \langle b, \sigma \rangle \to \mathscr{B}\,[\![b]\!]\,\sigma$$

per induzione strutturale

Consistenza: comandi

$\forall c \in Com.\ \forall \sigma, \sigma' \in \Sigma.$ $\langle c, \sigma \rangle \to \sigma' \quad \Leftrightarrow \quad \mathscr{C}\,[\![c]\!]\,\sigma = \sigma'$

possiamo scriverlo come

$\forall c \in Com.\ \forall \sigma \in \Sigma. \quad \langle c, \sigma \rangle \to \mathscr{C}\,[\![c]\!]\,\sigma$?

no, non c'e' una formula del tipo

$$\langle c, \sigma \rangle \to \bot$$

Consistenza: comandi

$\forall c \in Com.\ \forall \boldsymbol{\sigma}, \boldsymbol{\sigma}' \in \Sigma.\quad \langle c, \boldsymbol{\sigma} \rangle \to \boldsymbol{\sigma}' \quad \Leftrightarrow \quad \mathscr{C}\,[\![c]\!]\,\boldsymbol{\sigma} = \boldsymbol{\sigma}'$

$\forall c \in Com.\ \forall \boldsymbol{\sigma}, \boldsymbol{\sigma}' \in \Sigma.$

Correttezza

$$P(\langle c, \boldsymbol{\sigma} \rangle \to \boldsymbol{\sigma}') \stackrel{\text{def}}{=} \mathscr{C}\,[\![c]\!]\,\boldsymbol{\sigma} = \boldsymbol{\sigma}'$$

per induzione sulle regole

$\forall c \in Com.$

Completezza

$$P(c) \stackrel{\text{def}}{=} \forall \boldsymbol{\sigma}, \boldsymbol{\sigma}' \in \Sigma.\quad \mathscr{C}\,[\![c]\!]\,\boldsymbol{\sigma} = \boldsymbol{\sigma}' \quad \Rightarrow \quad \langle c, \boldsymbol{\sigma} \rangle \to \boldsymbol{\sigma}'$$

per induzione strutturale

Correttezza

$$\forall c \in Com,\ \forall \boldsymbol{\sigma}, \boldsymbol{\sigma}' \in \Sigma$$

$$P(\langle c, \boldsymbol{\sigma} \rangle \rightarrow \boldsymbol{\sigma}') \stackrel{\text{def}}{=} \mathscr{C}[\![c]\!]\,\boldsymbol{\sigma} = \boldsymbol{\sigma}'$$

per induzione sulle regole

$$\overline{\langle \mathbf{skip}, \sigma \rangle \to \sigma}$$

Vogliamo provare

$$P(\langle \mathbf{skip}, \sigma \rangle \to \sigma) \stackrel{\text{def}}{=} \mathscr{C}\,[\![\mathbf{skip}]\!]\,\sigma = \sigma$$

Ovviamente la preposizione e’ vera per definizione della semantica denotazionale

N.B. Possiamo assumere solo che la semantica operazionale delle espressioni aritmetiche mi dia m: non abbiamo nessuna ipotesi induttiva sulle espressioni aritmetiche!

$$\frac{\langle a, \sigma \rangle \to m}{\langle x := a, \sigma \rangle \to \sigma \left[{}^{m}/_{x}\right]}$$

Assumiamo $\langle a, \sigma \rangle \to m$ e quindi $\mathscr{A}\,[\![a]\!]\,\sigma = m$ per equivalenza della semantica operazionale e denotazionale delle espressioni aritmetiche.
Vogliamo provare che

$$P(\langle x := a, \sigma \rangle \to \sigma \left[{}^{m}/_{x}\right]) \stackrel{\text{def}}{=} \mathscr{C}\,[\![x := a]\!]\,\sigma = \sigma \left[{}^{m}/_{x}\right]$$

Per definizione della semantica denotazionale abbiamo che

$$\mathscr{C}\,[\![x := a]\!]\,\sigma = \sigma\left[{}^{\mathscr{A}\,[\![a]\!]\,\sigma}/_{x}\right] = \sigma\left[{}^{m}/_{x}\right]$$

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

Assumiamo

$$P(\langle c_0, \sigma \rangle \to \sigma'') \stackrel{\text{def}}{=} \mathscr{C}\,[\![c_0]\!]\,\sigma = \sigma''$$

$$P(\langle c_1, \sigma'' \rangle \to \sigma') \stackrel{\text{def}}{=} \mathscr{C}\,[\![c_1]\!]\,\sigma'' = \sigma'$$

Vogliamo provare

$$P(\langle c_0; c_1, \sigma \rangle \to \sigma') \stackrel{\text{def}}{=} \mathscr{C}\,[\![c_0; c_1]\!]\,\sigma = \sigma'$$

Per la definizione di semantica denotazionale e per ipotesi induttiva

$$\mathscr{C}\,[\![c_0; c_1]\!]\,\sigma = \mathscr{C}\,[\![c_1]\!]^*\,(\mathscr{C}\,[\![c_0]\!]\,\sigma) = \mathscr{C}\,[\![c_1]\!]^*\,\sigma'' = \mathscr{C}\,[\![c_1]\!]\,\sigma'' = \sigma'$$

Notare che l’operatore di lifting puo’ essere rimosso perche’ $\sigma'' \neq \bot$

$$\frac{\langle b, \sigma \rangle \to \mathbf{true} \quad \langle c_0, \sigma \rangle \to \sigma'}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma \rangle \to \sigma'}$$

Assumiamo

- $\langle b, \sigma \rangle \to \mathbf{true}$ e percio' $\mathscr{B}\,[\![b]\!]\,\sigma = \mathbf{true}$ per la corrispondenza

  tra semantica denotazionale e operazionale per le espressioni booleane

- $P(\langle c_0, \sigma \rangle \to \sigma') \stackrel{\text{def}}{=} \mathscr{C}\,[\![c_0]\!]\,\sigma = \sigma'$

vogliamo provare

$$P(\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma \rangle \to \sigma') \stackrel{\text{def}}{=} \mathscr{C}\,[\![\mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1]\!]\,\sigma = \sigma'$$

infatti abbiamo

$$\begin{aligned}
\mathscr{C}\,[\![\mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1]\!]\,\sigma &= \mathscr{B}\,[\![b]\!]\,\sigma \to \mathscr{C}\,[\![c_0]\!]\,\sigma, \mathscr{C}\,[\![c_1]\!]\,\sigma \\
&= \mathbf{true} \to \sigma', \mathscr{C}\,[\![c_1]\!]\,\sigma \\
&= \sigma'
\end{aligned}$$

$$\frac{\langle b, \sigma \rangle \to \mathbf{false}}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma \rangle \to \sigma}$$

Assumiamo $\langle b, \sigma \rangle \to \mathbf{false}$ e percio' $\mathscr{B}\,[\![b]\!]\,\sigma = \mathbf{false}.$

Vogliamo provare

$$P(\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma \rangle \to \sigma) \stackrel{\text{def}}{=} \mathscr{C}\,[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!]\,\sigma = \sigma$$

Per la proprieta' della semantica denotazionale

$$\begin{aligned}
\mathscr{C}\,[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!]\,\sigma &= \mathscr{B}\,[\![b]\!]\,\sigma \to \mathscr{C}\,[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!]^{*}\,(\mathscr{C}\,[\![c]\!]\,\sigma), \sigma \\
&= \mathbf{false} \to \mathscr{C}\,[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!]^{*}\,(\mathscr{C}\,[\![c]\!]\,\sigma), \sigma \\
&= \sigma
\end{aligned}$$

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

Assumiamo

- $\langle b,\sigma\rangle \to \mathbf{true}$ e percio' $\mathscr{B}[\![b]\!]\,\sigma = \mathbf{true}$
- $P(\langle c,\sigma\rangle \to \sigma'') \stackrel{\text{def}}{=} \mathscr{C}[\![c]\!]\,\sigma = \sigma''$
- $P(\langle \mathbf{while}\ b\ \mathbf{do}\ c,\sigma''\rangle \to \sigma') \stackrel{\text{def}}{=} \mathscr{C}[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!]\,\sigma'' = \sigma'$

Vogliamo provare

$$P(\langle \mathbf{while}\ b\ \mathbf{do}\ c,\sigma\rangle \to \sigma') \stackrel{\text{def}}{=} \mathscr{C}[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!]\,\sigma = \sigma'$$

$$\begin{aligned}
\mathscr{C}[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!]\,\sigma &= \mathscr{B}[\![b]\!]\,\sigma \to \mathscr{C}[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!]^*\,(\mathscr{C}[\![c]\!]\,\sigma),\sigma \\
&= \mathbf{true} \to \mathscr{C}[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!]^*\,\sigma'',\sigma \\
&= \mathscr{C}[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!]^*\,\sigma'' \\
&= \mathscr{C}[\![\mathbf{while}\ b\ \mathbf{do}\ c]\!]\,\sigma'' \\
&= \sigma'
\end{aligned}$$

L’operatore di lifting puo’ essere rimosso $\sigma'' \neq \bot$.

Completezza

$$\forall c \in Com$$

$$P(c) \stackrel{\text{def}}{=} \forall \sigma, \sigma' \in \Sigma. \quad \mathscr{C}\,[\![c]\!]\,\sigma = \sigma' \quad \Rightarrow \quad \langle c, \sigma \rangle \to \sigma'$$

per induzione strutturale

Vogliamo provare $P(\mathbf{skip}) \stackrel{\text{def}}{=} \forall \sigma, \sigma'. \mathscr{C}[\![\mathbf{skip}]\!]\sigma = \sigma' \Rightarrow \langle \mathbf{skip}, \sigma \rangle \to \sigma'$

Assumiamo $\mathscr{C}[\![\mathbf{skip}]\!]\sigma = \sigma'$

Allora $\sigma' = \sigma$

per la regola (skip) $\langle \mathbf{skip}, \sigma \rangle \to \sigma \ = \sigma'$

Proviamo $P(x := a) \stackrel{\text{def}}{=} \forall \sigma, \sigma'. \mathscr{C}[\![x := a]\!]\sigma = \sigma' \Rightarrow \langle x := a, \sigma \rangle \to \sigma'$

Assumiamo $\mathscr{C}[\![x := a]\!]\sigma = \sigma'$

Allora $\sigma' = \sigma[^{\mathscr{A}[\![a]\!]\sigma}/_x]$

Per consistenza delle espressioni $\langle a, \sigma \rangle \to \mathscr{A}[\![a]\!]\sigma$

Per la regola (asgn) $\langle x := a, \sigma \rangle \to \sigma[^{\mathscr{A}[\![a]\!]\sigma}/_x] = \sigma'$

Assumiamo
$$P(c_0) \stackrel{\text{def}}{=} \forall \sigma, \sigma''.\ \mathscr{C}[\![c_0]\!]\,\sigma = \sigma'' \Rightarrow \langle c_0, \sigma\rangle \to \sigma''$$
$$P(c_1) \stackrel{\text{def}}{=} \forall \sigma'', \sigma'.\ \mathscr{C}[\![c_1]\!]\,\sigma'' = \sigma' \Rightarrow \langle c_1, \sigma''\rangle \to \sigma'$$

Vogliamo provare $P(c_0;c_1) \stackrel{\text{def}}{=} \forall \sigma, \sigma'.\ \mathscr{C}[\![c_0;c_1]\!]\,\sigma = \sigma' \Rightarrow \langle c_0;c_1, \sigma\rangle \to \sigma'$

Assumiamo $\mathscr{C}[\![c_0;c_1]\!]\,\sigma = \sigma'$

Abbiamo $\mathscr{C}[\![c_0;c_1]\!]\,\sigma = \mathscr{C}[\![c_1]\!]^*(\mathscr{C}[\![c_0]\!]\,\sigma) = \sigma' \neq \bot$

percio' $\mathscr{C}[\![c_0]\!]\,\sigma = \sigma''$ per qualche $\sigma'' \neq \bot$

e $\mathscr{C}[\![c_1]\!]\,\sigma'' = \sigma'$

per ipotesi induttiva $\langle c_0, \sigma\rangle \to \sigma''$ $\langle c_1, \sigma''\rangle \to \sigma'$

Per la regola (seq) $\langle c_0;c_1, \sigma\rangle \to \sigma'$

Assumiamo $P(c_0) \stackrel{\text{def}}{=} \forall \sigma, \sigma'. \, \mathscr{C}\,[\![c_0]\!]\,\sigma = \sigma' \Rightarrow \langle c_0, \sigma \rangle \to \sigma'$

$P(c_1) \stackrel{\text{def}}{=} \forall \sigma, \sigma'. \, \mathscr{C}\,[\![c_1]\!]\,\sigma = \sigma' \Rightarrow \langle c_1, \sigma \rangle \to \sigma'$

proviamo $P(\textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1) \stackrel{\text{def}}{=} \forall \sigma, \sigma'. \, \mathscr{C}\,[\![\textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1]\!]\,\sigma = \sigma' \Rightarrow \langle \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1, \sigma \rangle \to \sigma'$

Assumiamo $\mathscr{C}\,[\![\textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1]\!]\,\sigma = \sigma'$

abbiamo $\mathscr{C}\,[\![\textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1]\!]\,\sigma = \mathscr{B}\,[\![b]\!]\,\sigma \to \mathscr{C}\,[\![c_0]\!]\,\sigma, \mathscr{C}\,[\![c_1]\!]\,\sigma = \sigma'$

e $\mathscr{B}\,[\![b]\!]\,\sigma = \textbf{false}$ o $\mathscr{B}\,[\![b]\!]\,\sigma = \textbf{true}$

se $\mathscr{B}\,[\![b]\!]\,\sigma = \textbf{false}$ $\quad \mathscr{C}\,[\![\textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1]\!]\,\sigma = \mathscr{C}\,[\![c_1]\!]\,\sigma = \sigma'$

$\langle b, \sigma \rangle \to \textbf{false}$ per ipotesi induttiva $\langle c_1, \sigma \rangle \to \sigma'$

Per la regola (ifff) $\langle \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1, \sigma \rangle \to \sigma'$

se $\mathscr{B}\,[\![b]\!]\,\sigma = \textbf{true}$ $\quad \mathscr{C}\,[\![\textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1]\!]\,\sigma = \mathscr{C}\,[\![c_0]\!]\,\sigma = \sigma'$

$\langle b, \sigma \rangle \to \textbf{true}$ per ipotesi induttiva $\langle c_0, \sigma \rangle \to \sigma'$

Per la regola (iftt) $\langle \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1, \sigma \rangle \to \sigma'$

Assumiamo $P(c) \stackrel{\text{def}}{=} \forall \sigma, \sigma''.\, \mathscr{C}\llbracket c \rrbracket \sigma = \sigma'' \Rightarrow \langle c, \sigma \rangle \to \sigma''$

Dimostriamo $P(\textbf{while } b \textbf{ do } c) \stackrel{\text{def}}{=} \forall \sigma, \sigma'.\, \mathscr{C}\llbracket \textbf{while } b \textbf{ do } c \rrbracket \sigma = \sigma' \Rightarrow \langle \textbf{while } b \textbf{ do } c, \sigma \rangle \to \sigma'$

abbiamo $\mathscr{C}\llbracket \textbf{while } b \textbf{ do } c \rrbracket \sigma = \text{fix } \Gamma_{b,c}\, \sigma = \left(\bigsqcup_{n \in \mathbb{N}} \Gamma_{b,c}^{n} \bot \right) \sigma$

$$\mathscr{C}\llbracket \textbf{while } b \textbf{ do } c \rrbracket \sigma = \sigma' \Rightarrow \langle \textbf{while } b \textbf{ do } c, \sigma \rangle \to \sigma'$$

sse $\left(\bigsqcup_{n \in \mathbb{N}} \Gamma_{b,c}^{n} \bot \right) \sigma = \sigma' \Rightarrow \langle \textbf{while } b \textbf{ do } c, \sigma \rangle \to \sigma'$

sse $\left(\exists n \in \mathbb{N}.\, (\Gamma_{b,c}^{n} \bot) \sigma = \sigma' \right) \Rightarrow \langle \textbf{while } b \textbf{ do } c, \sigma \rangle \to \sigma'$

sse $\forall n \in \mathbb{N}.\, \left(\Gamma_{b,c}^{n} \bot \sigma = \sigma' \Rightarrow \langle \textbf{while } b \textbf{ do } c, \sigma \rangle \to \sigma' \right)$

definiamo $A(n) \stackrel{\text{def}}{=} \forall \sigma, \sigma'.\, \Gamma_{b,c}^{n} \bot \sigma = \sigma' \Rightarrow \langle \textbf{while } b \textbf{ do } c, \sigma \rangle \to \sigma'$

proviamo $\forall n \in \mathbb{N}.\, A(n)$ per induzione matematica

Assumiamo $P(c) \stackrel{\text{def}}{=} \forall \sigma, \sigma''. \mathscr{C}[\![c]\!]\sigma = \sigma'' \Rightarrow \langle c, \sigma \rangle \to \sigma''$

proviamo $\forall n \in \mathbb{N}. A(n) \stackrel{\text{def}}{=} \forall \sigma, \sigma'. \Gamma^n_{b,c} \bot \sigma = \sigma' \Rightarrow \langle \textbf{while } b \textbf{ do } c, \sigma \rangle \to \sigma'$

$A(0) \stackrel{\text{def}}{=} \forall \sigma, \sigma'. \Gamma^0_{b,c} \bot \sigma = \sigma' \Rightarrow \langle \textbf{while } b \textbf{ do } c, \sigma \rangle \to \sigma'$

$\Gamma^0_{b,c} \bot \sigma = \bot \sigma = \bot$

la premessa $\Gamma^0_{b,c} \bot \sigma = \sigma'$ e' falsa $\sigma' \neq \bot$

A(0) e' vero

Assumiamo $P(c) \stackrel{\text{def}}{=} \forall \sigma, \sigma''. \mathscr{C}[\![c]\!]\sigma = \sigma'' \Rightarrow \langle c, \sigma \rangle \to \sigma''$

proviamo $\forall n \in \mathbb{N}. A(n) \stackrel{\text{def}}{=} \forall \sigma, \sigma'. \Gamma_{b,c}^{n} \bot \sigma = \sigma' \Rightarrow \langle \textbf{while } b \textbf{ do } c, \sigma \rangle \to \sigma'$

assumiamo $A(n) \stackrel{\text{def}}{=} \forall \sigma, \sigma'. \Gamma_{b,c}^{n} \bot \sigma = \sigma' \Rightarrow \langle \textbf{while } b \textbf{ do } c, \sigma \rangle \to \sigma'$

proviamo $A(n+1) \stackrel{\text{def}}{=} \forall \sigma, \sigma'. \Gamma_{b,c}^{n+1} \bot \sigma = \sigma' \Rightarrow \langle \textbf{while } b \textbf{ do } c, \sigma \rangle \to \sigma'$

assumiamo $\Gamma_{b,c}^{n+1} \bot \sigma = \Gamma_{b,c} \left(\Gamma_{b,c}^{n} \bot \right) \sigma = \sigma' \neq \bot$

by def $\mathscr{B}[\![b]\!]\sigma \to \left(\Gamma_{b,c}^{n} \bot \right)^{*} (\mathscr{C}[\![c]\!]\sigma), \sigma = \sigma'$

if $\mathscr{B}[\![b]\!]\sigma = \textbf{false}$ $\langle b, \sigma \rangle \to \textbf{false}$ $\sigma = \sigma'$

per la regola (whff)

$\langle \textbf{while } b \textbf{ do } c, \sigma \rangle \to \sigma = \sigma'$

if $\mathscr{B}[\![b]\!]\sigma = \textbf{true}$ $\langle b, \sigma \rangle \to \textbf{true}$ $\left(\Gamma_{b,c}^{n} \bot \right)^{*} (\mathscr{C}[\![c]\!]\sigma) = \sigma' \neq \bot$

percio' $\mathscr{C}[\![c]\!]\sigma = \sigma''$ per qualche $\sigma'' \neq \bot$

$\langle c, \sigma \rangle \to \sigma''$

$\left(\Gamma_{b,c}^{n} \bot \right) \sigma'' = \sigma'$

$\langle \textbf{while } b \textbf{ do } c, \sigma'' \rangle \to \sigma'$

per la regola(whtt)

$\langle \textbf{while } b \textbf{ do } c, \sigma \rangle \to \sigma'$

Considerazioni finali

Comandi

Semantica operazionale Big-step	Semantica denotazionale
Terminazione ✗	(funzioni parziali)
Determinismo ✓	
Equivalenza operazionale	Equivalenza denotazionale e' una congruenza

Consistenza
(correttezza+ completezza)

Equivalenza operazionale = Equivalenza denotazionale
sono congruenze

induzione ben fondata	teorema di punto fisso di Kleene