Semantica operazionale

↳ vicina alle operazioni che vengono svolte, come se fosse una macchina astratta

↳ Utile per dimostrare equivalenza di programmi

Semantica denotazionale

↳ modella le operazioni del programma come una funzione

Si basa sulle funzioni sui calcoli di punto fisso

Semantica assiomatica

Definiamo — metavariabili per definire regole e tutto il resto

N interi - n, m

T = {true, false} - t

Loc x, y — metavariabili

Aexp a

Bexp b

Com c

$\langle a, \sigma \rangle \to n$

$\langle b, \sigma \rangle \to b$

Aexp $a ::= n \mid x \mid a_0 + a_1 \mid a_0 \times a_1 \mid a_0 - a_1$

$2 + 3 \times 4 + 5$

↳ Ha significati diversi in base alle policy

Bexp $b ::= true \mid false \mid a_0 == a_1 \mid a_0 < a_1 \mid \neg b \mid b_1 \vee b_2 \mid b_1 \wedge b_2$

Com $c ::= skip \mid x := a \mid c_0 ; c_1 \mid if\ b\ then\ c_1\ else\ c_2 \mid while\ b\ do\ c$

$\sigma \in \Sigma$ stati $\quad \sigma : Loc \to N \quad \sigma(x)$

Configurazione $\langle a, \sigma \rangle$

Evaluation $\langle a, \sigma \rangle \to n$

$\langle n, \sigma \rangle \to n$

$\langle x, \sigma \rangle \to \sigma(x)$

$$\frac{\langle a_0, \sigma \rangle \to n_0 \qquad \langle a_1, \sigma \rangle \to n_1}{\langle a_0 + a_1, \sigma \rangle \to n}$$

↳ sintattico posso indicarlo con qualsiasi simbolo

$n = n_0 + n_1$

↳ col significato di somma

$$\frac{\langle 2, \sigma \rangle \to 2 \qquad \langle 3, \sigma \rangle \to 3}{\langle 2 \times 3, \sigma \rangle \to 6}$$

$$\frac{\langle 2, \sigma \rangle \to 4 \qquad \langle 3, \sigma \rangle \to 7}{\langle 2 \times 3, \sigma \rangle \to 28}$$

NON è una derivazione poiché una regola falsa (gli assiomi non sono veri)

$$\frac{\langle int, \sigma_0 \rangle \to 0 \qquad \langle 5, \sigma_0 \rangle \to 5}{\langle int + 5, \sigma_0 \rangle \to 5} \qquad \frac{\langle 7, \sigma_0 \rangle \to 7 \qquad \langle 9, \sigma_0 \rangle \to 9}{\langle 7 + 9, \sigma_0 \rangle \to 16}$$

$$\frac{\langle int + 5, \sigma_0 \rangle \to 5 \qquad \langle 7 + 9, \sigma_0 \rangle \to 16}{\langle (int + 5) + (7 + 9), \sigma_0 \rangle \to 21}$$

equivalenti:

$a_0 \sim a_1 \quad \forall \sigma \in \Sigma \quad \forall n \in N$

$\langle a_0, \sigma \rangle \to n \iff \langle a_1, \sigma \rangle \to n$

Due espressioni sono equivalenti se il loro risultato è lo stesso valore in ogni stato

$\langle true, \sigma_0 \rangle \to true$

$\langle false, \sigma_0 \rangle \to false$

$$\frac{\langle b, \sigma \rangle \to true}{\langle \neg b, \sigma \rangle \to false} \qquad \frac{\langle b, \sigma \rangle \to false}{\langle \neg b, \sigma \rangle \to true}$$

$$\frac{\langle a_0, \sigma_0 \rangle \to n_0 \qquad \langle a_1, \sigma \rangle \to n_1}{\langle a_0 == a_1, \sigma \rangle \to true} \quad n_0 = n_1$$

$$\frac{\langle b_1, \sigma \rangle \to t_1 \qquad \langle b_2, \sigma \rangle \to t_2}{\langle b_1 \wedge b_2, \sigma \rangle \to t = t_1 \wedge t_2}$$

$b_1 \sim b_2 \iff \forall \sigma \in \Sigma \ \forall t \in \{true, false\}$

$\langle b_0, \sigma \rangle \to t \iff \langle b_1, \sigma \rangle \to t$

$$\sigma[m/x](y) = \begin{cases} \sigma(y) & y \neq x \\ m \end{cases}$$

$\langle skip, \sigma \rangle \to \sigma$

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

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

$$\frac{\langle b, \sigma \rangle \to true \qquad \langle c_1, \sigma \rangle \to \sigma'}{\langle if\ b\ then\ c_1\ else\ c_2, \sigma \rangle \to \sigma'}$$

$$\frac{\langle b, \sigma \rangle \to false \qquad \langle c_2, \sigma \rangle \to \sigma'}{\langle if\ b \ldots\ldots, \sigma \rangle \to \sigma'}$$

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

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

$c_1 \sim c_2$ iff $\forall \sigma, \sigma' \in \Sigma \quad \langle c_1, \sigma \rangle \to \sigma' \iff \langle c_2, \sigma \rangle \to \sigma'$

while b do c $\sim$ if b then c; while b do c else skip

$\forall \sigma, \sigma' \in \Sigma \quad \langle w, \sigma \rangle \to \sigma' \iff \langle$ if b then c; w else skip$, \sigma \rangle \to \sigma'$

($\Rightarrow$)

$$\frac{\langle b, \sigma \rangle \to \text{false}}{\langle w, \sigma \rangle \to \sigma} \; (P_1)$$

$$\frac{\langle b, \sigma \rangle \to \text{false} \qquad \langle \text{skip}, \sigma \rangle \to \sigma}{\langle \text{if } b \text{ then } c; w \text{ else skip}, \sigma \rangle \to \text{skip}} \; (P_2)$$

$$\frac{\langle b, \sigma \rangle \to \text{true} \qquad \langle c, \sigma \rangle \to \sigma'' \qquad \langle w, \sigma'' \rangle \to \sigma'}{\langle w, \sigma \rangle \to \sigma'} \; (P_3)$$

$$\frac{\langle b, \sigma \rangle \to \text{true} \qquad \dfrac{\langle c, \sigma \rangle \to \sigma'' \qquad \langle w, \sigma'' \rangle \to \sigma'}{\langle c; w, \sigma \rangle \to \sigma'}}{\langle \text{if } b \text{ then } c; w \text{ else skip}, \sigma \rangle \to \sigma'}$$

$$\frac{\langle b, \sigma \rangle \to \text{true} \qquad \langle c; w, \sigma \rangle \to \sigma'}{\langle \text{if } \ldots\ldots, \sigma \rangle \to \sigma'}$$

$$\frac{\langle b, \sigma \rangle \to \text{true} \qquad \langle c, \sigma \rangle \to \sigma'' \qquad \langle w, \sigma'' \rangle \to \sigma'}{\langle \text{while } b \text{ do } c, \sigma \rangle \to \sigma'}$$

$$\frac{\langle b, \sigma \rangle \to \text{false}}{\langle \text{if } \ldots\ldots, \sigma \rangle \to \sigma} \qquad \frac{\langle b, \sigma \rangle \to \text{false}}{\langle w, \sigma \rangle \to \sigma}$$

---

if b then c_1 else $c_2 \sim$ if $\neg b$ then c_2 else c_1

$\langle P_1, \sigma \rangle \to \sigma' \iff \langle P_2, \sigma \rangle \to \sigma'$

$$\frac{\langle b, \sigma \rangle \to \text{true} \qquad \langle c_1, \sigma \rangle \to \sigma'}{\langle \text{if } b \text{ then } c_1 \text{ else } c_2, \sigma \rangle \to \sigma'} \iff \frac{\langle b, \sigma \rangle \to \text{true} \qquad \dfrac{\langle \neg b, \sigma \rangle \to \text{false} \qquad \langle c_1, \sigma \rangle \to \sigma'}{\langle \text{if } \neg b \text{ then } c_2 \text{ else } c_1, \sigma \rangle \to \sigma'}}{}$$

$$\frac{\langle b, \sigma \rangle \to \text{false} \qquad \langle c_2, \sigma \rangle \to \sigma'}{\langle \text{if } b \text{ then } c_1 \text{ else } c_2, \sigma \rangle \to \sigma'} \iff \frac{\langle b, \sigma \rangle \to \text{false} \qquad \dfrac{\langle \neg b, \sigma \rangle \to \text{true} \qquad \langle c_2, \sigma \rangle \to \sigma'}{\langle \text{if } \neg b \text{ then } c_2 \text{ else } c_1, \sigma \rangle \to \sigma'}}{}$$

---

if b then $c_1; c$ else $c_2; c \sim$ if b then c_1 else $c_2; c$

$$\frac{\langle b, \sigma \rangle \to \text{true} \qquad \dfrac{\langle c_1, \sigma \rangle \to \sigma'' \qquad \langle c, \sigma'' \rangle \to \sigma'}{\langle c_1; c, \sigma \rangle \to \sigma'}}{\langle \text{if } b \text{ then } c_1 \text{ else } c_2; c, \sigma \rangle \to \sigma'} \iff \frac{\langle b, \sigma \rangle \to \text{true} \qquad \langle c_1, \sigma \rangle \to \sigma''}{\langle \text{if } \neg b \text{ then } c_2 \text{ else } c_1, \sigma \rangle \to \sigma''} \qquad \frac{}{\langle c, \sigma'' \rangle \to \sigma'}}{\langle \text{if } b \text{ then } c_1 \text{ else } c_2; c, \sigma \rangle \to \sigma'}$$

Esercizi svolto da ado in classe

Corretto

$$\frac{\langle b, \sigma \rangle \to \text{false} \qquad \dfrac{\langle c_2, \sigma \rangle \to \sigma'' \qquad \langle c, \sigma'' \rangle \to \sigma'}{\langle c_2; c, \sigma \rangle \to \sigma'}}{\langle \text{if } b \text{ then } c_1 \text{ else } c_2, \sigma \rangle \to \sigma'} \iff \frac{\langle b, \sigma \rangle \to \text{false} \qquad \langle c_2, \sigma \rangle \to \sigma''}{\langle \text{if } \neg b \text{ then } c_2 \text{ else } c_1, \sigma \rangle \to \sigma''} \qquad \frac{}{\langle c, \sigma'' \rangle \to \sigma'}}{\langle \text{if } b \text{ then } c_1 \text{ else } c_2; c, \sigma \rangle \to \sigma'}$$

Correzione

$$\frac{\langle b, \sigma \rangle \to \text{true} \qquad \dfrac{\langle c_1, \sigma \rangle \to \sigma'' \qquad \langle c, \sigma'' \rangle \to \sigma'}{\langle c_1; c, \sigma \rangle \to \sigma'}}{\langle \text{if } b \text{ then } c_1; c \text{ else } c_2; c \rangle \to \sigma'} \Rightarrow \frac{\langle b, \sigma \rangle \to \text{true} \qquad \langle c_1, \sigma \rangle \to \sigma''}{\langle \text{if } b \text{ then } c_1 \text{ else } c_2, \sigma \rangle \to \sigma'} \qquad \frac{}{\langle c, \sigma'' \rangle \to \sigma'}}{\text{if } b \text{ then } c_1 \text{ else } c_2; c, \sigma \to \sigma'}$$

Identico

c_3; if b then c_1 else $c_2 \overset{?}{\sim}$ if b then $c_3; c_1$ else $c_3; c_2$

$$\frac{\langle c_1, \sigma \rangle \to \sigma'' \qquad \dfrac{\langle b, \sigma'' \rangle \to \text{true} \qquad \langle c_1, \sigma'' \rangle \to \sigma'}{\langle \text{if } b \text{ then } c_1 \text{ else } c_2, \sigma'' \rangle \to \sigma'}}{\langle c_3; \text{if } b \text{ then } c_1 \text{ else } c_2, \sigma \rangle \to \sigma'} \iff \frac{\langle b, \sigma \rangle \to \text{true} \qquad \dfrac{\langle c_1, \sigma \rangle \to \sigma'' \qquad \langle c_1, \sigma'' \rangle \to \sigma'}{\langle c_1 c_1, \sigma \rangle \to \sigma'}}{\langle \text{if } b \text{ then } c_3 c_1 \text{ else } c_3 c_2, \sigma \rangle \to \sigma'}$$

In generale NON è equivalente

Ma b è con una condizione

Ho bisogno che b valuti true sia prima che dopo l'esecuzione di c

$\langle b, \sigma \rangle \to \text{true} \iff \langle b, \sigma'' \rangle \to \text{true}$

$$\frac{\langle c_1, \sigma \rangle \to \sigma'' \qquad \dfrac{\langle b, \sigma'' \rangle \to \text{false} \qquad \langle c_2, \sigma'' \rangle \to \sigma'}{\langle \text{if } b \text{ then } c_1 \text{ else } c_2, \sigma'' \rangle \to \sigma'}}{\langle c_3; \text{if } b \text{ then } c_1 \text{ else } c_2, \sigma \rangle \to \sigma'} \iff \frac{\langle b, \sigma \rangle \to \text{false} \qquad \dfrac{\langle c_1, \sigma \rangle \to \sigma'' \qquad \langle c_2, \sigma'' \rangle \to \sigma'}{\langle c_1 c_2, \sigma \rangle \to \sigma'}}{\langle \text{if } b \text{ then } c_3 c_1 \text{ else } c_3 c_2, \sigma \rangle \to \sigma'}$$

$\parallel$ (IDEM)

p := 5 * 3
n := 0

p := 0

n := 3

while n > 0
  p = p+5
  n = n-1

$$\frac{\langle 5,\sigma\rangle \to 5 \quad \langle 3,\sigma\rangle \to 3}{\langle p:=5*3\rangle \to \sigma[15/p]} \qquad \langle n:=0,\sigma[15/p]\rangle \to \sigma[15/p][0/n]$$

$$\langle p:=5*3;\ n:=0,\sigma\rangle \to \sigma[15/p][0/n]$$

STEP

$$\langle n>0 \dots\dots\rangle \to T \qquad \langle \text{corpo}\rangle \to \sigma[10/p][1/n]$$

$$\langle \text{while} \dots\dots, \sigma[10/p][1/n]\rangle \to \sigma[15/p][0/n]$$

$$\langle n>0, \sigma[\dots]\rangle \to T \qquad \langle p:=p+5,\ n=n-1, \sigma[5/p][2/n]\rangle \to \sigma[10/p][1/n]$$

$$\langle \text{while} \dots\dots, \sigma[5/p][2/n]\rangle \to \sigma[15/p][0/n]$$

back propagation

STEP

$$\frac{\langle 0,\sigma\rangle \to \sigma}{\langle p:=0,\sigma\rangle \to \sigma[0/p]} \qquad \frac{\langle 3,\sigma\rangle \to 3}{\langle n:=3,\sigma[0/p]\rangle \to \sigma[0/p][3/n]}$$

$$\langle p:=0,\ n:=3,\sigma\rangle \to \sigma[0/p][3/n]$$

$$\frac{\langle p:=\sigma(0,3) \to \sigma[5/p][3/n] \qquad \langle n:=n-1,\sigma[5/p][3/n]\rangle \to \sigma[5/p][2/n]}{\langle n,\sigma,\sigma[0/p][3/n]\rangle \to \text{True} \qquad \langle p:=p+5;\ n:=n-1,\sigma[0/p][3/n]\rangle \to \sigma[5/p][2/n]}$$

$$\langle \text{while } n>0 \text{ do } p:=p+5,\ n:=n-1, \sigma[0/p][3/n]\rangle \to \sigma[15/p][0/n]$$

back propagation

$$\langle p:=0;\ n:=3;\ \text{while } n>0 \text{ do } p:=p+5;\ n=n-1;\ \sigma\rangle \to$$

Lezione 2

Semantica denotazionale → formalizza il calcolo del programma in funzioni

$\forall a \in Aexp$

$\langle a,\sigma\rangle \to m$

$\langle a,\sigma\rangle \to m'$

$\Rightarrow m = m'$ questo è il determinismo

$a := n \mid x \mid a_0 + a_1 \mid a_0 \times a_1 \mid a_0 - a_1$

dimostro P(n) $\quad b = true \mid false \mid a_0 == a_1$

dimostro P(x)

Se $P(a_0), P(a_1) \Rightarrow P(a_0 + a_1)$ (ipotesi induttiva)

$$\frac{\langle n,\sigma\rangle \to m'}{\langle n,\sigma\rangle \to m} \quad m = m' = n$$

$$\frac{\langle X,\sigma\rangle \to m}{\langle X,\sigma\rangle \to m'} \quad m = m' = \sigma(x)$$

assumiamo $P(a_0)$ e $P(a_1)$

$$\langle a_0,\sigma\rangle \to m_0 \quad \langle a_0,\sigma\rangle \to m_0' \Rightarrow m_0 = m_0'$$

$$\langle a_1,\sigma\rangle \to m_1 \quad \langle a_1,\sigma\rangle \to m_1' \Rightarrow m_1 = m_1'$$

$$\frac{\langle a_0,\sigma\rangle \to m_0 \qquad \langle a_1,\sigma\rangle \to m_1}{\langle a_0 + a_1,\sigma\rangle \to m} \quad m = m_0 + m_1$$

$$\frac{\langle a_0,\sigma\rangle \to m_0' \qquad \langle a_1,\sigma\rangle \to m_1'}{\langle a_0 + a_1,\sigma\rangle \to m'} \quad m' = m_0' + m_1'$$

Relazione ben fondata

$A \quad < \quad \leq \quad A \times A$

$a < b$ $\quad a \not< b$ $\quad \leq$

predecessore $a_n \longleftarrow \dots \longleftarrow a_2 < a_1 < a_0$

Dimostrare $\forall a \in A\ P(a) \iff \forall a \in A.\ (\forall b < a.\ P(b) \Rightarrow P(a))$

Euclid

while $(\neg(M=N))$ do
  if $M < N$
    then $N = N - M$
    else $M = M - N$

vogliamo dimostrare determino

$\sigma(N) \geq 1 \quad \sigma(N) \geq 1 \Rightarrow \forall b$

$P\ [\langle Euclid,\sigma\rangle \to \sigma']$

$\forall \sigma \in S = \{\sigma \in \Sigma \mid \sigma(N) \geq 1, \sigma(N) \geq 1\}$ vale $P(\sigma)$

$\sigma' < \sigma \iff (\sigma'(M) \leq \sigma(M)$ AND $\sigma'(N) \leq \sigma(N)$ AND $(\sigma'(M) \neq \sigma(M)$ OR $\sigma'(N) \neq \sigma(N))$

sia $\sigma \in S$ supponiamo che $\forall \sigma' \in S: \sigma' < \sigma$ vale $P(\sigma')$ $\Rightarrow P(\sigma)$

- $\sigma(M) = \sigma(N)$

$$\frac{\langle \neg(M=N),\sigma\rangle \to false}{\langle Euclid,\sigma\rangle \to \sigma}$$

Se vale

$$\frac{\langle \neg(M=N),\sigma\rangle \to true}{\langle Euclid,\sigma\rangle \to \sigma'}$$

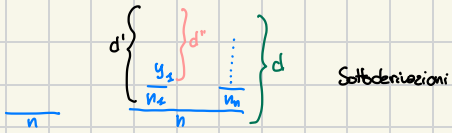
Svolgo

$\langle if \dots\dots,\sigma\rangle \to \sigma'', \langle Euclid,\sigma''\rangle \to \sigma'$

- $\sigma(M) \neq \sigma(N)$ $\quad \langle if\ M < N\ do\ N = N - M\ else\ M = M - N, \sigma\rangle \to \sigma''$

$$\sigma'' = \begin{cases} \sigma[\sigma(N) - \sigma(M)/N] & \text{se } \sigma(M) < \sigma(N) \\ \sigma[\sigma(M) - \sigma(N)/M] & \text{se } \sigma(N) < \sigma(M) \end{cases}$$

$\sigma'' < \sigma$ poiché sostituisco M o N con valori più piccoli



Sottoderivazioni

$d' < d$

R istanza di regole $\frac{x}{y}$ (premesse / oggetti derivati) $\frac{\phi}{y}$ $\frac{d_1 \dots d_n}{y}$ (d_i è derivazione di n') $\frac{n_1 \dots n_n}{y} \in R$

$x \subseteq R$

$\vdash_R y \quad \vdash \langle c, \sigma \rangle \to \sigma'$

$\forall d$ [$\langle c, \sigma_0 \rangle \to \sigma_1$, $\langle c, \sigma_0 \rangle \to \sigma$ $\Rightarrow \sigma_1 = \sigma$] $P(d)$

$\forall d' < d.\ P(d') \Rightarrow P(d)$

- $c \equiv skip$ $\langle skip, \sigma_0 \rangle \to \sigma_0$

  $\sigma_0 = \sigma_1 = \sigma$

- $C \equiv X := a$ $\dfrac{\langle a, \sigma_0 \rangle \to m_1}{\langle x := a, \sigma_0 \rangle \to \sigma_0[m_1/x]}$ $\dfrac{\langle a, \sigma_0 \rangle \to m_2}{\langle x := a, \sigma_0 \rangle \to \sigma_0[m_2/x]}$

- $C \equiv c_0 ; c_1$ devono raggiungere lo stesso stato

$$\frac{\langle c_0, \sigma \rangle \to \sigma_1' \quad \langle c_1, \sigma_1' \rangle \to \sigma_1}{\langle c_0 ; c_1, \sigma \rangle \to \sigma_1} \qquad \sigma_1' = \sigma_2' \qquad \frac{\langle c_0, \sigma \rangle \to \sigma_2' \quad \langle c_1, \sigma_2' \rangle \to \sigma_2}{\langle c_0 ; c_1, \sigma \rangle \to \sigma_2}$$

- $C \equiv$ if b then c_1 else c_2

$$\frac{\langle b, \sigma \rangle \to true \quad \langle c_1, \sigma \rangle \to \sigma_2}{\langle \text{if } b \text{ then } c_1 \text{ else } c_2, \sigma \rangle \to \sigma_2} \qquad \frac{\langle b, \sigma \rangle \to true \quad \langle c_1, \sigma \rangle \to \sigma''}{\langle \text{if } b \text{ then } c_1 \text{ else } c_2, \sigma \rangle \to \sigma''}$$

- $C \equiv$ while b do c

$$\frac{\langle b, \sigma \rangle \to true \quad \langle c, \sigma \rangle \to \sigma' \quad \langle \text{while } b \text{ do } c, \sigma'' \rangle \to \sigma'}{\langle \text{while } b \text{ do } c, \sigma \rangle \to \sigma'} \qquad \frac{\langle b, \sigma \rangle \to true \quad \langle c, \sigma \rangle \to \sigma''' \quad \langle \text{while } b \text{ do } c, \sigma''' \rangle \to \sigma^{IV}}{\langle \text{while } b \text{ do } c, \sigma \rangle \to \sigma^{IV}}$$

R $I_R = \{x \mid \vdash_R x\}$

$\forall x \in I_R.\ P(x) \iff \frac{x}{y} \in R \quad X \subseteq I_R$

$I_R \subseteq Q$ $\quad (\forall x \in X.\ P(x)) \Rightarrow P(y)$

Q è

R-chiuso $\forall x/y \in R \quad X \subseteq Q \Rightarrow y \in Q$

$Q = \{x \in I_R \mid P(x)\}$ $\quad \forall n \in X.\ n \in I_R \wedge P(n) \Rightarrow y \in Q$

$Q \subseteq I_R \quad I_R \subseteq Q$

$\hat{R}(B) = \{y \mid \exists x \subseteq B.\ (x/y) \in R\}$

B è R chiuso $\hat{R}(B) \subseteq B$

$A \subseteq B \Rightarrow \hat{R}(A) \subseteq \hat{R}(B)$

$A_0 = \hat{R}^0 = \phi$

$A_1 = \hat{R}^1(\phi) = \hat{R}(\phi)$ = assiomi

$A_2 = R^2(\phi) = \hat{R}(\hat{R}(\phi))$ = deriva ciò che ha come ipotesi gli assiomi

$A_0 = \phi \subseteq A_1 \qquad A_\omega = \bigcup_{n \in \omega} A_n$

$\hat{R}(A_0) \subseteq \hat{R}(A_1)$

$A_1 \subseteq A_2$

$A = \bigcup_{n \in \omega} A_n = I_R$

A é R-chiuso

$\hat{R}(A) = A$ fixpoint

A é least R-closed set

A é R-chiuso $x/y \in R \quad X \subseteq A \Rightarrow y \in A$

$x/y \in R \quad X \subseteq A$

$X \subseteq A_n \quad y \in \hat{R}(A_n) \subseteq A$

$\hat{R}(A) = A \supseteq \hat{R}(A) \subseteq A$ poiché A è R-chiuso

$y \in A \quad y \in A_n \quad y \in \hat{R}(A_{n-1})$

$X/y \in R \; X \subseteq A_{n-1} \subseteq A$

$X \subseteq A \quad X/y \in R \Rightarrow y \in \hat{R}(A)$

B é R-chiuso $A \subseteq B$

$\hat{R}(B) \subseteq B$ $\quad A_0 \subseteq B$

$A_n \subseteq B \quad A_{n+1} = \hat{R}(A_n) \subseteq \hat{R}(B) \subseteq B$ ($\hat{R}$ monotono; B è R chiuso)

$$fix(\hat{R}) = \bigcup_{n \in \omega} \hat{R}^n(\phi)$$

partial order

$(P, \sqsubseteq)$

riflessiva: $\forall p \in P \quad p \sqsubseteq p$

transitiva $\forall p,q,r \in P \quad p \sqsubseteq q \quad q \sqsubseteq r \Rightarrow q \sqsubseteq r$

antisimmetrica $\forall p,q \in P \quad p \sqsubseteq q$ e $q \sqsubseteq p \Rightarrow q = p$

p è upper bound $X \subseteq P \; \forall q \in X \; q \sqsubseteq p$

p least upper bound $X \subseteq P$ $\forall r$ ubd$x$ $p \sqsubseteq r$

partial order è completo

$\forall \; p_0 \sqsubseteq p_1 \sqsubseteq \ldots$

$\bigsqcup \{p_0, p_1, \ldots\} \in P$

$\bot_P$

...

Continua

$\bigcup_{n \in \omega} \hat{R}(B_n) = \hat{R}(\bigcup_{n \in \omega} B_n)$

$f : D \to E$

monotona $d \sqsubseteq d' \Rightarrow f(d) \sqsubseteq f(d')$

continua $\forall \; d_0 \sqsubseteq d_1 \sqsubseteq \ldots \quad \bigsqcup_{n \in \omega} f(d_n) = f(\bigsqcup_{n \in \omega} d_n)$

$f : D \to D$ D è cpo con $\bot_D$

e f è continua

$$fix(f) = \bigsqcup_{n \in \omega} f^n(\bot_D)$$

Lezione 3

Semantica denotazionale

È come una funzione parziale sugli stati:

$c_0 \sim c_1 \quad \forall \sigma, \sigma' \in \Sigma \quad \langle c_0, \sigma \rangle \to \sigma' \iff \langle c_1, \sigma \rangle \to \sigma'$

$$\{(\sigma,\sigma') \mid \langle c_0,\sigma\rangle \to \sigma'\} = \{(\sigma,\sigma') \mid \langle c_1,\sigma\rangle \to \sigma'\}$$

$\mathcal{A} : Aexp \to (\Sigma \to \mathbb{N})$ $\quad \mathcal{A}[\![a]\!]\sigma = n \quad (\sigma,n) \in \mathcal{A}[\![a]\!]$

$\mathcal{B} : Bexp \to (\Sigma \to \{true, false\})$ $\quad \mathcal{B}[\![b]\!]\sigma = t \quad (\sigma,t) \in \mathcal{B}[\![b]\!]$

$\mathcal{C} : Com \to (\Sigma \to \Sigma)$ $\quad C[\![c]\!]\sigma = \sigma' \quad \langle \sigma,\sigma' \rangle \in \mathcal{C}[\![c]\!]$

Aexp $a ::= n \mid x \mid a_0 + a_1 \mid a_0 - a_1 \mid a_0 \times a_1$

$\mathcal{A}[\![n]\!] = \{(\sigma, n) \mid \sigma \in \Sigma\}$

$\mathcal{A}[\![n]\!] = \{(\sigma, \sigma(x)) \mid \sigma \in \Sigma\}$

$\mathcal{A}[\![a_0 + a_1]\!] = \{(\sigma, n_0 + n_1) \mid (\sigma, n_0) \in \mathcal{A}[\![a_0]\!], (\sigma, n_1) \in \mathcal{A}[\![a_1]\!], \sigma \in \Sigma\}$

Bexp $b = true \mid false \mid a_0 = a_1 \mid a_0 \le a_1 \mid \neg b_1 \mid b_1 \wedge b_2 \mid b_1 \vee b_2$

$\mathcal{B}[\![true]\!] = \{(\sigma, true) \mid \forall \sigma \in \Sigma\}$

$\mathcal{B}[\![false]\!] = \{(\sigma, false) \mid \forall \sigma \in \Sigma\}$

$\mathcal{B}[\![a_0 = a_1]\!] = \{(\sigma, true) \mid \mathcal{A}[\![a_0]\!]\sigma = \mathcal{A}[\![a_1]\!]\sigma, \sigma \in \Sigma\} \cup \{(\sigma, false) \mid \mathcal{A}[\![a_0]\!]\sigma \neq \mathcal{A}[\![a_1]\!]\sigma, \sigma \in \Sigma\}$

$\mathcal{B}[\![\neg b]\!] = \{(\sigma, \neg t) \mid \mathcal{B}[\![b]\!]\sigma = t, \sigma \in \Sigma, (\sigma,t) \in \mathcal{B}[\![b]\!]\}$

$\mathcal{B}[\![b_1 \wedge b_2]\!] = \{(\sigma, t_0 \wedge t_1) \mid (\sigma, t_0) \in \mathcal{B}[\![b_1]\!], (\sigma, t_1) \in \mathcal{B}[\![b_1]\!], \sigma \in \Sigma\}$

Com $c ::= skip \mid x := a \mid c_0 ; c_1 \mid$ if b then c_0 else $c_1 \mid$ while b do c_0

$\mathcal{C}[\![skip]\!] = \{(\sigma,\sigma) \mid \sigma \in \Sigma\}$

$\mathcal{C}[\![x := a]\!] = \{(\sigma, \sigma[^{n}/_{x}]) \mid n = \mathcal{A}[\![a]\!]\sigma, \sigma \in \Sigma\}$

$\mathcal{C}[\![c_0 ; c_1]\!] = \mathcal{C}[\![c_1]\!] \circ \mathcal{C}[\![c_0]\!]$

$\mathcal{C}[\![$ if b then c_0 else $c_1]\!] = \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = true, (\sigma,\sigma') \in \mathcal{C}[\![c_0]\!]\} \cup \{(\sigma,\sigma) \mid \mathcal{B}[\![b]\!] = false, (\sigma,\sigma') \in \mathcal{C}[\![c_1]\!]\}$

while b do $c \equiv$ if b then c; w else skip (w)

$\mathcal{C}[\![$ while b do $c]\!] = \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = true, (\sigma,\sigma') \in \mathcal{C}[\![c;w]\!]\} \cup \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = false\}$

$= \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = true, (\sigma,\sigma') \in \mathcal{C}[\![w]\!] = \mathcal{C}[\![c]\!]\} \cup \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = false\}$

$\Gamma(\varphi) = \{(\sigma,\sigma') \mid \beta(\sigma) = true, (\sigma,\sigma') \in \varphi \circ \gamma\} \cup \{(\sigma,\sigma) \mid \beta(\sigma) = false\}$

$= \{(\sigma,\sigma') \mid \beta(\sigma) = true, (\sigma,\sigma'') \in \gamma, (\sigma'',\sigma') \in \varphi\} \cup \{(\sigma,\sigma) \mid \beta(\sigma) = false\}$

$\hat{R}$

$R = \{(\{(\sigma'',\sigma')\}/(\sigma,\sigma')) \mid \beta(\sigma) = true, (\sigma,\sigma'') \in \gamma\} \cup \{\phi/(\sigma,\sigma) \mid \beta(\sigma) = false\}$

$\varphi = fix\, \hat{R} = \Gamma(\varphi)$

$\mathcal{C}[\![$ while b do $c]\!] = fix\, \Gamma$

$\Gamma(\varphi) = \{(\sigma,\sigma') \mid \beta[\![b]\!]\sigma = true, (\sigma,\sigma) \in \varphi \circ \mathcal{C}[\![c]\!]\} \cup \{(\sigma,\sigma) \mid \beta[\![b]\!]\sigma = false\}$

$\Gamma(\varphi) = \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = true,\ (\sigma,\sigma') \in \varphi \circ \mathcal{C}[\![c]\!]\} \cup \{(\sigma,\sigma) \mid \mathcal{B}[\![b]\!]\sigma = false\}$

$\mathcal{C}[\![\text{while } b \text{ do } c]\!] = \Gamma(\mathcal{C}[\![w]\!])$

$= \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = true,\ (\sigma,\sigma') \in \mathcal{C}[\![w]\!] \circ \mathcal{C}[\![c]\!]\}$
$\cup \{(\sigma,\sigma) \mid \mathcal{B}[\![b]\!]\sigma = false\}$

$= \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = true,\ (\sigma,\sigma') \in \mathcal{C}[\![c;w]\!]\}$
$\cup \{(\sigma,\sigma) \mid \mathcal{B}[\![b]\!]\sigma = false,\ (\sigma,\sigma') \in \mathcal{C}[\![skip]\!]\}$

$= \mathcal{C}[\![\text{if } b \text{ then } c; w \text{ else skip}]\!]$

$\forall a \in AExp \quad \mathcal{A}[\![a]\!] = \{(\sigma,n) \mid \langle a,\sigma\rangle \to n\}$

$a = n$

$(\sigma,m) \in \mathcal{A}[\![n]\!] \iff m = n \quad \sigma \in \Sigma$

$\langle \sigma, n\rangle \to m \quad m = n$

$a = x \quad (\sigma,n) \in \mathcal{A}[\![x]\!] \iff \sigma(x) = n \quad \sigma \in \Sigma$

$\iff \langle x,\sigma\rangle \to n = \sigma(x)$

$P(a_0)\ P(a_1)$

$a = a_0 + a_1$

$(\sigma,n) \in \mathcal{A}[\![a_0 + a_1]\!] \iff n_0 + n_1 \quad (\sigma,n_0) \in \mathcal{A}[\![a_0]\!] \quad (\sigma,n_1) \in \mathcal{A}[\![n_1]\!] \quad \sigma \in \Sigma$

$$\langle a_0 + a_1, \sigma\rangle \to n \iff \frac{\langle a_0,\sigma\rangle \to n_0 \qquad \langle a_1,\sigma\rangle \to n_1}{\langle a_0 + a_1,\sigma\rangle \to n = n_0 + n_1}$$

$\forall b \in Bexp \quad \mathcal{B}[\![b]\!] = \{(\sigma,t) \mid \langle b,\sigma\rangle \to t\}$

$b = true \quad (\sigma,true) \in \mathcal{B}[\![b]\!] \ \forall \sigma \qquad \langle true,\sigma\rangle \to true \ \forall \sigma$

$b = a_0 = a_1 \quad \mathcal{B}[\![a_0 = a_1]\!] = \{(\sigma,true) \mid \mathcal{A}[\![a_0]\!]\sigma = \mathcal{A}[\![a_1]\!]\sigma\} \cup$
$\{(\sigma,false) \mid \mathcal{A}[\![a_0]\!]\sigma \neq \mathcal{A}[\![a_1]\!]\sigma\}$

$(\sigma,true) \in \mathcal{B}[\![a_0 = a_1]\!] \iff \mathcal{A}[\![a_0]\!]\sigma = \mathcal{A}[\![a_1]\!]\sigma$

$$\frac{\langle a_0,\sigma\rangle \to n_0 \quad \langle a_1,\sigma\rangle \to n_1 \quad n_0 = n_1}{\langle a_0 = a_1,\sigma\rangle \to true}$$

$(\sigma,false) \in \mathcal{B}[\![a_0 = a_1]\!]$

$b = b_1 \wedge b_2$ Assumiamo

$P(b_1)\ P(b_2)$

$(\sigma,t) \in \mathcal{B}[\![b_1 \wedge b_2]\!] \iff t = t_1 \wedge t_2 \qquad (\sigma,t_2) \in \mathcal{B}[\![b_1]\!] \quad (\sigma,t_2) \in \mathcal{B}[\![b_2]\!] \quad \sigma \in \Sigma$

$$\frac{\langle \sigma, b_1\rangle \to t_1 \qquad \langle \sigma, b_2\rangle \to t_2 \qquad t = t_1 \wedge t_2}{\langle b_1 \wedge b_2, \sigma\rangle \to t}$$

$\forall c \in Com \quad \mathcal{C}[\![c]\!] = \{(\sigma,\sigma') \mid \langle c,\sigma\rangle \to \sigma'\}$

$\langle c,\sigma\rangle \to \sigma' \Rightarrow (\sigma,\sigma') \in \mathcal{C}[\![c]\!]$

$c \equiv skip \quad \langle skip,\sigma\rangle \to \sigma \Rightarrow (\sigma,\sigma) \in \mathcal{C}[\![skip]\!]$

$c \equiv x := a \quad \dfrac{\langle a,\sigma\rangle \to n}{\langle x := a,\sigma\rangle \to \sigma[n/x]}$

$(\sigma,n) \in \mathcal{A}[\![a]\!]$

$\mathcal{C}[\![x:a]\!] = \{(\sigma,\sigma[n/x]) \mid (\sigma,n) \in \mathcal{A}[\![a]\!]\}$

$\Rightarrow (\sigma,\sigma[n/x]) \in \mathcal{C}[\![x := a]\!]$

$c \equiv c_0;c_1 \quad \dfrac{\langle c_0,\sigma\rangle \to \sigma'' \quad \langle c_1,\sigma''\rangle \to \sigma'}{\langle c_0;c_1,\sigma\rangle \to \sigma'}$ $\quad (\sigma,\sigma'') \in \mathcal{C}[\![c_0]\!]$ $\quad (\sigma'',\sigma') \in \mathcal{C}[\![c_1]\!]$ (per ipotesi induttiva)

$$\begin{aligned}\mathcal{C}[\![c_0;c_1]\!] &= \mathcal{C}[\![c_1]\!] \circ \mathcal{C}[\![c_0]\!] \\ &= \mathcal{C}[\![c_1]\!](\{\sigma'' \mid (\sigma,\sigma'') \in \mathcal{C}[\![c_0]\!]\}) \\ &= (\{(\sigma,\sigma') \mid (\sigma,\sigma'') \in \mathcal{C}[\![c_0]\!] \\ &\qquad (\sigma'',\sigma') \in \mathcal{C}[\![c_1]\!]\}\end{aligned}$$

Stiamo dimostrando
$\langle c,\sigma\rangle \to \sigma' \Rightarrow (\sigma,\sigma') \in \mathcal{C}[\![c]\!]$

$c \equiv$ if b then c_1 else c_2

$\dfrac{\langle b,\sigma\rangle \to true \quad \langle c_1,\sigma\rangle \to \sigma'}{\langle \text{if } b \text{ then } c_1 \text{ else } c_2,\sigma\rangle \to \sigma'}$

$(\sigma,true) \in \mathcal{B}[\![b]\!]$
$(\sigma,\sigma') \in \mathcal{C}[\![c_1]\!]$

$$\begin{aligned}\mathcal{C}[\![\text{if } b \text{ then } c_1 \text{ else } c_2]\!] &= \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = true, (\sigma,\sigma') \in \mathcal{C}[\![c_1]\!]\} \\ &\cup \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = false, (\sigma,\sigma') \in \mathcal{C}[\![c_2]\!]\} \\ &\Rightarrow (\sigma,\sigma') \in \mathcal{C}[\![\text{if } b \text{ then } c_1 \text{ else } c_2]\!]\end{aligned}$$

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

$\dfrac{\langle b,\sigma\rangle \to true \quad \langle c,\sigma\rangle \to \sigma'' \quad \langle w,\sigma''\rangle \to \sigma'}{\langle \text{while } b \text{ do } c,\sigma\rangle \to \sigma'}$

$\mathcal{B}[\![b]\!]\sigma = true$
$(\sigma,\sigma'') \in \mathcal{C}[\![c]\!] \quad (\sigma'',\sigma') \in \mathcal{C}[\![w]\!]$
$\mathcal{C}[\![w]\!]\sigma = \mathcal{C}[\![c;w]\!] = \mathcal{C}[\![w]\!](\mathcal{C}[\![c]\!]\sigma) = \mathcal{C}[\![w]\!],\sigma'' = \sigma'$
$(\sigma,\sigma') \in \mathcal{C}[\![w]\!]$

$$\begin{aligned}\mathcal{C}[\![w]\!] = \{&(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = true, (\sigma,\sigma') \in \mathcal{C}[\![c;w]\!]\} \\ &\cup \{(\sigma,\sigma) \mid \mathcal{B}[\![b]\!]\sigma = false\}\end{aligned}$$

Ora Stiamo dimostrando
$\langle c,\sigma\rangle \to \sigma' \Leftarrow (\sigma,\sigma') \in \mathcal{C}[\![c]\!]$

skip $\quad \mathcal{C}[\![skip]\!] = \{(\sigma,\sigma) \mid \sigma \in \Sigma\} \quad \langle skip,\sigma\rangle \to \sigma$

$x := a \quad (\sigma,\sigma') \in \mathcal{C}[\![x := a]\!] \iff \sigma' = \sigma[n/x] \quad (\sigma,n) \in \mathcal{A}[\![a]\!]$

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

$c_0;c_1 \quad (\sigma,\sigma') \in \mathcal{C}[\![c_0;c_1]\!]$
$(\sigma,\sigma'') \in \mathcal{C}[\![c_0]\!] \quad (\sigma'',\sigma') \in \mathcal{C}[\![c_1]\!]$

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

$c \equiv$ if b then c_0 else c_1

$$\mathcal{C}[\![c]\!] = \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = \text{true}, (\sigma,\sigma') \in \mathcal{C}[\![c_0]\!]\} \cup \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = \text{false}, (\sigma,\sigma') \in \mathcal{C}[\![c_1]\!]\}$$

$(\sigma,\sigma') \in \mathcal{C}[\![c_1]\!]$

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

$c \equiv$ while b do c_0 $\qquad (\sigma,\sigma') \in \mathcal{C}[\![c_0]\!] \iff \langle c_0,\sigma\rangle \to \sigma'$

$$\mathcal{C}[\![\text{while } b \text{ do } c_0]\!] = fix\ \Gamma = \bigcup_{n\in\omega} \Theta_n$$

$$\Gamma = \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = \text{true}, (\sigma,\sigma') \in \varphi \circ \mathcal{C}[\![c_0]\!]\} \cup \{(\sigma,\sigma) \mid \mathcal{B}[\![b]\!]\sigma = \text{false}\}$$

$$\Theta_0 = \phi \qquad \Theta_{n+1} = \Gamma(\Theta_n) = \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = \text{true}, (\sigma,\sigma') \in \Theta_n \circ \mathcal{C}[\![c_0]\!]\} \cup \{(\sigma,\sigma) \mid \mathcal{B}[\![b]\!]\sigma = \text{false}\}$$

th $(\sigma,\sigma') \in \Theta_n \Rightarrow \langle c,\sigma\rangle \to \sigma'$

$n = \phi$ $\Theta_0 = \phi$

Supponiamo valga per Θ_n

$$\frac{(\sigma,\sigma') \in \Theta_{n+1} \qquad \langle b,\sigma\rangle \to \text{true} \quad (\sigma,\sigma'') \in \mathcal{C}[\![c_0]\!] \quad (\sigma'',\sigma') \in \Theta_n}{\langle b,\sigma\rangle \to \text{true} \qquad \langle c_0,\sigma\rangle \to \sigma'' \quad \langle w,\sigma''\rangle \to \sigma'}$$

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

Esercizio

if b_1 then c_1 else (if $\neg b_2$ then c_2 else c_1) $\equiv$ if $b_1 \vee b_2$ then c_1 else c_2

Dobbiamo dimostrare che sono equivalenti

In questo caso lo facciamo con la semantica denotazionale

Sem operazionale $\forall \sigma,\sigma' \quad \langle P_1,\sigma\rangle \to \sigma' \iff \langle P_2,\sigma\rangle \to \sigma'$

$\mathcal{C}[\![$ if b_1 then c_1 else (if $\neg b_2$ then c_2 else c_1) $]\!]$

$$= \{(\sigma,\sigma') \mid \mathcal{B}[\![b_1]\!]\sigma = \text{true}, (\sigma,\sigma') \in \mathcal{C}[\![c_1]\!]\} \cup \{(\sigma,\sigma') \mid \mathcal{B}[\![b_1]\!]\sigma = \text{false}, (\sigma,\sigma') \in \mathcal{C}[\![\text{if } \neg b_2 \text{ then } c_2 \text{ else } c_1]\!]\}$$

$$= \{(\sigma,\sigma') \mid \mathcal{B}[\![b_1]\!]\sigma = \text{true}, (\sigma,\sigma') \in \mathcal{C}[\![c_1]\!]\} \cup \{(\sigma,\sigma') \mid \mathcal{B}[\![b_1]\!]\sigma = \text{false}, \mathcal{B}[\![b_2]\!]\sigma = \text{false}, (\sigma,\sigma') \in \mathcal{C}[\![c_2]\!]\} \cup \{(\sigma,\sigma') \mid \mathcal{B}[\![b_1]\!]\sigma = \text{false}, \mathcal{B}[\![b_2]\!]\sigma = \text{true}, (\sigma,\sigma') \in \mathcal{C}[\![c_1]\!]\}$$

$\mathcal{B}[\![b]\!]\sigma = \text{true} \leftrightarrow \mathcal{B}[\![\neg b]\!]\sigma = \text{false}$

$$= \{(\sigma,\sigma') \mid \mathcal{B}[\![b_1]\!] = \text{true} \vee \mathcal{B}[\![b_2]\!]\sigma = \text{true}, (\sigma,\sigma') \in \mathcal{C}[\![c_1]\!]\} \cup \{(\sigma,\sigma') \mid \mathcal{B}[\![b_1]\!]\sigma = \text{false} \wedge \mathcal{B}[\![b_2]\!]\sigma = \text{false}, (\sigma,\sigma') \in \mathcal{C}[\![c_2]\!]\}$$

$$= \{(\sigma,\sigma') \mid \mathcal{B}[\![b_1 \vee b_2]\!]\sigma = \text{true}, (\sigma,\sigma') \in \mathcal{C}[\![c_1]\!]\} \cup \{(\sigma,\sigma') \mid \mathcal{B}[\![b_1 \vee b_2]\!]\sigma = \text{false}, (\sigma,\sigma') \in \mathcal{C}[\![c_2]\!]\}$$

$$= \mathcal{C}[\![\text{if } b_1 \vee b_2 \text{ then } c_1 \text{ else } c_2]\!]$$

Esercizio

$n := n+1$; if $n \neq 0$ then c_1 else c_2 ≡ if $n+1 \neq 0$ then $n := n+1$ else $n := n+1$; c_2

Dimostrazione con semantica denotazionale

$$
\begin{aligned}
&\mathcal{C}[\![n := n+1 ; \text{if } n \neq 0 \text{ then } c_1 \text{ else } c_2]\!] \\
=\ &\mathcal{C}[\![\text{if } n \neq 0 \text{ then } c_1 \text{ else } c_2]\!]\sigma[\sigma(n)+1/n] \\
=\ &\{(\sigma[\sigma(n)+1/n], \sigma') \mid \mathcal{B}[\![n \neq 0]\!]\sigma[\sigma(n)+1/n] = true,\ \mathcal{C}[\![c_1]\!]\sigma[\sigma(n)+1/n] = \sigma'\} \\
&\cup \{(\sigma[\sigma(n)+1/n], \sigma') \mid \mathcal{B}[\![n \neq 0]\!]\sigma[\sigma(n)+1/x] = false,\ \mathcal{C}[\![c_2]\!]\sigma[\sigma(n)+1/x] = \sigma'\} \\
=\ &\{(\sigma,\sigma') \mid \mathcal{B}[\![n+1 \neq 0]\!]\sigma = true \quad (\sigma, \sigma[\sigma(n)+1/n]) \in \mathcal{C}[\![n := n+1]\!] \\
&\quad (\sigma[\sigma(n)+1/n], \sigma') \in \mathcal{C}[\![c_1]\!]\} \\
&\cup \{(\sigma,\sigma') \mid \mathcal{B}[\![n+1 \neq 0]\!]\sigma = false,\ (\sigma, \sigma[\sigma(n)+1/n]) \in \mathcal{C}[\![x := x+1]\!] \\
&\quad (\sigma[\sigma(n)+1/n]\sigma' \in \mathcal{C}[\![c_2]\!]\}
\end{aligned}
$$

$\mathcal{B}[\![n \neq 0]\!]\sigma[\sigma(n)+1/n] = true$
$\iff \mathcal{A}[\![n]\!]\sigma[\sigma(n)+1/n] \neq 0$
$\iff \sigma(n)+1 \neq 0$
$\iff \mathcal{B}[\![n+1 \neq 0]\!]\sigma = true$

Lezione 4

```
S := 0;
N := 1;
while ¬(N = 101)
    do  S := S+N
        N := N+1
```

$S = \sum_{i=0}^{100} i$

$\langle S := 0;\ n := 1;\ \text{while} \ldots\ldots, \sigma \rangle \rightarrow$

Se al posto di 101 ho P devo ragionare in modo più astratto su proprietà → con la semantica assiomatica posso ragionare in maniera più astratta

```
S := 0;
N := 1;
while ¬(N = P)
    do  S := S+N
        N := N+1
```

Le proprietà le mettiamo dentro le parentesi graffe

```
S := 0;
N := 1;
{s=0, n=1}
while ¬(N = 101)
    do  S := S+N
        N := N+1
{N = 101, S = ____ >
```

devo capire l'invariante del ciclo
↳ guardo le prime iterazioni

S=0 N=1
S=1 N=2
S=1+2 N=3
⋮
S= 1+2+.....+i
N= i+1

$S = 1+2+\ldots\ldots+N-1$

Lega i valori di S e N ci dice come si influenzano

```
S := 0;
N := 1;
{s=0, n=1}
while ¬(N = 101)
    do  S := S+N
        N := N+1
{N = 101, S = Σ_{i=1}^{100} i >
```

PRECONDIZIONE — comandi — POST CONDIZIONE

$\{A\}\ c\ \{B\}$

Asserzioni proprietà sugli stati

Partial Correctness Assertione

Se sono in uno stato che soddisfa A, e eseguo c con successo allora termino in uno stato che soddisfa B

JTN

Total correctness condition

$[A]\ c\ [B]$

Se sono in uno stato che soddisfa A, eseguo c con successo allora termino in uno stato che soddisfa B

$\sigma \models A$ σ soddisfa A

$\{A\}\ c\ \{B\}$

$\forall \sigma \quad (\sigma \models A \ \&\ \mathcal{C}[\![c]\!]\sigma \text{ termina}) \Rightarrow \mathcal{C}[\![c]\!]\sigma \models B$

$\mathcal{C}[\![c]\!]\sigma = \perp \quad \forall A \quad \perp \models A$

$\forall \sigma \quad \sigma \models A \Rightarrow \mathcal{C}[\![c]\!]\sigma \models B$

$$\{A\}\ c\ \{B\} \iff \forall \sigma \in \Sigma.\ \sigma \models A \Rightarrow \mathcal{C}[\![c]\!]\sigma \models B$$

Aexp $a ::= n \mid x \mid i \mid a_0 + a_1 \mid a_0 - a_1 \mid a_0 \times a_1$

$i \in \text{Intlbr}$

Assn $A ::= \text{true} \mid \text{false} \mid a_0 == a_1 \mid a_0 \le a_1 \mid A_0 \wedge A_1 \mid A_0 \vee A_1 \mid \neg A_0 \mid$

$A_0 \Rightarrow A_1 \mid \exists i.\ A \mid \forall i.\ A$

$\exists i.\ k = i \times l$ — i: bounded, k: free, l: free

$(i + 100 \le 77) \wedge (\forall i \quad j+1 = i+3)$ — i: free, j: free, i: bounded

$FV(n) = \emptyset = FV(x)$

$FV(i) = \{i\}$

$FV(a_0 + a_1) = FV(a_0) + FV(a_1)$

$FV(\text{true}) = FV(\text{false}) = \emptyset$

$FV(A_0 == A_1) = FV(A_0 \le A_1) = FV(A_0 \cup A_1)$

$FV(A_0 \wedge A_1) = FV(A_0 \vee A_1) = FV(A_0 \Rightarrow A_1) = FV(A_0) \cup FV(A_1)$

$FV(\neg A) = FV(A)$

$FV(\exists i.\ A) = FV(\forall i.\ A) = FV(A) \setminus \{i\}$

Assertione

A con free occurency i

$A = \forall_j \ldots\ldots i \ldots\ldots \exists i \ldots\ldots$

$a \in Aexp \quad A[a/i]$

↑ no ho occorrenze libere di $j \neq i$ non problema ma lo gestisco col renaming, noi ci mettiamo nel caso più semplice dicendo che a non ha variabili

Aexp

$n[a/i] = n$ $\quad (a_0 + a_1)[a/i] = a_0[a/i] + a_1[a/i]$

$x[a/i] = x$

$i[a/i] = a$ $\quad (a_0 \times a_1)[a/i] = a_0[a/i] \times a_1[a/i]$

Assn $\text{true}[a/i] = \text{true} \quad \text{false}[a/i] = \text{false}$

$(a_0 == a_1)[a/i] = a_0[a/i] == a_1[a/i]$

$(A_1 \overset{\vee\Rightarrow}{\wedge} A_2)[a/i] = A_1[a/i] \overset{\vee\Rightarrow}{\wedge} A_2[a/i]$

$(\forall_j.\ A)[a/i] = \forall_j.\ (A[a/i])$

$(\exists_j.\ A)[a/i] = \exists_j\ (A[a/j])$

$(\forall i\ A)[a/i] = \forall i\ A$

$(\exists i\ A)[a/i] = \exists i\ A$

$\{A\}\ c\ \{B\} \iff \forall \sigma \in \Sigma\ \ \sigma \vDash^I A \Rightarrow \mathcal{C}[\![c]\!]_\sigma \vDash^I B$

stati

Interpretazione $I : \text{Var} \to \mathbb{N}$ (valori)

$\mathcal{A}_v[\![a]\!]I\sigma \in \mathbb{N}$

$\mathcal{A}_v[\![n]\!]I\sigma = n$

$\mathcal{A}_v[\![x]\!]I\sigma = \sigma(x)$

$\mathcal{A}_v[\![i]\!]I\sigma = I(i)$

$\mathcal{A}_v[\![a_0 + a_1]\!]I\sigma = \mathcal{A}_v[\![a_0]\!]I\sigma + \mathcal{A}_v[\![a_1]\!]I\sigma$

$$I[n/i](j) = \begin{cases} I(j) & j \neq i \\ n & j = i \end{cases}$$

sigma soddisfa....

$\sigma \vDash^I \text{true}, \ \forall \sigma \in \Sigma$

$\sigma \vDash^I (a_0 = a_1)$, if $\mathcal{A}_v[\![a_0]\!]I\sigma = \mathcal{A}_v[\![a_1]\!]I\sigma$

$\sigma \vDash^I (a_0 \leq a_1)$, if $\mathcal{A}_v[\![a_0]\!]I\sigma \leq \mathcal{A}_v[\![a_1]\!]I\sigma$

$\sigma \vDash^I (A \wedge B)$, if $\sigma \vDash^I A$ and $\sigma \vDash^I B$

$\sigma \vDash^I (A \wedge B)$, if $\sigma \vDash^I A$ or $\sigma \vDash^I B$

$\sigma \vDash^I (\neg A)$, if $\sigma \nvDash^I A$

$\sigma \vDash^I A \Rightarrow B$, if $\sigma \nvDash^I A$ or $\sigma \vDash^I A$

$\sigma \vDash^I \forall i\ A$, if $\sigma \vDash^{I[n/i]} A\ \forall n$

$\sigma \vDash^I \exists i\ A$, if $\sigma \vDash^{I[n/i]} A\ \exists n$

Un asserzione è valida se è soddisfatta

Un asserzione è derivata se deriva dalla logica di or

$\sigma \vDash^I \{A\}\ c\ \{B\} \iff (\sigma \vDash^I A \Rightarrow \mathcal{C}[\![c]\!]_\sigma \vDash^I B)$

è valida quando

(questo vuol dire essere valida)

$\vDash \{A\}\ c\ \{B\} \quad \forall \sigma\ \forall I$

Regole

skip $\{A\}\ \text{skip}\ \{A\}$

A vale prima e dopo lo skip

assegnamento $\{B[^a/_x]\}\ x := a\ \{B\}$

cambia solo il valore di x

Esempio con intuizione

$\sigma(n) = 3 - 1 = 2$

$\sigma(n) + 1 = 3$

$\sigma \vDash x + 1 = 3 \longrightarrow \sigma(x) = 2$

$\sigma \vDash B[^{x+1}/_x]$

$x := x + 1$

$\sigma \vDash B$

Flow del ragionamento

$\sigma \vDash (x = 3)$ (B)

$\sigma(x) = 3$

sequenza

$$\frac{\{A\}\ c_0\ \{C\} \qquad \{C\}\ c_1\ \{B\}}{\{A\}\ c_0; c_1\ \{B\}}$$

if

$$\frac{\{A \wedge b\}\ c_1\ \{B\} \qquad \{A \wedge \neg b\}\ c_2\ \{B\}}{\{A\}\ \text{if } b \text{ then } c_1 \text{ else } c_2\ \{B\}}$$

while

$$\frac{\{A \wedge b\}\ c\ \{A\}}{\{A\}\ \text{while } b \text{ do } c\ \{A \wedge \neg b\}}$$

Consequence rule

Rafforzare la precondizione

Rilassare la post condizione

$$\frac{\vDash A \Rightarrow A' \qquad \{A'\}\ c\ \{B'\} \qquad \vDash B' \Rightarrow B}{\{A\}\ c\ \{B\}}$$

$\vdash \{A\}\ c\ \{B\}$ (DERIVATO) — sound ⇒ / complete ⇐ — $\vDash \{A\}\ c\ \{B\}$ (valido)

$\mathcal{A}_v[\![a_0[a/x]]\!]I\sigma = \mathcal{A}_v[\![a_0]\!]I\sigma[\mathcal{A}_v[\![a]\!]I\sigma/x]$

$a_0 \equiv n$ $\quad \mathcal{A}_v[\![n[a/x]]\!]I\sigma = \mathcal{A}_v[\![n]\!]I\sigma = n$

$a_0 = x$ $\quad \mathcal{A}_v[\![x[a/x]]\!]I\sigma = \mathcal{A}_v[\![a]\!]I\sigma$

$\mathcal{A}_v[\![x]\!]I\sigma[\mathcal{A}_v[\![a]\!]I\sigma/x] = \mathcal{A}_v[\![a]\!]I\sigma$

$a_0 = i$ $\quad \mathcal{A}_v[\![i[a/x]]\!]I\sigma = I(i)$

$\mathcal{A}_v[\![i]\!]I\sigma[\mathcal{A}_v[\![a]\!]I\sigma/x] = I(i)$

$\mathcal{A}_v[\![(a_0+a_1)[a/x]]\!]I\sigma = \mathcal{A}_v[\![a_0[a/x]]\!]I\sigma + \mathcal{A}_v[\![a_1[a/x]]\!]I\sigma$

$= \mathcal{A}_v[\![a_0+a_1]\!]I\sigma[\mathcal{A}_v[\![a]\!]I\sigma/x]$

$\sigma \vDash^I B[a/x] \iff \sigma[\mathcal{A}_v[\![a]\!]I\sigma/x] \vDash^I B$

$\sigma \vDash^I true[a/x] \Leftrightarrow \sigma \vDash^I true \Leftrightarrow \sigma[\mathcal{A}_v[\![a]\!]I\sigma/x] \vDash^I true$

$B \equiv a_0 = a_1$

$\sigma \vDash^I (a_0 = a_1)[a/x]$

$\Leftrightarrow \sigma \vDash^I a_0[a/x] = a_1[a/x]$

$\Leftrightarrow \mathcal{A}_v[\![a_0[a/x]]\!]I\sigma = \mathcal{A}_v[\![a_1[a/x]]\!]I\sigma$

$\Leftrightarrow \mathcal{A}_v[\![a_0]\!]I\sigma[\mathcal{A}_v[\![a]\!]I\sigma/x] = \mathcal{A}_v[\![a_1]\!]I\sigma[\mathcal{A}_v[\![a]\!]I\sigma/x]$

$\Leftrightarrow \sigma[\mathcal{A}_v[\![a]\!]I\sigma/x] \vDash^I a_0 = a_1$

$\sigma \vDash^I (A_0 \wedge A_1)[a/x]$

$\sigma \vDash^I A_0[a/x]$ e $\sigma \vDash^I A_1[a/x]$

Ok per ipotesi induttiva su $A_0 \cdot A_1$

Vogliamo dimostrare il teorema di soundness

$$\vdash \{A\}\, c\, \{B\} \Rightarrow \vDash \{A\}\, c\, \{B\}$$

Per dimostrare ciò dimostro che ogni regola è sound e così facendo dimostro che il sistema è sound

$\vdash \{A\}\ skip\ \{A\}$

$\vDash \{A\}\ skip\ \{A\}$ banale

Devo dimostrare

$\{A\}\ c\ \{B\}$

$\sigma \vDash A \Rightarrow \mathcal{C}[\![c]\!]\sigma \vDash B$

$\vdash \{B[a/x]\}\ x := a\ \{B\}$

$\mathcal{C}[\![x := a]\!] = \{(\sigma, \sigma[n/x]) \mid \sigma \in \Sigma \quad n = \mathcal{A}[\![a]\!]\sigma\}$

$\sigma \vDash^I B[a/x]$

$\sigma[\mathcal{A}[\![a]\!]\sigma/x] \vDash B$

① $\dfrac{\{A\}\ c_0\ \{C\} \qquad \{C\}\ c_1\ \{B\}}{\{A\}\ c_0; c_1\ \{B\}}$

$\sigma \vDash A \Rightarrow \mathcal{C}[\![c_0]\!]\sigma \vDash C$

$\mathcal{C}[\![c_0]\!](\mathcal{C}[\![c_0]\!]\sigma) \vDash B$

$$\frac{\{A \wedge b\}\ c_0\ \{B\} \qquad \{A \wedge \neg b\}\ c_1\ \{B\}}{\{A\}\ \text{if } b \text{ then } c_0 \text{ else } c_1\ \{B\}}$$

$\vDash \{A \wedge b\}\ c_0\ \{B\}$ $\qquad$ $\vDash \{A \wedge \neg b\}\ c_1\ \{B\}$

$\sigma \vDash A \wedge b \Rightarrow \mathcal{C}[\![c_0]\!]\sigma \vDash B$

$\sigma \vDash A \wedge \neg b \Rightarrow \mathcal{C}[\![c_1]\!]\sigma \vDash B$

$\vDash \{A\}$ if ..... $\{B\}$

$$\frac{\{A \wedge b\}\ c\ \{A\}}{\{A\}\ \text{while } b \text{ do } c\ \{A \wedge \neg b\}}$$

$\mathcal{C}[\![w]\!] = \bigcup_{n \in \omega} \Theta_n$

$\Theta_0 = \phi$

$\Theta_{n+1} = \{(\sigma,\sigma') \mid \mathcal{B}[\![b]\!]\sigma = \text{true},\ (\sigma,\sigma') \in \Theta_n \circ \mathcal{C}[\![c]\!]\}$
$\cup \{(\sigma,\sigma) \mid \mathcal{B}[\![b]\!]b = \text{false}\}$

$(\sigma,\sigma') \in \Theta_n$ $\qquad$ $\sigma \vDash A \Rightarrow \sigma' \vDash A \wedge \neg b$

$(\sigma,\sigma') \in \Theta_{n+1}$ $\quad \sigma \vDash A$ $\quad \sigma \vDash b$ $\quad (\sigma,\sigma') \in \Theta_n \circ \mathcal{C}[\![c]\!]$

$(\sigma,\sigma'') \in \mathcal{C}[\![c]\!]$ $\qquad$ $(\sigma'',\sigma') \in \Theta_n$

$\sigma'' \vDash A$ per ip. ind. $\sigma' \vDash A \wedge \neg b$

$$\frac{\vDash A \Rightarrow A' \qquad \{A'\}\ c\ \{B\} \vDash B' \Rightarrow B}{\{A\}\ c\ \{B\}}$$

$\sigma \vDash A \Rightarrow \sigma \vDash A' \Rightarrow \mathcal{C}[\![c]\!]\sigma \vDash B' \Rightarrow \mathcal{C}[\![c]\!]\sigma \vDash B$

Esercizio

$\{x = n \quad n \geq 0 \quad y = 1\}$

while $x > 0$ $\quad (I[x-1/x])[x*y/y]$

$y := x * y$ $\quad I[x-1/x]$

$x := x - 1$ $\quad I$

$\{y = n!\}$

$$\frac{I \wedge b \Rightarrow \hat{I} \qquad \hat{I} \text{ corpo } I}{I \wedge b \text{ corpo } I}$$

ppi

$x = n \quad y = 1$

$x = n-1 \quad y = n$

$x = n-2 \quad y = n \cdot (n-1)$

$x = n-3 \quad y = n \cdot (n-1) \cdot (n-2)$ $\quad$ Invariante $= X! * y = n! \quad \wedge \quad x \geq 0$

$I[x-1/x][x*y/y] = (x-1)! * x * y = n! \wedge x - 1 \geq 0$

$I \wedge b \equiv x! * y = n! \wedge x \geq 0 \wedge x > 0$

$\equiv x! * y = n! \wedge x > 0$

$\equiv (x-1)! * x * y = n! \wedge x - 1 \geq 0$

$x' * y = n! \wedge x \geq 0 \wedge x \neq 0$

$y = n!$

Dimostro che è invariante

$$\frac{\{I \wedge b\}\ c\ \{I\}}{\{I\}\ \text{while } \ldots.\ \{I \wedge \neg b\}}$$