Informatica

CdL in Matematica

Parte 5b

Roberto Zunino

Dimostrazione del Teorema di Correttezza: Preliminari

Lemma di sostituzione

FUORI ESAME

Lemma (sostituzione).

$$\langle e, \sigma \rangle \to_e v \ \wedge \ \sigma \vDash Q\{e/x\} \implies \sigma[x \mapsto v] \vDash Q$$

Dim. Una dimostrazione formale del lemma richiederebbe di definire precisamente il "linguaggio" delle proprietà Q. Lo evitiamo, ricorrendo all'intuizione.

Iniziamo osservando che, intuitivamente

$$\langle e, \sigma \rangle \to_e v \implies \Big(\sigma \vDash Q\{e/x\} \iff \sigma \vDash Q\{v/x\}\Big) \qquad (*)$$

siccome e e v hanno lo stesso valore sotto σ, quindi $Q\{e/x\}$ e $Q\{v/x\}$ sono proprietà equivalenti sotto σ.

Lemma di sostituzione

FUORI ESAME

Notiamo anche che la proprietà $Q\{v/x\}$ non dipende da x (perché è stata sostituita con v), per cui:

$$\sigma \vDash Q\{v/x\} \iff \sigma[x \mapsto u] \vDash Q\{v/x\} \qquad (**)$$

per qualsiasi valore $u \in \mathbb{Z}$.

Dimostriamo l'enunciato assumendo $\langle e, \sigma \rangle \to_e v$. Si ha:

$$\begin{array}{lll}
 & \sigma \vDash Q\{e/x\} & \\
\implies & \sigma \vDash Q\{v/x\} & [(*)] \\
\implies & \sigma[x \mapsto v] \vDash Q\{v/x\} & [(**) \text{ con } u = v] \\
\implies & \sigma[x \mapsto v] \vDash Q\{x/x\} & [(*) \text{ con } e = x \text{ e } \langle x, \sigma[x \mapsto v] \rangle \to_e v] \\
\implies & \sigma[x \mapsto v] \vDash Q & [Q\{x/x\} = Q]
\end{array}$$

Q.E.D.

Nota

FUORI ESAME

Diamo ora *due* dimostrazioni alternative del teorema di correttezza.

Queste due alternative seguono due strade diverse, nessuna delle quali è particolarmente più semplice dell'altra. La prima dimostrazione, per brevità, trascura il caso della regola [*PrePost*], accennando solo brevemente ad un suo trattamento. La seconda dimostrazione è invece completa.

Per l'esame, sufficiente studiarne una delle due.

Dimostrazione del Teorema di Correttezza:

Variante 1

Teorema di Correttezza

FUORI ESAME

Teorema. (Correttezza)

$$\vdash \{P\}\ c\ \{Q\} \qquad \Longrightarrow \qquad \vDash \{P\}\ c\ \{Q\}$$

Dim. Riscriviamo l'enunciato così:

$$\langle c, \sigma \rangle \to_b \sigma' \implies p(c, \sigma, \sigma')$$

dove

$$p(c, \sigma, \sigma') \iff \Big(\forall P, Q.\, \sigma \vDash P \wedge \vdash \{P\}\ c\ \{Q\} \implies \sigma' \vDash Q\Big)$$

e procediamo per induzione su $(\to_b)$.

Correttezza: Dimostrazione

FUORI ESAME

Dimostramo che la proprietà $p(c, \sigma, \sigma')$ è preservata da ogni regola di $(\rightarrow_b)$. Questo, per Tarski, è sufficiente a concludere.

Vedremo solo qualche caso, lasciando gli altri per esercizio.

Inoltre, per semplificare l'esposizione, ignoreremo inizialmente l'esistenza della regola *PrePost*. Dopo, daremo una intuizione su come la dimostrazione si può correggere per trattare anche quel caso.

Correttezza: Dimostrazione

FUORI ESAME

Caso Skip. Regola:

$$\frac{}{\langle \mathsf{skip}\ ,\ \sigma \rangle \rightarrow_b \sigma}[Skip]$$

Ipotesi induttive: nessuna.
Da dimostrare: $p(\mathsf{skip}, \sigma, \sigma)$.

Correttezza: Dimostrazione

FUORI ESAME

Caso Skip. Dobbiamo dimostrare che $p(\mathsf{skip}, \sigma, \sigma)$, cioè:

$$\{P\}\ \mathsf{skip}\ \{Q\} \wedge \sigma \vDash P \implies \sigma \vDash Q$$

Il fatto $\{P\}\ \mathsf{skip}\ \{Q\}$ può essere derivato solo con la regola *Skip* (e la *PrePost* che ignoriamo). Tale regola richiede $Q = P$, quindi resta da dimostrare che

$$\{P\}\ \mathsf{skip}\ \{P\} \wedge \sigma \vDash P \implies \sigma \vDash P$$

che è banale.

Correttezza: Dimostrazione

FUORI ESAME

Caso Let. Regola:

$$\frac{\langle e\ ,\ \sigma\rangle \to_e v}{\langle x := e\ ,\ \sigma\rangle \to_b \sigma[x \mapsto v]}[Let]$$

Ipotesi induttive: nessuna.
Condizione a lato: $\langle e\ ,\ \sigma\rangle \to_e v$
Da dimostrare: $p(x := e, \sigma, \sigma[x \mapsto v])$.

Correttezza: Dimostrazione

FUORI ESAME

Caso Let.
Dobbiamo dimostrare che $p(x := e\ , \sigma, \sigma[x \mapsto v])$, cioè:

$$\{P\}\ x := e\ \{Q\} \wedge \sigma \vDash P \implies \sigma[x \mapsto v] \vDash Q$$

Il fatto $\{P\}\ x := e\ \{Q\}$ può essere derivato solo con la regola *Let* (e la *PrePost* che ignoriamo). Tale regola richiede $P = Q\{e/x\}$, quindi basta dimostrare che

$$\sigma \vDash Q\{e/x\} \implies \sigma[x \mapsto v] \vDash Q$$

Ma l'implicazione sopra deriva direttamente dal lemma di sostituzione e dalla condizione a lato. Ricodiamo infatti che il lemma ci dice che:

$$\langle e, \sigma\rangle \to_e v \ \wedge\ \sigma \vDash Q\{e/x\} \implies \sigma[x \mapsto v] \vDash Q$$

Correttezza: Dimostrazione

FUORI ESAME

Caso Comp. Regola:

$$\frac{\langle c_1 \ , \ \sigma\rangle \rightarrow_b \sigma' \qquad \langle c_2 \ , \ \sigma'\rangle \rightarrow_b \sigma''}{\langle c_1; c_2 \ , \ \sigma\rangle \rightarrow_b \sigma''}[Comp]$$

Ipotesi induttive: $p(c_1, \sigma, \sigma')$ e $p(c_2, \sigma', \sigma'')$.
Da dimostrare: $p(c_1; c_2, \sigma, \sigma'')$.

Correttezza: Dimostrazione

FUORI ESAME

Caso Comp. Assumiamo per ipotesi induttiva che $p(c_1, \sigma, \sigma')$ e $p(c_2, \sigma', \sigma'')$. Dobbiamo dimostrare che $p(c_1; c_2, \sigma, \sigma'')$, cioè che

$$\{P\}\ c_1; c_2\ \{Q\} \wedge \sigma \vDash P \implies \sigma'' \vDash Q$$

Il fatto $\{P\}\ c_1; c_2\ \{Q\}$ può essere derivato solo con la regola *Comp* (*PrePost* a parte). Tale regola richiede che

$$\{P\}\ c_1\ \{R\} \qquad \{R\}\ c_2\ \{Q\}$$

per un qualche R. Da $\sigma \vDash P$, $p(c_1, \sigma, \sigma')$ e $\{P\}\ c_1\ \{R\}$ si ha che $\sigma' \vDash R$. Da questo, usando $p(c_2, \sigma', \sigma'')$ e $\{R\}\ c_2\ \{Q\}$ si ha infine che $\sigma'' \vDash Q$.

Correttezza: Dimostrazione

FUORI ESAME

Caso While-true. Regola:

$$\frac{\langle e, \sigma\rangle \to_e v \neq 0 \qquad \langle c; \mathsf{while}\ e \neq 0\ \mathsf{do}\ c\ ,\ \sigma\rangle \to_b \sigma'}{\langle \mathsf{while}\ e \neq 0\ \mathsf{do}\ c\ ,\ \sigma\rangle \to_b \sigma'}[While{-}true]$$

Poniamo $w = \mathsf{while}\ e \neq 0\ \mathsf{do}\ c$.

Ipotesi induttive: $p(c; w\ , \sigma, \sigma')$
Ipotesi dovuta alla condizione a lato: $\sigma \vDash e \neq 0$
Da dimostrare: $p(w\ , \sigma, \sigma')$

Correttezza: Dimostrazione

FUORI ESAME

Caso While-true. Dobbiamo dimostrare $p(w, \sigma, \sigma')$, cioè:

$$\{P\}\ w\ \{Q\} \wedge \sigma \vDash P \implies \sigma' \vDash Q$$

Il fatto $\{P\}\ w\ \{Q\}$ può essere derivato solo con la regola $While$ ($PrePost$ a parte). Questo richiede che $\{P \wedge e \neq 0\}\ c\ \{P\}$. Dalla regola $Comp$ ricaviamo

$$\{P \wedge e \neq 0\}\ c; w\ \{Q\} \qquad (*)$$

Dalle ipotesi abbiamo che $\sigma \vDash P$, ma per la condizione a lato possiamo rafforzarlo in $\sigma \vDash P \wedge e \neq 0$. Da questo, l'ipotesi induttiva $p(c; w, \sigma, \sigma')$ e da $(*)$ ricaviamo $\sigma' \vDash Q$ e quindi la tesi.

Teorema di Correttezza

FUORI ESAME

Gli altri casi sono lasciati per esercizio:

- **While-false**
- **If-true**
- **If-false**

Fine della dimostrazione (ignorando la $PrePost$)

Gestire la PrePost

FUORI ESAME

Per gestire correttamente anche il caso in cui $\vdash \{P\}\ c\ \{Q\}$ derivi da (una o più) applicazioni della regola $PrePost$, avremmo dovuto usare *di nuovo* il principio di induzione sulle regole di $\vdash \{P\}\ c\ \{Q\}$ in *ogni* caso visto prima, dovuto ad una regola di $(\rightarrow_b)$.

In altre parole, avremmo dovuto usare un'induzione "annidata", procedendo prima per induzione su $(\rightarrow_b)$ e poi, all'interno di ogni singolo caso, procedere per induzione su $\vdash \{P\}\ c\ \{Q\}$.

Non lo faremo, ma per fare un esempio svolgiamo il solo caso $Skip$.

Gestire la PrePost

FUORI ESAME

Caso skip. Devo dimostrare che $p(\mathsf{skip}, \sigma, \sigma)$, cioè che

$$\{P\}\ \mathsf{skip}\ \{Q\} \wedge \sigma \vDash P \implies \sigma \vDash Q$$

Basta dimostrare che

$$\{P\}\ \mathsf{skip}\ \{Q\} \implies q(P, Q)$$

dove

$$q(P, Q) \iff \Big(\sigma \vDash P \implies \sigma \vDash Q\Big)$$

Per farlo, applicando Knaster-Tarski, basta fare vedere che q è preservata da tutte le regole per $\{\mathrm{P}\}$ skip $\{\mathrm{Q}\}$.

Regola Skip: ho che $P = Q$ quindi è banale.
Regola Prepost: dall'ipotesi induttiva ho che $q(P', Q')$ con $P \implies P'$ e $Q' \implies Q$, da cui segue facilmente $q(P, Q)$.
Le altre regole non si appicano al comando skip.

Dimostrazione del Teorema di Correttezza:

Variante 2

Semantica Alternativa

FUORI ESAME

Esercizio. Modificate la regola $While - True$ come segue:

$$\frac{\langle e, \sigma\rangle \to_e z \neq 0 \quad \langle c,\ \sigma_1\rangle \to_b \sigma_2 \quad \langle \mathsf{while}\ e \neq 0\ \mathsf{do}\ c,\ \sigma_2\rangle \to_b \sigma_3}{\langle \mathsf{while}\ e \neq 0\ \mathsf{do}\ c,\ \sigma_1\rangle \to_b \sigma_3}$$

Quindi, dimostrate che la nuova semantica di IMP è equivalente a quella vecchia:

$$\forall c, \sigma, \sigma'. \quad \langle c, \sigma\rangle \to_b^{\mathsf{new}} \sigma' \iff \langle c, \sigma\rangle \to_b^{\mathsf{old}} \sigma'$$

Suggerimento: basta fare vedere come convertire una derivazione che usa la $While - True$ vecchia in una che usa solo la nuova, e viceversa.

Dimostrazione

Th. (Correttezza)

$$\vdash \{P\}\, c\, \{Q\} \implies \models \{P\}\, c\, \{Q\}$$

Dim. Procediamo direttamente per induzione su $\vdash$. Per dimostrare $(\vdash) \subseteq (\models)$ basta fare vedere che

$$\hat{\mathcal{R}}(\models) \subseteq (\models)$$

dove $\mathcal{R}$ è l'insieme di regole del sistema deduttivo delle triple di Hoare, che definisce $\vdash$.

Dobbiamo quindi dimostrare che $\models$ è preservato da ogni regola: procediamo per casi (partendo dai più semplici).

Caso Skip

$$\frac{}{\{P\}\ \mathsf{skip}\ \{P\}}\,[Skip]$$

Ipotesi induttive: nessuna
Da dimostrare: $\models \{P\}\ \mathsf{skip}\ \{P\}$, ovvero

$$\sigma \models P \wedge \langle \mathsf{skip}, \sigma \rangle \rightarrow_b \sigma' \implies \sigma' \models P$$

Invertendo l'ipotesi $\langle \mathsf{skip}, \sigma \rangle \rightarrow_b \sigma'$, notiamo che l'unica regola di $\rightarrow_b$ che può derivarla è la $[Skip]$, da cui $\sigma' = \sigma$. Quindi $\sigma' = \sigma \models P$.

Caso Let

FUORI ESAME

$$\frac{}{\{P\{e/x\}\}\ x\ :=\ e\ \{P\}}\,[Let]$$

Ipotesi induttive: nessuna.
Da dimostrare: $\models \{P\{e/x\}\}\ x\ :=\ e\ \{P\}$, ovvero

$$\sigma \models P\{e/x\} \wedge \langle x := e, \sigma\rangle \rightarrow_b \sigma' \implies \sigma' \models P$$

Invertendo l'ipotesi $\langle x := e, \sigma\rangle \rightarrow_b \sigma'$, osserviamo che la sola regola che può derivarla è la $[Let]$, che obbliga σ' ad essere $\sigma[x \mapsto v]$ dove v è tale che $\langle e, \sigma\rangle \rightarrow_e v$.
Dobbiamo quindi dimostrare

$$\sigma \models P\{e/x\} \wedge \langle e, \sigma\rangle \rightarrow_e v \implies \sigma[x \mapsto v] \models P$$

che deriva immediatamente dal Lemma di Sostituzione.

Caso Comp

$$\frac{\{P\}\ c_1\ \{Q\} \qquad \{Q\}\ c_2\ \{R\}}{\{P\}\ c_1; c_2\ \{R\}}[Comp]$$

Ipotesi induttive:

$$\begin{aligned} IP1: &\quad \models \{P\}\ c_1\ \{Q\} \\ IP2: &\quad \models \{Q\}\ c_2\ \{R\} \end{aligned}$$

Da dimostrare: $\{P\}\ c_1; c_2\ \{R\}$. Assumiamo quindi che $\sigma \models P$ e che $\langle c_1; c_2, \sigma\rangle \rightarrow_b \sigma'$ e dimostriamo $\sigma' \models R$.

Per inversione su $\langle c_1; c_2, \sigma\rangle \rightarrow_b \sigma'$, osservando che è derivabile solo con la regola $[Comp]$, otteniamo (A) $\langle c_1, \sigma\rangle \rightarrow_b \sigma''$ e (B) $\langle c_2, \sigma''\rangle \rightarrow_b \sigma'$ per un qualche σ''.

Da $\sigma \models P$, (IP1) e (A) abbiamo che $\sigma'' \models Q$.
Da ciò, (IP2) e (B) abbiamo la tesi $\sigma' \models R$.

Caso Prepost

$$\frac{P \implies P' \qquad \{P'\}\, c\, \{Q'\} \qquad Q' \implies Q}{\{P\}\, c\, \{Q\}}[PrePost]$$

Ipotesi induttive:

$$IP1: \quad \models \{P'\}\, c\, \{Q'\}$$

Condizioni a lato:

$$IP2: \quad P \implies P'$$
$$IP3: \quad Q' \implies Q$$

Da dimostrare: $\models \{P\}\, c\, \{Q\}$. Assumiamo quindi che (A) $\sigma \models P$ e (B) $\langle c, \sigma\rangle \to_b \sigma'$, e dimostriamo che $\sigma' \models Q$.

Da (A) e (IP2) deduciamo che $\sigma \models P'$.
Da ciò e (IP1) abbiamo $\sigma' \models Q'$.
Da ciò e (IP3) abbiamo la tesi $\sigma' \models Q$.

Caso If

$$\frac{\{P \wedge \phi\}\ c_1\ \{Q\} \qquad \{P \wedge \neg\phi\}\ c_2\ \{Q\}}{\{P\}\ \mathsf{if}\ \phi\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2\ \{Q\}}[If]$$

Sia $i = (\mathsf{if}\ \phi\ \mathsf{then}\ c_1\ \mathsf{else}\ c_2)$, ed e tale che $\phi = (e \neq 0)$.
Ipotesi induttive:

$$\begin{aligned} IP1: &\quad \models \{P \wedge \phi\}\ c_1\ \{Q\} \\ IP2: &\quad \models \{P \wedge \neg\phi\}\ c_2\ \{Q\} \end{aligned}$$

Da dimostrare: $\models \{P\}\ i\ \{Q\}$.

Assumiamo quindi che (A) $\sigma \models P$ e che (B) $\langle i, \sigma\rangle \rightarrow_b \sigma'$ e dimostriamo $\sigma' \models Q$.

Caso If-True

Ipotesi:

$$\begin{aligned} IP1: &\quad \models \{P \wedge \phi\}\ c_1\ \{Q\} \\ IP2: &\quad \models \{P \wedge \neg\phi\}\ c_2\ \{Q\} \\ A: &\quad \sigma \models P \\ B: &\quad \langle i, \sigma\rangle \rightarrow_b \sigma' \end{aligned}$$

Da dimostrare: $\sigma' \models Q$

Invertendo B sopra, notiamo che ci sono solo due regole che possono derivarlo. La prima è

$$\frac{\langle e, \sigma\rangle \rightarrow_e v \neq 0 \qquad \langle c_1, \sigma\rangle \rightarrow_b \sigma'}{\langle i, \sigma\rangle \rightarrow_b \sigma'}[If - True]$$

e dalla prima premessa ricaviamo $\sigma \models e \neq 0$ (cioè ϕ).
Da ciò e da (A) abbiamo che $\sigma \models P \wedge \phi$.
Da ciò, (IP1) e la seconda premessa, si ha la tesi $\sigma' \models Q$.

Caso If-False

Ipotesi:

$$\begin{aligned} IP1: &\quad \models \{P \wedge \phi\}\ c_1\ \{Q\} \\ IP2: &\quad \models \{P \wedge \neg\phi\}\ c_2\ \{Q\} \\ A: &\quad \sigma \models P \\ B: &\quad \langle i, \sigma\rangle \rightarrow_b \sigma' \end{aligned}$$

Da dimostrare: $\sigma' \models Q$

L'altro caso è analogo:

$$\frac{\langle e, \sigma\rangle \rightarrow_e 0 \qquad \langle c_2, \sigma\rangle \rightarrow_b \sigma'}{\langle i, \sigma\rangle \rightarrow_b \sigma'}[If - False]$$

Dalla prima premessa ricaviamo $\sigma \models e = 0$ (cioè $\neg\phi$).
Da ciò e da (A) abbiamo che $\sigma \models P \wedge \neg\phi$.
Da ciò, (IP2) e la seconda premessa, si ha la tesi $\sigma' \models Q$.

Caso While

FUORI ESAME

$$\frac{\{P \wedge \phi\}\ c\ \{P\}}{\{P\}\ \mathsf{while}\ \phi\ \mathsf{do}\ c\ \{P \wedge \neg\phi\}}[While]$$

Questo caso è, ovviamente, il più complesso di tutti.

Sia $w = (\mathsf{while}\ \phi\ \mathsf{do}\ c)$, ed e tale che $\phi = (e \neq 0)$.
Ipotesi induttive:

$$IP1: \qquad \models \{P \wedge \phi\}\ c\ \{P\}$$

Da dimostrare: $\models \{P\}\ w\ \{P \wedge \neg\phi\}$

Assumiamo quindi che (A) $\sigma \models P$ e che (B) $\langle w, \sigma\rangle \rightarrow_b \sigma'$ e dimostriamo $\sigma' \models P \wedge \neg\phi$.

Caso While: tentativo

FUORI ESAME

Ipotesi:

$$\begin{aligned} IP1: &\quad \models \{P \wedge \phi\}\ c\ \{P\} \\ A: &\quad \sigma \models P \\ B: &\quad \langle w, \sigma \rangle \to_b \sigma' \end{aligned}$$

Da dimostrare: $\sigma' \models P \wedge \neg\phi$

Qui invertire w, ahinoi, **non** basta: nel caso $While - True$ per esempio abbiamo

$$\frac{\langle e, \sigma \rangle \to_e v \neq 0 \qquad \langle c, \sigma \rangle \to_b \sigma'' \qquad \langle w, \sigma'' \rangle \to_b \sigma'}{\langle w, \sigma \rangle \to_b \sigma'} [While{-}True]$$

Qui (IP1), con la premessa $\langle c, \sigma \rangle \to_b \sigma''$ può darci informazioni su σ'', ma poi non c'è modo di arrivare fino a σ': avremmo bisogno di un'ipotesi induttiva anche per w.

Caso While

FUORI ESAME

Dobbiamo provare un'altra strada: invece di dimostrare che

Ipotesi	$IP1:$	$\models \{P \wedge \phi\}\ c\ \{P\}$
	$A:$	$\sigma \models P$
	$B:$	$\langle w, \sigma\rangle \rightarrow_b \sigma'$
Tesi		$\sigma' \models P \wedge \neg\phi$

dimostriamo che

Ipotesi	$IP1:$	$\models \{P \wedge \phi\}\ c\ \{P\}$
Tesi		$\forall \bar{c}, \bar{\sigma}, \bar{\sigma}'.\ \langle \bar{c}, \bar{\sigma}\rangle \rightarrow_b \bar{\sigma}' \implies p(\bar{c}, \bar{\sigma}, \bar{\sigma}')$
dove	$p(\bar{c}, \bar{\sigma}, \bar{\sigma}'):$	$(\bar{c} = w \wedge \bar{\sigma} \models P \implies \bar{\sigma}' \models P \wedge \neg\phi)$

Infatti l'asserto di sopra si ricava da quello di sotto prendendo $\bar{c} = w, \bar{\sigma} = \sigma, \bar{\sigma}' = \sigma'$.

Caso While

FUORI ESAME

$$p(\bar{c}, \bar{\sigma}, \bar{\sigma}') : \qquad (\bar{c} = w \wedge \bar{\sigma} \models P \implies \bar{\sigma}' \models P \wedge \neg\phi)$$

In una forma più compatta, riscriviamo il tutto come

Ipotesi	$IP1:$	$\models \{P \wedge \phi\}\ c\ \{P\}$
Tesi		$(\rightarrow_b) \subseteq p$

Qui potremmo procedere per induzione su $(\rightarrow_b)$. Prima di farlo, conviene riscriverlo ancora come

Ipotesi	$IP1:$	$\models \{P \wedge \phi\}\ c\ \{P\}$
Tesi		$(\rightarrow_b) \subseteq p \cap (\rightarrow_b)$

Ora, procediamo per induzione su $\rightarrow_b$, facendo vedere che la relazione $p \cap (\rightarrow_b)$ è preservata da tutte le regole della semantica big step $(\rightarrow_b)$.

Caso While: casi banali

FUORI ESAME

In pratica, dobbiamo fare vedere che, in ogni regola della semantica, supponendo sia p che $\rightarrow_b$ su ogni premessa, e l'eventuale condizione a lato, si può ricavare sia p che $\rightarrow_b$ sulla conclusione.

Si nota subito che $\rightarrow_b$ sulla conclusione vale banalmente, a causa della regola stessa, visto che $\rightarrow_b$ vale su tutte le premesse per ipotesi induttiva.

Quindi possiamo dimostrare solo p nella conclusione, avendo sia p che $\rightarrow_b$ nelle premesse.

Infine, notiamo che p è banalmente vero se $\bar{c}$ non è un while, quindi è sufficiente esaminare solo i casi relativi alle regole $[While - True, While - False]$.

Caso While-False

FUORI ESAME

$$p(\bar{c}, \bar{\sigma}, \bar{\sigma}') : \qquad (\bar{c} = w \wedge \bar{\sigma} \models P \implies \bar{\sigma}' \models P \wedge \neg\phi)$$

Osserviamo la regola $[While - False]$:

$$\frac{\langle \tilde{e}, \tilde{\sigma} \rangle \to_e 0}{\langle \textsf{while } \tilde{e} \neq 0 \textsf{ do } \tilde{c} \ , \ \tilde{\sigma} \rangle \to_b \tilde{\sigma}}$$

Ipotesi: nessuna induttiva, IP1 da prima.
Condizione a lato: $\langle \tilde{e}, \tilde{\sigma} \rangle \to_e 0$
Da dimostrare: $p(\textsf{while } \tilde{e} \neq 0 \textsf{ do } \tilde{c} \ , \ \tilde{\sigma} \ , \ \tilde{\sigma})$.

Per farlo, assumiamo che (A) $(\textsf{while } \tilde{e} \neq 0 \textsf{ do } \tilde{c}) = w$, e che (B) $\tilde{\sigma} \models P$. Dobbiamo fare vedere che $\tilde{\sigma} \models P \wedge \neg\phi$.

Da (A), ricaviamo $\phi = (\tilde{e} \neq 0)$, da cui, con la condizione a lato, segue che $\tilde{\sigma} \models \neg\phi$. Assieme a (B), ci fornisce la tesi $\tilde{\sigma} \models P \wedge \neg\phi$.

Caso While-True

FUORI ESAME

$$p(\bar{c}, \bar{\sigma}, \bar{\sigma}') : \qquad (\bar{c} = w \wedge \bar{\sigma} \models P \implies \bar{\sigma}' \models P \wedge \neg\phi)$$

Regola $[While - True]$:

$$\frac{\langle \tilde{e}, \tilde{\sigma} \rangle \to_e v \neq 0 \qquad \langle \tilde{c}\ ,\ \tilde{\sigma} \rangle \to_b \tilde{\sigma}'' \qquad \langle \text{while } \tilde{e} \neq 0 \text{ do } \tilde{c}\ ,\ \tilde{\sigma}'' \rangle \to_b \tilde{\sigma}'}{\langle \text{while } \tilde{e} \neq 0 \text{ do } \tilde{c}\ ,\ \tilde{\sigma} \rangle \to_b \tilde{\sigma}'}$$

Sia $\tilde{w} = (\text{while } \tilde{e} \neq 0 \text{ do } \tilde{c})$.

Ipotesi	$IP1:$	$\models \{P \wedge \phi\}\ c\ \{P\}$
(a lato)	$IP2:$	$\langle \tilde{e}, \tilde{\sigma} \rangle \to_e v \neq 0$
~~(induttiva)~~	~~$IP3:$~~	~~$p(\tilde{c}, \tilde{\sigma}, \tilde{\sigma}'')$~~
(induttiva)	$IP4:$	$\langle \tilde{c}, \tilde{\sigma} \rangle \to_b \tilde{\sigma}''$
(induttiva)	$IP5:$	$p(\tilde{w}, \tilde{\sigma}'', \tilde{\sigma}')$
~~(induttiva)~~	~~$IP6:$~~	~~$\langle \tilde{w}\ ,\ \tilde{\sigma}'' \rangle \to_b \tilde{\sigma}'$~~
Tesi		$p(\tilde{w}\ ,\ \tilde{\sigma}\ ,\ \tilde{\sigma}')$

(Non ci servono dopo)

Caso While-True

FUORI ESAME

$$p(\bar{c}, \bar{\sigma}, \bar{\sigma}') : \qquad (\bar{c} = w \wedge \bar{\sigma} \models P \implies \bar{\sigma}' \models P \wedge \neg\phi)$$

Per dimostrare che $p(\tilde{w}\ ,\ \tilde{\sigma}\ ,\ \tilde{\sigma}'')$, assumiamo $\tilde{w} = w$ e che (A) $\tilde{\sigma} \models P$, e procediamo col dimostrare che $\tilde{\sigma}' \models P \wedge \neg\phi$.

Da $\tilde{w} = w$, ricaviamo subito $\phi = (\tilde{e} \neq 0)$ e $\tilde{c} = c$, permettendoci qualche semplificazione.

Ipotesi	$IP1:$	$\models \{P \wedge \phi\}\ c\ \{P\}$
(a lato)	$IP2:$	$\langle \tilde{e}, \tilde{\sigma} \rangle \rightarrow_e v \neq 0$
(induttiva)	$IP4:$	$\langle c, \tilde{\sigma} \rangle \rightarrow_b \tilde{\sigma}''$
(induttiva)	$IP5:$	$p(w, \tilde{\sigma}'', \tilde{\sigma}')$
	$A:$	$\tilde{\sigma} \models P$
	$B:$	$\phi = (\tilde{e} \neq 0)$
Tesi		$\tilde{\sigma}' \models P \wedge \neg\phi$

Caso While-True

FUORI ESAME

$p(\bar{c}, \bar{\sigma}, \bar{\sigma}') : \quad (\bar{c} = w \wedge \bar{\sigma} \models P \implies \bar{\sigma}' \models P \wedge \neg\phi)$

Ipotesi	$IP1:$	$\models \{P \wedge \phi\}\ c\ \{P\}$
(a lato)	$IP2:$	$\langle \tilde{e}, \tilde{\sigma} \rangle \rightarrow_e v \neq 0$
(induttiva)	$IP4:$	$\langle c, \tilde{\sigma} \rangle \rightarrow_b \tilde{\sigma}''$
(induttiva)	$IP5:$	$p(w, \tilde{\sigma}'', \tilde{\sigma}')$
	$A:$	$\tilde{\sigma} \models P$
	$B:$	$\phi = (\tilde{e} \neq 0)$
Tesi		$\tilde{\sigma}' \models P \wedge \neg\phi$

Da (A), (IP2) e (B), otteniamo $\tilde{\sigma} \models P \wedge \phi$.
Da ciò e (IP4), usando (IP1) otteniamo $\tilde{\sigma}'' \models P$.
Da ciò e $w = w$, usando (IP5) otteniamo $\tilde{\sigma}' \models P \wedge \neg\phi$.
Abbiamo quindi ottenuto la tesi.

Q.E.D.