Completitud de la Semántica Axiomática (Lema 9.23)

Probaremos que $\forall S \; \forall Q \quad \vdash_p \{wlp(S,Q)\}\, S\, \{Q\}$

Por inducción estructural respecto de S:

- skip : Obviamente $wlp(skip, Q) \equiv Q$.
- $x := a$: Veamos que $wlp(x := a, Q) = Q[x \to \mathcal{A}[\![a]\!]]$

  Por la corrección de $[ass_p]$, basta ver que

  $\models_p \{P\}\, S\, \{Q\} \Rightarrow (P \Rightarrow Q[x \to \mathcal{A}[\![a]\!]])$

  lo cual es evidente, pues $\langle x := a, s\rangle \to s[x \leftarrow \mathcal{A}[\![a]\!]\, s]$
- $S_1 ; S_2$: Veamos que $wlp(S_1; S_2)\, Q) = wlp(S_1, wlp(S_2, Q))$

  Aplicando $[comp_p]$ y dos veces la hipótesis de inducción derivamos $\vdash_p \{wlp(S_1, wlp(S_2,Q))\}\, S_1; S_2\, \{Q\}$.

Si tomamos ahora P tal que $\vdash_p \{P\}\, S_1; S_2\, \{Q\}$

Veamos que $P \Rightarrow wlp(S_1, wlp(S_2, Q))$

Ello equivale a $\vdash_p \{P\}\, S_1\, \{wlp(S_2, Q)\}$

Sea s que verifica P. $\vdash_p \{P\}\, S_1; S_2\, \{Q\}$ puede cumplirse de tres maneras:

$\neg \exists\, s' \;\; \langle S_1, s\rangle \to s'\rangle$. En tal caso se cumple trivialmente $\vdash_p \{P\}\, S_1\, \{wlp(S_2, Q)\}$

$\exists\, s' \;\; \langle S_1, s\rangle \to s'$, pero $\neg \exists\, s'' \;\; \langle S_2, s'\rangle \to s''$, por lo que de nuevo $\vdash_p \{s'\}\, S_2\, \{Q\}$, o sea se cumple $wlp(S_2, Q)\, s'$ y por tanto $\vdash_p \{P\}\, S_1\, \{wlp(S_2, Q)\}$

Por último consideramos $\langle S_1, s\rangle \to s' \wedge \langle S_2, s'\rangle \to s''$.

Por hipótesis tendremos $Q\, s''$, y por tanto $wlp(S_2, Q)\, s'$ concluyendose de nuevo $\vdash_p \{P\}\, S_1\, \{wlp(S_2, Q)\}$

- if b then S_1 else S_2 : Veamos que

$$wlp_p(\text{if } b \text{ then } S_1 \text{ else } S_2, Q) \equiv \underbrace{\begin{cases} \mathcal{B}[\![b]\!] \wedge wlp(S_1, Q) \\ \mathcal{B}[\![\neg b]\!] \wedge wlp(S_2, Q) \end{cases}}_{W_{if}} \vee$$

De nuevo aplicando la hipótesis de inducción dos veces, la regla $[if_p]$, y la corrección del sistema de derivación, obtenemos $\vDash_p \{W_{if}\}$ if b then S_1 else S_2 $\{Q\}$

y si consideramos P tal que $\vDash_p \{P\}$ if b then S_1 else S_2 $\{Q\}$ basta discernir si s cumpliendo P satisface $\mathcal{B}[\![b]\!]$, o bien $\mathcal{B}[\![\neg b]\!]$, y la semántica operacional del lenguaje nos lleva a que ha de cumplirse $\{P\,s \wedge \mathcal{B}[\![b]\!]\}\ S_1\ \{Q\}$ y $\{P\,s \wedge \mathcal{B}[\![\neg b]\!]\}\ S_2\ \{Q\}$, de lo que se sigue que $P \Rightarrow W_{if}$.

- while b do S : Consideremos $P \equiv wlp(\text{while } b \text{ do } S, Q)$

Veamos que P cumple sendas propiedades relacionadas con la semántica "local" (última vuelta o una vuelta más) del while.

(I) $(\neg \mathcal{B}[\![b]\!] \wedge P) \Rightarrow Q$

Obvio, pues el while no hace nada (más), y por tanto termina con la identidad, en todo estado que satisfaga $\neg \mathcal{B}[\![b]\!]$

(II) $(\mathcal{B}[\![b]\!] \wedge P) \Rightarrow wlp(S, P)$

Si s cumple $\mathcal{B}[\![b]\!]$, la ejecución de while b do S s comienza con la de S (sobre el mismo s).

Si $\neg \exists\, s' \;\langle S, s\rangle \to s'$, entonces el bucle no termina y se cumplirá $wlp(S, P)\ s$.

Si $\langle S, s\rangle \to s'$, volvemos a distinguir dos casos:

- $\langle$ while b do $S, s'\rangle \to s''$, entonces también

tenemos $\langle \text{while } b \text{ do } S, s\rangle \longrightarrow s''$, y por tanto, al cumplirse $P\,s$ ha de cumplirse $P\,s''$, y de $\langle \text{while } b \text{ do } S, s'\rangle \to s''$ concluimos $P\,s'$ y de $\langle S, s\rangle \to s'$ llegamos a $wlp(S,P)\,s$

- Cuando $\neg\exists\, s'' \langle \text{while } b \text{ do } S, s'\rangle \to s''$, también tendremos $P\,s'$ y de nuevo concluimos $wlp(S,P)\,s$.

- Ahora, aplicando la hipótesis de inducción tendremos

  $\vdash_P \{wlp(S,P)\}\, S\, \{P\}$, lo que nos lleva a

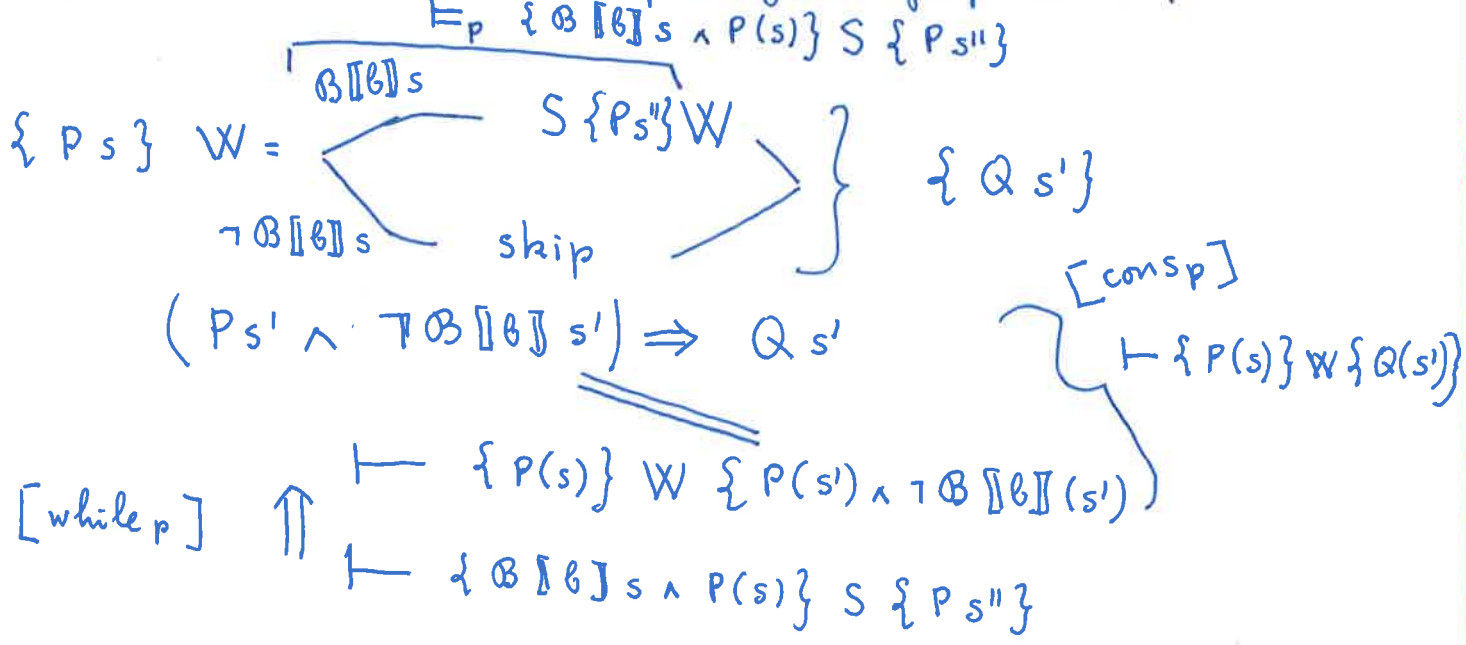
  $\vdash_P \{\mathcal{B}[\![b]\!] \wedge P\}\, S\, \{P\}$, lo que nos permite aplicar

  $[\text{while}_P]$ para concluir $\vdash_P \{P\}$ while b do S $\{\neg\mathcal{B}[\![b]\!] \wedge P\}$

  concluyendose por fin $\vdash_P \{P\}$ while b do S $\{Q\}$

Nota: Obsérvese que (II) es equivalente a $\models_P \{\mathcal{B}[\![b]\!] \wedge P\}\, S\, \{P\}$

La prueba para el While esquematizada gráficamente:

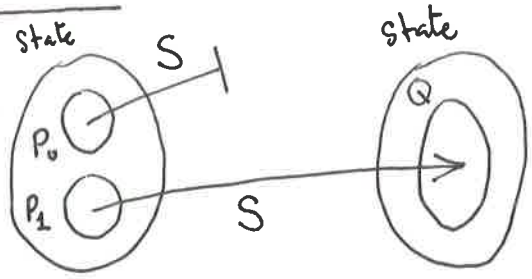


Completitud de la Semántica Axiomática (presentaciones gráficas)

Precondición más débil ($P = wlp(S,Q)$)

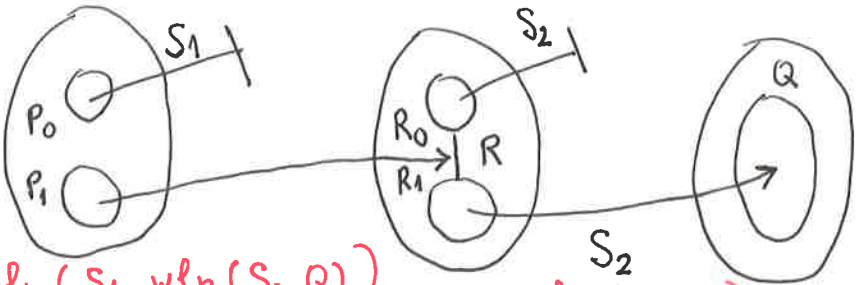
$P_0 = \{ s \in State \mid (S,s) \not\to \}$

$P_1 = \{ s \in State \mid \begin{matrix} \exists s'\ Q(s') \\ (S,s) \to s' \end{matrix} \}$

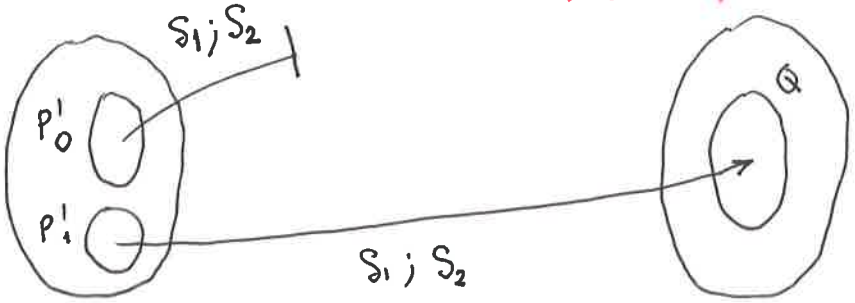


Corolario : $\forall Q\ \forall S \quad P_0 \Rightarrow wlp(S,Q)$

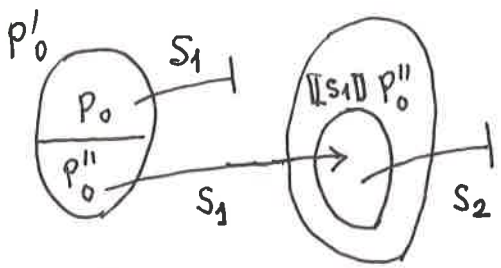
Secuencial Composition : $wlp(S_1; S_2, Q) = wlp(S_1, wlp(S_2,Q))$

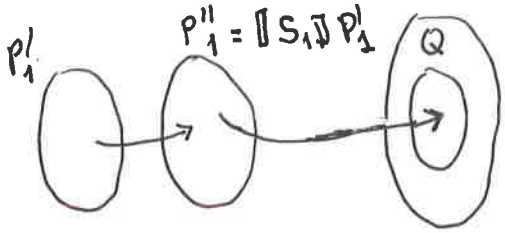


$wlp(S_1, wlp(S_2,Q))$ $\qquad$ $wlp(S_2,Q)$



$wlp(S_1; S_2, Q)$





$[\![S_1]\!]\ P''_0 = \{ s'' \mid \exists s \in P'_0 \ (S_1,s) \to s'' \} \subseteq R_0 \Rightarrow P''_0 \subseteq P_1$

$P''_1 \subseteq R_1 \Rightarrow P'_1 \subseteq P_1$

$\Big\}$ $P'_0 \cup P'_1$ $\cap$ $P_0 \cup P_1$

$P_0 \subseteq P'_0$ $\qquad [\![S_1]\!]\ P_1 = ([\![S_1]\!]\ P_1 \cap R_0) \cup ([\![S_1]\!]\ P_1 \cap R_1)$

$P_1 = [\![S_1]\!]^{-1}([\![S_1]\!]\ P_1 \cap R_0) \cup [\![S_1]\!]^{-1}([\![S_1]\!]\ P_1 \cap R_1)$

$\cap$ P'_0 $\qquad$ $=$ P'_1

$P_0 \cup P_1 \subseteq P'_0 \cup P'_1$

Instrucción While

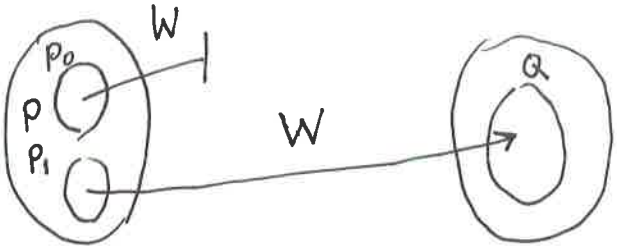
W

$P = wlp(\text{while } b \text{ do } S, Q) = (P_0 \cup P_1)$

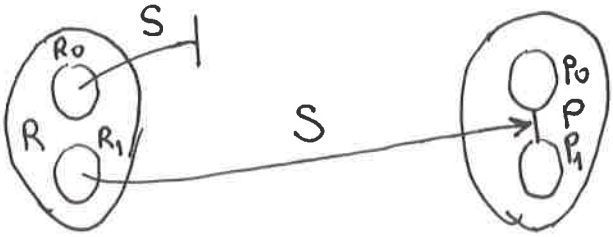
$\Downarrow$

$(\mathcal{B}[\![b]\!] \wedge P) \Rightarrow wlp(S, P) \; (= R = R_0 \cup R_1)$

$wlp(W, Q)$

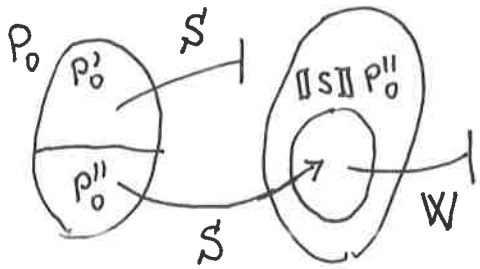


$wlp(S, P)$



Hay que ver que $\mathcal{B}[\![b]\!] \cap P = (\mathcal{B}[\![b]\!] \cap P_0) \cup (\mathcal{B}[\![b]\!] \cap P_1) \overset{?}{\subseteq} R_0 \cup R_1$

($\mathcal{B}[\![b]\!] \cap P_0 = P_0$, $\mathcal{B}[\![b]\!] \cap P_1 = P_2$)



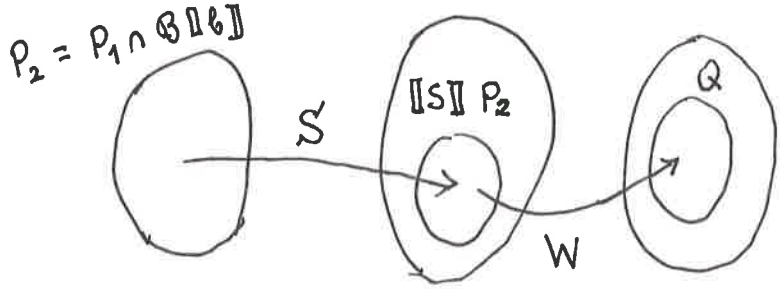
$P'_0 \subseteq R_0$

$[\![S]\!] P''_0 \subseteq P_0 \subseteq P_0 \cup P_1$

$\Downarrow$

$P''_0 \subseteq R_1$

$\Rightarrow P_0 \subseteq R_0 \cup R_1$



$[\![S]\!] P_2 \subseteq P_1 \subseteq P_0 \cup P_1$

$\Downarrow$

$P_2 \subseteq R_1 \subseteq R_0 \cup R_1$