

V SOUNDNESS AND SEMANTIC COMPLETENESS (SKETCH)

Theorem 7.21

Let $B \equiv (L, T, s, t)$ be a basic synchronous transition diagram and Q be a compositionally-inductive assertion network for B . We have that $B \vdash Q$ implies $\models \{Q_s\} B \{Q_t\}$.

Proof: It suffices to prove that for every computation

$$\langle s; \sigma \rangle \xrightarrow{\theta} \langle l; \sigma' \rangle$$

of $B \equiv (L, T, s, t)$ we have that $\sigma \models Q_s$ implies $(\sigma': h \mapsto \sigma(h).\theta) \models Q_l$, with Q compositionally inductive. This is proved by induction on the length of the computation. \square

Theorem 7.22

Let $P \equiv P_1 \parallel P_2$. We have that $\models \{\varphi_1\} P_1 \{\psi_1\}$ and $\models \{\varphi_2\} P_2 \{\psi_2\}$ imply $\models \{\varphi_1 \wedge \varphi_2\} P \{\psi_1 \wedge \psi_2\}$, provided ψ_i does not involve the variables of P_j and $\text{Chan}(\psi_i) \cap \text{Chan}(P_j) \subseteq \text{Chan}(P_i)$, $i \neq j$.

Proof: See next transparency.

SOUNDNESS OF THE PAR. COMP. RULE

Proof: Let $(\sigma, \sigma', \theta) \in O(P)$ s.t. $\sigma \Vdash \varphi_1 \wedge \varphi_2$, then, by def. of $O(P)$
 $(\sigma, \sigma'_i, \theta \downarrow P_i) \in O(P_i)$ and $\theta = \theta \downarrow \text{Chan}(P_1 \parallel P_2)$

We must prove that $(\sigma': h \mapsto \sigma(h). \theta) \Vdash \psi_1 \wedge \psi_2$

From $\Vdash \{\varphi_i\} P_i \{\psi_i\}$ we obtain $(\sigma'_i: h \mapsto \sigma(h). \theta \downarrow P_i) \Vdash \psi_i$

Since ψ_i does not involve the variables of $P_j, i \neq j$, this implies

$$(\sigma': h \mapsto \sigma(h). \theta \downarrow P_i) \Vdash \psi_i \quad (*)$$

Next, assumption $\text{Chan}(\psi_i) \cap \text{Chan}(P_j) \subseteq \text{Chan}(P_i), i \neq j$ is equiv. to

$$\text{Chan}(\psi_i) \subseteq C_i \text{ with } C_i \equiv (\text{CHAN} \setminus \text{Chan}(P_j)) \cup \text{Chan}(P_i).$$

Observe that $\text{Chan}(\psi_i) \subseteq C_i$ implies $\psi_i \uparrow C_i = \psi_i$ (**)

One can derive easily that $(\theta \downarrow (P_1 \parallel P_2)) \downarrow C_i = (\theta \downarrow P_i) \downarrow C_i$ (***)

$(*) + (**)$ + $(***)$ imply $(\sigma': h \mapsto \sigma(h). \theta \downarrow (P_1 \parallel P_2)) \Vdash \psi_i$

Since $\theta = \theta \downarrow (P_1 \parallel P_2)$ we conclude that

$$(\sigma': h \mapsto \sigma(h). \theta) \Vdash \psi_i, \text{ QED.}$$

7.4.5 Semantic Completeness

We want to prove completeness, that is, we want to prove that every valid partial correctness statement of a composite system P is derivable, i.e.,

Theorem 7.23

$$\models \{\varphi\} P \{\psi\} \Rightarrow \vdash \{\varphi\} P \{\psi\}.$$

We prove this by induction on the structure of P , restricting ourselves to the cases of basic transition diagrams and parallel composition. To this end we introduce the following characterisation of *strongest postconditions*.

Definition 7.24 Given a basic synchronous transition diagram $B \equiv (L, T, s, t)$, $l \in L$, and a precondition φ we define

$$SP_l(\varphi, B) \stackrel{\text{def}}{=} \{\sigma \mid \text{there exists } \sigma', \sigma'', \theta \text{ s.t. } \sigma' \models \varphi, \\ (\sigma', \sigma'', \theta) \in O_l(B), \text{ and } \sigma = (\sigma' : h \mapsto \sigma'(h) \cdot \theta)\}.$$

By $SP(\varphi, B)$, for $B \equiv (L, T, s, t)$, we denote $SP_t(\varphi, B)$. Similarly we define $SP(\varphi, P)$, for P a composite system, in terms of $O(P)$. \square

For the strongest postcondition we have the following properties.

Lemma 7.25 For P a sequential synchronous transition diagram or a composite system, one has that

$$\models \{\varphi\} P \{SP(\varphi, P)\},$$

and

$$\models \{\varphi\} P \{\psi\} \Rightarrow \models SP(\varphi, P) \rightarrow \psi.$$

Proof See Exercise 7.7. \square

We now prove our completeness result by induction on the complexity of composite systems, starting with basic synchronous transition diagrams.

Lemma 7.26 For B a basic synchronous transition diagram, we have

$$\models \{\varphi\} B \{\psi\} \Rightarrow \vdash \{\varphi\} B \{\psi\}.$$

Lemma 7.27 For $P \equiv P_1 \parallel P_2$ we have

$$\models \{\varphi\} P \{\psi\} \Rightarrow \vdash \{\varphi\} P \{\psi\}.$$

Lemma 7.28

$$\models (\exists \bar{x}_2. SP(\varphi', P_1) \uparrow C_1 \wedge \exists \bar{x}_1. SP(\varphi', P_2) \uparrow C_2 \wedge t \preceq h) \rightarrow SP(\varphi', P).$$

Pf.: $\varphi' \stackrel{\text{def}}{=} \varphi \wedge \bar{z} = \bar{x} \wedge t = h$, $\mathcal{X} = \text{var}(\varphi) \cup \text{var}(P)$

\uparrow log. vars

$$\bar{x}_i \stackrel{\text{def}}{=} \text{var}(P_i), i = 1, 2$$

$$C_i \stackrel{\text{def}}{=} \overline{\text{Chan}(P_j)} \cup \text{Chan}(P_i)$$

Lemma: For $P \equiv P_1 \parallel P_2$ we have $\vdash \{ \varphi \} P \{ \psi \} \Rightarrow \vdash \{ \varphi \} P \{ \psi \}$

Pf.: $\bar{x} = \text{var}(\varphi) \cup \text{var}(P)$, $\bar{x}_i = \text{var}(P_i)$, $C_i = \overline{\text{Chan}(P_j)} \cup \text{Chan}(P_i), i \neq j$

By induction, since $\vdash \{ \varphi' \} P_i \{ SP(\varphi', P_i) \}$, we have $\vdash \{ \varphi' \} P_i \{ SP(\varphi', P_i) \}$ \otimes
 with $\varphi' = \varphi \wedge \bar{z} = \bar{x} \wedge t = h$, t, z log. vars

Secondly, for arbitrary φ'' , $\vdash \varphi'' \rightarrow \varphi'' \uparrow C$, with $\varphi'' \uparrow C$ not depending on \bar{C} } $\otimes\otimes$
 $\vdash \varphi'' \rightarrow \exists x_j. \varphi''$, with $\exists x_j. \varphi''$ not depending on x_j

Next, $\text{Chan}(\varphi''_i) \cap \text{Chan}(P_j) \subseteq \text{Chan}(P_i), i \neq j \Leftrightarrow \text{Chan}(\varphi''_i) \subseteq C_i, i=1,2$

$\otimes + \otimes\otimes$ yield: $\vdash \{ \varphi' \} P_i \{ \exists x_j. (SP(\varphi', P_i) \uparrow C_i) \}$ (rule)
 $\otimes\otimes + \otimes\otimes\otimes$ yield: $\{ \exists x_j. (SP(\varphi', P_i) \uparrow C_i) \}$ satisfy conds of par. comp.

So, by the par. comp rule: $\vdash \{ \varphi' \} P \{ \exists x_2. SP(\varphi', P_1) \uparrow C_1 \wedge \exists x_1. SP(\varphi', P_2) \uparrow C_2 \}$

Now by the prefix inv. axiom,

$\vdash \{ \varphi' \wedge t = h \} P \{ \exists x_2. SP(\varphi', P_1) \uparrow C_1 \wedge \exists x_1. SP(\varphi', P_2) \uparrow C_2 \wedge t \leq h \}$

(apply $\xrightarrow{\text{initializ. rule}}$)

(Lemma 7.28) $\Rightarrow SP(\varphi', P) \Rightarrow SP(\varphi, P)$