Verifikation nebenläufiger Programme
Wintersemester 2004/05
Ulrich Hannemann Jan Bredereke

16 Semantic Completeness of the AFR-Method

Finally we are ready to establish semantic completeness of the AFR-method. Based on the compositional semantics $\mathcal{O}$ we define the following minimal predicates.

Definition 16.1 (Strongest l-condition for synchronous communication) We associate with a location l of a transition diagram P the strongest l-condition with respect to a given precondition φ:

$$SP_l(\varphi, P) \stackrel{\text{def}}{=} \{\sigma \mid \text{there exist } \sigma', \theta \text{ such that } \sigma' \models \varphi \text{ and } (\sigma', \sigma, \theta) \in \mathcal{O}_l(P)\}. \quad \square$$

Let $P \equiv P_1 \parallel \cdots \parallel P_n$ be a closed system, and $\{\varphi\}P\{\psi\}$ be a valid correctness formula.

We encode the above semantics $\mathcal{O}$ by introducing for each component P_i of P a history variable h_i, denoting a finite sequence of communication records $\langle (C_1, v), \ldots, (C_k, v_k) \rangle$, and by transforming an input-output transition $l \stackrel{a}{\rightarrow} l'$ into a transition with action $a' \stackrel{\text{def}}{=} b; C!e \rightarrow f \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h_i \mapsto \sigma(h_i) \cdot (C, e(\sigma)))$ in the case $a \equiv b; C!e \rightarrow f$, and into a transition with action $a' \equiv b; C?x \rightarrow f \circ g$, where $g(\sigma) \stackrel{\text{def}}{=} (\sigma : h_i \mapsto \sigma(h_i) \cdot (C, \sigma(x)))$ in the case $a \equiv b; C?x \rightarrow f$ (here '$\cdot$' denotes the append operation). Observe that evaluation of a' in σ with $\models b(\sigma)$ results in evaluating the $f \circ g$-part of a' in state $(\sigma : x \rightarrow v)$, for arbitrary values v, according to Definition 15.1. This models that x has received its value in the $b; C?x$-part of a', i.e., prior to executing $f \circ g$. Let $P' \equiv P'_1 \| \ldots \| P'_n$ denote the augmented transition diagram thus obtained (which is also closed).

The semantics of P'_i records its own sequence of communications θ_i, according to its $\mathcal{O}$-semantics, in auxiliary variable h_i, as stated below.

Lemma 16.2 For $(\sigma, \sigma', \theta_i) \in \mathcal{O}_{l_i}(P'_i)$,

$$(\sigma(h_i) = \langle\rangle \wedge (\langle s; \sigma \rangle \stackrel{\theta_i}{\rightarrow} \langle l_i; \sigma' \rangle)) \Rightarrow \sigma'(h_i) = \theta_i.$$

Proof
By induction on the length of the computation history θ_i.

■

Since $\mathcal{O}$ is correctly defined from an operational point of view, as proved in Theorem 15.7, we conclude that h_i records the correct communication history of process P_i.

After we have encoded the local communication histories θ_i into the history variables h_i by transforming P_i to P'_i, we would like to associate with each location l_i of P'_i the predicate $SP_{l_i}(\varphi, P'_i)$. However, since φ may involve variables of the other components, this choice of predicates is not allowed. To overcome this problem we introduce new logical variables $\bar{z}^i$, so-called *freeze* variables, corresponding to the variables $\bar{x}^i$ of P_i, and define

$$\varphi_i \stackrel{\text{def}}{=} \varphi \circ k \wedge \bar{z}^i = \bar{x}^i \wedge h_i = \langle\rangle,$$

where $k(\sigma) \stackrel{\text{def}}{=} (\sigma : \bar{x} \mapsto \sigma(\bar{z})), \bar{z} = \bar{z}^1, \ldots, \bar{z}^n$ and $\bar{x} = \bar{x}^1, \ldots, \bar{x}^n$.

So φ_i replaces in φ all the program variables $\bar{x}$ of P by their corresponding freeze variables $\bar{z}$ and identifies the freeze variables $\bar{z}^i$ with the corresponding local variables $\bar{x}^i$ of P_i (we define for sequences of variables $\bar{u} = (u_1, \ldots, u_m)$ and $\bar{v} = (v_1, \ldots, v_m)$, $\models \bar{u} = \bar{v}(\sigma)$ iff $\sigma(u_i) = \sigma(v_i)$, $1 \leq i \leq m$). Additionally φ_i initialises the history variable h_i to the empty sequence (denoted by $\langle\rangle$).

Let $\bar{u}$ be a set of program variables disjoint from $\bar{x}$ such that φ only involves the variables $\bar{x}$ and $\bar{u}$. It is not so difficult to check that $SP_{l_i}(\varphi_i, P_i')$ only involves the newly introduced freeze variables $\bar{z}$, the program variables of P_i', and the variables $\bar{u}$. Thus we derive that $SP_{l_i}(\varphi_i, P_i')$ does not involve the variables of the remaining components. This justifies the association of $SP_{l_i}(\varphi_i, P_i')$ with location l_i of P_i'.

Next we introduce the global invariant $I(h_1, \ldots, h_n)$.

Definition 16.3 (Global invariant) Let $I(h_1, \ldots, h_n)$ be the predicate such that

$$\sigma \models I(h_1, \ldots, h_n) \text{ iff there exists } \theta \text{ such that } \sigma(h_i) = \theta_i \text{ for every } i \in \{1, \ldots, n\},$$

where θ_i denotes the projection of θ along the channels of P_i.

■

The global invariant $I(h_1, \ldots, h_n)$ thus ensures the *compatibility* of the histories $h_1, \ldots, h_n$, i.e., that every value recorded as received is also recorded as being sent.

We have the following compositional characterisation of the strongest post-condition operator defined above. This characterisation holds for both open and closed networks.

Theorem 16.4
Let $P \equiv P_1 \parallel \cdots \parallel P_n$, for some $n \geq 2$, be a synchronous diagram. We express the diagram P modified with updates to the history variables $h_1, \ldots, h_n$ by $P' \equiv P_1' \parallel \cdots \parallel P_n'$. Let $l \equiv \langle l_1, \ldots, l_n \rangle$, with l_i a location of P_i'. We then have

$$\models I(h_1, \ldots, h_n) \wedge \bigwedge_i SP_{l_i}(\varphi_i, P_i') \leftrightarrow SP_l(\bigwedge_i \varphi_i, P').$$

(Here the index i is implicitly assumed to range over $\{1, \ldots, n\}$.)

Proof
Let $\sigma \models I \wedge \bigwedge_i SP_{l_i}(\varphi_i, P_i')$. By the definition of SP it follows that there exist states σ_i and histories θ_i, such that $(\sigma_i, \sigma, \theta_i) \in \mathcal{O}_{l_i}(P_i')$ and $\sigma_i \models \varphi_i$. Since φ_i stipulates that $\sigma_i(h_i) = \langle\rangle$, we have by Lemma 16.2 that $\theta_i = \sigma(h_i)$. Let σ' be such that σ', σ_i agree w.r.t. the variables of P_i', for $1 \leq i \leq n$, and σ', σ agree w.r.t. the remaining (logical) variables, and hence also agree with $\sigma_1, \ldots, \sigma_n$ w.r.t. these variables. It follows that $\sigma' \models \bigwedge_i \varphi_i$ and $(\sigma', \sigma_i', \theta_i) \in \mathcal{O}_{l_i}(P_i')$,

where σ_i' is obtained from σ by assigning to all the variables not belonging to P_i' their corresponding value in σ'. Since $\sigma \models I$ and $\theta_i = \sigma(h_i)$ we have that there exists a history θ such that θ_i equals the projection of θ along the channels of P_i'. By the compositionality of $\mathcal{O}$ we then derive that $(\sigma', \sigma, \theta) \in \mathcal{O}_l(P')$. In other words: $\sigma \in SP_l(\bigwedge_i \varphi_i, P')$.

To prove the other direction, let $\sigma \models SP_l(\bigwedge_i \varphi_i, P')$. So for some state σ' such that $\sigma' \models \bigwedge_i \varphi_i$ we have that $(\sigma', \sigma, \theta) \in \mathcal{O}_l(P')$, for some θ. By the compositionality of $\mathcal{O}$ we derive that $(\sigma', \sigma_i, \theta_i) \in \mathcal{O}_{l_i}(P_i')$, where θ_i denotes the projection of θ along the channels of P_i' and σ_i is obtained from σ by assigning to all the variables not belonging to P_i' their corresponding value in σ'. Thus by definition of *SP* and the fact that σ and σ_i by definition agree w.r.t. the variables of P_i' and the remaining variables of φ_i, we have that $\sigma \models SP_{l_i}(\varphi_i, P_i')$. Moreover since $\sigma'(h_i) = \langle\rangle$, for $1 \leq i \leq n$, we have by construction of P_i' that $\sigma(h_i) = \sigma_i(h_i) = \theta_i$, $1 \leq i \leq n$, i.e., $\sigma \models I$.

■

Local correctness of a component is straightforward, the proof is left as an exercise:

Lemma 16.5 (Local correctness) For each internal transition $l \xrightarrow{a} l'$ of a transition system P_i', with $a \equiv b \rightarrow f$, we have

$$\models SP_l(\varphi_i, P_i') \wedge b \rightarrow SP_{l'}(\varphi_i, P_i') \circ f.$$

Lemma 16.6 (Cooperation test) Let $l_1 \xrightarrow{a} l_2$ occur in P_i' and $l_1' \xrightarrow{a'} l_2'$ in P_j', with $a \equiv b; C!e \rightarrow f$ and $a' \equiv b'; C?x \rightarrow g$. Furthermore, let $I(h_1, \ldots, h_n)$ be the compatibility predicate defined above. We then have

$$\begin{aligned} &\models I \wedge SP_{l_1}(\varphi_i, P_i') \wedge SP_{l_1'}(\varphi_j, P_j') \wedge b \wedge b' \\ &\quad \rightarrow (I \wedge SP_{l_2}(\varphi_i, P_i') \wedge SP_{l_2'}(\varphi_j, P_j')) \circ f', \end{aligned}$$

where $f' \stackrel{\text{def}}{=} (f \circ g \circ (x := e))$.

Proof
In fact we prove the following implications:

$$\models I \rightarrow I \circ f',\ \models SP_{l_1}(\varphi_i, P_i') \wedge b \rightarrow SP_{l_2}(\varphi_i, P_i') \circ f'$$

and

$$\models SP_{l_1'}(\varphi_j, P_j') \wedge b' \rightarrow SP_{l_2'}(\varphi_j, P_j') \circ f'.$$

In order to prove the validity of $I \rightarrow I \circ f'$, let $\sigma \models I$ and $f'(\sigma) = \sigma'$. By the construction of P_i' and P_j' it follows that $\sigma'(h_i) = \sigma(h_i) \cdot (C, v)$ and $\sigma'(h_j) = \sigma(h_j) \cdot (C, v)$, where $v = e(\sigma)$. Moreover $\sigma'(h_k) = \sigma(h_k)$, for $k \neq i, j$. Thus by definition of I it follows immediately that $\sigma' \models I$.

Next we prove that $\models SP_{l_1}(\varphi_i, P_i') \wedge b \rightarrow SP_{l_2}(\varphi_i, P_i') \circ f'$. Let $\sigma \models SP_{l_1}(\varphi_i, P_i') \wedge b$. So there exist σ' and θ such that $\sigma' \models \varphi_i$ and $(\sigma', \sigma, \theta) \in \mathcal{O}_{l_1}(P_i')$. By definition of $\mathcal{O}$ it follows immediately that $(\sigma', f(\sigma), \theta \cdot (C, v)) \in \mathcal{O}_{l_2}(P_i')$, where $v = e(\sigma)$. By definition of *SP* we thus derive that $f(\sigma) \models SP_{l_2}(\varphi_i, P_i')$. Since $SP_{l_2}(\varphi_i, P_i')$ only involves the variables of P_i' and the freeze variables $\bar{z}$, we thus may conclude that $f'(\sigma) \models SP_{l_2}(\varphi_i, P_i')$, that is, $\sigma \models SP_{l_2}(\varphi_i, P_i') \circ f'$.

In order to prove the validity of the last implication, let $\sigma \models SP_{l'_1}(\varphi_j, P'_j)$. So there exist σ' and θ such that $\sigma' \models \varphi_j$ and $(\sigma', \sigma, \theta) \in \mathcal{O}_{l'_1}(P'_j)$. By definition of $\mathcal{O}$ it follows that $(\sigma', g(\sigma : x \mapsto v), \theta \cdot (C, v)) \in \mathcal{O}_{l'_2}(P'_j)$, for any value v. So in particular we have that $(\sigma', g(\sigma : x \mapsto v), \theta \cdot (C, v)) \in \mathcal{O}_{l'_2}(P'_j)$, for $v = e(\sigma)$, from which we derive by definition of SP that $g \circ x := e(\sigma) \models SP_{l'_2}(\varphi_i, P'_j)$. Since $SP_{l'_2}(\varphi_j, P'_j)$ only involves the variables of P'_j we thus may conclude that $f'(\sigma) \models SP_{l'_2}(\varphi_j, P'_j)$, that is, $\sigma \models SP_{l'_2}(\varphi_j, P'_j) \circ f'$.

■

We conclude the completeness proof with the remaining clauses.

Lemma 16.7 (Initialisation) We have

$$\models \varphi \rightarrow (I \wedge \bigwedge_i SP_{s_i}(\varphi_i, P'_i) \circ f),$$

where f assigns to history variable h_i the empty sequence $\langle\rangle$ and assigns to every freeze variable z the value of its corresponding (program) variable x.

Proof
Let $\sigma \models \varphi$. It follows that $f(\sigma) \models \varphi_i$ (note that h_i is assumed not to occur in φ). Furthermore we have that $(f(\sigma), f(\sigma), \langle\rangle) \in \mathcal{O}_{s_i}(P'_i)$, so we have that $f(\sigma) \models \bigwedge_i SP_{s_i}(\varphi_i, P'_i)$. Since $f(\sigma)(h_i)$ equals the empty sequence $\langle\rangle$ it trivially follows that $f(\sigma) \models I$.

■

Lemma 16.8 (Finalisation) We have

$$\models I \wedge \bigwedge_i SP_{t_i}(\varphi_i, P'_i) \rightarrow \psi.$$

Proof
Let $\sigma \models I \wedge \bigwedge_i SP_{t_i}(\varphi_i, P'_i)$. By Theorem 16.4 we derive that $\sigma \models SP_t(\bigwedge_i \varphi_i, P')$, where t denotes the final label of P'. By definition of SP we thus have for some state σ' and sequence of communications θ that $\sigma' \models \bigwedge_i \varphi_i$ and $(\sigma', \sigma, \theta) \in \mathcal{O}_t(P)$. Since $P'_1 \| \ldots \| P'_n$ contains no external channels, by the correctness of $\mathcal{O}$ (Theorem 15.7) we obtain that $\sigma \in \mathcal{M}[\![P']\!]\sigma'$. Furthermore observe that since $\bigwedge_i \varphi_i$ implies φ, $\sigma' \models \varphi$. Now the validity of $\{\varphi\}P\{\psi\}$ implies that of $\{\varphi\}P'\{\psi\}$, since the auxiliary variables h_i do not occur in φ, ψ. So we conclude that $\sigma \models \psi$.

■

As a consequence we have proved the following theorem.

Theorem 16.9 (Semantic Completeness)
The proof method of Apt, Francez & de Roever is semantically complete. □