4 Soundness and Completeness

In general, if a proof method is presented to establish properties of systems, then there are two basic questions which have to be considered.

- Is the proof method *sound*, that is, does *every* property which is proved using the method always hold? That is, is it a *valid* property?
- Is the method *complete*, that is, is it adequate for proving *any* valid property of the system?

We shall prove in the following sections that Floyd's inductive assertion method for sequential programming is sound and that it is complete in a restricted sense (since by Gödel's theorem no proof system for establishing validity of verification conditions exists).

4.1 Soundness

First we prove soundness of the inductive assertion method, i.e.,

Theorem 4.1 (Soundness of the inductive assertion method)
Let $P = (L, T, s, t)$. If $\mathcal{Q}$ is an inductive assertion network for P, $\models \varphi \rightarrow \mathcal{Q}_s$, and $\models \mathcal{Q}_t \rightarrow \psi$, then P is partially correct w.r.t. $< \varphi, \psi >$, i.e., $\models \{\varphi\}\ P\ \{\psi\}$ holds.

The proof of this theorem follows from Lemmas 4.2 and 4.3.

Lemma 4.2 Let $P = (L, T, s, t)$. If $\mathcal{Q}$ is an inductive assertion network for P then this assertion network is invariant for P.

Proof
Consider an execution sequence $\langle l_0; \sigma_0 \rangle \longrightarrow \langle l_1; \sigma_1 \rangle \longrightarrow \ldots$ of P, with $l_0 = s$ and $\models \mathcal{Q}_s(\sigma_0)$. From the definition of execution sequence there exists a sequence of instructions $c_0 \rightarrow f_0, c_1 \rightarrow f_1, \ldots$ such that for every $j \geq 0$, $(l_j, c_j \rightarrow f_j, l_{j+1}) \in T$, $c_j(\sigma_j) = tt$, and $\sigma_{j+1} = f_j(\sigma_j)$. We prove by induction on j that $\mathcal{Q}_j(\sigma_j) = tt$, where $\mathcal{Q}_j$ denotes the predicate associated with location l_j. The case that $j = 0$ follows immediately from $\models \mathcal{Q}_s(\sigma_0)$. Next we assume that we already have $\mathcal{Q}_j(\sigma_j) = tt$. Let $\pi_{j+1} \stackrel{\text{def}}{=} (l_j, c_j \rightarrow f_j, l_{j+1})$. Since the network is inductive, we know that the validity of $V_{\pi_{j+1}}$ holds for σ_j. Thus we have that

$$\models (\mathcal{Q}_j \wedge c_j \rightarrow (\mathcal{Q}_{j+1} \circ f_j))(\sigma_j),$$

by our induction hypothesis $\mathcal{Q}_j(\sigma_j) = tt$. Since the computation starting with σ_j at l_j did follow the transition π_{j+1}, the necessary condition for the existence of a π_{j+1} transition, c_j, must certainly hold. Thus we conclude that $(\mathcal{Q}_{j+1} \circ f_j)(\sigma_j)$ must also hold. On the other hand, σ_{j+1} is the state obtained from

σ_j by the transition π_{j+1} so that $\sigma_{j+1} = f_j(\sigma_j)$. Consequently it follows that $\mathcal{Q}_{j+1}(\sigma_{j+1}) = tt$.

■

Lemma 4.3 follows easily from the definitions.

Lemma 4.3 Let $P = (L, T, s, t)$. If $\mathcal{Q}$ is an invariant network for P, and $\models \varphi \rightarrow \mathcal{Q}_s$ and $\models \mathcal{Q}_t \rightarrow \psi$ hold, then P is partially correct w.r.t. $< \varphi, \psi >$, i.e., $\models \{\varphi\}\ P\ \{\psi\}$ holds.

■

Let us step back for an overview of the advantages offered by the inductive assertion method. At first glance it seems that we have complicated matters. Starting with the need to prove that all φ-computations satisfy ψ when they reach the exit location t, we have complicated the task by, e.g., also requiring a proof that when such computations reach any other location l, they must satisfy $\mathcal{Q}_l$. On the other hand, in general the $\varphi - \psi$ relationship has to be established for an *infinite* number of computations including a computation that goes exactly once around some loop, one that goes twice around that loop, etc. We have to consider more assertions to be verified, but over a *finite* number of transitions.

4.2 Semantic Completeness of the Inductive Assertion Method

Next we consider completeness of the inductive assertion method, i.e., we prove:

Theorem 4.4 (Semantic completeness)
Let $P = (L, T, s, t)$. If P is partially correct w.r.t. $< \varphi, \psi >$ then there exists an inductive assertion network $\mathcal{Q}$ for P s.t. $\models \varphi \rightarrow \mathcal{Q}_s$ and $\models \mathcal{Q}_t \rightarrow \psi$ hold. Moreover, for any invariant assertion network Ψ for P with $\models \varphi \rightarrow \Psi_s$ one has $\models \mathcal{Q}_l \rightarrow \Psi_l$ for all $l \in L$.

Proof
Assume P is partially correct w.r.t. $< \varphi, \psi >$. Then apply the inductive assertion method as follows:

- Let $\mathcal{Q}$ be the following assertion network for P: For each $l \in L$, we define a predicate $\mathcal{Q}_l$ such that for all $\sigma \in \Sigma$, $\models \mathcal{Q}_l(\sigma)$ *iff there exists a state* σ' *s.t.* $\models \varphi(\sigma')$ *and* $\langle s; \sigma' \rangle \longrightarrow^* \langle l; \sigma \rangle$. Here $\longrightarrow^*$ denotes the reflexive and transitive closure of the transition relation $\longrightarrow$ between configurations. By the definition of invariance of a network we immediately obtain for each invariant assertion network Ψ for P that if $\models \varphi \rightarrow \Psi_s$ holds, then $\models \mathcal{Q}_l \rightarrow \Psi_l$ holds, for each $l \in L$.

- We show that $\mathcal{Q}$ as defined above is an inductive assertion network. Consider a transition $\pi = (l, a, l')$, with $a = c \rightarrow f$. We have to prove $\models \mathcal{Q}_l \wedge c \rightarrow \mathcal{Q}_{l'} \circ f$. Let σ be a state such that $\models \mathcal{Q}_l(\sigma)$ and $\models c(\sigma)$. From $\models \mathcal{Q}_l(\sigma)$ we obtain that $\langle s; \sigma' \rangle \longrightarrow^* \langle l; \sigma \rangle$, for some initial state σ' which satisfies φ. Since $\models c(\sigma)$ there exists a computation step $\langle l; \sigma \rangle \longrightarrow \langle l'; f(\sigma) \rangle$. So we have $\langle s; \sigma' \rangle \longrightarrow^* \langle l'; f(\sigma) \rangle$, and thus by definition of $\mathcal{Q}_{l'}$ we conclude $\models \mathcal{Q}_{l'}(f(\sigma))$.

- We prove $\models \varphi \rightarrow \mathcal{Q}_s$ and $\models \mathcal{Q}_t \rightarrow \psi$.
  - Consider σ s.t. $\models \varphi(\sigma)$ holds. Since $\langle s;\sigma\rangle \longrightarrow^* \langle s;\sigma\rangle$, it follows immediately from the definition of $\mathcal{Q}_s$ that $\models \mathcal{Q}_s(\sigma)$ holds.
  - Let σ be such that $\models \mathcal{Q}_t(\sigma)$. From the definition of $\mathcal{Q}_t$ it then follows that $\sigma \in \mathcal{M}[\![P]\!](\sigma')$, for some σ' such that $\models \varphi(\sigma')$. Since P is partially correct w.r.t. $< \varphi, \psi >$ this leads to $\models \psi(\sigma)$.

■

In the above proof the so-called *reachability* predicates $\mathcal{Q}_l$ are characterised mathematically, and not by means of assertions in, e.g., first-order predicate logic. When formalising the inductive assertion method within some logical system such as Hoare logic – a necessary prerequisite for machine-checked proofs – it is mandatory to express $\mathcal{Q}_l$ by such an assertion. This is done by encoding computations within the standard model of the natural numbers using a technique called *Gödel encoding* [Göd31]. This explains why we are especially interested in transition diagrams over an underlying data domain which contains this standard model (or, alternatively, in proof methods in which all valid properties in this standard model have been added as axioms). Unfortunately, there exists no complete formal system for proving the verification conditions for such diagrams, and consequently there is no hope of obtaining a complete formal system for proving the correctness of such diagrams. (By a proof in a formal proof system we understand a finite sequence of formulae each of which is either an axiom of that system or obtained by applications of one of its inference rules to formulae which occur earlier in that sequence.)

In the above proof we have established *semantic completeness*, i.e., we have proved the existence of an assertion network $\mathcal{Q}$ such that all the associated verification conditions, plus $\models \varphi \rightarrow \mathcal{Q}_s$ and $\models \mathcal{Q}_t \rightarrow \psi$ hold. We did not express those predicates as assertions from first-order predicate logic. Rather, we gave a semantical description of their meaning.

It is important to observe that Theorem 4.4 does not claim that one can *prove* the verification conditions for P w.r.t. $\mathcal{Q}$ and prove $\models \varphi \rightarrow \mathcal{Q}_s$ and $\models \mathcal{Q}_t \rightarrow \psi$ within a formal proof system, e.g., using the axioms and rules for first-order predicate logic over the natural numbers. It merely states that these verification conditions and these implications are *valid*. By Gödel's incompleteness result [Göd31], no complete proof system exists for proving these verification conditions over the natural numbers.

We can construct for every $\mathcal{Q}_l$ a corresponding assertion from first-order predicate logic which has the same meaning as $\mathcal{Q}_l$. Having obtained such assertions, we have established another kind of completeness, called *relative* completeness. Relative completeness of a proof method implies that there exist proofs for every valid correctness statement, provided all valid assertions *over the underlying data domain* (or interpretation), *which is assumed to contain the standard model of the natural numbers*, are assumed as axioms.

This implies in the case of Theorem 4.4 that we may assume that every (valid) verification condition plus the (valid) implications $\varphi \rightarrow \mathcal{Q}_0$ and $\mathcal{Q}_t \rightarrow \psi$ can be used as axioms.

References

[Göd31] K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.