3 A Proof Method for Partial Correctness

3.1 Definition plus Example

The proof method presented here for establishing partial correctness is called the *inductive assertion method* [Flo67].

Given a program $P = (L, T, s, t)$, we define the following concepts:

- An *assertion network for* P is a function $\mathcal{Q}$ which associates to each location $l \in L$ a predicate $\mathcal{Q}_l$, sometimes expressed by $\mathcal{Q}(l)$.
- Given an assertion network $\mathcal{Q}$ for P and a transition $\pi = (l, a, l')$, with $a = c \to f$, define the *verification condition* V_π along π by

$$V_\pi \stackrel{\text{def}}{=} \mathcal{Q}_l \wedge c \to \mathcal{Q}_{l'} \circ f.$$

  The operation $\circ$ denotes functional composition, that is, $f \circ g$ denotes the function resulting from applying f after g. We use the binding convention that the operator $\circ$ binds stronger than the boolean operators, and that $\wedge$ has priority over $\to$. For later use we define $V(P, \mathcal{Q})$ as *the set of verification conditions associated by* $\mathcal{Q}$ *with* P*:*

$$V(P, \mathcal{Q}) \stackrel{\text{def}}{=} \{\mathcal{Q}_l \wedge c \to \mathcal{Q}_{l'} \circ f | (l, c \to f, l') \in T\}.$$

- An assertion network for P is said to be *inductive* if all verification conditions in $V(P, \mathcal{Q})$ are valid.
- An assertion network $\mathcal{Q}$ for P is said to be an *invariant network* if for every computation $\langle l_0; \sigma_0\rangle \longrightarrow \langle l_1; \sigma_1\rangle \longrightarrow \ldots$ of P with $l_0 = s$ and $\models \mathcal{Q}_s(\sigma_0)$ we have that $\models \mathcal{Q}_{l_i}(\sigma_i)$.
- An inductive assertion network $\mathcal{Q}$ is called *consistent* or *correct* w.r.t. $\langle \varphi, \psi\rangle$ if the additional verification conditions $\models \varphi \to \mathcal{Q}_s$ and $\models \mathcal{Q}_t \to \psi$ hold.

In many of the examples in this book we use as a particular convention that the set of labels L is enumerated in order to facilitate the definition of assertion networks by associating label l_i with predicate $\mathcal{Q}_i$. In this set up, $l_0 = s$ and the label with the highest index l_n stands for exit node t.

Example 3.1 To illustrate these concepts let us consider Figure 3 showing the program *Introot* for computing the integer square root of a nonnegative integer input y_1, and assigning it to y_2, where l_0 represents s, and l_3 represents t.

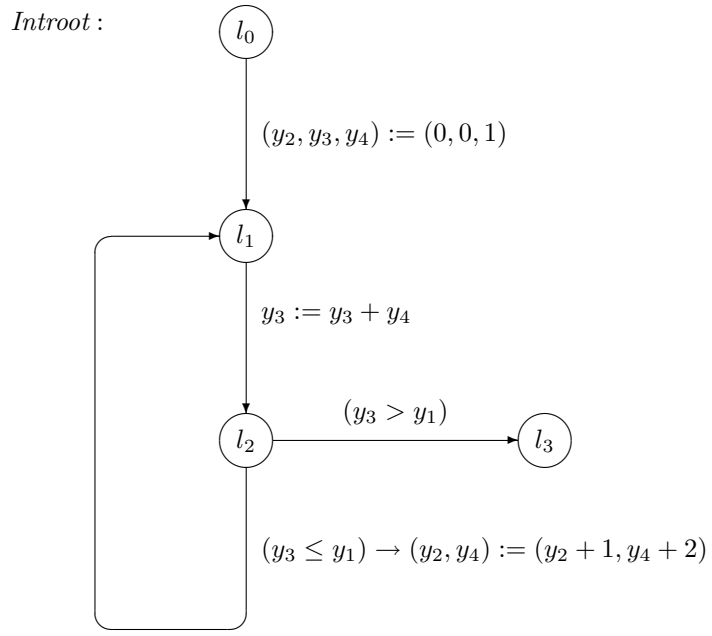

Figure 3: The program *Introot* for finding the integer root of y_1 and outputting the value of this root in y_2.

Assume the assertion network $\mathcal{Q}$ associates the predicates $\mathcal{Q}_0$, $\mathcal{Q}_1$, $\mathcal{Q}_2$, $\mathcal{Q}_3$ with the locations l_0, l_1, l_2, l_3, respectively. Corresponding to the four transitions

$$\begin{aligned}\pi_1 &: l_0 \rightarrow l_1\\ \pi_2 &: l_1 \rightarrow l_2\\ \pi_3 &: l_2 \rightarrow l_1\\ \pi_4 &: l_2 \rightarrow l_3\end{aligned}$$

there are four verification conditions to be checked. Consider first π_1. Its verification condition is given by:

$$V_{\pi_1}: \ \mathcal{Q}_0(y_1, y_2, y_3, y_4) \rightarrow \mathcal{Q}_1(y_1, 0, 0, 1).$$

Analogously, the verification conditions for the other transitions are derived:

$$\begin{aligned}V_{\pi_2}: &\ \mathcal{Q}_1(y_1, y_2, y_3, y_4) \rightarrow \mathcal{Q}_2(y_1, y_2, y_3 + y_4, y_4)\\ V_{\pi_3}: &\ \mathcal{Q}_2(y_1, y_2, y_3, y_4) \wedge (y_3 \leq y_1) \rightarrow \mathcal{Q}_1(y_1, y_2 + 1, y_3, y_4 + 2)\\ V_{\pi_4}: &\ \mathcal{Q}_2(y_1, y_2, y_3, y_4) \wedge (y_3 > y_1) \rightarrow \mathcal{Q}_3(y_1, y_2, y_3, y_4).\end{aligned}$$ □

Next we formulate Floyd's inductive assertion method for proving transition diagrams partially correct.

3.2 Floyd's Inductive Assertion Method

To prove $\models \{\varphi\}\ P\ \{\psi\}$, i.e., that a transition system P is partially correct w.r.t. a given specification $< \varphi, \psi >$, we use:

Definition 3.2 (Floyd's inductive assertion method)

1. Give an assertion network $\mathcal{Q}$ for P.
2. Prove that this assertion network is inductive, that is, for each transition (l, a, l') of P prove validity of its associated verification condition

$$\mathcal{Q}_l \wedge c \rightarrow \mathcal{Q}_{l'} \circ f,$$

   assuming that $a = c \rightarrow f$.
3. Prove that $\mathcal{Q}$ is consistent with $\langle \varphi, \psi \rangle$, i.e., that the additional verification conditions $\models \varphi \rightarrow \mathcal{Q}_s$ and $\models \mathcal{Q}_t \rightarrow \psi$ are valid. □

Example 3.3 (Continuation of Example 3.1) Consider the program *Introot* for integer root finding. We prove $\models \{y_1 \geq 0\}$ *Introot* $\{y_2^2 \leq y_1 < (y_2+1)^2\}$ using Floyd's method. Take the assertion network defined by:

$$\begin{aligned}
&\mathcal{Q}_0(\bar{y}) \stackrel{\text{def}}{=} y_1 \geq 0\\
&\mathcal{Q}_1(\bar{y}) \stackrel{\text{def}}{=} (y_2^2 \leq y_1) \wedge (y_3 = y_2^2) \wedge (y_4 = 2 * y_2 + 1)\\
&\mathcal{Q}_2(\bar{y}) \stackrel{\text{def}}{=} (y_2^2 \leq y_1) \wedge (y_3 = (y_2+1)^2) \wedge (y_4 = 2 * y_2 + 1)\\
&\mathcal{Q}_3(\bar{y}) \stackrel{\text{def}}{=} y_2^2 \leq y_1 < (y_2+1)^2.
\end{aligned}$$

We first show that this network is inductive.

Substituting the predicates $\mathcal{Q}_0$ and $\mathcal{Q}_1$ into V_{π_1} we must prove its validity:

$$\models (y_1 \geq 0) \rightarrow (0 \leq y_1) \wedge (0 = 0) \wedge (1 = 0 + 1)$$

is trivially valid.

Similarly for V_{π_2}:

$$\begin{aligned}
\models\ & (y_2^2 \leq y_1) \wedge (y_3 = y_2^2) \wedge (y_4 = 2 * y_2 + 1) \rightarrow\\
& (y_2^2 \leq y_1) \wedge (y_3 + y_4 = (y_2+1)^2) \wedge (y_4 = 2 * y_2 + 1).
\end{aligned}$$

Notice that $y_2^2 \leq y_1$ and $y_4 = 2 * y_2 + 1$ appear both in the antecedent and the consequent. Hence we show:

$$\models (y_3 = y_2^2) \wedge (y_4 = 2 * y_2 + 1) \rightarrow (y_3 + y_4 = (y_2+1)^2).$$

Substituting y_2^2 for y_3 and $2 * y_2 + 1$ for y_4 in the consequent we obtain

$$y_2^2 + 2 * y_2 + 1 = (y_2+1)^2,$$

which is obviously correct.

Next consider the validity of V_{π_3}:

$$\begin{aligned}
\models\ & (y_2^2 \leq y_1) \wedge (y_3 = (y_2+1)^2) \wedge (y_4 = 2 * y_2 + 1) \wedge (y_3 \leq y_1) \rightarrow\\
& ((y_2+1)^2 \leq y_1) \wedge (y_3 = (y_2+1)^2) \wedge (y_4 + 2 = 2 * (y_2+1) + 1).
\end{aligned}$$

One has that $((y_2+1)^2 \leq y_1)$ in the consequent follows from $y_3 = (y_2+1)^2$ and $y_3 \leq y_1$ in the antecedent, and hence this is a valid statement.

Finally, consider the validity of V_{π_4}:

$$\begin{aligned}
\models\ & (y_2^2 \leq y_1) \wedge (y_3 = (y_2+1)^2) \wedge (y_4 = 2 * y_2 + 1) \wedge (y_3 > y_1) \rightarrow\\
& (y_2^2 \leq y_1 < (y_2+1)^2).
\end{aligned}$$

The first conjunct of the consequent is $y_2^2 \leq y_1$ which already appears in the antecedent. The second conjunct $y_1 < (y_2+1)^2$ is a consequence of $y_3 = (y_2+1)^2$ and $y_3 > y_1$ – both appearing in the antecedent.

This establishes that $\mathcal{Q}_0, \mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3$ as defined above constitute an inductive assertion network . We will see that they are also *invariant assertions* (forming an invariant network). Thus, whenever an execution which started with $y_1 \geq 0$ reaches the point l_2 in the program,

$$\mathcal{Q}_2 \stackrel{\text{def}}{=} (y_2^2 \leq y_1) \wedge (y_3 = (y_2+1)^2) \wedge (y_4 = 2 * y_2 + 1)$$

must be true invariantly of the current values of the program variables. And, if we ever reach l_3, we are assured by $\mathcal{Q}_3$ that y_1 lies between y_2^2 and $(y_2+1)^2$ or equals y_2^2, in other words, y_2 is the best integer approximation from below to the square root of y_1, i.e., $y_2 = \lfloor \sqrt{y_1} \rfloor$.
In order to prove $\models \{y_1 \geq 0\} \mathit{Introot} \{y_2^2 \leq y_1 < (y_2+1)^2\}$ we must additionally prove $\models y_1 \geq 0 \rightarrow \mathcal{Q}_0$ and $\models \mathcal{Q}_3 \rightarrow y_2^2 \leq y_1 < (y_2+1)^2$, which are in this case obviously true. □

References

[Flo67] R.W. Floyd. Assigning meanings to programs. In *Proceedings AMS Symposium Applied Mathematics*, volume 19, pages 19–31, Providence, R.I., 1967. American Mathematical Society.