# Lecture #25: Axiomatic Semantics

## CS 6371: Advanced Programming Languages

Consider the following SIMPL program, which computes $y$ to be the sum of $1..x$:

$$w = (\texttt{while } 1\texttt{<=}x \texttt{ do } (y\texttt{:=}y\texttt{+}x; x\texttt{:=}x\texttt{-}1))$$

We wish to prove the partial-correctness of program $w$. That is, we wish to prove the following partial-correctness assertion:

$$\{(x = \bar{n}) \wedge (\bar{n} \geq 1) \wedge (y = 0)\}w\{y = \tfrac{1}{2}\bar{n}(\bar{n} + 1)\}$$

The first step is to find a suitable loop invariant $I$ for the while-loop. Suitable loop invariants always satisfy three criteria:

1. $I$ must be valid at the start of the loop.
2. Executing the loop body in *any* state where $I$ and the loop condition are both valid *always* results in a state where $I$ is still valid.
3. $I$ conjoined with the *negation* of the loop condition must imply the postcondition.

If you choose an invariant that is too weak, it will not be strong enough to prove the postcondition and condition 3 will fail. If you choose one that is too strong, it will be falsified on some loop iterations and conditions 1 or 2 will fail.

For example, suppose we choose $y = \frac{1}{2}\bar{n}(\bar{n} + 1)$ as our invariant. This is clearly strong enough to prove the postcondition (since it is identical to the postcondition) but it is not valid on every iteration. Instead, we might try $y = \frac{1}{2}\bar{n}(\bar{n} + 1) - \frac{1}{2}x(x + 1)$. This is valid on every iteration but it is not quite strong enough to prove the postcondition. To prove the postcondition we would also need to know that $x = 0$ at the end of the loop. The negation of the loop condition is $x < 1$, so to infer that $x = 0$ we need only combine this with $x \geq 0$. This leads us to the invariant $I \equiv ((x \geq 0) \wedge (y = \frac{1}{2}\bar{n}(\bar{n} + 1) - \frac{1}{2}x(x + 1)))$, which satisfies all three criteria.

Armed with this invariant, we can begin our proof as follows:

$$\dfrac{\models A_1 \qquad \dfrac{\dfrac{\mathcal{D}}{\{I \wedge (1 \leq x)\}y\texttt{:=}y\texttt{+}x; x\texttt{:=}x\texttt{-}1\{I\}}}{\{I\}w\{\neg(1 \leq x) \wedge I\}}(5) \qquad \models A_2}{\{(x = \bar{n}) \wedge (\bar{n} \geq 1) \wedge (y = 0)\}w\{y = \frac{1}{2}\bar{n}(\bar{n} + 1)\}}(6)$$

where assertions $A_1$ and $A_2$ are defined by

$$A_1 \equiv (x = \bar{n}) \wedge (\bar{n} \geq 1) \wedge (y = 0) \Longrightarrow I$$
$$A_2 \equiv \neg(1 \leq x) \wedge I \Longrightarrow (y = \tfrac{1}{2}\bar{n}(\bar{n} + 1))$$

(You should convince yourself that $A_1$ and $A_2$ are both tautological before continuing.)

Next we must fill in derivation $\mathcal{D}$. Rule 2 says that to prove a partial-correctness assertion involving a sequence of commands, we must find an assertion $C$ that can serve as a postcondition for the first command and a precondition for the second. So we want a derivation of the form:

$$\mathcal{D} = \frac{\dfrac{\mathcal{D}_1}{\{I \wedge (1 \leq x)\} y := y + x \{C\}} \qquad \dfrac{\mathcal{D}_2}{\{C\} x := x - 1 \{I\}}}{\{I \wedge (1 \leq x)\} y := y + x ; x := x - 1 \{I\}} (2)$$

for some assertion $C$. If we use Rule 4 to complete sub-derivation $\mathcal{D}_2$, then $C$ must be

$$C \equiv I[x - 1/x] \equiv (x - 1 \geq 0) \wedge (y = \tfrac{1}{2}\bar{n}(\bar{n} + 1) - \tfrac{1}{2}(x - 1)(x - 1 + 1))$$

To complete the proof, we only need to finish derivation $\mathcal{D}_1$ for our chosen $C$. Rule 4 says that if the postcondition is $C$ then the precondition must be $C' \equiv C[y + x/y] \equiv (x - 1 \geq 0) \wedge (y + x = \frac{1}{2}\bar{n}(\bar{n} + 1) - \frac{1}{2}(x - 1)(x - 1 + 1))$. Completing the proof therefore requires using the rule of consequence to show that $I \wedge (1 \leq x)$ implies $C'$:

$$\mathcal{D}_1 = \frac{\models A_3 \qquad \overline{\{C'\} y := y + x \{C\}}^{(4)} \qquad \models C \Rightarrow C}{\{I \wedge (1 \leq x)\} y := y + x \{C\}} (6)$$

where assertion $A_3$ is given by

$$A_3 \equiv I \wedge (1 \leq x) \Longrightarrow C'$$

(Once again, you should convince yourself that this assertion is really valid.)

The final proof therefore looks like this:

$$\frac{\models A_1 \qquad \dfrac{\dfrac{\dfrac{\models A_3 \qquad \overline{\{C'\} y := y + x \{C\}}^{(4)} \qquad \models C \Rightarrow C}{\{I \wedge (1 \leq x)\} y := y + x \{C\}} (6) \qquad \overline{\{C\} x := x - 1 \{I\}}^{(4)}}{\{I \wedge (1 \leq x)\} y := y + x ; x := x - 1 \{I\}} (2)}{\{I\} w \{\neg(1 \leq x) \wedge I\}} (5) \qquad \models A_2}{\{(x = \bar{n}) \wedge (\bar{n} \geq 1) \wedge (y = 0)\} w \{y = \frac{1}{2}\bar{n}(\bar{n} + 1)\}} (6)$$

where assertions $I$, $C$, $C'$, $A_1$, $A_2$, and $A_3$ are defined by:

$$\begin{aligned}
I &\equiv (x \geq 0) \wedge (y = \tfrac{1}{2}\bar{n}(\bar{n} + 1) - \tfrac{1}{2}x(x + 1)) \\
C &\equiv (x - 1 \geq 0) \wedge (y = \tfrac{1}{2}\bar{n}(\bar{n} + 1) - \tfrac{1}{2}(x - 1)(x - 1 + 1)) \\
C' &\equiv (x - 1 \geq 0) \wedge (y + x = \tfrac{1}{2}\bar{n}(\bar{n} + 1) - \tfrac{1}{2}(x - 1)(x - 1 + 1)) \\
A_1 &\equiv (x = \bar{n}) \wedge (\bar{n} \geq 1) \wedge (y = 0) \Longrightarrow I \\
A_2 &\equiv \neg(1 \leq x) \wedge I \Longrightarrow (y = \tfrac{1}{2}\bar{n}(\bar{n} + 1) - \tfrac{1}{2}x(x + 1)) \\
A_3 &\equiv I \wedge (1 \leq x) \Longrightarrow C'
\end{aligned}$$