Completeness of Axiomatic Semantics

(Supplement to CS263 Lecture Notes)

George Necula

September 26, 2001

We proved in class that the set of Hoare axioms is sound, that is, whenever $\vdash \{A\}\, c\, \{B\}$ we have that $\models \{A\}\, c\, \{B\}$.

In this note, I am going to show a proof of completeness of the axiom system. The goal is to show that if a triple is valid then there is a derivation for it:

$$\vdash \{A\}\, c\, \{B\} \quad \Rightarrow \quad \models \{A\}\, c\, \{B\}$$

A proof of completeness can also be found in Winskel's but for a definition of $\models \{A\}\, c\, \{B\}$ using denotational semantics. I am showing here a proof using operational semantics. The proof here is a little trickier because the operational semantics is not compositional.

1 Weakest Preconditions

A typical strategy for proving the completeness of a set of Hoare axioms is to introduce the notion of *weakest preconditions*. The weakest precondition of a command c with respect to a postcondition B, written $wp(c, b)$, is the assertion satisfied exactly by those initial states that lead c either to non-termination or to a final state that satisfies the postcondition B. It should be clear by this definition that the weakest precondition is unique up to equivalence of assertions.

We define the weakest preconditions inductively on the structure of commands, as follows:

$$\begin{array}{lcl}
wp(\texttt{skip}, B) & = & B \\
wp(x := e, B) & = & B[e/x] \\
wp(c_1; c_2, B) & = & wp(c_1, wp(c_2, B)) \\
wp(\texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2, B) & = & b \Rightarrow wp(c_1, B) \wedge \neg b \Rightarrow wp(c_2, B) \\
wp(\texttt{while}\ b\ \texttt{do}\ c, B) & = & \bigwedge_i F^i_{b,c,B}(\texttt{true})
\end{array}$$

where $F_{b,c,B}$ is defined as:

$$F_{b,c,B}(A) = b \Rightarrow wp(c, A) \wedge \neg b \Rightarrow B$$

In the rest of this note I will drop the subscripts from $F_{b,c,B}$ because they are easy to infer from the context. As discussed in class, the above form of the weakest precondition for the looping construct was chosen so that the following equivalence holds:

$$wp(\texttt{while}\ b\ \texttt{do}\ c, B) \equiv b \Rightarrow wp(c, wp(\texttt{while}\ b\ \texttt{do}\ c, B)) \wedge \neg b \Rightarrow B$$

It is important to note that $\bigwedge_i F^i(\texttt{true})$ is not a legal assertion in our assertion language. However, as it is proved in Winskel's, if the language of assertions contains multiplication, then there exists an equivalent legal assertion. Note that if the language of assertions contains only multiplication with constants (Presburger arithmetic), then it is not true that we can express all weakest preconditions! The proofs of these facts are beyond the scope of the course and of this note.

Now we are going to prove formally that the inductive definition of wp above agrees with our informal meaning of the weakest precondition. We state the required properties as two lemmas. Before we turn to the proofs of these lemmas we show how they can be used to derive the completeness of the axiom system.

Lemma 1 (wp is a precondition) *For any command c and assertion B, we have that $\vdash \{\, wp(c, B) \,\}\, c \,\{\, B \,\}$, provided that the derivation of assertions is complete, i.e., $\vdash A$ whenever $\models A$.*

Lemma 2 (wp is the weakest precondition) *For any command c, assertion B, and states σ and σ', if $\langle \sigma, c \rangle \Downarrow \sigma'$ and $\sigma' \models B$ then we have that $\sigma \models wp(c, B)$.*

Corollary 1 (Completeness) *For any command c and assertions A and B, if the derivation of assertions is complete and $\models \{\, A \,\}\, c \,\{\, B \,\}$ then $\vdash \{\, A \,\}\, c \,\{\, B \,\}$.*

Proof of Corollary 1: If $\models \{\, A \,\}\, c \,\{\, B \,\}$ then for any state $\sigma \models A$ we have (from Lemma 2) that $\sigma \models wp(c, B)$. Hence, by the definition of $\models$, we have that $\models A \Rightarrow wp(c, B)$. Now because we assume our derivation system for assertions (not triples) to be complete, there must exist a derivation $\mathcal{D}_1 :: \vdash A \Rightarrow wp(c, b)$.

From Lemma 1 we have that there exists a derivation $\mathcal{D}_2 :: \vdash \{\, wp(c, B) \,\}\, c \,\{\, B \,\}$. Now using the rule of consequence we can build the derivation $\mathcal{D}$:

$$\mathcal{D} :: \frac{\begin{array}{cc} \mathcal{D}_1 & \mathcal{D}_2 \\ \vdash A \Rightarrow wp(c, B) & \vdash \{\, wp(c, B) \,\}\, c \,\{\, B \,\} \end{array}}{\vdash \{\, A \,\}\, c \,\{\, B \,\}}$$

whose existence proves the corollary.

$\square$

Now we turn to proving the two key lemmas about the weakest preconditions.

PROOF OF LEMMA 1: Pick an arbitrary command c. We have to show that there exists a derivation of $\vdash \{ wp(c, B) \} \, c \, \{ B \}$. The proof is by induction on the structure of the command c.

Case: $c = \texttt{skip}$. We have to show that $\vdash \{ B \} \, \texttt{skip} \, \{ B \}$. This is an immediate instance of the `skip` axiom.

Case: $c = x := e$. We have to show that $\vdash \{ [e/x]B \} \, x := e \, \{ B \}$. This is again an instance of the assignment axiom.

Case: $c = c_1; c_2$. We must show that $\vdash \{ wp(c_1, wp(c_2, B)) \} \, c_1; c_2 \, \{ B \}$. By induction hypothesis on c_1 and c_2 we have that the derivations $\mathcal{D}_2 :: \vdash \{ wp(c_2, B) \} \, c_2 \, \{ B \}$ and $\mathcal{D}_1 :: \vdash \{ wp(c_1, wp(c_2, B)) \} \, c_1 \, \{ wp(c_2, B) \}$ exist. Now we can use the rule of sequencing to build the required derivation:

$$\mathcal{D} :: \frac{\begin{array}{c}\mathcal{D}_1 \\ \vdash \{ wp(c_1, wp(c_2, B)) \} \, c_1 \, \{ wp(c_2, B) \}\end{array} \quad \begin{array}{c}\mathcal{D}_2 \\ \vdash \{ wp(c_2, B) \} \, c_2 \, \{ B \}\end{array}}{\vdash \{ wp(c_1, wp(c_2, B)) \} \, c_1; c_2 \, \{ B \}} \, \texttt{seq}$$

Case: $c = \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2$. Let $W = b \Rightarrow wp(c_1, B) \land \neg b \Rightarrow wp(c_2, B)$. We have to show that

$$\mathcal{D} :: \vdash \{ W \} \, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \, \{ B \}$$

If we have the derivations $\mathcal{D}_1$, $\mathcal{D}_1'$, $\mathcal{D}_2$ and $\mathcal{D}_2'$ we can build $\mathcal{D}$ as follows:

$$\mathcal{D} = \frac{\dfrac{\begin{array}{c}\mathcal{D}_1 \\ \vdash W \land b \Rightarrow wp(c_1, B)\end{array} \quad \begin{array}{c}\mathcal{D}_1' \\ \vdash \{ wp(c_1, B) \} \, c_1 \, \{ B \}\end{array}}{\vdash \{ W \land b \} \, c_1 \, \{ B \}} \quad \dfrac{\begin{array}{c}\mathcal{D}_2 \\ \vdash W \land \neg b \Rightarrow wp(c_2, B)\end{array} \quad \begin{array}{c}\mathcal{D}_2' \\ \vdash \{ wp(c_2, B) \} \, c_2 \, \{ B \}\end{array}}{\vdash \{ W \land \neg b \} \, c_2 \, \{ B \}}}{\vdash \{ W \} \, \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \, \{ B \}} \, \texttt{if}$$

We can see that the existence of the derivations $\mathcal{D}_1'$ and $\mathcal{D}_2'$ is guaranteed by the induction hypothesis on c_1 and c_2 respectively. What remains to show is the existence of the derivations $\mathcal{D}_1$ and $\mathcal{D}_2$. I'll only show the existence of $\mathcal{D}_1$, the other case being similar.

It is sufficient to show that $\sigma \models W \wedge b \Rightarrow wp(c_1, B)$ for all $\sigma \in \Sigma$. Then, from the assumed completeness of the derivation system for assertions, we have the existence of $\mathcal{D}_1$.

Now pick an arbitrary σ such that $\sigma \models W \wedge b$. From the definition of W we notice that it must be the case that $\sigma \models wp(c_1, B)$, which is exactly what we need to complete this case of the proof.

Case: $c = \texttt{while}\ b\ \texttt{do}\ c$**.** As it has become the norm, the case for the looping construct is the most interesting one. Recall that

$$wp(\texttt{while}\ b\ \texttt{do}\ c, B) = W$$

such that $W \equiv b \Rightarrow wp(c, W) \wedge \neg b \Rightarrow B$. We have to show a derivation of $\vdash \{\, W \,\}\ \texttt{while}\ b\ \texttt{do}\ c\ \{\, B \,\}$. We can obtain such a derivation if we are able to show that derivations $\mathcal{D}_1$, $\mathcal{D}_2$ and $\mathcal{D}_3$ exist:

$$\mathcal{D} :: \quad \dfrac{\dfrac{\dfrac{\begin{matrix}\mathcal{D}_1 \\ \vdash W \wedge b \Rightarrow wp(c, W)\end{matrix} \quad \begin{matrix}\mathcal{D}_2 \\ \vdash \{\, wp(c, W) \,\}\, c\, \{\, W \,\}\end{matrix}}{\vdash \{\, W \wedge b \,\}\, c\, \{\, W \,\}}\ \texttt{cons}}{\vdash \{\, W \,\}\ \texttt{while}\ b\ \texttt{do}\ c\ \{\, W \wedge \neg b \,\}}\ \texttt{while} \qquad \begin{matrix}\mathcal{D}_3 \\ \vdash W \wedge \neg b \Rightarrow B\end{matrix}}{\vdash \{\, W \,\}\ \texttt{while}\ b\ \texttt{do}\ c\ \{\, B \,\}}\ \texttt{cons}$$

But $\mathcal{D}_2$ clearly exists because of the induction hypothesis on c.

We can also show, using the unwinding property of W, that $\models W \wedge b \Rightarrow wp(c, W)$ and also that $\models W \wedge \neg b \Rightarrow B$. From here we use the completeness of the derivation system for assertions and we obtain the required derivations $\mathcal{D}_1$ and $\mathcal{D}_3$ respectively.

This completes the proof of the Lemma 1.

$\square$

Proof of Lemma 2: The statement of Lemma 2 assumes the existence of an evaluation derivation $\mathcal{D} :: \langle \sigma, c \rangle \Downarrow \sigma'$. Since the evaluation judgment is not compositional we must immediately think of an induction on the structure of the evaluation judgment itself and not on the structure of the command.

Case: last rule in $\mathcal{D}$ is skip. We have in this case that $\sigma' = \sigma$ and that $wp(\texttt{skip}, B) = B$. Thus the desired conclusion $\sigma' \models wp(\texttt{skip}, B)$ follows directly from the assumption that $\sigma \models B$.

Case: last rule in $\mathcal{D}$ is assignment. We must prove that if $\sigma[x := n] \models B$ and $\langle \sigma, e \rangle \Downarrow n$ then $\sigma \models [e/x]B$. This is exactly the statement of the substitution lemma mentioned in class.

Case: last rule in $\mathcal{D}$ is the sequencing. In this case $\mathcal{D}$ has the following shape:

$$\mathcal{D} = \cfrac{\begin{array}{cc} \mathcal{D}_1 & \mathcal{D}_2 \\ \langle \sigma, c_1 \rangle \Downarrow \sigma' & \langle \sigma', c_2 \rangle \Downarrow \sigma'' \end{array}}{\langle \sigma, c_1; c_2 \rangle \Downarrow \sigma''} \ \texttt{seq}$$

We have the assumption $\sigma'' \models B$. From the induction hypothesis on $\mathcal{D}_2$ we have that $\sigma' \models wp(c_2, B)$ and then from the induction hypothesis on $\mathcal{D}_1$ we have that $\sigma \models wp(c_1, wp(c_2, B))$, which proves this case.

Case: last rule in $\mathcal{D}$ is while false. Thus $\mathcal{D}$ must be of the form:

$$\mathcal{D} = \cfrac{\begin{array}{c} \mathcal{D}_1 \\ \langle \sigma, b \rangle \Downarrow \texttt{false} \end{array}}{\langle \sigma, \texttt{while } b \texttt{ do } c \rangle \Downarrow \sigma} \ \texttt{whf}$$

Thus $\sigma' = \sigma$ and $\sigma \models B$ (by assumption). We must show that $\sigma \models W$, where W is the least solution to the fix-point equation

$$W \equiv b \Rightarrow wp(c, W) \wedge \neg b \Rightarrow B \tag{1}$$

To make progress we need to relate the evaluation of boolean expressions in a state to the satisfiability of the boolean expression (viewed as an assertion) in the given state. This is stated as Lemma 3 on page 6 and allows us to infer from $\mathcal{D}_1$ that $\sigma \models \neg b$ and hence that $\sigma \models \neg b \Rightarrow B$. It is then easy to show that $\sigma \models W$, which is what we have to show for this case of the proof. (This uses the fact that if $\sigma \models b$ then $\sigma \models \neg b \Rightarrow A$ for any assertion A.)

Case: last rule in $\mathcal{D}$ is while true. In this case $\mathcal{D}$ has the following shape:

$$\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_1 \\ \langle \sigma, b\rangle \Downarrow \texttt{true}\end{array} \quad \dfrac{\begin{array}{c}\mathcal{D}_2 \\ \langle \sigma, c\rangle \Downarrow \sigma''\end{array} \quad \begin{array}{c}\mathcal{D}_3 \\ \langle \sigma'', \texttt{while}\ b\ \texttt{do}\ c\rangle \Downarrow \sigma'\end{array}}{\langle \sigma, c; \texttt{while}\ b\ \texttt{do}\ c\rangle \Downarrow \sigma'}\ \texttt{seq}}{\langle \sigma, \texttt{while}\ b\ \texttt{do}\ c\rangle \Downarrow \sigma'}\ \texttt{wht}$$

Just as before, from $\mathcal{D}_1$ and Lemma 3 we have that $\sigma \models b$. Thus we need to prove that $\sigma \models wp(c, W)$. We first apply the induction hypothesis on $\mathcal{D}_3$ (with the assumption that $\sigma' \models B$) to deduce that $\sigma'' \models W$. Then, we use this as an assumption and we apply the induction hypothesis on $\mathcal{D}_2$ to deduce that $\sigma \models wp(c, W)$, which completes this case of the proof.

□

2 Helper Lemmas

Lemma 3

1. *If* $\langle \sigma, b\rangle \Downarrow \texttt{true}$ *then* $\sigma \models b$
2. *If* $\langle \sigma, b\rangle \Downarrow \texttt{false}$ *then* $\sigma \models \neg b$

PROOF OF LEMMA 3: The proof is easy by induction on the structure of the boolean expression b.

□