Axiomatic Semantics and Hoare-style Verification

Axiomatic semantics (or Hoare-style logic) defines the meaning of a statement in terms of its effects on assertions of truth that can be made about the associated program. A *Hoare Triple* encodes these assertions in the form $\{P\}S\{Q\}$ where P is the precondition, Q is the postcondition, and S is a piece of code of interest. Using derivation rules for Hoare triples, we can prove that these triples hold.

1. Prove $\{\texttt{x} > 1\}$ `x:=x+1; x:=-x` $\{\texttt{x} < 0\}$.

$$\dfrac{\vdash \texttt{x} > 1 \Rightarrow \texttt{x} + 1 > 2 \qquad \dfrac{\dfrac{}{\vdash \{\texttt{x}+1 > 2\}\ \texttt{x:=x+1}\ \{\texttt{x} > 2\}}\ \textit{assign} \qquad \dfrac{}{\vdash \{\texttt{x} > 2\}\ \texttt{x:=-x}\ \{-\texttt{x} > 2\}}\ \textit{assiqn}}{\vdash \{\texttt{x}+1 > 2\}\ \texttt{x:=x+1; x:=-x}\ \{-\texttt{x} > 2\}}\ \textit{seq} \qquad \vdash -\texttt{x} > 2 \Rightarrow \texttt{x} < 0}{\vdash \{\texttt{x} > 1\}\ \texttt{x:=x+1; x:=-x}\ \{\texttt{x} < 0\}}\ \textit{consq}$$

2. Prove that the program `x:=x+y; y:=x-y; x:=x-y` swaps the values of `x` and `y`. The conclusion should be:
$\{\texttt{x} = A \wedge \texttt{y} = B\}$ `x:=x+y; y:=x-y; x:=x-y` $\{\texttt{y} = A \wedge \texttt{x} = B\}$

   Let R be the derivation

$$\dfrac{\vdash \texttt{x} = A \wedge \texttt{y} = B \Rightarrow \texttt{x+y} = A + B \wedge \texttt{y} = B \qquad \dfrac{}{\vdash \{\texttt{x+y} = A + B \wedge \texttt{y} = B\}\ \texttt{x:=x+y}\ \{\texttt{x} = A + B \wedge \texttt{y} = B\}}\ \textit{assign} \qquad \vdash \texttt{x} = A + B \wedge \texttt{y} = B \Rightarrow \texttt{x} = A + B \wedge \texttt{x-y} = A}{\vdash \{\texttt{x} = A \wedge \texttt{y} = B\}\ \texttt{x:=x+y}\ \{\texttt{x} = A + B \wedge \texttt{x-y} = A\}}\ \textit{consq}$$

   Let S be the derivation

$$\dfrac{\vdash \texttt{x} = A + B \wedge \texttt{x-y} = A \Rightarrow \texttt{x} = A + B \wedge \texttt{x-y} = A \qquad \dfrac{}{\vdash \{\texttt{x} = A + B \wedge \texttt{x-y} = A\}\ \texttt{y:=x-y}\ \{\texttt{x} = A + B \wedge \texttt{y} = A\}}\ \textit{assign} \qquad \vdash \texttt{x} = A + B \wedge \texttt{y} = A \Rightarrow \texttt{x-y} = B \wedge \texttt{y} = A}{\vdash \{\texttt{x} = A + B \wedge \texttt{x-y} = A\}\ \texttt{y:=x-y}\ \{\texttt{x-y} = B \wedge \texttt{y} = A\}}\ \textit{consq}$$

   Let T be the derivation

$$\dfrac{}{\vdash \{\texttt{x-y} = B \wedge \texttt{y} = A\}\ \texttt{x:=x-y}\ \{\texttt{y} = A \wedge \texttt{x} = B\}}\ \textit{assign}$$

   Let U be the derivation

$$\dfrac{S \quad T}{\vdash \{\texttt{x} = A + B \wedge \texttt{x-y} = A\}\ \texttt{y:=x-y; x:=x-y}\ \{\texttt{y} = A \wedge \texttt{x} = B\}}\ \textit{seq}$$

   Putting these together, we then have the final derivation:

$$\dfrac{R \quad U}{\vdash \{\texttt{x} = A \wedge \texttt{y} = B\}\ \texttt{x:=x+y; y:=x-y; x:=x-y}\ \{\texttt{y} = A \wedge \texttt{x} = B\}}\ \textit{seq}$$