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

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

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:
$\{\mathtt{x} = A \wedge \mathtt{y} = B\}$ `x:=x+y; y:=x-y; x:=x-y` $\{\mathtt{y} = A \wedge \mathtt{x} = B\}$

Let R be the derivation

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

Let S be the derivation

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

Let T be the derivation

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

Let U be the derivation

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

Putting these together, we then have the final derivation:

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