Software Analysis & Verification **Due: May 12, 2020**

Homework 5

Instructor: Fei He
TA: Jianhui Chen, Fengmin Zhu

Chenhao Li (2017011466)

Read the instructions below carefully before you start working on the assignment:

- Please typeset your answers in the attached LaTeX source file, compile it to a PDF, and finally hand the PDF to Tsinghua Web Learning *before the due date*.
- Make sure you fill in your *name* and *Tsinghua ID*, and replace all "`TODO`"s with your solutions.
- Any kind of dishonesty is *strictly prohibited* in the full semester. If you refer to any material that is not provided by us, you *must cite* it.

Problem 1: Hoare Triples

Are the following Hoare triples valid? And why? Be careful to distinguish between partial correctness and total correctness.

1-1 $\{X = 0 \land Y = 1\}\ X := X + 1; Y := Y + 1\ \{X = 1 \land Y = 2\}$

Solution Yes.

$$\text{Seq}\dfrac{\text{Asgn}\dfrac{}{\{X = 0 \land Y = 1\}\ X := X + 1\ \{X = 1 \land Y = 1\}}\quad \text{Asgn}\dfrac{}{\{X = 1 \land Y = 1\}\ Y := Y + 1\ \{X = 1 \land Y = 2\}}}{\{X = 0 \land Y = 1\}\ X := X + 1; Y := Y + 1\ \{X = 1 \land Y = 2\}}$$

■

1-2 $\{\top\}$ while $X \leq 0$ do $X := X + 1$ end $\{X \geq 0\}$

Solution Yes.

- For starting environment satisfying $X \leq 0$, the while loop will proceed until condition $X \leq 0$ is violated, which implies $X \geq 0$.
- For starting environment satisfying $X > 0$, the while loop will terminate immediately, leaving X unchanged, thus satisfying $X \geq 0$.

■

1-3 $[\top]$ while $X > 0$ do $X := X - 1$ end $[X \leq 0]$

Solution Yes.

- For starting environment satisfying $X > 0$, the while loop will proceed until condition $X > 0$ is violated, which implies $X \leq 0$. Further, inside the loop body the value of X is decremented by 1, so its value will be reduced to $X \leq 0$ in finite times.
- For starting environment satisfying $X \leq 0$, the while loop will terminate immediately, leaving X unchanged, thus satisfying $X \leq 0$.

■

1-4 $\{\top\}$ while $X > 0$ do $X := X - 1$ end $\{X = 0\}$

Solution No. If this program starts from environment $\{X \mapsto -1\}$, the final environment will be $\{X \mapsto -1\}$, which does not satisfy the postcondition. ■

Problem 2: Weakest Liberal Precondition

2-1 Compute $\mathsf{wlp}(\text{if } X > 0 \text{ then } Y := X \text{ else } Y := -X, Y > 5)$.

Solution

$$
\begin{aligned}
&\mathsf{wlp}(\text{if } X > 0 \text{ then } Y := X \text{ else } Y := -X, Y > 5) \\
&= ((X > 0) \to \mathsf{wlp}(Y := X, Y > 5)) \land (\neg(X > 0) \to \mathsf{wlp}(Y := -X, Y > 5)) \\
&= ((X > 0) \to (X > 5) \land ((X \leq 0) \to (-X > 5)) \\
&= (\neg(X > 0) \lor (X > 5) \land (\neg(X \leq 0) \lor (X < -5)) \\
&= (X > 5) \lor (X < -5)
\end{aligned}
$$

■

2-2 Compute $\mathsf{wlp}(\text{while } X > 0 \text{ do } X := X + 1 \text{ end}, X \leq 0)$.

Solution $\mathsf{wlp}(\text{while } X > 0 \text{ do } X := X + 1 \text{ end}, X \leq 0) = \top$, let's prove by the definition of wlp.

1. $\{\top\}$ while $X > 0$ do $X := X + 1$ end $\{X \leq 0\}$ is valid:
   (a) Starting from an enviroment satisfying $X \leq 0$, the while loop will terminate immediately, leaving X unchanged, thus satisfying $X \leq 0$.
   (b) Starting from an enviroment satisfying $X > 0$, the while loop will not terminate because the loop body will increment X by 1, thus always satisfying condition $X > 0$.

   In conclusion, $\{P\}$ while $X > 0$ do $X := X + 1$ end $\{X \leq 0\}$ is valid for every P, so is for $\top$.
2. $\top$ is the weakest condition, because $P \to \top$ for every P.

■

Problem 3: Decorated Programs

The beauty of Hoare logic is that it is *compositional*: the structure of proofs exactly follows the structure of programs. This suggests that we can record the essential ideas of a proof (leaving out some low-level calculational details) by "decorating" a program with appropriate assertions on each of its commands. Such a *decorated program* carries within it an argument for its own correctness.

For example, consider the program (where m and p denote two constant integers):

$$
\begin{array}{l}
X := m; \\
Z := p; \\
\textsf{while } \neg(X = 0) \textsf{ do} \\
\quad Z := Z - 1; \\
\quad X := X - 1 \\
\textsf{end}
\end{array}
$$

To show that the above program satisfies precondition $\top$ and postcondition $Z = p - m$, we decorate the above as the following:

$$
\begin{array}{l}
\{\top\} \twoheadrightarrow \{m = m\} \\
X := m; \\
\{X = m\} \twoheadrightarrow \{X = m \wedge p = p\} \\
Z := p; \\
\{X = m \wedge Z = p\} \twoheadrightarrow \{Z - X = p - m\} \\
\textsf{while } \neg(X = 0) \textsf{ do} \\
\{Z - X = p - m \wedge X \neq 0\} \twoheadrightarrow \{(Z - 1) - (X - 1) = p - m\} \\
\quad Z := Z - 1; \\
\quad \{Z - (X - 1) = p - m\} \\
\quad X := X - 1 \\
\quad \{Z - X = p - m\} \\
\textsf{end} \\
\{Z - X = p - m \wedge \neg(X \neq 0)\} \twoheadrightarrow \{Z = p - m\}
\end{array}
$$

Concretely, a decorated program consists of the program commands interleaved with assertions – either a single assertion, or possibly two assertions separated by an implication "$\twoheadrightarrow$" (we use this strange notation to distinguish from our reduction relation $\rightarrow$). To check that a decorated program represents a valid proof, we check that each individual command is *locally consistent* with its nearby assertions, following the standard Hoare rules, e.g.

$$\{m = m\}\ X := m\ \{X = m\}$$

is valid by rule Asgn. Note that this hoare triple must not only be valid, but also be an *instantiation* of some Hoare rule. To convince yourself, carefully check that every such triples are indeed valid, and they are instantiations of the standard Hoare rules.

Now, it's your turn. Here is a program P that squares X by repeated addition:

$$
\begin{array}{l}
Y := 0; \\
Z := 0; \\
\textsf{while } \neg(Y = X) \textsf{ do} \\
\quad Z := Z + X; \\
\quad Y := Y + 1 \\
\textsf{end}
\end{array}
$$

We expect P to satisfy precondition $X = m$ and postcondition $X = m \times m$ for an arbitrary *natural number* m. Please write the corresponding decorated program which represents a valid proof of it.

Hint: you may need a "good" loop invariant.

Solution

$\{X = m\} \twoheadrightarrow \{X = m \wedge 0 = 0\}$
$Y := 0;$
$\{X = m \wedge Y = 0\} \twoheadrightarrow \{X = m \wedge Y = 0 \wedge 0 = 0\}$
$Z := 0;$
$\{X = m \wedge Y = 0 \wedge Z = 0\}\{Z = X \times Y \wedge X = m\}$
while $\neg(Y = X)$ do
  $\{Z = X \times Y \wedge X = m \wedge \neg(Y = X)\} \twoheadrightarrow \{Z + X = X \times (Y + 1) \wedge X = m\}$
  $Z := Z + X;$
  $\{Z = X \times (Y + 1) \wedge X = m\}$
  $Y := Y + 1$
  $\{Z = X \times Y \wedge X = m\}$
end
$\{Z = X \times Y \wedge X = m \wedge \neg\neg(Y = X)\} \twoheadrightarrow \{Z = m \times m\}$

■

Problem 4: Hoare Rules

The Hoare rules we have seen from lectures are *verification-friendly*, say they are strong enough to reason about almost all IMP programs. Suppose we add more extensions to IMP, which is our favorite thing, new Hoare rules need be specified to support these features. Again, these new rules should be verification-friendly. In this problem, you are asked to *design* (you do NOT need to proof your rule is sound) a couple of new Hoare rules that describe *partial correctness*.

4-1 Design a new Hoare rule for havoc (defined in the last homework).

Solution

$$\text{Havoc}\ \frac{\text{a is an arbitrary value}}{\{Q[a/X]\}\ \texttt{havoc}\ X\ \{Q\}}$$

■

4-2 Design a new Hoare rule for repeat-loop:

$$\texttt{repeat}\ c\ \texttt{until}\ b\ \texttt{end},$$

which behaves like a while-loop, except that the loop guard b is checked after each execution of the body c, with the loop repeating as long as the guard stays false. Because of this, the body will always execute at least once. Formally, the evaluation rules (of big-step operational semantics) are given by:

$$\text{(RepeatTrue)}\ \frac{\langle \sigma, c\rangle \Downarrow \sigma' \qquad \mathcal{B}[\![b]\!]_{\sigma'} = \top}{\langle \sigma, \texttt{repeat}\ c\ \texttt{until}\ b\ \texttt{end}\rangle \Downarrow \sigma'}$$

$$\text{(RepeatFalse)}\ \frac{\langle \sigma, c\rangle \Downarrow \sigma' \qquad \mathcal{B}[\![b]\!]_{\sigma'} = \bot \qquad \langle \sigma', \texttt{repeat}\ c\ \texttt{until}\ b\ \texttt{end}\rangle \Downarrow \sigma''}{\langle \sigma, \texttt{repeat}\ c\ \texttt{until}\ b\ \texttt{end}\rangle \Downarrow \sigma''}$$

Hint: "adapt" the Hoare rule for while-loops so that it works on repeat-loops.

Solution

$$\text{Repeat}\ \frac{\{P\}\ c\ \{Q\} \qquad \{Q \wedge b\}\ c\ \{Q\}}{\{P\}\ \texttt{repeat}\ c\ \texttt{until}\ b\ \texttt{end}\ \{Q \wedge \neg b\}}$$

■