Semantics of Programming Languages
Exercise Sheet 10

Exercise 10.1 Using the VCG

Use the VCG to prove correct a multiplication and a square root program:

\[
\text{definition } MUL :: \text{com where }
\]
\[
\begin{align*}
\text{"MUL} &= \text{\{ } Z := N 0 ; \text{\}; } \\
\text{"c"} &= N 0 ; \\
\text{WHILE ( Less (V "c") (V "y") ) DO } ( \\
\text{"z"} &:= \text{Plus (V "z") (V "x")}; \\
\text{"c"} &:= \text{Plus (V "c") (N 1)}) \text{"
}\end{align*}
\]

\[
\text{theorem } MUL\text{.partially.correct:}
\]
\[
\vdash \{ \lambda s. 0 \leq s "y" \land s=sorig \} \\
\text{MUL} \\
\{ \lambda s. s "z" = s "x" \ast s "y" \land (\forall v. v \notin \{"z","c"\} \rightarrow s v = sorig v) \}
\]

\[
\text{definition } SQRT :: \text{com where }
\]
\[
\begin{align*}
\text{"r"} &= N 0 ; \\
\text{"s"} &= N 1 ; \\
\text{WHILE ( Not ( Less (V "x") (V "s") ) ) DO } ( \\
\text{"r"} &:= \text{Plus (V "r") (N 1)}; \\
\text{"s"} &:= \text{Plus (V "s") (V "r")}; \\
\text{"r"} &:= \text{Plus (V "s") (N 1)}; \\
\text{"s"} &:= \text{Plus (V "s") (N 1)} \text{"
}\end{align*}
\]

\[
\text{theorem } SQRT\text{.partially.correct:}
\]
\[
\vdash \{ \lambda s. s=sorig \land s "x" \geq 0 \} \\
\text{SQRT} \\
\{ \lambda s. (s "r") \ast 2 \leq s "x" \land s "x" < (s "r" + 1) \ast 2 \land (\forall v. v \notin \{"s","r"\} \rightarrow s v = sorig v) \}
\]

Exercise 10.2 Total Correctness

Prove total correctness of the multiplication and square root program.
Rotated rule for sequential composition:

**lemmas** \( \text{Seq.bwd} = \text{Hoare}_\text{Total}.\text{Seq[rotated]} \)

Prove the following syntax-directed conditional rule (for total correctness):

**lemma** \( \text{IfT} \):

**assumes** "\( \vdash_t \{ P1 \} \ c_1 \ \{ Q \} \)" and "\( \vdash_t \{ P2 \} \ c_2 \ \{ Q \} \)"

**shows** "\( \vdash_t \{ s b v a l \ b \ s \rightarrow P1 \ s \ \land \ \neg \ b v a l \ b \ s \rightarrow P2 \ s \} \ IF \ b \ THEN \ c_1 \ ELSE \ c_2 \ \{ Q \} \)"

**lemmas** \( \text{hoareT\_rule[\text{intro}\?] = Seq.bwd \ Hoare}_\text{Total}.\text{Assign} \ Hoare\_\text{Total}\_\text{Assign}' \ \text{IfT} \)

**theorem** \( \text{MUL\_totally\_correct} \):

"\( \vdash \{ s . \ 0 \leq s "y" \ \land \ s = \text{sorig} \} \)"

\( \text{MUL} \) \( \{ s . \ s "z" = s "x" * s "y" \ \land \ (\forall v. v \notin \{"z","c"\} \rightarrow s v = \text{sorig} v)\} \)"

**theorem** \( \text{SQRT\_totally\_correct} \):

"\( \vdash \{ s . \ s = \text{sorig} \ \land \ s "x" \geq 0 \} \)"

\( \text{SQRT} \) \( \{ s . \ (s "r")^2 \leq s "x" \ \land \ s "x" < (s "r"+1)^2 \ \land \ (\forall v. v \notin \{"s","r"\} \rightarrow s v = \text{sorig} v)\} \)"

**Homework 10.1** Using the VCG

*Submission until Monday, January 20, 10:00am.*

Consider the following IMP program that given a value \( n \geq 0 \) in variable "\( n " \) computes \( 2^n \) and stores the result in variable "\( x " \).

**definition**

"\( \text{POWER2} \equiv \)"

\( \)"\( \)"\( \)"\( \)"

Using the VCG, prove the following Hoare triple, stating the program is correct.

**theorem** \( \text{POWER2\_correct} \):

"\( \vdash \{ s . \ s "n" = n \ \land \ n \geq 0 \} \)"

\( \text{POWER2} \) \( \{ s . \ s "x" = 2 ^ \ \text{nat} \ n \} \)"

**Hint:** The theorem collection algebra\_simpls and sledgehammer can be helpful to discharge proof obligations about arithmetic.
Homework 10.2 Collecting Semantics

Submission until Monday, January 20, 10:00am.

This question concerns the iterative computation of the collecting semantics of the following annotated command:

```
IF x < 0 THEN {A1}
    {A2}
    WHILE 0 < y DO
        {A3}
        (y := y + x {A4})
        {A5}
    ELSE {A6} SKIP {A7}
    {A8}
```

Show how the annotations change with each application of the step function. Fill in this table to show how the process evolves until a least fixpoint is reached:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>∅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A2</td>
<td>∅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A3</td>
<td>∅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A4</td>
<td>∅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A5</td>
<td>∅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A6</td>
<td>∅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A7</td>
<td>∅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A8</td>
<td>∅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Let $S$ be $\{< x := -2, y := 3>, < x := 1, y := 2>\}$ when you execute the step function. For brevity, write such a set of states as $-2,3 | 1,2$ when you fill in the table. Entries that do not change can be left blank.