CSC 503 Homework Assignment 11

Out: October 23, 2015
Due: October 30, 2015
rsandil

In the following proofs about programs, use the natural deduction proof environment, the `\Hcond` macro, and the Hoare-logic justifications `\Implied{}`, `\Assignment{}`, `\IfStatement{}`, `\PartialWhile{}`, `\InvariantGuard{}`, and `\TotalWhile{}` to present proofs of partial or total correctness. If you are not using LaTeX, you can substitute double parentheses for the Hoare condition delimiters $\llparenthesis\ \rrparenthesis$. For example, we can rewrite the proof in Example 4.13.1 on page 277 of the textbook as

1	$\llparenthesis y = 5 \rrparenthesis$	
2	$\llparenthesis y + 1 = 6 \rrparenthesis$	Implied
3	`x = y + 1;`	
4	$\llparenthesis x = 6 \rrparenthesis$	Assignment

The standard stmaryrd package is also used in these macros.

1. **[20 points]** Recall that the arithmetic expressions in the simple textbook programming language only refer to integers. Use the proof rule for assignment and integer arithmetic entailment as appropriate to show the validity of

$$\vdash_{\text{par}} \llparenthesis x > 1 \wedge y > 0 \rrparenthesis\ P\ \llparenthesis x > 1 \wedge y \geq 2 \rrparenthesis.$$

where P is the program

```
a = 2 * x;
y = x + a;
y = y - x;
```

Answer

1	$\llparenthesis x > 1 \wedge y > 0 \rrparenthesis$	
2	$\llparenthesis x > 1 \wedge 2x \geq 2 \rrparenthesis$	Implied
3	`a = 2 * x`	
4	$\llparenthesis x > 1 \wedge a \geq 2 \rrparenthesis$	Assignment
5	`y = x + a;`	
6	$\llparenthesis x > 1 \wedge y - x \geq 2 \rrparenthesis$	Assignment
7	`y = y - x;`	
8	$\llparenthesis x > 1 \wedge y \geq 2 \rrparenthesis$	Assignment

2. **[40 points]** Prove the validity of the sequent $\vdash_{\text{par}} \llparenthesis y > 0 \rrparenthesis\ Q\ \llparenthesis w = \max(y, z) \rrparenthesis$ where $\max(y, z)$ is the largest

number of y and z, and where the code of Q is given by

```
x = 0;
if (x < y) {
   if (y < z) {
      w = z;
   } else {
      w = y;
   };
} else {
   w = x;
}
```

Answer

```
1   $\llparenthesis y > 0 \rrparenthesis$
2   $\llparenthesis (0 < y \rightarrow ((y < z) \rightarrow z = max(y,z)) \wedge (\neg(y < z) \rightarrow y = max(y,z))) \rrparenthesis$
      $\wedge(\neg(0 < y) \rightarrow 0 = max(y,z))$                                   Implied
3   x = 0;
4   $\llparenthesis (x < y \rightarrow ((y < z) \rightarrow z = max(y,z)) \wedge (\neg(y < z) \rightarrow y = max(y,z))) \rrparenthesis$
      $\wedge(\neg(x < y) \rightarrow x = max(y,z))$                                   Assignment
5   if (x < y) {
6   $\llparenthesis (y < z \rightarrow z = max(y,z) \wedge \neg(y < z) \rightarrow y = max(y,z) \rrparenthesis$   If-Statement
7       if (y < z) {
8           $\llparenthesis z = \max(y,z) \rrparenthesis$                                  If-Statement
9           w = z;
10          $\llparenthesis w = \max(y,z) \rrparenthesis$                                  Assignment
11      } else {
12          $\llparenthesis y = \max(y,z) \rrparenthesis$                                  If-Statement
13          w = y;
14          $\llparenthesis w = \max(y,z) \rrparenthesis$                                  Assignment
15      };
16  $\llparenthesis w = \max(y,z) \rrparenthesis$                                          If-Statement
17  } else {
18      $\llparenthesis x = \max(y,z) \rrparenthesis$                                      If-Statement
19      w = x;
20      $\llparenthesis w = \max(y,z) \rrparenthesis$                                      Assignment
21  }
22  $\llparenthesis w = \max(y,z) \rrparenthesis$                                          If-Statement
```

NOTE: In line number 2 and 4 vertical line paranthesis is meant to enclose the complete statement split in multiline(2). Formatting in latex caused the problem.

3. **[40 points]** Prove the validity of the sequent $\vdash_{\text{par}} \llparenthesis w = x \wedge x \geq 0 \rrparenthesis \; R \; \llparenthesis z = x \cdot y \rrparenthesis$ where the code of R is given by

```
z = 0;
while (w != 0) {
    z = z + y;
    w = w - 1;
}
```

Answer

```
1   $\llparenthesis w = x \land x \geq 0 \rrparenthesis$
2   $\llparenthesis x = w \rrparenthesis$                                  Implied
3   $\llparenthesis 0 = (x - w)y \rrparenthesis$                           Implied
4   z = 0;
5   $\llparenthesis z = (x - w)y \rrparenthesis$                           Assignment
6   while (w != 0) {
7       $\llparenthesis z = (x - w)y \land \neg(w! = 0) \rrparenthesis$    Invariant Hyp. and Guard
8       $\llparenthesis z + y = (x - (w - 1))y \rrparenthesis$             Implied
9       z = z + y;
10      $\llparenthesis z = (x - (w - 1))y \rrparenthesis$                 Assignment
11      w = w - 1;
12      $\llparenthesis z = (x - w)y \rrparenthesis$                       Assignment
13  }
14  $\llparenthesis z = (x - w) \cdot y \land \neg(w! = 0) \rrparenthesis$     Partial-While
15  $\llparenthesis z = x \cdot y \rrparenthesis$                          Implied
```