ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

D. Basin and P. Müller

Formal Methods and Functional Programming

Exercise Sheet 13: Axiomatic Semantics, Total Correctness

Submission deadline: May 28th, 2012

Please submit your solution before **10:15am** on the submission date specified above. Solutions can be submitted via e-mail or by using the boxes in front of **CAB F 51.1**. Make sure that the first page (and preferably each sheet) always contains your name, the exercise sheet number as well as your tutor's name and the weekday (Tuesday or Wednesday) of your exercise group. Don't forget to staple your pages if you submit more than one page.

Assignment 1

Let s be the following statement:

```
y := 1;
z := 0;
while z<x do
  y := y * 2;
  z := z + 1
end
```

Our goal is to prove that $\vdash \{\ \mathtt{x} = X \ \wedge\ X \geq 0\ \}\ s\ \{\ \Downarrow \mathtt{y} = 2^X\ \}$

(a) Find a suitable loop invariant. You may use Dafny for help. **Hint:** Mention all of the variables used in the loop.

(b) Find a suitable loop variant. Again, you may use Dafny. A loop variant is given in Dafny in a `decreases` clause, as in the following example:

```
x := 100;
while x>0
  invariant x>=0;
  decreases x;
{ x:=x-1; }
```

(c) Give a complete proof outline for $\vdash \{\ \mathtt{x} = X \ \wedge\ X \geq 0\ \}\ s\ \{\ \Downarrow \mathtt{y} = 2^X\ \}$.

Assignment 2

Show that (for all statements s, for all boolean expressions b and for all predicates P and Q):

$$\vdash \{\ P\ \}\ \texttt{while}\ b\ \texttt{do}\ s\ \texttt{end}\ \{\ \Downarrow Q\ \}$$
$$\Leftrightarrow$$
there exists a predicate R *and an integer expression* e *such that:*
$P \Rightarrow R$ *and* $R \wedge \neg b \Rightarrow Q$ *and* $R \wedge b \Rightarrow e \geq 0$ *and* $\vdash \{\ R \wedge b \wedge e = Z\ \}\ s\ \{\ \Downarrow R \wedge e < Z\ \}$

Assignment 3

This question concerns termination and the Zune bug, as discussed in the lectures.

(a) Suppose that, for some statement s, the triple $\{$ *true* $\}\ s\ \{ \Downarrow$ *true* $\}$ can be derived. What does this tell us about s?

(b) Let s' be the following IMP statement:

```
while (365 < days) do
  if (L(year)) then
    if (366 < days) then
      days = days - 366; year = year + 1
    else
      skip
    end
  else
    days = days - 365; year = year + 1
  end
end
```

We assume that L(year) may be used as a boolean expression. Using `days` as a loop variant, attempt to derive that $\vdash \{$ *true* $\}\ s'\ \{ \Downarrow$ *true* $\}$. Where does your proof fail?

(c) Let s'' be the following (corrected) IMP statement:

```
while (L(year) and 366 < days or not L(year) and 365 < days) do
  if (L(year)) then
      days = days - 366
  else
      days = days - 365;
  end;
  year += 1
end
```

Show that $\vdash \{$ *true* $\}\ s''\ \{ \Downarrow$ *true* $\}$.

Assignment 4

Show that, for all statements s_1,s_2 and s_3, and for all predicates P and Q:

$$\vdash \{\ P\ \}\ (s_1; s_2); s_3\ \{\ Q\ \} \quad \Rightarrow \quad \vdash \{\ P\ \}\ s_1; (s_2; s_3)\ \{\ Q\ \}$$

Assignment 5 - Headache of the week

Write an IMP statement s to compute the floor of the square root of an integer, i.e.,

$$\vdash \{\ x = M \wedge y = N \wedge M > 0 \wedge N \geq 0\ \}\ s\ \{\ \Downarrow z^M \leq N \wedge N < (z{+}1)^M\ \}$$

Hint: You may use the program that you developed in Sheet 8. However, notice that IMP does not support procedures, so you may have to adapt the program to use nested loops.

Provide a proof outline for the above total correctness claim. You may use Dafny to discover loop invariants and variants.