Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

D. Basin and P. Müller

Formal Methods and Functional Programming

Exercise Sheet 11: Axiomatic Semantics

Submission deadline: May 24th, 2010

Please submit your solution before **9:15am** on the submission date specified above. Solutions can be submitted via e-mail or by using the boxes to the left of **RZ F1**. Make sure that the first page 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

a)

Consider the loop:

```
while i < k do
  i := i + 1;
  r := r * n
end
```

Which of the following formulas are invariants of this loop? For those which are not, show why the proof of invariant preservation (i.e., the premise of the axiomatic semantics rule for while loops) fails.

$$\mathtt{i} \geq 0 \land \mathtt{r} = \mathtt{n}^{\mathtt{i}} \tag{1}$$

$$\mathtt{i} \geq 0 \land \mathtt{i} \leq \mathtt{k} \land \mathtt{r} = \mathtt{n}^{\mathtt{i}} \tag{2}$$

$$\mathtt{i} \geq 0 \land \mathtt{i} < \mathtt{k} \land \mathtt{r} = \mathtt{n}^{\mathtt{i}} \tag{3}$$

b)

Use the above while loop to write a program s such that
$\vdash \{\, K \geq 1 \ \land K = \mathtt{k} \,\}\ s\ \{\, \mathtt{r} = \mathtt{n}^K \,\}$.

Assignment 2

Recall the rule of consequence as presented in the lecture

$$\frac{\{\,\mathbf{P}'\,\}\ s\ \{\,\mathbf{Q}'\,\}}{\{\,\mathbf{P}\,\}\ s\ \{\,\mathbf{Q}\,\}}\ \text{if } \mathbf{P} \Rightarrow \mathbf{P}' \text{ and } \mathbf{Q}' \Rightarrow \mathbf{Q}$$

and compare it to the following *unsound* variation

$$\frac{\{\,\mathbf{P}'\,\}\ s\ \{\,\mathbf{Q}'\,\}}{\{\,\mathbf{P}\,\}\ s\ \{\,\mathbf{Q}\,\}}\ \text{if } \mathbf{P}' \Rightarrow \mathbf{P} \text{ and } \mathbf{Q} \Rightarrow \mathbf{Q}'$$

Give textual arguments why the first rule is sound and why the second one is not and support your argumentation with two illustrating examples.

Assignment 3

Consider the following programme s computing the quotient and the remainder of $\frac{X}{Y}$.

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

Find a suitable precondition $\mathbf{P}$ and prove that
$\vdash \{\, \mathsf{x} = X \wedge \mathsf{y} = Y \wedge \mathbf{P} \,\}\ s\ \{\, \mathtt{X} = \mathtt{x} + \mathtt{Y} * \mathtt{z} \wedge \mathtt{Y} > \mathtt{x} \,\}$.

Assignment 4

Show, by structural induction on s, that $\vdash \{\ \mathbf{P}\ \}\ s\ \{\ 0 = 0\ \}$ for all statements s and all properties $\mathbf{P}$.

Assignment 5 - Headache of the week

Consider the following programme s computing the greatest common divisor (gcd) of two given positive integers:

```
b := x;
c := y;
while b # c do
  if b < c then
    c := c - b
  else
    b := b - c
  end
end;
z := b
```

Convince yourself that the programme terminates when `x` and `y` store positive integers.

Tasks:

1. Formalise the claim that the above programme computes the gcd of `x` and `y` as pre- and postcondition $\mathbf{P}, \mathbf{Q}$, respectively.
2. Find an invariant for the loop (and prove that it is preserved by the loop).
3. Show that $\vdash \{ \mathbf{P} \}\ s\ \{ \mathbf{Q} \}$.

Recall the definition of the gcd:
Let x, y be positive integers. The number z is the greatest common divisor of x and y iff $z|x$ and $z|y$ and there is no z', with $z' > z$, such that $z'|x$ and $z'|y$. Here, $z|x$ means that z divides x, i.e., $z \cdot k = x$, for some $k \in \mathbb{N}$.

Hint: Consider using a relationship between the input variables `x`, `y` and the 'loop' variables `b`, `c` as part of your loop invariant.