ETH zürich

P. Müller and D. Basin

Formal Methods and Functional Programming

Optional Exercises 13: Axiomatic Semantics

As usual, the solutions can be found at the end of the file.

Assignment 3 (Zune Bug)

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

Task 3.1. Suppose that, for some statement s, the triple $\{\ \textit{true}\ \}\ s\ \{\ \Downarrow \textit{true}\ \}$ can be derived. What does this tell us about s?

Task 3.2. 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 := year + 1
end
```

Show that $\vdash \{\ \textit{true}\ \}\ s\ \{\ \Downarrow \textit{true}\ \}$.

Assignment 4 (Total Correctness of Division)

Consider the following IMP program s:

```
while r >= 0 do
  r := r - d;
  q := q + 1
end;
r := r + d;
q := q - 1
```

The program s computes the quotient $\mathtt{q}$ and remainder $\mathtt{r}$ resulting from the division of a given non-negative integer N (initially stored in the variable $\mathtt{r}$) by a given positive integer D (stored in the variable $\mathtt{d}$).

Task 4.1. Find a suitable loop invariant and variant

Task 4.2. Show that

$$\vdash \{\, N \geq 0 \wedge D > 0 \wedge \mathtt{d} = D \wedge \mathtt{r} = N \wedge \mathtt{q} = 0 \,\}\; s \;\{\, \Downarrow N = \mathtt{q} \times D + \mathtt{r} \wedge \mathtt{r} \geq 0 \wedge \mathtt{r} < D \,\}.$$

Assignment 5 (Logarithm)

Let $\mathtt{s}$ be the following IMP program:

```
a := 1;
b := 0;
while a < n do
  a := a * 10;
  if (a <= n) then
    b := b + 1
  else
    skip
  end
end
```

The function computes $\lfloor \log_{10}(\mathtt{n}) \rfloor$, storing the result in $\mathtt{z}$. To express the floor of the logarithm, we will use two inequalities involving exponentiation.

Task 5.1. Try to find a loop invariant for this program.

Task 5.2. Using the loop invariant from the previous task, prove that the program computes $\log_{10}(\mathtt{n})$ rounded down, i.e., that

$$\vdash \{\ \mathtt{n} = N \land \mathtt{n} \geq 1\ \}\ s\ \{\ 10^{\mathtt{b}} \leq N \land N < 10^{\mathtt{b}+1}\ \}$$

Hint: If you are not able come up with an invariant, do a handstand:

$$(\mathtt{a} \leq \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}}) \land (\mathtt{a} > \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}+1}) \land 10^{\mathtt{b}} \leq \mathtt{n} \land \mathtt{n} = N$$

Solution of Assignment 3 (Zune Bug)

Task 3.1. If the triple $\{\ \textit{true}\ \}\ s\ \{\ \Downarrow \textit{true}\ \}$ can be derived, this means that the statement s is guaranteed to terminate (regardless of the initial state).

Task 3.2. We use *true* as the invariant for the loop, and days for the variant. The proof outline is:

$\{\textit{true}\}$

`while ((L(year) and 366 < days) or (not L(year) and 365 < days)) do`*

$\{((\texttt{L(year)} \ \wedge\ 366 < \texttt{days}) \vee (\neg\texttt{L(year)} \ \wedge\ 365 < \texttt{days})) \ \wedge\ \textit{true} \ \wedge\ \texttt{days} = V\}$

`if (L(year)) then`

$\{\texttt{L(year)} \wedge ((\texttt{L(year)} \ \wedge\ 366 < \texttt{days}) \vee (\neg\texttt{L(year)} \ \wedge\ 365 < \texttt{days})) \ \wedge\ \textit{true} \ \wedge\ \texttt{days} = V\}$

$\models$

$\{\texttt{days} - 366 < V\}$

`days := days - 366`

$\{\texttt{days} < V\}$

`else`

$\{\neg\texttt{L(year)} \wedge ((\texttt{L(year)} \ \wedge\ 366 < \texttt{days}) \vee (\neg\texttt{L(year)} \ \wedge\ 365 < \texttt{days})) \ \wedge\ \textit{true} \ \wedge\ \texttt{days} = V\}$

$\models$

$\{\texttt{days} - 365 < V\}$

`days := days - 365`

$\{\texttt{days} < V\}$

`end;`

$\{\texttt{days} < V\}$

`y:=y+1`

$\{\Downarrow \texttt{days} < V\}$

$\models$

$\{\Downarrow \textit{true} \ \wedge\ \texttt{days} < V\}$

`end`

$\{\Downarrow \neg((\texttt{L(year)} \ \wedge\ 366 < \texttt{days}) \vee (\neg\texttt{L(year)} \ \wedge\ 365 < \texttt{days})) \wedge \textit{true}\}$

$\models$

$\{\Downarrow \textit{true}\}$

(*) *side-condition: the while condition entails ($\models$)* $\texttt{days} \geq 0$

Solution of Assignment 4 (Total Correctness of Division)

Task 4.1. A suitable loop invariant is $N = \texttt{q} \times \texttt{d} + \texttt{r} \ \wedge\ \texttt{r} + \texttt{d} \geq 0 \ \wedge \texttt{d} = D \wedge\ \texttt{d} > 0$ and the loop variant is $\texttt{r}$.

Task 4.2. The proof outline is:

$\{N \geq 0 \ \wedge \ D > 0 \wedge \mathtt{d} = D \wedge \mathtt{r} = N \wedge \mathtt{q} = 0\}$

$\models$

$\{N = \mathtt{q} \times \mathtt{d} + \mathtt{r} \ \wedge \ \mathtt{r} + \mathtt{d} \geq 0 \ \wedge \mathtt{d} = D \wedge \ \mathtt{d} > 0\}$

```
while r >= 0 do*
```

$\{\mathtt{r} \geq 0 \ \wedge \ N = \mathtt{q} \times \mathtt{d} + \mathtt{r} \ \wedge \ \mathtt{r} + \mathtt{d} \geq 0 \ \wedge \ \mathtt{d} = D \ \wedge \ \mathtt{d} > 0 \ \wedge \ \mathtt{r} = Z\}$

$\models$

$\{N = (\mathtt{q} + 1) \times \mathtt{d} + \mathtt{r} - \mathtt{d} \ \wedge \ \mathtt{r} - \mathtt{d} + \mathtt{d} \geq 0 \ \wedge \ \mathtt{d} = D \ \wedge \ \mathtt{d} > 0 \ \wedge \ \mathtt{r} - \mathtt{d} < Z\}$

```
r := r - d;
```

$\{N = (\mathtt{q} + 1) \times \mathtt{d} + \mathtt{r} \ \wedge \ \mathtt{r} + \mathtt{d} \geq 0 \ \wedge \ \mathtt{d} = D \ \wedge \ \mathtt{d} > 0 \ \wedge \ \mathtt{r} < Z\}$

```
q := q + 1
```

$\{\Downarrow N = \mathtt{q} \times \mathtt{d} + \mathtt{r} \ \wedge \ \mathtt{r} + \mathtt{d} \geq 0 \ \wedge \ \mathtt{d} = D \ \wedge \ \mathtt{d} > 0 \ \wedge \ \mathtt{r} < Z\}$

```
end;
```

$\{\Downarrow \neg(\mathtt{r} \geq 0) \wedge N = \mathtt{q} \times \mathtt{d} + \mathtt{r} \ \wedge \ \mathtt{r} + \mathtt{d} \geq 0 \ \wedge \ \mathtt{d} = D \ \wedge \ \mathtt{d} > 0\}$

$\models (1)$

$\{\Downarrow N = (\mathtt{q} - 1) \times \mathtt{d} + \mathtt{r} + \mathtt{d} \ \wedge \ \mathtt{r} + \mathtt{d} \geq 0 \ \wedge \ \mathtt{r} + \mathtt{d} < \mathtt{d} \ \wedge \ \mathtt{d} = D \ \wedge \ \mathtt{d} > 0\}$

```
r := r + d;
```

$\{\Downarrow N = (\mathtt{q} - 1) \times \mathtt{d} + \mathtt{r} \ \wedge \ \mathtt{r} \geq 0 \ \wedge \ \mathtt{r} < \mathtt{d} \wedge \mathtt{d} = D \wedge \ \mathtt{d} > 0\}$

```
q := q - 1
```

$\{\Downarrow N = \mathtt{q} \times \mathtt{d} + \mathtt{r} \ \wedge \ \mathtt{r} \geq 0 \ \wedge \ \mathtt{r} < \mathtt{d} \ \wedge \ \mathtt{d} = D \wedge \ \mathtt{d} > 0\}$

$\models$

$\{\Downarrow N = \mathtt{q} \times D + \mathtt{r} \ \wedge \ \mathtt{r} \geq 0 \ \wedge \ \mathtt{r} < D\}$

(*) *side-condition:* $(\mathtt{r} \geq 0 \ \wedge \ N = \mathtt{q} \times \mathtt{d} + \mathtt{r} \ \wedge \ \mathtt{r} + \mathtt{d} \geq 0 \ \wedge \ \mathtt{d} = D \ \wedge \ \mathtt{d} > 0) \ \models \ \mathtt{r} \geq 0$

(1) $\neg(\mathtt{r} \geq 0)$ implies $\mathtt{r} + \mathtt{d} < \mathtt{d}$.

Solution of Assignment 5 (Logarithm)

Task 5.1. Our loop invariant is as follows:

$$(\mathtt{a} \leq \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}}) \wedge (\mathtt{a} > \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}+1}) \wedge 10^{\mathtt{b}} \leq \mathtt{n} \wedge \mathtt{n} = N$$

Task 5.2. Then the proof outline is:

$\{\mathtt{n} = N \wedge \mathtt{n} \geq 1\}$

$\models$

$\{\mathtt{n} = N \wedge \mathtt{n} \geq 1 \wedge 1 = 1 \wedge 0 = 0\}$

```
a := 1;
```

$\{\mathtt{n} = N \wedge \mathtt{n} \geq 1 \wedge \mathtt{a} = 1 \wedge 0 = 0\}$

```
b := 0;
```

$\{\mathtt{n} = N \wedge \mathtt{n} \geq 1 \wedge \mathtt{a} = 1 \wedge \mathtt{b} = 0\}$

$\models^{(\star)}$

$\{(\mathtt{a} \leq \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}}) \wedge (\mathtt{a} > \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}+1}) \wedge 10^{\mathtt{b}} \leq \mathtt{n} \wedge \mathtt{n} = N\}$

```
while a<n do
```

$\{\mathtt{a} < \mathtt{n} \wedge (\mathtt{a} \leq \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}}) \wedge (\mathtt{a} > \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}+1}) \wedge 10^{\mathtt{b}} \leq \mathtt{n} \wedge \mathtt{n} = N\}$

$\models$

$\{\mathtt{a} * 10 = 10^{\mathtt{b}+1} \wedge 10^{\mathtt{b}} < \mathtt{n} \wedge \mathtt{n} = N\}$

```
a := a*10;
```

$\{\mathtt{a} = 10^{\mathtt{b}+1} \wedge 10^{\mathtt{b}} < \mathtt{n} \wedge \mathtt{n} = N\}$

```
if (a <= n) then
```

$\{\mathtt{a} \leq \mathtt{n} \wedge \mathtt{a} = 10^{\mathtt{b}+1} \wedge 10^{\mathtt{b}} < \mathtt{n} \wedge \mathtt{n} = N\}$

$\models$

$\{\mathtt{a} = 10^{\mathtt{b}+1} \wedge 10^{\mathtt{b}+1-1} < \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{a} \leq \mathtt{n}\}$

```
b := b+1
```

$\{\mathtt{a} = 10^{\mathtt{b}} \wedge 10^{\mathtt{b}-1} < \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{a} \leq \mathtt{n}\}$

$\models^{(\star)}$

$\{(\mathtt{a} \leq \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}}) \wedge (\mathtt{a} > \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}+1}) \wedge 10^{\mathtt{b}} \leq \mathtt{n} \wedge \mathtt{n} = N\}$

```
else
```

$\{\neg(\mathtt{a} \leq \mathtt{n}) \wedge \mathtt{a} = 10^{\mathtt{b}+1} \wedge 10^{\mathtt{b}} < \mathtt{n} \wedge \mathtt{n} = N\}$

```
skip
```

$\{\neg(\mathtt{a} \leq \mathtt{n}) \wedge \mathtt{a} = 10^{\mathtt{b}+1} \wedge 10^{\mathtt{b}} < \mathtt{n} \wedge \mathtt{n} = N\}$

$\models^{(\star)}$

$\{(\mathtt{a} \leq \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}}) \wedge (\mathtt{a} > \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}+1}) \wedge 10^{\mathtt{b}} \leq \mathtt{n} \wedge \mathtt{n} = N\}$

```
end
```

$\{(\mathtt{a} \leq \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}}) \wedge (\mathtt{a} > \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}+1}) \wedge 10^{\mathtt{b}} \leq \mathtt{n} \wedge \mathtt{n} = N\}$

```
end
```

$\{\neg(\mathtt{a} < \mathtt{n}) \wedge (\mathtt{a} \leq \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}}) \wedge (\mathtt{a} > \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}+1}) \wedge 10^{\mathtt{b}} \leq \mathtt{n} \wedge \mathtt{n} = N\}$

$\models^{(1)}$

$\{10^{\mathtt{b}} \leq N \wedge N < 10^{\mathtt{b}+1}\}$

($\star$) For these steps we use that $\mathbf{P} \wedge \mathbf{R}$ entails $(\mathbf{P} \Rightarrow \mathbf{R}) \wedge (\neg\mathbf{P} \Rightarrow \mathbf{Q})$ for arbitrary assertions $\mathbf{P}, \mathbf{R}, \mathbf{Q}$.

(1) To justify this step, use the fact that $\mathtt{a} \geq \mathtt{n}$, and case split on $\mathtt{a} = \mathtt{n}$ or $\mathtt{a} > \mathtt{n}$: In the case where $\mathtt{a} = \mathtt{n}$ holds, from the first implication we deduce $\mathtt{a} = 10^{\mathtt{b}}$. Therefore, in this case, we have

$N = \mathtt{n} = \mathtt{a} = 10^{\mathsf{b}}$, from which the post-condition follows directly.

In the case where $\mathtt{a} > \mathtt{n}$ holds, we use the second implication to deduce $\mathtt{a} = 10^{\mathsf{b}+1}$. Our assumption is that $\mathtt{a} > \mathtt{n}$, and so we have $N < 10^{\mathsf{b}+1}$. From $10^{\mathsf{b}} \leq \mathtt{n}$, we deduce $10^{\mathsf{b}} \leq N$ as required.