ETH zürich

P. Müller and D. Basin

Formal Methods and Functional Programming

Solutions of Exercise Sheet 13: Axiomatic Semantics

Assignment 1 (Total Correctness of Exponentiation)

Task 1.1. A suitable loop invariant is $\mathtt{x} = X \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x}$, where X is the initial value of x. A suitable loop variant is $\mathtt{x} - \mathtt{z}$.

Task 1.2. The proof outline is:

$\{\mathtt{x} = X \wedge X \geq 0\}$
$\models$
$\{\mathtt{x} = X \wedge X \geq 0 \wedge 1 = 1\}$
  `y := 1;`
$\{\mathtt{x} = X \wedge X \geq 0 \wedge \mathtt{y} = 1\}$
$\models$
$\{\mathtt{x} = X \wedge X \geq 0 \wedge \mathtt{y} = 1 \wedge 0 = 0\}$
  `z := 0;`
$\{\mathtt{x} = X \wedge X \geq 0 \wedge \mathtt{y} = 1 \wedge \mathtt{z} = 0\}$
$\models$
$\{\mathtt{x} = X \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x}\}$
  `while z<x do`*
  $\{\mathtt{z} < \mathtt{x} \wedge \mathtt{x} = X \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x} \wedge (\mathtt{x} - \mathtt{z}) = V\}$
  $\models$
  $\{\mathtt{x} = X \wedge \mathtt{y} \cdot 2 = 2^{\mathtt{z}+1} \wedge \mathtt{z} + 1 \leq \mathtt{x} \wedge (\mathtt{x} - (\mathtt{z} + 1)) < V\}$
    `y := y * 2;`
  $\{\mathtt{x} = X \wedge \mathtt{y} = 2^{\mathtt{z}+1} \wedge \mathtt{z} + 1 \leq \mathtt{x} \wedge (\mathtt{x} - (\mathtt{z} + 1)) < V\}$
    `z := z + 1`
  $\{\Downarrow \mathtt{x} = X \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x} \wedge (\mathtt{x} - \mathtt{z}) < V\}$
  `end`
$\{\Downarrow \neg(\mathtt{z} < \mathtt{x}) \wedge \mathtt{x} = X \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x}\}$
$\models$
$\{\Downarrow \mathtt{y} = 2^X\}$

- The side condition (*) holds as $\mathtt{z} < x \land \mathtt{x} = X \land \mathtt{y} = 2^{\mathtt{z}} \land \mathtt{z} \leq \mathtt{x}$ entails $\mathtt{x} - \mathtt{z} > 0$.
- The last entailment uses that $\neg(\mathtt{z} < \mathtt{x})$ and $\mathtt{z} \leq \mathtt{x}$ implies $\mathtt{z} = \mathtt{x}$.

Assignment 2

Task 2.1. The function computes $\lfloor \sqrt{\mathtt{n}} \rfloor$, storing the result in $\mathtt{z}$. To express the floor of the square root we use two inequalities. In Viper syntax, this can be written as:

```
z * z <= n && (z + 1) * (z + 1) > n
```

Note that the two conditions imply $\mathtt{z} \geq 0$, as $\mathtt{z}^2 > (\mathtt{z}{+}1)^2$ for negative $\mathtt{z}$.

Task 2.2. A suitable loop invariant is:

$$(\mathtt{y}^2 \leq \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z}) \land (\mathtt{y}^2 > \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z} + 1) \land (\mathtt{z}^2 \leq \mathtt{n}) \land (\mathtt{z} \geq 0)$$

We have a case distinction on $\mathtt{y}$. As long as $\mathtt{y}^2 \leq \mathtt{n}$, $\mathtt{y}$ equals $\mathtt{z}$. Only if $\mathtt{y}^2 > \mathtt{n}$, we don't update $\mathtt{z}$ and $\mathtt{y}$ is one bigger than $\mathtt{z}$. Also we always guarantee that $\mathtt{z}^2 \leq \mathtt{n}$, i.e., we never overshoot. $\mathtt{z} \geq 0$ ensures that we get the positive square root. Together with the negated loop condition we are able to prove the post-condition.

Task 2.3. We choose the invariant to be

$$(\mathtt{y}^2 \leq \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z}) \land (\mathtt{y}^2 > \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z} + 1) \land (\mathtt{z}^2 \leq \mathtt{n}) \land (\mathtt{n} = N) \land (\mathtt{z} \geq 0)$$

Then the proof outline is:

$\{\mathtt{n} = N \wedge \mathtt{n} \geq 0\}$
$\models$
$\{(0^2 \leq \mathtt{n} \Rightarrow 0 = 0) \wedge (0^2 > \mathtt{n} \Rightarrow 0 = 0 + 1) \wedge 0^2 \leq \mathtt{n} \wedge \mathtt{n} = N \wedge 0 \geq 0\}$

```
y := 0;
```

$\{(\mathtt{y}^2 \leq \mathtt{n} \Rightarrow \mathtt{y} = 0) \wedge (\mathtt{y}^2 > \mathtt{n} \Rightarrow \mathtt{y} = 0 + 1) \wedge 0^2 \leq \mathtt{n} \wedge \mathtt{n} = N \wedge 0 \geq 0\}$

```
z := 0;
```

$\{(\mathtt{y}^2 \leq \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z}) \wedge (\mathtt{y}^2 > \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z} + 1) \wedge \mathtt{z}^2 \leq \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{z} \geq 0\}$

```
while y*y < n do
```

$\{\mathtt{y}^2 < \mathtt{n} \wedge (\mathtt{y}^2 \leq \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z}) \wedge (\mathtt{y}^2 > \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z} + 1) \wedge \mathtt{z}^2 \leq \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{z} \geq 0\}$
$\models$ (1)
$\{(\mathtt{y} + 1 - 1)^2 < \mathtt{n} \wedge \mathtt{y} + 1 = \mathtt{z} + 1 \wedge \mathtt{z}^2 \leq \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{z} \geq 0\}$

```
y := y + 1;
```

$\{(\mathtt{y} - 1)^2 < \mathtt{n} \wedge \mathtt{y} = \mathtt{z} + 1 \wedge \mathtt{z}^2 \leq \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{z} \geq 0\}$

```
if y * y <= n then
```

$\{\mathtt{y}^2 \leq \mathtt{n} \wedge (\mathtt{y} - 1)^2 < \mathtt{n} \wedge \mathtt{y} = \mathtt{z} + 1 \wedge \mathtt{z}^2 \leq \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{z} \geq 0\}$
$\models$
$\{\mathtt{y}^2 \leq \mathtt{n} \wedge (\mathtt{y} - 1)^2 < \mathtt{n} \wedge \mathtt{y} = \mathtt{z} + 1 \wedge (\mathtt{z} + 1 - 1)^2 \leq \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{z} + 1 \geq 0\}$

```
z := z + 1
```

$\{\mathtt{y}^2 \leq \mathtt{n} \wedge (\mathtt{y} - 1)^2 < \mathtt{n} \wedge \mathtt{y} = \mathtt{z} \wedge (\mathtt{z} - 1)^2 \leq \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{z} \geq 0\}$
$\models$ (2)
$\{(\mathtt{y}^2 \leq \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z}) \wedge (\mathtt{y}^2 > \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z} + 1) \wedge \mathtt{z}^2 \leq \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{z} \geq 0\}$

```
else
```

$\{\neg(\mathtt{y}^2 \leq \mathtt{n}) \wedge (\mathtt{y} - 1)^2 < \mathtt{n} \wedge \mathtt{y} = \mathtt{z} + 1 \wedge \mathtt{z}^2 \leq \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{z} \geq 0\}$

```
skip
```

$\{\neg(\mathtt{y}^2 \leq \mathtt{n}) \wedge (\mathtt{y} - 1)^2 < \mathtt{n} \wedge \mathtt{y} = \mathtt{z} + 1 \wedge \mathtt{z}^2 \leq \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{z} \geq 0\}$
$\models$ (2)
$\{(\mathtt{y}^2 \leq \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z}) \wedge (\mathtt{y}^2 > \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z} + 1) \wedge \mathtt{z}^2 \leq \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{z} \geq 0\}$

```
end
```

$\{(\mathtt{y}^2 \leq \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z}) \wedge (\mathtt{y}^2 > \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z} + 1) \wedge \mathtt{z}^2 \leq n \wedge \mathtt{n} = N \wedge \mathtt{z} \geq 0\}$

```
end
```

$\{\neg(\mathtt{y}^2 < \mathtt{n}) \wedge (\mathtt{y}^2 \leq \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z}) \wedge (\mathtt{y}^2 > \mathtt{n} \Rightarrow \mathtt{y} = \mathtt{z} + 1) \wedge \mathtt{z}^2 \leq \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{z} \geq 0\}$
$\models$ (3)
$\{\mathtt{z}^2 \leq N \wedge N < (\mathtt{z} + 1)^2\}$

(1) $\mathtt{y}^2 < \mathtt{n}$ and $\mathtt{y} \leq \mathtt{n}^2 \Rightarrow \mathtt{y} = \mathtt{z}$ imply $\mathtt{y} = \mathtt{z}$

(2) As either $\mathtt{y}^2 > \mathtt{n}$ or $\mathtt{y}^2 \leq \mathtt{n}$ are false, they vacuously imply the right hand side.

(3) $N < (z + 1)^2$ can be shown by a case distinction on y:

case $y^2 < n$**:** As $y^2 \geq n$, this case is not possible.

case $y^2 = n$**:** $y^2 = n \wedge (y^2 \leq n \Rightarrow y = z)$ implies $y^2 = z^2$ and then $N = n = y^2 = z^2 < (z + 1)^2$
The last step requires $z \geq 0$

case $y^2 > n$**:** $y^2 > n \land (y^2 > n \Rightarrow y = z + 1)$ implies $y^2 = (z + 1)^2$ and then $N = n < y^2 = (z + 1)^2$

Task 2.4. Recall that the variant must be at least 0 (provided that the loop condition holds). $n - y * y$ is an easy variant, since y increases, so the variant clearly decreases, and we directly get from the loop condition that it is at least 0. $n - y$ also works, but it requires more work to prove that it is not negative.