ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

D. Basin and P. Müller

Formal Methods and Functional Programming

Solutions of Exercise Sheet 12: Axiomatic Semantics

Assignment 1

(a) (try by hand)

(b) The loop invariant isn't true when the loop is first reached.

(c) The loop invariant isn't (always) preserved by executing the loop body (in particular, for the last iteration).

(d) The loop invariant along with the negated while-condition doesn't give us enough information about the value of `i` to show the post-condition.

(e) One possibility is $K = \mathtt{k} \wedge \mathtt{i} \leq \mathtt{k} \wedge \mathtt{r} = \mathtt{n}^{\mathtt{i}}$ where K is the original value of the variable `k`.

(f) We show $\vdash \{\, \mathtt{k} \geq 1 \ \wedge K = \mathtt{k} \,\}\ s\ \{\, \mathtt{r} = \mathtt{n}^K \,\}$ as follows:

$\{\, \mathtt{k} \geq 1 \wedge K = \mathtt{k} \,\}$
$\Rightarrow$
$\{\, K = \mathtt{k} \wedge \mathtt{k} \geq 1 \wedge 0 = 0 \,\}$
`i := 0;`
$\{\, K = \mathtt{k} \wedge \mathtt{k} \geq 1 \wedge \mathtt{i} = 0 \,\}$
$\Rightarrow$
$\{\, K = \mathtt{k} \wedge \mathtt{k} \geq 1 \wedge \mathtt{i} = 0 \wedge 1 = 1 \,\}$
`r := 1;`
$\{\, K = \mathtt{k} \wedge \mathtt{k} \geq 1 \wedge \mathtt{i} = 0 \wedge \mathtt{r} = 1 \,\}$
$\Rightarrow$
$\{\, K = \mathtt{k} \wedge \mathtt{i} \leq \mathtt{k} \wedge \mathtt{r} = \mathtt{n}^{\mathtt{i}} \,\}$
`while i<k do`
$\{\, K = \mathtt{k} \wedge \mathtt{i} \leq \mathtt{k} \wedge \mathtt{r} = \mathtt{n}^{\mathtt{i}} \wedge \mathtt{i} < \mathtt{k} \,\}$
$\Rightarrow$
$\{\, K = \mathtt{k} \wedge \mathtt{i} + 1 \leq \mathtt{k} \wedge \mathtt{r} * \mathtt{n} = \mathtt{n}^{\mathtt{i}+1} \,\}$

$\mathtt{i} := \mathtt{i} + 1;$

$\{\, K = \mathtt{k} \wedge \mathtt{i} \leq \mathtt{k} \wedge \mathtt{r} * \mathtt{n} = \mathtt{n}^{\mathtt{i}} \,\}$

$\mathtt{r} := \mathtt{r} * \mathtt{n}$

$\{\, K = \mathtt{k} \wedge \mathtt{i} \leq \mathtt{k} \wedge \mathtt{r} = \mathtt{n}^{\mathtt{i}} \,\}$

end

$\{\, K = \mathtt{k} \wedge \mathtt{i} \geq \mathtt{k} \wedge \mathtt{i} \leq \mathtt{k} \wedge \mathtt{r} = \mathtt{n}^{\mathtt{i}} \,\}$
$\Rightarrow$
$\{\, \mathtt{r} = \mathtt{n}^{K} \,\}$

(g) One possibility is $X = \mathtt{x} + Y * \mathtt{z}$, where X and Y are the original values of x and y, respectively.

(h) One possibility is $\mathtt{x} \leq \mathtt{y} \wedge (\mathtt{x} + \mathtt{y})/2 = (X + Y)/2$, where X and Y are the original values of x and y, respectively.

Assignment 2

$\{\mathtt{n} = N \wedge \mathtt{n} \geq 1\}$
$\Rightarrow$
$\{\mathtt{n} = N \wedge \mathtt{n} \geq 1 \wedge 1 = 1 \wedge 0 = 0\}$
`a := 1;`
$\{\mathtt{n} = N \wedge \mathtt{n} \geq 1 \wedge \mathtt{a} = 1 \wedge 0 = 0\}$
`b := 0;`
$\{\mathtt{n} = N \wedge \mathtt{n} \geq 1 \wedge \mathtt{a} = 1 \wedge \mathtt{b} = 0\}$
$\Rightarrow$
$\{(\mathtt{a} \leq \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}}) \wedge (\mathtt{a} > \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}+1}) \wedge 10^{\mathtt{b}} \leq \mathtt{n} \wedge \mathtt{n} = N\}$
`while a<n do`
  $\{(\mathtt{a} \leq \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}}) \wedge (\mathtt{a} > \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}+1}) \wedge 10^{\mathtt{b}} \leq \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{a} < \mathtt{n}\}$
  $\Rightarrow$
  $\{\mathtt{a} * 10 = 10^{\mathtt{b}+1} \wedge 10^{\mathtt{b}} < \mathtt{n} \wedge \mathtt{n} = N\}$
  `a := a*10;`
  $\{\mathtt{a} = 10^{\mathtt{b}+1} \wedge 10^{\mathtt{b}} < \mathtt{n} \wedge \mathtt{n} = N\}$
  `if (a <= n) then`
    $\{\mathtt{a} = 10^{\mathtt{b}+1} \wedge 10^{\mathtt{b}} < \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{a} \leq \mathtt{n}\}$
    $\Rightarrow$
    $\{\mathtt{a} = 10^{\mathtt{b}+1} \wedge 10^{\mathtt{b}+1-1} < \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{a} \leq \mathtt{n}\}$
    `b := b+1`
    $\{\mathtt{a} = 10^{\mathtt{b}} \wedge 10^{\mathtt{b}-1} < \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{a} \leq \mathtt{n}\}$
    $\Rightarrow$
    $\{(\mathtt{a} \leq \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}}) \wedge (\mathtt{a} > \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}+1}) \wedge 10^{\mathtt{b}} \leq \mathtt{n} \wedge \mathtt{n} = N\}$
  `else`
    $\{\mathtt{a} = 10^{\mathtt{b}+1} \wedge 10^{\mathtt{b}} < \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{a} > \mathtt{n}\}$
    `skip`
    $\{\mathtt{a} = 10^{\mathtt{b}+1} \wedge 10^{\mathtt{b}} < \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{a} > \mathtt{n}\}$
    $\Rightarrow$
    $\{(\mathtt{a} \leq \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}}) \wedge (\mathtt{a} > \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}+1}) \wedge 10^{\mathtt{b}} \leq \mathtt{n} \wedge \mathtt{n} = N\}$
  `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`
$\{(\mathtt{a} \leq \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}}) \wedge (\mathtt{a} > \mathtt{n} \Rightarrow \mathtt{a} = 10^{\mathtt{b}+1}) \wedge 10^{\mathtt{b}} \leq \mathtt{n} \wedge \mathtt{n} = N \wedge \mathtt{a} \geq \mathtt{n}\}$
$\Rightarrow^{\star}$
$\{10^{\mathtt{b}} \leq N \wedge N < 10^{\mathtt{b}+1}\}$

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

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

Assignment 3

The intuition of the **sound rule of consequence** is the following: if we execute a statement s in a state satisfying the constraints $\mathbf{P}'$ (the precondition, e.g. $x \geq 0$) and if the final state satisfies the constraints $\mathbf{Q}'$ (the postcondition, e.g., $x \leq 0$), we then can conclude that s will also execute successfully in a state satisfying the *stronger* constraints $\mathbf{P}$ (e.g. $x \geq 5$) and that the final state at least satisfies the *weaker* constraints $\mathbf{Q}$ (e.g., $x \leq 5$).

Assume we have proved the triple $\{\ x \geq 0\ \}\ s\ \{\ x \leq 0\ \}$ for an algorithm that we implemented as s and that now is to be used by our co-worker Alice.
She does not need to know the actual implementation, but we provide her with the pre- and postcondition (the *contract*) so that she knows when (i.e., in which states) she can successfully use our algorithm and which final states her own program needs to be able to handle afterwards.

We could provide her with the conditions $\mathbf{P}'$ and $\mathbf{Q}'$, but we decide to give her $\mathbf{P}$ and $\mathbf{Q}$ instead. This is valid, because our algorithm s will execute successfully if invoked in a state where $x \geq 5$, since we proved that it does so in all states where $x \geq 0$.
Due to the postcondition $\mathbf{Q}$ that we gave her, Alice implemented her program in a way such that it successfully operates on all states where $x \leq 5$. This is perfectly fine since s only yields final states where $x \leq 0$.

Now consider the **unsound rule**. This time, let $\mathbf{P}'$, $\mathbf{Q}'$, $\mathbf{P}$ and $\mathbf{Q}$ be $x \geq 5$, $x \leq 5$, $x \geq 0$ and $x \leq 0$, respectively.

If Alice invokes s in a state where $x \geq 0$, an error might occur since our algorithm only guarantees successful termination in all states where $x \geq 5$.
Analogously, if Alice expects that the states resulting from the invocation of s satisfy $x \leq 0$, her own computations might fail since s can actually yield states where $x \leq 5$.

Let's consider **concrete counterexamples** where $\{\ \mathbf{P}'\ \}\ s\ \{\ \mathbf{Q}'\ \}$ is a valid triple, where $\mathbf{P}' \Rightarrow \mathbf{P}$ and $\mathbf{Q} \Rightarrow \mathbf{Q}'$, but where $\{\ \mathbf{P}\ \}\ s\ \{\ \mathbf{Q}\ \}$ is not a valid triple. For example, consider:

$$\frac{\{\ \mathtt{x} > 1\ \}\ \mathtt{x} := \mathtt{x} + 1\ \{\ x > 2\ \}}{\{\ \mathtt{x} \geq 1\ \}\ \mathtt{x} := \mathtt{x} + 1\ \{\ x > 2\ \}}\ \text{unsound } \textsc{Cons}$$

If we begin a state where $x = 1$ then the precondition of this triple holds, but after execution of the statement, the postcondition of the triple will be false. Therefore, this rule allows us to deduce unsound conclusions.

Similarly, the following example shows that strengthening the post-condition leads to unsoundness:

$$\frac{\{\ \mathtt{x} \geq 1\ \}\ \mathtt{x} := \mathtt{x} + 1\ \{\ x \geq 2\ \}}{\{\ \mathtt{x} \geq 1\ \}\ \mathtt{x} := \mathtt{x} + 1\ \{\ x > 2\ \}}\ \text{unsound } \textsc{Cons}$$

Assignment 4

The right-to-left direction ($\Leftarrow$) can be shown directly: Suppose that there exists R with $\vdash \{\ P\ \}\ s_1\ \{\ R\ \}$ and $\vdash \{\ R\ \}\ s_2\ \{\ Q\ \}$. Then we can construct the following derivation:

$$\frac{\{\ P\ \}\ s_1\ \{\ R\ \}\quad \{\ R\ \}\ s_2\ \{\ Q\ \}}{\{\ P\ \}\ s_1; s_2\ \{\ Q\ \}}\ \textsc{Seq}_{Ax}$$

For the left-to-right direction ($\Rightarrow$) we proceed by induction on the shape of the derivation of $\{\ P\ \}\ s_1; s_2\ \{\ Q\ \}$, considering cases for the last rule applied. Given the form of the statement, there are only two possible cases - either the rule for sequential composition or the rule of consequence was the last rule applied:

Case 1 - sequential composition rule: Then we are done, since, from the form of the rule, there must be some predicate R such that we have derivations for $\{\ P\ \}\ s_1\ \{\ R\ \}$ and $\{\ R\ \}\ s_2\ \{\ Q\ \}$, as required.

Case 2 - rule of consequence: Then from the form of the rule, there must be some predicates P' and Q' such that $P \Rightarrow P'$ and $Q' \Rightarrow Q$ and we have a (sub-)derivation for $\{\ P'\ \}\ s_1; s_2\ \{\ Q'\ \}$. By applying the induction hypothesis to this sub-derivation, we know that there exists R' such that $\vdash \{\ P'\ \}\ s_1\ \{\ R'\ \}$ and $\vdash \{\ R'\ \}\ s_2\ \{\ Q'\ \}$. Using the rule of consequence, we can extend these two derivations:

$$\frac{\{\ P'\ \}\ s_1\ \{\ R'\ \}}{\{\ P\ \}\ s_1\ \{\ R'\ \}}\ \textsc{Cons}_{Ax}\qquad \frac{\{\ R'\ \}\ s_2\ \{\ Q'\ \}}{\{\ R'\ \}\ s_2\ \{\ Q\ \}}\ \textsc{Cons}_{Ax}$$

Then we are done, choosing R to be R'.

Assignment 5 - Headache of the week

(a) $\{\ \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0 \wedge X_0 > 0 \wedge Y_0 > 0\ \}\ s\ \{\ \mathtt{z} = \mathit{gcd}(X_0, Y_0))\ \}$

(b) A suitable loop invariant is: $\mathit{gcd}(\mathtt{x}, \mathtt{y}) = \mathit{gcd}(\mathtt{b}, \mathtt{c}) \wedge \mathtt{b} > 0 \wedge \mathtt{c} > 0 \wedge \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0$ (preservation shown below)

(c) Here is the proof outline:

$\{\mathtt{x} = X_0 \wedge \mathtt{y} = Y_0 \wedge X_0 > 0 \wedge Y_0 > 0\}$
`b := x;`
$\{\mathtt{x} = X_0 \wedge \mathtt{y} = Y_0 \wedge X_0 > 0 \wedge Y_0 > 0 \wedge \mathtt{b} = X_0\}$
`c := y;`
$\{\mathtt{x} = X_0 \wedge \mathtt{y} = Y_0 \wedge X_0 > 0 \wedge Y_0 > 0 \wedge \ b = X_0 \wedge \ c = Y_0\}$
$\Rightarrow$
$\{\mathit{gcd}(\mathtt{x},\mathtt{y}) = \mathit{gcd}(\mathtt{b},\mathtt{c}) \wedge \mathtt{b} > 0 \wedge \mathtt{c} > 0 \wedge \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0\}$
`while b#c do`
  $\{\mathit{gcd}(\mathtt{x},\mathtt{y}) = \mathit{gcd}(\mathtt{b},\mathtt{c}) \wedge \mathtt{b} > 0 \wedge \mathtt{c} > 0 \wedge \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0 \wedge \mathtt{b} \neq \mathtt{c}\}$
  `if b < c then`
    $\{\mathit{gcd}(\mathtt{x},\mathtt{y}) = \mathit{gcd}(\mathtt{b},\mathtt{c}) \wedge \mathtt{b} > 0 \wedge \mathtt{c} > 0 \wedge \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0 \wedge \mathtt{b} \neq \mathtt{c} \wedge \mathtt{b} < \mathtt{c}\}$
    $\Rightarrow$
    $\{\mathit{gcd}(\mathtt{x},\mathtt{y}) = \mathit{gcd}(\mathtt{b},(\mathtt{c}-\mathtt{b}+\mathtt{b})) \wedge \mathtt{b} > 0 \wedge (\mathtt{c}-\mathtt{b}) > 0 \wedge \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0 \wedge \mathtt{b} < (\mathtt{c}-\mathtt{b}+\mathtt{b})\}$
    `c := c - b;`
    $\{\mathit{gcd}(\mathtt{x},\mathtt{y}) = \mathit{gcd}(\mathtt{b},(\mathtt{c}+\mathtt{b})) \wedge \mathtt{b} > 0 \wedge \mathtt{c} > 0 \wedge \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0 \wedge \mathtt{b} < (\mathtt{c}+\mathtt{b})\}$
    $\Rightarrow$
    $\{\mathit{gcd}(\mathtt{x},\mathtt{y}) = \mathit{gcd}(\mathtt{b},\mathtt{c}) \wedge \mathtt{b} > 0 \wedge \mathtt{c} > 0 \wedge \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0\}$
  `else`
    $\{\mathit{gcd}(\mathtt{x},\mathtt{y}) = \mathit{gcd}(\mathtt{b},\mathtt{c}) \wedge \mathtt{b} > 0 \wedge \mathtt{c} > 0 \wedge \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0 \wedge \mathtt{b} \neq \mathtt{c} \wedge \mathtt{b} \geq \mathtt{c}\}$
    $\Rightarrow$
    $\{\mathit{gcd}(\mathtt{x},\mathtt{y}) = \mathit{gcd}((\mathtt{b}-\mathtt{c}+\mathtt{c}),\mathtt{c}) \wedge (\mathtt{b}-\mathtt{c}) > 0 \wedge \mathtt{c} > 0 \wedge \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0 \wedge (\mathtt{b}-\mathtt{c}+\mathtt{c}) > \mathtt{c}\}$
    `b := b - c;`
    $\{\mathit{gcd}(\mathtt{x},\mathtt{y}) = \mathit{gcd}((\mathtt{b}+\mathtt{c}),\mathtt{c}) \wedge \mathtt{b} > 0 \wedge \mathtt{c} > 0 \wedge \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0 \wedge (\mathtt{b}+\mathtt{c}) > \mathtt{c}\}$
    $\Rightarrow$
    $\{\mathit{gcd}(\mathtt{x},\mathtt{y}) = \mathit{gcd}(\mathtt{b},\mathtt{c}) \wedge \mathtt{b} > 0 \wedge \mathtt{c} > 0 \wedge \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0\}$
  `end`
  $\{\mathit{gcd}(\mathtt{x},\mathtt{y}) = \mathit{gcd}(\mathtt{b},\mathtt{c}) \wedge \mathtt{b} > 0 \wedge \mathtt{c} > 0 \wedge \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0\}$
`end;`
$\{\mathit{gcd}(\mathtt{x},\mathtt{y}) = \mathit{gcd}(\mathtt{b},\mathtt{c}) \wedge \mathtt{b} > 0 \wedge \mathtt{c} > 0 \wedge \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0 \wedge \mathtt{b} = \mathtt{c}\}$
`z := b`
$\{\mathit{gcd}(\mathtt{x},\mathtt{y}) = \mathit{gcd}(\mathtt{b},\mathtt{c}) \wedge \mathtt{b} > 0 \wedge \mathtt{c} > 0 \wedge \mathtt{x} = X_0 \wedge \mathtt{y} = Y_0 \wedge \mathtt{b} = \mathtt{c} \wedge \mathtt{z} = \mathtt{b}\}$
$\Rightarrow$
$\{\mathtt{z} = \mathit{gcd}(X_0, Y_0)\}$