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 2

Assignment 1

We first present a solution that proves a more general result using one of the extra rules described in the extra material (available from the course website). Then, we also give a straight-forward solution that proves the claim directly.

(a) Assuming X_0 is the original value of x, a suitable loop invariant is $\mathtt{x} = X_0 \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x}$.

(b) A suitable loop variant is $(\mathtt{x} - \mathtt{z})$. We can now prove the following triple, characterising the general behaviour of the statement s (using the invariant and variant above): $\{\ \mathtt{x} = X_0 \wedge X_0 \geq 0\ \}\ s\ \{\ \Downarrow \mathtt{x} = X_0 \wedge \mathtt{y} = 2^{X_0}\ \}$. Here is the proof outline:

$\{\mathtt{x} = X_0 \wedge X_0 \geq 0\}$
$\Rightarrow$
$\{\mathtt{x} = X_0 \wedge X_0 \geq 0 \wedge 1 = 1\}$
`y := 1;`
$\{\mathtt{x} = X_0 \wedge X_0 \geq 0 \wedge \mathtt{y} = 1\}$
$\Rightarrow$
$\{\mathtt{x} = X_0 \wedge X_0 \geq 0 \wedge \mathtt{y} = 1 \wedge 0 = 0\}$
`z := 0;`
$\{\mathtt{x} = X_0 \wedge X_0 \geq 0 \wedge \mathtt{y} = 1 \wedge \mathtt{z} = 0\}$
$\Rightarrow$
$\{\mathtt{x} = X_0 \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x}\}$
`while z<x do`
  $\{\mathtt{x} = X_0 \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x} \wedge \mathtt{z} < \mathtt{x} \wedge (\mathtt{x} - \mathtt{z}) = V_0\}^\star$
  $\Rightarrow$
  $\{\mathtt{x} = X_0 \wedge \mathtt{y} \cdot 2 = 2^{\mathtt{z}+1} \wedge \mathtt{z} + 1 \leq \mathtt{x} \wedge (\mathtt{x} - (\mathtt{z} + 1)) < V_0\}$
  `y := y * 2;`
  $\{\mathtt{x} = X_0 \wedge \mathtt{y} = 2^{\mathtt{z}+1} \wedge \mathtt{z} + 1 \leq \mathtt{x} \wedge (\mathtt{x} - (\mathtt{z} + 1)) < V_0\}$
  `z := z + 1`
  $\{\Downarrow \mathtt{x} = X_0 \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x} \wedge (\mathtt{x} - \mathtt{z}) < V_0\}$
`end`
$\{\Downarrow \mathtt{x} = X_0 \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x} \wedge \mathtt{z} \geq \mathtt{x}\}$
$\Rightarrow$
$\{\Downarrow \mathtt{x} = X_0 \wedge \mathtt{y} = 2^{X_0}\}$

* *side-condition: this predicate implies* $(\mathtt{x} - \mathtt{z}) \geq 0$

However, the next part of the question requires us to make use of this loop in a more-specific context (when we know $\mathtt{x} = 10$ in the precondition, and do not use the logical variable X_0).

(c) We wish to prove that $\vdash \{\ \mathtt{x} = 10\ \}\ s\ \{\ \Downarrow \mathtt{y} = 1024\ \}$. We could of course construct an entirely new proof outline to show this triple. However, the recipe above tells us how to adapt our existing proof to this more-specific context: using the recipe we can re-use our previous proof for the loop. Firstly, we need to find an expression e such that $X_0 = e$ in the precondition of s. Here, we obviously choose e to be 10. Now, according to the recipe, we can adapt our proven assertion $\{\ \mathtt{x} = X_0 \wedge X_0 \geq 0\ \}\ s\ \{\ \Downarrow \mathtt{x} = X_0 \wedge \mathtt{y} = 2^{X_0}\ \}$ to the new assertion $\{\ (X_0 \geq 0)[\mathtt{x}/X_0] \wedge \mathtt{x} = 10\ \}\ s\ \{\ \Downarrow (\mathtt{x} = X_0 \wedge \mathtt{y} = 2^{X_0})[10/X_0]\ \}$, i.e., we obtain the triple $\{\ \mathtt{x} \geq 0 \wedge \mathtt{x} = 10\ \}\ s\ \{\ \Downarrow \mathtt{x} = 10 \wedge \mathtt{y} = 2^{10}\ \}$. Finally, we can obtain the desired triple using the rule of consequence:

$$\frac{\{\ \mathtt{x} \geq 0 \wedge \mathtt{x} = 10\ \}\ s\ \{\ \Downarrow x = 10 \wedge \mathtt{y} = 2^{10}\ \}}{\{\ \mathtt{x} = 10\ \}\ s\ \{\ \Downarrow \mathtt{y} = 1024\ \}}\ \textsc{Cons}$$

And now the solution that does not use the extra rule:

(a) A suitable loop invariant is $\mathtt{x} = 10 \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x}$.

(b) A suitable loop variant is $(\mathtt{x} - \mathtt{z})$, as before.

(c) We can now directly prove the claimed triple: $\vdash \{\ \mathtt{x} = 10\ \}\ s\ \{\ \Downarrow \mathtt{y} = 1024\ \}$. Here is the proof outline:

$\{\mathtt{x} = 10\}$
$\Rightarrow$
$\{\mathtt{x} = 10 \wedge 1 = 1\}$
`y := 1;`
$\{\mathtt{x} = 10 \wedge \mathtt{y} = 1\}$
$\Rightarrow$
$\{\mathtt{x} = 10 \wedge \mathtt{y} = 1 \wedge 0 = 0\}$
`z := 0;`
$\{\mathtt{x} = 10 \wedge \mathtt{y} = 1 \wedge \mathtt{z} = 0\}$
$\Rightarrow$
$\{\mathtt{x} = 10 \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x}\}$
`while z<x do`
  $\{\mathtt{x} = 10 \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x} \wedge \mathtt{z} < \mathtt{x} \wedge (\mathtt{x} - \mathtt{z}) = V_0\}^\star$
  $\Rightarrow$
  $\{\mathtt{x} = 10 \wedge \mathtt{y} \cdot 2 = 2^{\mathtt{z}+1} \wedge \mathtt{z} + 1 \leq \mathtt{x} \wedge (\mathtt{x} - (\mathtt{z} + 1)) < V_0\}$
  `y := y * 2;`
  $\{\mathtt{x} = 10 \wedge \mathtt{y} = 2^{\mathtt{z}+1} \wedge \mathtt{z} + 1 \leq \mathtt{x} \wedge (\mathtt{x} - (\mathtt{z} + 1)) < V_0\}$
  `z := z + 1`
  $\{\Downarrow \mathtt{x} = 10 \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x} \wedge (\mathtt{x} - \mathtt{z}) < V_0\}$
`end`
$\{\Downarrow \mathtt{x} = 10 \wedge \mathtt{y} = 2^{\mathtt{z}} \wedge \mathtt{z} \leq \mathtt{x} \wedge \mathtt{z} \geq \mathtt{x}\}$
$\Rightarrow$
$\{\Downarrow \mathtt{x} = 10 \wedge \mathtt{y} = 2^{10}\}$

* *side-condition: this predicate implies* $(\mathtt{x} - \mathtt{z}) \geq 0$

Assignment 2

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

$$\dfrac{\dfrac{\{ P' \}\ s_1\ \{ \Downarrow R' \} \quad \{ R' \}\ s_2\ \{ \Downarrow Q' \}}{\{ P' \}\ s_1; s_2\ \{ \Downarrow Q' \}}\ \textsc{Seq}}{\{ P \}\ s_1; s_2\ \{ \Downarrow Q \}}\ \textsc{Cons}$$

For the left-to-right direction ($\Rightarrow$) we proceed by induction on the structure of the derivation of $\{ P \}\ s_1; s_2\ \{ \Downarrow Q \}$, 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 from the form of the rule, there must be some predicate R such that we have derivations for $\{ P \}\ s_1\ \{ \Downarrow R \}$ and $\{ R \}\ s_2\ \{ Q \}$. Choosing P' to be P, Q' to be Q and R' to be R, we have exactly the four properties 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 $\{ P'' \}\ s_1; s_2\ \{ \Downarrow Q'' \}$. By applying the induction hypothesis to this sub-derivation, we know that there exist P',Q' and R' such that $P'' \Rightarrow P'$ and $Q' \Rightarrow Q''$ and $\vdash \{ P' \}\ s_1\ \{ \Downarrow R' \}$ and $\vdash \{ R' \}\ s_2\ \{ \Downarrow Q' \}$. By transitivity of implication, we have $P \Rightarrow P'$ and $Q' \Rightarrow Q$, which concludes the case.

Assignment 3

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

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

(b) See the lecture slides, p.210

(c) See the lecture slides, p.211

Assignment 4

Note that there are two ways to proceed - we could either apply the result of Sheet 12 Assignment 2 directly (twice), or work by induction on the structure of the assumed derivation, and then use Sheet 12 Assignment 2 (once) during the proof. The latter approach yields a simpler proof, since

the induction hypothesis makes everything straightforward in the case that the rule of consequence was the last applied.

We proceed by induction on the structure of the derivation of $\{\ P\ \}\ (s_1; s_2); s_3\ \{\ \Downarrow Q\ \}$, 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 from the form of the rule, there must be some predicate R such that we have derivations for $\{\ P\ \}\ (s_1; s_2)\ \{\ \Downarrow R\ \}$ and $\{\ R\ \}\ s_3\ \{\ \Downarrow Q\ \}$. By applying the result of Sheet 12 Assignment 2 to the former of these two derivations, we know that there exist predicates P',R',T' such that $P \Rightarrow P'$ and $R' \Rightarrow R$ and $\vdash \{\ P'\ \}\ s_1\ \{\ \Downarrow T'\ \}$ and $\vdash \{\ T'\ \}\ s_2\ \{\ \Downarrow R'\ \}$. Combining all of this information together, we can construct the following derivation:

$$\dfrac{\dfrac{\{\ P'\ \}\ s_1\ \{\ \Downarrow T'\ \} \qquad \dfrac{\{\ T'\ \}\ s_2\ \{\ \Downarrow R'\ \} \qquad \dfrac{\{\ R\ \}\ s_3\ \{\ \Downarrow Q\ \}}{\{\ R'\ \}\ s_3\ \{\ \Downarrow Q\ \}}\ \textsc{Cons}}{\{\ T'\ \}\ s_2; s_3\ \{\ \Downarrow Q\ \}}\ \textsc{Seq}}{\{\ P'\ \}\ s_1; (s_2; s_3)\ \{\ \Downarrow Q\ \}}\ \textsc{Seq}}{\{\ P\ \}\ s_1; (s_2; s_3)\ \{\ \Downarrow Q\ \}}\ \textsc{Cons}$$

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 $\{\ P'\ \}\ (s_1; s_2); s_3\ \{\ \Downarrow Q'\ \}$. By applying the induction hypothesis to this sub-derivation, we know that there exists a derivation of $\{\ P'\ \}\ s_1; (s_2; s_3)\ \{\ \Downarrow Q'\ \}$. Extending this new derivation by the rule of consequence, we obtain $\{\ P\ \}\ s_1; (s_2; s_3)\ \{\ \Downarrow Q\ \}$ as required.

Assignment 5 - Headache of the week

The code used for s is (as used in Sheet 7 question 1) as follows:

```
z := 0;
v := 0;
while v<y do
  v := 1;
  i := 0;
  while i<x do
    v := v*(z+1);
    i := i+1
  end;
  if v<=y then
    z := z+1
  else
    skip
```

```
  end
end
```

For the outer loop, the invariant used (see Sheet 7 solutions for a discussion of the main idea) is:

$$\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{\leq}\mathtt{y} \wedge (\mathtt{v}{\leq}\mathtt{y} \Rightarrow \mathtt{v}{=}\mathtt{z}^{\mathtt{x}}) \wedge (\mathtt{v}{>}\mathtt{y} \Rightarrow \mathtt{v}{=}(\mathtt{z}+1)^{\mathtt{x}})$$

and the variant used is $\max(0, (\mathtt{y} - \mathtt{v}))$.

For the inner loop, the invariant used is:

$$\mathtt{x}{=}X_0 \wedge X_0{>}0 \wedge \mathtt{i}{\leq}\mathtt{x} \wedge \mathtt{v}{=}(\mathtt{z}{+}1)^{\mathtt{i}} \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge \mathtt{y}{=}Y_0 \wedge V_0{=}(\mathtt{y} - \mathtt{z}^{\mathtt{x}})$$

where we use $(\mathtt{x} - \mathtt{i})$ as variant.

The proof outline is as follows:

$\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge Y_0{>}0\}$
$\Rightarrow$
$\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge Y_0{>}0 \wedge 0{=}0\}$
`z := 0;`
$\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge Y_0{>}0 \wedge \mathtt{z}{=}0\}$
$\Rightarrow$
$\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge Y_0{>}0 \wedge \mathtt{z}{=}0 \wedge 0{=}0\}$
`v := 0;`
$\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge Y_0{>}0 \wedge \mathtt{z}{=}0 \wedge \mathtt{v}{=}0\}$
$\Rightarrow$
$\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{\leq}\mathtt{y} \wedge (\mathtt{v}{\leq}\mathtt{y} \Rightarrow \mathtt{v}{=}\mathtt{z}^{\mathtt{x}}) \wedge (\mathtt{v}{>}\mathtt{y} \Rightarrow \mathtt{v}{=}(\mathtt{z}+1)^{\mathtt{x}})\}$
`while v<y do`
  $\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{\leq}\mathtt{y} \wedge (\mathtt{v}{\leq}\mathtt{y} \Rightarrow \mathtt{v}{=}\mathtt{z}^{\mathtt{x}}) \wedge (\mathtt{v}{>}\mathtt{y} \Rightarrow \mathtt{v}{=}(\mathtt{z}+1)^{\mathtt{x}}) \wedge \mathtt{v}{<}\mathtt{y} \wedge V_0{=}\max(0,(\mathtt{y}-\mathtt{v}))\}^{\star}$
  $\Rightarrow$
  $\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge V_0{=}(\mathtt{y}{-}\mathtt{z}^{\mathtt{x}}) \wedge 1 = 1\}$
  `v := 1;`
  $\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge V_0{=}(\mathtt{y}{-}\mathtt{z}^{\mathtt{x}}) \wedge \mathtt{v} = 1\}$
  $\Rightarrow$
  $\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge V_0{=}(\mathtt{y}{-}\mathtt{z}^{\mathtt{x}}) \wedge \mathtt{v} = 1 \wedge 0 = 0\}$
  `i := 0;`
  $\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge V_0{=}(\mathtt{y}{-}\mathtt{z}^{\mathtt{x}}) \wedge \mathtt{v} = 1 \wedge \mathtt{i} = 0\}$
  $\Rightarrow$
  $\{\mathtt{x}{=}X_0 \wedge X_0{>}0 \wedge \mathtt{i}{\leq}\mathtt{x} \wedge \mathtt{v}{=}(\mathtt{z}{+}1)^{\mathtt{i}} \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge \mathtt{y}{=}Y_0 \wedge V_0{=}(\mathtt{y}-\mathtt{z}^{\mathtt{x}})\}$
  `while i<x do`
    $\{\mathtt{x}{=}X_0 \wedge X_0{>}0 \wedge \mathtt{i}{\leq}\mathtt{x} \wedge \mathtt{v}{=}(\mathtt{z}{+}1)^{\mathtt{i}} \wedge \mathtt{i}{<}\mathtt{x} \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge \mathtt{y}{=}Y_0 \wedge V_0{=}(\mathtt{y}-\mathtt{z}^{\mathtt{x}}) \wedge V_1{=}(\mathtt{x}{-}\mathtt{i})\}^{\star\star}$
    $\Rightarrow$
    $\{\mathtt{x}{=}X_0 \wedge X_0{>}0 \wedge (\mathtt{i}{+}1){\leq}\mathtt{x} \wedge (\mathtt{v}{*}(\mathtt{z}{+}1)){=}(\mathtt{z}{+}1)^{\mathtt{i}+1} \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge \mathtt{y}{=}Y_0 \wedge V_0{=}(\mathtt{y}-\mathtt{z}^{\mathtt{x}}) \wedge (\mathtt{x}{-}(\mathtt{i}{+}1)){<}V_1\}$
    `v := v*(z+1);`
    $\{\mathtt{x}{=}X_0 \wedge X_0{>}0 \wedge (\mathtt{i}{+}1){\leq}\mathtt{x} \wedge \mathtt{v}{=}(\mathtt{z}{+}1)^{\mathtt{i}+1} \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge \mathtt{y}{=}Y_0 \wedge V_0{=}(\mathtt{y}-\mathtt{z}^{\mathtt{x}}) \wedge (\mathtt{x}{-}(\mathtt{i}{+}1)){<}V_1\}$
    `i := i+1`
    $\{\Downarrow \mathtt{x}{=}X_0 \wedge X_0{>}0 \wedge \mathtt{i}{\leq}\mathtt{x} \wedge \mathtt{v}{=}(\mathtt{z}{+}1)^{\mathtt{i}} \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge \mathtt{y}{=}Y_0 \wedge V_0{=}(\mathtt{y}-\mathtt{z}^{\mathtt{x}}) \wedge (\mathtt{x}{-}\mathtt{i}){<}V_1\}$
  `end;`
  $\{\Downarrow \mathtt{x}{=}X_0 \wedge X_0{>}0 \wedge \mathtt{i}{\leq}\mathtt{x} \wedge \mathtt{v}{=}(\mathtt{z}{+}1)^{\mathtt{i}} \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge \mathtt{y}{=}Y_0 \wedge V_0{=}(\mathtt{y}-\mathtt{z}^{\mathtt{x}}) \wedge \mathtt{i}{\geq}\mathtt{x}\}$
  $\Rightarrow$
  $\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{v}{=}(\mathtt{z}{+}1)^{\mathtt{x}} \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge V_0{=}(\mathtt{y}-\mathtt{z}^{\mathtt{x}})\}$
  `if v<=y then`
    $\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{v}{=}(\mathtt{z}{+}1)^{\mathtt{x}} \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge V_0{=}(\mathtt{y}-\mathtt{z}^{\mathtt{x}}) \wedge \mathtt{v}{\leq}\mathtt{y}\}$
    $\Rightarrow$
    $\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{v}{=}(\mathtt{z}{+}1)^{\mathtt{x}} \wedge \mathtt{v}{\leq}\mathtt{y} \wedge (\mathtt{z}{+}1){\geq}0 \wedge (\mathtt{z}{+}1{-}1)^{\mathtt{x}}{<}\mathtt{y} \wedge V_0{=}(\mathtt{y}-(\mathtt{z}{+}1{-}1)^{\mathtt{x}})\}$
    `z := z+1`
    $\{\Downarrow \mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{v}{=}\mathtt{z}^{\mathtt{x}} \wedge \mathtt{v}{\leq}\mathtt{y} \wedge \mathtt{z}{\geq}0 \wedge (\mathtt{z}{-}1)^{\mathtt{x}}{<}\mathtt{y} \wedge V_0{=}(\mathtt{y}-(\mathtt{z}{-}1)^{\mathtt{x}})\}$
    $\Rightarrow$
    $\{\Downarrow \mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{\leq}\mathtt{y} \wedge (\mathtt{v}{\leq}\mathtt{y} \Rightarrow \mathtt{v}{=}\mathtt{z}^{\mathtt{x}}) \wedge (\mathtt{v}{>}\mathtt{y} \Rightarrow \mathtt{v}{=}(z+1)^{\mathtt{x}}) \wedge \max(0,(\mathtt{y}-\mathtt{v})){<}V_0\}$
  `else`
    $\{\mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{v}{=}(\mathtt{z}{+}1)^{\mathtt{x}} \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge V_0{=}(\mathtt{y}-\mathtt{z}^{\mathtt{x}}) \wedge \mathtt{v}{>}\mathtt{y}\}$
    `skip`
    $\{\Downarrow \mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{v}{=}(\mathtt{z}{+}1)^{\mathtt{x}} \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge V_0{=}(\mathtt{y}-\mathtt{z}^{\mathtt{x}}) \wedge \mathtt{v}{>}\mathtt{y}\}$
    $\Rightarrow$
    $\{\Downarrow \mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{\leq}\mathtt{y} \wedge (\mathtt{v}{\leq}\mathtt{y} \Rightarrow \mathtt{v}{=}\mathtt{z}^{\mathtt{x}}) \wedge (\mathtt{v}{>}\mathtt{y} \Rightarrow \mathtt{v}{=}(\mathtt{z}+1)^{\mathtt{x}}) \wedge \max(0,(\mathtt{y}-\mathtt{v})){<}V_0\}$
  `end`
  $\{\Downarrow \mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{\leq}\mathtt{y} \wedge (\mathtt{v}{\leq}\mathtt{y} \Rightarrow \mathtt{v}{=}\mathtt{z}^{\mathtt{x}}) \wedge (\mathtt{v}{>}\mathtt{y} \Rightarrow \mathtt{v}{=}(\mathtt{z}+1)^{\mathtt{x}}) \wedge \max(0,(\mathtt{y}-\mathtt{v})){<}V_0\}$
`end`
$\{\Downarrow \mathtt{x}{=}X_0 \wedge \mathtt{y}{=}Y_0 \wedge X_0{>}0 \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{\leq}\mathtt{y} \wedge (\mathtt{v}{\leq}\mathtt{y} \Rightarrow \mathtt{v}{=}\mathtt{z}^{\mathtt{x}}) \wedge (\mathtt{v}{>}\mathtt{y} \Rightarrow \mathtt{v}{=}(\mathtt{z}+1)^{\mathtt{x}}) \wedge \mathtt{v}{\geq}\mathtt{y}\}$
$\Rightarrow$
$\{\Downarrow (\mathtt{v}{=}Y_0 \wedge \mathtt{v}{=}Z^{X_0} \wedge Z^{X_0}{\leq}Y_0 \wedge \mathtt{v}{\geq}Y_0) \vee (\mathtt{v}{>}Y_0 \wedge \mathtt{v}{=}(\mathtt{z}{+}1)^{X_0} \wedge \mathtt{z}^{X_0}{\leq}Y_0)\}$
$\Rightarrow$
$\{\Downarrow \mathtt{z}^{X_0}{\leq}Y_0 \wedge (\mathtt{z}{+}1)^{X_0} > Y_0\}$

* *side-condition: this predicate implies* $\max(0,(\mathtt{y}-\mathtt{v})) \geq 0$

** *side-condition: this predicate implies* $(\mathtt{x}{-}\mathtt{i}) \geq 0$

Assignment 6

(a) We use the following Promela model.

```
#define initX 3
#define initY 7

int x = initX, y = initY;

inline s() {
  y = 0;
  do
  :: x > 0 -> y = y + x; x = x - 2;
  :: else -> break
  od
}

init {
  printf("Starting in state where x = %d\n", x);
  s();
  assert y == 4;
  printf("Finishing in state where y = %d\n", y);
}
```

What changes do we need to make to the model if we want to use `proctype s()` instead of `inline s()`?

(b) The model is as follows.

```
init {
  int x;

  if
  :: x = 1
  :: x = 2; x = x + 2
  fi;

  assert (x == 1 || x == 4);
  printf("Value of x is %d\n", x);
}
```

(c) The model is as follows.

```
int x;

init {
```

```
  run Left();
  run Right();

  /* wait for processes to terminate */
  _nr_pr == 1;

  printf("Value of x is %d\n", x);
  assert x == 1 || x == 3 || x == 4;
}

proctype Left() {
  x = 1;
}

proctype Right() {
  x = 2;
  x = x + 2
}
```