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 13: Axiomatic Semantics, Total Correctness

Assignment 1

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

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

(c) The proof outline follows:

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

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

Assignment 2

The right-to-left direction ($\Leftarrow$) can be shown directly: Applying $\textsc{WhileToT}_{\textsc{Ax}}$ rule, to obtain $\vdash \{\ R\ \}$ `while` b `do` s `end` $\{\ \Downarrow R \wedge \neg b\ \}$, and then apply the rule of consequence to obtain $\vdash \{\ P\ \}$ `while` b `do` s `end` $\{\ \Downarrow Q\ \}$ as required.

For the left-to-right direction ($\Rightarrow$) we proceed by induction on the shape of the derivation of $\vdash \{\ P\ \}$ `while` b `do` s `end` $\{\ \Downarrow Q\ \}$, considering cases for the last rule applied. Given the form of the statement, there are only two possible cases - either the rule for while loops or the rule of consequence was the last rule applied:

Case 1 - while rule: Then from the form of the rule, we obtain $Q = P \wedge \neg b$ and $\vdash \{\ P \wedge b \wedge e' = Z\ \}\ s\ \{\ \Downarrow P \wedge e' < Z\ \}$. We can conclude by choosing R to be P and e' to be e.

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 $\vdash \{\ P'\ \}$ `while` b `do` s `end` $\{\ \Downarrow Q'\ \}$. By applying the induction hypothesis to this sub-derivation, we know that there exists some predicate R' and some expression e' such that $P' \Rightarrow R'$ and $R' \wedge \neg b \Rightarrow Q'$ and $R' \wedge b \Rightarrow e' \geq 0$ and $\vdash \{\ R' \wedge b \wedge e' = Z\ \}\ s\ \{\ \Downarrow R' \wedge e' < Z\ \}$.

From $P \Rightarrow P'$ and $P' \Rightarrow R'$, we obtain $P \Rightarrow R'$. Similarly, from $R' \wedge \neg b \Rightarrow Q'$ and $Q' \Rightarrow Q$ we obtain $R' \wedge \neg b \Rightarrow Q$. Then we are done, choosing $R = R'$ and $e' = e$.

Assignment 3

(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.206

(c) The proof outline is:

$\{\mathit{true}\}$
`while (L(year) and 366 < days or not L(year) and 365 < days) do`
$\{((\texttt{L(year)} \ \wedge \ 366 < \texttt{days}) \vee (\neg\texttt{L(year)} \ \wedge \ 365 < \texttt{days})) \ \wedge \ \texttt{days} = V\}^{\star}$
`if (L(year)) then`
$\{((\texttt{L(year)} \ \wedge \ 366 < \texttt{days}) \vee (\neg\texttt{L(year)} \ \wedge \ 365 < \texttt{days})) \ \wedge \ \texttt{days} = V \ \wedge \ \texttt{L(year)}\}$
$\Rightarrow$
$\{366 < \texttt{days} \ \wedge \ \texttt{days} = V \ \wedge \ \texttt{L(year)}\}$
$\Rightarrow$
$\{\texttt{days} - 366 < V\}$
`days := days - 366`
$\{\texttt{days} < V\}$
`else`
$\{((\texttt{L(year)} \ \wedge \ 366 < \texttt{days}) \vee (\neg\texttt{L(year)} \ \wedge \ 365 < \texttt{days})) \ \wedge \ \texttt{days} = V \ \wedge \ \neg\texttt{L(year)}\}$
$\Rightarrow$
$\{365 < \texttt{days} \ \wedge \ \texttt{days} = V \ \wedge \ \neg\texttt{L(year)}\}$
$\Rightarrow$
$\{\texttt{days} - 365 < V\}$
`days := days - 365`
$\{\texttt{days} < V\}$
`end;`
$\{\texttt{days} < V\}$
`y:=y+1`
$\{\texttt{days} < V\}$
`end`
$\{\Downarrow \mathit{true} \ \wedge \ \neg((\texttt{L(year)} \ \wedge \ 366 < \texttt{days}) \vee (\neg\texttt{L(year)} \ \wedge \ 365 < \texttt{days}))\}$
$\Rightarrow$
$\{\Downarrow \mathit{true}\}$

* *side-condition: this predicate implies* $\texttt{days} \geq 0$

Assignment 4

Note that there are two ways to proceed - we could either apply the result of Sheet 12, Assignment 4 directly (twice), or work by induction on the structure of the assumed derivation, and then use Sheet 12, Assignment 4 (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 $\{ \ P \ \} \ (s_1; s_2); s_3 \ \{ \ Q \ \}$, 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 $\{ \ P \ \} \ (s_1; s_2) \ \{ \ R \ \}$ and $\{ \ R \ \} \ s_3 \ \{ \ Q \ \}$. By applying the result of Sheet 12 Assignment 4 to the former of these two derivations, we know that there exists a predicate T, such that $\vdash \{ \ P \ \} \ s_1 \ \{ \ T \ \}$ and $\vdash \{ \ T \ \} \ s_2 \ \{ \ R \ \}$.

Combining all of this information together, we can construct the following derivation:

$$\dfrac{\{\ P\ \}\ s_1\ \{\ T\ \} \qquad \dfrac{\{\ T\ \}\ s_2\ \{\ R\ \} \quad \{\ R\ \}\ s_3\ \{\ Q\ \}}{\{\ T\ \}\ s_2; s_3\ \{\ Q\ \}}\ \textsc{Seq}}{\{\ P\ \}\ s_1; (s_2; s_3)\ \{\ Q\ \}}\ \textsc{Seq}$$

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

Assignment 5 - Headache of the week

Our code used for s is as follows (of course other solutions are possible):

```
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 is:

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

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

For the inner loop, the invariant used is:

$$\mathtt{x}{=}M \wedge M{>}0 \wedge \mathtt{i}{\leq}\mathtt{x} \wedge \mathtt{v}{=}(\mathtt{z}{+}1)^{\mathtt{i}} \wedge \mathtt{z}{\geq}0 \wedge \mathtt{z}^{\mathtt{x}}{<}\mathtt{y} \wedge \mathtt{y}{=}N \wedge V{=}(\mathtt{y} - \mathtt{z}^{\mathtt{x}})$$

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

The proof outline is as follows:

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

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

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