6.0/4.0 VU Formal Methods in Computer Science

Exercises Block 3

Tanja Sisel, sisel@logic.at

AB Theoretische Informatik und Logik
Institut für Computersprachen

May 2012

Program Syntax

Exercise

Show that the following TPL program is syntactically correct:

$$\textbf{if } x > 0 \textbf{ then while } x = y \textbf{ do } y := y + 1; \textbf{skip od else abort fi}$$

$\rightarrow$ try to construct program using TPL syntax

TPL Syntax (1)

Programs

$$
\begin{array}{rll}
\mathcal{P} ::= & \textbf{skip} & \text{no operation} \\
& \mid \textbf{abort} & \text{error exit} \\
& \mid \mathcal{V} := \mathcal{E} & \text{assignment} \\
& \mid \mathcal{P}; \mathcal{P} & \text{sequential composition} \\
& \mid \textbf{if } \mathcal{E} \textbf{ then } \mathcal{P} \textbf{ else } \mathcal{P} \textbf{ fi} & \text{if-then-else} \\
& \mid \textbf{while } \mathcal{E} \textbf{ do } \mathcal{P} \textbf{ od} & \text{loops}
\end{array}
$$

Expressions, Variables, Numerals and Operators

$$
\begin{array}{rl}
\mathcal{E} ::= & \mathcal{V} \mid \mathcal{N} \mid \mathcal{U}\,\mathcal{E} \mid (\mathcal{E}\,\mathcal{B}\,\mathcal{E}) \\
\mathcal{V} ::= & x \mid y \mid \cdots \mid x_0 \mid x_1 \mid \cdots \mid \text{any word except key words} \mid \cdots \\
\mathcal{N} ::= & 0 \mid 1 \mid \cdots \mid 9 \mid 10 \mid 11 \mid \cdots \mid 42 \mid \cdots \\
\mathcal{U} ::= & + \mid - \mid \neg \mid \cdots \\
\mathcal{B} ::= & + \mid - \mid * \mid / \mid < \mid \leq \mid = \mid \geq \mid > \mid \wedge \mid \vee \mid \Rightarrow \mid \cdots
\end{array}
$$

Program Syntax

$$\textbf{if } x > 0 \textbf{ then while } x = y \textbf{ do } y := y + 1; \textbf{skip od else abort fi}$$

$\mathcal{P}$

Program Syntax

if $x > 0$ **then while** $x = y$ **do** $y := y + 1;$ **skip od else abort fi**

$\mathcal{P} \Rightarrow$ **if** $\mathcal{E}$ **then** $\mathcal{P}$ **else** $\mathcal{P}$ **fi**

Program Syntax

$$\textbf{if } x > 0 \textbf{ then while } x = y \textbf{ do } y := y + 1; \textbf{skip od else abort fi}$$

$$\begin{aligned}\mathcal{P} &\Rightarrow \textbf{if } \mathcal{E} \textbf{ then } \mathcal{P} \textbf{ else } \mathcal{P} \textbf{ fi} \\ &\overset{*}{\Rightarrow} \textbf{if } (\mathcal{E}\,\mathcal{B}\,\mathcal{E}) \textbf{ then while } \mathcal{E} \textbf{ do } \mathcal{P} \textbf{ od else abort fi}\end{aligned}$$

Program Syntax

$$\textbf{if } x > 0 \textbf{ then while } x = y \textbf{ do } y := y + 1; \textbf{skip od else abort fi}$$

$$\begin{aligned}
\mathcal{P} &\Rightarrow \textbf{if } \mathcal{E} \textbf{ then } \mathcal{P} \textbf{ else } \mathcal{P} \textbf{ fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (\mathcal{E}\,\mathcal{B}\,\mathcal{E}) \textbf{ then while } \mathcal{E} \textbf{ do } \mathcal{P} \textbf{ od else abort fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (\mathcal{V} > \mathcal{N}) \textbf{ then while } (\mathcal{E}\,\mathcal{B}\,\mathcal{E}) \textbf{ do } \mathcal{P}; \mathcal{P} \textbf{ od else abort fi}
\end{aligned}$$

Program Syntax

$$\textbf{if } x > 0 \textbf{ then while } x = y \textbf{ do } y := y + 1; \textbf{skip od else abort fi}$$

$$\begin{aligned}
\mathcal{P} &\Rightarrow \textbf{if } \mathcal{E} \textbf{ then } \mathcal{P} \textbf{ else } \mathcal{P} \textbf{ fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (\mathcal{E}\,\mathcal{B}\,\mathcal{E}) \textbf{ then while } \mathcal{E} \textbf{ do } \mathcal{P} \textbf{ od else abort fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (\mathcal{V} > \mathcal{N}) \textbf{ then while } (\mathcal{E}\,\mathcal{B}\,\mathcal{E}) \textbf{ do } \mathcal{P}; \mathcal{P} \textbf{ od else abort fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (x > 0) \textbf{ then while } (\mathcal{V} = \mathcal{V}) \textbf{ do } \mathcal{V} := \mathcal{E}; \textbf{skip od else abort fi}
\end{aligned}$$

Program Syntax

$$\textbf{if } x > 0 \textbf{ then while } x = y \textbf{ do } y := y + 1; \textbf{skip od else abort fi}$$

$$\begin{aligned}
\mathcal{P} &\Rightarrow \textbf{if } \mathcal{E} \textbf{ then } \mathcal{P} \textbf{ else } \mathcal{P} \textbf{ fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (\mathcal{E}\,\mathcal{B}\,\mathcal{E}) \textbf{ then while } \mathcal{E} \textbf{ do } \mathcal{P} \textbf{ od else abort fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (\mathcal{V} > \mathcal{N}) \textbf{ then while } (\mathcal{E}\,\mathcal{B}\,\mathcal{E}) \textbf{ do } \mathcal{P}; \mathcal{P} \textbf{ od else abort fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (x > 0) \textbf{ then while } (\mathcal{V} = \mathcal{V}) \textbf{ do } \mathcal{V} := \mathcal{E}; \textbf{skip od else abort fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (x > 0) \textbf{ then while } (x = y) \textbf{ do } y := (\mathcal{E}\,\mathcal{B}\,\mathcal{E}); \textbf{skip od else abort fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (x > 0) \textbf{ then while } (x = y) \textbf{ do } y := (\mathcal{V} + \mathcal{N}); \textbf{skip od else abort fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (x > 0) \textbf{ then while } (x = y) \textbf{ do } y := (y + 1); \textbf{skip od else abort fi}
\end{aligned}$$

Program Syntax

$$\textbf{if } x > 0 \textbf{ then while } x = y \textbf{ do } y := y + 1; \textbf{skip od else abort fi}$$

$$\begin{aligned}
\mathcal{P} &\Rightarrow \textbf{if } \mathcal{E} \textbf{ then } \mathcal{P} \textbf{ else } \mathcal{P} \textbf{ fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (\mathcal{E}\,\mathcal{B}\,\mathcal{E}) \textbf{ then while } \mathcal{E} \textbf{ do } \mathcal{P} \textbf{ od else abort fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (\mathcal{V} > \mathcal{N}) \textbf{ then while } (\mathcal{E}\,\mathcal{B}\,\mathcal{E}) \textbf{ do } \mathcal{P}; \mathcal{P} \textbf{ od else abort fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (x > 0) \textbf{ then while } (\mathcal{V} = \mathcal{V}) \textbf{ do } \mathcal{V} := \mathcal{E}; \textbf{skip od else abort fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (x > 0) \textbf{ then while } (x = y) \textbf{ do } y := (\mathcal{E}\,\mathcal{B}\,\mathcal{E}); \textbf{skip od else abort fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (x > 0) \textbf{ then while } (x = y) \textbf{ do } y := (\mathcal{V} + \mathcal{N}); \textbf{skip od else abort fi} \\
&\overset{*}{\Rightarrow} \textbf{if } (x > 0) \textbf{ then while } (x = y) \textbf{ do } y := (y + 1); \textbf{skip od else abort fi} \\
&\sim \textbf{if } x > 0 \textbf{ then while } x = y \textbf{ do } y := y + 1; \textbf{skip od else abort fi}
\end{aligned}$$

TPL Statements

Exercise

- Define the syntax and semantics of TPL with **repeat** p **until** e statements instead of **while**-loops
- Extend the Hoare calculus accordingly.

The final definitions should not refer to **while**-statements.

TPL Statements

Exercise

- Define the syntax and semantics of TPL with **repeat** p **until** e statements instead of **while**-loops
- Extend the Hoare calculus accordingly.

The final definitions should not refer to **while**-statements.

Syntax

$$\mathcal{P} ::= \textbf{skip} \mid \cdots \mid \textbf{if } \mathcal{E} \textbf{ then } \mathcal{P} \textbf{ else } \mathcal{P} \textbf{ fi} \mid \textbf{repeat } \mathcal{P} \textbf{ until } \mathcal{E}$$

TPL Statements

Semantics

$$
\begin{aligned}
[\![\textbf{repeat } p \textbf{ until } e]\!]\,\sigma &= [\![p; \textbf{while } \neg e \textbf{ do } p \textbf{ od}]\!]\,\sigma \\
&= [\![\textbf{while } \neg e \textbf{ do } p \textbf{ od}]\!]\,[\![p]\!]\,\sigma
\end{aligned}
$$

TPL Statements

Semantics

$$
\begin{aligned}
[\textbf{repeat } p \textbf{ until } e]\,\sigma &= [p; \textbf{while } \neg e \textbf{ do } p \textbf{ od}]\,\sigma \\
&= [\textbf{while } \neg e \textbf{ do } p \textbf{ od}]\,[p]\,\sigma \\
&= \begin{cases} [\textbf{while } \neg e \textbf{ do } p \textbf{ od}]\,[p]\,[p]\,\sigma & \text{if } [\neg e]\,[p]\,\sigma \neq 0 \\ [p]\,\sigma & \text{if } [\neg e]\,[p]\,\sigma = 0 \end{cases}
\end{aligned}
$$

TPL Statements

Semantics

$$
\begin{aligned}
[\textbf{repeat}\ p\ \textbf{until}\ e]\,\sigma &= [p; \textbf{while}\ \neg e\ \textbf{do}\ p\ \textbf{od}]\,\sigma \\
&= [\textbf{while}\ \neg e\ \textbf{do}\ p\ \textbf{od}]\,[p]\,\sigma \\
&= \begin{cases} [\textbf{while}\ \neg e\ \textbf{do}\ p\ \textbf{od}]\,[p]\,[p]\,\sigma & \text{if } [\neg e]\,[p]\,\sigma \neq 0 \\ [p]\,\sigma & \text{if } [\neg e]\,[p]\,\sigma = 0 \end{cases} \\
&= \begin{cases} [p; \textbf{while}\ \neg e\ \textbf{do}\ p\ \textbf{od}]\,[p]\,\sigma & \text{if } [e]\,[p]\,\sigma = 0 \\ [p]\,\sigma & \text{if } [e]\,[p]\,\sigma \neq 0 \end{cases}
\end{aligned}
$$

TPL Statements

Semantics

$$
\begin{aligned}
[\textbf{repeat } p \textbf{ until } e]\,\sigma &= [p; \textbf{while } \neg e \textbf{ do } p \textbf{ od}]\,\sigma \\
&= [\textbf{while } \neg e \textbf{ do } p \textbf{ od}]\,[p]\,\sigma \\
&= \begin{cases} [\textbf{while } \neg e \textbf{ do } p \textbf{ od}]\,[p]\,[p]\,\sigma & \text{if } [\neg e]\,[p]\,\sigma \neq 0 \\ [p]\,\sigma & \text{if } [\neg e]\,[p]\,\sigma = 0 \end{cases} \\
&= \begin{cases} [p; \textbf{while } \neg e \textbf{ do } p \textbf{ od}]\,[p]\,\sigma & \text{if } [e]\,[p]\,\sigma = 0 \\ [p]\,\sigma & \text{if } [e]\,[p]\,\sigma \neq 0 \end{cases} \\
&= \begin{cases} [\textbf{repeat } p \textbf{ until } e]\,[p]\,\sigma & \text{if } [e]\,[p]\,\sigma = 0 \\ [p]\,\sigma & \text{if } [e]\,[p]\,\sigma \neq 0 \end{cases}
\end{aligned}
$$

TPL Statements

Hoare Calculus

$$\dfrac{\dfrac{\dfrac{\dfrac{}{}\ (\mathrm{wht}'')}{}\ (\mathrm{lc})}{}\ (\mathrm{sc})}{}$$

$$\dfrac{}{\{\, F \,\}\ \textbf{repeat}\ p\ \textbf{until}\ e\ \{\, G \,\}}$$

TPL Statements

Hoare Calculus

$$\dfrac{\dfrac{\dfrac{}{}\ (\mathrm{wht}'')}{}\ (\mathrm{lc})}{\dfrac{\{\,F\,\}\ p;\ \textbf{while}\ \neg e\ \textbf{do}\ p\ \textbf{od}\ \{\,G\,\}}{\{\,F\,\}\ \textbf{repeat}\ p\ \textbf{until}\ e\ \{\,G\,\}}}\ (\mathrm{sc})$$

TPL Statements

Hoare Calculus

$$
\dfrac{\dfrac{\{\,F\,\}\;p\;\{\,Inv\,\} \qquad \dfrac{\dfrac{\qquad\qquad}{\qquad\qquad}\;(\mathrm{wht}'')}{\{\,Inv\,\}\;\textbf{while}\;\neg e\;\textbf{do}\;p\;\textbf{od}\;\{\,G\,\}}\;(\mathrm{lc})}{\{\,F\,\}\;p;\textbf{while}\;\neg e\;\textbf{do}\;p\;\textbf{od}\;\{\,G\,\}}\;(\mathrm{sc})}{\{\,F\,\}\;\textbf{repeat}\;p\;\textbf{until}\;e\;\{\,G\,\}}
$$

TPL Statements

Hoare Calculus

$$
\dfrac{
  \dfrac{
    \{\, F \,\}\; p \;\{\, Inv \,\}
    \qquad
    \dfrac{
      \dfrac{}{\{\, Inv \,\}\;\textbf{while}\;\neg e\;\textbf{do}\;p\;\textbf{od}\;\{\, Inv \wedge e \,\}}\;(\mathrm{wht}'')
      \qquad
      Inv \wedge e \Rightarrow G
    }{
      \{\, Inv \,\}\;\textbf{while}\;\neg e\;\textbf{do}\;p\;\textbf{od}\;\{\, G \,\}
    }\;(\mathrm{lc})
  }{
    \{\, F \,\}\; p;\textbf{while}\;\neg e\;\textbf{do}\;p\;\textbf{od}\;\{\, G \,\}
  }\;(\mathrm{sc})
}{
  \{\, F \,\}\;\textbf{repeat}\;p\;\textbf{until}\;e\;\{\, G \,\}
}
$$

TPL Statements

Hoare Calculus

$$\dfrac{\{\, F \,\}\, p \,\{\, Inv \,\} \qquad \dfrac{\dfrac{\{\, Inv \wedge \neg e \wedge t = t_0 \,\}\, p \,\{\, Inv \wedge 0 \leq t < t_0 \,\}}{\{\, Inv \,\}\, \textbf{while } \neg e \textbf{ do } p \textbf{ od} \,\{\, Inv \wedge e \,\}}\,(\mathrm{wht}'') \qquad Inv \wedge e \Rightarrow G}{\{\, Inv \,\}\, \textbf{while } \neg e \textbf{ do } p \textbf{ od} \,\{\, G \,\}}\,(\mathrm{lc})}{\dfrac{\{\, F \,\}\, p; \textbf{while } \neg e \textbf{ do } p \textbf{ od} \,\{\, G \,\}}{\{\, F \,\}\, \textbf{repeat } p \textbf{ until } e \,\{\, G \,\}}}\,(\mathrm{sc})$$

TPL Statements

Hoare Calculus

$$\dfrac{\{\,F\,\}\,p\,\{\,Inv\,\} \qquad \dfrac{\dfrac{\{\,Inv \land \neg e \land t = t_0\,\}\,p\,\{\,Inv \land 0 \le t < t_0\,\}}{\{\,Inv\,\}\ \textbf{while}\ \neg e\ \textbf{do}\ p\ \textbf{od}\,\{\,Inv \land e\,\}}\,(\mathrm{wht}'') \qquad Inv \land e \Rightarrow G}{\{\,Inv\,\}\ \textbf{while}\ \neg e\ \textbf{do}\ p\ \textbf{od}\,\{\,G\,\}}\,(\mathrm{lc})}{\dfrac{\{\,F\,\}\,p;\ \textbf{while}\ \neg e\ \textbf{do}\ p\ \textbf{od}\,\{\,G\,\}}{\{\,F\,\}\ \textbf{repeat}\ p\ \textbf{until}\ e\,\{\,G\,\}}}\,(\mathrm{sc})$$

$$\frac{\{\,F\,\}\,p\,\{\,Inv\,\} \qquad \{\,Inv \land \neg e \land t = t_0\,\}\,p\,\{\,Inv \land 0 \le t < t_0\,\} \qquad Inv \land e \Rightarrow G}{\{\,F\,\}\ \textbf{repeat}\ p\ \textbf{until}\ e\,\{\,G\,\}}$$

Proving Total Correctness

Exercise

Prove the total correctness of the assertion below. You may have to strengthen the precondition to show termination.

$\{\, 1 \colon x = x_0 \,\}$
$y := 0;$
while $x \neq 0$ **do**
  $x := x - 2;$
  $y := y + 3$
od
$\{\, 2 \colon 2y = 3x_0 \,\}$

Hint: Use $3x + 2y = 3x_0$ as a starting point for the invariant.
Extend it if necessary to prove termination.

Proving Total Correctness

Total Correctness $=$ Partial Correctness $+$ Termination

Proving Total Correctness

Total Correctness = Partial Correctness + Termination

Reason for non-termination: loops!
$\rightarrow$ find bound function

Proving Total Correctness

Total Correctness = Partial Correctness + Termination

Reason for non-termination: loops!
$\rightarrow$ find bound function

2 approaches:

- Prove partial correctness and afterwards termination
- Prove total correctness $\rightarrow$ use rules for t.c.

Termination

How to find a bound function t

Termination

How to find a bound function t

- t is bounded from below: $INV \Rightarrow t \geq 0$

Termination

How to find a bound function t

- t is bounded from below: $INV \Rightarrow t \geq 0$
- t decreases in every loop iteration: $t < t_0$

Termination

How to find a bound function t

- t is bounded from below: $INV \Rightarrow t \geq 0$
- t decreases in every loop iteration: $t < t_0$
- t is integer

Termination

How to find a bound function t

- t is bounded from below: $INV \Rightarrow t \geq 0$
- t decreases in every loop iteration: $t < t_0$
- t is integer

while $x < y$ **do**
  $x := x + 1;$
  $y := y - 1;$
od

Termination

How to find a bound function t

- t is bounded from below: $INV \Rightarrow t \geq 0$
- t decreases in every loop iteration: $t < t_0$
- t is integer

while $x < y$ **do**
  $x := x + 1;$
  $y := y - 1;$
od

$t = (y - x)$

Termination

How to find a bound function t

- t is bounded from below: $INV \Rightarrow t \geq 0$
- t decreases in every loop iteration: $t < t_0$
- t is integer

while $x < y$ **do**
  $x := x + 1;$
  $y := y - 1;$
od

$t = (y - x) \qquad t \geq 0$

Termination

How to find a bound function t

- t is bounded from below: $INV \Rightarrow t \geq 0$
- t decreases in every loop iteration: $t < t_0$
- t is integer

while $x < y$ **do**
  $x := x + 1;$
  $y := y - 1;$
od

$t = (y - x) \qquad t \geq 0$

$x \neq y$ instead of $x < y$

Termination

How to find a bound function t

- t is bounded from below: $INV \Rightarrow t \geq 0$
- t decreases in every loop iteration: $t < t_0$
- t is integer

while $x < y$ **do**
  $x := x + 1;$
  $y := y - 1;$
od

$t = (y - x) \qquad t \geq 0$

$x \neq y$ instead of $x < y$
$t = (y - x) \qquad t \geq 0$ only if $x \leq y$

Termination

How to find a bound function t

- t is bounded from below: $INV \Rightarrow t \geq 0$
- t decreases in every loop iteration: $t < t_0$
- t is integer

while $x < y$ **do**
$x := x + 1;$
$y := y - 1;$
od

$t = (y - x) \qquad t \geq 0$

$x \neq y$ instead of $x < y$
$t = (y - x) \qquad t \geq 0$ only if $x \leq y \qquad \rightarrow$ add to INV

General Remarks

- $x > (x/2)$ only for $x > 0$

General Remarks

- $x > (x/2)$ only for $x > 0$
- Caution: Integers!

General Remarks

- $x > (x/2)$ only for $x > 0$
- Caution: Integers!

  Consequences:

  - $(x/2) \times 2 = x$ only for even numbers

General Remarks

- $x > (x/2)$ only for $x > 0$
- Caution: Integers!

  Consequences:

  - $(x/2) \times 2 = x$ only for even numbers
  - $x > y$ doesn't imply $(x/2) > (y/2)$

General Remarks

- $x > (x/2)$ only for $x > 0$
- Caution: Integers!

  Consequences:
  - $(x/2) \times 2 = x$ only for even numbers
  - $x > y$ doesn't imply $(x/2) > (y/2)$
- $x = x_0$ in PRE and $t = x$:

General Remarks

- $x > (x/2)$ only for $x > 0$
- Caution: Integers!

  Consequences:

  - $(x/2) \times 2 = x$ only for even numbers
  - $x > y$ doesn't imply $(x/2) > (y/2)$

- $x = x_0$ in PRE and $t = x$:

  Don't replace t_0 by x_0 to show termination $(t < t_0)$!!!

General Remarks

- $x > (x/2)$ only for $x > 0$
- Caution: Integers!

  Consequences:
  - $(x/2) \times 2 = x$ only for even numbers
  - $x > y$ doesn't imply $(x/2) > (y/2)$
- $x = x_0$ in PRE and $t = x$:

  Don't replace t_0 by x_0 to show termination $(t < t_0)$!!!
  - x_0: value of x at the beginning of the program
  - t_0: value of x at the beginning of the current loop iteration

Analyze Program

$\{\, 1\colon x = x_0 \,\}$
$y := 0;$
while $x \neq 0$ **do**
  $x := x - 2;$
  $y := y + 3$
od
$\{\, 2\colon 2y = 3x_0 \,\}$

Analyze Program

$\{\, 1\colon x = x_0 \,\}$
$y := 0;$
while $x \neq 0$ **do**
  $x := x - 2;$
  $y := y + 3$
od
$\{\, 2\colon 2y = 3x_0 \,\}$

Pre: $x = x_0$

Analyze Program

$\{\, 1\colon x = x_0 \,\}$
$y := 0;$
while $x \neq 0$ **do**
  $x := x - 2;$
  $y := y + 3$
od
$\{\, 2\colon 2y = 3x_0 \,\}$

Pre: $x = x_0 \land x \geq 0$

Analyze Program

$\{\, 1\colon\ x = x_0 \,\}$
$y := 0;$
while $x \neq 0$ **do**
    $x := x - 2;$
    $y := y + 3$
od
$\{\, 2\colon\ 2y = 3x_0 \,\}$

Pre: $x = x_0 \wedge x \geq 0 \wedge \text{even}(x)$

Analyze Program

$\{\, 1\colon x = x_0 \,\}$
$y := 0;$ $x := -2;$
while $x \neq 0$ **do**
  $x := x - 2;$
  $y := y + 3$
od
$\{\, 2\colon 2y = 3x_0 \,\}$

Pre: $x = x_0 \wedge x \geq 0 \wedge \text{even}(x)$

Analyze Program

$\{\, 1\colon\ x = x_0 \,\}$
$y := 0;$
while $x \neq 0$ **do**
  $x := x - 2;$
  $y := y + 3$
od
$\{\, 2\colon\ 2y = 3x_0 \,\}$

Pre: $x = x_0 \wedge x \geq 0 \wedge \text{even}(x)$

INV: $3x + 2y = 3x_0 \wedge x \geq 0 \wedge \text{even}(x)$

Analyze Program

$\{\, 1\colon x = x_0 \,\}$
$y := 0;$
while $x \neq 0$ **do**
  $x := x - 2;$
  $y := y + 3$
od
$\{\, 2\colon 2y = 3x_0 \,\}$

Pre: $x = x_0 \wedge x \geq 0 \wedge \mathrm{even}(x)$

INV: $3x + 2y = 3x_0 \wedge x \geq 0 \wedge \mathrm{even}(x)$

Bound function: ?

Analyze Program

$\{ 1\colon x = x_0 \}$
$y := 0;$
while $x \neq 0$ **do**
  $x := x - 2;$
  $y := y + 3$
od
$\{ 2\colon 2y = 3x_0 \}$

Pre: $x = x_0 \wedge x \geq 0 \wedge \text{even}(x)$

INV: $3x + 2y = 3x_0 \wedge x \geq 0 \wedge \text{even}(x)$

Bound function: x!

Hoare Calculus

T_0: $Inv \land e \land t = t_0$

T: $Inv \land 0 \leq t < t_0$

e: $x \neq 0$

t: x

H: $T[y/y+3]$

$$\{\, F \,\}\; y := 0;\, \textbf{while}\ e\ \textbf{do}\ x := x - 2; y := y + 3\ \textbf{od}\, \{\, G \,\}$$

Hoare Calculus

T_0: $Inv \wedge e \wedge t = t_0$ e: $x \neq 0$ H: $T[y/y+3]$
T: $Inv \wedge 0 \leq t < t_0$ t: x

$$\frac{\{\,F\,\}\ y := 0\ \{\,INV\,\} \qquad \{\,INV\,\}\ \textbf{while}\ e\ \textbf{do}\ \ldots \textbf{od}\ \{\,G\,\}}{\{\,F\,\}\ y := 0; \textbf{while}\ e\ \textbf{do}\ x := x - 2; y := y + 3\ \textbf{od}\ \{\,G\,\}}\ \text{(sc)}$$

Hoare Calculus

T_0: $Inv \wedge e \wedge t = t_0$ e: $x \neq 0$ H: $T[y/y+3]$

T: $Inv \wedge 0 \leq t < t_0$ t: x

$$\dfrac{\dfrac{F \Rightarrow I \quad \overset{\text{(as)}}{\{\, I \,\}\, y := 0 \,\{\, INV \,\}}}{\{\, F \,\}\, y := 0 \,\{\, INV \,\}}\ \text{(lc)} \qquad \{\, INV \,\}\ \textbf{while}\ e\ \textbf{do}\ \ldots \textbf{od}\ \{\, G \,\}}{\{\, F \,\}\, y := 0;\ \textbf{while}\ e\ \textbf{do}\ x := x - 2; y := y + 3\ \textbf{od}\ \{\, G \,\}}\ \text{(sc)}$$

Hoare Calculus

T_0: $Inv \wedge e \wedge t = t_0$ e: $x \neq 0$ H: $T[y/y+3]$
T: $Inv \wedge 0 \leq t < t_0$ t: x

$$\{\, INV \,\}\ \textbf{while}\ e\ \textbf{do}\ x := x - 2; y := y + 3\ \textbf{od}\ \{\, G \,\}$$

$$\dfrac{\dfrac{F \Rightarrow I \quad \overset{\text{(as)}}{\{\, I \,\}\ y := 0\ \{\, INV \,\}}}{\{\, F \,\}\ y := 0\ \{\, INV \,\}}\text{(lc)} \qquad \{\, INV \,\}\ \textbf{while}\ e\ \textbf{do}\ \ldots \textbf{od}\ \{\, G \,\}}{\{\, F \,\}\ y := 0; \textbf{while}\ e\ \textbf{do}\ x := x - 2; y := y + 3\ \textbf{od}\ \{\, G \,\}}\text{(sc)}$$

Hoare Calculus

T_0: $Inv \wedge e \wedge t = t_0$ e: $x \neq 0$ H: $T[y/y+3]$

T: $Inv \wedge 0 \leq t < t_0$ t: x

$$\frac{\{\, INV \,\}\ \textbf{while}\ e\ \textbf{do}\ x := x-2; y := y+3\ \textbf{od}\ \{\, INV \wedge \neg e \,\} \qquad INV \wedge \neg e \Rightarrow G}{\{\, INV \,\}\ \textbf{while}\ e\ \textbf{do}\ x := x-2; y := y+3\ \textbf{od}\ \{\, G \,\}}\ (\mathrm{lc})$$

$$\frac{\dfrac{F \Rightarrow I \quad \overset{(\mathrm{as})}{\{\, I \,\}\ y := 0\ \{\, INV \,\}}}{\{\, F \,\}\ y := 0\ \{\, INV \,\}}\ (\mathrm{lc}) \qquad \{\, INV \,\}\ \textbf{while}\ e\ \textbf{do}\ \ldots\ \textbf{od}\ \{\, G \,\}}{\{\, F \,\}\ y := 0; \textbf{while}\ e\ \textbf{do}\ x := x-2; y := y+3\ \textbf{od}\ \{\, G \,\}}\ (\mathrm{sc})$$

Hoare Calculus

T_0: $Inv \wedge e \wedge t = t_0$

T: $Inv \wedge 0 \leq t < t_0$

e: $x \neq 0$

t: x

H: $T[y/y+3]$

$$\dfrac{\dfrac{\{\, T_0 \,\}\, x := x-2; y := y+3 \,\{\, T \,\}}{\{\, INV \,\}\ \textbf{while}\ e\ \textbf{do}\ x := x-2; y := y+3\ \textbf{od}\, \{\, INV \wedge \neg e \,\}}\,(\text{wht}'') \qquad INV \wedge \neg e \Rightarrow G}{\{\, INV \,\}\ \textbf{while}\ e\ \textbf{do}\ x := x-2; y := y+3\ \textbf{od}\, \{\, G \,\}}\,(\text{lc})$$

$$\dfrac{\dfrac{F \Rightarrow I \quad \overset{(\text{as})}{\{\, I \,\}\, y := 0 \,\{\, INV \,\}}}{\{\, F \,\}\, y := 0 \,\{\, INV \,\}}\,(\text{lc}) \qquad \{\, INV \,\}\ \textbf{while}\ e\ \textbf{do}\ \ldots \textbf{od}\, \{\, G \,\}}{\{\, F \,\}\, y := 0; \textbf{while}\ e\ \textbf{do}\ x := x-2; y := y+3\ \textbf{od}\, \{\, G \,\}}\,(\text{sc})$$

Hoare Calculus

T_0: $Inv \wedge e \wedge t = t_0$ e: $x \neq 0$ H: $T[y/y+3]$

T: $Inv \wedge 0 \leq t < t_0$ t: x

$$
\dfrac{\dfrac{\dfrac{\{\,T_0\,\}\; x := x - 2\;\{\,H\,\} \qquad \dfrac{}{\{\,H\,\}\; y := y + 3\;\{\,T\,\}}\,\text{(as)}}{\{\,T_0\,\}\; x := x - 2;\, y := y + 3\;\{\,T\,\}}\,\text{(sc)}}{\{\,INV\,\}\;\textbf{while}\; e\;\textbf{do}\; x := x - 2;\, y := y + 3\;\textbf{od}\;\{\,INV \wedge \neg e\,\}}\,\text{(wht'')} \qquad INV \wedge \neg e \Rightarrow G}{\{\,INV\,\}\;\textbf{while}\; e\;\textbf{do}\; x := x - 2;\, y := y + 3\;\textbf{od}\;\{\,G\,\}}\,\text{(lc)}
$$

$$
\dfrac{\dfrac{F \Rightarrow I \qquad \dfrac{}{\{\,I\,\}\; y := 0\;\{\,INV\,\}}\,\text{(as)}}{\{\,F\,\}\; y := 0\;\{\,INV\,\}}\,\text{(lc)} \qquad \{\,INV\,\}\;\textbf{while}\; e\;\textbf{do}\;\ldots\textbf{od}\;\{\,G\,\}}{\{\,F\,\}\; y := 0;\,\textbf{while}\; e\;\textbf{do}\; x := x - 2;\, y := y + 3\;\textbf{od}\;\{\,G\,\}}\,\text{(sc)}
$$

Hoare Calculus

T_0: $Inv \wedge e \wedge t = t_0$ e: $x \neq 0$ H: $T[y/y+3]$

T: $Inv \wedge 0 \leq t < t_0$ t: x

$$
\dfrac{\dfrac{\dfrac{\dfrac{T_0 \Rightarrow J \quad \overset{\text{(as)}}{\{\, J \,\}\, x := x - 2 \,\{\, H \,\}}}{\{\, T_0 \,\}\, x := x - 2 \,\{\, H \,\}}\,\text{(lc)} \qquad \overset{\text{(as)}}{\{\, H \,\}\, y := y + 3 \,\{\, T \,\}}}{\{\, T_0 \,\}\, x := x - 2; y := y + 3 \,\{\, T \,\}}\,\text{(sc)}}{\{\, INV \,\}\, \textbf{while } e \textbf{ do } x := x - 2; y := y + 3 \textbf{ od} \,\{\, INV \wedge \neg e \,\}}\,\text{(wht'')} \qquad INV \wedge \neg e \Rightarrow G}{\{\, INV \,\}\, \textbf{while } e \textbf{ do } x := x - 2; y := y + 3 \textbf{ od} \,\{\, G \,\}}\,\text{(lc)}
$$

$$
\dfrac{\dfrac{F \Rightarrow I \quad \overset{\text{(as)}}{\{\, I \,\}\, y := 0 \,\{\, INV \,\}}}{\{\, F \,\}\, y := 0 \,\{\, INV \,\}}\,\text{(lc)} \qquad \{\, INV \,\}\, \textbf{while } e \textbf{ do } \ldots \textbf{od} \,\{\, G \,\}}{\{\, F \,\}\, y := 0; \textbf{while } e \textbf{ do } x := x - 2; y := y + 3 \textbf{ od} \,\{\, G \,\}}\,\text{(sc)}
$$

Hoare Calculus

T_0: $Inv \wedge e \wedge t = t_0$ e: $x \neq 0$ H: $T[y/y+3]$
T: $Inv \wedge 0 \leq t < t_0$ t: x

$$\dfrac{\dfrac{\dfrac{\dfrac{T_0 \Rightarrow J \quad \overset{(\text{as})}{\{\,J\,\}\; x := x-2\; \{\,H\,\}}}{\{\,T_0\,\}\; x := x-2\; \{\,H\,\}}\;(\text{lc}) \qquad \overset{(\text{as})}{\{\,H\,\}\; y := y+3\; \{\,T\,\}}}{\{\,T_0\,\}\; x := x-2;\, y := y+3\; \{\,T\,\}}\;(\text{sc})}{\{\,INV\,\}\; \textbf{while}\; e\; \textbf{do}\; x := x-2;\, y := y+3\; \textbf{od}\; \{\,INV \wedge \neg e\,\}}\;(\text{wht}'') \quad INV \wedge \neg e \Rightarrow G}{\{\,INV\,\}\; \textbf{while}\; e\; \textbf{do}\; x := x-2;\, y := y+3\; \textbf{od}\; \{\,G\,\}}\;(\text{lc})$$

$$\dfrac{\dfrac{F \Rightarrow I \quad \overset{(\text{as})}{\{\,I\,\}\; y := 0\; \{\,INV\,\}}}{\{\,F\,\}\; y := 0\; \{\,INV\,\}}\;(\text{lc}) \qquad \{\,INV\,\}\; \textbf{while}\; e\; \textbf{do}\; \ldots \textbf{od}\; \{\,G\,\}}{\{\,F\,\}\; y := 0;\, \textbf{while}\; e\; \textbf{do}\; x := x-2;\, y := y+3\; \textbf{od}\; \{\,G\,\}}\;(\text{sc})$$

I: $Inv[y/0]$ J: $H[x/x-2]$

Hoare Calculus cont

We have to prove three implications.

Implication (1):

$$F \Rightarrow Inv[y/0]$$

Hoare Calculus cont

We have to prove three implications.

Implication (1):

$$F \Rightarrow Inv[y/0]$$

$$(x = x_0 \land x \geq 0 \land \text{even}(x)) \Rightarrow (3x + 2 \cdot 0 = 3x_0 \land x \geq 0 \land \text{even}(x))$$

Hoare Calculus cont

We have to prove three implications.

Implication (1):

$$F \Rightarrow Inv[y/0]$$

$$(x = x_0 \wedge x \geq 0 \wedge \text{even}(x)) \Rightarrow (3x + 2 \cdot 0 = 3x_0 \wedge x \geq 0 \wedge \text{even}(x))$$

Hoare Calculus cont

We have to prove three implications.

Implication (1):

$$F \Rightarrow Inv[y/0]$$

$$(x = x_0 \land x \geq 0 \land \mathrm{even}(x)) \Rightarrow (3x + 2 \cdot 0 = 3x_0 \land x \geq 0 \land \mathrm{even}(x))$$

Implication (2):

$$Inv \land x \neq 0 \land t = t_0 \Rightarrow H[x/x-2]$$

Hoare Calculus cont

We have to prove three implications.

Implication (1):

$$F \Rightarrow Inv[y/0]$$

$$(x = x_0 \wedge x \geq 0 \wedge \text{even}(x)) \Rightarrow (3x + 2 \cdot 0 = 3x_0 \wedge x \geq 0 \wedge \text{even}(x))$$

Implication (2):

$$\begin{aligned}
&Inv \wedge x \neq 0 \wedge t = t_0 \Rightarrow H[x/x-2] \\
&Inv \wedge x \neq 0 \wedge x = t_0 \Rightarrow (3(x-2) + 2(y+3) = 3x_0 \wedge (x-2) \geq 0 \\
&\qquad\qquad\qquad\qquad\quad \wedge \text{even}(x-2) \wedge 0 \leq (x-2) < t_0)
\end{aligned}$$

Hoare Calculus cont

We have to prove three implications.

Implication (1):

$$F \Rightarrow Inv[y/0]$$

$$(x = x_0 \wedge x \geq 0 \wedge \text{even}(x)) \Rightarrow (3x + 2 \cdot 0 = 3x_0 \wedge x \geq 0 \wedge \text{even}(x))$$

Implication (2):

$$\begin{aligned}
&Inv \wedge x \neq 0 \wedge t = t_0 \Rightarrow H[x/x-2] \\
&Inv \wedge x \neq 0 \wedge x = t_0 \Rightarrow (3(x-2) + 2(y+3) = 3x_0 \wedge (x-2) \geq 0 \\
&\qquad\qquad\qquad\qquad\quad \wedge \text{even}(x-2) \wedge 0 \leq (x-2) < t_0) \\
&Inv \wedge x \neq 0 \Rightarrow (3x + 2y = 3x_0 \wedge \text{even}(x-2) \wedge 0 \leq (x-2) < x)
\end{aligned}$$

Hoare Calculus cont

We have to prove three implications.

Implication (1):

$$F \Rightarrow Inv[y/0]$$

$$(x = x_0 \wedge x \geq 0 \wedge \text{even}(x)) \Rightarrow (3x + 2 \cdot 0 = 3x_0 \wedge x \geq 0 \wedge \text{even}(x))$$

Implication (2):

$$\begin{aligned}
&Inv \wedge x \neq 0 \wedge t = t_0 \Rightarrow H[x/x-2] \\
&Inv \wedge x \neq 0 \wedge x = t_0 \Rightarrow (3(x-2) + 2(y+3) = 3x_0 \wedge (x-2) \geq 0 \\
&\qquad\qquad\qquad\qquad\qquad \wedge \text{even}(x-2) \wedge 0 \leq (x-2) < t_0) \\
&Inv \wedge x \neq 0 \Rightarrow (3x + 2y = 3x_0 \wedge \text{even}(x-2) \wedge 0 \leq (x-2) < x) \\
&(3x + 2y = 3x_0 \wedge x \geq 0 \wedge \text{even}(x)) \wedge x \neq 0 \Rightarrow (3x + 2y = 3x_0 \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \wedge \text{even}(x-2) \wedge 0 \leq (x-2) < x)
\end{aligned}$$

Hoare Calculus cont

We have to prove three implications.

Implication (1):

$$F \Rightarrow Inv[y/0]$$
$$(x = x_0 \land x \geq 0 \land \text{even}(x)) \Rightarrow (3x + 2 \cdot 0 = 3x_0 \land x \geq 0 \land \text{even}(x))$$

Implication (2):

$$
\begin{aligned}
& Inv \land x \neq 0 \land t = t_0 \Rightarrow H[x/x-2] \\
& Inv \land x \neq 0 \land x = t_0 \Rightarrow (3(x-2) + 2(y+3) = 3x_0 \land (x-2) \geq 0 \\
& \qquad\qquad\qquad\qquad\qquad \land \text{even}(x-2) \land 0 \leq (x-2) < t_0) \\
& Inv \land x \neq 0 \Rightarrow (3x + 2y = 3x_0 \land \text{even}(x-2) \land 0 \leq (x-2) < x) \\
& (3x + 2y = 3x_0 \land x \geq 0 \land \text{even}(x)) \land x \neq 0 \Rightarrow (3x + 2y = 3x_0 \\
& \qquad\qquad\qquad\qquad\qquad\qquad \land \text{even}(x-2) \land 0 \leq (x-2) < x)
\end{aligned}
$$

Hoare Calculus cont

We have to prove three implications.

Implication (1):

$$F \Rightarrow Inv[y/0]$$

$$(x = x_0 \wedge x \geq 0 \wedge \text{even}(x)) \Rightarrow (3x + 2 \cdot 0 = 3x_0 \wedge x \geq 0 \wedge \text{even}(x))$$

Implication (2):

$$\begin{aligned}
&Inv \wedge x \neq 0 \wedge t = t_0 \Rightarrow H[x/x-2] \\
&Inv \wedge x \neq 0 \wedge x = t_0 \Rightarrow (3(x-2) + 2(y+3) = 3x_0 \wedge (x-2) \geq 0 \\
&\qquad\qquad\qquad\qquad\qquad \wedge \text{even}(x-2) \wedge 0 \leq (x-2) < t_0) \\
&Inv \wedge x \neq 0 \Rightarrow (3x + 2y = 3x_0 \wedge \text{even}(x-2) \wedge 0 \leq (x-2) < x) \\
&(3x + 2y = 3x_0 \wedge x \geq 0 \wedge \text{even}(x)) \wedge x \neq 0 \Rightarrow (3x + 2y = 3x_0 \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \wedge \text{even}(x-2) \wedge 0 \leq (x-2) < x)
\end{aligned}$$

Implication (3):

$$Inv \wedge \neg e \Rightarrow G$$

Hoare Calculus cont

We have to prove three implications.

Implication (1):

$$F \Rightarrow Inv[y/0]$$

$$(x = x_0 \land x \geq 0 \land \text{even}(x)) \Rightarrow (3x + 2 \cdot 0 = 3x_0 \land x \geq 0 \land \text{even}(x))$$

Implication (2):

$$Inv \land x \neq 0 \land t = t_0 \Rightarrow H[x/x-2]$$

$$Inv \land x \neq 0 \land x = t_0 \Rightarrow (3(x-2) + 2(y+3) = 3x_0 \land (x-2) \geq 0$$

$$\land \text{even}(x-2) \land 0 \leq (x-2) < t_0)$$

$$Inv \land x \neq 0 \Rightarrow (3x + 2y = 3x_0 \land \text{even}(x-2) \land 0 \leq (x-2) < x)$$

$$(3x + 2y = 3x_0 \land x \geq 0 \land \text{even}(x)) \land x \neq 0 \Rightarrow (3x + 2y = 3x_0$$

$$\land \text{even}(x-2) \land 0 \leq (x-2) < x)$$

Implication (3):

$$Inv \land \neg e \Rightarrow G$$

$$(3x + 2y = 3x_0 \land x \geq 0 \land \text{even}(x) \land x = 0) \Rightarrow 2y = 3x_0$$

Annotation Calculus

$\{\, 1\colon x = x_0 \wedge x \geq 0 \wedge \mathrm{even}(x) \,\}$

$y := 0;$

while $x \neq 0$ **do**

$\quad x := x - 2;$

$\quad y := y + 3$

od

$\{\, 2\colon 2y = 3x_0 \,\}$

Annotation Calculus

$\{\, 1\colon x = x_0 \wedge x \geq 0 \wedge \mathrm{even}(x) \,\}$

$y := 0;$
$\{\, 3\colon \mathit{Inv} \equiv 3x + 2y = 3x_0 \wedge x \geq 0 \wedge \mathrm{even}(x) \,\}$ (wht$''$)
while $x \neq 0$ **do**
$\{\, 4\colon \mathit{Inv} \wedge x \neq 0 \wedge t = t_0 \,\}$ (wht$''$)

$x := x - 2;$

$y := y + 3$
$\{\, 5\colon \mathit{Inv} \wedge 0 \leq t < t_0 \,\}$ (wht$''$)
od
$\{\, 6\colon \mathit{Inv} \wedge x = 0 \,\}$ (wht$''$)
$\{\, 2\colon 2y = 3x_0 \,\}$

Annotation Calculus

$\{\, 1\colon x = x_0 \wedge x \geq 0 \wedge \text{even}(x) \,\}$

$y := 0;$

$\{\, 3\colon \mathit{Inv} \equiv 3x + 2y = 3x_0 \wedge x \geq 0 \wedge \text{even}(x) \,\}$ (wht$''$)

while $x \neq 0$ **do**

$\{\, 4\colon \mathit{Inv} \wedge x \neq 0 \wedge t = t_0 \,\}$ (wht$''$)

$x := x - 2;$

$\{\, 7\colon (\mathit{Inv} \wedge 0 \leq t < t_0)[y/y+3] \,\}$ (as$\uparrow$)

$y := y + 3$

$\{\, 5\colon \mathit{Inv} \wedge 0 \leq t < t_0 \,\}$ (wht$''$)

od

$\{\, 6\colon \mathit{Inv} \wedge x = 0 \,\}$ (wht$''$)

$\{\, 2\colon 2y = 3x_0 \,\}$

Annotation Calculus

$\{\,1\colon x = x_0 \wedge x \geq 0 \wedge \mathrm{even}(x)\,\}$

$y := 0;$

$\{\,3\colon \mathit{Inv} \equiv 3x + 2y = 3x_0 \wedge x \geq 0 \wedge \mathrm{even}(x)\,\}$ (wht″)

while $x \neq 0$ **do**

$\{\,4\colon \mathit{Inv} \wedge x \neq 0 \wedge t = t_0\,\}$ (wht″)

$\{\,8\colon (\mathit{Inv} \wedge 0 \leq t < t_0)[y/y+3][x/x-2]\,\}$ (as↑)

$x := x - 2;$

$\{\,7\colon (\mathit{Inv} \wedge 0 \leq t < t_0)[y/y+3]\,\}$ (as↑)

$y := y + 3$

$\{\,5\colon \mathit{Inv} \wedge 0 \leq t < t_0\,\}$ (wht″)

od

$\{\,6\colon \mathit{Inv} \wedge x = 0\,\}$ (wht″)

$\{\,2\colon 2y = 3x_0\,\}$

Annotation Calculus

$$
\begin{array}{ll}
\{\, 1\colon x = x_0 \land x \geq 0 \land \text{even}(x) \,\} & \\
\quad \{\, 9\colon \mathit{Inv}[y/0] \,\} & (\text{as}\uparrow) \\
y := 0; & \\
\quad \{\, 3\colon \mathit{Inv} \equiv 3x + 2y = 3x_0 \land x \geq 0 \land \text{even}(x) \,\} & (\text{wht}'') \\
\textbf{while } x \neq 0 \textbf{ do} & \\
\qquad \{\, 4\colon \mathit{Inv} \land x \neq 0 \land t = t_0 \,\} & (\text{wht}'') \\
\quad \{\, 8\colon (\mathit{Inv} \land 0 \leq t < t_0)[y/y+3][x/x-2] \,\} & (\text{as}\uparrow) \\
\qquad x := x - 2; & \\
\quad \{\, 7\colon (\mathit{Inv} \land 0 \leq t < t_0)[y/y+3] \,\} & (\text{as}\uparrow) \\
\qquad y := y + 3 & \\
\qquad \{\, 5\colon \mathit{Inv} \land 0 \leq t < t_0 \,\} & (\text{wht}'') \\
\textbf{od} & \\
\quad \{\, 6\colon \mathit{Inv} \land x = 0 \,\} & (\text{wht}'') \\
\{\, 2\colon 2y = 3x_0 \,\} &
\end{array}
$$

Annotation Calculus

$$
\begin{array}{ll}
\{\,1\colon x = x_0 \wedge x \geq 0 \wedge \mathrm{even}(x)\,\} & \\
\;\{\,9\colon \mathit{Inv}[y/0]\,\} & (\mathrm{as}\uparrow) \\
y := 0; & \\
\;\{\,3\colon \mathit{Inv} \equiv 3x + 2y = 3x_0 \wedge x \geq 0 \wedge \mathrm{even}(x)\,\} & (\mathrm{wht}'') \\
\mathbf{while}\ x \neq 0\ \mathbf{do} & \\
\quad\{\,4\colon \mathit{Inv} \wedge x \neq 0 \wedge t = t_0\,\} & (\mathrm{wht}'') \\
\;\{\,8\colon (\mathit{Inv} \wedge 0 \leq t < t_0)[y/y+3][x/x-2]\,\} & (\mathrm{as}\uparrow) \\
\quad x := x - 2; & \\
\;\{\,7\colon (\mathit{Inv} \wedge 0 \leq t < t_0)[y/y+3]\,\} & (\mathrm{as}\uparrow) \\
\quad y := y + 3 & \\
\quad\{\,5\colon \mathit{Inv} \wedge 0 \leq t < t_0\,\} & (\mathrm{wht}'') \\
\mathbf{od} & \\
\;\{\,6\colon \mathit{Inv} \wedge x = 0\,\} & (\mathrm{wht}'') \\
\{\,2\colon 2y = 3x_0\,\} &
\end{array}
$$

It remains to prove the implications

$$1 \Rightarrow 9 \qquad\qquad 4 \Rightarrow 8 \qquad\qquad 6 \Rightarrow 2$$

Proving Total Correctness with WP

$\{ F \}\, p\, \{ G \}$ totally correct $\iff F \quad \Rightarrow \mathrm{wp}(p, \quad G \quad)$

Proving Total Correctness with WP

$\{ F \} \, p \, \{ G \}$ totally correct $\iff F \quad \Rightarrow \mathrm{wp}(p, \quad G \quad)$

WP of Sequential Composition

$\mathrm{wp}(p; q, G) = \mathrm{wp}(p, \mathrm{wp}(q, G))$

Proving Total Correctness with WP

$\{ F \}\, p\, \{ G \}$ totally correct $\iff F \;\; \Rightarrow \mathrm{wp}(p, \;\; G \;\;)$

WP of Sequential Composition

$\mathrm{wp}(p; q, G) = \mathrm{wp}(p, \mathrm{wp}(q, G))$

WP of While

0 iterations: $F_0 = \neg e \wedge G$

Proving Total Correctness with WP

$\{ F \}\, p\, \{ G \}$ totally correct $\iff F \;\; \Rightarrow \mathrm{wp}(p, \;\; G \;\;)$

WP of Sequential Composition

$\mathrm{wp}(p; q, G) = \mathrm{wp}(p, \mathrm{wp}(q, G))$

WP of While

0 iterations: $F_0 = \neg e \wedge G$

1 iteration: $F_1 = e \wedge \mathrm{wp}(p, F_0)$

Proving Total Correctness with WP

$\{ F \} \, p \, \{ G \}$ totally correct $\iff F \quad \Rightarrow \mathrm{wp}(p, \quad G \quad)$

WP of Sequential Composition

$\mathrm{wp}(p; q, G) = \mathrm{wp}(p, \mathrm{wp}(q, G))$

WP of While

0 iterations: $F_0 = \neg e \land G$

1 iteration: $F_1 = e \land \mathrm{wp}(p, F_0)$

2 iterations: $F_2 = e \land \mathrm{wp}(p, F_1)$

Proving Total Correctness with WP

$\{ F \} \, p \, \{ G \}$ totally correct $\iff F \quad \Rightarrow \text{wp}(p, \quad G \quad)$

WP of Sequential Composition

$\text{wp}(p; q, G) = \text{wp}(p, \text{wp}(q, G))$

WP of While

0 iterations: $F_0 = \neg e \wedge G$

1 iteration: $F_1 = e \wedge \text{wp}(p, F_0)$

2 iterations: $F_2 = e \wedge \text{wp}(p, F_1)$

$\vdots \qquad \vdots$

i iterations: $F_i = e \wedge \text{wp}(p, F_{i-1}) \quad (\text{for } i > 0)$

Weakest Precondition

$\mathrm{wp}(y := 0; \textbf{while} \ \cdots, 2y = 3x_0)$

$= \mathrm{wp}(y := 0, \mathrm{wp}(\textbf{while} \ \cdots, 2y = 3x_0))$

Weakest Precondition

$\mathrm{wp}(y := 0; \textbf{while } \cdots, 2y = 3x_0)$

$= \mathrm{wp}(y := 0, \mathrm{wp}(\textbf{while } \cdots, 2y = 3x_0))$

$\mathrm{wp}(\textbf{while } x \neq 0 \textbf{ do } x := x - 2; y := y + 3 \textbf{ do}, 2y = 3x_0) = \exists i \geq 0\ F_i$

Weakest Precondition

$\mathrm{wp}(y := 0; \textbf{while } \cdots, 2y = 3x_0)$

$= \mathrm{wp}(y := 0, \mathrm{wp}(\textbf{while } \cdots, 2y = 3x_0))$

$\mathrm{wp}(\textbf{while } x \neq 0 \textbf{ do } x := x - 2; y := y + 3 \textbf{ do}, 2y = 3x_0) = \exists i \geq 0\ F_i$

$F_0 : x = 0 \wedge 2y = 3x_0$

Weakest Precondition

$\text{wp}(y := 0; \textbf{while } \cdots, 2y = 3x_0)$

$= \text{wp}(y := 0, \text{wp}(\textbf{while } \cdots, 2y = 3x_0))$

$\text{wp}(\textbf{while } x \neq 0 \textbf{ do } x := x - 2; y := y + 3 \textbf{ do}, 2y = 3x_0) = \exists i \geq 0\ F_i$

$F_0 : x = 0 \land 2y = 3x_0$

$F_1 : x \neq 0 \land \text{wp}(x := x - 2; y := y + 3, x = 0 \land 2y = 3x_0)$

Weakest Precondition

$\text{wp}(y := 0; \textbf{while } \cdots, 2y = 3x_0)$

$= \text{wp}(y := 0, \text{wp}(\textbf{while } \cdots, 2y = 3x_0))$

$\text{wp}(\textbf{while } x \neq 0 \textbf{ do } x := x - 2; y := y + 3 \textbf{ do}, 2y = 3x_0) = \exists i \geq 0\ F_i$

$$F_0 : x = 0 \land 2y = 3x_0$$

$$F_1 : x \neq 0 \land \text{wp}(x := x - 2; y := y + 3, x = 0 \land 2y = 3x_0)$$

$$= x \neq 0 \land x - 2 = 0 \land 2(y + 3) = 3x_0$$

Weakest Precondition

wp($y := 0;$ **while** $\cdots$, $2y = 3x_0$)

$= \text{wp}(y := 0, \text{wp}(\textbf{while } \cdots , 2y = 3x_0))$

wp(**while** $x \neq 0$ **do** $x := x - 2; y := y + 3$ **do**, $2y = 3x_0) = \exists i \geq 0\, F_i$

$$\begin{aligned}
F_0 :& x = 0 \wedge 2y = 3x_0 \\
F_1 :& x \neq 0 \wedge \text{wp}(x := x - 2; y := y + 3,\ x = 0 \wedge 2y = 3x_0) \\
&= x \neq 0 \wedge x - 2 = 0 \wedge 2(y + 3) = 3x_0 \\
&= (x = 2 \wedge 2y + 6 = 3x_0)
\end{aligned}$$

Weakest Precondition

$\text{wp}(y := 0; \textbf{while} \ \cdots, 2y = 3x_0)$

$= \text{wp}(y := 0, \text{wp}(\textbf{while} \ \cdots, 2y = 3x_0))$

$\text{wp}(\textbf{while}\ x \neq 0\ \textbf{do}\ x := x - 2; y := y + 3\ \textbf{do}, 2y = 3x_0) = \exists i \geq 0\ F_i$

$$F_0 : x = 0 \land 2y = 3x_0$$
$$F_1 : x \neq 0 \land \text{wp}(x := x - 2; y := y + 3, x = 0 \land 2y = 3x_0)$$
$$= x \neq 0 \land x - 2 = 0 \land 2(y + 3) = 3x_0$$
$$= (x = 2 \land 2y + 6 = 3x_0)$$
$$F_i : x = 2i \land 2y + 6i = 3x_0$$

Weakest Precondition

$\mathrm{wp}(y := 0; \textbf{while } \cdots, 2y = 3x_0)$

$= \mathrm{wp}(y := 0, \mathrm{wp}(\textbf{while } \cdots, 2y = 3x_0))$

$\mathrm{wp}(\textbf{while } x \neq 0 \textbf{ do } x := x - 2; y := y + 3 \textbf{ do}, 2y = 3x_0) = \exists i \geq 0\ F_i$

$$
\begin{aligned}
F_0 :& x = 0 \wedge 2y = 3x_0 \\
F_1 :& x \neq 0 \wedge \mathrm{wp}(x := x - 2; y := y + 3, x = 0 \wedge 2y = 3x_0) \\
&= x \neq 0 \wedge x - 2 = 0 \wedge 2(y + 3) = 3x_0 \\
&= (x = 2 \wedge 2y + 6 = 3x_0) \\
F_i :& x = 2i \wedge 2y + 6i = 3x_0 \\
&= (x = 2i \wedge 2y + 3x = 3x_0) \quad \text{(guess)}
\end{aligned}
$$

Weakest Precondition

$\mathrm{wp}(y := 0; \textbf{while } \cdots, 2y = 3x_0)$

$= \mathrm{wp}(y := 0, \mathrm{wp}(\textbf{while } \cdots, 2y = 3x_0))$

$\mathrm{wp}(\textbf{while } x \neq 0 \textbf{ do } x := x - 2; y := y + 3 \textbf{ do}, 2y = 3x_0) = \exists i \geq 0\ F_i$

$$
\begin{aligned}
F_0 :& x = 0 \wedge 2y = 3x_0 \\
F_1 :& x \neq 0 \wedge \mathrm{wp}(x := x - 2; y := y + 3, x = 0 \wedge 2y = 3x_0) \\
& = x \neq 0 \wedge x - 2 = 0 \wedge 2(y + 3) = 3x_0 \\
& = (x = 2 \wedge 2y + 6 = 3x_0) \\
F_i :& x = 2i \wedge 2y + 6i = 3x_0 \\
& = (x = 2i \wedge 2y + 3x = 3x_0) \quad \text{(guess)} \\
F_{i+1} :& x \neq 0 \wedge \mathrm{wp}(x := x - 2; y := y + 3, x = 2i \wedge 2y + 3x = 3x_0)
\end{aligned}
$$

Weakest Precondition

$\mathrm{wp}(y := 0; \textbf{while } \cdots, 2y = 3x_0)$

$= \mathrm{wp}(y := 0, \mathrm{wp}(\textbf{while } \cdots, 2y = 3x_0))$

$\mathrm{wp}(\textbf{while } x \neq 0 \textbf{ do } x := x - 2; y := y + 3 \textbf{ do}, 2y = 3x_0) = \exists i \geq 0\, F_i$

$$
\begin{aligned}
F_0 :& x = 0 \wedge 2y = 3x_0 \\
F_1 :& x \neq 0 \wedge \mathrm{wp}(x := x - 2; y := y + 3, x = 0 \wedge 2y = 3x_0) \\
&= x \neq 0 \wedge x - 2 = 0 \wedge 2(y + 3) = 3x_0 \\
&= (x = 2 \wedge 2y + 6 = 3x_0) \\
F_i :& x = 2i \wedge 2y + 6i = 3x_0 \\
&= (x = 2i \wedge 2y + 3x = 3x_0) \quad \text{(guess)} \\
F_{i+1} :& x \neq 0 \wedge \mathrm{wp}(x := x - 2; y := y + 3, x = 2i \wedge 2y + 3x = 3x_0) \\
&= (x = 2(i + 1) \wedge 2(y + 3) + 3(x - 2) = 3x_0)
\end{aligned}
$$

Weakest Precondition

wp($y := 0;$ **while** $\cdots$, $2y = 3x_0$)

$= \text{wp}(y := 0, \text{wp}(\textbf{while } \cdots, 2y = 3x_0))$

wp(**while** $x \neq 0$ **do** $x := x - 2; y := y + 3$ **do**, $2y = 3x_0$) $= \exists i \geq 0\ F_i$

$$
\begin{aligned}
F_0 :& x = 0 \land 2y = 3x_0 \\
F_1 :& x \neq 0 \land \text{wp}(x := x - 2; y := y + 3,\ x = 0 \land 2y = 3x_0) \\
&= x \neq 0 \land x - 2 = 0 \land 2(y + 3) = 3x_0 \\
&= (x = 2 \land 2y + 6 = 3x_0) \\
F_i :& x = 2i \land 2y + 6i = 3x_0 \\
&= (x = 2i \land 2y + 3x = 3x_0) \quad \text{(guess)} \\
F_{i+1} :& x \neq 0 \land \text{wp}(x := x - 2; y := y + 3,\ x = 2i \land 2y + 3x = 3x_0) \\
&= (x = 2(i + 1) \land 2(y + 3) + 3(x - 2) = 3x_0) \\
&= (x = 2(i + 1) \land 2y + 3x = 3x_0) \quad \text{(proof)}
\end{aligned}
$$

Weakest Precondition cont.

$\text{wp}(\textbf{while } x \neq 0 \textbf{ do } x := x - 2; y := y + 3 \textbf{ do}, 2y = 3x_0)$

$= \exists i \geq 0\, x = 2i \wedge 2y + 3x = 3x_0$

Weakest Precondition cont.

$\text{wp}(\textbf{while } x \neq 0 \textbf{ do } x := x - 2; y := y + 3 \textbf{ do}, 2y = 3x_0)$

$= \exists i \geq 0\, x = 2i \wedge 2y + 3x = 3x_0$

$= x \geq 0 \wedge \text{even}(x) \wedge 2y + 3x = 3x_0$

Weakest Precondition cont.

wp(**while** $x \neq 0$ **do** $x := x - 2; y := y + 3$ **do**, $2y = 3x_0$)

$= \exists i \geq 0\, x = 2i \wedge 2y + 3x = 3x_0$
$= x \geq 0 \wedge \text{even}(x) \wedge 2y + 3x = 3x_0$

wp($y := 0$, $x \geq 0 \wedge \text{even}(x) \wedge 2y + 3x = 3x_0$)

$= x \geq 0 \wedge \text{even}(x) \wedge 3x = 3x_0$

Weakest Precondition cont.

$\mathrm{wp}(\textbf{while } x \neq 0 \textbf{ do } x := x - 2; y := y + 3 \textbf{ do}, 2y = 3x_0)$

$= \exists i \geq 0\, x = 2i \wedge 2y + 3x = 3x_0$

$= x \geq 0 \wedge \mathrm{even}(x) \wedge 2y + 3x = 3x_0$

$\mathrm{wp}(y := 0, x \geq 0 \wedge \mathrm{even}(x) \wedge 2y + 3x = 3x_0)$

$= x \geq 0 \wedge \mathrm{even}(x) \wedge 3x = 3x_0$

$= x \geq 0 \wedge \mathrm{even}(x) \wedge x = x_0$

Weakest Precondition cont.

$\text{wp}(\textbf{while } x \neq 0 \textbf{ do } x := x - 2; y := y + 3 \textbf{ do}, 2y = 3x_0)$

$= \exists i \geq 0\, x = 2i \wedge 2y + 3x = 3x_0$
$= x \geq 0 \wedge \text{even}(x) \wedge 2y + 3x = 3x_0$

$\text{wp}(y := 0, x \geq 0 \wedge \text{even}(x) \wedge 2y + 3x = 3x_0)$

$= x \geq 0 \wedge \text{even}(x) \wedge 3x = 3x_0$
$= x \geq 0 \wedge \text{even}(x) \wedge x = x_0$

$F \Rightarrow \text{wp}(\textbf{while } x \neq 0 \textbf{ do } x := x - 2; y := y + 3 \textbf{ do}, 2y = 3x_0)$

$x \geq 0 \wedge \text{even}(x) \wedge x = x_0 \Rightarrow x \geq 0 \wedge \text{even}(x) \wedge x = x_0$ (Tautology)

Weakest Precondition cont.

$\text{wp}(\textbf{while } x \neq 0 \textbf{ do } x := x - 2; y := y + 3 \textbf{ do}, 2y = 3x_0)$

$= \exists i \geq 0\, x = 2i \wedge 2y + 3x = 3x_0$

$= x \geq 0 \wedge \text{even}(x) \wedge 2y + 3x = 3x_0$

$\text{wp}(y := 0, x \geq 0 \wedge \text{even}(x) \wedge 2y + 3x = 3x_0)$

$= x \geq 0 \wedge \text{even}(x) \wedge 3x = 3x_0$

$= x \geq 0 \wedge \text{even}(x) \wedge x = x_0$

$F \Rightarrow \text{wp}(\textbf{while } x \neq 0 \textbf{ do } x := x - 2; y := y + 3 \textbf{ do}, 2y = 3x_0)$

$x \geq 0 \wedge \text{even}(x) \wedge x = x_0 \Rightarrow x \geq 0 \wedge \text{even}(x) \wedge x = x_0$ (Tautology)

{F}p{G} totally correct