VU Programm- und Systemverifikation
Solution: Hoare Logic

June 5, 2017

Task 1: The domain of all variables in the program are the natural numbers including 0. The required invariant is $a \geq b$.

$\{\texttt{true}\}$
$\{\texttt{true}\}$ ⑧
`if (x > y) {`
  $\{x \geq y\}$ ⑦
  `a = x;`
  $\{a \geq y\}$ ⑥
  `b = y;`
  $\{a \geq b\}$
`} else {`
  $\{y \geq x\}$ ⑤
  `a = y;`
  $\{a \geq x\}$ ④
  `b = x;`
  $\{a \geq b\}$
`}`
$\{a \geq b\}$
`while ((a-b)>0) {`
  $\{a > b\}$ ②
  `a = a-1;`
  $\{a \geq b\}$ ①
`}`
$\{\neg(a > b) \wedge (a \geq b)\}$ ③
$\{a = b\}$ ⑨

① loop invariant $a \geq b$

② assignment: $\dfrac{}{\{a-1 \geq b\}\ \texttt{a=a-1}\ \{a \geq b\}}$

consequence: $\dfrac{(a-1 \geq b) \Rightarrow (a > b) \quad \{a-1 \geq b\}\ \texttt{a=a-1}\ \{a \geq b\}}{\{a > b\}\ \texttt{a=a-1}\ \{a \geq b\}}$

③ loop: $\dfrac{\{(a > b) \wedge (a \geq b)\}\ \texttt{a=a-1}\ \{a \geq b\}}{\{a \geq b\}\ \texttt{while (a>b) \{ a=a-1 \}}\ \{a \geq b\}}$

④ assignment: $\dfrac{}{\{a \geq x\}\ \texttt{b=x}\ \{a \geq b\}}$

⑤ assignment: $\dfrac{}{\{y \geq x\}\ \texttt{a=y}\ \{a \geq x\}}$

⑥ assignment: $\dfrac{}{\{a \geq y\}\ \texttt{b=y}\ \{a \geq b\}}$

⑦ assignment: $\dfrac{}{\{x \geq y\}\ \texttt{a=x}\ \{a \geq x\}}$

⑧ apply composition to branches

consequence: $\dfrac{(x > y) \Rightarrow (x \geq y) \quad \{x \geq y\}\ \texttt{a=x}\ \{a \geq y\}}{\{x > y\}\ \texttt{a=x}\ \{a \geq y\}}$

then conditional:
$\dfrac{\{(x > y)\}\ \texttt{a=x; b=y;}\ \{a \geq b\} \qquad \{(y \geq x)\}\ \texttt{a=y; b=x;}\ \{a \geq b\}}{\{\texttt{true}\}\ \texttt{if (x>y) \{a=x; b=y;\} else \{a=y; b=x;\}...}\ \{a \geq b\}}$

⑨ Finally, $(a \leq b) \wedge (a \geq b) \Rightarrow (a = b)$

Task 2: The domain of all variables in the program are the integers, and `N` is a positive constant. The required invariant is $(x + y = N) \wedge (x \geq 0)$.

$\{\mathsf{true}\}$
$\{(N = N) \wedge (N \geq 0)\}$ ⑥
`x := N;`
$\{(x = N) \wedge (x \geq 0)\}$ ⑤
`y := 0;`
$\{(x + y = N) \wedge (x \geq 0)\}$ ④
`while (x > 0) {`
  $\{(x + y = N) \wedge (x > 0)\}$ ③
  `x = x - 1;`
  $\{(x + y + 1 = N) \wedge (x \geq 0)\}$ ②
  `y = y + 1;`
  $\{(x + y = N) \wedge (x \geq 0)\}$ ①
`}`
$\{\neg(x > 0) \wedge (x + y = N) \wedge (x \geq 0)\}$ ④
$\{\mathtt{y} = \mathtt{N}\}$ ⑦

① loop invariant $(x + y = N) \wedge (x \geq 0)$

② assignment: $\dfrac{}{\{(x+y+1=N)\wedge(x\geq 0)\}\ \mathtt{y=y+1}\ \{(x+y=N)\wedge(x\geq 0)\}}$

③ assignment: $\dfrac{}{\{(x+y=N)\wedge(x-1\geq 0)\}\ \mathtt{x=x-1}\ \{(x+y+1=N)\wedge(x\geq 0)\}}$

apply composition, then

consequence: $\dfrac{(x-1\geq 0)\Rightarrow(x>0) \quad \{(x+y=N)\wedge(x-1\geq 0\}\ \mathtt{x=x-1;\ y=y+1}\ \{(x+y=N)\wedge(x\geq 0)\}}{\{(x+y=N)\wedge(x\geq 0)\}\ \mathtt{x=x-1;\ y=y-1}\ \{(x+y=N)\wedge(x\geq 0)\}}$

④ loop: $\dfrac{\{(x>0)\wedge(x+y=N)\wedge(x\geq 0)\}\ \mathtt{x=x-1;\ y=y+1}\ \{(x+y=N)\wedge(x\geq 0)\}}{\{(x+y=N)\wedge(x\geq 0)\}\ \mathtt{while\ (x>0)\ \{\ x=x-1;\ y=y+1;\ \}}\ \{\neg(x>0)\wedge(x+y=N)\wedge(x\geq 0)\}}$

⑤ assignment: $\dfrac{}{\{(x=N)\wedge(x\geq 0)\}\ \mathtt{y=0}\ \{(x+y=N)\wedge(x\geq 0)\}}$

⑥ assignment: $\dfrac{}{\{(N=N)\wedge(N\geq 0)\}\ \mathtt{x=N}\ \{(x=N)\wedge(x\geq 0)\}}$

The precondition is true since we assumed that $N \geq 0$.

⑦ Finally, $(x \leq 0) \wedge (x \geq 0) \wedge (x + y = N) \Rightarrow (y = N)$ (consequence)

Upload a pdf file with your solutions to TUWEL by June 8, 2014.