Danny MILOSAVLJEVIC, Mat. 0826039

assignment: $\frac{}{\{Q[E/x]\}\ x := E\ \{Q\}}$

composition: $\frac{\{P\}\ C_1\ \{R\} \quad \{R\}\ C_2\ \{Q\}}{\{P\}\ C_1; C_2\ \{Q\}}$

conditional: $\frac{\{B \wedge P\}\ C_1\ \{Q\} \quad \{\neg B \wedge P\}\ C_2\ \{Q\}}{\{P\}\ \text{if } B \text{ then } C_1 \text{ else } C_2\ \{Q\}}$

while loop: $\frac{\{P \wedge B\}\ C\ \{P\}}{\{P\}\ \text{while } B \text{ do } C\ \{\neg B \wedge P\}}$

VU Programm- und Systemverifikation

Homework: Hoare Logic

OK to: strengthen pre-conditions, weaken post-conditions

May 27, 2015

Task 1 (8 points): Prove the Hoare Triple below (assume that the domain of all variables in the program are the natural numbers including 0). You need to find a sufficiently strong loop invariant. Annotate the following code directly with the required assertions. Justify each assertion by stating which Hoare rule you used to derive it.

$a \geq b$?

{true}

```
if (x > y) {
```
$\{x > y\}$ c

```
  a = x;
```
$\{x > y \wedge a > y\}$ a

```
  b = y;
```
$\{x > y \wedge a > y \wedge a > b\}$ a

$\{a \geq b\}$ weakened postcondition

```
} else {
```
$\{x \leq y\}$ c

```
  a = y;
```
$\{x \leq y \wedge x \leq a\}$ a

```
  b = x;
```
$\{x \leq y \wedge x \leq a \wedge \underbrace{b \leq a}_{a \geq b}\}$ a

```
}
```
$\{a \geq b\}$

```
while ((a-b)>0) {
```
$(\{a-1 \geq b\} = \{a > b\}) \wedge \{a \geq b\}$ w

```
  a = a-1;
```
$\{a \geq b\}$

```
}
```
$\{a \leq b \wedge a \geq b\} = \{a = b\}$ w

$\{a = b\}$

Danny MILOŠAVLJEVIĆ, Mat. 0826039

Task 2 (7 points): Prove the Hoare Triple below (assume that the domain of all variables in the program are the integers, and that N is a positive constant). You need to find a sufficiently strong loop invariant. Annotate the following code directly with the required assertions. Justify each assertion by stating which Hoare rule you used to derive it.

{true}
$\{N=N\}$
`x := N;`
$\{x+0=N\}$
`y := 0;`
$\{x+y=N\}$
`while (x > 0) {`
$\{x>0,\ x+y=N\}$ W a
`x = x - 1;`
$\{x+1>0,\ x+1+y=N\}$ a
`y = y + 1;`
$\{x+1>0,\ x+y=N\}$ a
$x \geq 0$
`}`
$\{(x \geq 0) \wedge x+y=N \wedge x \geq 0\}$ W d.h. $x=0 \wedge x+y=N$
$\{y = N\}$

$+$ | $x_n = N-n$, $y_n = n$

$(x_n + y_n = N) = P$

Upload a pdf file with your solutions to TUWEL by June 10, 2015.