CSE526: Principles of Programming Languages
Scott Stoller
hw3: Hoare logic
version: 5pm,1feb2004
due: 26 feb 2004
Answer

Yiping Han

1st March 2004

1 Problem

1. Prove correctness of the following program for computing integer square roots in linear time. Specifically, prove

$$\{x >= 0\} r := 0;\ \text{while } x >= (r+1)^2 \text{ do } r := r+1 \{r^2 <= x < (r+1)^2\}$$

As indicated on [Reynolds, page 57], you do not need to prove predicate-logic assertions (such as $x < x+1$) that occur in the proof, but the assertions should be valid.

You may structure your proof in the linear format described in [Reynolds, chapter 3] or as a proof tree (if you are comfortable with that concept).

2 Proof 1:

1. $\{x \geq 0\} r := 0 \{x \geq r^2\}$ (AS)

2. $\{x \geq (r+1)^2\} r := r+1 \{x \geq r^2\}$ (AS)
3. $x \geq r^2 \wedge x \geq (r+1)^2 \iff x \geq (r+1)^2$
4. $\{x \geq r^2 \wedge x \geq (r+1)^2\} r := r+1 \{x \geq r^2\}$ (SP,2,3)
5. $\{x \geq r^2\}$
   while $x >= (r+1)^2$ do $r := r+1$
   $\{x \geq r^2 \wedge x < (r+1)^2\}$ (WHP,4)

6. $\{x \geq 0\}$
   $r := 0;$ while $x >= (r+1)^2$ do $r := r+1$
   $\{x \geq r^2 \wedge x < (r+1)^2\}$ (SQ,1,5)

END OF PROOF

3 Proof 2:

1. $\{x \geq 0\} r := 0 \{x \geq r^2\}$ (AS)
2. $\{x \geq r^2\} \iff \{(x \geq r^2 \wedge x < (r+1)^2) \vee (x \geq r^2 \wedge x \geq (r+1)^2)\}$

3. $\{x \geq r^2 \wedge x < (r+1)^2 \wedge x \geq (r+1)^2\}$
   r:=r+1
   $\{x \geq r^2 \wedge x < (r+1)^2\}$

4. $\{x \geq r^2 \wedge x < (r+1)^2\}$
while $x >= (r+1)^2$ do $r := r+1$
$\{x \geq r^2 \wedge x < (r+1)^2\}$ (WHP,3)

5. $\{x \geq r^2 \wedge x \geq (r+1)^2\} r := r+1 \{x \geq r^2\}$ (AS)

6. $\{x \geq r^2 \wedge x \geq (r+1)^2\}$
while $x >= (r+1)^2$ do $r := r+1$
$\{x \geq r^2 \wedge x < (r+1)^2\}$ (WHP,5)

7. $\{x \geq r^2\}$ while $x >= (r+1)^2$ do $r := r+1$
$\{x \geq r^2 \wedge x < (r+1)^2\}$ (DA,2,4,6)

8. $\{x \geq 0\}$
$r := 0;$ while $x >= (r+1)^2$ do $r := r+1$
$\{x \geq r^2 \wedge x < (r+1)^2\}$ (SQ,1,7)

END OF PROOF