Deductive Program Verification: Solutions to Exercise #1

Yih-Kuen Tsay
(with help from Ming-Hsien Tsai)
Dept. of Information Management, National Taiwan University

FLOLAC 2007: July 2–13, 2007

Note

We assume the binding powers of the various operators decrease in this order: $(\cdot)^n$ (exponentiation), $\{+, -\}$, $\neg$, $\{=, \geq, \leq\}$, $\{\forall, \exists\}$, $\{\wedge, \vee\}$, $\rightarrow$, $\leftrightarrow$, $\equiv$.

Solutions

1. Prove the partial correctness of the following annotated program segment: (40 points)

   $\{g = 0 \wedge p = n \wedge n \geq 1\}$
   S_1: **while** $p \geq 2$ **do**
   $\quad S_2$: $g, p := g + 1, p - 1$
   od
   $\{g = n - 1\}$

   Solution.

   Let P denote "$g + p = n \wedge p \geq 1$" (the loop invariant) and B "$p \geq 2$".

$$\dfrac{\dfrac{\text{pred. calculus + algebra}}{g = 0 \wedge p = n \wedge n \geq 1 \rightarrow P} \qquad \dfrac{\pi}{\{P\}\ S_1\ \{P \wedge \neg B\}}\text{(While)} \qquad \dfrac{\text{pred. calculus + algebra}}{P \wedge \neg B \rightarrow g = n - 1}}{\{g = 0 \wedge p = n \wedge n \geq 1\}\ S_1\ \{g = n - 1\}}\text{(Cons.)}$$

   π :

$$\dfrac{\dfrac{\text{pred. calculus + algebra}}{P \wedge B \rightarrow (g+1) + (p-1) = n \wedge (p-1) \geq 1} \qquad \dfrac{}{\{(g+1) + (p-1) = n \wedge (p-1) \geq 1\}\ S_2\ \{P\}}\text{(Assign.)}}{\{P \wedge B\}\ S_2\ \{P\}}\text{(S. Pre)}$$

   The whole proof may be summarized as the following proof outline:

$\{g = 0 \wedge p = n \wedge n \geq 1\}$
$\{\text{invariant: } g + p = n \wedge p \geq 1\}$
S_1: **while** $p \geq 2$ **do**
    $\{g + p = n \wedge p \geq 1 \wedge p \geq 2\}$
    $\{(g+1) + (p-1) = n \wedge (p-1) \geq 1\}$
    S_2: $g, p := g+1, p-1$
    $\{g + p = n \wedge p \geq 1\}$
od
$\{g + p = n \wedge p \geq 1 \wedge \neg(p \geq 2)\}$
$\{g = n - 1\}$

□

2. Prove the total correctness of the following annotated program segment: (60 points)

$\{x = n \wedge n \geq 0\}$
S_1: $y := 0$;
S_2: **while** $x > 0$ **do**
    S_3: $y := y + (2x - 1)$;
    S_4: $x := x - 1$
od
$\{y = n^2\}$

Solution.

$$\dfrac{\pi_1 \qquad \dfrac{\text{pred. calculus + algebra}}{x \geq 0 \wedge y = n^2 - x^2 \wedge \neg(x > 0) \rightarrow y = n^2}}{\{x = n \wedge n \geq 0\}\ S_1; S_2\ \{y = n^2\}}\ (\text{W. Post.})$$

π_1:

$$\dfrac{\dfrac{\pi_3 \qquad \dfrac{}{\{x \geq 0 \wedge 0 = n^2 - x^2\}\ S_1\ \{x \geq 0 \wedge y = n^2 - x^2\}}\ (\text{Assign.})}{\{x = n \wedge n \geq 0\}\ S_1\ \{x \geq 0 \wedge y = n^2 - x^2\}}\ (\text{S. Pre.}) \qquad \pi_2}{\{x = n \wedge n \geq 0\}\ S_1; S_2\ \{x \geq 0 \wedge y = n^2 - x^2 \wedge \neg(x > 0)\}}\ (\text{Sequence})$$

π_2:

$$\dfrac{\dfrac{\pi_4 \qquad \dfrac{}{\{x - 1 \geq 0 \wedge y = n^2 - (x-1)^2\}\ S_4\ \{x \geq 0 \wedge y = n^2 - x^2\}}\ (\text{Assign.})}{\{x \geq 0 \wedge y = n^2 - x^2 \wedge x > 0\}\ S_3; S_4\ \{x \geq 0 \wedge y = n^2 - x^2\}}\ (\text{Sequence})}{\{x \geq 0 \wedge y = n^2 - x^2\}\ S_2\ \{x \geq 0 \wedge y = n^2 - x^2 \wedge \neg(x > 0)\}}\ (\text{While})$$

For termination, the rank function needed in the While rule is simply x; detail omitted.

π_3:

$$\frac{\text{pred. calculus + algebra}}{x = n \wedge n \geq 0 \rightarrow x \geq 0 \wedge 0 = n^2 - x^2}$$

π_4:

$$\dfrac{\pi_5 \qquad \dfrac{}{\{x-1 \geq 0 \wedge y+(2x-1) = n^2-(x-1)^2\}\ S_3\ \{x-1 \geq 0 \wedge y = n^2-(x-1)^2\}}\text{(Assign.)}}{\{x \geq 0 \wedge y = n^2 - x^2 \wedge x > 0\}\ S_3\ \{x-1 \geq 0 \wedge y = n^2-(x-1)^2\}}\text{(S. Pre.)}$$

π_5:

$$\frac{\text{pred. calculus + algebra}}{x \geq 0 \wedge y = n^2 - x^2 \wedge x > 0 \rightarrow x-1 \geq 0 \wedge y+(2x-1) = n^2-(x-1)^2}$$

The whole proof may be summarized as the following proof outline:

$\{x = n \wedge n \geq 0\}$
$\{x \geq 0 \wedge 0 = n^2 - x^2\}$
S_1: $y := 0$;
$\{$invariant: $x \geq 0 \wedge y = n^2 - x^2\}$ $\{$rank function: $x\}$
S_2: **while** $x > 0$ **do**
  $\{x \geq 0 \wedge y = n^2 - x^2 \wedge x > 0\}$
  $\{x-1 \geq 0 \wedge y+(2x-1) = n^2-(x-1)^2\}$
  S_3: $y := y+(2x-1)$;
  $\{x-1 \geq 0 \wedge y = n^2-(x-1)^2\}$
  S_4: $x := x-1$
  $\{x \geq 0 \wedge y = n^2 - x^2\}$
od
$\{x \geq 0 \wedge y = n^2 - x^2 \wedge \neg(x > 0)\}$
$\{y = n^2\}$

$\square$