Week3 - FPV Week 3 exercise solutions and notes

Funktionale Programmierung (Technische Universität München)

Friday III - EN - 13/5/2022

Freitag, 20. Mai 2022 09:57

Zulip-Links:

- FPV-Announcements
- FPV-Lecture
- FPV-TechSupport
- FPV-Organization
- **FPV-Memes**
- FPV_T_III EN

MiniJava 2.0

In the lecture, the weakest precondition operator has been defined for all statements of MiniJava. In this assignment, we consider an extension of the MiniJava language, which provides four new statements.

1. rand x
   Assigns a random value to variable x.
2. x = either $e_0, \ldots, e_k$
   Assigns one of the values of the expressions $e_0, \ldots, e_k$ to variable x non-deterministicaly.
3. x = in a..b
   Assigns the value $\mathbb{I}$ to variable x, if the value of expression e is in the range $[a, b]$ and 0 if e is not in the range or the range is empty ($a > b$).
4. stop
   Immediately stops the program.

Define the weakest precondition operator $\mathbf{WP}[\![\ldots]\!](B)$ for each of these statements.

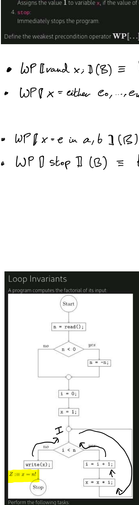
- $WP[\![\text{rand } x]\!](B) \equiv \forall x.\, B$
- $WP[\![x = \text{either } e_0, \ldots, e_k]\!](B) \equiv B[e_0/x] \wedge \ldots \wedge B[e_k/x] = \forall e \in \{e_0, \ldots, e_k\}.\ B[e/x]$

  $\left[WP[\![x := e]\!](B) = B[e/x] \right]$
- $WP[\![x = e \text{ in } a,b]\!](B) \equiv (a \le e \le b \wedge B[e/x]) \vee ((e < a \vee b < e) \wedge B[0/x])$
- $WP[\![\text{stop}]\!](B) \equiv \text{true}$

stop → false $\Rightarrow B$, since unreachable, so no precondition needed.

Loop Invariants

A program computes the factorial of its input



Perform the following tasks.

1. Discuss the problem that arises when computing weakest preconditions to prove Z.
2. How can you use weakest preconditions to prove Z anyway?
3. Try proving Z using the the loop-invariant $x \ge 0 \text{ and } i = 0 \wedge x = 1 \wedge n = 0$ at the end of the loop body and in particular discuss these questions.
   - a) How has a useful loop invariant be related to Z?
   - b) What happens if the loop-invariant is chosen too strong?
   - c) What happens if the loop-invariant is chosen too weak?
   - d) Can you give a meaningful lower and upper bound for useful loop-invariants?
4. Retry proving Z using the loop invariant $x = n!$ (again at the end of the loop body) and improve this invariant until the proof succeeds.

① We have a loop.

② Recall local consistency: We say the assertions of a program are locally consistent, if for every program point s, the postcond. B & precond. A:

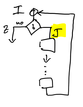
$$A \Rightarrow WP[\![s]\!](B)$$

Recall: One can verify an assertion Z at the end of the program if every program point is annotated, the beginning of the program with true, and all assertions are locally consistent.

$\Rightarrow$ Find loop invariant I and show its local consistency.

Loop invariant: Assertion that holds *before* the loop and often an arbitrary number of iterations.

"Useful" loop invariant: A loop invariant I which is locally consistent with Z.



$I \Rightarrow WP[\![b]\!](\neg J)$

Finding a (useful) loop invariant

1. Computation has to be explicit, else it has to contain the gradual computation or the way to Z.
2. All meaningful relations between variables should appear. Also all known bounds on the variables.
3. It should stay to the back condition

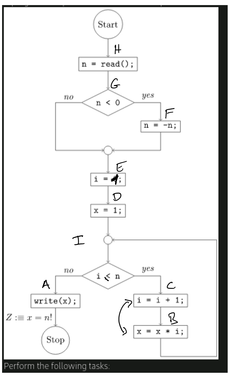
$\Rightarrow$ the strongest loop invariant which still holds

$\rightarrow$ a strong enough loop invariant

$$I \equiv x = i! \wedge i \le n \wedge i \ge 0 \wedge n \ge 0$$

$I \equiv x = i!$

- $WP[\![\text{write}(x)]\!](Z) \equiv Z \equiv x = n!$
- $WP[\![x = x \cdot i]\!](I) \equiv x \cdot i = i! \quad \not\Leftarrow \quad x = (i-1)! \equiv B$
- $WP[\![i = i+1]\!](B) \equiv x = i!$
- $WP[\![\text{cond}]\!] \equiv \ldots \Leftarrow I$



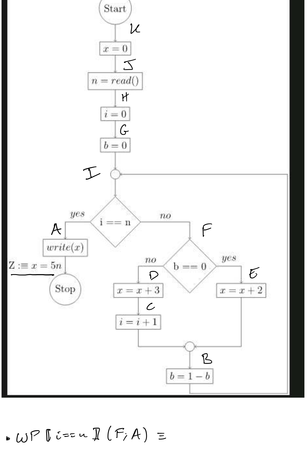
Perform the following tasks.

$I \equiv x = i! \wedge i \le n+1 \wedge i \ge 0 \quad \wedge n \ge 0$

- $WP[\![\text{write}(x)]\!](Z) \equiv x = n! \equiv: A$
- $WP[\![i = i+1]\!](I) \equiv x = i! \wedge i \le n \wedge i+1 > 0 \wedge n \ge 0$
- $WP[\![x = x \cdot i]\!](B) \equiv x \cdot i = i! \wedge i \le n \wedge i \ge 0 \wedge n \ge 0$

Two b, or Not Two b

Prove Z using weakest preconditions.



$I \equiv x = 5i + 2b \wedge b \in \{0,1\} \wedge i \le n \wedge (i = n \Rightarrow b = 0)$

$WP[\![\text{write}(x)]\!](Z) \equiv Z \equiv: A$

$WP[\![b = 1-b]\!](I) \equiv$

$x = 5i - 2b + 2 \wedge b \in \{0,1\} \wedge i \le n \wedge (i = n \Rightarrow b = 1) \equiv: B$

$WP[\![i = i+1]\!](B) \equiv x = 5i - 2b + 7 \wedge b \in \{0,1\} \wedge (i+1 = n \Rightarrow b = 1) \equiv: C$

$WP[\![x = x+3]\!](C) \equiv x = 5i - 2b + 4 \wedge b \in \{0,1\} \wedge (i+1 = n \Rightarrow b = 1) \equiv: D$

$WP[\![x = x+2]\!](B) \equiv x = 5i - 2b \wedge b \in \{0,1\} \wedge (i = n \Rightarrow b = 1) \equiv: E$

$WP[\![b := 0]\!](D, E) \equiv$

$(b = 1 \wedge x = 5i - 2b + 4 \wedge (i+1 = n \Rightarrow b = 1) \wedge b \in \{0,1\})$

$(b = 0 \wedge x = 5i - 2b \wedge (i = n \Rightarrow b = 1) \wedge b \in \{0,1\})$

$\Leftarrow (b = 1 \wedge x = 5i + 2b \wedge i \neq n) \vee (b = 0 \wedge x = 5i + 2b \wedge i \neq n)$

$\equiv x = 5i + 2b \wedge i \neq n \wedge b \in \{0,1\} \equiv: F$

- $WP[\![i == n]\!](F, A) \equiv$

$\mathbf{WP}[\![x = x + 2]\!](A)$
$\equiv \mathbf{WP}[\![x = x + 2]\!](x = 5i - 2b + 2 \wedge b \in \{0,1\} \wedge (i = n \iff b = 1))$
$\equiv x = 5i - 2b \wedge b \in \{0,1\} \wedge (i = n \iff b = 1) \equiv: D$

$\mathbf{WP}[\![b := 0]\!](C, D)$
$\equiv \mathbf{WP}[\![b := 0]\!]((x = 5i - 2b + 4 \wedge b \in \{0,1\} \wedge (i + 1 = n \iff b = 1), x = 5i - 2b \wedge b \in \{0,1\} \wedge (i = n \iff b = 1)))$
$\equiv ((b = 1 \wedge x = 5i - 2b + 4 \wedge (i + 1 = n \iff b = 1)) \vee (b = 0 \wedge x = 5i - 2b \wedge (i = n \iff b = 1)))$
$\equiv ((b = 1 \wedge x = 5i + 2) \vee (b = 0 \wedge x = 5i + i \neq n))$
$\iff (b = 1 \wedge x = 5i + 2b \wedge i \neq n) \vee (b = 0 \wedge x = 5i + 2b \wedge i \neq n)$
$\equiv x = 5i + 2b \wedge i \neq n \wedge b \in \{0,1\} \equiv: E$

$\mathbf{WP}[\![i == n]\!](E, Z)$
$\equiv \mathbf{WP}[\![i == n]\!](x = 5i + 2b \wedge b \in \{0,1\}, x = 5n)$
$\equiv ((i \neq n \wedge x = 5i + 2b \wedge b \in \{0,1\}) \vee (i = n \wedge x = 5n))$
$\iff ((i \neq n \wedge x = 5i + 2b \wedge b \in \{0,1\}) \wedge (i = n \iff b = 0)) \vee (i = n \wedge x = 5n \wedge (i = n \iff b = 0) \wedge b \in \{0,1\})$
$\equiv ((i \neq n \wedge x = 5i + 2b \wedge b \in \{0,1\}) \wedge (i = n \iff b = 0)) \vee (i = n \wedge x = 5i + 2b \wedge (i = n \iff b = 0) \wedge b \in \{0,1\})$
$\equiv x = 5i + 2b \wedge b \in \{0,1\} \wedge (i = n \iff b = 0) \equiv: I$

$\mathbf{WP}[\![b := 0]\!](I)$
$\equiv \mathbf{WP}[\![b := 0]\!](x = 5i + 2b \wedge b \in \{0,1\} \wedge (i = n \iff b = 0))$
$\equiv x = 5i \equiv: F$

$\mathbf{WP}[\![i := 0]\!](F)$
$\equiv \mathbf{WP}[\![i := 0]\!](x = 5i)$
$\equiv x = 0 \equiv: G$

$\mathbf{WP}[\![x = \text{read}()]\!](G)$
$\equiv \mathbf{WP}[\![x = \text{read}()]\!](x = 0)$
$\equiv x = 0 \equiv: H$

$\mathbf{WP}[\![x = 0]\!](H)$
$\equiv \mathbf{WP}[\![x = 0]\!](x = 0)$
$\equiv \text{true}$