Formální Metody a Specifikace
Cvičení 4b (103)

7. duben 2011

1 Exercise 7

Extend the definition of the notion "transition relation" from the lecture with the case that $s(pc)$ points to a program line corresponding to (the beginning or end) of a (Java/C/C++) for-loop. Here, handle the loop directly, and do *not* translate it to an if-then-goto construction. You may ignore the initialization part of the loop (i.e., assume that it is empty).

(2 points)

From now on, when proving some predicate-logical formula, you may assume the axioms of all necessary theories. Moreover, in addition to the Peano axioms, you may assume all facts that intuitively hold for the natural numbers (e.g., associativity, commutativity of addition and multiplication) and all relevant definitions (e.g., the definition of division of natural numbers). Also, you may use the proof rules liberally. That is, you do not have to follow the proof rules in all details, as long as you are aware of how the missing details would look like.

2 Exercise 8

```
    $x \in \mathbb{N}$
1:  **while** $x \geq 0$ **do**
2:      $x \leftarrow x/2$
3:      **print** $10/x$
```

Let

- $I :\Leftrightarrow pc = 1 \land x \geq 7$, and
- $O :\Leftrightarrow pc = 3 \Rightarrow x \neq 0$.

For each $\phi \in \{BMC(1), \ldots, BMC(10)\}$, prove either $\models \phi$, or $\models \neg\phi$. Some of the proofs will look similar. In such cases, it is not necessary to write down all of them. Instead, it suffices to explain the differences between them.

(3 points)

3 Exercise 9

```
1: $x \leftarrow a[2]$
2: $a \leftarrow \text{write}(a, 2, a[1])$
3: $a \leftarrow \text{write}(a, 1, x)$
```

Let

- $I :\Leftrightarrow pc = 1 \wedge \forall i \in \{1, \ldots 10\} \,.\, a[i] \leq 10$, and
- $O :\Leftrightarrow \forall i \in \{1, \ldots 10\} \,.\, a[i] \leq 10$.

For each $\phi \in \{BMC(1), BMC(2), BMC(3)\}$, prove either $\models \phi$, or $\models \neg\phi$.

(2 points)

4 Exercise 10

```
1: $x_0 \leftarrow x$
2: for $i \leftarrow 1$ to 7 do $x \leftarrow x + 2$
3: return x
```

Assume that the initialization condition I is $pc = 1 \wedge i = 1$.

- Is $pc = 3 \Rightarrow x = 564$ an invariant? If no, exchange the number 564 with a term in such a way that the result is an invariant.
- Let V be the result of the previous item. Is V an *inductive* invariant? If no, provide an inductive invariant that implies V.

In the lecture, we did not formalize the operational semantics of for-loops. Still, line 2 has an obvious meaning that you can use.

(2 points)