Formální Metody a Specifikace
Cvičení 5a (101,102)

14. duben 2011

1 Exercise 10

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

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

- 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)

2 Exercise 11

Write down and check all verification conditions for the following program:

```
$x \leftarrow 0$
@ $x = 0$
for $i \leftarrow 1$ to 10 do
    @ $x = \sum_{k=1}^{i-1} a[k]$
    $x \leftarrow x + a[i]$
    @ $x = \sum_{k=1}^{i} a[k]$
@ $x = \sum_{k=1}^{10} a[k]$
return $x$
```

(2 points)

3 Exercise 12

Try to show the correctness of the following algorithm by adding the necessary assertions and checking the corresponding verification conditions. If it is not correct, remove the mistake (keeping the general structure of the algorithm), and show the correctness of the changed algorithm.

- Input: $x, y \in \mathcal{N}$
- Ouput: xy

```
$r \leftarrow x$; $i \leftarrow 1$
**while** $i < y$
    $r \leftarrow r + x$
    $i \leftarrow i + 1$
**return** $r$
```

(2 points)

4 Exercise 13

Try to show the correctness of the following algorithm by adding the necessary assertions and checking the corresponding verification conditions. If it is not correct, remove the mistake (keeping the general structure of the algorithm), and show the correctness of the changed algorithm.

- Input: $a \in \mathcal{A}_{10}$
- Output: $c \in \mathcal{A}_{10}$, $a = c$

```
**for** $i \leftarrow 1$ **to** 10 **do**
    $b[i] \leftarrow a[11 - i]$
**for** $i \leftarrow 1$ **to** 10 **do**
    $a[i] \leftarrow b[11 - i]$
**return** $a$
```

(2 points)