Laboratory: *Reasoning about Programs I*

Objectives

1. Write program specification, invariants, termination terms and prove them with `RISC ProofNavigator`.

Example 1

Consider the following algorithm finding the smallest index r of an occurrence of value x in array a ($r = -1$, if x does not occur in a).

```
i := 0; r := -1; n = len(a);
while i < n && r = -1 do
    if a[i] = x
        then r := i
    else i := i + 1
return r
```

Write for the algorithm a suitable specification, derive a loop invariant and termination term and prove the total correctness of the algorithm with `RISC ProofNavigator`.

Solution. The precondition is $P :\Longleftrightarrow \top$ and the postcondition is

$$Q :\Longleftrightarrow ((r = -1 \wedge \underset{\substack{i\\0\le i<len(a)}}{\forall} a[i] \neq x) \vee (0 \le r < len(a) \wedge a[r] = x \wedge \underset{\substack{i\\0\le i<r}}{\forall} a[i] \neq x))$$

The invariant is

$$I :\Longleftrightarrow n = len(a) \wedge 0 \le i \le n \wedge \underset{\substack{j\\0\le j<i}}{\forall} a[j] \neq x \wedge (r = -1 \vee (r = i \wedge i < n \wedge a[r] = x))\text{(see derivation on the whiteboard).}$$

A termination term is $t(i) = n - i$.
Check the file `linsearch.pn` (it can be found on the virtual machine on the directory `examples-ProofNavigatorCVC3`)

Example 2

Consider the following algorithm computing the natural power a^p of a non-zero real number $a \in \mathbb{R}^*$, $p \in \mathbb{N}$.

```
int power (int a, int p)
    rez := 1; i   := 0;
    while i < p do
```

```
        i := i + 1;
        rez := rez * a
    return rez
```

Write for the algorithm a suitable specification, derive a loop invariant and prove the partial correctness of the algorithm with `RISC ProofNavigator`.

Solution. The precondition is $P :\iff a \in \mathbb{R}^* \ \wedge \ p \in \mathbb{N}$ and the postcondition is $Q :\iff rez = \prod_{i=1}^{p} a$. We synthesize a suitable invariant I for the loop above. We have the following:

#iter	i	rez
0	0	1
1	1	$1 * a = a$
2	2	$a * a = a^2$
...	...	...
k	k	$a^{k-1} * a = a^k$
$k+1$	$k+1$	$a^k * a = a^{k+1}$
...	...	...
p	p	$a^{p-1} * a = a^p$

We conjecture that the loop invariant is $rez = \prod_{j=1}^{i} a$. We formalize the problem and prove it with `RISC ProofNavigator`.

Example 3

Write an algorithm computing the sum of the first n natural numbers and prove its partial correctness with `RISC ProofNavigator`.

Hint. A suitable invariant for the loop invariant is:

$$I :\iff s = \sum_{j=1}^{i-1} j \wedge 1 \leq i \leq n + 1$$

.