Prof. Bernd Finkbeiner, Ph.D.
Peter Faymonville, M.Sc.
Michael Gerke, B.Sc.

Winter term 2011/2012
Problem Set 11

Verification

Please write the names of all group members on the solutions you hand in.

Tool: πVC

You should use the tool πVC to solve the problems of this set. A modified version of the tool for this lecture is available from the lecture website. In order to run it, run the command `java -jar PiGui.jar`. You will need an internet connection to successfully compile and verify programs. After you have successfully proved the desired properties, you can submit your solution directly from within the tool.
Hint 1: The small window on the bottom right might be to small to see all the contents on a small screen. It does not have scoll bars, but it is scrollable to ensure your access to the vital information which properties are proven and which are not.
Hint 2: If you get stuck with the proof you can email us for some additional hints.

Problem 1: Abs

Prove partial correctness of the program Abs using πVC. You can download the file `Abs.pi` from the lecture website.

```
@pre $\top$
@post $\forall i. 0 \leq i < |rv| \rightarrow rv[i] \geq 0$
int[] abs(int[] $a_0$) {
  int[] $a := a_0$;
  for
    @ $\top$
    (int $i := 0$; $i < |a|$; $i := i + 1$) {
    if ($a[i] < 0$) {
      $a[i] := -a[i]$;
    }
  }
  return $a$;
}
```

Figure 1: Computing the absolute values of an array

Problem 2: Insertion Sort

Prove partial correctness of the program InsertionSort using πVC. You can download the file `InsertionSort.pi` from the lecture website.

```
@pre $\top$
@post sorted$(rv, 0, |rv| - 1)$
int[] InsertionSort(int[] $a_0$) {
  int[] $a := a_0$;
  for @ $\top$
    (int $i := 1$; $i < |a|$; $i := i + 1$) {
    int $t := a[i]$;
    for @ $\top$
      (int $j := i - 1$; $j \geq 0$; $j := j - 1$) {
      if $(a[j] \leq t)$ break;
      $a[j+1] := a[j]$;
    }
    $a[j+1] := t$;
  }
  return $a$;
}
```

Figure 2: InsertionSort

Problem 3: Cooper's Method

Apply quantifier-elimination to the following $\Sigma_{\mathbb{Z}}$-formulae.

1. $\forall y.\ 3 < x + 2y \vee 2x + y < 3$
2. $\exists y.\ 3 < x + 2y \vee 2x + y < 3$