universität innsbruck

Program Verification	SS 2024	LVA 703083+703084
Sheet 11		Deadline: June 11, 2024, 3pm

- Prepare your solutions on paper.
- Mark the exercises in OLAT before the deadline.
- If you used IMP2 and Isabelle, then upload your Isabelle file in OLAT.
- Marking an exercise means that a significant part of that exercise has been treated.

For Exercises 1 and 2.2 you can develop a solution on paper or in Isabelle using IMP2.

Exercise 1 *Proof Tableaux* **7 p.**

Consider the following algorithm *Copy*

```
a := x;
y := 0;
while (a != 0) {
  y := y + 1;
  a := a - 1;
}
```

1. Show partial correctness of *Copy*, i.e., develop a proof tableau for $(\!|x \geq 0|\!)\ \mathit{Copy}\ (\!|x = y|\!)$ using the while-rule. (3 points)
2. Show total correctness of *Copy*, i.e., develop a proof tableau for $(\!|x \geq 0|\!)\ \mathit{Copy}\ (\!|x = y|\!)$ using the while-total-rule. (2 points)
3. Does the partial correctness property $(\!|\mathsf{true}|\!)\ \mathit{Copy}\ (\!|x = y|\!)$ hold? Either argue why it does not hold, or prove it. (2 points)

Exercise 2 *Non-Termination of Imperative Programs* **5 p.**

The Hoare-calculus can not only be used to prove termination (with the while-total-rule), but it can also be used to prove non-termination via the while-rule.

1. On slide 6/57 a Hoare-triple is given that characterizes termination of a program w.r.t. those inputs that satisfy φ.

   Now provide a Hoare-triple (for partial correctness) that encodes that program P does not terminate on inputs that satisfy φ. (3 points)
2. Prove non-termination of the factorial program for all inputs $x < 0$ by constructing a suitable proof tableau. (2 points)

   ```
   y := 1;
   while (x != 0) {
     y := y * x;
     x := x - 1
   }
   ```

Exercise 3 *Soundness of Hoare-Calculus* **8 p.**

In the lecture we only considered partial correctness of the Hoare-calculus, i.e., we proved:

$$\vdash (\!|\varphi|\!)\, P\, (\!|\psi|\!) \longrightarrow\, \models (\!|\varphi|\!)\, P\, (\!|\psi|\!)$$

In this exercise we consider total correctness.

1. We say that a relation $\to$ is deterministic, if for all a there is at most one b such that $a \to b$. Prove that for deterministic $\to$, termination is equivalent to normalization, i.e., there is no infinite $\to$-sequence starting from a is equivalent to $\exists b.\ a \to^! b$. (3 points)
2. Provide a definition of $\models_{total} (\!|\varphi|\!)\, P\, (\!|\psi|\!)$, i.e., a semantic notion of total correctness. You can exploit that $\hookrightarrow$ is deterministic. (2 points)
3. How would you try to prove $\vdash (\!|\varphi|\!)\, P\, (\!|\psi|\!) \longrightarrow\, \models_{total} (\!|\varphi|\!)\, P\, (\!|\psi|\!)$ for the Hoare-calculus with while-total rule? Just state the main property you would try to prove, and state which proof principle (induction, proof by contradiction, etc.) you would apply, with a brief justification why this looks like a promising attempt. (3 points)