universität innsbruck

Program Verification	SS 2021	LVA 703083+703084
Sheet 14		Deadline: June 22, 2021, 8am

- Prepare your solutions on paper.
- Marking an exercise in OLAT means that a significant part of that exercise has been treated.
- Upload your solution in OLAT as a single PDF file.
- **This is a bonus exercise sheet.**

Exercise 1 *Repetition: Proofs by Induction on Terms* 9 p.

Recall that $\mathcal{V}$ denotes a typed set of variables. Let $\mathcal{V}, \mathcal{V}'$ be two typed sets of variables.
The merge of two sets of variables is defined as $\mathcal{V} \cup \mathcal{V}'$, and implicitly assumes that there are no conflicting variables assignments. For instance $\{x : \mathsf{Nat}, y : \mathsf{List}\} \cup \{x : \mathsf{Nat}, z : \mathsf{Nat}\}$ is possible and results in $\{x : \mathsf{Nat}, y : \mathsf{List}, z : \mathsf{Nat}\}$, but $\{x : \mathsf{Nat}, y : \mathsf{List}\} \cup \{x : \mathsf{List}, z : \mathsf{Nat}\}$ is not allowed.

1. Show that the set of typed terms is monotone: $\mathcal{T}(\Sigma, \mathcal{V})_\tau \subseteq \mathcal{T}(\Sigma, \mathcal{V} \cup \mathcal{V}')_\tau$. (3 points)
2. Show soundness of the type inference algorithm, cf. slide 4/8–9: if $\mathit{infer\_type}\ \Sigma\ \tau\ t = \mathit{return}\ \mathcal{V}$ then
   - $\mathcal{V}$ is well-defined (no conflicting variable assignments) and
   - $t \in \mathcal{T}(\Sigma, \mathcal{V})_\tau$

   (6 points)

Exercise 2 *Semantics of Imperative Programs* 6 p.

Prove the other direction of the equivalence of big-step semantics (see exercise sheet 12) and small-step semantics:

$$(C, \alpha) \hookrightarrow^* (\texttt{skip}, \beta) \longrightarrow (C, \alpha) \to \beta$$

Clearly state which kind of induction you are using.
Hint: In the proof you will most likely figure out one required auxiliary property of $\hookrightarrow$ that you should clearly state as lemma, but don't need to prove.

Exercise 3 *Soundness of Hoare-Calculus* 5 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. Provide a definition of $\models_{total} (\!|\varphi|\!)\, P\, (\!|\psi|\!)$, i.e., a semantic notion of total correctness. You can exploit that $\hookrightarrow$ is deterministic, i.e., for all a there is at most one b such that $a \hookrightarrow b$. (2 points)
2. 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)