universität innsbruck

| Program Verification | SS 2023 | LVA 703083+703084 |
|---|---|---|
| Sheet 5 | | Deadline: April 26, 2023, 10am |

- Prepare your solutions on paper.
- Mark the exercises in OLAT before the deadline.
- Marking an exercise means that a significant part of that exercise has been treated.

## Exercise 1 *Confluence and Normal Forms* **4 p.**

1. Recall the notion of confluence: $\hookrightarrow$ is confluent if and only if for all terms $s, t, u$: whenever $t \hookrightarrow^* s$ and $t \hookrightarrow^* u$ then there is some term $v$ such that $s \hookrightarrow^* v$ and $u \hookrightarrow^* v$.

   Prove that normal forms are unique for confluent $\hookrightarrow$: whenever $\hookrightarrow$ is confluent and $t \hookrightarrow^! s$ and $t \hookrightarrow^! u$, then $s = u$. (2 points)

2. On slide 3/56 it was stated that $\ell\alpha\downarrow = r\alpha\downarrow$ follows from $\ell\alpha \hookrightarrow r\alpha$.

   Perform a proof of a more general result: whenever $s \hookrightarrow^* t$ for some confluent and terminating relation $\hookrightarrow$, then $s\downarrow = t\downarrow$. (2 points)

## Exercise 2 *Freshness of Variables* **4 p.**

Consider slides slides 3/70–72. It was shown that freshness of variables is essential for the induction formula. However, in the proof on slide 3/72 freshness is never mentioned.
Identify the step(s) of the proof which break without freshness of the $x_i$, and make the reasoning more explicit, so that one can clearly see the necessity of freshness.

## Exercise 3 *Axioms about Equality* **12 p.**

On slide 3/74 we have seen that there are not enough properties about the equality predicates $=_\tau$. Among these missing properties are reflexivity and symmetry of $=_\tau$.
One way to get access to these properties is by proving that these formulas are valid in the standard model.

1. Prove that $=_\tau$ is symmetric, i.e., $\mathcal{M} \models \forall x, y.\, x =_\tau y \longleftrightarrow y =_\tau x$ for the standard model $\mathcal{M}$. (2 points)

Instead of proving that properties via the standard model, an alternative approach is to show that the missing properties are already consequences of $AX$ (assuming that $AX$ includes the induction formulas as well as the decomposition- and disjoint-theorems of slide 3/60).

2. Show $AX \models \forall xs.\, xs =_{\mathsf{List}} xs$ via a natural deduction proof in the style of slide 3/74.

   Here, you can assume the standard definition of lists of natural numbers via Nil and Cons and you can assume $\forall x.\, x =_{\mathsf{Nat}} x$ as axiom (which can be proven in a similar way). For the reasoning about Boolean connectives you can be sloppy, but you should be detailed in proof steps that involve using axioms of $AX$, i.e., make precise which axioms you are using. (4 points)

3. Show that $=_{\mathsf{Nat}}$ is symmetric by deducing $AX \models \forall x, y.\, x =_{\mathsf{Nat}} y \longrightarrow y =_{\mathsf{Nat}} x$ as in part (2).
   Hint: Use induction on $x$ for the formula $\psi_n := \forall y.\, x =_{\mathsf{Nat}} y \longrightarrow y =_{\mathsf{Nat}} x$.

   Be careful with the correct usage of quantifiers in your proof.

(a) Write down the fully spelled out formula that you get when using $\psi_n$ in the induction scheme for natural numbers. (2 points)

(b) Perform the proof. For this part you can assume an additional axiom scheme for case analysis on natural numbers:

$$\vec{\forall}\,(\varphi[x/\mathsf{Zero}] \longrightarrow (\forall z.\, \varphi[x/\mathsf{Succ}(z)]) \longrightarrow \varphi)$$

where $z$ must be fresh for $\varphi$. This scheme is an easy consequence of the induction scheme for natural numbers.

Hint: in each case of the induction proof, you need to perform one case analysis. (4 points)