Program Verification	SS 2021	LVA 703083+703084
Sheet 6		Deadline: April 27, 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.

Exercise 1 *Induction Formulas* **10 p.**

1. On slide 3/71 the induction formula for arbitrary data-types has been defined. Explicitly write down the induction formula for an arbitrary formula φ and the following datatype; don't forget to mention conditions on freshness of variables.

$$\mathsf{data}\ \mathsf{Tree} = \mathsf{Empty} : \mathsf{Tree} \mid \mathsf{Node} : \mathsf{Tree} \times \mathsf{Nat} \times \mathsf{Tree} \to \mathsf{Tree}$$

(3 points)

2. Now consider a concrete property, namely we assume that there are two functions on trees

$$\mathsf{flatten} : \mathsf{Tree} \to \mathsf{List}$$
$$\mathsf{mergeTree} : \mathsf{Tree} \times \mathsf{Tree} \to \mathsf{Tree}$$

in combination with the standard append function on lists.

The aim is to prove the following property by induction on t_1:

$$\forall t_1, t_2.\ \mathsf{flatten}(\mathsf{mergeTree}(t_1, t_2)) =_{\mathsf{List}} \mathsf{append}(\mathsf{flatten}(t_1), \mathsf{flatten}(t_2))$$

Explicitly write down the induction formula for this property, where all substitutions have been fully applied. (3 points)

3. Soundness of the induction formulas has been proven on slide 3/72. However, the proof never explicitly mentions freshness of the variables, which is essential (cf. slide 3/70).

Study the proof on slide 3/72 and extend the argumentation of each step that is based on the freshness condition. (4 points)

Exercise 2 *Axioms about Equality* **10 p.**

On slide 3/74 we have seen that there are not enough axioms about the equality predicates $=_\tau$. Among the missing axioms are reflexivity and symmetry of $=_\tau$.
On the previous exercise sheet we have seen one way to get access to these new axioms, namely by proving that the formulas are valid in the standard model.
In this exercise, we show that these properties are already consequences of AX (which in particular include the decomposition- and disjoint-theorems of slide 3/60), so that reflexivity and symmetry are just derived properties.

1. 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)

2. 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 (1).
   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 ψ_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 φ. 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)