universität innsbruck

Program Verification	SS 2024	LVA 703083+703084
Sheet 1		Deadline: March 12, 2024, 3pm

- 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 *Specifications in Predicate-Logic* **10 p.**

Recall the specification of a sorting algorithm on slide 1/12.

1. Extend the formula for a sorting algorithm so that it is guaranteed that xs and ys contain the same elements. Here you can assume that an array like xs has elements that are indexed from 0 to $length(xs) - 1$. Feel free to use arbitrary quantifiers and logical connectives as used in the "Logic" lecture. (3 points)
2. Does your formula fully specify sorting algorithms, in the case that input arrays contain distinct elements? If not, provide an algorithm that satisfies the formula, but has a behavior which a usual sorting algorithm does not have. (2 points)
3. Does your formula fully specify sorting algorithms for arbitrary inputs, even in the case the input is non distinct? If not, provide an algorithm that satisfies the formula, but has a behavior which a usual sorting algorithm does not have. (2 points)
4. Modify the formula so that it specifies a variant of a sorting algorithm, namely one which removes duplicates. E.g., sorting with removal of duplicates applied on $[1, 2, 1]$ must result in $[1, 2]$ and not in $[1, 1, 2]$. (3 points)

Exercise 2 *Induction Proof* **3 p.**

Consider the *append*-algorithm and the induction proof on slides 1/17–18. Perform a similar proof and show that Nil is a right-neutral element, i.e., $\mathsf{append}(xs, \mathsf{Nil}) = xs$. Explicitly write down the induction hypothesis and the steps that you did in the equational reasoning. (3 points)

Exercise 3 *Inductively Defined Sets* **7 p.**

Let R be a binary relation. The transitive closure of R (usually written R^+) is defined as the inductive set T:

$$\frac{(x, y) \in R}{(x, y) \in T} \qquad\qquad \frac{(x, y) \in R \quad (y, z) \in T}{(x, z) \in T}$$

We further define that a binary relation S is transitive iff[1] for all x, y, z it holds that whenever $(x, y) \in S$ and $(y, z) \in S$ then $(x, z) \in S$.

1. Define a formula $\varphi(S)$ which states that S is transitive. (1 point)
2. Write down the structural induction rule of the set T, cf. slide 2/12. Since the inductively defined set is a set of pairs, the property P from the slides will be a property of pairs, i.e., $P(x, y)$. (2 points)

[1] "iff" means "if and only if"

3. Prove that T is the least transitive set that contains R in the following sense: whenever $R \subseteq S$ and S is transitive then $T \subseteq S$, i.e., $\forall x, y.\, (x, y) \in T \longrightarrow (x, y) \in S$. (4 points)

4. Optional, will be discussed during seminar, if time permits: prove that T is transitive.