universität innsbruck

Program Verification	SS 2023	LVA 703083+703084
Sheet 10		Deadline: May 31, 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 *Contexts and Subterms* — 9 p.

The set of contexts $\mathcal{C}$ can formally be defined as follows, where $\Box$ represents the hole and types are ignored for simplicity.

$$\frac{}{\Box \in \mathcal{C}} \qquad \frac{t_1 \in \mathcal{T}(\Sigma, \mathcal{V}) \quad \dots \quad C \in \mathcal{C} \quad \dots \quad t_n \in \mathcal{T}(\Sigma, \mathcal{V})}{f(t_1, \dots, C, \dots, t_n)}$$

1. Provide a recursive definition of plugging a term t into the hole of a context C, i.e., define $C[t]$. (1 point)
2. Prove $s \hookrightarrow t \longrightarrow C[s] \hookrightarrow C[t]$. Which induction scheme are you using? (2 points)
3. Prove $s \trianglerighteq t \longrightarrow \exists C.\ s = C[t]$. Which induction scheme are you using? (2 points)
4. Prove that $SN(\hookrightarrow)$ implies $SN(\hookrightarrow \circ \trianglerighteq)$ where $\circ$ here denotes relation composition. (4 points)
   Hint: You should start your proof with an infinite $(\hookrightarrow \circ \trianglerighteq)$-sequence and then show that from this sequence one can construct an infinite $\hookrightarrow$-sequence with the help of the previous results.

   Note that this is the main property to ensure that the induction rule wrt. algorithms (slide 5/32) is an instance of well-founded induction. The reason is that there we provide IHs which correspond to subterms of rhss. Therefore, for each equation $\ell = r$ and subterm u of r that leads to an IH, we have $\ell \hookrightarrow r \trianglerighteq u$, so the subterm u of the rhs is smaller than the lhs ℓ wrt. the strongly normalizing relation $\hookrightarrow \circ \trianglerighteq$.

Exercise 2 *Equational Reasoning and Induction* — 11 p.

Consider the following program.

$$\begin{aligned}
&\mathsf{plus}(\mathsf{Succ}(x), y) = \mathsf{Succ}(\mathsf{plus}(x, y))\\
&\mathsf{plus}(\mathsf{Zero}, y) = y\\
&\mathsf{times}(\mathsf{Succ}(x), y) = \mathsf{plus}(y, \mathsf{times}(x, y))\\
&\mathsf{times}(\mathsf{Zero}, y) = \mathsf{Zero}
\end{aligned}$$

The aim is to prove commutativity of multiplication, so $\forall x, y. \mathsf{times}(x, y) =_{\mathsf{Nat}} \mathsf{times}(y, x)$. To solve this problem you will need to identity and prove several additional properties. In the upcoming exercise, you should perform the proof of commutativity as far as possible. You can assume that plus is commutative, as this property was already proven in the lecture.

1. Identify a first additional property and prove it. (2 points)
2. Identify a second additional property and prove it. (3 points)
3. Identify a third additional property and prove it. (3 points)

4. Finalise the overall proof of commutativity of multiplication. (3 points)

Of course, if you don't need three additional properties, then that is also fine and you can still mark all parts in OLAT.