Prof. Dr. A. Poetzsch-Heffter
Dipl.-Inf. P. Michel
Dipl.-Inf. C. Feller

University of Kaiserslautern
Department of Computer Science
Software Technology Group

Exercise Sheet 4: Specification and Verification with Higher-Order Logic (Summer Term 2012)

Date: 02.05.2012

Exercise 1 Foundations

a) (Prepare!) What is the order of the following formulas?
  - $\text{Suc}(0) \neq 0$
  - $\forall n.\ \text{Suc}(n) \neq 0$
  - $\forall n\ m.\ \text{Suc}(n) = \text{Suc}(m) \longrightarrow n = m$
  - $\forall P.\ P(0) \wedge \Big(\forall n.\ P(n) \longrightarrow P(\text{Suc}(n))\Big) \longrightarrow \forall n.\ P(n)$

b) (Prepare!) Determine which of these terms are syntactically correct. For the correct terms give possible types for all occurring variables and the complete term.
  - $(\lambda x.\ x = a)\ b$
  - $(\lambda x = x)$
  - $(\lambda x.\ True) = (\lambda x.\ (f\ g\ x) = y)$
  - $(x \longrightarrow x) = (b\ b)$

c) (Prepare!) Consider the following set of sets $U = \{\{1\}, \{1, 2\}\}$, which is not a universe. For each of the closure conditions violated by U, give an example set which should have been included in U.

d) (Prepare!) Consider the standard model $M = \langle (D_\alpha)_{\alpha \in \tau}, J \rangle$ for the set of types τ and constants defined in the lecture, where we consider the additional binary constant symbol $+ : ind \Rightarrow ind \Rightarrow ind$. The frame $(D_\alpha)_{\alpha \in \tau}$ is defined by $D_{bool} = \{T, F\}$, $D_{ind} = \mathbb{N}$ and $D_{\alpha \Rightarrow \beta} = D_\alpha \Rightarrow D_\beta$, i.e. the set of all functions from α to β. J interprets all constants as defined in the lecture and $+$ as the usual addition on natural numbers. Consider the following formula:

$$a = b \longrightarrow (\lambda x.x + a) = (\lambda x.b + x)$$

  - Prove that the formula is satisfiable with regard to M, by giving an assignment under which the formula evaluates to T.
  - Is the formula valid with regard to M?

Exercise 2 Conservative Extensions

a) (Prepare!) Let $T = (\chi, \Sigma, A)$ be the core HOL theory as defined in the lecture. Consider the following extension of T:

$$T' = (\chi, \Sigma, A \cup \{(\neg P \longrightarrow P) \longrightarrow P\})$$

Is T' a conservative extension of T?

b) (Prepare!) In the lecture we defined the type set of typed sets (slide 179), using the conservative extension schema for type definitions (slide 177).

Based on the types of core HOL and nat, define the type $mset$ of typed multisets in the same style.

Hint: Multisets are sets where the same element can appear more than once.

c) (Prepare!) Based on the types of core HOL and nat, define the type $list$ of typed lists.

d) Define both types in Isabelle/HOL using `typedef` and define additional helpful functions on the types.

e) Define simple generic properties of the newly defined functions and prove them (e.g. the empty list does not contain any elements, formulated on the two constants `empty` and `contains`).

Handling (type-)definitions: Functions on newly defined types are likely defined as `definitions` and involve applications of `Rep_t` and `Abs_t`. Isabelle/HOL does **not** automatically use definitions for simplification. As definitions define equalities, however, you can use the proof command `apply (subst myfunction_def)` to unfold them. Using the same command you can unfold the definition of the type (`t_def`) and the two axioms `Rep_t_inverse` and `Abs_t_inverse`.