Prof. Dr. A. Poetzsch-Heffter
M.Sc. Peter Zeller
Dipl.-Inf. C. Feller

University of Kaiserslautern
Department of Computer Science
Software Technology Group

Exercise Sheet 3: Specification and Verification with Higher-Order Logic (Summer Term 2014)

Please prepare the marked tasks for the exercise on Wednesday, May 21, 2014
Submit your solutions to the hand-in tasks before Wednesday, May 28, 2014

Exercise 1 Methods and Rules in Isabelle/HOL

a) (Prepare!) Apply the rule

$$[\![(?a, ?b) \in ?r^*; \bigwedge x.\ ?P\ x\ x; \bigwedge x\ y\ z.\ [\![(x, y) \in ?r^*;\ ?P\ x\ y;\ (y, z) \in ?r]\!] \Longrightarrow ?P\ x\ z]\!] \Longrightarrow ?P\ ?a\ ?b$$

with the method `erule` to the following subgoal by hand (i.e. on paper):

$$(i, j) \in s^* \Longrightarrow 0 \le (dist\ i\ j)$$

Hint: Don't be distracted by unknown function names; you don't have to know anything about their meaning. Just apply the rule syntactically.

b) In this exercise we want to practice the use of different methods (like `rule`, `erule` or `frule`) to prove properties in propositional and predicate logic. You should only use the methods `rule`, `erule`, `frule`, `drule`, the respective `_tac` methods and `assumption`. Do **not** use other methods like `simp`. You should only use the rules of the first exercise sheet, together with the following additional rules: `conjE`, `impE`, `iffI`, `iffE`, and `classical`.

*Hint: You can write "**thm** `classical`" in Isabelle/HOL to see the concrete definition of the rule.*

Prove the following theorems:

1. $A \wedge B \longrightarrow B \wedge A$
2. $(A \vee A) = (A \wedge A)$
3. $A \longrightarrow B \longrightarrow A$
4. $(A \longrightarrow (B \longrightarrow C)) \longrightarrow ((A \longrightarrow B) \longrightarrow (A \longrightarrow C))$
5. $(\neg A \longrightarrow \neg B) \longrightarrow (B \longrightarrow A)$
6. $\neg\neg A \longrightarrow A$
7. $A \vee \neg A$
8. $(\exists x.\ \forall y.\ P\ x\ y) \longrightarrow (\forall y.\ \exists x.\ P\ x\ y)$
9. $((\forall x.\ P\ x) \wedge (\forall x.\ Q\ x)) = (\forall x.\ (P\ x \wedge Q\ x))$
10. $((\exists x.\ P\ x) \vee (\exists x.\ Q\ x)) = (\exists x.\ (P\ x \vee Q\ x))$
11. $(\neg(\forall x.\ P\ x)) = (\exists x.\ \neg P\ x)$

Exercise 2 Rewriting and Simplification

In this exercise we want to do proofs by just rewriting. Please download the file `Sheet3_Rewrite.thy` from the website. You are only allowed to use the lemmas defined in this file and you are only allowed to use them with the `subst` method. As the only exception you are allowed to use `(rule TrueI)` to finish a subgoal.

Prove the following theorems:

a) `length [a] = 1`

b) `(A ∧ B ∧ C) = (B ∧ A ∧ C)`

c) `(a * (Suc (Suc (Suc (Suc 0))))) div (Suc (Suc (Suc (Suc 0)))) = a`

d) `(Suc x) * (Suc x) = Suc (x*x + 2*x)`

Exercise 3 Prime numbers (Hand in!)

Please download the file `Sheet3_Primes.thy` from the website. This file contains an unfinished proof for a theorem, which states that there is an infinite number of primes. Your task is to finish this proof by formalizing the following informal proof:

Lemma: For every number greater or equal to 2 there exists some prime which divides the number.

Proof: By induction over n.

Induction Hypothesis: For every number k between 2 and $n-1$ there exists some prime which divides k.

Induction Step (show the statement for n using the Induction Hypothesis): If n is prime the step is trivial. If n is not prime, then there exists a number k with $2 \leq k < n$ which divides n (by the definition of prime number). From the induction hypothesis we get a prime number k' which divides k. By transitivity of "divides" k' also divides n. So with k' we have a prime number dividing n.

Theorem: There are infinitely many primes.

Proof: Suppose for the sake of contradiction that the set S of primes is finite. Then ΠS is well defined. Let $P = 1 + \Pi S$. Then there exists some prime q which divides P. Because $q \in S$, q also divides ΠS. If a number divides two numbers n and m, then it also divides the difference $m - n$. Therefore q divides the difference $P - \Pi S$, which is 1. Only 1 divides 1, so $q = 1$, but it also is a prime number. This is a contradiction and the proof is complete.

Hints:

- ΠS denotes the product of all numbers in the set S, for example $\Pi\{2, 3, 5\} = 2 \cdot 3 \cdot 5 = 30$.
- In Isabelle `n dvd m` denotes the fact that `n` divides `m`, for example `3 dvd 12`.
- The induction rule used for the first lemma is called `full_nat_induct`. The difference to the usual induction over natural numbers is, that one can assume, that the hypothesis holds for all numbers smaller than n, whereas in the usual induction rule it can only be assumed for the direct predecessor.
- The following theorems might be helpful: `dvd_diff_nat`, `dvd_setprod`, `dvd_trans`.
- `Collect P` is the set of all elements for which `P` holds true.