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 5: Specification and Verification with Higher-Order Logic (Summer Term 2014)

Please prepare the marked tasks for the exercise on Wednesday, June 4, 2014

## Exercise 1 Inductive sets

Consider the following inductive definition of provable formulas:

```
datatype form =
    Var string
  | Imp form form
  | Neg form

inductive provable :: "form set ⇒ form ⇒ bool" (infixr "⊢" 50) where
  p_assumpt: "p∈Γ ⟹ Γ ⊢ p"
| p_impI: "⟦Γ ∪ {p} ⊢ q⟧ ⟹ Γ ⊢ Imp p q"
| p_mp: "⟦Γ ⊢ Imp p q; Γ ⊢ p⟧ ⟹ Γ ⊢ q"
```

a) (Prepare!) Write down (on paper) the function $F_{provable}$ used in the normalized form of the inductive definition. Have a look at the $F_{even}$ function from the lecture slides for an example.

b) (Prepare!) Explain why the set of all sequents is a fixed point of $F_{provable}$.

c) (Prepare!) Explain why the set of all sequents is not the least fixed point of $F_{provable}$.

d) Download the file `Sheet5_inductive.thy` from the website. This file contains a similar inductive definition with some additional formulas.
Compare your function definition from a) with the theorem `provable_def`.
*Hint:* Use the command **`thm`** `provable_def` to see the definition of the theorem.

e) Prove that `{} ⊢ Imp A (Imp B A)`

f) Prove that `{} ⊢ Imp (Neg(Neg A)) A`

g) Prove that the defined calculus is sound.
*Hint:* Use the induction rule `provable.induct`.

h) Prove that `¬ ({} ⊢ Var ''x'')`

i) Prove the following weakening rule: `⟦A ⊢ P; A ⊆ B⟧ ⟹ B ⊢ P`

j) (optional) A set of formulas $S$ is called inconsistent if there exists a formula $p$, such that $S \vdash p$ and $S \vdash \neg p$. Show that $S \vdash F$ if and only if $S \cup \{Neg\ F\}$ is inconsistent.

k) (optional) Download the file `Sheet5_inductive_completeness.thy` from the website and finish the proofs marked with `sorry`. With this you will prove that the given calculus is complete and thus we know exactly what the least fix point of the inductive definition is.