Dr. Matthias Heizmann
Tanja Schindler
Dominik Klumpp

Hand in until 10:00 on May 6, 2019
Discussion: May 6, 2019

# Tutorial for Program Verification

## Exercise Sheet 1

Solutions to the exercises can be submitted via one of the postboxes in building 51. Alternatively, you may submit your solution via email to the address that is obtained by replacing NoSpam with Dominik's family name in NoSpam@informatik.uni-freiburg.de.

**Exercise 1: Natural Deduction Proofs** 4 Points

Prove the following implications in the Natural Deduction proof system $\mathcal{N}_{\mathsf{PL}}$. That is, for an implication $\{F_1, \dots, F_n\} \vDash F$, use the rules of $\mathcal{N}_{\mathsf{PL}}$ to build a derivation that shows this implication holds.

(a) $\{A \to B\} \vDash \neg B \to \neg A$

(b) $\{A \to (B \to C)\} \vDash A \land B \to C$

**Exercise 2: Fool proof system** 2 Points

Let us consider the "fool proof system" which is an extension of $\mathcal{N}_{\mathsf{PL}}$ by the following two rules.

$$(\mathsf{FOOL}_i)\frac{\Gamma \vDash F_1 \lor F_2}{\Gamma \vDash F_i}\; i \in \{1, 2\}$$

Construct a derivation where the root node is labelled by $\{\mathbf{true}\} \vDash \mathbf{false}$. (Which demonstrates that this proof system is useless because we can derive implications that do not hold.)

---

In this course, we follow a new paradigm where a small amount of topics is not presented in the lecture. A special kind of (rather simple) exercises should help participants to get familiar with these topics. These exercises (and if neccessary also the topics) are discussed before the next lecture starts.

This week, we would like you to have a look on the lecture slides on the semantics of first-order logic.

**Exercise 3: Vocabularies** 1 Point

(a) State a vocabulary such that the number of $FOL$ terms is finite but not zero.

(b) State a vocabulary such that the number of $FOL$ terms is infinite.

(c) How many $FOL$ formulas do we have if the vocabulary is $\mathcal{V} = (\emptyset, \emptyset, \emptyset, \emptyset)$?

**Exercise 4: Models for Quantifier-free Formulas** 3 Points

Consider the vocabulary $\mathcal{V} = (\{x, y, z\}, \emptyset, \{f, g\}, \{p\})$ and the following formula.

$$\varphi: \; p(f(x, y), z) \rightarrow p(y, g(z, x))$$

(a) Consider the model $\mathcal{M} = (\mathcal{D}, \mathcal{I})$, where $\mathcal{D} = \mathbb{Z}$ and $\mathcal{I}$ maps $f$ to the addition function ("+"), $g$ to the subtraction function ("-"), and $p$ to the strictly smaller relation ("<"). Consider the variable assignment $\rho$ such that $\rho(x) = 13$, $\rho(y) = 42$, and $\rho(z) = 1$.

(i) What is $[\![\varphi]\!]_{\mathcal{M},\rho}$? Show also intermediate results for at least three different subterms.

(ii) Let us define $\rho'$ as $\rho \lhd \{x \mapsto 55\}$ What is $[\![\varphi]\!]_{\mathcal{M},\rho'}$?

(iii) State an interpretation function $\mathcal{I}'$ such that for the model $\mathcal{M}' = (\mathcal{D}, \mathcal{I}')$ the truth value $[\![\varphi]\!]_{\mathcal{M}',\rho}$ is different from the truth value $[\![\varphi]\!]_{\mathcal{M},\rho}$.

(iv) State a formula $\varphi'$ that also contains the symbols $x, y, z, f, g, p$ such that the truth value $[\![\varphi']\!]_{\mathcal{M},\rho}$ is different from the truth value $[\![\varphi]\!]_{\mathcal{M},\rho}$.

(b) Consider the interpretation domain $\mathcal{D}_{\mathsf{RPS}} = \{\mathsf{Rock}, \mathsf{Paper}, \mathsf{Scissors}\}$, the function $\mathsf{fst} : \mathcal{D}_{\mathsf{RPS}} \times \mathcal{D}_{\mathsf{RPS}} \rightarrow \mathcal{D}_{\mathsf{RPS}}$ that is defined as $\mathsf{fst}(x, y) = x$ for all $x, y \in \mathcal{D}_{\mathsf{RPS}}$ and the binary relation $R_{\mathsf{win}} \subseteq \mathcal{D}_{\mathsf{RPS}} \times \mathcal{D}_{\mathsf{RPS}}$ which is defined as follows.

$$R_{\mathsf{win}} = \{(\mathsf{Rock}, \mathsf{Scissors}), (\mathsf{Scissors}, \mathsf{Paper}), (\mathsf{Paper}, \mathsf{Rock})\}$$

Let $\mathcal{M} = (\mathcal{D}_{\mathsf{RPS}}, \mathcal{I})$ be the model whose interpretation function $\mathcal{I}$ maps $f$ to $\mathsf{fst}$, $g$ to $\mathsf{fst}$, and $p$ to $R_{\mathsf{win}}$. Let $\rho$ be the variable assignment that is defined as follows $\rho(x) = \mathsf{Rock}$, $\rho(y) = \mathsf{Paper}$, $\rho(z) = \mathsf{Scissors}$.

(i) What is $[\![\varphi]\!]_{\mathcal{M},\rho}$? Show also intermediate results for at least three different subterms.

(ii) State a formula $\varphi'$ that also contains the symbols $x, y, z, f, g, p$ such that the truth value $[\![\varphi']\!]_{\mathcal{M},\rho}$ is different from the truth value $[\![\varphi]\!]_{\mathcal{M},\rho}$.

**Exercise 5: Models for Quantified Formulas** 2 Points

Consider the vocabulary $\mathcal{V} = (\{x, y, z\}, \{c\}, \{f\}, \{p\})$ and the following formula.

$$\varphi: \; \forall x. \exists y. p(f(c, y), x)$$

(a) Consider the model $\mathcal{M} = (\mathcal{D}, \mathcal{I})$, where $\mathcal{D} = \mathbb{Z}$ and $\mathcal{I}$ maps $c$ to the integer number 2, $f$ to the multiplication function ("·"), and $p$ to the equality relation ("="). Let $\rho$ be the variable assignment that is defined as $\rho(x) = 42$, $\rho(y) = 17$ and $\rho(z) = 23$. What is $[\![\varphi]\!]_{\mathcal{M},\rho}$? Justify your answer.

(b) Find two models $\mathcal{M}_i = (\mathcal{D}_i, \mathcal{I}_i)$ such that $[\![\varphi]\!]_{\mathcal{M}_i,\rho_i}$ is different from $[\![\varphi]\!]_{\mathcal{M},\rho}$ for $i \in \{1, 2\}$. The interpretation domain $\mathcal{D}_1$ should also be $\mathbb{Z}$, the interpretation domain $\mathcal{D}_2$ should be some different set.

**Exercise 6: FOL Satisfiability** 2 Points

For each of the following formulas $\varphi$ give a model $\mathcal{M}_i$ with $[\![\varphi]\!]_{\mathcal{M}_i,\rho} =$ **true**. You do not have to give a variable assignment $\rho$ because for each of the formulas the evaluation to a truth value is independent of the variable assignment.

(a) $\varphi_1 : equals(add(2, 2), 5)$

(b) $\varphi_2 : \forall x.\ p(x, x)$

(c) $\varphi_3 : \exists y.\ \forall x.\ p(x, y)$

(d) $\varphi_4 : \forall x.\ (p(x, f(x)) \land \neg p(f(x), x))$