Dr. Matthias Heizmann
Dominik Klumpp

Hand in until 10:00 on May 25, 2020
Discussion: May 25, 2020

# Tutorial for Program Verification
## Exercise Sheet 3

In this exercise we practice conducting proofs in the Natural Deduction proof system for propositional logic, $\mathcal{N}_{\mathsf{PL}}$. We then continue with First-Order Logic.

Submit your solution by uploading it as PDF in ILIAS.

**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 $\{F_1, \ldots, F_n\} \models F$, use the rules of $\mathcal{N}_{\mathsf{PL}}$ to build a derivation that shows this implication holds.

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

(b) $\{A \to (B \to C)\} \models A \wedge B \to C$

**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.

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

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

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

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

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

(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 or subformulas.

   (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 $\mathsf{fst} : \mathcal{D}_{\mathsf{RPS}} \times \mathcal{D}_{\mathsf{RPS}} \to \mathcal{D}_{\mathsf{RPS}}$ 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 or subformulas.

(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 4: 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 ("$\cdot$"), 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 $\mathcal{M}_i = (\mathcal{D}_i, \mathcal{I}_i)$ and two variable assignments $\rho_i$ 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 5: FOL Satisfiability** 2 Points

For each of the following formulas $\varphi$ give a model $\mathcal{M}_i$ with $[\![\varphi]\!]_{\mathcal{M}_i,\rho} = \textbf{true}$. 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) $\varphi_4 : \forall x.\ (p(x, f(x)) \land \neg p(f(x), x))$

**Exercise 6: Free Variables and Substitutions** 2 Points

Consider the formulas $\varphi_i$ and the substitutions $\sigma_i$ for $i \in \{1, 2\}$ displayed below.

(i) Compute the set of free variables freevars$(\varphi_i)$ for $i \in \{1, 2\}$.

(ii) Compute the result $\varphi_i \sigma_i$ for $i \in \{1, 2\}$.

$\varphi_1 : \forall x'.\ (p(x, x') \land \exists x.\ p(x', x))$ and $\sigma_1 : \{x \mapsto a\}$
$\varphi_2 : \forall y.\ p(x, y, z)$ and $\sigma_2 : \{x \mapsto f(z), z \mapsto f(y)\}$