Introduction to Logic (Spring 2020)

Assignment 9

Monday 11th May 2020

Instructions This sheet contains two kinds of assignments: exercises and homework. The first are not mandatory and are meant for practising during the exercise class or by yourself. Tutors will be available during the exercise class to help with the assignment. Homework assignments are mandatory, and the combined grade of the homework makes 30% of the final grade. The grade for the homework on this sheet corresponds to the number of points obtained + 1. Maximally 9 points can be obtained.

Handing in your answers Submit your solution through **Blackboard** as a single PDF file named `hw9sN.pdf`, where N is your student number. The document has to be created using LaTeX (or variants like XeLaTeX). A template is available on the website of the course and on Blackboard. Please **use the proper logic connectives and proof rules** as they are shown in the template. If you do not have a working LaTeX installation, then you can use Overleaf (`https://www.overleaf.com/`). Make sure that your **name, student number and studies** are **clearly written on the document**. All students have to prepare and submit their own solution. Only submit the 2 exercise(s) marked as **Homework**. Answers have to be provided in **Dutch or English**. Submissions that fail to meet these requirements are not considered.

Deadline The homework must be uploaded before **Friday 22nd May 2020 2:30pm**.

Learning Objectives After completing this assignment, you should be able to **use first-order logic with equality** in formalisations and **prove statements in $\mathbf{ND}_1^=$**. Moreover, you should be able to **use uniqueness quantification**.

Exercise 1

a) Formalise the sentence

> "Pavel owes money to everyone but himself"

as a formula φ in first-order logic with equality. You need one constant p for "Pavel" and one binary predicate symbol O for "owes to".

b) Derive for your formula φ the following sequent in $\mathbf{ND}_1^=$ using a Fitch-style proof.

$$\varphi \vdash \neg O(p, p)$$

Exercise 2

Let $\mathcal{L}$ be a signature with a unary predicate symbol P. We define P_1 to be the formula

$$P_1 \quad = \quad \forall y. \forall z. P(y) \wedge P(z) \rightarrow y \doteq z,$$

which expresses that there can be maximally one object that fulfils P. Prove the following logical equivalence in $\mathbf{ND}_1^=$:

$$\vdash (\exists! x. P(x)) \leftrightarrow ((\exists x. P(x)) \wedge P_1)$$

To approach the proof of this formula, do both implications in separate proofs and refer to them in the proof of the logical equivalence. Furthermore, use the derived rules for the uniqueness quantifier from lemma 9.11 in the lecture notes.

Exercise 3 *Graph Reachability*

We have seen that compactness prevents us from giving a *formula* that expresses reachability in graphs. In this exercise, we will see that reachability can be expressed by appropriately defining a *predicate*. Let $\mathcal{L}$ be the signature $(\{E, R\}, \{n_1, \ldots, n_4\}, \mathrm{ar})$ with $\mathrm{ar}(E) = \mathrm{ar}(R) = 2$ and $\mathrm{ar}(n_k) = 0$ for $k = 1, \ldots 4$. The intention is that $E(x, y)$ holds if there is an edge between x and y in a given graph, and $R(x, y)$ holds if the node y is reachable from x. We will use the constants n_k later to model the nodes of a concrete graph.

Reachability R is the reflexive and transitive closure of the edge relation E. In other words, each node x must be related to itself via E (reflexivity), and if there is an edge from x to some z and y is reachable from z, then y is also reachable from x (transitivity).

a) Give two formulas φ_r and φ_t with free variables x and y that express, respectively, reflexivity and transitivity. That is to say, that the formula φ_R given by

$$\forall x. \forall y. R(x, y) \leftrightarrow \varphi_r \vee \varphi_t$$

expresses that R is the reachability relation in the graph with edges E.

b) Let $\varphi_{R,1}$, $\varphi_{R,2}$ and $\varphi_{R,3}$ be given by

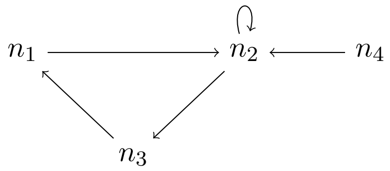
$$\begin{aligned}\varphi_{R,1} &= \forall x.\, \forall y.\, R(x,y) \to \varphi_r \vee \varphi_t\\ \varphi_{R,2} &= \forall x.\, \forall y.\, \varphi_r \to R(x,y)\\ \varphi_{R,3} &= \forall x.\, \forall y.\, \varphi_t \to R(x,y)\end{aligned}$$

Derive the following sequent in $\mathbf{ND}_1^=$ using Fitch-style.

$$\varphi_{R,1}, \varphi_{R,2}, \varphi_{R,3} \vdash \varphi_R$$

Note that the proof merely uses the rules for quantifiers and propositional connectives, not those for equality.

c) Consider the following graph G.



Give formulas $\varphi_{E,1}, \ldots, \varphi_{E,5}$ that describe the edge of G.

d) Give a proof in $\mathbf{ND}_1^=$ using Fitch-style of $\varphi_R, \varphi_{E,1}, \ldots, \varphi_{E,5} \vdash R(n_4, n_3)$. Use b) to simplify the task.

Exercise 4

A *group* G is given by a binary map $\dot{+}\colon G \times G \to G$ and an element $\dot{0}$ of G, such that

1. for all x in G, $x \dot{+} \dot{0} = \dot{0} \dot{+} x = x$,
2. for all x, y, z in G, $x \dot{+} (y \dot{+} z) = (x \dot{+} y) \dot{+} z$, and
3. for every x in G there is a y in G, such that $x \dot{+} y = \dot{0}$ and $y \dot{+} x = \dot{0}$.

The equations 1 - 3 are called the *group axioms*. Groups appear everywhere in computer science and mathematics, with very popular applications in cryptography. The goal of this exercise is to formally reason about groups in first-order logic with equality.

Let $\mathcal{L}$ be the signature with function symbols $\dot{+}$ and $\dot{0}$ of arity 2 and 0, respectively. Let us write, as above, the symbol $\dot{+}$ in infix notation, that is, we write $s \dot{+} t$ instead of $\dot{+}(s,t)$ for terms s and t. We define $\mathcal{L}^=$-formulas $\varphi_{1,l}$ and $\varphi_{1,r}$ by

$$\varphi_{1,l} = \forall x.\, \dot{0} \dot{+} x \doteq x \quad \text{and} \quad \varphi_{1,r} = \forall x.\, x \dot{+} \dot{0} \doteq x$$

that formalise together the first group axiom.

a) Give $\mathcal{L}^{=}$-formulas φ_2 and φ_3 that formalise the axioms 2 and 3 from above.

b) Give a formula φ_u that expresses the uniqueness of y in the third group axiom. The element y is called the *inverse* of x.

c) Prove in $\mathbf{ND}_1^{=}$ that the inverse y of x in the third axiom is unique, that is, derive $\vdash \varphi_u$ for your formula in $\mathbf{ND}_1^{=}$. Use Fitch-style as usual.

Homework 1

______/4 p.

Let P be a unary predicate symbol and b a constant. Prove the sequent

$$P(b) \vdash \forall x. (x \doteq b \to P(x))$$

in $\mathbf{ND}_1^{=}$ using Fitch-style.

Homework 2

______/5 p.

Let $\mathcal{L}$ be a signature with binary function symbols $\dotplus$ and $\star$, and one binary predicate symbol $\mid$. We write these symbols in infix notation: $s \dotplus t$, $s \star t$ and $s \mid t$. The intention is that $\dotplus$ represents addition and $\star$ multiplication of natural numbers, while $m \mid n$ shall say that m divides n.

a) Give an $\mathcal{L}^{=}$-formula φ with free variables m and n, such that $\varphi \leftrightarrow n \mid m$ correctly axiomatises the divisibility relation.

b) Give an $\mathcal{L}^{=}$-formula ψ that expresses that every natural number m can divided by any number n with remainder: $m = nk + r$ for unique k and r, where n does not divide r.

Typesetting remark: $\dotplus$ can be typeset by `\dotplus`, $\star$ by `\star`, and $\mid$ by `\mid`.