UNIVERSITY OF OSLO

Faculty of Mathematics and Natural Sciences

Examination in MAT-INF3600 — Mathematical logic.

Day of examination: Monday, December 7, 2009.

Examination hours: 9.00 – 12.00.

This problem set consists of 4 pages.

Appendices: None.

Permitted aids: None.

Please make sure that your copy of the problem set is complete before you attempt to answer anything.

Problem 1

> **Theorem (A).** Let $\mathcal{L}$ be a first-order language and let ϕ be an $\mathcal{L}$-formula such that the term t is substitutable for the variable x in ϕ. We have
>
> $$T \vdash \phi \quad \Rightarrow \quad T \vdash \phi_t^x$$
>
> for any $\mathcal{L}$-theory T.

a) Prove Theorem **(A)** by constructing a derivation of ϕ_t^x from a derivation of ϕ. Name the (logical) axioms and the inference rules involved in the derivation.

Let $\circ$ be a binary function symbol, and let a, b and e be constant symbols. Let $\mathcal{L}_{BS}$ be the first-order language $\{a, b, e, \circ\}$, and let B be the $\mathcal{L}_{BS}$-theory consisting of the following non-logical axioms:

B1 $\forall x\, [\, x = e \circ x\,]$

B2 $\forall x\, [\, x = x \circ e\,]$

B3 $\forall xyz\, [\, x \circ (y \circ z) = (x \circ y) \circ z\,]$

B4 $\forall x\, [\, e \neq a \circ x \ \wedge \ e \neq b \circ x\,]$

B5 $\forall xy\, [\, x \neq y \ \rightarrow \ (a \circ x \neq a \circ y \wedge b \circ x \neq b \circ y)\,]$

(Continued on page 2.)

Theorem (B). $B \vdash \forall x[e \circ x = x \circ e]$.

b) Prove Theorem **(B)** by giving a B-derivation of $\forall x[e \circ x = x \circ e]$. Name the logical and the non-logical axioms involved in the derivation. You may refer to Theorem **(A)**. Hint: You will need the logical axiom

$$x_1 = y_1 \ \wedge \ x_2 = y_2 \ \rightarrow \ (x_1 = x_2 \ \rightarrow \ y_1 = y_2) \qquad \text{(E3)}$$

c) Prove that

$$B \vdash \forall x y_1 \ldots y_n \, [\, (y_n \circ (y_{n-1} \circ \ldots (y_1 \circ e) \ldots)) \circ x \ = \ (y_n \circ (y_{n-1} \circ \ldots (y_1 \circ (x \circ e)) \ldots)) \,]$$

for any $n \geq 0$. Hints: Use induction on n. The case $n = 0$ follows from Theorem **(B)**.

We define the *prime terms* of the language $\mathcal{L}_{BS}$ by

- e is a prime term
- $(a \circ t)$ is a prime term if t is a prime term
- $(b \circ t)$ is a prime term if t is a prime term.

Hence, e.g., $(a \circ (b \circ (b \circ e)))$ is a prime term whereas $((a \circ b) \circ (e \circ b))$ is not.

Theorem (C). For any variable-free $\mathcal{L}_{BS}$-term t there exists a prime term p such that $B \vdash t = p$.

d) Prove Theorem **(C)**.

Problem 2

We will use some notation from Levis & Papadimitriou's textbook: Σ^* denotes the set of all strings over the alphabet Σ, and $|\alpha|$ denotes the length of the string α. We use ϵ to denote the empty string, and $\alpha \cdot \beta$ denotes the concatenation of the strings α and β. Occasionally, we will write $\alpha\beta$ in place of $\alpha \cdot \beta$. When convenient, we may also drop parenthesis and write e.g. $\alpha\beta\gamma$ in place of $(\alpha\beta)\gamma$.

We will now define the $\mathcal{L}_{BS}$-structure $\mathfrak{B}$. The universe of $\mathfrak{B}$ is the set $\{0, 1\}^*$, that is, the set of all bit sequences: $\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, \ldots$. Furthermore,

- $e^{\mathfrak{B}} = \epsilon$ (the empty string)
- $a^{\mathfrak{B}} = 0$ (the string where the one and only bit is 0)
- $b^{\mathfrak{B}} = 1$ (the string where the one and only bit is 1)

(Continued on page 3.)

and $\circ^{\mathfrak{B}} = \cdot$ (the concatenation operator). Hence, we have e.g. that $\epsilon \circ^{\mathfrak{B}} 100 = 100 \circ^{\mathfrak{B}} \epsilon = 100$ and $101 \circ 1001 = 1011001$. It is obvious that $\mathfrak{B}$ is a model for the theory B, that is, $\mathfrak{B} \models B$.

a) Is B a consistent theory? Give a short answer, and justify the answer by referring to a theorem in Leary's textbook.

b) Do we have $B \vdash a \neq b$? Do we have $B \vdash a = b$? Justify your answers.

We say that α is a substring of β iff there exists γ_1 and γ_2 such that $\gamma_1\alpha\gamma_2 = \beta$.

c) Give an $\mathcal{L}_{BS}$-formula θ such that

$$\mathfrak{B} \models \theta[s[y|\alpha][x|\beta]] \Leftrightarrow \alpha \text{ is a substring of } \beta \ .$$

Give an $\mathcal{L}_{BS}$-formula η such that

$$\mathfrak{B} \models \eta[s[x|\alpha]] \quad \Leftrightarrow \quad \alpha \in \{0\}^* \ .$$

d) Give an $\mathcal{L}_{BS}$-formula *Add* such that $\mathfrak{B} \models \mathit{Add}[s[x|\alpha]]$ holds if and only if

- α is of the form $\alpha \equiv 1\gamma_1 1\gamma_2 1\gamma_3 1$ where $\gamma_1, \gamma_2, \gamma_3 \in \{0\}^*$, and
- $|\gamma_1| + |\gamma_2| = |\gamma_3|$.

(Hint: Use the formulas from Problem **b**.)

Theorem (D). There exist $\mathcal{L}_{BS}$-formulas *Mul* and *Exp* such that

- $\mathfrak{B} \models \mathit{Mul}[s[x|\alpha]]$ if and only if
  - α is of the form $\alpha \equiv 1\gamma_1 1\gamma_2 1\gamma_3 1$ where $\gamma_1, \gamma_2, \gamma_3 \in \{0\}^*$, and
  - $|\gamma_1| \times |\gamma_2| = |\gamma_3|$
- $\mathfrak{B} \models \mathit{Exp}[s[x|\alpha]]$ if and only if
  - α is of the form $\alpha \equiv 1\gamma_1 1\gamma_2 1\gamma_3 1$ where $\gamma_1, \gamma_2, \gamma_3 \in \{0\}^*$, and
  - $|\gamma_1|^{|\gamma_2|} = |\gamma_3|$.

The proof of Theorem **(D)** is involved, and you are *not* asked to prove this theorem.

Let $\mathcal{L}_{NT}$ be the first-order language of number theory, that is, $\mathcal{L}_{NT} = \{0, S, +, \times, E, <\}$, and let $\mathfrak{N}$ be the standard $\mathcal{L}_{NT}$-structure. Both $\mathcal{L}_{NT}$ and $\mathfrak{N}$ are known from Leary's textbook. Furthermore, let Σ be an alphabet containing all the symbols of the first-order languages $\mathcal{L}_{NT}$ and $\mathcal{L}_{BS}$.

(Continued on page 4.)

e) Argue that there exists a recursive (Turing computable) function $f : \Sigma^* \to \Sigma^*$ such that for any $\mathcal{L}_{NT}$-sentence ϕ

$$\mathfrak{N} \models \phi \quad \Leftrightarrow \quad \mathfrak{B} \models f(\phi) \; .$$

You may refer to Theorem **(D)**.

Let

$$Th(\mathfrak{B}) \;=\; \{\, \phi \mid \phi \text{ is an } \mathcal{L}_{BS}\text{-sentence and } \mathfrak{B} \models \phi \,\}$$

and

$$Pr(B) \;=\; \{\, \phi \mid \phi \text{ is an } \mathcal{L}_{BS}\text{-sentence and } B \vdash \phi \,\} \; .$$

f) Is the set $Th(\mathfrak{B})$ recursive (decidable)? Is the set $Th(\mathfrak{B})$ recursively enumerable (semi-decidable)? Is the set $Pr(B)$ recursively enumerable (semi-decidable)? Justify your answers.

g) Is the theory $B \cup \{a \neq b\}$ complete or incomplete? Justify your answer.

END