UPPSALA UNIVERSITET
Matematiska institutionen
Erik Palmgren

EXERCISES 1
APPLIED LOGIC, Fall-09
2009-09-04

Predicate logic, its semantics and decidability problems

1. Some review exercises in predicate logic to do (if necessary):

   2.1: 1,3

   2.2: 3,4

   2.3: 2,3,4,7,13

   2.4: 2,6,11,12

   of the textbook (Huth and Ryan 2004).

2. * Do some of the prepared exercises in the ProofWeb system. (Follow the link on the course web page for instructions.)

3. Decide whether the following *instances* of Post's correspondence problem (PCP) are solvable. Provide a solution, or give a proof that no solution is possible!

   (a) $(11, 0),\ (10, 1)$
   (b) $(000, 0),\ (0, 0000)$
   (c) $(00, 10),\ (01, 0), (0, 110000)$

4. Solve PCP for the sequence of pairs

$$(001, 0),\ (01, 011),\ (01, 101),\ (10, 001).$$

   (Hint (?): It is not so easy if one gets started in the wrong way. One solution gives a binary string of total length 154. Use a computer program if it gets too tedious ...)

5. (Definability) Let $\mathcal{M}$ be a model for the language L and let $A = |\mathcal{M}|$ be its universe. A subset $S \subseteq A^n$ is *(first-order) definable* in $\mathcal{M}$ if there is an L-formula φ with free variables among $x_1, \ldots, x_n$ such that

$$S = \{(a_1, \ldots, a_n) \in A^n : \mathcal{M} \models_\ell \varphi \text{ and } \ell(x_1) = a_1, \ldots, \ell(x_n) = a_n\}$$

A relation $R \subseteq A^n$ is *definable in* $\mathcal{M}$ if the corresponding subset R is definable. A function $f : A^n \to A$ is *definable in* $\mathcal{M}$ if its graph

$$\operatorname{graph} f = \{(a_1, \ldots, a_n, b) \in A^{n+1} : f(a_1, \ldots, a_n) = b\}$$

is a definable subset in $\mathcal{M}$.

Show that the subsets, relations or functions in (a) – (h) below are definable in $\mathcal{N} = \langle \mathbb{N}; +, \cdot, 0, 1\rangle$ using as simple formulas as seems possible.

For instance the set of even numbers is defined by

$$\{m \in \mathbb{N} : \mathcal{N} \models_\ell (\exists x)\ x + x = y \text{ and } \ell(y) = m\}$$

This also shows that the predicate x *is even* is definable. The function $f(x) = x^2$ is defined by

$$\{(m, n) \in \mathbb{N}^2 : \mathcal{N} \models_\ell x \cdot x = y \text{ and } \ell(x) = m, \ell(y) = n\}.$$

(a) x is odd

(b) $y = x(x + 1)/2$

(c) $x \leq y$

(d) x divides y

(e) x is the sum of two prime numbers

(f) $z = \max(x, y)$

(g) ** $y = x!$. [Look up and use Gödel's technique of the β-function and the Chinese remainder theorem.]

(h) $y = 2^{2^{2^{2^{2}}}}$

▷ Let L be a first-order language with finitely many symbols. A structure $\mathcal{M}$ for L is called *decidable,* if there is an algorithm which for every closed first order formula φ in the language L decides whether $\mathcal{M} \models \varphi$ holds or not. A well-known example of an *undecidable* structure is the structure of natural numbers $\mathcal{N} = \langle \mathbb{N}, +, \cdot, 0, 1\rangle$.

6. (Definability and decidability) Recall that in automata theory one studies languages as subsets of strings over a fixed alfabet. Let $\Sigma = \{a, b\}$ be an alfabet, and let Σ^* be the set of finite strings. Thus

$$\Sigma^* = \{\epsilon, a, b, aa, ab, ba, bb, aaa, aab, \ldots\}$$

Here ϵ is the empty string. Let & denote concatenation of strings, so $baba\&bba = bababba$. We may now regard $\langle \Sigma^*;\ \& \rangle$ as a first-order structure with concatenation as the only operation. Find elementary propositions (formulas) over $\langle \Sigma^*;\ \& \rangle$ that definies the following properties (note that $=$ may be used)

(a) x is a substring of y

(b) x is an empty string (you may not mention ϵ)

(c) x is a string of length 1 (you may not mention 0 or 1) (Hint: use (a) and (b). How many substrings can such a string have?)

(d) x is a string of length 4.

Consider now an extended structure $\langle \Sigma^*;\ \&, *, a, b, \epsilon \rangle$ where a, b, ϵ are constants (so they may be mentioned in elementary propositions) and moreover there is a "string duplicator" $*$ that satisfies the following

$$\begin{array}{rcll} u * \epsilon & = & \epsilon & \text{(erase)} \\ u * (a\&v) & = & u * v & \text{(take a pause)} \\ u * (b\&v) & = & (u * v)\&u & \text{(make a copy).} \end{array}$$

Thus $ab * bab = abab$ and $ab * aa = \epsilon$.

(e) Prove that the structure $\langle \Sigma;\ \&, *, a, b, \epsilon \rangle$ is undecidable, by showing that *if* it was decidable, then we could decide $\langle \mathbb{N}, +, \cdot, 0, 1 \rangle$ as well, contradicting a well-known theorem.

(f)** If we remove the duplication operation from the structure in (e), does it become decidable? I.e. is the structure $\langle \Sigma;\ \&, a, b, \epsilon \rangle$ decidable?

———