Universität Koblenz-Landau

FB 4 Informatik

Prof. Dr. Viorica Sofronie-Stokkermans **November 22, 2016**

Exercises for "Formal Specification and Verification"
Exercise sheet 3

Exercise 3.1:
Let $\Sigma = (\Omega, \Pi)$ be a signature, where $\Omega = \{f/2,\ g/1,\ a/0,\ b/0\}$ and $\Pi = \{p/2\}$; let X be the set of variables $\{x, y, z\}$. Which of the following expressions are terms over Σ and X, which are atoms/literals/clauses/formulae, which are neither?

(a) $\neg p(g(a), f(x, y))$
(b) $f(x, x) \approx x$
(c) $p(f(x, a), x) \vee p(a, b)$
(d) $p(\neg g(x), g(y))$
(e) $\neg p(f(x, y))$
(f) $p(a, b) \wedge p(x, y) \wedge y$
(g) $\exists y(\neg p(f(y, y), y))$
(h) $\forall x \forall y(g(p(x, y)) \approx g(x))$

Exercise 3.2:
Let $\Sigma = (S, \Omega, \Pi)$ be a many-sorted signature, where $S = \{\mathsf{int}, \mathsf{list}\}$, $\Omega = \{\mathsf{cons}, \mathsf{car}, \mathsf{cdr}, \mathsf{nil}, b\}$ and $\Pi = \{p\}$ with the following arities:

$a(\mathsf{cons}) = \mathsf{int}, \mathsf{list} \to \mathsf{list}$ $\quad a(\mathsf{car}) = \mathsf{list} \to \mathsf{int}$ $\quad a(\mathsf{cdr}) = \mathsf{list} \to \mathsf{list}$
$a(\mathsf{nil}) = \to \mathsf{list}$ (i.e. nil is a constant of sort list)
$a(b) = \to \mathsf{int}$ (i.e. b is a constant of sort int)
$a(p) = \mathsf{int}, \mathsf{list}$.

Let X_{int} be the set of variables of sort int containing $\{i, j, k\}$, and let X_{list} be the set of variables of sort list containing $\{x, y, z\}$. Let $X = \{X_{\mathsf{int}}, X_{\mathsf{list}}\}$.

Which of the following expressions are terms over Σ and X, which are atoms/literals/clauses/formulae (in first-order logic with equality, where equality between terms of sort int is $\approx_i$ and equality between terms of sort list is $\approx_l$), which are neither?

(a) $\mathsf{cons}(\mathsf{cons}(b, \mathsf{nil}), \mathsf{nil})$
(b) $\mathsf{cons}(b, \mathsf{cons}(b, \mathsf{nil}))$
(c) $\neg p(b, \mathsf{cons}(b, \mathsf{cons}(b, \mathsf{nil})))$
(d) $\neg p(\mathsf{cons}(b, \mathsf{nil}), \mathsf{cons}(b, \mathsf{cons}(b, \mathsf{nil})))$

(e) $\mathsf{cons}(b, \mathsf{cons}(b, \mathsf{nil})) \approx_l \mathsf{cons}(\mathsf{cons}(x, b), \mathsf{nil})$
(f) $\mathsf{cons}(i, \mathsf{cons}(b, \mathsf{nil})) \approx j$
(g) $p(\neg\mathsf{car}(x), x)$
(h) $\neg p(\mathsf{car}(x), x) \vee p(j, \mathsf{cons}(j, x))$
(i) $\neg p(b, x) \vee p(b, \mathsf{cons}(b, x)) \vee b$
(j) $\forall i : \mathsf{int}, \forall x : \mathsf{list}\ (\mathsf{cons}(\mathsf{car}(x), \mathsf{cdr}(x)) \approx_l x)$
(k) $\exists i : \mathsf{int}, \forall y : \mathsf{list}\ (\mathsf{cons}(b, p(x, y)) \approx_l \mathsf{cdr}(y))$

Exercise 3.3:
Compute the results of the following substitutions:

(a) $f(g(x), x)[g(a)/x]$
(b) $p(f(y, x), g(x))[x/y]$
(c) $\forall y(p(f(y, x), g(y)))[x/y]$
(d) $\forall y(p(f(y, x), x))[y/x]$
(e) $\forall y(p(f(z, g(y)), g(x)) \vee \exists z(g(z) \approx y))[g(b)/z]$
(f) $\exists y\big(f(x, y) \approx x \rightarrow \forall x(f(x, y) \approx x)\big)[g(y)/y, g(z)/x]$

Exercise 3.4:
Let $\Sigma = (\Omega, \Pi)$, where $\Omega = \{0/0, s/1, +/2\}$ and $\Pi = \emptyset$ (i.e. the only predicate symbol is $\approx$). Consider the following formulae in the signature Σ:

1. $F_1 = \forall x\ (x + 0 \approx x)$
2. $F_2 = \forall x, y\ (x + s(y) \approx s(x + y))$
3. $F_3 = \forall x, y\ \ (x + y \approx y + x)$.

Find a Σ-structure in which F_1 and F_2 are valid but F_3 is not.

Exercise 3.5:
$\Sigma = (\Omega, \Pi)$ with $\Omega = \{b/0, f/1\}$ and $\Pi = \{p/1\}$.

(1) How many different Herbrand interpretations over Σ exist? Explain briefly.
(2) Consider the formula $F := p(f(f(b))) \wedge \forall x\,(p(x) \rightarrow p(f(x)))$. How many different Herbrand models over Σ does the formula F have? Explain briefly.
(3) Every Herbrand interpretation which is a model of F is also a model of $G := \forall x\, p(f(f(x)))$.
Give an example of an algebra that is a model of F but not of G.
(4) Let $\mathcal{A}$ be a Herbrand interpretation over Σ and let $\sim$ be the binary relation on T_Σ defined by:

$$t_1 \sim t_2 \text{ iff } \forall x\,(f(f(f(x))) = x) \models t_1 \approx t_2.$$

- Is $\sim$ a congruence relation on $\mathcal{A}$?
- Describe the quotient structure $\mathcal{A}/\sim$.
- Describe the class $\{\mathcal{A}/\sim \mid \mathcal{A}$ Herbrand interpretation over $\Sigma\}$.

Exercise 3.6:
Consider the following specification of binary trees (in a variant of the CASL syntax)

spec BinTree =
sort elem, tree
operations $a :\to \mathsf{elem}$
$\mathsf{empty} :\to \mathsf{tree}$
$\mathsf{leaf} : \mathsf{elem} \to \mathsf{tree}$
$\mathsf{make} : \mathsf{tree}, \mathsf{tree} \to \mathsf{tree}$
$\mathsf{right} : \mathsf{tree} \to \mathsf{tree}$
$\mathsf{left} : \mathsf{tree} \to \mathsf{tree}$
Axioms: $\forall x_1, x_2 : \mathsf{tree}, \forall e : \mathsf{elem}$:
- $\mathsf{right}(\mathsf{empty}) \approx \mathsf{empty}$
- $\mathsf{right}(\mathsf{leaf}(e)) \approx \mathsf{empty}$
- $\mathsf{left}(\mathsf{empty}) \approx \mathsf{empty}$
- $\mathsf{left}(\mathsf{leaf}(e)) \approx \mathsf{empty}$
- $\mathsf{left}(\mathsf{make}(x_1, x_2)) \approx x_1$
- $\mathsf{right}(\mathsf{make}(x_1, x_2)) \approx x_2$

(1) Let $\mathcal{F}$ be the set of axioms in the specification above. Which of the following hold?

(1a) $\mathcal{F} \models \mathsf{left}(\mathsf{make}(\mathsf{empty}, \mathsf{empty})) \approx \mathsf{empty}$

(1b) $\mathcal{F} \models \mathsf{make}(x_1, x_2) = \mathsf{empty}$

(1c) $\mathcal{F} \models (x_2 \approx \mathsf{empty} \wedge x_3 \approx \mathsf{make}(x_1, \mathsf{empty})) \to \mathsf{make}(\mathsf{left}(\mathsf{make}(x_1, x_2)), \mathsf{right}(\mathsf{leaf}(e)) \approx x_3$

(1d) $\mathcal{F} \models \mathsf{make}(x_1, \mathsf{make}(x_2, x_3)) = x_2$

(2) Let $\sim$ be defined on T_Σ by:

$$t_1 \sim t_2 \text{ iff } \mathcal{F} \models t_1 \approx t_2.$$

Describe the quotient algebra $\mathcal{T}_\Sigma/\sim$.

(3) Let $\sim'$ be defined on T_Σ by

$$t_1 \sim' t_2 \text{ iff } (\mathcal{F} \cup \{\forall x\, \mathsf{left}(x) \approx \mathsf{right}(x)\} \models t_1 \approx t_2).$$

Describe the quotient algebra $\mathcal{T}_\Sigma/\sim'$.

Please submit your solution until Wednesday, November 31, 2016 at 12:00. Please do not forget to write your name on your solution.

Submission possibilities:

- By e-mail to `sofronie@uni-koblenz.de` with the keyword "Homework FSV" in the subject.
- Hand it in to me (Room B225) or drop it in the box in front of Room B224.