Universität Koblenz-Landau

FB 4 Informatik

Prof. Dr. Viorica Sofronie-Stokkermans **May 14, 2014**

Exercises for "Formal Specification and Verification"
Exercise sheet 3

Exercise 3.1:
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 3.2:
Prove or refute the following statements:

(a) If F is a first-order formula, then F is valid if and only if $F \rightarrow \bot$ is unsatisfiable.
(b) If F and G are first-order formulae, F is valid, and $F \rightarrow G$ is valid, then G is valid.
(c) If F and G are first-order formulae, F is satisfiable, and $F \rightarrow G$ is satisfiable, then G is satisfiable.
(d) If F is a first-order formula and x a variable, then F is unsatisfiable if and only if $\exists xF$ is unsatisfiable.
(e) If F and G are first-order formulae and x is a variable then $\forall x(F \wedge G) \models \forall xF \wedge \forall xG$ and $\forall xF \wedge \forall xG \models \forall x(F \wedge G)$.
(f) If F and G are first-order formulae and x is a variable then $\exists x(F \wedge G) \models \exists xF \wedge \exists xG$ and $\exists xF \wedge \exists xG \models \exists x(F \wedge G)$.

Exercise 3.3:
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.

Definitions and notations:

Let $\Sigma{=}(\Omega, \Pi)$ be a signature and $\mathcal{A}{=}(U, \{f_\mathcal{A}{:}U^n{\to}U\}_{f/n\in\Omega}, \{p_\mathcal{A}{:}U^m{\to}\{0,1\}_{p/m\in\Pi}\})$ be a Σ-structure.

- An equivalence relation $\sim\subseteq U{\times}U$ is a *congruence relation*[1] if it is compatible with the operations and predicates, i.e. for every $f/n{\in}\Omega$ and $p/m{\in}\Pi$:

$$\forall x_1, \dots, x_n, y_1, \dots, y_n \in U,\; (x_1 \sim y_1 \wedge \dots \wedge x_n \sim y_n \to f_\mathcal{A}(x_1, \dots, x_n) \sim f_\mathcal{A}(y_1, \dots, y_n))$$
$$\forall x_1, \dots, x_m, y_1, \dots, y_m \in U,\; (x_1 \sim y_1 \wedge \dots \wedge x_m \sim y_m \to p_\mathcal{A}(x_1, \dots, x_m) = p_\mathcal{A}(y_1, \dots, y_m)).$$

- *The quotient structure* is $\hat{\mathcal{A}}{=}\mathcal{A}/{\sim}{=}(\hat{U}, \{f_{\hat{\mathcal{A}}}{:}\hat{U}^n{\to}\hat{U}\}_{f/n\in\Omega}, \{p_{\hat{\mathcal{A}}}{:}\hat{U}^m{\to}\{0,1\}_{p/m\in\Pi})$, where:
  - $\hat{U} = U/{\sim} = \{[x] \mid x \in U\}$, where $[x] = \{y \in U \mid x \sim y\}$
  - $f_{\hat{\mathcal{A}}}([x_1], \dots, [x_n]) = [f(x_1, \dots, x_n)]$ for every $f/n \in \Omega$
  - $p_{\hat{\mathcal{A}}}([x_1], \dots, [x_m]) = p(x_1, \dots, x_n)$ for every $p/m \in \Pi$.

- A *term Σ-structure* (or a *Herbrand interpretation over* Σ) is a Σ-structure $\mathcal{A}$ having as universe the set T_Σ of ground terms and the operations defined by $f_\mathcal{A}(t_1, \dots, t_n) = f(t_1, \dots, t_n)$ and arbitrarily defined predicates.

- If $\Pi = \emptyset$ (i.e. $\approx$ is the unique predicate) then there is only one term Σ-structure (Herbrand interpretation), which we will denote with $\mathcal{T}_\Sigma$.

Exercise 3.4:
$\Sigma = (\Omega, \Pi)$ 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 $F := p(f(f(b))) \wedge \forall x\, (p(x) \to p(f(x)))$. 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 3.5:
Consider the following specification of binary trees (in a variant of the CASL syntax)

[1] In the many-sorted case the definitions are similar, with the difference that $T_\Sigma = \{T^s_\Sigma\}_{s\in S}$, where T^s_Σ is the set of all terms of sort s, and a congruence relation $\sim$ consists of a family of equivalence relations $\{\sim_s\subseteq U_s \times U_s\}_{s\in S}$ which is compatible with the operations and predicates (similar definition, but the sorts of the variables x_i, y_i correspond to the arity of f; for comparing two terms of sort s the predicate $\sim_s$ is used).

spec $\mathsf{BinTree} =$

sort $\mathsf{elem}, \mathsf{tree}$

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, May 21, 2014 at 11:00. 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.