Formal Methods for High-Assurance Software Engineering

HomeWork Assignment 06

Shahin Roozkhosh
shahin@bu.edu
U01670169

October 2020

Problem 1. Do Exercise 7 in fode. Write the wff's for the first-order definability of gcd in two different ways.

Solution. In this solution we use what proved in Exercise 4 where it's showed $\varphi_{<}(x,y)$ first-order definable in $(\mathbb{N};+,0)$.

$$\varphi_{gcd}(x,y,v) \stackrel{\text{def}}{=} (v|x) \wedge (v|y) \wedge \forall w \Big(\big((w|x) \wedge (w|y) \big) \Longrightarrow (w \approx (v \vee \varphi_{<}(w,v) \Big)$$
$$\varphi'_{gcd}(x,y,v) \stackrel{\text{def}}{=} \forall w \Big(\big((w|x) \wedge (w|y) \big) \Longleftrightarrow (w|v) \Big) \qquad (1)$$

Problem 2.

Solution.

Exercise 10

Show that the predicate prime : $\mathbb{N} \longrightarrow \{T,F\}$ is first-order definable in the structure $(\mathbb{N};|,+,0)$.

In Exercise 9 we defined $\varphi'_{\times}(x,y,z)$ in $(\mathbb{N};|,+,0)$. Note that at the end of exercise, it is showd that $succ$ which used in that definition, is definable using only $\{+,0\}$ based on what happened in Exercise 8. Hence just like what is done in other excercises, we take it for granted that $\varphi'_{\times}(x,y,z)$ is definable in $\varphi'_{\times}(x,y,z)$.

Here's the definition of the predicate **prime**: $\mathbb{N} \longrightarrow \{T,F\}$:

$$\varphi_{prime}(x) \stackrel{\text{def}}{=} \neg\Big(\exists z\ \exists y\Big(\Big(\varphi'_{\times}(z,y,x)\Big) \wedge \Big(\neg(x \approx x)\ \wedge\ \neg(y \approx x)\Big)\Big)\Big) \tag{2}$$

Another definition:

$$\varphi_{prime}(x) \stackrel{\text{def}}{=} \Big(\varphi_{<}(1,x)\Big) \wedge \forall y\Big((y|x) \Longrightarrow \big((y \approx 1) \vee (y \approx x)\big)\Big) \tag{3}$$

Exercise 11

Show that the predicate coprime : $\mathbb{N} \longrightarrow \{T,F\}$ is first-order definable in the structure $(\mathbb{N};|,+,0)$

Here, we kindle use the definition of gcd we provided in Problem 1 of this homework.

$$\varphi'_{gcd}(x,y,v) \stackrel{\text{def}}{=} \forall w\Big(\Big((w|x) \wedge (w|y)\Big) \Longleftrightarrow (w|v)\Big) \tag{4}$$

$$\varphi_{coprime}(x,y) \stackrel{\text{def}}{=} \varphi'_{gcd}(x,y,1) \tag{5}$$

Problem 3.

12.a

Solution. Answer: **invalid**

We provide an example model which does not satisfy it:

In the model $\mathscr{M} = (a,b,S)$ Let $S^{\mathscr{M}} : \{(a,b)(b,a)(a,a)\}$ Then, in the following formula:

$$(\forall x \forall y(S(x,y) \Longrightarrow S(y,x)) \Longrightarrow (\forall x \neg S(x,x)) \tag{6}$$

For any given pair, it's reverse is in the defined relation. This makes the left hand side valid. Hence the right hand side is not valid since by letting $x \equiv a$, $S(x,x) \equiv S(a,a)$ is in the model while according to the right hand side it shouldn't be.

12.b

Solution. Answer: **valid**

$$\exists y(((\forall x\ P(x)) \Longrightarrow P(y)) \tag{7}$$

Semantically speaking, it is intuitive since the left hand side is independent of y, hence we can consider two cases.

- There exists a y_0 which makes $P(y_0)$ false, hence by picking this y_0 the right hand side becomes equivalent to FALSE which makes the formula valid.
- Otherwise, if there isn't any y_0 which makes $P(y_0)$ false, P(y) should be a tautology which makes the formula equivalent to $T \Longrightarrow T$ which is also valid.

More formal proof:

1	$P(x)$	assume
2	y_0	fresh
3	$\forall x\ P(x)$	assume
4	$P(y_0)$	1,3
5	$(\forall x P(x)) \Longrightarrow P(y_0)$	$\rightarrow$i, $2-4$
6	$\exists y(((\forall x\ P(x)) \Longrightarrow P(y))$	$\exists y$i $2-5$

12.c

Solution. Answer: **valid**

$$(\forall x\ (P(x) \Longrightarrow \exists y\ Q(y))) \Longrightarrow (\forall x\ \exists y(P(x) \Longrightarrow Q(y))) \tag{8}$$

1	$(\forall x\,(P(x) \Longrightarrow \exists y\, Q(y)))$	assume
2	y_0	fresh
3	$P(x) \Longrightarrow \exists y\, Q(y)$	$\forall x$e 1
4	$P(x)$	assume
5	$\exists y\, Q(y)$	$\rightarrow$e, 3, 4
6	$Q(y_0)$	$\exists x$e, 2, 5
7	$P(x) \Longrightarrow Q(y_0)$	$\rightarrow$i, 4 − 6
8	$\exists y(P(x) \Longrightarrow Q(y))$	$\exists y$i 7
9	$\forall x \exists y(P(x) \Longrightarrow Q(y))$	$\forall x$i, 2 − 8
10	$(\forall x\,(P(x) \Longrightarrow \exists y\, Q(y))) \Longrightarrow (\forall x\, \exists y(P(x) \Longrightarrow Q(y)))$	$\rightarrow$i, 1 − 9

Problem 4. Show that "$\uparrow$" (exponentiation) is first-order definable in the model $(\mathbb{N}, \approx, <, +, ., S, 0)$.

Solution. In this solution we used two hints provided by Prof. Kfoury:
(1) Assume the existence of a binary function D on the natural numbers which can encode finite sequences of natural numbers, in the following sense: For every finite sequence $(a_0, a_1, \ldots, a_n)$ of length n, there is an s such that $D(s,i) = a_i$ for every $i \leqslant n$.

(2) With the function D you can define exponentiation $\uparrow$ as follows:
a $\uparrow b = \{$ the smallest s such that $D(s,0) = 1$ and for every $i < b$ it is the case that $D(s,i+1) = D(s,i) \times a\}$.

$$\varphi_{\uparrow}(x,y,z) \stackrel{\text{def}}{=} \exists u \Big(\Big(\forall v \forall t \,\Big((v < y) \wedge \varphi_D(u,v,t) \Longrightarrow \varphi_D(u, v{+}1, z.t)\Big)\Big) \wedge \varphi_D(u,y,z) \wedge \varphi_D(u,0,1)\Big)$$

Problem 5.

Solution. `https://github.com/ro0zkhosh/CS511/blob/master/HW6/problem5.py`

Problem 6.

Solution. https://github.com/ro0zkhosh/CS511/blob/master/HW6/problem6.py