CS 511 Formal Methods for High-Assurance Software Engineering
Homework Assignment 06 - Selected Solution

Jiawen Liu

Problem 1.

1. $\phi_{gdc}(x,y,v) \stackrel{\text{def}}{=} (v|x) \land (v|y) \land \forall w.\Big(\big((w|x) \land (w|y)\big) \to \big(v \approx w \lor \phi_<(w,v)\big)\Big)$

2. $\phi_{gdc}(x,y,v) \stackrel{\text{def}}{=} \forall w.\Big(\big((w|x) \land (w|y)\big) \leftrightarrow (w|v)\Big)$

Problem 2. We know $x < y$ is first order definable in $(\mathbb{N}, 0, +)$ by wff $\phi_<(x,y)$.
We also know $\mathsf{succ}(x) = y$ is definable in $(\mathbb{N}, <)$ by wff $\phi_{succ}(x,y)$.

1.
$$\begin{aligned} \phi_{prime}(x) = \quad & \exists v.\exists u.\big(\phi_<(0,v) \land \phi_<(0,u) \land (v+u \approx x)\big) && (x > 1) \\ & \land \forall w.\big((w|x) \to (\phi_{succ}(0,w) \lor x \approx w)\big) && \text{(x is prime)} \end{aligned}$$

2.
$$\phi_{coprime}(x,y) = \quad \forall w.\big(\phi_{gcd}(x,y,w) \to (\phi_{succ}(0,w)\big)$$

Problem 3.

1. This is invalid.
   Let domain be $\{a,b\}$, $S = \{(a,b),(a,a),(b,a)\}$, we then have $\forall x.\forall y.(S(x,y) \to S(y,x))$ is true. However, there exists $x = a$ s.t. $S(x,x)$ is also true.

2.

1	$\forall x.\ P(x)$	assumption
2	$P(x_0)$	$(\mathrm{e}\forall x.\ )1$
3	$(\forall x.\ P(x)) \to P(x_0)$	$\to\mathrm{i}1-2$
4	$\exists y.\ ((\forall x.\ P(x)) \to P(y))$	$(\mathrm{i}\exists y.\ )3$

3.

	1	$\forall x.\ (P(x) \to \exists y.\ Q(y))$	assumption
x_0	2		fresh
	3	$P(x_0) \to \exists y.\ Q(y)$	$\forall x.$ e 1
	4	$P(x_0)$	assumption
	5	$\exists y.\ Q(y)$	$\to$e 3,4
y_0	6		fresh
	7	$Q(y_0)$	assumption
	8	$Q(y_0)$	$\exists y.$ e 5,6 − 7
	9	$P(x_0) \to Q(y_0)$	$\to$i 4 − 8
	10	$\exists y.\ (P(x_0) \to Q(y))$	$\exists y.$ i 9
	11	$\forall x.\exists y.\ (P(x_0) \to Q(y))$	$\forall x.$ i 2 − 10
	12	$\forall x.\ (P(x) \to \exists y.\ Q(y)) \to \forall x.\exists y.\ (P(x_0) \to Q(y))$	$\to$i 1 − 11

Problem 4.

- Let $\phi(x,y,z)$ defined inductively as follows:
  $\phi(x,0,1)$
  $\phi(x,y,z) \stackrel{\text{def}}{=} \exists j.\exists w.\ (j+1) = y \wedge (w \times x = z) \wedge \phi(x,j,w)$.

- By the hint from piazza, 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 $(a_0, a_1, \cdots, a_n)$ of length n, there is an s such that $D(s,i) = a_i$ for every $i \leq n$.
  We first have $\phi'(s,x,y)$ defined as:

$$\phi'(s,x,y) \stackrel{\text{def}}{=} (D(s,0) \approx 1 \wedge \forall i.\ \big((i < y) \to D(s,i+1) \approx D(s,i) \times x\big)).$$

  Then, we have the $m = x \uparrow y$ defined by $\phi(m,x,y)$ as:

$$\phi_{\uparrow}(m,x,y) \stackrel{\text{def}}{=} \phi'(m,x,y) \wedge \forall s.\ \big(\phi'(s,x,y) \to (s \approx m) \vee (\phi_{<}(m,s))\big)$$

Problem 5. `https://github.com/jiawenliu/CS511/blob/master/homework/hw6/hw6-p5.py`

Problem 6. `https://github.com/jiawenliu/CS511/blob/master/homework/hw6/hw6-p6.py`