CS81 HW#4 Spring 2012

Logical Problems Let L_S be a first-order language with one constant e and one binary function f. So $S = \{e^{(0)}, f^{(2)}\}$. Consider the following first-order sentences over L_S.

$$
\begin{aligned}
\phi_1 &= (\forall x)(\forall y)(\forall z)[f(x, f(y, z)) = f(f(x, y), z)] \\
\phi_2 &= (\forall x)[f(x, e) = x] \\
\phi_3 &= (\forall x)(\exists y)[f(x, y) = e] \\
\phi_4 &= (\forall x)(\exists y)[f(y, x) = e] \\
\phi_5 &= (\forall x)[(\forall y)(f(y, x) = y) \to (x = e)] \\
\phi_6 &= (\forall x)(\forall y)(\forall z)[(f(x, z) = e) \to (f(f(x, y), z) = y)] \\
\phi_7 &= (\forall x)(\forall y)(\forall z)[((f(x, y) = e) \wedge (f(x, z) = e)) \to (y = z)]
\end{aligned}
$$

Let $\Phi = \{\phi_1, \phi_2, \phi_3\}$. Prove or disprove the following semantic entailments:

1. $\Phi \models \phi_4$.
2. $\Phi \models \phi_5$.
3. $\Phi \models \phi_6$.
4. $\Phi \models \phi_7$.

You may need to invoke some rules on equality.

Example: We show $\Phi \models (\forall x)[f(e,x) = x]$. This shows e is a *left*-identity element.

1	$(\forall x)(\forall y)(\forall z)[f(x, f(y,z)) = f(f(x,y),z)]$	**premise**: associative law
2	$(\forall x)[f(x,e) = x]$	**premise**: identity law
3	$(\forall x)(\exists y)[f(x,y) = e]$	**premise**: right-inverse law
4	$f(a,e) = a$	$\forall\mathcal{E}$, 2
5	$(\exists y)[f(a,y) = e]$	**each element** a **has an inverse**: $\forall\mathcal{E}$, 3
6	$f(a,\hat{b}) = e$	**say** $\hat{b}$ **is the inverse of** a: $\exists\mathcal{E}$, 5
7	$f(e,a) = f(e,a)$	$=\mathcal{I}$
8	$f(e,a) = f(f(a,\hat{b}),a)$	**use** $e = a \circ \hat{b}$: $=\mathcal{E}$, 7, 6
9	$(\forall y)(\forall z)[f(a, f(y,z)) = f(f(a,y),z)]$	$\forall\mathcal{E}$, 1
10	$(\forall z)[f(a, f(\hat{b},z)) = f(f(a,\hat{b}),z)]$	$\forall\mathcal{E}$, 9
11	$f(a, f(\hat{b},a)) = f(f(a,\hat{b}),a)$	$\forall\mathcal{E}$, 10
12	$f(e,a) = f(a, f(\hat{b},a))$	**associative law**: $=\mathcal{E}$, 11, 8
13	$f(f(\hat{b},a),e) = f(\hat{b},a)$	**identity law on** $\hat{b} \circ a$: $=\mathcal{E}$, 4
14	$(\exists y)[f(\hat{b},y) = e]$	$\hat{b}$ **has an inverse**: $\forall\mathcal{E}$, 3
15	$f(\hat{b},\hat{c}) = e$	**say** $\hat{c}$ **is the inverse of** $\hat{b}$: $\exists\mathcal{E}$, 14
16	$f(f(\hat{b},a), f(\hat{b},\hat{c})) = f(\hat{b},a)$	**use** $e = \hat{b} \circ \hat{c}$: $=\mathcal{E}$, 13, 15
17	$(\forall y)(\forall z)[f(\hat{b}, f(y,z)) = f(f(\hat{b},y),z)]$	$\forall\mathcal{E}$, 1
18	$(\forall z)[f(\hat{b}, f(a,z)) = f(f(\hat{b},a),z)]$	$\forall\mathcal{E}$, 17
19	$f(\hat{b}, f(a,d)) = f(f(\hat{b},a),d)$	$\forall\mathcal{E}$, 18
20	$f(\hat{b},\hat{c}) = f(\hat{b},\hat{c})$	$=\mathcal{I}$
21	$f(\hat{b}, f(a, f(\hat{b},\hat{c}))) = f(f(\hat{b},a), f(\hat{b},\hat{c}))$	$=\mathcal{E}$, 19, 20
22	$f(\hat{b}, f(a, f(\hat{b},\hat{c}))) = f(\hat{b},a)$	= Elimination, 21, 16

23	$(\forall y)(\forall z)[f(a, f(y, z)) = f(f(a, y), z)]$	$\forall\mathcal{E}$, 1
24	$(\forall z)[f(a, f(\hat{b}, z)) = f(f(a, \hat{b}), z)]$	$\forall\mathcal{E}$, 23
25	$f(a, f(\hat{b}, \hat{c})) = f(f(a, \hat{b}), \hat{c})$	$\forall\mathcal{E}$, 24
26	$f(\hat{b}, f(f(a, \hat{b}), \hat{c})) = f(\hat{b}, a)$	$=$ Elimination, 22, 25
27	$f(\hat{b}, f(e, \hat{c})) = f(\hat{b}, a)$	**use** $e = a \circ \hat{b}$: $= \mathcal{E}$, 26, 6
28	$(\forall y)(\forall z)[f(\hat{b}, f(y, z)) = f(f(\hat{b}, y), z)]$	$\forall\mathcal{E}$, 1
29	$(\forall z)[f(\hat{b}, f(e, z)) = f(f(\hat{b}, e), z)]$	$\forall\mathcal{E}$, 28
30	$f(\hat{b}, f(e, \hat{c})) = f(f(\hat{b}, e), \hat{c})$	$\forall\mathcal{E}$, 29
31	$f(f(\hat{b}, e), \hat{c}) = f(\hat{b}, a)$	$=$ Elimination, 27, 30
32	$f(\hat{b}, e) = \hat{b}$	$= \mathcal{E}$, 4
33	$f(\hat{b}, \hat{c}) = f(\hat{b}, a)$	**use** $\hat{b} \circ e = \hat{b}$: $= \mathcal{E}$, 31, 32
34	$e = f(\hat{b}, a)$	**use** $\hat{b} \circ \hat{c} = e$: $= \mathcal{E}$, 33, 15
35	$f(e, a) = f(a, e)$	**use** $\hat{b} \circ a = e$: $= \mathcal{E}$, 12, 34
36	$f(e, a) = a$	**use** $a \circ e = a$: $= \mathcal{E}$, 35, 4
37	$(\forall x)[f(e, x) = x]$	e **is left-identity for each** a: $\forall\mathcal{I}$, 36