Solutions

1.
```
mul m Zero = Zero
mul m (Suc n) = add m (mul m n)

exp m Zero = Suc Zero
exp m (Suc n) = mul m (exp m n)

sup m Zero = Suc Zero   (other choices ok)
sup m (Suc n) = exp m (sup m n)

f 0 m n = m + n
f (k+1) m 0 = k
f (k+1) m (n+1) = f k m (f (k+1) m n)
```
   This is essentially how the Ackermann function was defined by himself. It has applications in algorithm theory and the theory of computation.

2. (a) Show that `add Zero (Suc m) = add (Suc Zero) m`.
   `add Zero (Suc m) = Suc m`
   `add (Suc Zero) m = Suc (add Zero m) = Suc m`

   (b) Assume `add k (Suc m) = add (Suc k) m` for a fixed but arbitrary `k` and for all `m`.
   Show that `add (Suc k) (Suc m) = add (Suc (Suc k)) m` for all `m`.
   `add (Suc k) (Suc m) = Suc (add k (Suc m)) = Suc(add (Suc k) m) = add (Suc (Suc k)) m`.

3. **Sats.** Let $p \in$ `Tree a` $\to \mathbb{B}$ be a property. If
   (a) p(`Leaf x`) for all x in a and
   (b) p(`t1`) and p(`t2`) implies p(`Node t1 t2`) for all `t1, t2` in `Tree a`
   then p(`t`) is true for all `t` in `Tree a`. ■

4. One auxiliary function is required.

$$\begin{aligned}
\mathcal{P}[\![0]\!] &= 1\\
\mathcal{P}[\![1]\!] &= 1\\
\mathcal{P}[\![0\ n]\!] &= 2\cdot\mathcal{P}[\![n]\!]\\
\mathcal{P}[\![1\ n]\!] &= 2\cdot\mathcal{P}[\![n]\!]
\end{aligned}$$

$$\begin{aligned}
\mathcal{N}[\![0]\!] &= 0\\
\mathcal{N}[\![1]\!] &= 1\\
\mathcal{N}[\![0\ n]\!] &= \mathcal{N}[\![n]\!]\\
\mathcal{N}[\![1\ n]\!] &= \mathcal{P}[\![n]\!]+\mathcal{N}[\![n]\!]
\end{aligned}$$

5. Prove that $\mathcal{A}[\![a[y\mapsto a_0]]\!]\sigma = \mathcal{A}[\![a]\!](\sigma[y\mapsto\mathcal{A}[\![a_0]\!]\sigma])$ for all $a \in$ **Aexp**.

   (a) Show that $\mathcal{A}[\![n[y\mapsto a_0]]\!]\sigma = \mathcal{A}[\![n]\!](\sigma[y\mapsto\mathcal{A}[\![a_0]\!]\sigma])$ for all $n \in$ Num.
   $\mathcal{A}[\![n[y\mapsto a_0]]\!]\sigma = \mathcal{A}[\![n]\!]\sigma = \mathcal{N}[\![n]\!]$.
   $\mathcal{A}[\![n]\!](\sigma[y\mapsto\mathcal{A}[\![a_0]\!]\sigma]) = \mathcal{N}[\![n]\!]$.

(b) The case when a is variable different from x is similar to the previous case. In the other case prove that $\mathcal{A}[\![y[y \mapsto a_0]]\!]\sigma = \mathcal{A}[\![y]\!](\sigma[y \mapsto \mathcal{A}[\![a_0]\!]\sigma])$.
$\mathcal{A}[\![y[y \mapsto a_0]]\!]\sigma = \mathcal{A}[\![a_0]\!]\sigma$.
$\mathcal{A}[\![y]\!](\sigma[y \mapsto \mathcal{A}[\![a_0]\!]\sigma]) = (\sigma[y \mapsto \mathcal{A}[\![a_0]\!]\sigma])y = \mathcal{A}[\![a_0]\!]\sigma]$.

(c) Next consider the case when $a = a_1 + a_2$. Assume that $\mathcal{A}[\![a_1[y \mapsto a_0]]\!]\sigma = \mathcal{A}[\![a_1]\!](\sigma[y \mapsto \mathcal{A}[\![a_0]\!]\sigma])$ and $\mathcal{A}[\![a_2[y \mapsto a_0]]\!]\sigma = \mathcal{A}[\![a_2]\!](\sigma[y \mapsto \mathcal{A}[\![a_0]\!]\sigma])$.

$$\begin{aligned}&\mathcal{A}[\![(a_1 + a_2)[y \mapsto a_0]]\!]\sigma = \mathcal{A}[\![a_1[y \mapsto a_0] + a_2[y \mapsto a_0]]\!]\sigma = \\ &\mathcal{A}[\![a_1[y \mapsto a_0]]\!]\sigma + \mathcal{A}[\![a_2[y \mapsto a_0]]\!]\sigma = \\ &\mathcal{A}[\![a_1]\!](\sigma[y \mapsto \mathcal{A}[\![a_0]\!]\sigma]) + \mathcal{A}[\![a_2]\!](\sigma[y \mapsto \mathcal{A}[\![a_0]\!]\sigma]) = \\ &\mathcal{A}[\![a_1 + a_2]\!](\sigma[y \mapsto \mathcal{A}[\![a_0]\!]\sigma])\end{aligned}$$

(d) The remaining two cases are analogous.

6.

$$\begin{aligned}\texttt{true}[y \mapsto a] &= \texttt{true} \\ \texttt{false}[y \mapsto a] &= \texttt{false} \\ (a_1 = a_2)[y \mapsto a] &= (a_1[y \mapsto a] = a_2[y \mapsto a]) \\ (a_1 \le a_2)[y \mapsto a] &= (a_1[y \mapsto a] \le a_2[y \mapsto a]) \\ (\neg b)[y \mapsto a] &= \neg b[y \mapsto a] \\ (b_1 \wedge b_2)[y \mapsto a] &= (b_1[y \mapsto a] \wedge b_2[y \mapsto a])\end{aligned}$$

Proof by induction over b.

Base 1: $b = \texttt{true}$.

$\mathcal{B}[\![\texttt{true}[y \mapsto a]]\!]\sigma = \mathcal{B}[\![\texttt{true}]\!]\sigma = \mathbf{tt}$.

$\mathcal{B}[\![\texttt{true}]\!](\sigma[y \mapsto \mathcal{A}[\![a_0]\!]\sigma]) = \mathbf{tt}$

Base 2: $b = \texttt{false}$. Similar.

Base 3: $b = (a_1 = a_2)$.

$$\begin{aligned}\mathcal{B}[\![(a_1 = a_2)[y \mapsto a]]\!]\sigma &= \mathcal{B}[\![(a_1[y \mapsto a] = a_2[y \mapsto a])]\!]\sigma \\ &= (\mathcal{A}[\![a_1[y \mapsto a]]\!]\sigma = \mathcal{A}[\![a_2[y \mapsto a]]\!]\sigma) \\ &= (\mathcal{A}[\![a_1]\!](\sigma[y \mapsto \mathcal{A}[\![a]\!]\sigma]) = \mathcal{A}[\![a_2]\!](\sigma[y \mapsto \mathcal{A}[\![a]\!]\sigma])) \\ &= \mathcal{B}[\![a_1 = a_2]\!](\sigma[y \mapsto \mathcal{A}[\![a]\!]\sigma])\end{aligned}$$

Base 4: $b = (a_1 \le a_2)$. Similar.

Induction 1: $b = (\neg b_0)$. Assume that $\mathcal{B}[\![b_0[y \mapsto a]]\!]\sigma = \mathcal{B}[\![b_0]\!](\sigma[y \mapsto \mathcal{A}[\![a]\!]\sigma])$.

Prove that $\mathcal{B}[\![\neg(b_0)[y \mapsto a]]\!]\sigma = \mathcal{B}[\![\neg(b_0)]\!](\sigma[y \mapsto \mathcal{A}[\![a]\!]\sigma])$. Quite mechanical ...

Induction 2: $b = (b_1 \wedge b_2)$. Two assumptions, but otherwise similar.

7.

$$\langle\, \texttt{0} \,\rangle \to 0 \qquad \langle\, \texttt{1} \,\rangle \to 1$$

$$\frac{\langle\, n \,\rangle \to z}{\langle\, n\ \ \texttt{0} \,\rangle \to 2z} \qquad \frac{\langle\, n \,\rangle \to z}{\langle\, n\ \ \texttt{1} \,\rangle \to 2z + 1}$$

8. First we prove that for all $n \in \text{Num}$: if $\mathcal{N}[\![n]\!] = z$ then there is a derivation tree for $\langle\, n \,\rangle \to z$. The proof is by induction over the structure of n.

- Assume that $\mathcal{N}[\![0]\!] = z$. Then z must be 0. But since $\langle\, 0 \,\rangle \to 0$ is an axiom there is a trivial derivation tree for it. The case 1 is similar.
- Next consider the case $n\ 0$. The inductive assumption is that if $\mathcal{N}[\![n]\!] = z'$ then there is a derivation tree for $\langle\, n \,\rangle \to z'$. We have to prove that if $\mathcal{N}[\![n\ 0]\!] = z$ then there is a derivation tree for $\langle\, n\ 0 \,\rangle \to z$. Now if $\mathcal{N}[\![n\ 0]\!] = z$ then $\mathcal{N}[\![n]\!] = z'$ where $z' = z/2$. From the inductive assumption it follows that there is a derivation tree for $\langle\, n \,\rangle \to z/2$. Using the natural semantic rule for $n\ 0$ we can build the required derivation tree. The case $n\ 1$ is similar.

It remains to prove that for all derivation trees: if the root of the derivation tree is $\langle\, n \,\rangle \to z$ then $\mathcal{N}[\![n]\!] = z$. The proof is by induction over the shape of derivation trees. ...

9.

$$\frac{\langle S, \sigma\rangle \to \sigma'}{\langle \texttt{if}\ b\ \texttt{then}\ S, \sigma\rangle \to \sigma'} \qquad \text{if } \mathcal{B}[\![b]\!]\sigma = \text{tt}$$

$$\langle \texttt{if}\ b\ \texttt{then}\ S, \sigma\rangle \to \sigma \qquad \text{if } \mathcal{B}[\![b]\!]\sigma = \text{ff}$$

10.

$$\langle\, \texttt{do}\ S\ \texttt{while}\ b, \sigma \,\rangle \Rightarrow \langle\, S;\ \texttt{if}\ b\ \texttt{then do}\ S\ \texttt{while}\ b\ \texttt{else skip}, \sigma \,\rangle$$

The following will give the same semantics but is not "small step semantics".

$$\frac{\langle\, S, \sigma \,\rangle \Rightarrow \sigma'}{\langle\, \texttt{do}\ S\ \texttt{while}\ b, \sigma \,\rangle \Rightarrow \langle\, \texttt{do}\ S\ \texttt{while}\ b, \sigma' \,\rangle}$$

if $\mathcal{B}[\![b]\!]\sigma' = \text{tt}$

$$\frac{\langle\, S, \sigma \,\rangle \Rightarrow \sigma'}{\langle\, \texttt{do}\ S\ \texttt{while}\ b, \sigma \,\rangle \Rightarrow \sigma'}$$

if $\mathcal{B}[\![b]\!]\sigma' = \text{ff}$

11. With the first replacements we cannot prove e.g. $\langle \texttt{if 0} = \texttt{1 then skip else skip}, \sigma\rangle \to \sigma$. In the second suggestion with `b = true`, S_0=`skip`, and S_1=`while true do skip` we cannot use the rule since there is no derivation tree for $\langle S_1, \sigma\rangle \to \sigma'$.

12. We shall prove that

$$\langle S_1, \sigma\rangle \Rightarrow^k \sigma' \text{ implies } \langle S_1; S_2, \sigma\rangle \Rightarrow^k \langle S_2, \sigma'\rangle$$

for all $S_1, S_2, \sigma, \sigma'$ and k. We use induction over k.
Base. For $k = 0$ the assertion is vacously true since $\langle S_1, \sigma\rangle \Rightarrow^0 \sigma'$ cannot be true.

$k = 1$ is left as an exercise. You will need the rule $[comp^2_{SOS}]$.
Inductive step. Let $k_0 \geq 1$ be any fixed number.
Assume that $(\langle S_1, \sigma\rangle \Rightarrow^{k_0} \sigma')$ implies $(\langle S_1; S_2, \sigma\rangle \Rightarrow^{k_0} \langle S_2, \sigma'\rangle)$ for all $S_1, S_2, \sigma, \sigma'$.
We shall show that $(\langle S_1, \sigma\rangle \Rightarrow^{k_0+1} \sigma')$ implies $(\langle S_1; S_2, \sigma\rangle \Rightarrow^{k_0+1} \langle S_2, \sigma'\rangle)$ for all $S_1, S_2, \sigma, \sigma'$.
Now let $\langle S_1, \sigma\rangle \Rightarrow \langle S_1', \sigma''\rangle \Rightarrow^{k_0} \sigma'$ be the first step in this derivation sequence.
By $[\text{comp}^1_{SOS}]$ it follows that $\langle S_1; S_2, \sigma\rangle \Rightarrow \langle S_1'; S_2, \sigma''\rangle$.
Using the induction assumption with $\sigma = \sigma''$ we have
$\langle S_1'; S_2, \sigma''\rangle \Rightarrow^{k_0} \langle S_2, \sigma'\rangle$. We conclude by transitivity that $\langle S_1; S_2, \sigma\rangle \Rightarrow^{k_0+1} \langle S_2, \sigma'\rangle$.

13. Take $S_1 = \texttt{skip}$ and $S_2 = \texttt{while}\ \neg(\texttt{x} = \texttt{0})\ \texttt{do x} := \texttt{x} - \texttt{1}$, σ a state where $\sigma = [x \mapsto 2]$ and $\sigma' = [x \mapsto 1]$.