Assignment 1

Anyang He (heanyang1)

Problem 1

Part 1:

$$
\begin{aligned}
\textsf{Property } p ::= \quad & \varepsilon \\
| \quad & > n \mid = n \mid < n \\
| \quad & = s \\
| \quad & (p) \\
| \quad & p_1 \vee p_2 \mid p_1 \wedge p_2 \\
\\
\textsf{Schema } \tau ::= \quad & \textsf{number}\langle p \rangle \mid \textsf{string}\langle p \rangle \mid \textsf{bool} \\
| \quad & [\tau] \\
| \quad & \{(s : \tau)^*\}
\end{aligned}
$$

Part 2:

$$\frac{}{\textsf{false} \sim \textsf{bool}} \text{ (S-Bool-False)} \qquad \frac{}{\textsf{true} \sim \textsf{bool}} \text{ (S-Bool-True)}$$

$$\frac{}{s \sim \textsf{string}\langle \varepsilon \rangle} \text{ (S-String-Terminate)} \qquad \frac{}{n \sim \textsf{number}\langle \varepsilon \rangle} \text{ (S-Number-Terminate)}$$

$$\frac{s = s_0}{s \sim \textsf{string}\langle = s_0 \rangle} \text{ (S-String-Equal)} \qquad \frac{n = n_0}{n \sim \textsf{number}\langle = n_0 \rangle} \text{ (S-Number-Equal)}$$

$$\frac{n > n_0}{n \sim \textsf{number}\langle > n_0 \rangle} \text{ (S-Number-Greater)} \qquad \frac{n < n_0}{n \sim \textsf{number}\langle < n_0 \rangle} \text{ (S-Number-Lesser)}$$

$$\frac{s \sim \textsf{string}\langle p_1 \rangle \;\; s \sim \textsf{string}\langle p_2 \rangle}{s \sim \textsf{string}\langle p_1 \wedge p_2 \rangle} \text{ (S-String-And)} \qquad \frac{s \sim \textsf{string}\langle p_1 \rangle}{s \sim \textsf{string}\langle p_1 \vee p_2 \rangle} \text{ (S-String-Or)}$$

$$\frac{n \sim \textsf{number}\langle p_1 \rangle \;\; n \sim \textsf{number}\langle p_2 \rangle}{n \sim \textsf{number}\langle p_1 \wedge p_2 \rangle} \text{ (S-Number-And)} \qquad \frac{n \sim \textsf{number}\langle p_1 \rangle}{n \sim \textsf{number}\langle p_1 \vee p_2 \rangle} \text{ (S-Number-Or)}$$

$$\frac{\forall i = 0 \ldots |j| - 1.\; j_i \sim \tau}{[j^*] \sim [\tau]} \text{ (S-List)} \qquad \frac{\forall s' \in s.\; j_{s'} \sim \tau_{s'}}{\{(s : j)^*\} \sim \{(s : \tau)^*\}} \text{ (S-Dict)}$$

Problem 2

Part 1:

$$\frac{}{(\varepsilon, j)\ \mathsf{val}}\ (\textsc{A-Terminate}) \qquad \frac{j = \{s' : j', \dots\}}{(.sa, j) \mapsto (a, j')}\ (\textsc{A-Dict}) \qquad \frac{j = [\dots, j_n, \dots]}{([n]a, j) \mapsto (a, j_n)}\ (\textsc{A-Index})$$

$$\frac{}{(|\varepsilon, j) \mapsto (\varepsilon, j)}\ (\textsc{A-Map-Empty}) \qquad \frac{\forall n = 0 \dots |j| - 1.\ (a, j_n) \mapsto (a', j'_n)}{(|a, j) \mapsto (|a', [\dots, j'_n, \dots])}\ (\textsc{A-Map})$$

Part 2:

$$\frac{}{\varepsilon \sim \tau}\ (\textsc{V-Terminate}) \qquad \frac{a \sim \tau}{.sa \sim \{s : \tau, \dots\}}\ (\textsc{V-Dict}) \qquad \frac{a \sim \tau}{[n]a \sim [\tau]}\ (\textsc{V-Index})$$

$$\frac{a \sim \tau}{|a \sim [\tau]}\ (\textsc{V-Map})$$

I made a stronger claim here so that the V-Map part can be proved clearly. The idea is that any object with the same type can be accessed in the same way.

(Strong) Accessor safety: for all a, τ such that $a \sim \tau$, there exists accessors $a_1, a_2, \dots, a_k$ such that $a_1 = a, a_k = \varepsilon$ and for all $j \sim \tau$, then there exists objects $j_1, j_2, \dots, j_k$ such that $j_1 = j$,

$$(a_1, j_1) \mapsto (a_2, j_2) \mapsto \dots \mapsto (a_k, j_k). \tag{1}$$

Proof.

1. If $a = \varepsilon$, by V-Terminate, for all τ, $a \sim \tau$.

   For every j, define $a_1 = a = \varepsilon, j_1 = j$. Because $(a, j) = (a_1, j_1) = (\varepsilon, j_1)$, therefore the theorem holds for $a = \varepsilon$.

2. Suppose that $a = .s'a'$, $a' \sim \tau'$, there exists accessors $a_1, a_2, \dots, a_k$ such that $a_1 = a', a_k = \varepsilon$ and for all $j \sim \tau'$, there exists objects $j_1, j_2, \dots, j_k$ such that $j_1 = j$ and equation (1) holds.

   By V-Dict, $a \sim \{s' : \tau', \dots\}$ (which means $a \sim \{(s : \tau)^*\}$ such that $s' \in s$ and $\tau_{s'} = \tau'$).

   For all $j \sim \{s' : \tau', \dots\}$, by inversion lemma and S-Dict, $j = \{(s : j)^*\}$ and $j_{s'} \sim \tau_{s'} = \tau'$.

   Because $j_{s'} \sim \tau'$, by inductive hypothesis, there exists objects $j_{s'}^{(1)}, j_{s'}^{(2)}, \dots, j_{s'}^{(k)}$ such that $j_{s'} = j_{s'}^{(1)}$,

   $$(a_1, j_{s'}^{(1)}) \mapsto (a_2, j_{s'}^{(2)}) \mapsto \dots \mapsto (a_k, j_{s'}^{(k)}).$$

   Because $j = \{(s : j)^*\}$, $s' \in s$, by A-Dict, $(a, j) \mapsto (a', j_{s'}) = (a_1, j_{s'}^{(1)})$.

   Therefore the theorem holds for $a = .s'a'$ where $a, a_1, a_2, \dots, a_k$ described above is the set of accessors that satisfies the condition.

3. Suppose that $a = [n]a'$, $a' \sim \tau'$, and for all $j \sim \tau'$, there exists accessors $a_1, a_2, \ldots, a_k$ such that $a_1 = a', a_k = \varepsilon$ and for all $j \sim \tau'$, then there exists objects $j_1, j_2, \ldots, j_k$ such that $j_1 = j$ and equation (1) holds.

   By V-Index, $a \sim [\tau']$.

   For all $j \sim [\tau']$, by inversion lemma and S-List, $j = [\ldots, j_n, \ldots]$ and $j_n \sim \tau'$.

   By inductive hypothesis, there exists objects $j_n^{(1)}, j_n^{(2)}, \ldots, j_n^{(k)}$ such that $j_n = j_n^{(1)}$,

   $$(a_1, j_n^{(1)}) \mapsto (a_2, j_n^{(2)}) \mapsto \ldots \mapsto (a_k, j_n^{(k)}).$$

   Because $j = [\ldots, j_n, \ldots]$, by A-Index, $(a, j) \mapsto (a', j_n) = (a_1, j_n^{(1)})$.

   Therefore the theorem holds for $a = [n]a'$ where $a, a_1, a_2, \ldots, a_k$ described above is the set of accessors that satisfies the condition.

4. Suppose that $a = |a'$, $a' \sim \tau'$, there exists accessors $a_1, a_2, \ldots, a_k$ such that $a_1 = a', a_k = \varepsilon$ and for all $j \sim \tau'$, then there exists objects $j_1, j_2, \ldots, j_k$ such that $j_1 = j$ and equation (1) holds.

   We claim that $|a_1, |a_2, \ldots, |a_k, \varepsilon$ is the accessors that makes the theorem hold for $a = |a'$.

   By V-Map, $a \sim [\tau']$. For every $j \sim [\tau']$, we need to find the objects $j^{(1)}, j^{(2)}, \ldots, j^{(k+1)}$ such that

   $$(a, j) = (|a_1, j^{(1)}) \mapsto (|a_2, j^{(2)}) \mapsto \ldots \mapsto (|a_k, j^{(k)}) \mapsto (\varepsilon, j^{(k+1)}). \tag{2}$$

   By inductive hypothesis, for all n, there exists objects $j_n^{(1)}, j_n^{(2)}, \ldots, j_n^{(k)}$ such that $j_n = j_n^{(1)}$,

   $$(a_1, j_n^{(1)}) \mapsto (a_2, j_n^{(2)}) \mapsto \ldots \mapsto (a_k, j_n^{(k)}).$$

   Let

   $$j^{(1)} = [\ldots, j_n^{(1)}, \ldots], \quad j^{(2)} = [\ldots, j_n^{(2)}, \ldots], \quad \ldots \quad j^{(k)} = j^{(k+1)} = [\ldots, j_n^{(k)}, \ldots],$$

   then by A-Map, $(a_i, j_n^{(i)}) \mapsto (a_{i+1}, j_n^{(i+1)})$ implies $(|a_i, j^{(i)}) \mapsto (|a_{i+1}, j^{(i+1)})$. Therefore

   $$(|a_1, j^{(1)}) \mapsto (|a_2, j^{(2)}) \mapsto \ldots \mapsto (|a_k, j^{(k)}).$$

   Because $a_k = \varepsilon$, by A-Map-Empty, $(|a_k, j^{(k)}) \mapsto (\varepsilon, j^{(k)}) = (\varepsilon, j^{(k+1)})$.

   Because $j_n = j_n^{(1)}$, therefore $j = [\ldots, j_n, \ldots] = [\ldots, j_n^{(1)}, \ldots] = j^{(1)}$. Therefore the $j^{(i)}$ satisfies equation (2). □