Assignment 1

He Anyang

Problem 1

Part 1:

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

Part 2:

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

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

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

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

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

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

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

Problem 2

Part 1:

$$\frac{a \mapsto \varepsilon}{(a, j) \mapsto (\varepsilon, j)}\ (\textsc{A-Terminate}) \qquad \frac{a \mapsto .s'a' \quad j \mapsto \{(s : j)^*\} \quad s' \in s}{(a, j) \mapsto (a', j_{s'})}\ (\textsc{A-Dict})$$

$$\frac{a \mapsto [n]a' \quad j = [\dots, j_n, \dots]}{(a, j) \mapsto (a', j_n)}\ (\textsc{A-Index})$$

$$\frac{a \mapsto |a' \quad j = [\dots, j_n, \dots] \quad (a', j_n) \overset{*}{\mapsto} (\varepsilon, j'_n)}{(a, j) \mapsto (\varepsilon, [\dots, j'_n, \dots])}\ (\textsc{A-Map})$$

Part 2:

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

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

Accessor safety: for all a, j, τ, if $a \sim \tau$ and $j \sim \tau$, then there exists a j' such that $(a, j) \overset{*}{\mapsto} (\varepsilon, j')$.

Proof.

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

   By A-Terminate, $(a, j) \mapsto (\varepsilon, j)$ holds for all $j \sim \tau$, therefore the theorem holds for $a = \varepsilon$.

2. Suppose that $a = .s'a'$, and for all a', j, τ', if $a' \sim \tau'$ and $j \sim \tau'$, then there exists j' such that $(a', j) \overset{*}{\mapsto} (\varepsilon, j')$.

   By V-Dict, $a \sim \{s' : \tau', \dots\}$ (which means $a \sim \tau''$ for all $\tau'' = \{(s : \tau)^*\}$ 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 assumption, there exists j' such that $(a', j_{s'}) \overset{*}{\mapsto} (\varepsilon, j')$.

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

3. Suppose that $a = [n]a'$, and for all a', j, τ', if $a' \sim \tau'$ and $j \sim \tau'$, then there exists j' such that $(a', j) \overset{*}{\mapsto} (\varepsilon, j')$.

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

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

By assumption, there exists j' such that $(a', j_n) \overset{*}{\mapsto} (\varepsilon, j')$.

Because $j = [\dots, j_n, \dots]$, by A-Index, $(a, j) \mapsto (a', j_n)$. Therefore $(a, j) \overset{*}{\mapsto} (\varepsilon, j')$.

4. Suppose that $a = |a'$, and for all a', j, τ', if $a' \sim \tau'$ and $j \sim \tau'$, then there exists j' such that $(a', j) \overset{*}{\mapsto} (\varepsilon, j')$.

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

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

   By assumption, for all n, exists j_n' such that $(a', j_n) \overset{*}{\mapsto} (\varepsilon, j_n')$.

   Because $j = [\dots, j_n, \dots]$, $(a', j_n) \overset{*}{\mapsto} (\varepsilon, j_n')$, by A-Map, $(a, j) \overset{*}{\mapsto} (\varepsilon, [\dots, j_n', \dots])$

$\square$