Assignment 1

Vivek Pandya (vpandya)

Problem 1

Part 1:

$$
\begin{aligned}
\textsf{NumerOperation}\ nop &::= \quad =|\neq|<|> \\
\textsf{StringOperation}\ sop &::= \quad =|\neq \\
\textsf{Property}\ p &::= \ \varepsilon \\
&\ \mid\ nop\,\textsf{n} \\
&\ \mid\ sop\,\textsf{s} \\
&\ \mid\ \textsf{p1} \vee \textsf{p2} \\
&\ \mid\ \textsf{p1} \wedge \textsf{p2} \\
\\
\textsf{bool} &::= \ true \mid false \\
\textsf{Schema}\ \tau &::= \ \textsf{number}\langle p \rangle \\
&\ \mid\ \textsf{string}\langle p \rangle \\
&\ \mid\ \textsf{bool} \\
&\ \mid\ [\,\tau\,] \\
&\ \mid\ \{(\,s : \tau\,)^{\,*}\}
\end{aligned}
$$

Part 2:

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

$$\frac{}{n \sim \textsf{number}}\ (\textsc{S-Num}) \qquad \frac{}{s \sim \textsf{string}}\ (\textsc{S-String})$$

$$\frac{(n\, nop\, n_1)}{n \sim (\textsf{number} < nop\, n_1 >)}\ (\textsc{S-Num-Property}) \qquad \frac{(s\, sop\, s_1)}{s \sim \textsf{string} < sop\, s_1 >}\ (\textsc{S-String-Property})$$

$$\frac{n \sim \textsf{number} < p1 > \quad n \sim \textsf{number} < p2 >}{n \sim \textsf{number} < p_1 \wedge p_2 >}\ (\textsc{S-Num-Property-And})$$

$$\frac{n \sim \textsf{number} < p_1 >}{n \sim \textsf{number} < p_1 \vee p_2 >}\ (\textsc{S-Num-Property-Or})$$

$$\frac{s \sim \textsf{string} < p1 > \quad s \sim \textsf{string} < p2 >}{s \sim \textsf{string} < p_1 \wedge p_2 >}\ (\textsc{S-String-Property-And})$$

$$\frac{s \sim \textsf{string} < p_1 >}{s \sim \textsf{string} < p_1 \vee p_2 >}\ (\textsc{S-String-Property-Or})$$

$$\frac{}{\{\} \sim \tau}\ (\textsc{S-Empty-Object}) \qquad \frac{}{[\,] \sim \tau}\ (\textsc{S-Empty-Array})$$

$$\frac{\forall i \in [|j|].j_i \sim \tau}{[\,j_1, ..., j_n] \sim \tau}\ (\textsc{S-Array}) \qquad \frac{\forall s^{'} \in s.j_{s'} \sim \tau}{\{(s:j)^*\} \sim \tau}\ (\textsc{S-Object})$$

Problem 2

Part 1:

$$\frac{}{(\varepsilon, j) \mapsto j} \text{(EPSILON-ACCESSOR)} \qquad \frac{s' \in s}{(.s'a, \{(s:j)^*\}) \mapsto (a : j_{s'})} \text{(KEY-ACCESSOR)}$$

$$\frac{0 \leq k \leq n}{([k]a,\ [j_0, j_1, j_2, ..., j_k, ..., j_n]) \mapsto (a, j_k)} \text{(ARRAY-ACCESSOR)}$$

$$\frac{}{(|\varepsilon, [j_0, j_1, j_2, ..., j_k, ..., j_n]) \mapsto (\varepsilon,\ [j_0, j_1, j_2, ..., j_k, ..., j_n])} \text{(MPAS-EPSILON-ACCESSOR)}$$

$$\frac{a \mapsto a' \quad \forall i \in [|j|].(a, j_i) \mapsto (a', j_i')}{(|a, [j_1, ..., j_k, ..., j_n]) \mapsto (|a', [j_1', ..., j_k', ..., j_n'])]} \text{(MAPS-ACCESSOR)}$$

Part 2:

$$\frac{}{\varepsilon \sim \tau} \text{(VALID-EPSILON-ACCESSOR)}$$

$$\frac{\{(s:j)^*\} \sim \tau \ \ s' \in s \ \ j \sim \tau' \ \ a \sim \tau'}{.s'a \sim \tau} \text{(VALID-KEY-ACCESSOR)}$$

$$\frac{[j] \sim \tau \ \ j \sim \tau' \ \ a \sim \tau'}{[n]a \sim \tau} \text{(VALID-ARRAY-ACCESSOR)}$$

$$\frac{[j] \sim \tau \ \ j \sim \tau' \ \ a \sim \tau'}{|a \sim \tau} \text{(VALID-MAPS-ACCESSOR)}$$

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. $P(a) = \forall j, \tau\ .\ a \sim \tau \wedge j \sim \tau \implies (a, j) \overset{*}{\mapsto} (\varepsilon, j')$

Now we want to prove that

$\forall a P(a) \iff P(\varepsilon) \wedge (\forall a P(a) \Rightarrow P(.sa)) \wedge (\forall a P(a) \Rightarrow P([n]a)) \wedge (\forall a P(a) \Rightarrow P(|a))$

Induction Hypothesis (IH): $\forall a P(a)\, holds\, true,\ i.e\, we\, accept\, that\, (a, j) \overset{*}{\mapsto} (\varepsilon, j')\, where\, a \sim \tau \wedge j \sim \tau$

• Let $a = \varepsilon$ then based on EPSILON-ACCESSOR rule defined in problem 2.1 it is trivial to see that accessor safety holds for ε

• Let P(.sa) if we have $.sa \sim \tau'$ then by inversion on VALID-KEY-ACCESSOR rule we know that $\tau' = (s : \tau)* \wedge a \sim \tau$

now for any $j^{''} \sim \tau^{'}$ based on KEY-ACCESSOR rule defined in problem 2.1 we have $(.sa, j^{''}) \mapsto (a, j)$ and then due to IH we can have $(a, j) \overset{*}{\mapsto} (\varepsilon, j^{'})$ thus $(.sa, j^{''}) \overset{*}{\mapsto} (\varepsilon, j^{'})$

• Let P([n]a) if we have $[n]a \sim \tau^{'}$ then by inversion on VALID-ARRAY-ACCESSOR rule we know that $\tau^{'} = [\tau] \wedge a \sim \tau$

now for any $j^{''} \sim \tau^{'}$ based on ARRAY-ACCESSOR rule defined in problem 2.1 we have $([n]a, j^{''}) \mapsto (a, j)$ and then due to IH we can have $(a, j) \overset{*}{\mapsto} (\varepsilon, j^{'})$ thus $([n]a, j^{''}) \overset{*}{\mapsto} (\varepsilon, j^{'})$

• Let P(|a) if we have $|a \sim \tau^{'}$ then by inversion on VALID-MAPS-ACCESSOR rule we know that $\tau^{'} = [\tau] \wedge a \sim \tau$

now for any $j^{''} \sim \tau^{'}$ based on MAPS-ACCESSOR rule defined in problem 2.1 we have $(|a, j^{''}) \mapsto (|a^{'}, j)$ now based on IH we can assume $a^{'}$ is safe accessor on j by using MAPS-ACCESSOR and MAPS-EPSILON-ACCESSOR as required (each time for next accessor IH holds true) and then we can have $(|a^{'}, j) \overset{*}{\mapsto} (\varepsilon, j^{'})$ thus $(|a, j^{''}) \overset{*}{\mapsto} (\varepsilon, j^{'})$

Thus for all cases accessor safety holds.

$\square$