1 Typing Rules

Changed SS8.

1.1 Expression Typing $(C \vdash e : \tau)$

$$\text{SS0}\ \frac{C \vdash \tau \qquad \Gamma(x) = \tau}{C \vdash x : \tau}$$

$$\text{SS1}\ \frac{}{C \vdash n : \text{int}}$$

$$\text{SS2}\ \frac{C \vdash e1 : \text{int} \qquad C \vdash e2 : \text{int}}{C \vdash e1\ op\ e2 : \text{int}}$$

$$\text{SS3}\ \frac{C \vdash \tau \qquad \tau \neq \text{handle}(\rho', \tau')}{C \vdash Uninit : \tau}$$

$$\text{SS4}\ \frac{C \vdash e : \tau * \rho \qquad \Delta(\rho) = \tau \qquad \tau \notin \{Unknown, \text{char}\}}{C \vdash \text{load } e : \tau}$$

$$\text{SS5}\ \frac{C \vdash e : \tau * \rho \qquad \Delta(\rho) = Unknown \qquad C \vdash x : \text{handle}(\rho, Unknown)}{C \vdash \text{loadFromU } x, e : \text{int}}$$

$$\text{SS5CHAR}\ \frac{C \vdash e : \tau * \rho \qquad \Delta(\rho) = Unknown \qquad C \vdash x : \text{handle}(\rho, Unknown)}{C \vdash \text{loadcFromU } x, e : \text{char}}$$

$$\text{SS6}\ \frac{\Delta(\rho) = \tau \qquad C \vdash x : \text{handle}(\rho, \tau) \qquad C \vdash e : \text{int}}{C \vdash \text{poolalloc}(x, e) : \tau * \rho}$$

$$\text{SS7}\ \frac{\Delta(\rho) = \tau \qquad C \vdash x : \text{handle}(\rho, \tau) \qquad C \vdash e : \text{int}}{C \vdash \text{castint2ptr } x, e \text{ to } \tau * \rho : \tau * \rho}$$

$$\text{SS8}\ \frac{C \vdash \tau' * \rho \qquad C \vdash e : \tau * \rho}{C \vdash \text{cast } e \text{ to } \tau' * \rho : \tau' * \rho}$$

$$\text{SS9}\ \frac{\Delta(\rho) = \tau \qquad C \vdash x : \text{handle}(\rho, \tau) \qquad C \vdash e2 : \tau * \rho \qquad C \vdash e3 : \text{int}}{C \vdash x, \&e2[e3] : \tau * \rho}$$

$$\text{SS10}\ \frac{C \vdash e : \tau \qquad \tau \neq \text{handle}(\rho, \tau')}{C \vdash \text{cast } e \text{ to int} : \text{int}}$$

1.2 Statement Typing $(C \vdash s)$

$$\text{SS11}\ \frac{}{C \vdash \epsilon}$$

$$\text{SS12}\ \frac{C \vdash s1 \qquad C \vdash s2}{C \vdash s1; s2}$$

$$\text{SS13}\ \frac{C \vdash x : \tau \qquad C \vdash e : \tau}{C \vdash x = e}$$

$$\text{SS14}\ \frac{\Delta(\rho) = \tau \qquad C \vdash e1 : \tau * \rho \qquad C \vdash e2 : \tau \qquad \tau \notin \{Unknown, \text{char}\}}{C \vdash \text{store } e2, e1}$$

$$\text{SS14CHAR}\ \frac{\Delta(\rho) = \text{char} \qquad C \vdash e1 : \tau * \text{char} \qquad C \vdash e2 : \text{char}}{C \vdash \text{storec } e2, e1}$$

$$\text{SS15}\ \frac{\Delta(\rho) = Unknown \qquad C \vdash e1 : \tau * \rho \qquad C \vdash e2 : \tau \qquad C \vdash x : \text{handle}(\rho, Unknown)}{C \vdash \text{storeToU}x, e2, e1}$$

$$\text{SS15CHAR}\ \frac{\Delta(\rho) = Unknown \qquad C \vdash e1 : \tau * \rho \qquad C \vdash e2 : \text{char} \qquad C \vdash x : \text{handle}(\rho, Unknown)}{C \vdash \text{storecToU}x, e2, e1}$$

$$\text{SS16}\ \frac{\Delta(\rho) = \tau \qquad C \vdash x : \text{handle}(\rho, \tau) \qquad C \vdash e2 : \tau * \rho}{C \vdash \text{poolfree}(x, e2)}$$

$$\text{SS17}\ \frac{C \vdash \tau \qquad \Gamma[x \mapsto \text{handle}(\rho, \tau)], \Delta[\rho \mapsto \tau] \vdash s \qquad x \notin \Gamma \qquad \rho \notin \Delta}{C(= \Gamma, \Delta) \vdash \text{poolinit}(\rho, \tau)x\{s\}}$$

1.3 Type Typing $(C \vdash \tau)$

Got rid of SS20 and wrote it directly in all of the rules. Also changed SS21, SS22 and SS23.

SS18 $\dfrac{}{C \vdash \text{int}}$

SS19 $\dfrac{}{C \vdash Unknown}$

SS21 $\dfrac{\Delta(\rho) = \tau \qquad C \vdash \tau}{C \vdash \tau * \rho}$

SS22 $\dfrac{\Delta(\rho) = Unknown \qquad C \vdash \tau}{C \vdash \tau * \rho}$

SS23 $\dfrac{\Delta(\rho) = \tau \qquad C \vdash \tau}{C \vdash \text{handle}(\rho, \tau)}$

2 References

[1] Dinakar Dhurjati, Sumant Kowshik, and Vikram Adve. *SAFECode: Enforcing Alias Analysis for Weakly Typed Languages*. PLDI, June 2006.