`salt4`: Boxes

`CS392-M1`: *Rust, In Practice and in Theory*

Syntax

x	(variables, $\mathcal{V}$)
n	(integers, $\mathbb{Z}$)
$w ::= x \mid \texttt{*}\ w$	(place expression, $\mathcal{W}$)
$e ::= \texttt{()} \mid n \mid \texttt{copy}\ w \mid w \mid \texttt{\&}\ w \mid \texttt{\&mut}\ w \mid w\ \texttt{=}\ e \mid \texttt{\{}\ p\ \texttt{\}} \mid \texttt{box}\ e$	(expressions, $\mathcal{E}$)
$s ::= \texttt{let}\ x\ \texttt{=}\ e \mid \texttt{let mut}\ x\ \texttt{=}\ e \mid e$	(statements, $\mathcal{S}$)
$p ::= e \mid s\ \texttt{;}\ p$	(programs, $\mathcal{P}$)

Typing

$$
\begin{array}{lr}
l & \text{(lifetimes, Lt)} \\
t ::= \texttt{()} \mid \texttt{i32} \mid \texttt{\&}\, w \mid \texttt{\&mut}\, w \mid \square\, t & \text{(types, } \mathcal{T}\text{)} \\
\tilde{t} ::= \lfloor t \rfloor \mid t \mid \square\, \tilde{t} & \text{(partial types, } \tilde{\mathcal{T}}\text{)} \\
m ::= \mathsf{imm} \mid \mathsf{mut} & \text{(mutability)} \\
u ::= \langle \tilde{t} \rangle_l^m & \text{(slot types, } \mathrm{S}_{\mathcal{T}}\text{)}
\end{array}
$$

$$
\Gamma \in \mathcal{V} \mapsto \mathrm{S}_{\mathcal{T}} \qquad \text{(contexts)}
$$

$$
\begin{array}{lr}
\mathsf{copyable}(t) & \text{(copyability)} \\
\Gamma \vdash \mathsf{readable}(w) & \text{(readability)} \\
\Gamma \vdash \mathsf{writable}(w) & \text{(writability)} \\
\Gamma \vdash \mathsf{mutable}(w) & \text{(mutability)} \\
\Gamma \vdash \tilde{t} \approx \tilde{t} & \text{(type compatibility)} \\
\Gamma \vdash \tilde{t} : l & \text{(lifetimes)} \\
\Gamma \vdash w : u & \text{(place expressions)} \\
\Gamma \vdash \langle e : t \rangle_l \dashv \Gamma & \text{(expressions)} \\
\Gamma \vdash \langle s \rangle_l \dashv \Gamma & \text{(statments)} \\
\Gamma \vdash \langle p : t \rangle_l \dashv \Gamma & \text{(programs)}
\end{array}
$$

$$\frac{(x \mapsto \langle \tilde{t} \rangle_l^m) \in \Gamma}{\Gamma \vdash x : \langle \tilde{t} \rangle_l^m}\ \textsc{var} \qquad \frac{\Gamma \vdash w : \langle \texttt{\&}\ x \rangle_{l_1}^{m_1} \qquad \Gamma \vdash x : \langle \tilde{t} \rangle_{l_2}^{m_2}}{\Gamma \vdash * w : \langle \tilde{t} \rangle_{l_2}^{m_2}}\ \textsc{deref}$$

$$\frac{\Gamma \vdash w : \langle \texttt{\&mut}\ x \rangle_{l_1}^{m_1} \qquad \Gamma \vdash x : \langle \tilde{t} \rangle_{l_2}^{m_2}}{\Gamma \vdash * w : \langle \tilde{t} \rangle_{l_2}^{m_2}}\ \textsc{mutDeref} \qquad \frac{\Gamma \vdash w : \langle \square\ \tilde{t} \rangle_l^m}{\Gamma \vdash * w : \langle \tilde{t} \rangle_l^m}\ \textsc{box}$$

$$\frac{}{\Gamma \vdash \langle \texttt{()} : \texttt{()} \rangle_l \dashv \Gamma}\ \textsc{unit} \qquad \frac{n \in \mathbb{Z}}{\Gamma \vdash \langle n : \texttt{i32} \rangle_l \dashv \Gamma}\ \textsc{int} \qquad \frac{\nexists y, j.(y \mapsto \langle \texttt{\&mut}\ *^j x \rangle_l^m) \in \Gamma}{\Gamma \vdash \mathsf{readable}(*^k x)}\ \textsc{readable}$$

$$\frac{}{\mathsf{copyable}\ (\texttt{()})}\ \textsc{copyUnit} \qquad \frac{}{\mathsf{copyable}\ (\texttt{i32})}\ \textsc{copyInt} \qquad \frac{}{\mathsf{copyable}\ (\texttt{\&}\ w)}\ \textsc{copyRef}$$

$$\frac{\Gamma \vdash w : \langle t \rangle_{l_1}^m \qquad \Gamma \vdash \mathsf{readable}(w) \qquad \mathsf{copyable}\ (t)}{\Gamma \vdash \langle \mathsf{copy}\ w : t \rangle_{l_2} \dashv \Gamma}\ \textsc{placeCopy}$$

$$\frac{\Gamma \vdash \mathsf{readable}(*^k x) \qquad \nexists y, j.(y \mapsto \langle \texttt{\&}\ *^j x \rangle_l^m) \in \Gamma}{\Gamma \vdash \mathsf{writable}(*^k x)}\ \textsc{writable}$$

$$\mathsf{move}(\Gamma, x) = \Gamma[x \mapsto \langle \lfloor t \rfloor \rangle_l^m] \qquad \text{where} \qquad (x \mapsto \langle t \rangle_l^m) \in \Gamma$$

$$\mathsf{move}(\Gamma, *^{k+1} x) =$$

$$\frac{\Gamma \vdash w : \langle t \rangle^{m}_{l_1} \qquad \Gamma \vdash \mathsf{writable}(w)}{\Gamma \vdash \langle w : t \rangle_{l_2} \dashv \mathsf{move}(\Gamma, w)}\ \textsc{placeMove}$$

$$\frac{\Gamma \vdash x : \langle \texttt{\&mut}\ w \rangle^{m}_{l_1} \qquad \Gamma \vdash \mathsf{writable}(x)}{\Gamma \vdash \langle x : \texttt{\&mut}\ w \rangle_{l_2} \dashv \Gamma[x \mapsto \langle \lfloor \texttt{\&mut}\ w \rfloor \rangle^{m}_{l_1}]}\ \textsc{placeMove} \qquad \frac{\Gamma \vdash w : \langle t \rangle^{m}_{l_1} \qquad \Gamma \vdash \mathsf{readable}(w)}{\Gamma \vdash \langle \texttt{\&}\ w : \texttt{\&}\ w \rangle_{l_2} \dashv \Gamma}\ \textsc{ref}$$

$$\frac{(x \mapsto \langle t \rangle^{\mathsf{mut}}_{l}) \in \Gamma}{\Gamma \vdash \mathsf{mutable}(x)}\ \textsc{mutVar} \qquad \frac{(x \mapsto \langle \texttt{\&mut}\ w \rangle^{m}_{l}) \in \Gamma \qquad \Gamma \vdash \mathsf{mutable}(*^{k} w)}{\Gamma \vdash \mathsf{mutable}(*^{k+1} x)}\ \textsc{mutDeref}$$

$$\frac{\Gamma \vdash w : \langle t \rangle^{\mathsf{mut}}_{l_1} \qquad \Gamma \vdash \mathsf{writable}(w) \qquad \Gamma \vdash \mathsf{mutable}(w)}{\Gamma \vdash \langle \texttt{\&mut}\ w : \texttt{\&mut}\ w \rangle_{l_2} \dashv \Gamma}\ \textsc{mutRef} \qquad \frac{}{\Gamma \vdash \texttt{()} \approx \texttt{()}}\ \approx\textsc{-unit}$$

$$\frac{}{\Gamma \vdash \texttt{i32} \approx \texttt{i32}}\ \approx\textsc{-int} \qquad \frac{\Gamma \vdash w_1 : \langle \tilde{t}_1 \rangle^{m_1}_{l_1} \qquad \Gamma \vdash w_2 : \langle \tilde{t}_2 \rangle^{m_2}_{l_2} \qquad \Gamma \vdash \tilde{t}_1 \approx \tilde{t}_2}{\Gamma \vdash \texttt{\&}\ w_1 \approx \texttt{\&}\ w_2}\ \approx\textsc{-ref}$$

$$\frac{\Gamma \vdash w_1 : \langle \tilde{t}_1 \rangle^{m_1}_{l_1} \qquad \Gamma \vdash w_2 : \langle \tilde{t}_2 \rangle^{m_2}_{l_2} \qquad \Gamma \vdash \tilde{t}_1 \approx \tilde{t}_2}{\Gamma \vdash \texttt{\&mut}\ w_1 \approx \texttt{\&mut}\ w_2}\ \approx\textsc{-mutRef} \qquad \frac{\Gamma \vdash \tilde{t}_1 \approx \tilde{t}_2}{\Gamma \vdash \Box\, \tilde{t}_1 \approx \Box\, \tilde{t}_2}\ \approx\textsc{-box}$$

$$\frac{\Gamma \vdash t_1 \approx \tilde{t}_2}{\Gamma \vdash \lfloor t_1 \rfloor \approx \tilde{t}_2}\ \approx\textsc{-partial}_1 \qquad \frac{\Gamma \vdash \tilde{t}_1 \approx t_2}{\Gamma \vdash \tilde{t}_1 \approx \lfloor t_2 \rfloor}\ \approx\textsc{-partial}_2$$

$$\begin{aligned}
\mathsf{write}(\Gamma, x, t) &= \Gamma[x \mapsto \langle t \rangle^{m}_{l}] \quad \text{where} \quad (x \mapsto \langle \cdot \rangle^{m}_{l}) \in \Gamma \\
\mathsf{write}(\Gamma, *^{k+1} x, t) &= \mathsf{write}(\Gamma, *^{k} w, t) \quad \text{where} \quad (x \mapsto \langle \texttt{\&mut}\ w \rangle^{m}_{l}) \in \Gamma
\end{aligned}$$

$$\begin{aligned}
\mathsf{replace}(\texttt{\&}\ *^{k+1} w_1, w_1, \texttt{\&}\ w_2) &= \texttt{\&}\ *^{k} w_2 \\
\mathsf{replace}(\texttt{\&}\ *^{k+1} w_1, w_1, \texttt{\&mut}\ w_2) &= \texttt{\&}\ *^{k} w_2 \\
\mathsf{replace}(\texttt{\&mut}\ *^{k+1} w_1, w_1, \texttt{\&}\ w_2) &= \texttt{\&mut}\ *^{k} w_2 \\
\mathsf{replace}(\texttt{\&mut}\ *^{k+1} w_1, w_1, \texttt{\&mut}\ w_2) &= \texttt{\&mut}\ *^{k} w_2 \\
\mathsf{replace}(t_1, w, t_2) &= t_1 \\
\mathsf{replace}(\lfloor t_1 \rfloor, w, t_2) &= \lfloor \mathsf{replace}(t_1, w, t_2) \rfloor \\
\mathsf{replace}(\Gamma, w, t_2) &= \{x \mapsto \langle \mathsf{replace}(\tilde{t}_1, w, t_2) \rangle^{m}_{l} : (x \mapsto \langle \tilde{t}_1 \rangle^{m}_{l}) \in \Gamma\}
\end{aligned}$$

$$\mathsf{update}(\Gamma, w, t_2) = \mathsf{replace}(\mathsf{write}(\Gamma, w, t_2), w, t_2)$$

$$\mathsf{drop}(\Gamma, l) = \Gamma \setminus \{x \mapsto \langle \tilde{t} \rangle^{m}_{l} : (x \mapsto \langle \tilde{t} \rangle^{m}_{l}) \in \Gamma\}$$

$$\frac{}{\Gamma \vdash \texttt{i32} : l}\ \textsc{IntLftm} \qquad \frac{G \vdash w : \langle t \rangle^{m}_{l_1} \qquad l_1 \leq l_2}{\Gamma \vdash \texttt{\&}\, w : l_2}\ \textsc{RefLtfm}$$

$$\frac{\Gamma \vdash w : \langle t \rangle^{m}_{l_1} \qquad l_1 \leq l_2}{\Gamma \vdash \texttt{\&mut}\, w : l_2}\ \textsc{MutRefLftm} \qquad \frac{\Gamma \vdash t : l}{\Gamma \vdash \Box\, t : l}\ \textsc{BoxLftm}$$

$$\frac{\begin{array}{c}\Gamma_1 \vdash w : \langle \tilde{t}_1 \rangle^{\mathsf{mut}}_{l_1} \qquad \Gamma_1 \vdash e : t_2 \dashv \Gamma_2 \qquad \Gamma_2 \vdash \tilde{t}_1 \approx t_2 \\ \Gamma_2 \vdash t_2 : l_1 \qquad \Gamma_3 = \mathsf{update}(\Gamma, w, t_2) \qquad \Gamma_3 \vdash \mathsf{writable}(w)\end{array}}{\Gamma_1 \vdash \langle w \texttt{ = } e : \texttt{()} \rangle_{l_2} \dashv \Gamma_3}\ \textsc{Assign}$$

$$\frac{\Gamma_1 \vdash \langle p : t \rangle_{l+1} \dashv \Gamma_2 \qquad \Gamma_2 \vdash t : l}{\Gamma_1 \vdash \langle \{\ p\ \} : t \rangle_l \dashv \mathsf{drop}(\Gamma_2, l+1)}\ \textsc{Block} \qquad \frac{\Gamma_1 \vdash \langle e : t \rangle_l \dashv \Gamma_2 \qquad x \notin \mathrm{dom}(\Gamma_2)}{\Gamma_1 \vdash \langle \texttt{let}\ x \texttt{ = } e \rangle_l \dashv \Gamma_2[x \mapsto \langle t \rangle^{\mathsf{imm}}_l]}\ \textsc{Let}$$

$$\frac{\Gamma_1 \vdash \langle e : t \rangle_l \dashv \Gamma_2 \qquad x \notin \mathrm{dom}(\Gamma_2)}{\Gamma_1 \vdash \langle \texttt{let mut}\ x \texttt{ = } e \rangle_l \dashv \Gamma_2[x \mapsto \langle t \rangle^{\mathsf{mut}}_l]}\ \textsc{LetMut} \qquad \frac{\Gamma_1 \vdash \langle e : t \rangle_l \dashv \Gamma_2}{\Gamma_1 \vdash \langle e \rangle_l \dashv \Gamma_2}\ \textsc{ExprStmt}$$

$$\frac{\Gamma_1 \vdash \langle s \rangle_l \dashv \Gamma_2 \qquad \Gamma_2 \vdash \langle p : t \rangle_l \dashv \Gamma_3}{\Gamma_1 \vdash \langle s\ \texttt{;}\ p : t \rangle_l \dashv \Gamma_3}\ \textsc{Prog}$$

Evaluation

$$
\begin{array}{rr}
\ell ::= \ell_x & \text{(locations, } \mathcal{L}\text{)} \\
v ::= () \mid n \mid \ell & \text{(values, } \mathbb{V}\text{)} \\
\tilde{v} ::= \bot \mid v & \text{(partial values, } \tilde{\mathbb{V}}\text{)} \\
r ::= \langle \tilde{v} \rangle_l & \text{(slot types, } \mathbb{S}_{\mathbb{V}}\text{)}
\end{array}
$$

$$
S \in \mathcal{L} \mapsto \mathbb{S}_{\mathbb{V}} \qquad \text{(store)}
$$

$$
\begin{array}{rr}
S \vdash \langle e \Downarrow v \rangle_l \dashv S & \text{(expressions)} \\
S \vdash \langle s \rangle_l \dashv S & \text{(statements)} \\
S \vdash \langle p \Downarrow v \rangle_l \dashv S & \text{(programs)}
\end{array}
$$

$$\frac{}{S \vdash x \rightsquigarrow \ell_x}\ \textsc{locVar} \qquad \frac{S \vdash w \rightsquigarrow \ell_x \qquad (\ell_x \mapsto \langle \ell_y \rangle_l) \in S}{S \vdash \texttt{*}\, w \rightsquigarrow \ell_y}\ \textsc{locDeref}$$

$$\frac{}{S \vdash \langle \texttt{()} \Downarrow \texttt{()} \rangle_l \dashv S}\ \textsc{unit} \qquad \frac{n \in \mathbb{Z}}{S \vdash \langle n \Downarrow n \rangle_l \dashv S}\ \textsc{int}$$

$$\frac{S \vdash w \rightsquigarrow \ell_x \qquad (\ell_x \mapsto \langle v \rangle_{l_1}) \in S}{S \vdash \langle \mathsf{copy}\ w \Downarrow v \rangle_{l_2} \dashv S}\ \textsc{placeCopy} \qquad \frac{S \vdash w \rightsquigarrow \ell_x \qquad (\ell_x \mapsto \langle v \rangle_{l_1}) \in S}{S \vdash \langle w \Downarrow v \rangle_{l_2} \dashv S[\ell_x \mapsto \langle \bot \rangle_{l_1}]}\ \textsc{move}$$

$$\frac{S \vdash w \rightsquigarrow \ell_x}{S \vdash \langle \texttt{\&}\, w \Downarrow \ell_x \rangle_l \dashv S}\ \textsc{ref} \qquad \frac{S \vdash w \rightsquigarrow \ell_x}{S \vdash \langle \texttt{\&mut}\ w \Downarrow \ell_x \rangle_l \dashv S}\ \textsc{mutRef}$$

$$\frac{S \vdash w \rightsquigarrow \ell_x \qquad (\ell_x \mapsto \langle \tilde{v} \rangle_{l_1}) \in S_1 \qquad S_1 \vdash \langle e \Downarrow v \rangle_{l_2} \dashv S_2}{S_1 \vdash \langle w \texttt{ = } e \Downarrow \texttt{()} \rangle_{l_2} \dashv S_2[\ell_x \mapsto \langle v \rangle_{l_1}]}\ \textsc{assign}$$

$$\mathsf{drop}(S, l) = S \setminus \{\ell \mapsto \langle \tilde{v} \rangle_l : (\ell \mapsto \langle \tilde{v} \rangle_l) \in S\}$$

$$\frac{S_1 \vdash \langle p \Downarrow v \rangle_{l+1} \dashv S_2}{S_1 \vdash \{\ p\ \} \Downarrow v \dashv \mathsf{drop}(S_2, l+1)}\ \textsc{block} \qquad \frac{S_1 \vdash \langle e \Downarrow v \rangle_l \dashv S_2}{S_1 \vdash \langle \texttt{let}\ x \texttt{ = } e \rangle_l \dashv S_2[\ell_x \mapsto \langle v \rangle_l]}\ \textsc{let}$$

$$\frac{S_1 \vdash \langle e \Downarrow v \rangle \dashv S_2}{S_1 \vdash \langle \texttt{let mut}\ x \texttt{ = } e \rangle \dashv S_2[\ell_x \mapsto \langle v \rangle_l]}\ \textsc{letMut} \qquad \frac{S_1 \vdash \langle e \Downarrow v \rangle_l \dashv S_2}{S_1 \vdash \langle e \rangle_l \dashv S_2}\ \textsc{exprStmt}$$

$$\frac{S_1 \vdash \langle s \rangle_l \dashv S_2 \qquad S_2 \vdash \langle p \Downarrow v \rangle_l \dashv S_3}{S_1 \vdash \langle s\ \texttt{;}\ p \Downarrow v \rangle_l \dashv S_3}\ \textsc{prog}$$