

salt2: Mutable References

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

Syntax

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

Typing

$t ::= (\textcolor{red}{\circ}) \mid \textcolor{red}{i32} \mid \& w \mid \&\text{mut} w$	(types, \mathcal{T})
$\tilde{t} ::= \lfloor t \rfloor \mid t$	(partial types, $\tilde{\mathcal{T}}$)
$m ::= \text{imm} \mid \text{mut}$	(mutability)
$u ::= \langle \tilde{t} \rangle^m$	(slot types, $\mathbb{S}_{\mathcal{T}}$)
$\Gamma \in \mathcal{V} \mapsto \mathbb{S}_{\mathcal{T}}$	(contexts)
$\text{copyable}(t)$	(copyability)
$\Gamma \vdash w : u$	(place expressions)
$\Gamma \vdash \text{readable}(w)$	(readability)
$\Gamma \vdash \text{writable}(w)$	(writability)
$\Gamma \vdash \tilde{t} \approx \tilde{t}$	(type compatibility)
$\Gamma \vdash e : t \dashv \Gamma$	(expressions)
$\Gamma \vdash s \dashv \Gamma$	(statements)
$\Gamma \vdash p : t \dashv \Gamma$	(programs)
$\frac{(x \mapsto \langle \tilde{t} \rangle^m) \in \Gamma}{\Gamma \vdash x : \langle \tilde{t} \rangle^m} \text{ (var)}$	
$\frac{\Gamma \vdash w_1 : \& w_2^{m_1} \quad \Gamma \vdash w_2 : t^{m_2}}{\Gamma \vdash * w_1 : t^{m_2}} \text{ (deref)}$	
$\frac{}{\Gamma \vdash (\textcolor{red}{\circ}) : (\textcolor{red}{\circ}) \dashv \Gamma} \text{ (unit)}$	
$\frac{n \in \mathbb{Z}}{\Gamma \vdash n : \textcolor{red}{i32} \dashv \Gamma} \text{ (int)}$	
$\frac{\#y, l. (y \mapsto \&\text{mut} *^l x) \in \Gamma}{\Gamma \vdash \text{readable}(*^k x)} \text{ (readable)}$	
$\frac{}{\text{copyable}(\textcolor{red}{\circ})} \text{ (copy-unit)}$	

$$\begin{array}{c}
\frac{}{\text{copyable}(\text{i32})} \text{ (copy-int)} \\
\frac{}{\text{copyable}(\& w)} \text{ (copy-brw)} \\
\frac{\Gamma \vdash w : \langle t \rangle^m \quad \Gamma \vdash \text{readable}(w) \quad \text{copyable}(t)}{\Gamma \vdash \text{copy } w : t \dashv \Gamma} \text{ (place-copy)} \\
\frac{\Gamma \vdash \text{readable}(*^k x) \quad \nexists y, l. (y \mapsto \& *^l x) \in \Gamma}{\Gamma \vdash \text{writable}(*^k x)} \text{ (writable)} \\
\frac{\Gamma \vdash x : \langle \&\text{mut } w \rangle^m \quad \Gamma \vdash \text{writable}(x)}{\Gamma \vdash x : \&\text{mut } w \dashv \Gamma[x \mapsto \lfloor \&\text{mut } w \rfloor]} \text{ (place-move)} \\
\frac{\Gamma \vdash w : \langle t \rangle^m \quad \Gamma \vdash \text{readable}(w)}{\Gamma \vdash \& w : \& w \dashv \Gamma} \text{ (brw)} \\
\frac{\Gamma \vdash w : \langle t \rangle^{\text{mut}} \quad \Gamma \vdash \text{writable}(w) \quad \Gamma \vdash \text{mutable}(w)}{\Gamma \vdash \&\text{mut } w : \&\text{mut } w \dashv \Gamma} \text{ (mut-brw)} \\
\frac{}{\Gamma \vdash \text{i32} \approx \text{i32}} \text{ (\approx-int)} \\
\frac{}{\Gamma \vdash () \approx ()} \text{ (\approx-unit)} \\
\frac{\Gamma \vdash w_1 : \tilde{t}_1^m \quad \Gamma \vdash w_2 : \tilde{t}_2^m \quad \Gamma \vdash \tilde{t}_1 \approx \tilde{t}_2}{\Gamma \vdash \& w_1 \approx \& w_2} \text{ (\approx-brw)} \\
\frac{\Gamma \vdash w_1 : \tilde{t}_1^m \quad \Gamma \vdash w_2 : \tilde{t}_2^m \quad \Gamma \vdash \tilde{t}_1 \approx \tilde{t}_2}{\Gamma \vdash \&\text{mut } w_1 \approx \&\text{mut } w_2} \text{ (\approx-mbrw)} \\
\frac{\Gamma \vdash t_1 \approx \tilde{t}_2}{\Gamma \vdash \lfloor t_1 \rfloor \approx \tilde{t}_2} \text{ (\approx-partial}_1\text{)} \\
\frac{\Gamma \vdash \tilde{t}_1 \approx t_2}{\Gamma \vdash \tilde{t}_1 \approx \lfloor t_2 \rfloor} \text{ (\approx-partial}_2\text{)}
\end{array}$$

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

$$\begin{aligned}
\text{replace}(\&*^{k+1} w_1, w_1, \&[\text{mut}] w_2) &= \&*^k w_2 \\
\text{replace}(\&\text{mut } *^{k+1} w_1, w_1, \&[\text{mut}] w_2) &= \&\text{mut } *^k w_2 \\
\text{replace}(t_1, w, t_2) &= t_1 \\
\text{replace}(\lfloor t_1 \rfloor, w, t_2) &= \lfloor \text{replace}(t_1, w, t_2) \rfloor \\
\text{replace}(\Gamma, w, t_2) &= \{x \mapsto \text{replace}(\tilde{t}_1, w, t_2) : (x \mapsto \tilde{t}_1) \in \Gamma\}
\end{aligned}$$

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

$$\begin{array}{c}
\frac{\Gamma_1 \vdash w : \langle \tilde{t}_1 \rangle^{\mathbf{mut}} \quad \Gamma_1 \vdash e : t_2 \dashv \Gamma_2 \quad \Gamma_2 \vdash \tilde{t}_1 \approx t_2 \quad \Gamma_3 = \mathsf{update}(\Gamma, w, t_2) \quad \Gamma_3 \vdash \mathsf{writable}(w)}{\Gamma_1 \vdash w = e : () \dashv \Gamma_3} \text{(assign)} \\[10pt]
\frac{\Gamma_1 \vdash e : t \dashv \Gamma_2}{\Gamma_1 \vdash e \dashv \Gamma_2} \text{(expr-stmt)} \\[10pt]
\frac{\Gamma_1 \vdash e : t \dashv \Gamma_2 \quad x \notin \mathsf{dom}(\Gamma_2)}{\Gamma_1 \vdash \mathsf{let}\ x = e \dashv \Gamma_2[x \mapsto t^{\mathbf{imm}}]} \text{(let)} \\[10pt]
\frac{\Gamma_1 \vdash e : t \dashv \Gamma_2 \quad x \notin \mathsf{dom}(\Gamma_2)}{\Gamma_1 \vdash \mathsf{let}\ \mathsf{mut}\ x = e \dashv \Gamma_2[x \mapsto t^{\mathbf{mut}}]} \text{(let-mut)} \\[10pt]
\frac{\Gamma_1 \vdash s \dashv \Gamma_2 \quad \Gamma_2 \vdash p : t \dashv \Gamma_3}{\Gamma_1 \vdash s ; p : t \dashv \Gamma_3} \text{(prog)}
\end{array}$$

Evaluation

$$\begin{array}{ll}
 \ell ::= \ell_x & (\text{locations}, \mathcal{L}) \\
 v ::= \textcolor{red}{\circ} \mid n \mid \ell & (\text{values}, \mathbb{V}) \\
 \tilde{v} ::= \perp \mid v & (\text{partial values}, \tilde{\mathbb{V}}) \\
 \end{array}$$

$$S \in \mathcal{L} \mapsto \tilde{\mathbb{V}} \quad (\text{store})$$

$$\begin{array}{ll}
 \langle S, e \rangle \Downarrow \langle S, v \rangle & (\text{expressions}) \\
 \langle S, s \rangle \Downarrow S & (\text{statements}) \\
 \langle S, p \rangle \Downarrow \langle S, v \rangle & (\text{programs}) \\
 \end{array}$$

$$\overline{x \rightsquigarrow \ell_x} \text{ (loc-var)}$$

$$\frac{w \rightsquigarrow \ell_x \quad (\ell_x \mapsto \ell_y) \in S}{* w \rightsquigarrow \ell_y} \text{ (loc-drf)}$$

$$\overline{\langle S, \textcolor{red}{\circ} \rangle \Downarrow \langle S, \textcolor{red}{\circ} \rangle} \text{ (unit)}$$

$$\overline{\langle S, n \rangle \Downarrow \langle S, n \rangle} \text{ (int)}$$

$$\frac{w \rightsquigarrow \ell_x \quad (\ell_x \mapsto v) \in S}{\langle S, \text{copy } w \rangle \Downarrow \langle S, v \rangle} \text{ (place-copy)}$$

$$\frac{w \rightsquigarrow \ell_x \quad (\ell_x \mapsto v) \in S}{\langle S, w \rangle \Downarrow \langle S[\ell_x \mapsto \perp], v \rangle} \text{ (move)}$$

$$\overline{\langle S, \& w \rangle \Downarrow \langle S, \ell \rangle} \text{ (brw)}$$

$$\overline{\langle S, \&\text{mut } w \rangle \Downarrow \langle S, \ell \rangle} \text{ (mut-brw)}$$

$$\begin{array}{c}
\frac{w \rightsquigarrow \ell_x \quad (\ell_x \mapsto \tilde{v}) \in S_1 \quad \langle S_1, e \rangle \Downarrow \langle S_2, v \rangle}{\langle S_1, w = e \rangle \Downarrow \langle S_2[\ell_x \mapsto v], \textcolor{red}{(_) } \rangle} \text{(assign)} \\[10pt]
\frac{\langle S_1, e \rangle \Downarrow \langle S_2, v \rangle}{\langle S_1, e \rangle \Downarrow S_2} \text{(expr-stmt)} \\[10pt]
\frac{\langle S_1, e \rangle \Downarrow \langle S_2, v \rangle}{\langle S_1, \text{let } x = e \rangle \Downarrow S_2[\ell_x \mapsto v]} \text{(let)} \\[10pt]
\frac{\langle S_1, e \rangle \Downarrow \langle S_2, v \rangle}{\langle S_1, \text{let mut } x = e \rangle \Downarrow S_2[\ell_x \mapsto v]} \text{(let-mut)} \\[10pt]
\frac{\langle S_1, e \rangle \Downarrow \langle S_2, v \rangle}{\langle S_1, e \rangle \Downarrow S_2} \text{(expr-stmt)} \\[10pt]
\frac{\langle S_1, s \rangle \Downarrow S_2 \quad \langle S_2, p \rangle \Downarrow \langle S_3, v \rangle}{\langle S_1, s ; p \rangle \Downarrow \langle S_3, v \rangle} \text{(prog)}
\end{array}$$