

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})
$e ::= () \mid n \mid \text{copy } w \mid w \mid \& w \mid \&\text{mut } w \mid w = e$	(expressions, \mathcal{E})
$s ::= \text{let } x = e \mid \text{let mut } x = e \mid e$	(statements, \mathcal{S})
$p ::= e \mid s \ ; \ p$	(programs, \mathcal{P})

Typing

$t ::= () \mid \textcolor{red}{i}32 \mid \& w \mid \textcolor{red}{\&mut} w$	(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, $\mathcal{S}_{\mathcal{T}}$)
$\Gamma \in \mathcal{V} \mapsto \mathcal{S}_{\mathcal{T}}$	(contexts)
$\text{copyable}(t)$	(copyability)
$\Gamma \vdash \text{readable}(w)$	(readability)
$\Gamma \vdash \text{writable}(w)$	(writability)
$\Gamma \vdash \tilde{t} \approx \tilde{t}$	(type compatibility)
$\Gamma \vdash w : u$	(place expressions)
$\Gamma \vdash e : t \dashv \Gamma$	(expressions)
$\Gamma \vdash s \dashv \Gamma$	(statements)
$\Gamma \vdash p : t \dashv \Gamma$	(programs)

$$\begin{array}{c}
\frac{(x \mapsto \langle t \rangle^m) \in \Gamma}{\Gamma \vdash x : \langle t \rangle^m} \text{VAR} \qquad \frac{\Gamma \vdash w : \langle \& x \rangle^{m_1} \quad \Gamma \vdash x : \langle t \rangle^{m_2}}{\Gamma \vdash * w : \langle t \rangle^{m_2}} \text{DEREF} \\
\\
\frac{\Gamma \vdash w : \langle \&\text{mut } x \rangle^{m_1} \quad \Gamma \vdash x : \langle t \rangle^{m_2}}{\Gamma \vdash * w : \langle t \rangle^{m_2}} \text{MUTDEREF} \qquad \frac{}{\Gamma \vdash () : () \dashv \Gamma} \text{UNIT} \qquad \frac{n \in \mathbb{Z}}{\Gamma \vdash n : \text{i32} \dashv \Gamma} \text{INT} \\
\\
\frac{\nexists y, l. (y \mapsto \langle \&\text{mut } *^l x \rangle^m) \in \Gamma}{\Gamma \vdash \text{readable}(*^k x)} \text{READABLE} \qquad \frac{}{\text{copyable}(())} \text{COPYUNIT} \qquad \frac{}{\text{copyable}(\text{i32})} \text{COPYINT} \\
\\
\frac{}{\text{copyable}(\& w)} \text{COPYREF} \qquad \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{PLACECOPY} \\
\\
\frac{\Gamma \vdash \text{readable}(*^k x) \quad \nexists y, l. (y \mapsto \langle \& *^l x \rangle^m) \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 \langle \&\text{mut } w \rangle^m]} \text{PLACEMOVE} \qquad \frac{\Gamma \vdash w : \langle t \rangle^m \quad \Gamma \vdash \text{readable}(w)}{\Gamma \vdash \& w : \& w \dashv \Gamma} \text{REF} \\
\\
\frac{(x \mapsto \langle t \rangle^{\text{mut}}) \in \Gamma}{\Gamma \vdash \text{mutable}(x)} \text{MUTVAR} \qquad \frac{(x \mapsto \langle \&\text{mut } w \rangle^m) \in \Gamma \quad \Gamma \vdash \text{mutable}(*^k w)}{\Gamma \vdash \text{mutable}(*^{k+1} x)} \text{MUTDEREF} \\
\\
\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{MUTREF} \qquad \frac{}{\Gamma \vdash () \approx ()} \approx\text{-UNIT} \\
\\
\frac{}{\Gamma \vdash \text{i32} \approx \text{i32}} \approx\text{-INT} \qquad \frac{\Gamma \vdash w_1 : \langle \tilde{t}_1 \rangle^{m_1} \quad \Gamma \vdash w_2 : \langle \tilde{t}_2 \rangle^{m_2} \quad \Gamma \vdash \tilde{t}_1 \approx \tilde{t}_2}{\Gamma \vdash \& w_1 \approx \& w_2} \approx\text{-REF} \\
\\
\frac{\Gamma \vdash w_1 : \langle \tilde{t}_1 \rangle^{m_1} \quad \Gamma \vdash w_2 : \langle \tilde{t}_2 \rangle^{m_2} \quad \Gamma \vdash \tilde{t}_1 \approx \tilde{t}_2}{\Gamma \vdash \&\text{mut } w_1 \approx \&\text{mut } w_2} \approx\text{-MUTREF} \qquad \frac{\Gamma \vdash t_1 \approx \tilde{t}_2}{\Gamma \vdash [t_1] \approx \tilde{t}_2} \approx\text{-PARTIAL}_1 \\
\\
\frac{\Gamma \vdash \tilde{t}_1 \approx t_2}{\Gamma \vdash \tilde{t}_1 \approx [t_2]} \approx\text{-PARTIAL}_2
\end{array}$$

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

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

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

$$\frac{\Gamma_1 \vdash w : \langle \tilde{t}_1 \rangle^{\text{mut}} \quad \Gamma_1 \vdash e : t_2 \dashv \Gamma_2 \quad \Gamma_2 \vdash \tilde{t}_1 \approx t_2 \quad \Gamma_3 = \text{update}(\Gamma, w, t_2) \quad \Gamma_3 \vdash \text{writable}(w)}{\Gamma_1 \vdash w = e : \langle \rangle \dashv \Gamma_3} \text{ ASSIGN}$$

$$\frac{\Gamma_1 \vdash e : t \dashv \Gamma_2 \quad x \notin \text{dom}(\Gamma_2)}{\Gamma_1 \vdash \text{let } x = e \dashv \Gamma_2[x \mapsto \langle t \rangle^{\text{imm}}]} \text{ LET} \qquad \frac{\Gamma_1 \vdash e : t \dashv \Gamma_2 \quad x \notin \text{dom}(\Gamma_2)}{\Gamma_1 \vdash \text{let mut } x = e \dashv \Gamma_2[x \mapsto \langle t \rangle^{\text{mut}}]} \text{ LETMUT}$$

$$\frac{\Gamma_1 \vdash e : t \dashv \Gamma_2}{\Gamma_1 \vdash e \dashv \Gamma_2} \text{ EXPRSTMT} \qquad \frac{\Gamma_1 \vdash s \dashv \Gamma_2 \quad \Gamma_2 \vdash p : t \dashv \Gamma_3}{\Gamma_1 \vdash s ; p : t \dashv \Gamma_3} \text{ PROG}$$

Evaluation

$\ell ::= \ell_x$ (locations, \mathcal{L})
 $v ::= \textcolor{red}{()} \mid n \mid \ell$ (values, \mathbb{V})
 $\tilde{v} ::= \perp \mid v$ (partial values, $\tilde{\mathbb{V}}$)

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

$S \vdash w \rightsquigarrow \ell$ (place locations)
 $S \vdash e \Downarrow v \dashv S$ (expressions)
 $S \vdash s \dashv S$ (statements)
 $S \vdash p \Downarrow v \dashv S$ (programs)

$$\begin{array}{c}
 \frac{}{S \vdash x \rightsquigarrow \ell_x} \text{LOCVAR} \qquad \frac{S \vdash w \rightsquigarrow \ell_x \quad (\ell_x \mapsto \ell_y) \in S}{S \vdash * w \rightsquigarrow \ell_y} \text{LOCDEREF} \qquad \frac{}{S \vdash \textcolor{red}{()} \Downarrow \textcolor{red}{()} \dashv S} \text{UNIT} \\
 \\
 \frac{n \in \mathbb{Z}}{S \vdash n \Downarrow n \dashv S} \text{INT} \qquad \frac{S \vdash w \rightsquigarrow \ell_x \quad (\ell_x \mapsto v) \in S}{S \vdash \text{copy } w \Downarrow v \dashv S} \text{PLACECOPY} \\
 \\
 \frac{S \vdash w \rightsquigarrow \ell_x \quad (\ell_x \mapsto v) \in S}{S \vdash w \Downarrow v \dashv S[\ell_x \mapsto \perp]} \text{MOVE} \qquad \frac{S \vdash w \rightsquigarrow \ell_x}{S \vdash \textcolor{red}{\&} w \Downarrow \ell_x \dashv S} \text{REF} \qquad \frac{S \vdash w \rightsquigarrow \ell_x}{S \vdash \textcolor{red}{\&\text{mut}} w \Downarrow \ell_x \dashv S} \text{MUTREF} \\
 \\
 \frac{S \vdash w \rightsquigarrow \ell_x \quad (\ell_x \mapsto \tilde{v}) \in S_1 \quad S_1 \vdash e \Downarrow v \dashv S_2}{S_1 \vdash w = e \Downarrow \textcolor{red}{()} \dashv S_2[\ell_x \mapsto v]} \text{ASSIGN} \qquad \frac{S_1 \vdash e \Downarrow v \dashv S_2}{S_1 \vdash \text{let } x = e \dashv S_2[\ell_x \mapsto v]} \text{LET} \\
 \\
 \frac{S_1 \vdash e \Downarrow v \dashv S_2}{S_1 \vdash \text{let mut } x = e \dashv S_2[\ell_x \mapsto v]} \text{LETMUT} \qquad \frac{S_1 \vdash e \Downarrow v \dashv S_2}{S_1 \vdash e \dashv S_2} \text{EXPRSTMT} \\
 \\
 \frac{S_1 \vdash s \dashv S_2 \quad S_2 \vdash p \Downarrow v \dashv S_3}{S_1 \vdash s ; p \Downarrow v \dashv S_3} \text{PROG}
 \end{array}$$