FR Type / Borrow Safety II

Thm (Type / Borrow Safety):

data:

- S_1 : store
- Γ_1, Γ_2 : typing env.
- e : expression
- τ : type
- ℓ : lifetime
- γ : fresh variable

premises:

- S_1 is valid (no dup. owned loc. $\ell_n^\bullet \ldots \ell_n^\bullet$)
- Γ_1 is ℓ-well-formed $\begin{cases} \text{① referent outlives reference} \\ \text{② everything outlives } \ell \end{cases}$
- Γ_1 is borrow safe (mutiple refs $\Rightarrow$ immutable)
- $\Gamma_1 \sim S_1$
- $\boxed{\Gamma_1 \vdash \langle e : \tau \rangle^\ell \dashv \Gamma_2}$ (e is well-typed)

conclusions:

- $\exists\, S_2$ (store), v (value) s.t. $\langle S_1 \triangleright e \Downarrow S_2 \triangleright v \rangle^\ell$ (progress)
  - $S_2 \vdash v \sim \tau$ (value typing, valid typing) (preservation)

- $\Gamma_2 \sim S_2$

why the added binding?

- $\boxed{S_2[l_\gamma \mapsto \langle v \rangle^l]}$ is valid
- $\Gamma_2[\gamma \mapsto \langle \tau \rangle^l]$ is l-well-formed
- $\Gamma_2[\gamma \mapsto \langle \tau \rangle^l]$ is borrow safe (borrow safety)

<u>Proof</u>. By induction on derivations,

case (int):

$$\frac{}{\Gamma \vdash \langle c : \text{int} \rangle^l \dashv \Gamma} \text{(int)}$$

$$\frac{}{\langle S \triangleright c \Downarrow S \triangleright c \rangle^l} \text{(int-eval)}$$

$S \vdash c \sim \text{int}$ ✓

$\Gamma \sim S$ ✓

$S[l_\gamma \mapsto \langle c \rangle^l]$ is valid ✓

$\Gamma[\gamma \mapsto \langle \text{int} \rangle^l]$ is l-w.f. ✓

$\Gamma[\gamma \mapsto \langle \text{int} \rangle^l]$ is borrow safe ✓

case (copy):

$$\frac{\Gamma \vdash w : \langle \tau \rangle^{m} \quad \boxed{\mathrm{copy}(\tau)} \quad \boxed{\neg\, \mathrm{rdP}(\Gamma, w)}}{\Gamma \vdash \langle \hat{w} : \tau \rangle^{\ell} \dashv \Gamma}\ (\mathrm{copy})$$

$$\frac{\mathrm{read}(S, w) = \langle v \rangle^{m}}{\langle S \triangleright \hat{w} \Downarrow S \triangleright v \rangle^{\ell}}\ (\mathrm{copy\text{-}eval})$$

not partial if τ is not partial

<u>Lemma</u>: If $\Gamma \vdash w : \langle \tau \rangle^{m}$ and $S \sim \Gamma$, then $\exists v.$ s.t. $\mathrm{read}(S, w) = \langle v \rangle^{m}$ and $S \vdash v \sim \tau$

$S \vdash v \sim \tau$ ✓

$\Gamma \sim S$ ✓

$S[\ell_\gamma \mapsto \langle v \rangle^\ell]$ is valid because by $copy(\tau)$, $\tau = int$ or $\tau = \&w$ ✓

so $v \neq \ell_n^\bullet$

$\Gamma[\gamma \mapsto \langle \tau \rangle^\ell]$ is ℓ-wf. ✓

$\Gamma[\gamma \mapsto \langle \tau \rangle^\ell]$ is borrow safe since w is not read prohibited in Γ.

case (move):

$$\frac{\Gamma \vdash w : \langle \tau \rangle^m \qquad \boxed{\neg\, wP(\Gamma, \tau)}}{\Gamma \vdash \langle w : \tau \rangle^\ell \dashv \mathrm{move}(\Gamma, w)} \ (\text{move})$$

$$\frac{\mathrm{read}(S_1, w) = \langle v \rangle^m}{\langle S_1 \rhd w \Downarrow \mathrm{write}(S, w, \bot) \rhd v \rangle^\ell} \ (\text{move-eval})$$

$S_2 = \mathrm{write}(S, w, \bot) \quad v = v$ ✓ (by prev. lemma)

$S_2 \vdash v \sim \tau$ ✓ (by prev. lemma)

$\Gamma_2 \sim S_2$

move $(\Gamma_1, w) \sim$ write $(S, w, \bot)$

Lemma: if $\Gamma \sim S$ then move $(\Gamma, w) \sim$ write $(S, w, \bot)$

$S_2[\ell_\gamma \mapsto \langle v \rangle^\ell]$ is valid

write $(S_1, w, \bot)[\ell_\gamma \mapsto \langle v \rangle^\ell]$ is valid because if $v = \ell_n^\bullet$ then we removed it from S_1 ✓

$\Gamma[\gamma \mapsto \langle \tau \rangle^\ell]$ is ℓ-wf ✓

$\Gamma[\gamma \mapsto \langle \tau \rangle^\ell]$ is borrow-safe because if $\tau = \&\text{mut } u$ then the type is moved out by move. If $\tau = \& u$ then we're okay by write prohibit.

write prohibit

case (box):

$$\frac{\Gamma_1 \vdash \langle e : \tau \rangle^{\ell} \dashv \Gamma_2}{\Gamma_1 \vdash \langle \mathrm{box}\, e : \Box \tau \rangle^{\ell} \dashv \Gamma_2}\ (\mathrm{box})$$

by IH $\exists\, S_2, v$ s.t. $\langle S_1 \triangleright e \Downarrow S_2 \triangleright v \rangle^{\ell}$ so

$$\frac{\langle S_1 \triangleright e \Downarrow S_2 \triangleright v \rangle^{\ell} \qquad n \text{ is fresh}}{\langle S_1 \triangleright \mathrm{box}\, e \Downarrow \underbrace{S_2[\ell_n \mapsto v]}_{S_2} \triangleright \underbrace{\ell_n^{\bullet}}_{v} \rangle^{\ell}}\ (\mathrm{box\text{-}eval})$$