FR Type / Borrow Checking (III)

$$\frac{\Gamma \vdash \langle t : T \rangle^{\ell} \dashv \Gamma_2}{\Gamma_1 \vdash \langle \text{box } t : \square T \rangle^{\ell} \dashv \Gamma_2} \text{(box)}$$

$$\frac{\Gamma_1 \vdash \langle t_1 : T_1 \rangle^{\ell} \dashv \Gamma_2 \quad \Gamma_2 \vdash \langle t_2 : T_2 \rangle^{\ell} \dashv \Gamma_3 \quad \dots \quad \Gamma_k \vdash \langle t_k : T_k \rangle^{\ell} \dashv \Gamma_{k+1}}{\Gamma_1 \vdash \langle t_1; t_2 \dots; t_k : T_k \rangle^{\ell} \dashv \Gamma_{k+1}} \text{(seq)}$$

$$\frac{\Gamma \vdash \langle t_1; \ldots; t_k : T \rangle^{m} \dashv \Gamma_2 \qquad \Gamma_2 \vdash T \gtrsim \ell \qquad \Gamma_3 = \mathrm{drop}(\Gamma_2, m)}{\Gamma_1 \vdash \langle \{\, t_1; \ldots; t_k \,\}^{m} : T \rangle^{\ell} \dashv \Gamma_3}$$

non-ex.

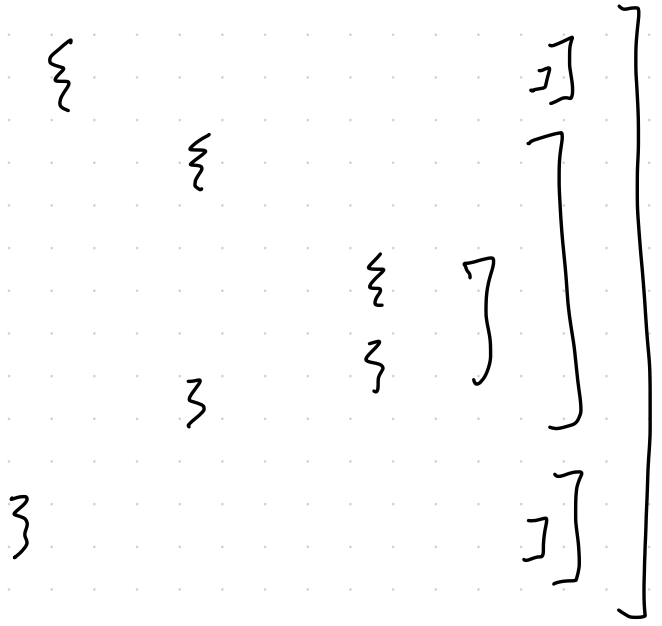
```
{
    let mut x = 0;
    &x
}^m
```

not well-typed

Def. 3.21 $\Gamma \vdash T \gtrsim l$

context type lifetime

$$\frac{}{\Gamma \vdash \text{int} \gtrsim l} \qquad \frac{\Gamma \vdash T \gtrsim l}{\Gamma \vdash \square\, T \gtrsim l} \qquad \frac{\Gamma \vdash u : \langle T \rangle^{m} \quad m \gtrsim l}{\Gamma \vdash \&[\text{mut}]\, u \gtrsim l}$$



Lifetime structure

Declaration

$$\frac{x \notin \mathrm{dom}(\Gamma_1) \qquad \Gamma_1 \vdash \langle t : T \rangle^{\ell} \dashv \Gamma_2 \qquad \Gamma_3 = \Gamma_2[x \mapsto \langle T \rangle^{\ell}]}{\Gamma_1 \vdash \langle \text{let mut } x = t : \varepsilon \rangle^{\ell} \dashv \Gamma_3}$$

Assignment

"compatible with"

partial

$$\frac{\Gamma_1 \vdash w : \langle \tilde{T}_1 \rangle^{m} \qquad \Gamma_1 \vdash \langle t : T_2 \rangle^{\ell} \dashv \Gamma_2 \qquad \Gamma_2 \vdash \tilde{T}_1 \approx T_2 \qquad \Gamma_2 \vdash T_2 \geq m \qquad \Gamma_3 = \mathrm{write}(\Gamma_2, w, T_2) \qquad \neg \mathrm{writeProhibited}(\Gamma_3, w)}{\Gamma_1 \vdash \langle w = t : \varepsilon \rangle^{\ell} \dashv \Gamma_3}$$

non-ex.

```
{
    let mut x = 0;
    let mut y = &x;
    {
        let mut z = 1;
        y = &z;
    }^m
}^l
```

not well-typed

Def 3.22

$$\Gamma \vdash \tilde{T}_1 \approx \tilde{T}_2$$

Context; partial types

$$\frac{}{\Gamma \vdash \text{int} \approx \text{int}}$$

$$\frac{\Gamma \vdash \tilde{T}_1 \approx \tilde{T}_2}{\Gamma \vdash \square \tilde{T}_1 \approx \square \tilde{T}_2}$$

$$\frac{\Gamma \vdash T_1 \approx \tilde{T}_2}{\Gamma \vdash \lfloor T_1 \rfloor \approx \tilde{T}_2} \qquad \frac{\Gamma \vdash \tilde{T}_1 \approx T_2}{\Gamma \vdash \tilde{T}_1 \approx \lfloor T_2 \rfloor}$$

$$\frac{\Gamma \vdash u : \langle \tilde{T}_1 \rangle^{m_1} \quad \Gamma \vdash w : \langle \tilde{T}_2 \rangle^{m_2} \quad \Gamma \vdash \tilde{T}_1 \approx \tilde{T}_2}{\Gamma \vdash \&u \approx \Gamma \vdash \&w} \qquad \frac{\Gamma \vdash u : \langle \tilde{T}_1 \rangle^{m_1} \quad \Gamma \vdash w : \langle \tilde{T}_2 \rangle^{m_2} \quad \Gamma \vdash \tilde{T}_1 \approx \tilde{T}_2}{\Gamma \vdash \&\mathrm{mut}\, u \approx \Gamma \vdash \&\mathrm{mut}\, w}$$

ex.

$$\{ x \mapsto \langle \mathrm{int} \rangle^m, \; y \mapsto \langle [\mathrm{int}] \rangle^n \} \vdash \&x \approx \&y$$

Write:

```
let mut y = 0;
let mut x = 1;
let p = &mut x;
let q = &mut p;
*q = &mut y;
```

type of p?

weak: &mut x, y

strong: ~~&mut~~ &y

$$\text{update}(\Gamma, \pi, \tilde{T}, T) = (\Gamma, T)$$

Γ: context, π: path, $\tilde{T}$: partial type, T: type

$$\text{update}(\Gamma, \varepsilon, \tilde{T}_1, T_2) = (\Gamma, T_2)$$

T_2: replacement

$$\text{update}^{k \geq 1}(\Gamma, \varepsilon, T_1, T_2) = (\Gamma, T_1 \sqcup T_2) \quad \text{(weak update)}$$

$$\text{update}(\Gamma, *\pi, \square \tilde{T}_1, T_2) = (\Gamma', \square \tilde{T}_1') \quad \text{where}$$

$$(\Gamma', \tilde{T}_1') = \text{update}(\Gamma, \pi, \tilde{T}_1, T_2)$$

"recurse under box"

$$\text{update}(\Gamma, *\pi, \&\text{mut } u, T_2) = (\Gamma', \&\text{mut } u) \quad \text{where}$$

no replacement

$$\Gamma' = \text{write}(\Gamma, \pi u, T)$$

add π to u

$$\text{write}(\Gamma, \pi x, T) = \Gamma'[x \mapsto \langle \tilde{T}_2 \rangle^{l}] \quad \text{where}$$

context, l-value, ty, path

$$\Gamma(x) = \langle \tilde{T}_1 \rangle^{l}$$

"check Γ for x"

$(\Gamma', \tilde{T}_2) = update(\Gamma, \pi, \tilde{T}_1, T)$ "update type at x"

e

{

let mut x = 0 ; t_1

let mut y = &x ; t_2

{

let mut z = 1 ; t_4

y = &z ; t_5

}^{m} t_3

}^{l}

$\emptyset \vdash \langle e \rangle^n \dashv$

$\emptyset \vdash \langle t_1 ; t_2 ; t_3 \rangle^l \dashv$

$\emptyset \vdash t_1 \dashv \{ x \mapsto \langle int \rangle^l \}$

$\{ x \mapsto \langle int \rangle^l \} \vdash t_2 \dashv \{ x \mapsto \langle int \rangle^l, y \mapsto \langle \&x \rangle^l \}$

$\{ x \mapsto \langle int \rangle^{\ell},\ y \mapsto \langle \&x \rangle^{\ell} \} \vdash \langle \{ t_4 ; t_5 \}^{m} \rangle^{\ell} \dashv$

$\{ x \mapsto \langle int \rangle^{\ell},\ y \mapsto \langle \&x \rangle^{\ell} \} \vdash \langle t_4 ; t_5 \rangle^{m} \dashv$

Γ

$\{ x \mapsto \langle int \rangle^{\ell},\ y \mapsto \langle \&x \rangle^{\ell},\ z \mapsto \langle int \rangle^{m} \} \vdash y = \&z$

- $\Gamma \vdash x : \langle int \rangle^{\ell}$
- $\Gamma \vdash \langle \&z : int \rangle^{m} \dashv \Gamma$
- $\Gamma \vdash int \simeq int$
- $\Gamma \vdash \&z \succeq \ell$ ✗
  - $\Gamma \vdash z : \langle int \rangle^{m}$
  - $m \succeq \ell$ ✗ $\quad \ell \succeq m$