FR Extensions

$$\frac{S \triangleright t_1 \longrightarrow S \triangleright t_1'}{S \triangleright (t_1, t_2) \longrightarrow S \triangleright (t_1', t_2)}$$

$$\frac{S \triangleright t_2 \longrightarrow S \triangleright t_2'}{S \triangleright (v, t_2) \longrightarrow S \triangleright (v, t_2')}$$

$$E ::= [\![\cdot]\!] \mid (E, E)$$

$$\frac{S \triangleright t \longrightarrow S \triangleright t'}{S \triangleright E[\![t]\!] \longrightarrow S \triangleright E[\![t']\!]}$$

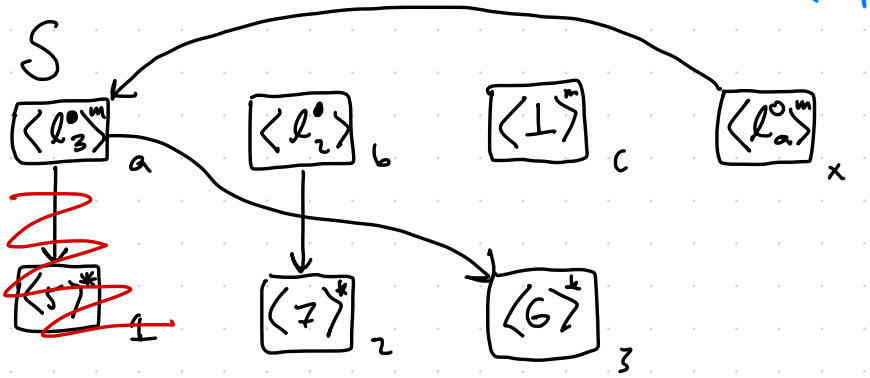
```
{
    let mut a = box 1;      // ℓ1
    let mut b = box 2;
    let mut c = box 3;
    let mut x = &mut a;     // ℓa
    *x = 4;
    **x = *b;
    **x = 5;
    *x = c;                 // ℓ3
    **x = 6;
}^m
*b = 7;
*c = 7
c = Box 10
```

$$\Gamma = a \mapsto \langle \square\,\text{int} \rangle^m,\ b \mapsto \langle \square\,\text{int} \rangle^m,\ c \mapsto \langle \lfloor \square\,\text{int} \rfloor \rangle^m,\ x \mapsto \langle \&\text{mut } a \rangle^m$$

$$\frac{\Gamma \vdash x : \&\text{mut } a \qquad \Gamma \vdash a : \square\,\text{int}}{\Gamma \vdash *x : \square\,\text{int}} \qquad \frac{\Gamma \vdash *x : \square\,\text{int}}{\Gamma \vdash **x : \text{int}}$$

$\text{read}(S, {}^{*}{}^{*}x) = \langle 1 \rangle^{*}$

$\text{drop}(S, \{1\})$ (nop)



$\text{write}(\Gamma, {}^{+}x, \square\,\text{int})$

If-expressions

syntax

$$t ::= \text{if } t \{ \vec{t} \}^m \text{ else } \{ \vec{t} \}^n$$
$$\mid t == t$$

$$v ::= \text{true} \mid \text{false}$$

$$T ::= \text{bool}$$

typing:

$$\Gamma_1 \vdash \langle t : \text{bool} \rangle^{\ell} \dashv \Gamma_2$$

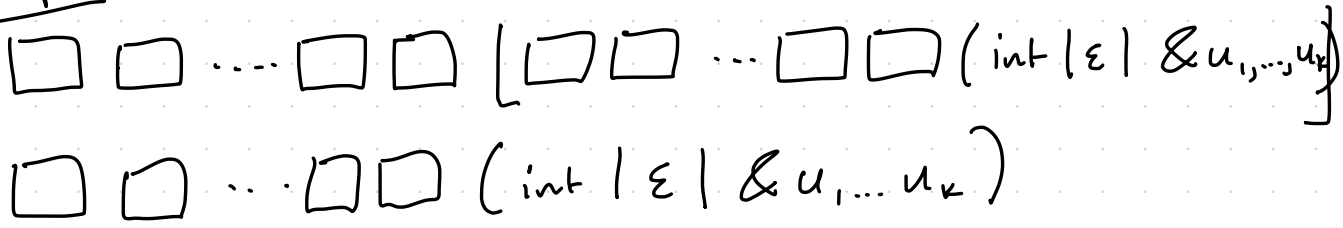
$$\Gamma_2 \vdash \langle \{ \vec{t} \}^n : T_1 \rangle^{\ell} \dashv \Gamma_3$$

$$\Gamma_2 \vdash \langle \{ \vec{s} \}^m : T_2 \rangle^{\ell} \dashv \Gamma_4$$

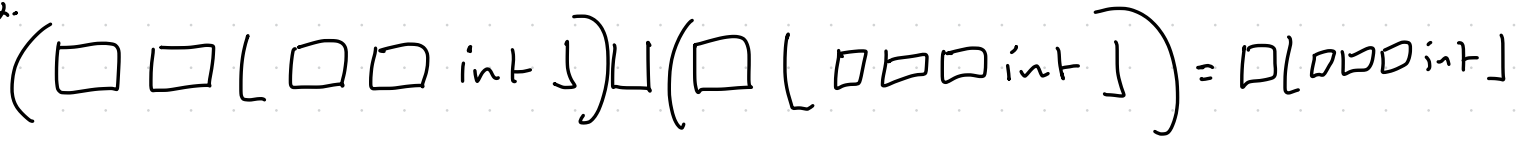
$$\Gamma_1 \vdash \langle \text{if } t \{ \vec{t} \}^n \text{ else } \{ \vec{s} \}^m : T_1 \sqcup T_2 \rangle \dashv \Gamma_3 \sqcup \Gamma_4$$

Type Join

types:



- ex.



conservatively choose level of undefinedness

- $\&\, x \sqcup \&\, y, z = \&\, x, y, z$

combine references

Def. 3.7 Type Strengthening:

$$\frac{}{\tilde{T} \sqsubseteq \tilde{T}} \qquad \frac{\tilde{T}_1 \sqsubseteq \tilde{T}_2}{\Box \tilde{T}_1 \sqsubseteq \Box \tilde{T}_2}$$

$$\frac{}{\&\, u_1, \ldots, u_k \sqsubseteq \&\, u_1, \ldots, u_k, u_{k+1} \ldots, u_n}$$

$$\frac{T_1 \sqsubseteq T_2}{\lfloor T_1 \rfloor \sqsubseteq \lfloor T_2 \rfloor} \qquad \frac{T_1 \sqsubseteq T_2}{T_1 \sqsubseteq \lfloor T_2 \rfloor} \qquad \frac{\tilde{T}_1 \sqsubseteq \lfloor T_2 \rfloor}{\Box \tilde{T}_1 \sqsubseteq \lfloor \Box T \rfloor}$$

Def 3.8 $T_1 \sqcup T_2 = T_3$ where T_3 is smallest s.t. $T_1 \sqsubseteq T_3$ and $T_2 \sqsubseteq T_3$