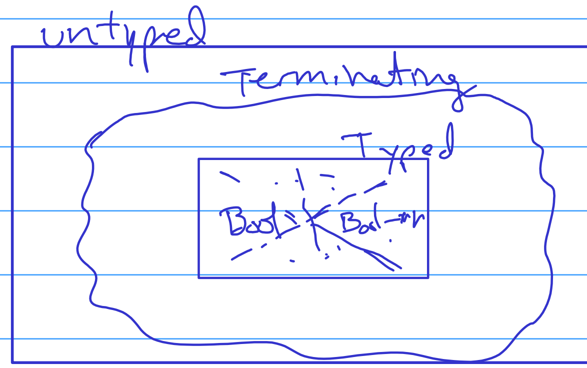
Logical Relations & Termination

- STLC - "Reducibility"
- System F



Recall,

<u>Def.</u> (closed) e is <u>closed</u> if it has no FV

<u>Def.</u> (well-typed) e is <u>well typed</u> if $\exists \Gamma, \tau.\ \Gamma \vdash e : \tau$

<u>Def.</u> (terminating) e is <u>terminating</u> if $\exists e'$, $e \mapsto^* e'$ and $e' \not\mapsto$

<u>Theorem</u>: If e is closed & well typed, then e is terminating.

Recall,

$b ::= \mathrm{True} \mid \mathrm{False}$

$e ::= x \mid \lambda x.e \mid e_1 e_2 \mid b \mid \text{if } e_1 \text{ then } e_2 \text{ else } e_3$

$\tau ::= \mathrm{bool} \mid \tau_1 \to \tau_2$

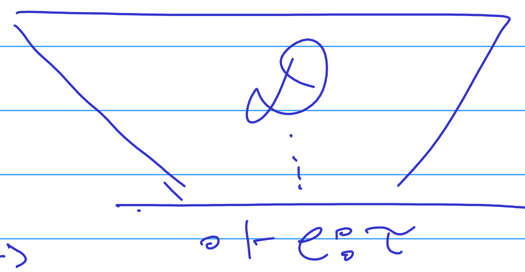
$$(\lambda x.e)\, e' \longmapsto e[e'/x]$$

$$\text{if True then } e_1 \text{ else } e_2 \longmapsto e_1$$
$$\text{if False then } e_1 \text{ else } e_2 \longmapsto e_2$$

Theorem: If $\bullet \vdash e : \tau$ is derivable, then $\exists e'$
$e \longmapsto^* e' \not\longmapsto$

Proof: (First try) By induction on the derivation $\mathcal{D}$ of $\bullet \vdash e : \tau$.

Consider all the possible derivations that could have led to



Show that, in each case, we have $e \longmapsto^* e' \not\longmapsto$ for some e'.

- case: e a variable – impossible because there's no rule that ends with $\bullet \vdash x : \tau$.

- case: $\mathcal{D} = \dfrac{}{\bullet \vdash \mathrm{True} : \tau}$ Let $e = e' = \mathrm{True}$ ✓

  (False is similar)

- case: $\mathcal{D} = \dfrac{\overset{\mathcal{D}_1}{\bullet \vdash e_1 : \mathrm{Bool}} \quad \overset{\mathcal{D}_2}{\bullet \vdash e_2 : \tau} \quad \overset{\mathcal{D}_3}{\bullet \vdash e_3 : \tau}}{\bullet \vdash \text{if } e_1 \text{ then } e_2 \text{ else } e_3 : \tau}$

  IH For $i = 1, 2, 3$, $\exists i'$ s.t. $e_i \longmapsto^* e_i' \not\longmapsto$

  Show: $\exists e$ if e_1 then e_2 else $e_3 \longmapsto e \not\longmapsto$.

  if e_1 then e_2 else $e_3 \longmapsto^*$ if e_1' then e_2 else e_3 by IH ✓

Suppose $e_1' = b$. Then the ite expr evaluates to whatever e_2 (or e_3) evaluates to.
Let $j=2$ if $b=\text{True}$, $j=3$ if $b=\text{False}$.

Then $\text{if } e_1 \text{ then } e_2 \text{ else } e_3 \longmapsto^{*} e_j' \not\longmapsto$.

N.B. "terminating" just means we don't get stuck.

"Terminating" + "Type Safety" means not only do we not get stuck, but also we get a value of the expected type.

Here we are only concerned with termination. So we also consider the case $e_1' \neq b : \text{Bool}$. In this case, then
$\{\text{If } e_1' \text{ then } e_2 \text{ else } e_3\}$
cannot take a step, so it has already terminated.

(Alternatively, we could argue by Type safety that the case $e_1' \neq b : \text{Bool}$ won't happen.)

Case $\mathcal{D} = \dfrac{x:\tau \vdash e:\tau'}{\bullet \vdash \lambda x{:}\tau.\, e : \tau \to \tau'}$

This case doesn't happen.

(why?)

Paul Downen

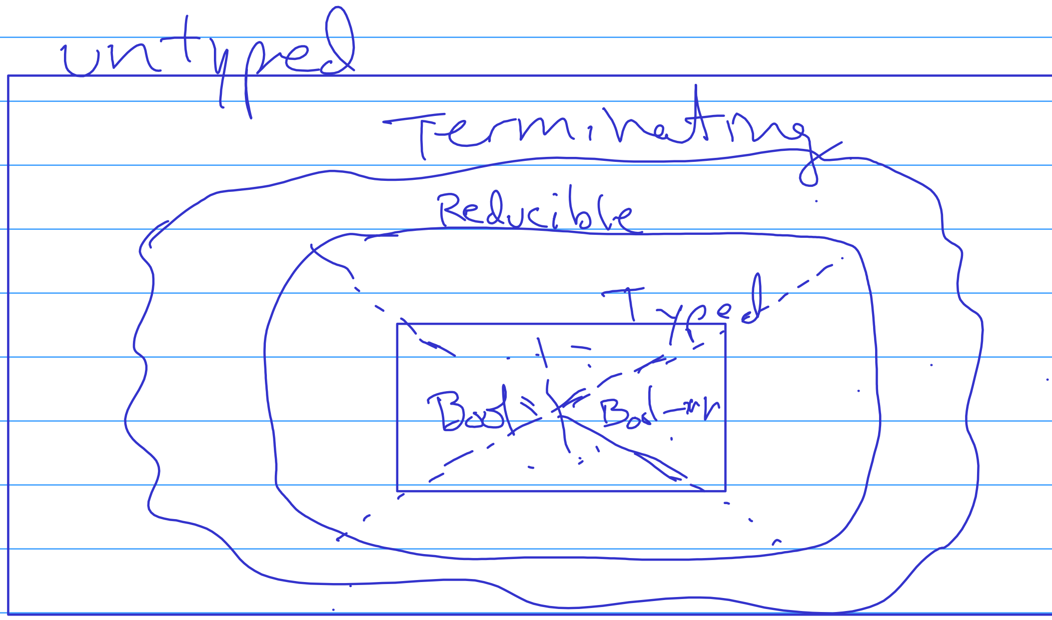
• Case $\mathcal{D} = \dfrac{\overset{\mathcal{D}_1 ::}{\cdot \vdash e_1 : \tau \to \tau'} \quad \overset{\mathcal{D}_2 ::}{\cdot \vdash e_2 : \tau}}{\cdot \vdash e_1 e_2 : \tau}$

IH: for $i = 1, 2$ $\quad e_i \longmapsto^* e_i' \not\longmapsto$

Suppose $e_1' = \lambda x. e'$: $e_1 e_2 \longmapsto^* (\lambda x. e') e_2 \longmapsto e'[e_2/x]$

Problem: The IH is too weak to help here.

Logical Relations to the rescue!



Reducibility

irreducible will mean that not only does the evaluation terminate, but also ...

Paul Downen (Lecture 9) [2018/07/08] 5

Terminating $:= \{ e \mid \exists e' \; e \mapsto^* e' \not\mapsto \}$

Definition of "meaning" (denoted by $[\![\cdot]\!]$)

$[\![\text{Bool}]\!] = \{ \text{True}, \text{False} \}^*$

where $*$ means include all expressions that reduce to a Boolean.

Formally, $\mathbb{C}^* = \{ e \mid \exists e' \in \mathbb{C}.\ e \mapsto^* e' \}$

example If False then $\lambda x.x$ else TRUE is in $[\![\text{Bool}]\!]$.

Properties of expansion (Homework: Prove these)

- if $\mathbb{C} \subseteq$ Terminating then $\mathbb{C}^* \subseteq$ Terminating
- $\mathbb{C} \subseteq \mathbb{C}^*$
- $\mathbb{C}^{**} = \mathbb{C}^*$ (Notice: $*$ is a closure operator.)

$[\![\tau_1 \to \tau_2]\!] = \{ e \in \text{Terminating} \mid \forall e' \in [\![\tau_1]\!] \;\; e\,e' \in [\![\tau_2]\!] \}$

We want to define $[\![\Gamma \vdash e : \tau]\!]$

First define $[\![\Gamma]\!]$

$[\![\Gamma]\!] = \{ \sigma \in Subst \mid \forall (x:\tau) \in \Gamma.\ x[\sigma] \in [\![\tau]\!] \}$

$[\![\Gamma \vdash e : \tau]\!] = \forall \sigma \in [\![\Gamma]\!].\ e[\sigma] \in [\![\tau]\!].$

Lemma (Fundamental lemma)

If $\Gamma \vdash e : \tau$ is derivable, then $[\![\Gamma \vdash e : \tau]\!]$ is true.

Proof: By induction on the given derivation of $\Gamma \vdash e : \tau$.

- case: $\mathcal{D} = \dfrac{}{\Gamma, x:\tau \vdash x:\tau}$

Show $[\![\Gamma, x:\tau \vdash x:\tau]\!]$ is true

Suppose $\sigma \in [\![\Gamma, x:\tau]\!]$

show $x[\sigma] \in [\![\tau]\!]$

But this is the very def of $[\![\Gamma, x:\tau]\!]$!

- Case $\mathcal{D} = \dfrac{\Gamma \vdash e_1 : \tau \to \tau' \quad \Gamma \vdash e_2 : \tau}{\Gamma \vdash e_1 e_2 : \tau}$

IH : $[\![\Gamma \vdash e_1 : \tau \to \tau']\!]$ is true
$[\![\Gamma \vdash e_2 : \tau]\!]$ is true

Show $[\![\Gamma \vdash e_1 e_2 : \tau']\!]$

Suppose $\sigma \in [\![\Gamma]\!]$ Show $(e_1 e_2)[\sigma] \in [\![\tau']\!]$

$e_1 e_2 [\sigma] = e_1[\sigma]\, e_2[\sigma]$ $\quad e_1[\sigma] \in [\![\tau \to \tau']\!]$
$e_2[\sigma] \in [\![\tau]\!]$

- $\mathcal{D} = \dfrac{\Gamma, x : \tau \vdash e : \tau'}{\Gamma \vdash \lambda x. e : \tau \to \tau'}$

IH = $[\![\Gamma\, x.\tau \vdash e : \tau']\!]$ is true

Show : $[\![\Gamma \vdash \lambda x. e : \tau \to \tau']\!]$

Suppose $\sigma \in [\![\Gamma]\!]$. Show $(\lambda x. e)[\sigma]$
$= \lambda x. (e[\sigma]) \in [\![\tau']\!]$

Suppose $e_2 \in [\![\tau]\!]$, Show

$(\lambda x. e[\sigma])\, e_2 \in [\![\tau']\!]$
$\longmapsto e[\sigma, e_2/x] \in [\![\tau']\!]$

$\sigma, e_2/x \in [\![\Gamma, x : \tau]\!]$

Paul Downen (Lect 9) [2018/07/08]

Lemma: $[\![\tau]\!] \subseteq$ Terminating

Lemma: (Expansion) If $e \mapsto^* e'$ and $e' \in [\![\tau]\!]$ then $e \in [\![\tau]\!]$

i.e. $[\![\tau]\!]^* \subseteq [\![\tau]\!]$

Corollary (of Fundamental Lemma)

If $\bullet \vdash e : \tau$ is derivable then $e \in [\![\tau]\!]$, thus e is terminating.