

Proving ML
Contextual Equivalences
via

"Logical" Relations

[OS & PE, section 5]

Proving ML
Contextual Equivalences
via

(Kripke)"Logical" Relations

[OS & PE, section 5]

$p \triangleq$

```
let a = ref 0 in
fun(x : int) -> (a := !a + x ; !a)
```

$m \triangleq$

```
let b = ref 0 in
fun(y : int) -> (b := !b - y ; 0 - !b)
```

Are these Caml expressions (of type $\text{int} \rightarrow \text{int}$) contextually equivalent?

Yes! Recall the informal argument why $p =_{\text{ctx}} m$ holds...

2

'Logical' simulation relation between ML programs, parameterised by state-relations

For each state-relation $r \in \text{Rel}(w_1, w_2)$ we can define relations

$e_1 \leq_r e_2 : ty$ ($e_1 \in \text{Prog}_{ty}(w_1), e_2 \in \text{Prog}_{ty}(w_2)$)

(for each type ty), with the properties (I), (II) & (III)...

Kripke-style worlds: w_1, w_2, \dots are finite sets of locations.

States in world w : $\text{St}(w) \triangleq \mathbb{Z}^w$. Programs in world w :

$\text{Prog}_{ty}(w) \triangleq \{ e \in \text{Prog}_{ty} \mid \text{loc}(e) \subseteq w \}$.

State-relations: $r, r', \dots \in \text{Rel}(w_1, w_2)$ are ^{non-empty*} subsets of $\text{St}(w_1) \times \text{St}(w_2)$.

[* simplifies defⁿ of \leq_r at ground types]

Growth of the state

If	$s, e \Rightarrow v, s'$
then	$\text{dom}(s) \subseteq \text{dom}(s')$

E.g.

$\emptyset, p \Rightarrow (\text{fun}(x:\text{int}) \rightarrow l := !l + 1; !l), \{l \mapsto 0\}$

\swarrow $\text{dom}(\emptyset) = \emptyset \subseteq \{l\} = \text{dom} \{l \mapsto 0\}$ \nearrow

(III) The relationship between \leq_r and contextual equivalence

For all types ty , finite sets w of locations, and programs
 $e_1, e_2 \in \text{Prog}_{ty}(w)$

$$e_1 \leq_{\text{ctx}} e_2 : ty \quad \text{iff} \quad e_1 \leq_{id_w} e_2 : ty$$

where $id_w \in \text{Rel}(w, w)$ is the identity state-relation for w :

$$id_w \triangleq \{ (s, s) \mid s \in \text{St}(w) \}.$$

Hence e_1 and e_2 are contextually equivalent iff both $e_1 \leq_{id_w} e_2 : ty$
and $e_2 \leq_{id_w} e_1 : ty$.

(I) The simulation property of \leq_r

To prove $e_1 \leq_r e_2 : ty$, it suffices to show that whenever

$$\begin{cases} (s_1, s_2) \in r \\ s_1, e_1 \Rightarrow v_1, s'_1 \end{cases}$$

then there exists $r' \triangleright r$ and v_2, s'_2 such that

$$\begin{cases} s_2, e_2 \Rightarrow v_2, s'_2 \\ (s'_1, s'_2) \in r' \end{cases}$$

and $v_1 \leq_{r'} v_2 : ty$.

This uses the notion of extension of state-relations:

$r' \triangleright r$ holds iff $r' = r \otimes r''$ for some r'' —see Definition 5.1.

Given $\begin{cases} r \in \text{Rel}(w_1, w_2) \\ r' \in \text{Rel}(w'_1, w'_2) \end{cases}$, $r' \triangleright r$ means :

see also
Ex. B.5

- $w'_1 \supseteq w_1$
- $w'_2 \supseteq w_2$
- $r' = r \otimes r''$ for some $r'' \in \text{Rel}(w'_1 - w_1, w'_2 - w_2)$

where $r \otimes r'' \triangleq \{(s_1 s''_1, s_2 s''_2) \mid (s_1, s_2) \in r \ \& \ (s''_1, s''_2) \in r''\}$

given states s & s' , ss' is the state with
 $\text{dom}(ss') = \text{dom}(s) \cup \text{dom}(s')$
 and $(ss')(l) = \begin{cases} s'(l) & \text{if } l \in \text{dom}(s') \\ s(l) & \text{if } l \in \text{dom}(s) - \text{dom}(s') \end{cases}$

Recall:

Canonical forms (a.k.a. values) = closed expressions in the subset of all expressions generated by the grammar

$$\begin{aligned} V ::= & \quad x \quad f && (x, f \in \text{Var}) \\ & \quad \text{true} \\ & \quad \text{false} \\ & \quad n && (n \in \mathbb{Z}) \\ & \quad () \\ & \quad v, v \\ & \quad \text{fun } (x : ty) \rightarrow e \\ & \quad \text{fun } f = (x : ty) \rightarrow e && (l \in \text{Loc}) \\ & \quad l \end{aligned}$$

(II) The extensionality properties of \leq_r on canonical forms

- For $ty \in \{\text{bool}, \text{int}, \text{unit}\}$, $v_1 \leq_r v_2 : ty$ iff $v_1 = v_2$.
- $v_1 \leq_r v_2 : \text{int ref}$ iff $!v_1 \leq_r !v_2 : \text{int}$ and for all $n \in \mathbb{Z}$, $(v_1 := n) \leq_r (v_2 := n) : \text{unit}$.
- $v_1 \leq_r v_2 : ty_1 * ty_2$ iff $\text{fst } v_1 \leq_r \text{fst } v_2 : ty_1$ and $\text{snd } v_1 \leq_r \text{snd } v_2 : ty_2$.

- $v_1 \leq_r v_2 : ty_1 \rightarrow ty_2$ iff for all $r' \triangleright r$ and all v'_1, v'_2
 $v'_1 \leq_{r'} v'_2 : ty_1 \supset v_1 v'_1 \leq_{r'} v_2 v'_2 : ty_2$

The last property is characteristic of (Kripke) logical relations (Plotkin 1973; O'Hearn and Riecke 1995).

Outline of the proof of $p =_{\text{ctx}} m : \text{int} \rightarrow \text{int}$ (cf. Slide 2)

$$\emptyset, p \Rightarrow (\text{fun}(x : \text{int}) \rightarrow l_1 := !l_1 + x ; !l_1), \{l_1 \mapsto 0\}$$

$$\emptyset, m \Rightarrow (\text{fun}(y : \text{int}) \rightarrow l_2 := !l_2 - x ; 0 - !l_2), \{l_2 \mapsto 0\}$$

Define

$$r \triangleq \{ (s_1, s_2) \mid s_1(l_1) = -s_2(l_2) \} \in \text{Rel}(\{l_1\}, \{l_2\}).$$

Then $r \triangleright id_{\emptyset}, (\{l_1 \mapsto 0\}, \{l_2 \mapsto 0\}) \in r$, and from Slide 20

$$(\text{fun}(x : \text{int}) \rightarrow l_1 := !l_1 + x ; !l_1) \leq_r$$

$$(\text{fun}(y : \text{int}) \rightarrow l_2 := !l_2 - x ; 0 - !l_2) : \text{int} \rightarrow \text{int}.$$

So by Slide 19, $p \leq_{id_{\emptyset}} m : \text{int} \rightarrow \text{int}$.

Hence by Slide 21, $p \leq_{\text{ctx}} m : \text{int} \rightarrow \text{int}$.

Similarly $m \leq_{\text{ctx}} p : \text{int} \rightarrow \text{int}$.

Outline of the proof of $p =_{\text{ctx}} m : \text{int} \rightarrow \text{int}$ (cf. Slide 2)

$$\emptyset, p \Rightarrow (\text{fun}(x : \text{int}) \rightarrow l_1 := !l_1 + x ; !l_1), \{l_1 \mapsto 0\}$$

$$\emptyset, m \Rightarrow (\text{fun}(y : \text{int}) \rightarrow l_2 := !l_2 - x ; 0 - !l_2), \{l_2 \mapsto 0\}$$

Define

$$r \triangleq \{ (s_1, s_2) \mid s_1(l_1) = -s_2(l_2) \} \in \text{Rel}(\{l_1\}, \{l_2\}).$$

Then $r \triangleright id_{\emptyset}, (\{l_1 \mapsto 0\}, \{l_2 \mapsto 0\}) \in r$, and from Slide 20

$$(\text{fun}(x : \text{int}) \rightarrow l_1 := !l_1 + x ; !l_1) \leq_r$$

$$(\text{fun}(y : \text{int}) \rightarrow l_2 := !l_2 - x ; 0 - !l_2) : \text{int} \rightarrow \text{int}.$$

So by Slide 19, $p \leq_{id_{\emptyset}} m : \text{int} \rightarrow \text{int}$.

Hence by Slide 21, $p \leq_{\text{ctx}} m : \text{int} \rightarrow \text{int}$.

Similarly $m \leq_{\text{ctx}} p : \text{int} \rightarrow \text{int}$.

$$v \leq_r v' : \text{int} \rightarrow \text{int}$$

iff {slide 20}

$$\forall r' \triangleright r, \forall n, n' \in \mathbb{Z}. n \leq_r n' : \text{int} \supset vn \leq_{r'} v'n' : \text{int}$$

iff {slide 20}

$$\forall r' \triangleright r, \forall n \in \mathbb{Z}. vn \leq_{r'} v'n : \text{int}$$



prove this via
property (I)

$$r \triangleq \{(s_1, s_2) \mid s_1(l_1) = -s_2(l_2)\}$$

$$r' \triangleright r \supset vn \leq_{r'} v'n : \text{int}$$

Proof: If $(s_1, s_2) \in r'$ then since $r' \triangleright r$, we have

$$s_1(l_1) = -s_2(l_2) = k, \text{ say}$$

$$\text{So } \left. \begin{array}{l} s_1, vn \Rightarrow n', s_1[l_1 \mapsto n'] \\ s_2, v'n \Rightarrow n', s_2[l_2 \mapsto -n'] \end{array} \right\} \text{ where } n' \triangleq k+n$$

and $n' \leq_r n' : \text{int}$ {slide 20}

$$(s[l_1 \mapsto n'], s_2[l_2 \mapsto -n']) \in r' \quad \{r' \triangleright r\}$$

So $vn \leq_{r'} v'n : \text{int}$ holds by the simulation property of \leq_r (Slide 19).

Summary

- To prove $e_1 \leq_{ctx} e_2 : ty$, prove $e_1 \leq_{id_w} e_2 : ty$ instead (where $w \supseteq \text{locs}(e_1, e_2)$)
— relying on property (III) of \leq_r
- Try to prove $e_1 \leq_{id_w} e_2 : ty$ via the simulation property (I) of \leq_r and the extensionality properties (II) of \leq_r on canonical forms.

Exercise (B.7, p 410)

If $f \in \text{Prog}_{\text{int} \rightarrow \text{int}}$ satisfies

- $\text{loc}(f) = \emptyset$
- $\emptyset, fn \Downarrow$ for all $n \in \mathbb{Z}$

then $f \cong_{ctx} \text{memo}_f : \text{int} \rightarrow \text{int}$ where

$\text{memo}_f \triangleq$ let $a = \text{ref } 0$ in
let $r = \text{ref}(f 0)$ in
fun($x : \text{int}$) \rightarrow
 (if $x = !a$ then () else $a := x ; r := fx$);
 !r

Summary

- To prove $e_1 \leq_{ctx} e_2 : ty$, prove $e_1 \leq_{id_w} e_2 : ty$ instead (where $w \supseteq \text{locs}(e_1, e_2)$)
— relying on property (III) of \leq_r

this is only a sufficient, not a necessary condition for $e_1 \leq_{ctx} e_2 : ty$ to hold — for example...

A nasty contextual equivalence

let $a = \text{ref } 0$ in

$\text{fun } (f : \text{unit} \rightarrow \text{unit}) \rightarrow (a := 1 ; f() ; !a)$

\cong_{ctx}

$\text{fun } (f : \text{unit} \rightarrow \text{unit}) \rightarrow f() ; 1$

$: (\text{unit} \rightarrow \text{unit}) \rightarrow \text{int}$

Valid, but can't use the simulation property (I) to prove it. (See [15], Example 5.9.)