(Ⅲ) The relationship between $\leq_r$ and contextual equivalence

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

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

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

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

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 $r' \rhd r$ 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:

$\boxed{r' \rhd r}$ holds iff $r' = r \otimes r''$ for some r''—see Definition 5.1.

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

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

We have yet to prove the existence of a family of relations $\leq_r$ satisfying (I), (II) & (III)

The obvious strategy:

[15] — take (I) as the <u>definition</u> of $\leq_r$ on expressions in terms of $\leq_r$ on canonical forms

— define $\leq_r$ on canonical forms by <u>induction on the structure of types</u>, using (II)

<u>BUT</u> this definition of $\leq_r$ fails to satisfy (III) (probably).

(I) The relation we are interested in *is a retract of* a larger one with better structural properties.

$$
\begin{tikzcd}
\Downarrow \arrow[r, hook] \arrow[d, hook] & \searrow \arrow[l, bend left] \arrow[d, hook] \\
\text{States} \times \text{Programs} \arrow[r, hook] & \text{States} \times \text{Frame Stacks} \times \text{Programs} \arrow[l, bend left]
\end{tikzcd}
$$

$$
\begin{aligned}
(s\ ,\ e) &\longmapsto \langle s\ ,\ \mathcal{I}d\ ,\ e\rangle \\
(s\ ,\ \mathcal{F}s[e]) &\longmapsfrom \langle s\ ,\ \mathcal{F}s\ ,\ e\rangle
\end{aligned}
$$

We have yet to prove the existence of a family of relations $\leq_r$ satisfying (I), (II) & (III)

The non-obvious strategy:

- use $\langle s, Fs, e\rangle \to \langle s', Fs', e'\rangle$ operational semantics instead of $s, e \Rightarrow v, s'$
- define $\leq_r$ for frame stacks as well as expressions & canonical forms

(II) Logical simulation relation

For all worlds w_1, w_2, state-relations $r \in Rel(w_1, w_2)$ and types ty, we define

$$\boxed{\begin{array}{ll} (1) & \leq_r \subseteq Prog_{ty}(w_1) \times Prog_{ty}(w_2) \\ (2) & Stack_{ty}(r) \subseteq Stack_{ty}(w_1) \times Stack_{ty}(w_2) \\ (3) & Val_{ty}(r) \subseteq Val_{ty}(w_1) \times Val_{ty}(w_2) \end{array}}$$

$\left.\begin{array}{l}\text{(1) defined in terms of (2)} \\ \text{(2) defined in terms of (3)}\end{array}\right\}$ for all r & ty simultaneously

(3) defined by induction on structure of ty (for all r simultaneously)

Definition of the logical simulation relation

$$e_1 \leq_r e_2 : ty \triangleq$$
$$\forall r' \rhd r, (s'_1, s'_2) \in r', (\mathcal{F}s_1, \mathcal{F}s_2) \in \mathbf{Stack}_{ty}(r').$$
$$\langle s'_1\ , \mathcal{F}s_1\ , e_1 \rangle\searrow\ \supset\ \langle s'_2\ , \mathcal{F}s_2\ , e_2 \rangle\searrow$$

where

$$(\mathcal{F}s_1, \mathcal{F}s_2) \in \mathbf{Stack}_{ty}(r') \triangleq$$
$$\forall r'' \rhd r', (s''_1, s''_2) \in r'', (v_1, v_2) \in \mathbf{Val}_{ty}(r'').$$
$$\langle s''_1\ , \mathcal{F}s_1\ , v_1 \rangle\searrow\ \supset\ \langle s''_2\ , \mathcal{F}s_2\ , v_2 \rangle\searrow$$

and where $\mathbf{Val}_{ty}(r'')$ is defined in terms of $- \leq_{r''} - : ty$ by induction on the structure of ty as follows...

(cf. extensionality properties (II))

[OS&PE, p395]

- $(v_1, v_2) \in Val_{gnd}(r) \equiv v_1 = v_2 \quad (gnd = bool, int, unit)$
- $(v_1, v_2) \in Val_{int\,ref}(r) \equiv$
  $!v_1 \leqslant_r !v_2 : int \;\&\; \forall n \in \mathbb{Z} (v_1 := n \leqslant_r v_2 := n : unit)$
- $(v_1, v_2) \in Val_{ty_1 * ty_2}(r) \equiv$
  $fst\, v_1 \leqslant_r fst\, v_2 : ty_1 \;\&\; snd\, v_1 \leqslant_r snd\, v_2 : ty_2$
- $(v_1, v_2) \in Val_{ty_1 \to ty_2}(r) \equiv$
  $\forall r' \rhd r, \quad \forall v_1', v_2'$
  $v_1' \leqslant_{r'} v_2' : ty_1 \supset v_1 v_1' \leqslant_{r'} v_2 v_2' : ty_2$

$\boxed{\text{Theorem. } \leq_r \text{ has properties (I), (II) \& (III)}}$

Will sketch the proof — see Sections 4 & 5 of

AMP & I.D.B. Stark, "Operational Reasoning for Functions with Local State" (CUP, 1998)

for details.

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

- For $ty \in \{\texttt{bool}, \texttt{int}, \texttt{unit}\}$, $v_1 \leq_r v_2 : ty$ iff $v_1 = v_2$.

- $v_1 \leq_r v_2 : \texttt{int ref}$ iff $!v_1 \leq_r\ !v_2 : \texttt{int}$ and for all $\texttt{n} \in \mathbb{Z}$, $(v_1 := \texttt{n}) \leq_r (v_2 := \texttt{n}) : \texttt{unit}$.

- $v_1 \leq_r v_2 : ty_1 * ty_2$ iff $\texttt{fst}\ v_1 \leq_r \texttt{fst}\ v_2 : ty_1$ and $\texttt{snd}\ v_1 \leq_r \texttt{snd}\ v_2 : ty_2$.

- $v_1 \leq_r v_2 : ty_1 \texttt{ -> } ty_2$ iff for all $r' \rhd r$ 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).

Proof of (II)

Follows from

$$\boxed{v_1 \leqslant_r v_2 : ty \equiv (v_1, v_2) \in Val_{ty}(r)}$$

which is proved by induction on the structure of ty (see [15] Lemma 4.4).

(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 $r' \rhd r$ 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:

$\boxed{r' \rhd r}$ holds iff $r' = r \otimes r''$ for some r''—see Definition 5.1.

Proof of (I)

Follows from

$$\boxed{\langle s, Fs, e\rangle \searrow \;\equiv\; \exists s', v\,(s, e \Rightarrow v, s' \;\&\; \langle s', Fs, v\rangle \searrow)}$$

(proved directly from the definitions of $\searrow$ and $\Rightarrow$)

(III) The relationship between $\leq_r$ and contextual equivalence

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

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

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

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

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

Proof of (III)

Follows from

(a) $e \leq_r e' \leq_{ctx} e'' \supset e \leq_r e''$

(b) $(Id, Id) \in Stack_{ty}(id_w)$

have easy proofs

(c) if $\{x : ty\} \vdash e : ty'$ & $loc(e) \subseteq w$, then

$$e_1 \leq_{id_w} e_2 : ty \supset e[e_1/x] \leq_{id_w} e[e_2/x] : ty'$$

proof is involved

From (c) we get $e \leq_{id_w} e : ty$ for all $e \in Prog_{ty}(w)$.

Hence $e_1 \leq_{ctx} e_2 \supset e_1 \leq_{id_w} e_1 \leq_{ctx} e_2$

$\supset e_1 \leq_{id_w} e_2$ by (a).

Proof of (III)

Follows from

(a) $e \leq_r e' \leq_{ctx} e'' \supset e \leq_r e''$

(b) $(Id, Id) \in Stack_{ty}(id_\omega)$

(c) if $\{x : ty\} \vdash e : ty'$ & $loc(e) \subseteq \omega$, then

$e_1 \leq_{id_\omega} e_2 : ty \supset e[e_1/x] \leq_{id_\omega} e[e_2/x] : ty'$

Conversely, if $e_1 \leq_{id_\omega} e_2 : ty$ then for all $\{x : ty\} \vdash e : ty'$

$$\begin{aligned} s, e[e_1/x] \Downarrow &\supset \langle s, Id, e[e_1/x] \rangle \searrow \\ &\supset \langle s, Id, e[e_2/x] \rangle \searrow \quad \text{by (b)+(c)} \\ &\supset s, e[e_2/x] \Downarrow \end{aligned}$$

Hence $e_1 \leq_{ctx} e_2 : ty$.

So it just remains to prove

$$\boxed{\begin{array}{l}\text{(c) if } \{x : ty\} \vdash e : ty' \ \& \ loc(e) \subseteq w, \text{ then} \\ \quad e_1 \leqslant_{id_w} e_2 : ty \supset e[e_1/x] \leqslant_{id_w} e[e_2/x] : ty'\end{array}}$$

Corollary of

"Fundamental Property of Logical Relations"

for $\leqslant_{id_w}$

First we extend $\leqslant_r$ to (well-typed) expressions with free variables:

Given $\Gamma \vdash e_1 : ty$ & $\Gamma \vdash e_2 : ty$ where $\Gamma = \{x_1 \mapsto ty_1, \ldots, x_n \mapsto ty_n\}$ say,

and given $r \in Rel(\omega_1, \omega_2)$ where $loc(e_i) \subseteq \omega_i$,

define $\boxed{\Gamma \vdash e_1 \leqslant_r e_2 : ty}$

to mean

$$\forall r' \rhd r$$

$$\forall (v_i, v_i') \in Val_{ty_i}(r') \quad (i = 1, \ldots, n)$$

$$e_1[v_1/x_1, \ldots v_n/x_n] \leqslant_{r'} e_2[v_1'/x_1, \ldots, v_n'/x_n] : ty$$