

Proof of Lemma 4

18 October 2017

00:32

By induction on (1), analysis on last rule

Case S-CONS : $e = c$, $\sigma = \text{type of } c$, $\tilde{e} = c$

(a) follows from (SE-CONST).

(b) follows from (V-CONS)

(c) follows from (EE-CONST) \blacksquare

Case S-VAR : $e = x$, $\Gamma(x) = \sigma^P$, $\tilde{e} = x$

Using Lemma (3).(1) :

(4) $f(x) = c$, $c : \sigma$, and $\tilde{f}(x) = c$

(a) follows from (SE-VAR)

(b) follows from (4)

(c) follows from (EE-VAR) \blacksquare

Case S-ADD : $e = e_1 + e_2$, $\sigma = \text{uint}$, $\tilde{e} = \tilde{e}_1 +_P \tilde{e}_2$

From the premises of (S-ADD) :

(4) $\Gamma \vdash e_1 : \text{uint}^P \rightsquigarrow \tilde{e}_1$

(5) $\Gamma \vdash e_2 : \text{uint}^P \rightsquigarrow \tilde{e}_2$

Using I.H. on (4) and (5) :

(6) $f \vdash e_1 \Downarrow C_1$

(7) $C_1 : \text{uint}$

(8) $\tilde{f} \vdash \tilde{e}_1 \Downarrow C_1$

$$(9) \quad \gamma \vdash e_2 \Downarrow c_2$$

$$(10) \quad c_2 : \text{unit}$$

$$(11) \quad \tilde{\gamma} \vdash \tilde{e}_2 \Downarrow c_2$$

Using Lemma (1):

$$(12) \quad c_1 = n,$$

$$(13) \quad c_2 = n_2$$

(a) follows from (SE-ADD) using (6) and (9), and
 $c = n_1 + n_2$ (with (12) and (13))

(b) follows from (W-CONS)

(c) follows from (EE-PADD) using (8) and (11), with
 (12) and (13) #

Case S-COND: $c = \text{cond}(e, e_1, e_2)$, $\tilde{e} = \text{cond}_e(\tilde{e}, \tilde{e}_1, \tilde{e}_2)$

In the rule (S-COND), since $\ell' = P$, we must have $\ell = P$

\therefore Inverting (S-COND), we get :

$$(4) \quad \Gamma \vdash e : \text{bool}^P \rightsquigarrow \tilde{e}$$

$$(5) \quad \Gamma \vdash e_1 : \sigma^P \rightsquigarrow \tilde{e}_1$$

$$(6) \quad \Gamma \vdash e_2 : \sigma^P \rightsquigarrow \tilde{e}_2$$

Applying I.M. on (4), (5), and (6) :

$$(7) \quad \gamma \vdash e \Downarrow c \quad (8) \quad c : \text{bool} \quad (9) \quad \tilde{\gamma} \vdash \tilde{e} \Downarrow c$$

$\sim \sim \sim \sim$

- (10) $\tilde{f} \vdash e_1 \Downarrow c_1$ (11) $c_1 : \sigma$ (12) $\tilde{f} \vdash e_1 \Downarrow c$
 (13) $\tilde{f} \vdash e_2 \Downarrow c_2$ (14) $c_2 : \sigma$ (15) $\tilde{f} \vdash \tilde{e}_2 \Downarrow c_2$

Using Lemma (1) on (8) : $c = T$ or $c = \perp$

Subcase $c = T$:

- (a) follows from (SE-LWD) with (7) and (10), and $v = c$,
 (b) follows from (11)
 (c) follows from (EE-PLOWD) with (9) and (12)

Subcase $c = \perp$: Analogous to $c = T$

Case S-GT : Similar to (S-ADD) \blacksquare

Case S-AREAD :

$$e = x[e], l = P, \tilde{e} = x[\tilde{e}]$$

Inverting (S-AREAD) :

$$(4) \Gamma \vdash x : \sigma^P[n] \rightsquigarrow x$$

$$(5) \Gamma \vdash e : \text{unit}^P \rightsquigarrow \tilde{e}$$

$$(6) \Gamma \vdash e < n$$

$$\text{From (4)} : \tau(x) = \sigma^P[n]$$

(S-VAR is the only rule that can derive (4), (S-SUB) is not possible since array type, other rules are syntactically diff.)

Using Lemma (3) with (4) :

$$(7) \quad f(n) = [c_i]_n$$

$$(8) \quad \forall i \in 0..n-1. \quad c_i : \sigma$$

$$(9) \quad \tilde{f}(x) = [c_i]_n$$

Soundness of bounds checking :

$$\forall \Gamma, e, n, f$$

$$\text{if (1) } \Gamma \vdash e : \text{unit}^{\Gamma} \rightsquigarrow -$$

$$(2) \quad \Gamma \not\vdash e < n$$

$$(3) \quad \Gamma \vdash f \hookrightarrow - ; - , -$$

$$(4) \quad f \vdash e \Downarrow n'$$

Then $n' < n$

Using I.M. on (5) :

$$(10) \quad f \vdash e \Downarrow c$$

$$(11) \quad c : \text{unit}$$

$$(12) \quad \tilde{f} \vdash \tilde{e} \Downarrow c$$

Using Lemma (1) in (11) :

$$(12') \quad c = n'$$

Using soundness of bounds checking

with (5), (6), (2), and (10) :

(13) $n' < n$

Using (SE-VAR) with (7) :

(14) $\mathcal{g} \vdash x \Downarrow [C_n]$

Using (EE-VAR) with (9) :

(15) $\mathcal{g} \vdash x \Downarrow [C_n]$

(a) follows from (SE-AREAD) with
· (4), (10), (12'), and (13),

and $C_n = C_{n'}$

(b) follows from (8)

(c) follows from (EE-AREAD) with
(12), (12'), (15), and (13) with

$$\tilde{W}_n = C_{n'}$$



Case S-INP : Not possible

Case S-SUB : Not possible

Case S-ARR : Not possible

QED

Proof of Lemma (5)

18 October 2017 00:39

Proof by induction on (1), analysis on the last rule:

Case S-VAR : $e = x$, $\tilde{e} = \sigma^P(r)$, $\tilde{\epsilon} = x$

Using Lemma (3) . (3) :

$$(3) \quad g(x) = [c_i]_n$$

$$(4) \quad \forall i \in \{0..n-1\}. \quad c_i : \sigma$$

$$(5) \quad \tilde{g}(x) = [\tilde{c}_i]_n$$

(a) follows from (SE-VAR) with (3)

(b) follows from (4)

(c) follows from (EE-VAR) with (4)



Cases (S-CONS), (S-ADD), (S-COND), (S-LT)

(S-AREAD), (S-INP), (S-SUB)

are not possible.



Case S-ARR : $e = [e_i]_n$, $\tilde{e} = [\tilde{e}_i]_n$, $\ell = P$

Inverting (S-ARR) :

$$(3) \quad \forall i \in 0..n-1. \quad r \vdash e_i : \sigma^P \rightsquigarrow \tilde{e}_i$$

Using Lemma (4) with (3) :

$$\forall i \in 0..n-1 \quad (5) \quad \vdash e_i \Downarrow c_i$$

$$(6) \quad c_i : \sigma$$

$$(2) \quad \tilde{p} \vdash \tilde{e}_i \Downarrow c_i$$

(a) follows from (SE-ARR) with (5) and

$$v = [c_i]_n$$

(b) follows from (6)

(c) follows from (EE-ARR) with (7). \blacksquare

Qed

Proof of Lemma (6)

18 October 2017 01:33

By induction on (1), analysis on the last rule

Case S-cons : Not possible 

Case - S-VAR : $e = x$, $\tau = \sigma^m$, $\tilde{e} = x$

Using Lemma (3).(2) :

$$(4) \quad f(x) = c$$

$$(5) \quad c : \sigma$$

$$(6) \quad \tilde{f}(x) = r$$

$$(7) \quad (\hat{f}_1[r], \hat{f}_2[r]) = E_m(c)$$

(a) follows from (SE-VAR)

(b) follows from (5)

(c) follows from (EE-VAR) with $k^e = r$

(d) follows from (KTE-R)

(e) follows from (7). 

Assume : $D_m(E_m(c)) = c$

(Lemma ED)

Case S-ADD : $e = e_1 + e_2$, $\tau = A$, $\tilde{e} = \tilde{e}_1 + \tilde{e}_2$

Inverting (S-ADD) :

(3) $P \vdash e_1 : \text{Unit}^A \rightsquigarrow \tilde{e}_1$

(4) $\Gamma \vdash e_2 : \text{Unit}^A \rightsquigarrow \tilde{e}_2$

Applying I.H. on (3) and (4) :

(5) $f \vdash e, \Downarrow c_1$

(6) $c_1 : \text{unit}$

(7) $\tilde{f} \vdash \tilde{e}_1 \Downarrow k_1^e$

(8) $\hat{f}_1, \hat{f}_2 \vdash k_1^e \Downarrow b_{11}, b_{21}$

(9) $c_1 = D_A(b_{11}, b_{21})$

(10) $f \vdash e_2 \Downarrow c_2$

(11) $c_2 : \text{unit}$

(12) $\tilde{f} \vdash \tilde{e}_2 \Downarrow k_2^e$

(13) $\hat{f}_1, \hat{f}_2 \vdash k_2^e \Downarrow b_{12}, b_{22}$

(14) $c_2 = D_A(b_{12}, b_{22})$

Using Lemma (1) on (6) and (11):

(15) $c_1 = n_1$, (16) $c_2 = n_2$

(a) follows from (SE-ADD) with (5) and (10), and

$$c = n_1 + n_2$$

(b) follows from (V-CONS)

(c) follows from (EE-ADD) with (7) and (12), and

$$k^e = \text{Add}(k_1^e, k_2^e)$$

(d) follows from (CKTE-ADD) with (8), (13), (9), (14),
(15), (16), and $(b_1, b_2) = E_A(n_1 + n_2)$

(e) follows from (Lemma ED). \blacksquare

Case S-cond : we have two subcases, $\ell = P$ or $\ell = IS$

Subcase S-cond: $e = \text{cond}(e_1, e_2)$, $\ell = P$, $\ell' = m$, $\tilde{e} = \text{cond}(\tilde{e}_1, \tilde{e}_2)$

Inverting (S-cond), we get :

(3) $\Gamma \vdash e : \text{bool}^P \rightsquigarrow \tilde{e}$

(4) $\Gamma \vdash e_1 : \sigma^m \rightsquigarrow \tilde{e}_1$

(5) $\Gamma \vdash e_2 : \sigma^m \rightsquigarrow \tilde{e}_2$

Using Lemma (4) with (3) and (2) :

(6) $\mathfrak{f} \vdash e \Downarrow c$

(7) $c : \text{bool}$

(8) $\mathfrak{f} \vdash \tilde{e} \Downarrow c$

Using Lemma (1) with (7) :

(9) $c = T \text{ or } c = \perp$

Using Thm on (4) and (5) :

(10) $\mathfrak{f} \vdash e_1 \Downarrow c_1$

(11) $c_1 : \sigma$

(12) $\mathfrak{f} \vdash \tilde{e}_1 \Downarrow k_1^e$

(13) $\mathfrak{f}_1, \mathfrak{f}_2 \vdash k_1^e \Downarrow b_{11}, b_{21}$

(14) $c_1 = D_m(b_{11}, b_{21})$

(15) $\mathfrak{f} \vdash e_2 \Downarrow c_2$

(16) $c_2 : \sigma$

(17) $\mathfrak{f} \vdash \tilde{e}_2 \Downarrow k_2^e$

$$(18) \quad \hat{f}_1, \hat{f}_2 \vdash k^e \Downarrow b_{12}, b_{22}$$

$$(19) \quad c_2 = D_m(b_{12}, b_{22})$$

(a) follows from (SE-COND) with (6), (7), (9), (10) & (15)
with $v = c_1$ if $c = T$, $v = c_2$ if $c = \perp$

(b) follows from (11) and (16)

(c) follows from (EE-PCOND) with (8), (9), (12), (17)
with $k^Q = k^e$ if $c = T$, $\tilde{v} = k^e_2$ if $c = \perp$

(d) follows from (13) if $c = T$, (18) if $c = \perp$

(e) follows from (4) if $c = T$, (9) if $c = \perp$ •

Subcase S-COND: $l = B$, $e = \text{cond}(e_1, e_2, e_3)$, $\tilde{e} = \text{cond}(\tilde{e}_1, \tilde{e}_2, \tilde{e}_3)$
 $m = l' = B$

Inverting (S-COND):

$$(3) \quad \Gamma \vdash e : \text{bool}^B \rightsquigarrow \tilde{e}$$

$$(4) \quad \Gamma \vdash e_1 : \sigma^B \rightsquigarrow \tilde{e}_1$$

$$(5) \quad \Gamma \vdash e_2 : \sigma^B \rightsquigarrow \tilde{e}_2$$

Using I.H. on (3), (4), and (5) :

$$(6) \quad f \vdash e \Downarrow c$$

$$(7) \quad c : \text{bool}$$

$$(8) \quad \tilde{f} \vdash \tilde{e} \Downarrow k^e$$

$$(9) \quad \hat{f}_1, \hat{f}_2 \vdash k^e \Downarrow b_1, b_2$$

$$(10) \quad c = D_B(b_1, b_2)$$

$$(11) \quad f \vdash e_1 \Downarrow c_1 \quad (12) \quad c_1 : \sigma \quad (13) \quad \tilde{f} \vdash \tilde{e}_1 \Downarrow k^e_1$$

$$(14) \quad \hat{f}_1, \hat{f}_2 \vdash k^e_1 \Downarrow b_{11}, b_{21} \quad (15) \quad c_1 = D_B(b_{11}, b_{21})$$

(16) $\hat{f} \vdash e_2 \Downarrow C_2$ (17) $C_2 : \sigma$ (18) $\tilde{f} \vdash \tilde{e}_2 \Downarrow k_2^e$

(19) $\hat{f}_1, \hat{f}_2 \vdash k_2^e \Downarrow b_{12}, b_{22}$ (20) $C_2 = \mathcal{E}_B(b_{12}, b_{22})$

And Lemma (1) with (7) gives :

(21) $C = T$ or $C = \perp$

(a) follows with (C), (21), (11), and (16) with
 $v = c_1$ if $C = T$, $v = \perp$ if $C = \perp$

(b) follows from (12) and (17)

(c) follows from (EE-SECOND) with (8), (13), and (18)
and $k^e = \text{Max}(k^e, k_1^e, k_2^e)$

(d) follows from (9), (14), (19), (10), (15), (20), and (21)
with $(b'_1, b'_2) = \mathcal{E}_B(c_1)$ if $C = T$ or $\mathcal{E}_B(C_2)$ if $C = \perp$

(e) follows from (Lemma ED).



Case S-GT : (Similar to S-ADD)



Case S-AREAD : Should follows proof of scalar expressions.

Case S-INP : $e = \text{inj}$, $\tilde{e} = \text{in}^m j$

Input Assumption : If $\Gamma \vdash \text{inj} : \sigma^m \rightsquigarrow \text{in}^m j$

$f \vdash \text{inj} \Downarrow C_1$

$\tilde{f} \vdash \text{in}^m j \Downarrow \text{In}^m j$

$\hat{f}_1, \hat{f}_2 \vdash \text{In}^m j \Downarrow \mathcal{E}_m(C_2)$

Then $C_i : \sigma$ and $C_1 = \perp$

The proof follows from input assumption. \blacksquare

Case S-SUB:

Subcase $l = p$: $\tilde{e} = \tilde{e}' \triangleright m$

Inverting S-SUB:

(3) $\Gamma \vdash e: \sigma^p \rightsquigarrow \tilde{e}'$

Using Lemma (4) with (3) and (2):

(4) $f \vdash e \Downarrow c$

(5) $c : \sigma$

(6) $f' \vdash \tilde{e}' \Downarrow c$

(a) and (b) follow from (4) and (5).

(c) follows from (EE-WERCE) with $\tilde{w} = c$
and $k^e = c \triangleright m$

(d) follows from (EKTE-WERCE), with

$$(p_1, b_1) = E_m(c)$$

(e) follows from Lemma ED. \blacksquare

Subcase $l = m'$: $\tilde{e} = \tilde{e}' \triangleright m$

Inverting (S-SUB):

(3) $\Gamma \vdash e: \sigma^{m'} \rightsquigarrow \tilde{e}'$

Using I.H. on (3):

(4) $f \vdash e \Downarrow c$

- (5) $C : \sigma$
 (6) $\tilde{f} \vdash \tilde{e}' \Downarrow k^e'$
 (7) $\hat{f}_1, \hat{f}_2 \vdash k^e' \Downarrow b'_1, b'_2$
 (8) $C = D_m, (b'_1, b'_2)$

- (a) and (b) follow from (4) & (5)
 (c) follows from (EE-COERCE) with $k^e = k^e' \Delta m$
 (d) follows from (7) & (8), with $b_1, b_2 = \mathcal{E}_m(C)$
 (e) follows from Lemma ED.

□

QED

Proof of Lemma (7)

18 October 2017 15:38

By induction on (1).

Case (S-VAR) uses Lemma (3)

Case (S-ARR) uses Iⁿ.

Both follow the same pattern as Lemma (5)

Other cases are not possible.

Proof of Lemma (8)

18 October 2017 15:48

(The first case of the proof was written with Induction on (1). But since no I.M. it's fine)

By induction on (3), analysis on the last rule.

Case C-DECL : $S = \forall x = e, \tilde{S} = \exists x = \tilde{e}, \Gamma' = \Gamma, x : \tau$

We consider (4) subcases : $\tau = \sigma^P, \tau = \sigma^M, \tau = \sigma^P(n), \tau = \sigma^M(n)$

Subcase 1 : $\tau = \sigma^P$

Inverting C-DECL:

(4) $\Gamma \vdash e : \sigma^P \rightsquigarrow \tilde{e}$

Using Lemma (4) with (4) :

(5) $f \vdash e \Downarrow C \quad (6) \quad c : \sigma \quad (7) \quad \tilde{f} \vdash \tilde{e} \Downarrow C$

For (3), only (SC-DECL) is possible. Therefore:

(6) $f' = f[x \mapsto c] \quad (7) \quad \emptyset = \bullet$

(a) follows from (EC-DECL) with (7)

and $\tilde{f}' = \tilde{f}[x \mapsto c], k^S = \bullet$

(b) follows from (UKTC-EMP) with $\hat{f}'_i = \hat{f}_i$

To prove (c), we need:

$\Gamma, x : \sigma^P \vdash f[x \mapsto c] \hookrightarrow \tilde{f}[x \mapsto c]; \hat{f}_1, \hat{f}_2$

which follows from (EN- $\rho\beta\tau$) with (6) & (2) \bullet

We assume α -renaming, i.e. whenever

we write $\tilde{\Gamma}, x : \tau$, x is fresh in Γ .

Lemma: $\Gamma \vdash f \hookrightarrow \tilde{f}; \dots \Rightarrow \text{dom}(\Gamma) = \text{dom}(f)$
 $\wedge \text{dom}(\tilde{f}) \subseteq \text{dom}(\Gamma)$

Subcase 2 : $\tau = \sigma^m$

Inverting (C-DECL) :

(4) $\Gamma \vdash e : \sigma^m \rightsquigarrow \tilde{e}$

Using Lemma (6) :

(5) $f + e \Downarrow c \quad (6) \quad (:\sigma \quad (7) \quad f \vdash \tilde{e} \Downarrow k^e$

(8) $\hat{f}_1, \hat{f}_2 \vdash k^e \Downarrow b_1, b_2 \quad (9) \quad c = \text{Dom}(b_1, b_2)$

For (3) only (C-DECL) is possible. So :

(10) $f' = f[x \mapsto c] \quad (11) \quad 0 = \cdot$

(a) follows from (EC-DECLCKT) with (7)

and $\tilde{f}' = \tilde{f}[x \mapsto r], k' = \text{Bind}(k^e, r)$

(b) follows from (KTC-BIND) with 8

and $\hat{f}'_1 = \hat{f}_1[r \mapsto b_1], \hat{f}'_2 = \hat{f}_2[r \mapsto b_2]$

For (c) we want to show :

$\Gamma, x : \sigma^m \quad (x) = \sigma^m \quad \checkmark$

$f'(x) = c \quad \checkmark$

$c : \sigma \rightarrow \text{from } (6) \quad \checkmark$

$r \notin \tilde{f} \rightarrow \text{from (EC-DECLCKT)} \quad \checkmark$

$b_1, b_2 = E_m(c) \rightarrow (\text{from } t_1)) \quad \checkmark$
 $\Gamma \vdash f \hookrightarrow \tilde{f}; \hat{p}_1, \hat{p}_2 \quad \text{from premise}$

$\Gamma, x : \sigma^m \vdash f' \hookrightarrow \tilde{f}[x \mapsto r]; \hat{f}, (r \mapsto b_1), \hat{f}_2(r \mapsto b_2)$

follows from (EN-SBT). \otimes

Array subcases are analogous

②

Case (SC-ASSGN) : Similar to variable declaration case with no array subcases.

③

Case (SC-FORT):

$s = \text{for } x \text{ in } n_1 \dots n_2 \text{ do } s$

$f' = f_1 \setminus x \quad O = O$

Inverting (SC-FORT):

(4) $f[x \mapsto n_1] + \text{loop } x \text{ until } n_2 \text{ do } s \Downarrow f_1; O$

Inverting (C-FOR) with (1) :

(5) $\tilde{s} = \text{for } (x := n_1; x \leq n_2; ++x) \tilde{s}$

(6) $\tilde{f} = f \quad (8) \quad \Gamma, x : \text{uint}^P \vdash s \rightsquigarrow \tilde{s} / \underline{\quad}$

(7) $x \notin \text{modifies}(s)$

We want to apply I.4.1. on (4)

But first we have to establish (1) & (2)

For (1), we want to establish

(9) $\Gamma, x: \text{uint}^P \vdash \text{loop } x \text{ until } n_2 \text{ do } s \rightsquigarrow$
 $\text{loop } x \text{ until } n_2 \text{ do } \tilde{s} / \Gamma, x: \text{uint}^P$

It follows from (C-WOP) and (8)

For (2), we want to establish

(10) $\Gamma, x: \text{uint}^P \vdash f[x \mapsto n_1] \hookrightarrow \tilde{f}[x \mapsto n_1]; \hat{f}_1, \hat{f}_2$

It follows from (EN-PBT)

Now we apply IN. with (9), (10), and (7) to get

(11) $\tilde{f}(x \mapsto n_1) \vdash \text{loop } x \text{ until } n_2 \text{ do } \tilde{s} \Downarrow \tilde{f}'; k^s$

(12) $\hat{f}_1, \hat{f}_2 \vdash k^s \Downarrow \hat{f}'_1, \hat{f}'_2; 0$

(13) $\Gamma, x: \text{uint}^P \vdash f, \hookrightarrow \tilde{f}'; \hat{f}', \hat{f}''_2$

To prove (a) we need to prove :

$\tilde{f} \vdash \text{for } (x := n_1; x \leq n_2; ++x) \tilde{s} \Downarrow \tilde{f}''; k^s$

Follows using (EC-FORT) with (11) and

$$\tilde{f}'' = \tilde{f}' \setminus \{x\}$$

To prove (b) we need to prove :

$\hat{f}_1, \hat{f}_2 \vdash k^s \Downarrow \hat{f}'_1, \hat{f}'_2 ; O$

follows from (12)

To prove (c) we need to prove :

$\Gamma \vdash f, \set{x} \rightsquigarrow \tilde{f} \setminus \{x\}; \hat{f}'_1, \hat{f}'_2$

Follows using (EN-PBT) on (13)



Case (SC-WOPT):

$s = \text{loop } x \text{ until } n_2 \text{ do } s$ $\tilde{s} = \text{loop } x \text{ until } n_2 \text{ do } \tilde{f}$
 $f' = f$ $O = \text{emp}$ $f(x) > n_2$

TODO: Fix in SC-WOPT to say $O = \text{emp}$

Inverting (1) with (C-loop) :

(4) $\Gamma(x) = \text{until } r$

(5) $\Gamma \vdash s \rightsquigarrow \tilde{s} \mid r$

Using Lemma (3) with (2) and (4) :

(6) $\tilde{f}(x) = f(x)$

(a) follows from (EL-WOPT) with (6)

and $\tilde{f}' = \tilde{f}$, $k^s = \text{emp}$.

(b) follows from (CKTC-EMP).

(C) follows since no env. changes



Case $(SC_LOOP\ I)$:

$\frac{}{S = \text{loop } x \text{ until } n_2 \text{ do } s} f' = f_2 \quad O = O_1; O_2$

Inverting $(SC_LOOP\ I)$:

(4) $f(x) \leq n_2$

(5) $f \vdash s \Downarrow f_1; O_1$

(6) $[f_1]_{\text{dom}(f)} [x \mapsto f(x) + 1] \vdash \text{loop } x \text{ until } n_2 \text{ do } s \Downarrow f_2; O_2$

Inverting (C_LOOP) on (1) :

(7) $\Gamma(x) = \text{uint}^P$

(8) $\Gamma \vdash s \rightsquigarrow \tilde{s} \mid \Gamma_i$

(9) $\Gamma' = \Gamma$

Using Lemma (3) with (2) and (7) :

(10) $\tilde{f}(x) = f(x) \text{ and } \tilde{f}(x) \leq n_2$

Using I.H. with (8), (2), and (5) :

(11) $\tilde{f} \vdash \tilde{s} \Downarrow \tilde{f}; k^s$

(12) $\hat{f}_1; \hat{f}_2 \vdash k^s \Downarrow \hat{f}', \hat{f}_2'; O_1$

(13) $\Gamma_1 \vdash f_1 \hookrightarrow \hat{f}_1; \hat{f}', \hat{f}_2'$

To do: change the env compilation judgment

We need to allow for $\cdot \hookrightarrow \cdot ; \hat{f}_1, \hat{f}_2$
Basically \hat{f}_1 and \hat{f}_2 grow additionally (never shrink)

A few lemmas:

- (i) If $\Gamma \vdash s \hookrightarrow \tilde{f} \mid \Gamma'$ then $\tilde{\Gamma} \supseteq \underline{\Gamma}$ (extension)
- (ii) If $\Gamma \vdash f \hookrightarrow \tilde{f} ; \hat{f}_1, \hat{f}_2$ then
 $\text{dom}(f) = \text{dom}(g)$ and $\text{dom}(\tilde{f}) \subseteq \text{dom}(f)$
- (iii) If $\Gamma \vdash f \hookrightarrow \tilde{f} ; \hat{f}_1, \hat{f}_2$
and $\Gamma, f \vdash \hat{f}_1 ; \tilde{f}'_1, \hat{f}'_2$
and $\tilde{\Gamma}' \supseteq \tilde{\Gamma}$ (i.e. extension of Γ)

Then

$$\Gamma \vdash [f_1]_{\text{dom } f} \hookrightarrow [\tilde{f}_1]_{\text{dom}(\tilde{f})} ; \hat{f}'_1, \hat{f}'_2$$

With lemma (iii) on (2) and (13):

$$(14) \quad \Gamma \vdash [f_1]_{\text{dom } f} \hookrightarrow [\tilde{f}_1]_{\text{dom}(\tilde{f})} ; \hat{f}'_1, \hat{f}'_2$$

Since $\Gamma(x) = \text{Unit } \mathbb{P}$, $\text{dom}(\Gamma) = \text{dom}(f)$

$$(15) \quad \Gamma \vdash [f_1]_{\text{dom } f} [x \mapsto f(x) + 1]$$

$$\hookrightarrow [\tilde{f}_1]_{\text{dom } \tilde{f}} [x \mapsto \tilde{f}(x) + 1] ; \hat{f}'_1, \hat{f}'_2$$

With (1), (15), using I.H. on (6):

$$(16) \quad [\tilde{f}_1]_{\text{dom } \tilde{f}} [x \mapsto \tilde{f}(x) + 1]$$

" \approx . , "

$\vdash_{\text{loop}} x \text{ until } n_2 \text{ do } \tilde{f}_2 \text{ ; } k'_2$

(17) $\tilde{f}'_1; \hat{f}'_2 \vdash_{\kappa^S_2} \tilde{f}''_1; \hat{f}''_2; O_2$

(18) $\Gamma \vdash f_2 \hookrightarrow \tilde{f}_2; \hat{f}''_1; \hat{f}''_2$

(a) follows with (EC-loop I) from (10), (11), (16)
with $\tilde{f}' = \tilde{f}_2$, $\kappa^S = k'_1; k'_2$

(b) follows from (EKTc-SEQ) with (12) and (17)

For (c), we want to prove

$\Gamma \vdash f_2 \hookrightarrow \tilde{f}_2; \hat{f}''_1; \tilde{f}''_2$

which follows from (18).



Cases (SC-AWRITE) and (SC-JF) showed
follow similarly.

Case SC-OUT : $S = \text{out } e$, $f' = f$

Inverting SC-OUT :

(4) $f \vdash e \Downarrow C$

(5) $O = C$

Inverting (C-OUT) on (1) :

(6) $\Gamma \vdash e : \sigma^m \rightarrow \tilde{e}$ (7a) $\tilde{S} = \text{out } \tilde{e}$

$$(6) \quad \Gamma \vdash e : \sigma \rightarrow c \quad (\text{?}) \quad \tilde{s} = \text{out } \tilde{e}$$

Using Lemma (6) with (6) & (2) :

$$(8) \quad C : \sigma \vdash \tilde{e} \Downarrow k^c$$

$$(9) \quad \tilde{f} \vdash \tilde{e} \Downarrow k^c$$

$$(10) \quad \hat{f}_1, \hat{f}_2 \vdash k^c \Downarrow b_1, b_2$$

$$(11) \quad C = D_m(b_1, b_2).$$

(a) follows from (EC-OUT) with (9)
 $k^s = \text{Out } k^c$ and $\tilde{f}' = \tilde{f}$

(b) follows from (10) and (11)
with $\hat{f}_1' = \hat{f}_1$ and $\hat{f}_2' = \hat{f}_2$

(c) is straightforward since none of the env changes.



Case $(\xi_{C-\text{SEQ}})$:

Using IH. we'll have :

$$(4) \quad \tilde{f} \vdash \tilde{s}, \Downarrow \hat{f}_1 ; k^s_1$$

$$(5) \quad \hat{f}_1 ; \hat{f}_2 \vdash k^s_1 \Downarrow \hat{f}_1 ; \hat{f}_2 ; O_1$$

$$(6) \quad \Gamma' \vdash f' \hookrightarrow \tilde{f}_1 ; \hat{f}_1 ; \hat{f}_2$$

$$(7) \quad \tilde{f}_1 \vdash \tilde{s}_2 \Downarrow \tilde{f}_2 ; k^s_2$$

(8) $\hat{f}_1'; \hat{f}_2' \vdash k_2 \Downarrow \hat{f}_1'', \hat{f}_2'' ; O_2$

(9) $\Gamma'' \vdash f'' \hookrightarrow \tilde{f}_2; \hat{f}_1'', \hat{f}_2''$

(a) follows from ($\in C\text{-SEQ}$)

(b) from ($Ck \cap C - S \in Q$)

(c) from (9).

■

Change premise in EC-Loop Γ to be source
 $(\gamma, [x] + 1)$ also in the Semantics.

Proof of Lemma 9 and 10

19 October 2017

16:52

By mutual induction

Induction on derivation (1) for \mathcal{G}

Induction on derivation (1) and $n_2 - f(x)$ for 16

Lemma 9 : (case analysis on (1))

Case C-DECL: $\Gamma' = \Gamma, x : z$

$$\text{Sub case } \tau = \sigma^p :$$

Using Lemma (4)

(3) \int_0^t $1 - e^{-\frac{1}{2} \sigma^2 s} c(s) ds$

(a) follows from (SC-DECL) with
with $f' = f(x \mapsto c)$

(b) follow from (EN-PBT)

Other cases are analogous.

 Case C_VASSN : Similar to (C-DECL).

Case C-FOR :

use c = x :
 $s = \text{for } x \text{ in } n_1..n_2 \text{ do } s \quad r' = r$

Inverting (C-for) :

$$(3) \quad \Gamma, x : \text{unit}^P \vdash \text{loop } x \text{ until } n_2 \text{ does } \rightarrow -$$

$\Gamma, x : \text{unit}^P$

Apply I'n. of Lemma (10) using (3)

with $P = P_0 \times \min^P$ and $f = f[x \mapsto n_1]$

(4) $f[x \mapsto n_1] \vdash_{\text{loop}} x \text{ until } n_2 \text{ does } \Downarrow f'$; 0

(5) $\Gamma, x : \text{uint}^P \vdash f' \hookrightarrow \tilde{\Gamma}' ; \hat{\tilde{\Gamma}}'_1, \hat{\tilde{\Gamma}}'_2$

(a) follows from (EC-FORT) with (4) and

$$f' = f' \setminus \{x\}$$

To show (b), we need to show :

$$\Gamma \vdash f' \setminus \{x\} \hookrightarrow \dots$$

follows from (5)

(case C_LOOP covered by Lemma 10)

Other cases should be analogous.

Lemma 10 : Inverting (1) :

(3) $\Gamma(x) = \text{uint}^P$

(4) $\Gamma \vdash s \rightsquigarrow \tilde{s} \mid \Gamma'$

(5) $x \notin \text{modifiers}(s)$

Using Lemma (3) :

(6) $f(x) : \text{uint}$

if $f(x) > n_2$ Then (EC-COUNT)

else Using Inv. on Lemma (1) with (4) :

(7) $f \vdash s \Downarrow f, j^0$

Since $x \notin \text{modifiers}(s)$, $f(x) = f(x)$

Let $f_2 = [f_1]_{\text{dom}(f)} \left(x \mapsto f(x) + 1 \right)$

We have $\vdash f_2 \hookrightarrow \neg j \dashv \dashv$

and $n_2 - f_2(x) < n_2 - f(x)$

\therefore we can use Thm. to get

(8) $f_2 \vdash \text{loop } x \text{ until } n_2 \text{ do } s \Downarrow f_3 ; 0_2$

(9) $\vdash f_3 \hookrightarrow \neg j \dashv \dashv$

Now (a) follows using $(SC_LOOP \sqsupseteq)$

and (b) follows from (9).



Proof of Theorem (1)

19 October 2017

22:34

Using Lemmas (8), (9), and (10).