Proof of Lemma 4

18 October 2017 00:32

By induction on (1), analysis on last rule

Case S_CONS : $e = C$, $\sigma = \text{typeof}(c)$, $\tilde{e} = C$

(a) follows from (SE_CONST).

(b) follows from (V_CONS)

(c) follows from (EE_CONST) ∎

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) ∎

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) $f \vdash e_2 \Downarrow c_2$

(10) $c_2 : \text{uint}$

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

Using Lemma (1):

(12) $c_1 = n_1$

(13) $c_2 = n_2$

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

(b) follows from (V_CONS)

(c) follows from (EE_PADD) using (8) and (11), with (12) and (13) ∎

Case S_COND: $e = \text{cond}(e, e_1, e_2)$, $\tilde{e} = \text{cond}_\ell(\tilde{e}, \tilde{e_1}, \tilde{e_2})$

In the rule (S_COND), since $d' = P$, we must have $\ell = P$

∴ Inverting (S_COND), we get:

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

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

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

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

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

(10) $\tilde{\mathcal{F}} \vdash e_1 \Downarrow c_1$ (11) $c_1 : \sigma$ (12) $\mathcal{F} \vdash e_1 \Downarrow c_1$

(13) $\tilde{\mathcal{F}} \vdash e_2 \Downarrow c_2$ (14) $c_2 : \sigma$ (15) $\tilde{\mathcal{F}} \vdash \tilde{e}_2 \Downarrow c_2$

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

Subcase $c = T$:

(a) follows from (SE_COND) with (7) and (10), and $v = c_1$

(b) follows from (11)

(c) follows from (EE_PCOND) with (9) and (12)

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

Case S_GT : Similar to (S_ADD)

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) $\Gamma \vdash e : \mathrm{int}^{P} \rightsquigarrow \tilde{e}$

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

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

(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) $f(n) = [c_i]_n$

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

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

Soundness of bounds checking:

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

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

(2) $\Gamma \models e < n$

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

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

Then $n' < n$

Using I.H. on (5):

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

(11) $c : \text{uint}$

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

Using Lemma (1) on (11):

(13) $c = n'$

Using soundness of bounds checking

with (5), (6), (9), and (10):

(13) $n' < n$

Using (SE_VAR) with (7):

(14) $\S \vdash x \Downarrow [C_i]_n$

Using (EE_VAR) with (9):

(15) $\S \vdash x \Downarrow [C_i]_n$

(a) follows from (SE_AREAD) with (14), (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 : $e = x$, $\tau = \sigma^{\mathbb{P}}[n]$, $\tilde{e} = x$

Using Lemma (3). (3) :

(3) $g(x) = [C_i]_n$

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

(5) $f(x) = [C_i]_n$

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

Using Lemma (4) with (3) :

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

(6) $C_i : \sigma$

(7) $\tilde{f} \vdash \tilde{e_i} \Downarrow c_i$

(a) follows from (SE_ARR) with (5) and $V = [c_i]_n$

(b) follows from (6)

(c) follows from (EE_ARR) with (7). ▨

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) $f(x) = c$

(5) $c : \sigma$

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

(7) $(\hat{f}_1[r], \hat{f}_2[r]) = \mathcal{E}_m(c)$

(a) follows from (SE_VAR)

(b) follows from (5)

(c) follows from (EE_VAR) with $k^e = r$

(d) follows from (EKTE_R)

(e) follows from (7). ∎

Assume : $\mathcal{D}_m(\mathcal{E}_m(c)) = c$ (Lemma ED)

Case S_ADD : $e = e_1 + e_2$, $\ell = A$, $\tilde{e} = \tilde{e_1} + \tilde{e_2}$

Inverting (S_ADD) :

(3) $\Gamma \vdash e_1 : \text{uint}^A \rightsquigarrow \tilde{e_1}$

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

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

..

(5) $\mathcal{G} \vdash e_1 \Downarrow c_1$

(6) $c_1 : \mathrm{uint}$

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

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

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

(10) $\mathcal{G} \vdash e_2 \Downarrow c_2$

(11) $c_2 : \mathrm{uint}$

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

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

(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_SADD) with (7) and (12), and $k^e = \mathrm{Add}(k_1^e, k_2^e)$

(d) follows from (CKTE_ADD) with (8), (13), (9), (14), (15), (16), and $(b_1, b_2) = \mathcal{E}_A(n_1 + n_2)$

(e) follows from (Lemma ED). ∎

Case S_COND : We have two subcases, $l = P$ or $l = IS$

Subcase S_COND: $e = cond(e, e_1, e_2)$, $l = P$, $l' = m$, $\tilde{e} = cond(\tilde{e}, \tilde{e_1}, \tilde{e_2})$

Inverting (S_COND), we get :

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

(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) $f \vdash e \Downarrow c$

(7) $c : bool$

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

Using Lemma (1) with (7) :

(9) $c = T$ or $c = \bot$

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

(10) $f \vdash e_1 \Downarrow c_1$

(11) $c_1 : \sigma$

(12) $\tilde{f} \vdash \tilde{e_1} \Downarrow k^e_1$

(13) $\hat{f}_1, \hat{f}_2 \vdash k^e_1 \Downarrow b_{11}, b_{21}$

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

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

(16) $c_2 : \sigma$

(17) $\tilde{f} \vdash \tilde{e_2} \Downarrow k^e_2$

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

(19) $c_2 = Dm(b_{12}, b_{22})$

(a) follows from (SE_COND) with (6), (7), (9), (10) & (15) with $v = c_1$ if $c = T$, $v = c_2$ if $c = \bot$

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

(c) follows from (EE_PCOND) with (8), (9), (12), (17) with $k^Q = k_1^e$ if $c = T$, $\tilde{v} = k_2^e$ if $c = \bot$

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

(e) follows from (14) if $c = T$, (19) if $c = \bot$ •

Subcase S_COND: $k = B$, $e = cond(e, e_1, e_2)$, $\tilde{e} = cond_k(\tilde{e}, \tilde{e_1}, \tilde{e_2})$

$m = k' = B$

Inverting (S_COND):

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

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

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

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

(6) $\rho \vdash e \Downarrow c$

(7) $c : bool$

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

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

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

(11) $\rho \vdash e_1 \Downarrow c_1$ (12) $c_1 : \sigma$ (13) $\tilde{\rho} \vdash \tilde{e_1} \Downarrow k_1^e$

(14) $\hat{\rho}_1, \hat{\rho}_2 \vdash k_1^e \Downarrow b_{11}, b_{21}$ (15) $c_1 = D_B(b_{11}, b_{21})$

(16) $\rho \vdash e_2 \Downarrow c_2$ (17) $c_2 : \sigma$ (18) $\tilde{\rho} \vdash \tilde{e}_2 \Downarrow k^e_2$

(19) $\hat{\rho}_1, \hat{\rho}_2 \vdash k^e_2 \Downarrow b_{12}, b_{22}$ (20) $c_2 = \mathcal{D}_B(b_{12}, b_{22})$

And Lemma (1) with (7) gives:

(21) $c = T$ or $c = \underline{1}$

(a) follows with (6), (21), (11), and (16) with
$v = c_1$ if $c = T$, $v = c_2$ if $c = \underline{1}$

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

(c) follows from (EE_SCOND) with (8), (13), and (18)
and $k^e = \mathrm{Max}(k^e, k^e_1, k^e_2)$

(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 $c = T$

(e) follows from (Lemma ED).

Case S_GT: (Similar to S_ADD)

Case S_AREAD: Should follows proof of scalar expressions.

Case S_INP: $e = \mathrm{in}_j$, $\tilde{e} = \mathrm{in}^m_j$

Input assumption: If $\Gamma \vdash \mathrm{in}_j : \sigma^m$ ws in^m_j

$\rho \vdash \mathrm{in}_j \Downarrow c_1$

$\tilde{\rho} \vdash \mathrm{in}^m_j \Downarrow \mathrm{In}^m_j$

$\hat{\rho}_1, \hat{\rho}_2 \vdash \mathrm{In}^m_j \Downarrow \mathcal{E}_m(c_2)$

Then $c_i : \sigma$ and $c_1 = c_2$

The proof follows from input assumption. ∎

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) $\rho \vdash e \Downarrow c$

(5) $c : \sigma$

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

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

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

(d) follows from (EKTE_COERCEC), with $(b_1, b_2) = \mathcal{E}_m(c)$

(e) follows from Lemma ED. ∎

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) $\rho \vdash e \Downarrow c$

(5) $C : \sigma$

(6) $\tilde{\rho} \vdash \tilde{e'} \Downarrow ke'$

(7) $\hat{f}_1, \hat{f}_2 \vdash ke' \Downarrow b_1', b_2'$

(8) $C = D_{m'}(b_1', b_2')$

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

(c) follows from (EE_COERCE) with $ke = ke' \triangleright m$

(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 I.H.

Both follow the same pattern as Lemma (5)

Other cases are not possible.

Proof of Lemma (8)

18 October 2017 15:48

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

Case C_DECL : $S = \psi\ x = e$, $\widetilde{S} = \tau\ x = \widetilde{e}$, $\Gamma' = \Gamma, x : \tau$

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) $\Gamma \vdash e : \sigma^p \rightsquigarrow \widetilde{e}$

Using Lemma (4) with (4) :

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

For (3), only (SC_DECL) is possible. Therefore :

(6) $f' = f[x \mapsto C]$ (7) $O = \bullet$

(a) follows from (EC_DECL) with (7)

and $\widetilde{f}' = \widetilde{f}[x \mapsto C]$, $k^s = \bullet$

(b) follows from (CKTC_EMP) with $\hat{p}_i' = \hat{p}_i$

To prove (c), we need :

$$\Gamma, x : \sigma^p \vdash f[x \mapsto C] \hookrightarrow \widetilde{f}[x \mapsto C]; \hat{f}_1, \hat{f}_2$$

which follows from (EN_PST) with (6) & (2) ●

We assume α-renaming, i.e. whenever we write $\Gamma, x : \tau$, x is fresh in Γ.

Lemma: $\Gamma \vdash \rho \hookrightarrow \tilde{\rho}; -, - \Rightarrow dom(\Gamma) = dom(\rho) \wedge dom(\tilde{\rho}) \subseteq dom(\Gamma)$

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

Inverting (C_DECL):

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

Using Lemma (6):

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

(8) $\hat{\rho}_1, \hat{\rho}_2 \vdash k^e \Downarrow b_1, b_2$ (9) $c = Dm(b_1, b_2)$

For (3) only (C_DECL) is possible. So:

(10) $\rho' = \rho[x \mapsto c]$ (11) $\theta = \cdot$

(a) follows from (EC_DECLCKT) with (7) and $\tilde{\rho}' = \tilde{\rho}[x \mapsto r]$, $k^s = Bind(k^e, r)$

(b) follows from (CKTC_BIND) with 8 and $\hat{\rho}_1' = \hat{\rho}_1[r \mapsto b_1]$, $\hat{\rho}_2' = \hat{\rho}_2[r \mapsto b_2]$

For (c) we want to show:

$\Gamma, x : \sigma^m \; (x) = \sigma^m$ ✓

$\rho'(x) = c$ ✓

$c : \sigma$ → from (6) ✓

$r \notin \tilde{\rho}$ → from (EC_DECLCKT) ✓

$b_1, b_2 = \mathcal{E}_m(c)$ → (from 4)) ✓

$\Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2$ ✓ from premise

$b_1, b_2 = \text{cmd}(\ell) \to (\text{from } \Theta)$ ✓

$\Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2$ ✓ from premise

$\Gamma, x : \sigma^m \vdash \rho' \hookrightarrow \tilde{\rho}[x \mapsto r]; \hat{\rho}_1[r \mapsto b_1], \hat{\rho}_2[r \mapsto b_2]$

follows from (EN_SBT). ●

Array subcases are analogous

■

Case (C_VASSGN): Similar to variable declaration case with no array subcases.

■

Case (C_FOR):

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

$\tilde{S} = \text{for } x \text{ in } n_1 .. n_2 \text{ do } \tilde{s}$

$\Gamma' = \Gamma$

Inverting (C_FOR):

(4) $\Gamma, x : \text{uint}^\rho \vdash s \rightsquigarrow \tilde{s} \mid \Gamma_1$

Only rule possible for (3) is (SC_FORT). So:

(5) $\rho[x \mapsto n_1] \vdash \text{loop } x \text{ until } n_2 \text{ do } s \Downarrow \rho_1; \diamond$

(6) $\rho' = \rho_1 \setminus \{x\}$