Proof of Lemma 4

18 October 2017 00:32

By induction on (1), analysis on last rule

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

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

(a) follows from (SE_VAR)

(b) follows from (4) $\blacksquare$

(c) follows from (EE_VAR)

Case S_ADD : $e = e_1 + e_2$, $\sigma = uint$, $\tilde{e} = \tilde{e}_1 +_P \tilde{e}_2$

From the premises of (S_ADD):

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

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

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

(6) $\rho \vdash e_1 \Downarrow c_1$

(7) $c_1 : uint$

(8) $\tilde{\rho} \vdash \tilde{e}_1 \Downarrow c_1$

(9) $\rho \vdash e_2 \Downarrow c_2$

(10) $c_2 : uint$

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

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 ($\Downarrow$_CONS)

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

Case S_COND: $e = cond(e, e_1, e_2)$, $\tilde{e} = cond_\ell(\tilde{e}, \tilde{e}_1, \tilde{e}_2)$

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

∴ Inverting (S_COND), we get:

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

(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) $\rho \vdash e \Downarrow c$ (8) $c : bool$ (9) $\tilde{\rho} \vdash \tilde{e} \Downarrow c$

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

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

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

Subcase $c = \top$:

(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 $c = \top$ ∎

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

(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) $\rho(x) = [c_i]_n$

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

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

Soundness of bounds checking:

$\forall \Gamma, e, n, \rho$

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

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

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

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

Then $n' < n$

Using I.H. on (5):

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

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

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

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) $\xi \vdash x \Downarrow [c_i]_n$

Using (EE_VAR) with (9) :

(15) $\xi \vdash x \Downarrow [c_i]_n$

(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 $\tilde{w}_n = c'_{n}$ ∎

<u>Case S-INP</u> : Not possible

<u>Case S_SUB</u> : Not possible

<u>Case S_ARR</u> : Not possible

$\boxed{\text{Qed}}$

Proof of Lemma (5)

18 October 2017 00:39

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) $\rho(x) = c$

(5) $c : \sigma$

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

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

(a) follows from (SE_VAR)

(b) follows from (5)

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

(d) follows from (KTE_R)

(e) follows from (7). ■

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

Case S_ADD : $e = e_1 + e_2$, $l = A$, $\tilde{e} = \tilde{e}_1 + \tilde{e}_2$

Inverting (S_ADD) :

(3) $\Gamma \vdash e_1 : uint^A \rightsquigarrow \tilde{e}_1$

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

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

(5) $\rho \vdash e_1 \Downarrow c_1$

(6) $c_1 : uint$

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

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

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

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

(11) $c_2 : uint$

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

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

(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
$k^e = Add(k_1^e, k_2^e)$

(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). ∎