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

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

(7) $c_1 : \text{uint}$

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

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

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

(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) ∎

<u>Case S_COND</u>: $e = \text{cond}(e, e_1, e_2)$, $\tilde{e} = \text{cond}_\ell(\tilde{e}, \tilde{e}_1, \tilde{e}_2)$

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

$\therefore$ 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) $\rho \vdash e \Downarrow c$ (8) $c : \text{bool}$ (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) $\Gamma \vdash e : \mathrm{uint}^P \rightsquigarrow \tilde{e}$

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

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

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

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):

(12') $c = n'$

Using soundness of bounds checking

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

(13) $n' < n$

Using (SE_VAR) with (7):

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

Using (EE_VAR) with (9):

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

(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