Explicit CN Soundness Proof

Dhruv Makwana

June 21, 2021

1 Weakening

If $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \sqsubseteq \mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}'$ and $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash J$ then $\mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}' \vdash J$.

PROOF SKETCH: Induction over the typing judgements.

ASSUME: 1. $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \sqsubseteq \mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}'$
2. $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash J$

PROVE: $\mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}' \vdash J$.

2 Substitution

2.1 Weakening for Substitution

Weakening for substitution: as above, but with $J = (\sigma) : (\mathcal{C}''; \mathcal{L}''; \Phi''; \mathcal{R}'')$.

PROOF SKETCH: Induction over the substitution.

ASSUME: 1. $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \sqsubseteq \mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}'$
2. $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash (\sigma) : (\mathcal{C}''; \mathcal{L}''; \Phi''; \mathcal{R}'')$

PROVE: $\mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}' \vdash (\sigma) : (\mathcal{C}''; \mathcal{L}''; \Phi''; \mathcal{R}'')$.

2.2 Substitution Lemma

If $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash (\sigma) : (\mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}')$ and $\mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}' \vdash J$ then $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash \sigma(J)$.

PROOF SKETCH: Induction over the typing judgements.

ASSUME: 1. $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash (\sigma) : (\mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}')$
2. $\mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}' \vdash J$

PROVE: $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash \sigma(J)$.

$\langle 1 \rangle 1$. CASE: TY_PVAL_VAR.
$\mathcal{C}'; \mathcal{L}'; \Phi' \vdash x \Rightarrow \beta$

$\langle 2 \rangle 1$. Have $x : \beta \in \mathcal{C}'$ (or $x : \beta \in \mathcal{L}'$).

$\langle 2 \rangle 2$. So $\exists \mathit{pval}.\ \mathcal{C}; \mathcal{L}; \Phi \vdash \mathit{pval} \Rightarrow \beta$ by TY_SUBS_CONS_{COMP,LOG}.

$\langle 2 \rangle 3$. Since $\mathit{pval} = \sigma(x)$, we are done.

⟨1⟩2. CASE: TY_TPE_LET.
$\mathcal{C}'; \mathcal{L}'; \Phi' \vdash \texttt{let}\ \mathit{pat} = \mathit{pexpr}\ \texttt{in}\ \mathit{tpexpr} \Leftarrow y_2 : \beta_2.\ \mathit{term}_2$

⟨2⟩1. By induction,
1. $\mathcal{C}; \mathcal{L}; \Phi \vdash \sigma(\mathit{pexpr}) \Rightarrow y_1 : \beta_1.\ \sigma(\mathit{term}_1)$
2. $\mathcal{C}, \mathcal{C}_1; \mathcal{L}, y_1 : \beta_1; \Phi, \mathit{term}_1, \Phi' \vdash \sigma(\mathit{tpexpr}) \Leftarrow y_2 : \beta_2.\ \sigma(\mathit{term}_2)$.

⟨2⟩2. $\mathcal{C}; \mathcal{L}; \Phi \vdash \sigma(\texttt{let}\ \mathit{pat} = \mathit{pexpr}\ \texttt{in}\ \mathit{tpexpr} \Leftarrow y_2 : \beta_2.\ \mathit{term}_2)$ as required.

⟨1⟩3. CASE: TY_TVAL_LOG.
$\mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}' \vdash \texttt{done}\ \mathit{pval}, \overline{\mathit{spine\_elem}} \Leftarrow \exists y : \beta.\ \mathit{ret}$

⟨2⟩1. By inversion and then induction,
1. $\mathcal{C}; \mathcal{L}; \Phi \vdash \sigma(\mathit{pval})\beta$
2. $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash \sigma(\texttt{done}\ \overline{\mathit{spine\_elem}}) \Leftarrow \sigma([\mathit{pval}/y]\mathit{ret})$.

⟨2⟩2. Therefore $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash \sigma(\texttt{done}\ \mathit{pval}, \overline{\mathit{spine\_elem}} \Leftarrow \exists y : \beta.\mathit{ret})$.

⟨1⟩4. CASE: TY_SPINE_RES.
$\mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}'_1, \mathcal{R}_2 \vdash x = \mathit{res\_term}, \overline{x = \mathit{spine\_elem}} :: \mathit{res} \multimap \mathit{arg} \gg \mathit{res\_term}/x, \psi; \mathit{ret}$

⟨2⟩1. By inversion and then induction,
1. $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R}_1 \vdash \underline{x = \sigma(\mathit{res\_term})} \Leftarrow \sigma(\mathit{res})$
2. $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R}_2 \vdash \overline{x = \sigma(\mathit{spine\_elem})} :: \sigma(\mathit{res}) \multimap \sigma(\mathit{arg}) \gg \sigma(\psi); \sigma(\mathit{ret})$

⟨2⟩2. Hence $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R}_1, \mathcal{R}_2 \vdash \sigma(x = \mathit{res\_term}, \overline{x = \mathit{spine\_elem}} :: \mathit{res} \multimap \mathit{arg} \gg \mathit{res\_term}/x, \psi; \mathit{ret})$

2.3 Identity Extension

If $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash (\sigma) : (\mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}')$ then $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R}_1, \mathcal{R} \vdash (\sigma, \mathrm{id}) : (\mathcal{C}, \mathcal{C}'; \mathcal{L}, \mathcal{L}'; \Phi, \Phi'; \mathcal{R}_1, \mathcal{R}')$.

PROOF SKETCH: Induction over the substitution.

ASSUME: $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash (\sigma) : (\mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}')$

PROVE: $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R}_1, \mathcal{R} \vdash (\sigma, \mathrm{id}) : (\mathcal{C}, \mathcal{C}'; \mathcal{L}, \mathcal{L}'; \Phi, \Phi'; \mathcal{R}_1, \mathcal{R}')$.

2.4 Usable Substitution Lemma

If $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash (\sigma) : (\mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}')$ and $\mathcal{C}, \mathcal{C}'; \mathcal{L}, \mathcal{L}'; \Phi, \Phi'; \mathcal{R}_1, \mathcal{R}' \vdash J$ then $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R}_1, \mathcal{R} \vdash \sigma(J)$.

PROOF SKETCH: Apply identity extension then substitution lemma.

ASSUME: 1. $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash (\sigma) : (\mathcal{C}'; \mathcal{L}'; \Phi'; \mathcal{R}')$
2. $\mathcal{C}, \mathcal{C}'; \mathcal{L}, \mathcal{L}'; \Phi, \Phi'; \mathcal{R}_1, \mathcal{R}' \vdash J$

PROVE: $\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R}_1, \mathcal{R} \vdash \sigma(J)$.

3 Progress

If $\cdot; \cdot; \cdot; \mathcal{R} \vdash e \Leftrightarrow t$ then either value(e) or $\forall h : R.\ \exists e', h'.\ \langle h; e \rangle \longrightarrow \langle h'; e' \rangle$.

PROOF SKETCH: Induction over the typing rules.

ASSUME: $\cdot;\cdot;\cdot;\mathcal{R} \vdash e \Leftrightarrow t$
PROVE: either value(e) or $\forall h : R.\ \exists e', h'.\ \langle h; e\rangle \longrightarrow \langle h'; e'\rangle$.

4 Framing

If $\langle h_1; e\rangle \longrightarrow \langle h_1'; e'\rangle$ and h_1, h_2 disjoint then $\langle h_1 + h_2; e\rangle \longrightarrow \langle h_1' + h_2; e'\rangle$.

PROOF SKETCH: Induction over the operational rules.

ASSUME: 1. $\langle h_1; e\rangle \longrightarrow \langle h_1'; e'\rangle$
2. h_1, h_2 disjoint.

PROVE: $\langle h_1 + h_2; e\rangle \longrightarrow \langle h_1' + h_2; e'\rangle$.

5 Type Preservation

If $\cdot;\cdot;\cdot;\mathcal{R} \vdash e \Leftrightarrow t$ then $\forall h : \mathcal{R}, e', h' : \mathcal{R}'.\ \langle h; e\rangle \longrightarrow \langle h'; e'\rangle \implies \cdot;\cdot;\cdot;\mathcal{R}' \vdash e' \Leftrightarrow t$.

PROOF SKETCH: Induction over the typing rules.

ASSUME: 1. $\cdot;\cdot;\cdot;\mathcal{R} \vdash e \Leftrightarrow t$
2. arbitrary $h : \mathcal{R}, e', h' : \mathcal{R}'$
3. $\langle h; e\rangle \longrightarrow \langle h'; e'\rangle$.

PROVE: $\cdot;\cdot;\cdot;\mathcal{R}' \vdash e' \Leftrightarrow t$.

6 Typing Judgements

object_value_jtype	$::=$	
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi \vdash \mathit{object\_value} \Rightarrow \texttt{obj}\, \beta$
pval_jtype	$::=$	
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi \vdash \mathit{pval} \Rightarrow \beta$
res_jtype	$::=$	
	$\mid$	$\Phi \vdash \mathit{res} \equiv \mathit{res}'$
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash \mathit{res\_term} \Leftarrow \mathit{res}$
spine_jtype	$::=$	
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash \overline{x_i = \mathit{spine\_elem}_i}^{\,i} :: \mathit{arg} \gg \sigma; \mathit{ret}$
pexpr_jtype	$::=$	
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi \vdash \mathit{pexpr} \Rightarrow \mathit{ident}{:}\beta.\, \mathit{term}$
tpval_jtype	$::=$	
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi \vdash \mathit{tpval} \Leftarrow \mathit{ident}{:}\beta.\, \mathit{term}$
tpexpr_jtype	$::=$	
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi \vdash \mathit{tpexpr} \Leftarrow \mathit{ident}{:}\beta.\, \mathit{term}$
action_jtype	$::=$	
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash \mathit{mem\_action} \Rightarrow \mathit{ret}$
memop_jtype	$::=$	
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash \mathit{mem\_op} \Rightarrow \mathit{ret}$
seq_expr_jtype	$::=$	
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash \mathit{seq\_expr} \Rightarrow \mathit{ret}$
is_expr_jtype	$::=$	
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash \mathit{is\_expr} \Rightarrow \mathit{ret}$
tval_jtype	$::=$	
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash \mathit{tval} \Leftarrow \mathit{ret}$
texpr_jtype	$::=$	
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash \mathit{seq\_texpr} \Leftarrow \mathit{ret}$
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash \mathit{is\_texpr} \Leftarrow \mathit{ret}$
	$\mid$	$\mathcal{C}; \mathcal{L}; \Phi; \mathcal{R} \vdash \mathit{texpr} \Leftarrow \mathit{ret}$

7 Opsem Judgements

$\mathit{pure\_opsem\_jtype}$	$::=$	
	$\mid$	$\langle \mathit{pexpr} \rangle \longrightarrow \langle \mathit{pexpr}' \rangle$
	$\mid$	$\langle \mathit{pexpr} \rangle \longrightarrow \langle \mathit{tpexpr}{:}(y{:}\beta.\, \mathit{term}) \rangle$
	$\mid$	$\langle \mathit{tpexpr} \rangle \longrightarrow \langle \mathit{tpexpr}' \rangle$

$\mathit{opsem\_jtype}$	$::=$	
	$\mid$	$\langle \mathit{seq\_expr} \rangle \longrightarrow \langle \mathit{texpr}{:}\mathit{ret} \rangle$
	$\mid$	$\langle h; \mathit{seq\_texpr} \rangle \longrightarrow \langle h'; \mathit{texpr} \rangle$
	$\mid$	$\langle h; \mathit{mem\_op} \rangle \longrightarrow \langle h'; \mathit{tval} \rangle$
	$\mid$	$\langle h; \mathit{mem\_action} \rangle \longrightarrow \langle h'; \mathit{tval} \rangle$
	$\mid$	$\langle h; \mathit{is\_expr} \rangle \longrightarrow \langle h'; \mathit{is\_expr}' \rangle$
	$\mid$	$\langle h; \mathit{is\_texpr} \rangle \longrightarrow \langle h'; \mathit{texpr} \rangle$
	$\mid$	$\langle h; \mathit{texpr} \rangle \longrightarrow \langle h'; \mathit{texpr}' \rangle$