Explicit CN Soundness Proof

Dhruv Makwana

June 16, 2021

1 Typing Judgements

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

$$
\begin{array}{lll}
 & | & \mathcal{C};\mathcal{L};\Phi;\mathcal{R} \vdash \mathit{tval} \Leftarrow \mathit{ret} \\
\\
\mathit{texpr\_jtype} & ::= & \\
 & | & \mathcal{C};\mathcal{L};\Phi;\mathcal{R} \vdash \mathit{seq\_texpr} \Leftarrow \mathit{ret} \\
 & | & \mathcal{C};\mathcal{L};\Phi;\mathcal{R} \vdash \mathit{is\_texpr} \Leftarrow \mathit{ret} \\
 & | & \mathcal{C};\mathcal{L};\Phi;\mathcal{R} \vdash \mathit{texpr} \Leftarrow \mathit{ret}
\end{array}
$$

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

3 Substitution

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

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

4 Opsem Judgements

$$
\begin{array}{lll}
\mathit{pure\_opsem\_jtype} & ::= & \\
 & | & \langle \mathit{pexpr} \rangle \longrightarrow \langle \mathit{pexpr}' \rangle \\
 & | & \langle \mathit{pexpr} \rangle \longrightarrow \langle \mathit{tpexpr}{:}(y{:}\beta.\,\mathit{term}) \rangle \\
 & | & \langle \mathit{tpexpr} \rangle \longrightarrow \langle \mathit{tpexpr}' \rangle \\
\\
\mathit{opsem\_jtype} & ::= & \\
 & | & \langle \mathit{seq\_expr} \rangle \longrightarrow \langle \mathit{texpr}{:}\mathit{ret} \rangle \\
 & | & \langle h; \mathit{seq\_texpr} \rangle \longrightarrow \langle h'; \mathit{texpr} \rangle \\
 & | & \langle h; \mathit{mem\_op} \rangle \longrightarrow \langle h'; \mathit{tval} \rangle \\
 & | & \langle h; \mathit{mem\_action} \rangle \longrightarrow \langle h'; \mathit{tval} \rangle \\
 & | & \langle h; \mathit{is\_expr} \rangle \longrightarrow \langle h'; \mathit{is\_expr}' \rangle \\
 & | & \langle h; \mathit{is\_texpr} \rangle \longrightarrow \langle h'; \mathit{texpr} \rangle \\
 & | & \langle h; \mathit{texpr} \rangle \longrightarrow \langle h'; \mathit{texpr}' \rangle
\end{array}
$$

5 Progress

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

6 Framing

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

7 Type Preservation

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