

1 Formal Development

Correctness theorem that we will aim at:

If:

- $\Gamma \vdash s \rightsquigarrow \tilde{s} \mid \Gamma'$
- $\Gamma \sim \rho$
- $\Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2$
- $\rho \vdash s \downarrow \rho'; O$

Then:

- $\tilde{\rho} \vdash \tilde{s} \Longrightarrow \tilde{\rho}'; \kappa$
- $\hat{\rho}_1, \hat{\rho}_2 \vdash \kappa \longmapsto \tilde{\rho}'_1, \tilde{\rho}'_2; O$

σ	$::=$	Base type
		uint
		bool
ψ	$::=$	Source type
		σ
		$\sigma[n]$
c	$::=$	Constant
		n
		\top
		\perp
e	$::=$	Source expression
		c
		x
		$e_1 + e_2$
		cond (e, e_1, e_2)
		$e_1 > e_2$
		$x[e]$
		input $_i^\sigma$
s	$::=$	Source statement
		ψx
		$x := e$
		for x in $n_1 \dots n_2 \{s\}$
		$x[e_1] := e_2$
		if (e, s_1, s_2)
		out e
		$s_1; s_2$

Figure 1: Source language

v	$::=$	Source value
		c
		$[c_i]_n$
ρ	$::=$	Source runtime environment
		\cdot
		$\rho[x \mapsto v]$
O	$::=$	Source observation
		\cdot
		v, O

Figure 2: Source runtime

$$\boxed{\rho \vdash e \downarrow v}$$

$$\begin{array}{c}
\frac{}{\rho \vdash c \downarrow c} \text{ SE_CONST} \\
\\
\frac{}{\rho \vdash x \downarrow \rho(x)} \text{ SE_VAR} \\
\\
\frac{\rho \vdash e_i \downarrow n_i}{\rho \vdash e_1 + e_2 \downarrow n_1 + n_2} \text{ SE_ADD} \\
\\
\frac{\begin{array}{l} \rho \vdash e \downarrow c \\ c = \top \Rightarrow i = 1 \\ c = \perp \Rightarrow i = 2 \\ \rho \vdash e_i \downarrow v \end{array}}{\rho \vdash \mathbf{cond}(e, e_1, e_2) \downarrow v} \text{ SE_COND} \\
\\
\frac{\rho \vdash e_i \downarrow n_i}{\rho \vdash e_1 > e_2 \downarrow n_1 > n_2} \text{ SE_GT} \\
\\
\frac{\begin{array}{l} \rho \vdash e \downarrow n_1 \\ \rho \vdash x \downarrow [c_i]_{n_2} \\ n_1 < n_2 \end{array}}{\rho \vdash x[e] \downarrow c_n} \text{ SE_AREAD} \\
\\
\frac{\begin{array}{l} \sigma = \mathbf{bool} \Rightarrow c = \top \vee c = \perp \\ \sigma = \mathbf{uint} \Rightarrow c = n \end{array}}{\rho \vdash \mathbf{input}_i^\sigma \downarrow c} \text{ SE_INP}
\end{array}$$

Figure 3: Source expression evaluation

$$\boxed{\rho \vdash s \downarrow \rho'; O}$$

$$\begin{array}{c}
\frac{\text{default}(\psi) = v}{\rho \vdash \psi \ x \downarrow \rho[x \mapsto v]; \cdot} \quad \text{SC_DECL} \\
\\
\frac{\rho \vdash e \downarrow v}{\rho \vdash x := e \downarrow \rho[x \mapsto v]; \cdot} \quad \text{SC_ASSGN} \\
\\
\frac{\rho[x \mapsto n_1] \vdash \mathbf{loop} \ x \ \mathbf{until} \ n_2 \ \{s\} \downarrow \rho_1; O}{\rho \vdash \mathbf{for} \ x \ \mathbf{in} \ n_1 \dots n_2 \ \{s\} \downarrow \rho_1 \setminus x; O} \quad \text{SC_FORT} \\
\\
\frac{\rho(x) > n_2}{\rho \vdash \mathbf{loop} \ x \ \mathbf{until} \ n_2 \ \{s\} \downarrow \rho; O} \quad \text{SC_LOOP} \\
\\
\frac{\begin{array}{l} \rho(x) \leq n_2 \\ \rho \vdash s \downarrow \rho_1; O_1 \\ ([\rho_1]_{\text{dom}(\rho)})[x \mapsto \rho(x) + 1] \vdash \mathbf{loop} \ x \ \mathbf{until} \ n_2 \ \{s\} \downarrow \rho_2; O_2 \end{array}}{\rho \vdash \mathbf{loop} \ x \ \mathbf{until} \ n_2 \ \{s\} \downarrow \rho_2; O_1, O_2} \quad \text{SC_LOOPI} \\
\\
\frac{\begin{array}{l} \rho \vdash x \downarrow [c_i]_{n_2} \\ \rho \vdash e_1 \downarrow n_1 \\ \rho \vdash e_2 \downarrow c \\ n_1 < n_2 \end{array}}{\rho \vdash x[e_1] := e_2 \downarrow \rho[x \mapsto [c_i]_{n_2}[n_1 \mapsto c]]; \cdot} \quad \text{SC_AWRITE} \\
\\
\frac{\begin{array}{l} \rho \vdash e \downarrow c \\ c = \top \Rightarrow i = 1 \\ c = \perp \Rightarrow i = 2 \\ \rho \vdash s_i \downarrow \rho'; O \end{array}}{\rho \vdash \mathbf{if}(e, s_1, s_2) \downarrow \rho'; O} \quad \text{SC_IF} \\
\\
\frac{\rho \vdash e \downarrow v}{\rho \vdash \mathbf{out} \ e \downarrow \rho; v, \cdot} \quad \text{SC_OUT} \\
\\
\frac{\begin{array}{l} \rho \vdash s_1 \downarrow \rho_1; O_1 \\ \rho_1 \vdash s_2 \downarrow \rho_2; O_2 \end{array}}{\rho \vdash s_1; s_2 \downarrow \rho_2; O_1, O_2} \quad \text{SC_SEQ}
\end{array}$$

Figure 4: Source command evaluation

$$\boxed{v : \psi}$$

$$\begin{array}{c}
\frac{}{c : \delta(c)} \quad \text{V_CONS} \\
\\
\frac{c_i : \sigma}{[c_i]_n : \sigma[n]} \quad \text{V_ARR}
\end{array}$$

Figure 5: Value typing

m	$::=$	\mathcal{A} \mathcal{B}	Secret label
ℓ	$::=$	\mathcal{P} m	Label
τ	$::=$	σ^ℓ $\sigma^\ell[n]$	Type
\tilde{e}	$::=$	c x $\tilde{e}_1 +_\ell \tilde{e}_2$ $\mathbf{cond}_\ell(\tilde{e}, \tilde{e}_1, \tilde{e}_2)$ $\tilde{e}_1 >_\ell \tilde{e}_2$ $x[\tilde{e}]$ $\mathbf{input}_i^{(\sigma^m)}$ $\tilde{e} \triangleright m$ $[\tilde{e}_i]_n$	Target expression
\tilde{s}	$::=$	$\tau \ x = \tilde{e}$ $x := \tilde{e}$ $\mathbf{for}(x := n_1; x \leq n_2; x := x + 1) \ \tilde{s}$ $x[\tilde{e}_1] := \tilde{e}_2$ $\mathbf{if}(\tilde{e}, \tilde{s}_1, \tilde{s}_2)$ $\mathbf{out} \ \tilde{e}$ $\tilde{s}_1; \tilde{s}_2$	Target statement
Γ	$::=$	\cdot $\Gamma, x : \tau$	Type environment

Figure 6: Target language

$$\boxed{\Gamma \vdash e : \tau \rightsquigarrow \tilde{e}}$$

$$\begin{array}{c}
\overline{\Gamma \vdash c : \delta(c)^{\mathcal{P}} \rightsquigarrow c} \quad \text{S_CONS} \\
\\
\frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau \rightsquigarrow x} \quad \text{S_VAR} \\
\\
\frac{\Gamma \vdash e_i : \text{uint}^{\mathcal{P}} \rightsquigarrow \tilde{e}_i}{\Gamma \vdash e_1 + e_2 : \text{uint}^{\mathcal{P}} \rightsquigarrow \tilde{e}_1 +_{\mathcal{P}} \tilde{e}_2} \quad \text{S_PADD} \\
\\
\frac{\Gamma \vdash e_i : \text{uint}^{\mathcal{A}} \rightsquigarrow \tilde{e}_i}{\Gamma \vdash e_1 + e_2 : \text{uint}^{\mathcal{A}} \rightsquigarrow \tilde{e}_1 +_{\mathcal{A}} \tilde{e}_2} \quad \text{S_SADD} \\
\\
\frac{\Gamma \vdash e : \text{bool}^{\mathcal{P}} \rightsquigarrow \tilde{e} \quad \Gamma \vdash e_i : \sigma^{\ell} \rightsquigarrow \tilde{e}_i}{\Gamma \vdash \mathbf{cond}(e, e_1, e_2) : \sigma^{\ell} \rightsquigarrow \mathbf{cond}_{\mathcal{P}}(\tilde{e}, \tilde{e}_1, \tilde{e}_2)} \quad \text{S_PCOND} \\
\\
\frac{\Gamma \vdash e : \text{bool}^{\mathcal{B}} \rightsquigarrow \tilde{e} \quad \Gamma \vdash e_i : \sigma^{\mathcal{B}} \rightsquigarrow \tilde{e}_i}{\Gamma \vdash \mathbf{cond}(e, e_1, e_2) : \sigma^{\mathcal{B}} \rightsquigarrow \mathbf{cond}_{\mathcal{B}}(\tilde{e}, \tilde{e}_1, \tilde{e}_2)} \quad \text{S_SCOND} \\
\\
\frac{\Gamma \vdash e_i : \text{uint}^{\mathcal{P}} \rightsquigarrow \tilde{e}_i}{\Gamma \vdash e_1 > e_2 : \text{bool}^{\mathcal{P}} \rightsquigarrow \tilde{e}_1 >_{\mathcal{P}} \tilde{e}_2} \quad \text{S_PGT} \\
\\
\frac{\Gamma \vdash e_i : \text{uint}^{\mathcal{B}} \rightsquigarrow \tilde{e}_i}{\Gamma \vdash e_1 > e_2 : \text{bool}^{\mathcal{B}} \rightsquigarrow \tilde{e}_1 >_{\mathcal{B}} \tilde{e}_2} \quad \text{S_SGT} \\
\\
\frac{\Gamma \vdash x : \sigma^{\ell}[n] \rightsquigarrow x \quad \Gamma \vdash e : \text{uint}^{\mathcal{P}} \rightsquigarrow \tilde{e} \quad \Gamma \models e < n}{\Gamma \vdash x[e] : \sigma^{\ell} \rightsquigarrow x[\tilde{e}]} \quad \text{S_AREAD} \\
\\
\overline{\Gamma \vdash \mathbf{input}_i^{\sigma} : \sigma^m \rightsquigarrow \mathbf{input}_i^{(\sigma^m)}} \quad \text{S_INP} \\
\\
\frac{\Gamma \vdash e : \sigma^{\ell} \rightsquigarrow \tilde{e}}{\Gamma \vdash e : \sigma^m \rightsquigarrow \tilde{e} \triangleright m} \quad \text{S_SUB}
\end{array}$$

Figure 7: Expression compilation

$$\boxed{\Gamma \vdash s \rightsquigarrow \tilde{s} \mid \Gamma'}$$

$$\frac{
\begin{array}{l}
\psi = \sigma \Rightarrow \tau = \sigma^\ell \\
\psi = \sigma[n] \Rightarrow \tau = \sigma^\ell[n] \\
\tilde{e} = \mathbf{default}(\tau)
\end{array}
}{\Gamma \vdash \psi x \rightsquigarrow \tau x = \tilde{e} \mid \Gamma, x : \tau} \quad \text{C_DECL}$$

$$\frac{
\begin{array}{l}
\Gamma(x) = \sigma^\ell \\
\Gamma \vdash e : \sigma^\ell \rightsquigarrow \tilde{e}
\end{array}
}{\Gamma \vdash x := e \rightsquigarrow x := \tilde{e} \mid \Gamma} \quad \text{C_VASSGN}$$

$$\frac{
\begin{array}{l}
\Gamma, x : \mathbf{uint}^{\mathcal{P}} \vdash s \rightsquigarrow \tilde{s} \mid - \\
x \notin \mathbf{modifies}(s)
\end{array}
}{\Gamma \vdash \mathbf{for } x \mathbf{ in } n_1 \dots n_2 \{s\} \rightsquigarrow \mathbf{for}(x := n_1; x \leq n_2; x := x + 1) \tilde{s} \mid \Gamma} \quad \text{C_FOR}$$

$$\frac{
\begin{array}{l}
\Gamma \vdash x : \sigma^\ell[n] \rightsquigarrow x \\
\Gamma \vdash e_1 : \mathbf{uint}^{\mathcal{P}} \rightsquigarrow \tilde{e}_1 \\
\Gamma \vdash e_2 : \sigma^\ell \rightsquigarrow \tilde{e}_2 \\
\Gamma \models e_1 < n
\end{array}
}{\Gamma \vdash x[e_1] := e_2 \rightsquigarrow x[\tilde{e}_1] := \tilde{e}_2 \mid \Gamma} \quad \text{C_AWRITE}$$

$$\frac{
\begin{array}{l}
\Gamma \vdash e : \mathbf{bool}^{\mathcal{P}} \rightsquigarrow \tilde{e} \\
\Gamma \vdash s_i \rightsquigarrow \tilde{s}_i \mid -
\end{array}
}{\Gamma \vdash \mathbf{if}(e, s_1, s_2) \rightsquigarrow \mathbf{if}(\tilde{e}, \tilde{s}_1, \tilde{s}_2) \mid \Gamma} \quad \text{C_IF}$$

$$\frac{
\Gamma \vdash e : \sigma^m \rightsquigarrow \tilde{e}
}{\Gamma \vdash \mathbf{out } e \rightsquigarrow \mathbf{out } \tilde{e} \mid \Gamma} \quad \text{C_OUT}$$

$$\frac{
\begin{array}{l}
\Gamma \vdash s_1 \rightsquigarrow \tilde{s}_1 \mid \Gamma_1 \\
\Gamma_1 \vdash s_2 \rightsquigarrow \tilde{s}_2 \mid \Gamma_2
\end{array}
}{\Gamma \vdash s_1; s_2 \rightsquigarrow \tilde{s}_1; \tilde{s}_2 \mid \Gamma_2} \quad \text{C_SEQ}$$

Figure 8: Command compilation

r	$::=$		Wire id range
\tilde{w}	$::=$		Compiled base value
	$ $	c	
	$ $	r	
\tilde{v}	$::=$		Compiled value
	$ $	\tilde{w}	
	$ $	$[\tilde{w}_i]_n$	
κ	$::=$		Circuit
	$ $	\cdot	
	$ $	$\oplus(r_1, r_2, r_3)$	
	$ $	$\text{Mux}(r_1, r_2, r_3, r_4)$	
	$ $	$\text{Gt}(r_1, r_2, r_3)$	
	$ $	$\tilde{w} \triangleright_m r$	
	$ $	$\text{Inp}_i \triangleright_m r$	
	$ $	$\text{Out}(r)$	
	$ $	κ_1, κ_2	
$\tilde{\rho}$	$::=$		Runtime environment
	$ $	\cdot	
	$ $	$\tilde{\rho}[x \mapsto \tilde{v}]$	

Figure 9: Target runtime

$$\boxed{\tilde{\rho} \vdash \tilde{e} \Downarrow \tilde{v}; \kappa}$$

$$\begin{array}{c}
\frac{}{\tilde{\rho} \vdash c \Downarrow c; \cdot} \text{EE_CONST} \\
\\
\frac{}{\tilde{\rho} \vdash x \Downarrow \tilde{\rho}[x]; \cdot} \text{EE_VAR} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e}_i \Downarrow n_i; \kappa_i}{\tilde{\rho} \vdash \tilde{e}_1 +_{\mathcal{P}} \tilde{e}_2 \Downarrow n_1 + n_2; \kappa_1, \kappa_2} \text{EE_PADD} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e}_i \Downarrow r_i; \kappa_i \quad r_3 = \text{next_range}()}{\tilde{\rho} \vdash \tilde{e}_1 +_{\mathcal{A}} \tilde{e}_2 \Downarrow r_3; \kappa_1, \kappa_2, \oplus(r_1, r_2, r_3)} \text{EE_SADD} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e} \Downarrow c; \kappa \quad c = \top \Rightarrow i = 1 \quad c = \perp \Rightarrow i = 2 \quad \tilde{\rho} \vdash \tilde{e}_i \Downarrow \tilde{v}; \kappa_1}{\tilde{\rho} \vdash \mathbf{cond}_{\mathcal{P}}(\tilde{e}, \tilde{e}_1, \tilde{e}_2) \Downarrow \tilde{v}; \kappa, \kappa_1} \text{EE_PCOND} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e} \Downarrow r; \kappa \quad \tilde{\rho} \vdash \tilde{e}_i \Downarrow r_i; \kappa_i \quad r_3 = \text{next_range}()}{\tilde{\rho} \vdash \mathbf{cond}_{\mathcal{B}}(\tilde{e}, \tilde{e}_1, \tilde{e}_2) \Downarrow r_3; \kappa, \kappa_1, \kappa_2, \text{Mux}(r, r_1, r_2, r_3)} \text{EE_SCOND} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e}_i \Downarrow n_i; \kappa_i}{\tilde{\rho} \vdash \tilde{e}_1 >_{\mathcal{P}} \tilde{e}_2 \Downarrow n_1 > n_2; \kappa_1, \kappa_2} \text{EE_PGT} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e}_i \Downarrow r_i; \kappa_i \quad r_3 = \text{next_range}()}{\tilde{\rho} \vdash \tilde{e}_1 >_{\mathcal{B}} \tilde{e}_2 \Downarrow r_3; \kappa_1, \kappa_2, \text{Gt}(r_1, r_2, r_3)} \text{EE_SGT} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e} \Downarrow n_1; \kappa_1 \quad \tilde{\rho} \vdash x \Downarrow [\tilde{w}_i]_{n_2}; \kappa_2 \quad n_1 < n_2}{\tilde{\rho} \vdash x[\tilde{e}] \Downarrow \tilde{w}_n; \kappa_1, \kappa_2} \text{EE_AREAD} \\
\\
\frac{r = \text{next_range}()}{\tilde{\rho} \vdash \mathbf{input}_i^{(\sigma^m)} \Downarrow r; \text{Inp}_i \triangleright_m r} \text{EE_INP} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e} \Downarrow r; \kappa \quad r' = \text{next_range}()}{\tilde{\rho} \vdash \tilde{e} \triangleright_m m \Downarrow r'; \kappa, r \triangleright_m r'} \text{EE_COERCE} \\
\\
\frac{\tilde{\rho} \vdash \tilde{e}_i \Downarrow \tilde{w}_i; \kappa_i}{\tilde{\rho} \vdash [\tilde{e}_i]_n \Downarrow [\tilde{w}_i]_n; \kappa_i} \text{EE_ARR}
\end{array}$$

Figure 10: Target expression evaluation

$$\boxed{\tilde{\rho} \vdash \tilde{s} \Longrightarrow \tilde{\rho}'; \kappa}$$

$$\frac{\tilde{\rho} \vdash \tilde{e} \Downarrow \tilde{v}; \kappa}{\tilde{\rho} \vdash \tau x = \tilde{e} \Longrightarrow \tilde{\rho}[x \mapsto \tilde{v}]; \kappa} \text{ EC_DECL}$$

$$\frac{\tilde{\rho} \vdash \tilde{e} \Downarrow \tilde{v}; \kappa}{\tilde{\rho} \vdash x := \tilde{e} \Longrightarrow \tilde{\rho}[x \mapsto \tilde{v}]; \kappa} \text{ EC_ASSGN}$$

$$\frac{\tilde{\rho}[x \mapsto n_1] \vdash \mathbf{loop} \ x \ \mathbf{until} \ n_2 \ \{\tilde{s}\} \Longrightarrow \tilde{\rho}_1; \kappa}{\tilde{\rho} \vdash \mathbf{for}(x := n_1; x \leq n_2; x := x + 1) \ \tilde{s} \Longrightarrow \tilde{\rho}_1 \setminus x; \kappa} \text{ EC_FORT}$$

$$\frac{\tilde{\rho}[x] > n_2}{\tilde{\rho} \vdash \mathbf{loop} \ x \ \mathbf{until} \ n_2 \ \{\tilde{s}\} \Longrightarrow \tilde{\rho}; \cdot} \text{ EC_LOOP}$$

$$\frac{\begin{array}{l} \tilde{\rho}[x] \leq n_2 \\ \tilde{\rho} \vdash \tilde{s} \Longrightarrow \tilde{\rho}_1; \kappa_1 \\ ([\tilde{\rho}_1]_{\text{dom}(\tilde{\rho})})[x \mapsto \tilde{\rho}[x] + 1] \vdash \mathbf{loop} \ x \ \mathbf{until} \ n_2 \ \{\tilde{s}\} \Longrightarrow \tilde{\rho}_2; \kappa_2 \end{array}}{\tilde{\rho} \vdash \mathbf{loop} \ x \ \mathbf{until} \ n_2 \ \{\tilde{s}\} \Longrightarrow \tilde{\rho}_2; \kappa_1, \kappa_2} \text{ EC_LOOPI}$$

$$\frac{\begin{array}{l} \tilde{\rho} \vdash x \Downarrow [\tilde{w}_i]_{n_2}; \cdot \\ \tilde{\rho} \vdash \tilde{e}_1 \Downarrow n_1; \kappa_1 \\ \tilde{\rho} \vdash \tilde{e}_2 \Downarrow \tilde{w}; \kappa_2 \\ n_1 < n_2 \end{array}}{\tilde{\rho} \vdash x[\tilde{e}_1] := \tilde{e}_2 \Longrightarrow \tilde{\rho}[x \mapsto [\tilde{w}_i]_{n_2}[n_1 \mapsto \tilde{w}]]; \kappa_1, \kappa_2} \text{ EC_AWRITE}$$

$$\frac{\begin{array}{l} \tilde{\rho} \vdash \tilde{e} \Downarrow c; \kappa_1 \\ c = \top \Rightarrow i = 1 \\ c = \perp \Rightarrow i = 2 \\ \tilde{\rho} \vdash \tilde{s}_i \Longrightarrow \tilde{\rho}'; \kappa_2 \end{array}}{\tilde{\rho} \vdash \mathbf{if}(\tilde{e}, \tilde{s}_1, \tilde{s}_2) \Longrightarrow \tilde{\rho}'; \kappa_1, \kappa_2} \text{ EC_IF}$$

$$\frac{\tilde{\rho} \vdash \tilde{e} \Downarrow r; \kappa}{\tilde{\rho} \vdash \mathbf{out} \ \tilde{e} \Longrightarrow \tilde{\rho}; \kappa, \text{Out}(r)} \text{ EC_OUT}$$

$$\frac{\begin{array}{l} \tilde{\rho} \vdash \tilde{s}_1 \Longrightarrow \tilde{\rho}_1; \kappa_1 \\ \tilde{\rho}_1 \vdash \tilde{s}_2 \Longrightarrow \tilde{\rho}_2; \kappa_2 \end{array}}{\tilde{\rho} \vdash \tilde{s}_1; \tilde{s}_2 \Longrightarrow \tilde{\rho}_2; \kappa_1, \kappa_2} \text{ EC_SEQ}$$

Figure 11: Target command evaluation

b	::=	Share (byte string)
$\hat{\rho}$::=	Circuit environment
		\cdot
		$\hat{\rho}[r \mapsto b]$

Figure 12: Circuit runtime

$$\boxed{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa \mapsto \widehat{\rho}'_1, \widehat{\rho}'_2; O}$$

$$\begin{array}{c}
\frac{}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \cdot \mapsto \widehat{\rho}_1, \widehat{\rho}_2; \cdot} \text{CKT_EMP} \\
\\
\frac{n_1 = \mathcal{D}_{\mathcal{A}}(\widehat{\rho}_1[r_1], \widehat{\rho}_2[r_1]) \quad n_2 = \mathcal{D}_{\mathcal{A}}(\widehat{\rho}_1[r_2], \widehat{\rho}_2[r_2]) \quad (b_1, b_2) = \mathcal{E}_{\mathcal{A}}(n_1 + n_2)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \oplus(r_1, r_2, r_3) \mapsto \widehat{\rho}_1[r_3 \mapsto b_1], \widehat{\rho}_2[r_3 \mapsto b_2]; \cdot} \text{CKT_ADD} \\
\\
\frac{\top = \mathcal{D}_{\mathcal{B}}(\widehat{\rho}_1[r_1], \widehat{\rho}_2[r_1]) \quad c = \mathcal{D}_{\mathcal{B}}(\widehat{\rho}_1[r_2], \widehat{\rho}_2[r_2]) \quad (b_1, b_2) = \mathcal{E}_{\mathcal{B}}(c)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \text{Mux}(r_1, r_2, r_3, r_4) \mapsto \widehat{\rho}_1[r_4 \mapsto b_1], \widehat{\rho}_2[r_4 \mapsto b_2]; \cdot} \text{CKT_MUXT} \\
\\
\frac{\perp = \mathcal{D}_{\mathcal{B}}(\widehat{\rho}_1[r_1], \widehat{\rho}_2[r_1]) \quad c = \mathcal{D}_{\mathcal{B}}(\widehat{\rho}_1[r_3], \widehat{\rho}_2[r_3]) \quad (b_1, b_2) = \mathcal{E}_{\mathcal{B}}(c)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \text{Mux}(r_1, r_2, r_3, r_4) \mapsto \widehat{\rho}_1[r_4 \mapsto b_1], \widehat{\rho}_2[r_4 \mapsto b_2]; \cdot} \text{CKT_MUXF} \\
\\
\frac{n_1 = \mathcal{D}_{\mathcal{B}}(\widehat{\rho}_1[r_1], \widehat{\rho}_2[r_1]) \quad n_2 = \mathcal{D}_{\mathcal{B}}(\widehat{\rho}_1[r_2], \widehat{\rho}_2[r_2]) \quad (b_1, b_2) = \mathcal{E}_{\mathcal{B}}(n_1 > n_2)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \text{Gt}(r_1, r_2, r_3) \mapsto \widehat{\rho}_1[r_3 \mapsto b_1], \widehat{\rho}_2[r_3 \mapsto b_2]; \cdot} \text{CKT_GT} \\
\\
\frac{(b_1, b_2) = \mathcal{E}_m(c)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash c \triangleright_m r_2 \mapsto \widehat{\rho}_1[r_2 \mapsto b_1], \widehat{\rho}_2[r_2 \mapsto b_2]; \cdot} \text{CKT_COERCEC} \\
\\
\frac{c = \mathcal{D}_{m_1}(\widehat{\rho}_1[r_1], \widehat{\rho}_2[r_1]) \quad (b_1, b_2) = \mathcal{E}_m(c)}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash r_1 \triangleright_m r_2 \mapsto \widehat{\rho}_1[r_2 \mapsto b_1], \widehat{\rho}_2[r_2 \mapsto b_2]; \cdot} \text{CKT_COERCER} \\
\\
\frac{(b_1, b_2) = \mathcal{E}_m(\text{get_input}(i))}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \text{Inp}_i \triangleright_m r \mapsto \widehat{\rho}_1[r_2 \mapsto b_1], \widehat{\rho}_2[r_2 \mapsto b_2]; \cdot} \text{CKT_INP} \\
\\
\frac{c = \mathcal{D}_m(\widehat{\rho}_1[r], \widehat{\rho}_2[r])}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \text{Out}(r) \mapsto \widehat{\rho}_1, \widehat{\rho}_2; c, \cdot} \text{CKT_OUT} \\
\\
\frac{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa_1 \mapsto \widehat{\rho}'_1, \widehat{\rho}'_2; O_1 \quad \widehat{\rho}'_1, \widehat{\rho}'_2 \vdash \kappa_2 \mapsto \widehat{\rho}''_1, \widehat{\rho}''_2; O_2}{\widehat{\rho}_1, \widehat{\rho}_2 \vdash \kappa_1, \kappa_2 \mapsto \widehat{\rho}''_1, \widehat{\rho}''_2; O_1, O_2} \text{CKT_SEQ}
\end{array}$$

Figure 13: Circuit evaluation

$$\boxed{\Gamma \sim \rho}$$

$$\frac{}{\cdot \sim \cdot} \quad \text{SEN_EMP}$$

$$\frac{v : \psi \quad \psi \sim \tau \quad \Gamma \sim \rho}{\Gamma, x : \tau \sim \rho[x \mapsto v]} \quad \text{SEN_BND}$$

Figure 14: Source environment and type environment consistency

$$\boxed{\Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2}$$

$$\frac{}{\Gamma \vdash \cdot \hookrightarrow \cdot; \cdot, \cdot} \quad \text{EN_EMP}$$

$$\frac{\Gamma(x) = \sigma^{\mathcal{P}} \quad \Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2}{\Gamma \vdash \rho[x \mapsto c] \hookrightarrow \tilde{\rho}[x \mapsto c]; \hat{\rho}_1, \hat{\rho}_2} \quad \text{EN_PBT}$$

$$\frac{\Gamma(x) = \sigma^m \quad r = \text{next_range}() \quad (b_1, b_2) = \mathcal{E}_m(c) \quad \Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2}{\Gamma \vdash \rho[x \mapsto c] \hookrightarrow \tilde{\rho}[x \mapsto r]; \hat{\rho}_1[r \mapsto b_1], \hat{\rho}_2[r \mapsto b_2]} \quad \text{EN_SBT}$$

$$\frac{\Gamma(x) = \sigma^{\mathcal{P}}[n] \quad \Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2}{\Gamma \vdash \rho[x \mapsto [c_i]_n] \hookrightarrow \tilde{\rho}[x \mapsto [c_i]_n]; \hat{\rho}_1, \hat{\rho}_2} \quad \text{EN_PARR}$$

$$\frac{\Gamma(x) = \sigma^m[n] \quad r_i = \text{next_range}() \quad (b_{1\ i}, b_{2\ i}) = \mathcal{E}_m(c_i) \quad \Gamma \vdash \rho \hookrightarrow \tilde{\rho}; \hat{\rho}_1, \hat{\rho}_2}{\Gamma \vdash \rho[x \mapsto [c_i]_n] \hookrightarrow \tilde{\rho}[x \mapsto [r_i]_n]; \hat{\rho}_1[r_i \mapsto b_{1\ i}], \hat{\rho}_2[r_i \mapsto b_{2\ i}]} \quad \text{EN_SARR}$$

Figure 15: Source environment to target environment compilation