

Technical Report

January 19, 2012

1 Correctness

Theorem 1 (Typing Correctness). *If $\Gamma \vdash M : T$, σ is a valid interpretation of Γ then*

$$\llbracket \Gamma \rrbracket^\sigma \vdash [M]_p^\sigma : \llbracket T \rrbracket_p^\sigma$$

where p is the last forcing condition occurring in σ .

Proof. By induction on the structure of $\Gamma \vdash M : T$.

- ABS :

$$\text{ABSTR} \frac{\text{HYP IND} \frac{}{\llbracket \Gamma, x : A \rrbracket^{\sigma+(x,T,q)} \vdash [M]_q^{\sigma+(x,T,q)} : [U]_q^{\sigma+(x,T,q)}}}{\llbracket \Gamma \rrbracket^\sigma \vdash \lambda q : \mathcal{P}_p.\lambda x : \llbracket T \rrbracket_q^\sigma.[M]_q^{\sigma+(x,T,q)} : \Pi q : \mathcal{P}_p.\Pi x : \llbracket T \rrbracket_q^\sigma.[U]_q^{\sigma+(x,T,q)} + \text{proof obligation}}}{\text{SUBSET} \frac{}{\llbracket \Gamma \rrbracket^\sigma \vdash \lambda q : \mathcal{P}_p.\lambda x : \llbracket T \rrbracket_q^\sigma.[M]_q^{\sigma+(x,T,q)} : \left\{ f : \Pi q : \mathcal{P}_p.\Pi x : \llbracket T \rrbracket_q^\sigma.[U]_q^{\sigma+(x,T,q)} \mid \mathbf{comm}_\Pi(f, T, U, q) \right\}}}$$

with the proof obligation $\mathbf{comm}_\Pi(\lambda q : \mathcal{P}_p.\lambda x : \llbracket T \rrbracket_q^\sigma.[M]_q^{\sigma+(x,T,q)}, T, U, q)$

- VAR :

$$\text{VAR} \frac{\vdash \mathbf{wf}(x : [A]_{\sigma_2(x)}^\sigma, \llbracket \Gamma \rrbracket^\sigma)}{x : [A]_{\sigma_2(x)}^\sigma, \llbracket \Gamma \rrbracket^\sigma \vdash x : [A]_{\sigma_2(x)}^\sigma} \\ \frac{}{x : [A]_{\sigma_2(x)}^\sigma, \llbracket \Gamma \rrbracket^\sigma \vdash \theta_{\sigma_2(x) \rightarrow p}^{\sigma, A} x : [A]_p^\sigma}$$

- PROD :

To prove $\llbracket \Gamma \rrbracket^\sigma \vdash [\Pi x : T.U]_p^\sigma : \mathbf{Sh}(p, s_2)$ we use the rule PAIR with the two following proof trees :

$$\text{PROJ-1} \frac{q : \mathcal{P}_p, r : \mathcal{P}_q, \llbracket \Gamma, x : T \rrbracket^{\sigma+(x,T,r)} \vdash [U]_r^{\sigma+(x,T,r)} : \mathbf{Sh}(r, s_2)}{\llbracket \Gamma \rrbracket^\sigma, q : \mathcal{P}_p, r : \mathcal{P}_q, x : \llbracket T \rrbracket_r^\sigma \vdash [U]_r^{\sigma+(x,T,r)} : s_2} \\ \text{PROD} \frac{}{\llbracket \Gamma \rrbracket^\sigma, q : \mathcal{P}_p \vdash \Pi r : \mathcal{P}_q.\Pi x : \llbracket T \rrbracket_r^\sigma.[U]_r^{\sigma+(x,T,r)} : s_2} \\ \text{SUBSET} \frac{}{\llbracket \Gamma \rrbracket^\sigma, q : \mathcal{P}_p \vdash \left\{ f : \Pi r : \mathcal{P}_q.\Pi x : \llbracket T \rrbracket_r^\sigma.[U]_r^{\sigma+(x,T,r)} \mid \mathbf{comm}_\Pi(f, T, U, q) \right\} : s_2} \\ \text{ABSTR} \frac{}{\llbracket \Gamma \rrbracket^\sigma \vdash \lambda q : \mathcal{P}_p. \underbrace{\left\{ f : \Pi r : \mathcal{P}_q.\Pi x : \llbracket T \rrbracket_r^\sigma.[U]_r^{\sigma+(x,T,r)} \mid \mathbf{comm}_\Pi(f, T, U, q) \right\}}_M : \mathcal{P}_p \rightarrow s_2} \\ \text{APP} \frac{}{q : \mathcal{P}_p, r : \mathcal{P}_q, f : [\Pi x : T.U]_q^\sigma, s : \mathcal{P}_r, \llbracket \Gamma \rrbracket^\sigma \vdash fs : \Pi x : \llbracket T \rrbracket_r^\sigma.[U]_r^{\sigma+(x,T,r)}} \\ \text{ABSTR} \frac{}{\llbracket \Gamma \rrbracket^\sigma \vdash \lambda q : \mathcal{P}_p.\lambda r : \mathcal{P}_q.\lambda f : [\Pi x : T.U]_q^\sigma.\lambda s : \Pi q : \mathcal{P}_p.\Pi r : \mathcal{P}_q.[\Pi x : T.U]_q^\sigma \rightarrow [\Pi x : T.U]_r^\sigma} \\ \text{CONV} \frac{}{\llbracket \Gamma \rrbracket^\sigma \vdash \lambda q : \mathcal{P}_p.\lambda r : \mathcal{P}_q.\lambda f : [\Pi x : T.U]_q^\sigma.\lambda s : \mathcal{P}_r.fs : \Pi q : \mathcal{P}_p.\Pi r : \mathcal{P}_q.Mq \rightarrow Mr}$$

with the proof obligations

$$\mathbf{trans}(\lambda q : \mathcal{P}_p.\lambda r : \mathcal{P}_q.\lambda f : \llbracket \Pi x : T.U \rrbracket_q^\sigma.\lambda s : \mathcal{P}_r.fs, p)$$

and

$$\mathbf{refl}(\lambda q : \mathcal{P}_p.\lambda r : \mathcal{P}_q.\lambda f : \llbracket \Pi x : T.U \rrbracket_q^\sigma.\lambda s : \mathcal{P}_r.fs, p)$$

- APP :

$$\text{APP} \frac{\llbracket \Gamma \rrbracket^\sigma \vdash [M]_p^\sigma p : \Pi x : \llbracket T \rrbracket_p^\sigma. \llbracket U \rrbracket_p^{\sigma+(x,T,p)} \llbracket \Gamma \rrbracket^\sigma \vdash [N]_p^\sigma : \llbracket T \rrbracket_p^\sigma}{\llbracket \Gamma \rrbracket^\sigma \vdash [M]_p^\sigma p [N]_p^\sigma : \llbracket U \rrbracket_p^{\sigma+(x,T,p)} \{ [N]_p^\sigma / x \}}$$

$$\text{CONV} \frac{\llbracket \Gamma \rrbracket^\sigma \vdash [M]_p^\sigma p [N]_p^\sigma : \llbracket U \rrbracket_p^{\sigma+(x,T,p)} \{ [N]_p^\sigma / x \}}{\llbracket \Gamma \rrbracket^\sigma \vdash \mathbf{app}_{T,U,N}([M]_p^\sigma p [N]_p^\sigma) : \llbracket U \{N/x\} \rrbracket_p^\sigma}$$

- AX :

To prove $\llbracket \Gamma \rrbracket^\sigma \vdash (\lambda q : \mathcal{P}_p.\mathbf{Sh}(q, \text{Type}_i), \mathbf{ShC}(p, \text{Type}_i)) : \mathbf{Sh}(p, \text{Type}_{i+1})$ we use the rule PAIR with the two following proof trees :

$$\text{SUM} \frac{\llbracket \Gamma \rrbracket^\sigma, q : \mathcal{P}_p \vdash \mathcal{P}_q \rightarrow \text{Type}_i : \text{Type}_{i+1} \dots}{\llbracket \Gamma \rrbracket^\sigma, q : \mathcal{P}_p \vdash \Sigma f : \mathcal{P}_q \rightarrow \text{Type}_i. \{ \theta : \Pi r : \mathcal{P}_q. \Pi s : \mathcal{P}_r. fr \rightarrow fs \mid \mathbf{trans}(\theta, q) \wedge \mathbf{refl}(\theta, q) \} : \text{Type}_{i+1}}$$

$$\text{ABSTR} \frac{\llbracket \Gamma \rrbracket^\sigma \vdash \lambda q : \mathcal{P}_p. \mathbf{Sh}(q, \text{Type}_i) : \mathcal{P}_p \rightarrow \text{Type}_{i+1}}{\llbracket \Gamma \rrbracket^\sigma \vdash \lambda q : \mathcal{P}_p. \mathbf{Sh}(q, \text{Type}_i), \mathbf{ShC}(p, \text{Type}_i) : \mathbf{Sh}(p, \text{Type}_{i+1})}$$

$$\text{SUM} \frac{\llbracket \Gamma \rrbracket^\sigma, q : \mathcal{P}_p, r : \mathcal{P}_q, f : \mathbf{Sh}(q, \text{Type}_i). \vdash (\lambda s : \mathcal{P}_r. (\pi_1 f) s, \lambda s : \mathcal{P}_r. \lambda t : \mathcal{P}_s. \lambda x : (\pi_1 f) s. (\pi_2 f) stx) : \mathbf{Sh}(r, \text{Type}_i)}{\llbracket \Gamma \rrbracket^\sigma \vdash \mathbf{ShC}(p, \text{Type}_i) : \Pi q : \mathcal{P}_p. \Pi r : \mathcal{P}_q. \mathbf{Sh}(q, \text{Type}_i) \rightarrow \mathbf{Sh}(r, \text{Type}_i)}$$

$$\text{CONV} \frac{\llbracket \Gamma \rrbracket^\sigma \vdash \mathbf{ShC}(p, \text{Type}_i) : \Pi q : \mathcal{P}_p. \Pi r : \mathcal{P}_q. Mq \rightarrow Mr}{\llbracket \Gamma \rrbracket^\sigma \vdash \mathbf{ShC}(p, \text{Type}_i) : \{ \theta : \Pi q : \mathcal{P}_p. \Pi r : \mathcal{P}_q. Mq \rightarrow Mr \mid \mathbf{trans}(\theta, p) \wedge \mathbf{refl}(\theta, p) \}}$$

$$\text{SUBSET}$$

with proof obligations :

- $\mathbf{trans}(\mathbf{ShC}(p, \text{Type}_i), p)$
- $\mathbf{refl}(\mathbf{ShC}(p, \text{Type}_i), p)$
- $\mathbf{trans}(\lambda s : \mathcal{P}_r. \lambda t : \mathcal{P}_s. \lambda x : (\pi_1 f) s. (\pi_2 f) stx, r)$
- $\mathbf{refl}(\lambda s : \mathcal{P}_r. \lambda t : \mathcal{P}_s. \lambda x : (\pi_1 f) s. (\pi_2 f) stx, r)$

The proof of

$$\llbracket \Gamma \rrbracket^\sigma \vdash (\lambda q : \mathcal{P}_p. \mathbf{Sh}(q, \text{Prop}), \mathbf{ShC}(p, \text{Prop})) : \mathbf{Sh}(p, \text{Type}_0)$$

is done in the same way, with less proof obligations.

- CONV :

$$\text{CONV}^* \frac{\llbracket \Gamma \rrbracket^\sigma \vdash [M]_p^\sigma : \llbracket T \rrbracket_p^\sigma T \simeq U}{\llbracket \Gamma \rrbracket^\sigma \vdash [\mathbf{conv}_{T,U} M]_p^\sigma : \llbracket U \rrbracket_p^\sigma}$$

□

2 Definition of some proof terms

The proof-terms in the prototype are generated using proof obligations of Russell. Then using the tactic **autorewrite** with the equality from **refl**, **trans** and **comm**, we can prove them automatically.

To give some clues about the shape of these proof-terms, we provide for some of them their translation.

Definition 1. The term **subst_eq_{M,T}** is of type

$$\Pi N : T. \Pi p : \mathcal{P}. \Pi q : \mathcal{P}_p. ([N]_q^\sigma = \theta_{p \rightarrow q}^{\sigma, T} [N]_p^\sigma) \rightarrow ([M \{N/x\}]_q^\sigma = [M]_q^{\sigma+(x, T, q)} \{[N]_p^\sigma/x\})$$

It is defined as :

- **subst_eq_{x,U}** $p q N \pi_{N,p,q} = \pi_{N,p,q}$
- **subst_eq_{T,U}** $p q N \pi_{N,p,q} = \mathbf{eq_refl}$ otherwise

Definition 2. The term **mono_subst_{M,T}^σ** is of type

$$\Pi N : T. \Pi p : \mathcal{P}. \Pi q : \mathcal{P}_q. ([M]_q^{\sigma+(x, T, q)} \{(\theta_{p \rightarrow q}^{\sigma, T} N)/x\} = [M]_q^{\sigma+(x, T, p)} \{N/x\})$$

It is defined by induction on N :

- **mono_subst_{x,T}^σ** $= \lambda N : T. \lambda p : \mathcal{P}. \lambda q : \mathcal{P}_p. \mathbf{trans}(\theta, p) p q q$
- **mono_subst_{M,T}^σ** $= \text{some } \mathbf{eq_rect} \mathbf{mono_subst}_{M',T}^\sigma .$

Definition 3. The term **mono_trad_N^σ** is of type

$$\Pi p : \mathcal{P}. \Pi q : \mathcal{P}_q. ([N]_q^\sigma = \theta_{p \rightarrow q}^{\sigma, T} [N]_p^\sigma)$$

It is defined by induction on N :

- **mono_trad_x^σ** $= \lambda p : \mathcal{P}. \lambda q : \mathcal{P}_p. \mathbf{trans}(\theta, \sigma_2(x)) \sigma_2(x) p p$
- **mono_trad_{MN}^σ** $= \lambda p : \mathcal{P}. \lambda q : \mathcal{P}_p. (\mathbf{comm}_\Pi(M, T, U, p) N) + \text{some } \mathbf{eq_rect} \mathbf{mono_trad}_M^\sigma \text{ and } \mathbf{eq_rect} \mathbf{mono_trad}_N^\sigma .$
- **mono_trad_M^σ** $= \mathbf{eq_refl}$ otherwise.

The correctness of the definition of **mono_trad_{MN}^σ** is given by the following lemma.

Lemma 1.

$$\theta_{p \rightarrow q}^{\sigma, U} \{x/N\} (\mathbf{eq_rect} \llbracket U \rrbracket_p^\sigma \mathbf{id} \llbracket U \rrbracket_p^\sigma \{x/\llbracket N \rrbracket_p^\sigma\}) (\mathbf{subst_eq}_{T,U} p p N (\mathbf{mono_trad}_N^\sigma p p)) R$$

is equal to

$$\mathbf{eq_rect} \llbracket U \{x/N\} \rrbracket_q^\sigma \mathbf{id} \llbracket U \rrbracket_q^\sigma \{x/\llbracket N \rrbracket_q^\sigma\} (\mathbf{subst_eq}_{T,U} q q N (\mathbf{mono_trad}_N^\sigma q q)) (\theta_{p \rightarrow q}^{\sigma+(x, T, p), U} R)$$

Proof. Using proof irrelevance (or at least the axiom K), we can identify **mono_trad_N^σ** $p p$ to **eq_refl** and then reduce **eq_rect** . \square

Definition 4. The term **commlam_{M,T}** is of type **comm_Π**($[\lambda x : T. M]_p^\sigma, T, U, p$). It is defined by

$$\mathbf{eq_ind_r} (\llbracket U \rrbracket_s^{\sigma+(x, T, s)}) (\theta_{r \rightarrow s}^{\sigma+(x, T, r), T} [M]_r^{\sigma+(x, T, r)} \{N/x\}) (\dots) \left[\mathbf{eq_ind} (\llbracket U \rrbracket_s^{\sigma+(x, T, s)}) ([M]_s^{\sigma+(x, T, s)} \{\theta_{r \rightarrow s}^{\sigma, T} N/x\}) (\dots) \mathbf{reflexivity} \right]$$

Definition 5. $[\mathbf{app}_{T,U,N} M]_p^\sigma \stackrel{def}{=} \mathbf{eq_rect} \llbracket U \{x/N\} \rrbracket_p^\sigma \mathbf{id} (\llbracket U \rrbracket_p^{\sigma+(x, T, p)} \{x/\llbracket N \rrbracket_p^\sigma\}) (\mathbf{subst_eq}_{T,U} p p N (\mathbf{mono_trad}_N^\sigma p p)) [M]_p^\sigma$