Abstract

Categories and Subject Descriptors CR-number [*subcategory*]: third-level

Keywords gradual types, Clojure

Tobin-Hochstadt and Felleisen [1, 2]

References

[1] S. Tobin-Hochstadt and M. Felleisen. The design and implementation of typed scheme. *SIGPLAN Not.*, 43 (1):395–406, Jan. 2008. ISSN 0362-1340. URL `http://doi.acm.org/10.1145/1328897.1328486`.

[2] S. Tobin-Hochstadt and M. Felleisen. Logical types for untyped languages. *SIGPLAN Not.*, 45(9):117–128, Sept. 2010. ISSN 0362-1340. URL `http://doi.acm.org/10.1145/1932681.1863561`.

$$
\begin{array}{lll}
v & ::= \#\mathsf{f} \mid \#\mathsf{t} & \text{Values} \\
e & ::= x \mid v \mid (e\ e) \mid \lambda x^{\tau}.e \mid (\textbf{if}\ e\ e\ e) \mid (\textbf{let}\ (x\ e)\ e) \mid (\textbf{begin}\ e\ e) \mid (\mathit{cons}\ e\ e) & \text{Expressions} \\
\\
\mathcal{R} & ::= \{\omega \mid \psi\} & \text{Refinement Types} \\
\\
\sigma,\tau & ::= \textbf{\#t} \mid \textbf{\#f} \mid \textbf{N} \mid (\bigcup \overrightarrow{\mathcal{R}}) \mid x{:}\mathcal{R} \to \mathcal{R} \mid \langle \mathcal{R}, \mathcal{R} \rangle & \text{Types} \\
\\
\kappa & ::= \omega \mid x & \text{Object Variables} \\
\\
\psi & ::= \tau_{\pi(\kappa)} \mid \overline{\tau}_{\pi(\kappa)} \mid \psi \supset \psi \mid \psi \wedge \psi \mid \psi \vee \psi \mid \mathbb{tt} \mid \mathbb{ff} \mid \pi(\kappa) \equiv \pi(\kappa) & \text{Propositions} \\
o & ::= \pi(\kappa) \mid \emptyset & \text{Objects} \\
\pi & ::= \overrightarrow{pe} & \text{Paths} \\
pe & ::= \textbf{car} \mid \textbf{cdr} & \text{Path Elements} \\
\\
\Gamma & ::= \overrightarrow{\psi} & \text{Proposition Environment}
\end{array}
$$

Figure 1. Syntax of Terms, Types, Propositions, and Objects

$$
\begin{array}{lcl}
\top & = & \{\omega \mid \mathbb{tt}\} \\
\bot & = & \{\omega \mid \mathbb{ff}\} \\
\textbf{B} & = & (\bigcup \{\omega \mid \textbf{\#t}_{\omega}\}\ \{\omega \mid \textbf{\#f}_{\omega}\})
\end{array}
$$

Figure 2. Refinement Type Abbreviations

T-VAR
$$\frac{\omega \notin \mathrm{fv}(\Gamma) \qquad \Gamma \vdash \tau_x}{\Gamma \vdash x : \{\omega \mid \tau_{\omega} \wedge \omega \equiv x\}}$$

T-TRUE
$$\Gamma \vdash \#\mathsf{t} : \{\omega \mid \textbf{\#t}_{\omega}\}$$

T-FALSE
$$\Gamma \vdash \#\mathsf{f} : \{\omega \mid \textbf{\#f}_{\omega}\}$$

T-IF
$$\frac{\omega_1 \notin \mathrm{fv}(\Gamma) \qquad \Gamma \vdash e_1 : \{\omega_1 \mid \psi_1\} \qquad \Gamma, \overline{\textbf{\#f}}_{\omega_1}, \psi_1 \vdash e_2 : \mathcal{R} \qquad \Gamma, \textbf{\#f}_{\omega_1}, \psi_1 \vdash e_3 : \mathcal{R}}{\Gamma \vdash (\textbf{if}\ e_1\ e_2\ e_3) : \mathcal{R}}$$

T-APP
$$\frac{\omega \notin \mathrm{fv}(\Gamma) \qquad \mathcal{R} = \{\omega \mid \psi\} \qquad \Gamma \vdash e : \{\omega_0 \mid (x{:}\mathcal{R} \to \mathcal{R}')_{\omega_0}\} \qquad \Gamma \vdash e' : \{\omega \mid \psi\}}{\Gamma \vdash (e\ e') : \mathcal{R}[\omega/x]}$$

T-SUBSUME
$$\frac{\Gamma \vdash e : \mathcal{R} \qquad \Gamma \vdash \mathcal{R} <: \mathcal{R}'}{\Gamma \vdash e : \mathcal{R}'}$$

T-LET
$$\frac{x, \omega_1 \notin \mathrm{fv}(\Gamma) \qquad \Gamma \vdash e_1 : \{\omega_1 \mid \psi_1\} \qquad \Gamma, \psi_1[\omega_1/x] \vdash e : \mathcal{R}}{\Gamma \vdash (\textbf{let}\ (x\ e_1)\ e) : \mathcal{R}}$$

T-CONS
$$\frac{\Gamma \vdash e_1 : \mathcal{R}_1 \qquad \Gamma \vdash e_2 : \mathcal{R}_2}{\Gamma \vdash (\mathit{cons}\ e_1\ e_2) : \langle \mathcal{R}_1, \mathcal{R}_2 \rangle}$$

T-CAR
$$\frac{\omega, \omega_1 \notin \mathrm{fv}(\Gamma) \qquad \Gamma \vdash e : \{\omega_1 \mid \psi_1\} \qquad \psi_1 \vdash \langle \top, \top \rangle_{\omega_1}}{\Gamma \vdash (\mathit{car}\ e) : \{\omega \mid \psi_1 \wedge \textbf{car}(\omega_1) \equiv \omega\}}$$

T-CDR
$$\frac{\omega, \omega_1 \notin \mathrm{fv}(\Gamma) \qquad \Gamma \vdash e : \{\omega_1 \mid \psi_1\} \qquad \psi_1 \vdash \langle \top, \top \rangle_{\omega_1}}{\Gamma \vdash (\mathit{cdr}\ e) : \{\omega \mid \psi_1 \wedge \textbf{cdr}(\omega_1) \equiv \omega\}}$$

T-ABS
$$\frac{x \notin \mathrm{fv}(\Gamma) \qquad \mathcal{R} = \{\omega \mid \psi\} \qquad \Gamma, \psi[x/\omega] \vdash e : \mathcal{R}'}{\Gamma \vdash \lambda x^{\mathcal{R}}.e : x{:}\mathcal{R} \to \mathcal{R}'}$$

Figure 3. Typing Rules

S-REFL
$$\Gamma \vdash \tau <: \tau$$

S-PAIR
$$\frac{\Gamma \vdash \mathcal{R}_1 \sqsubseteq \mathcal{R}_1' \qquad \Gamma \vdash \mathcal{R}_2 \sqsubseteq \mathcal{R}_2'}{\Gamma \vdash \langle \mathcal{R}_1, \mathcal{R}_2 \rangle <: \langle \mathcal{R}_1', \mathcal{R}_2' \rangle}$$

S-FUN
$$\frac{x \notin \mathrm{fv}(\Gamma) \qquad \Gamma \vdash \mathcal{R}_1' \sqsubseteq \mathcal{R}_1 \qquad \Gamma \vdash \mathcal{R}_2 \sqsubseteq \mathcal{R}_2'}{\Gamma \vdash x{:}\mathcal{R}_1 \to \mathcal{R}_2 <: x{:}\mathcal{R}_1' \to \mathcal{R}_2'}$$

S-UNIONSUPER
$$\frac{\exists i.\ \Gamma \vdash \tau <: \sigma_i}{\Gamma \vdash \tau <: (\bigcup \overrightarrow{\sigma}^{i})}$$

S-UNIONSUB
$$\frac{\overrightarrow{\Gamma \vdash \tau_i <: \sigma}^{i}}{\Gamma \vdash (\bigcup \overrightarrow{\tau}^{i}) <: \sigma}$$

SR-REFINE
$$\frac{\omega \notin \mathrm{fv}(\Gamma) \qquad \Gamma \vdash \psi_1 \supset \psi_2}{\Gamma \vdash \{\omega \mid \psi_1\} \sqsubseteq \{\omega \mid \psi_2\}}$$

Figure 4. Subtyping rules

$$
\textsc{L-Atom}\ \frac{\psi \in \Gamma}{\Gamma \vdash \psi}
\qquad
\textsc{L-True}\ \Gamma \vdash \mathtt{tt}
\qquad
\textsc{L-False}\ \frac{\Gamma \vdash \mathtt{ff}}{\Gamma \vdash \psi}
\qquad
\textsc{L-AndI}\ \frac{\begin{array}{c}\Gamma \vdash \psi_1 \\ \Gamma \vdash \psi_2\end{array}}{\Gamma \vdash \psi_1 \wedge \psi_2}
$$

$$
\textsc{L-AndE}\ \frac{\Gamma, \psi_1 \vdash \psi \text{ or } \Gamma, \psi_2 \vdash \psi}{\Gamma, \psi_1 \wedge \psi_2 \vdash \psi}
\qquad
\textsc{L-ImplI}\ \frac{\Gamma, \psi_1 \vdash \psi_2}{\Gamma \vdash \psi_1 \supset \psi_2}
\qquad
\textsc{L-ImplE}\ \frac{\begin{array}{c}\Gamma \vdash \psi_1 \\ \Gamma \vdash \psi_1 \supset \psi_2\end{array}}{\Gamma \vdash \psi_2}
$$

$$
\textsc{L-OrI}\ \frac{\Gamma \vdash \psi_1 \text{ or } \Gamma \vdash \psi_2}{\Gamma \vdash \psi_1 \vee \psi_2}
\qquad
\textsc{L-OrE}\ \frac{\begin{array}{c}\Gamma, \psi_1 \vdash \psi \\ \Gamma, \psi_2 \vdash \psi\end{array}}{\Gamma, \psi_1 \vee \psi_2 \vdash \psi}
\qquad
\textsc{L-Sub}\ \frac{\Gamma \vdash \tau_{\pi(\kappa)} \qquad \vdash \tau <: \sigma}{\Gamma \vdash \sigma_{\pi(\kappa)}}
\qquad
\textsc{L-SubNot}\ \frac{\Gamma \vdash \overline{\sigma}_{\pi(\kappa)} \qquad \vdash \tau <: \sigma}{\Gamma \vdash \overline{\tau}_{\pi(\kappa)}}
$$

$$
\textsc{L-Alias}\ \frac{\Gamma \vdash \psi \qquad \Gamma \vdash \pi(\kappa_1) \equiv \kappa_2 \text{ or } \Gamma \vdash \kappa_2 \equiv \pi(\kappa_1)}{\Gamma \vdash \psi[\pi(\kappa_1)/\kappa_2]}
\qquad
\textsc{L-Bot}\ \frac{\Gamma \vdash \bot_{\pi(\kappa)}}{\Gamma \vdash \psi}
\qquad
\textsc{L-Update}\ \frac{\Gamma \vdash \tau_{\pi'(\kappa)} \qquad \Gamma \vdash \nu_{\pi(\pi'(\kappa))}}{\Gamma \vdash \mathsf{update}(\Gamma, \tau, \nu, \pi)_{\pi'(\kappa)}}
$$

Figure 5. Proof System

$$
\begin{array}{lcll}
\Gamma[o/\kappa] & = & \overrightarrow{\psi[o/\kappa]} & \Gamma = \overrightarrow{\psi} \\
\psi_+|\psi_-[o/\kappa] & = & \psi_+[o/\kappa]|\psi_-[o/\kappa] & \\
 & & & \\
\nu_{\pi(\kappa)}[\pi'(\kappa')/\kappa] & = & (\nu[\pi'(\kappa')/\kappa])_{\pi(\pi'(\kappa'))} & \\
\nu_{\pi(\kappa)}[\emptyset/\kappa]_+ & = & \mathtt{tt} & \\
\nu_{\pi(\kappa)}[\emptyset/\kappa]_- & = & \mathtt{ff} & \\
\nu_{\pi(\kappa)}[o/\kappa'''] & = & \nu_{\pi(\kappa)} & \kappa \neq \kappa''' \text{ and } \kappa''' \notin \text{fv}(\nu) \\
\nu_{\pi(\kappa)}[o/\kappa''']_+ & = & \mathtt{tt} & \kappa \neq \kappa''' \text{ and } \kappa''' \in \text{fv}(\nu) \\
\nu_{\pi(\kappa)}[o/\kappa''']_- & = & \mathtt{ff} & \kappa \neq \kappa''' \text{ and } \kappa''' \in \text{fv}(\nu) \\
\mathtt{tt}[o/\kappa] & = & \mathtt{tt} & \\
\mathtt{ff}[o/\kappa] & = & \mathtt{ff} & \\
(\psi_1 \supset \psi_2)[o/\kappa]_+ & = & \psi_1[o/\kappa]_- \supset \psi_2[o/\kappa]_+ & \\
(\psi_1 \supset \psi_2)[o/\kappa]_- & = & \psi_1[o/\kappa]_+ \supset \psi_2[o/\kappa]_- & \\
(\psi_1 \vee \psi_2)[o/\kappa] & = & \psi_1[o/\kappa] \vee \psi_2[o/\kappa] & \\
(\psi_1 \wedge \psi_2)[o/\kappa] & = & \psi_1[o/\kappa] \wedge \psi_2[o/\kappa] & \\
(\pi'(\kappa') \equiv \pi''(y'))[\pi(\kappa''')/\kappa] & = & \pi'(\kappa')[\pi(\kappa''')/\kappa] \equiv \pi''(y')[\pi(\kappa''')/\kappa] & \\
(\pi(\kappa'') \equiv \pi'(\kappa'''))[\emptyset/\kappa] & = & \pi(\kappa'') \equiv \pi'(\kappa''') & \kappa \neq \kappa'' \text{ and } \kappa \neq \kappa''' \\
(\pi(\kappa) \equiv \pi'(\kappa''))[\emptyset/\kappa'''] & = & \mathtt{tt} & \\
 & & & \\
\pi(\kappa)[\pi'(\kappa'')/\kappa] & = & \pi(\pi'(\kappa'')) & \\
\pi(\kappa)[\emptyset/\kappa] & = & \emptyset & \\
\pi(\kappa)[o/\kappa'''] & = & \pi(\kappa) & \kappa \neq \kappa''' \\
\emptyset[o/\kappa] & = & \emptyset & \\
 & & & \\
\{\omega \mid \psi\}[o/\kappa] & = & \{\omega \mid \psi[o/\kappa]\} & \kappa \neq \omega \\
\{\omega \mid \psi\}[o/\kappa] & = & \{\omega \mid \psi\} & \\
(x{:}\sigma \to \tau)[o/\kappa] & = & x{:}\sigma[o/\kappa] \to \tau[o/\kappa] & x \neq \kappa \\
(x{:}\sigma \to \tau)[o/\kappa] & = & x{:}\sigma[o/\kappa] \to \tau &
\end{array}
$$

Figure 6. Substitution

$$
\begin{array}{lcl}
\delta_\tau(number?) & = & x{:}\top \to \{\omega \mid \mathbf{B}_\omega \wedge \overline{\mathbf{\#f}}_\omega \supset \mathbf{N}_x \wedge \mathbf{\#f}_\omega \supset \overline{\mathbf{N}}_x\} \\
\delta_\tau(boolean?) & = & x{:}\top \to \{\omega \mid \mathbf{B}_\omega \wedge \overline{\mathbf{\#f}}_\omega \supset \mathbf{B}_x \wedge \mathbf{\#f}_\omega \supset \overline{\mathbf{B}}_x\} \\
\delta_\tau(cons?) & = & x{:}\top \to \{\omega \mid \mathbf{B}_\omega \wedge \overline{\mathbf{\#f}}_\omega \supset \langle \top, \top \rangle_x \wedge \mathbf{\#f}_\omega \supset \overline{\langle \top, \top \rangle}_x\} \\
\delta_\tau(add1) & = & x{:}\,\mathbf{N} \to \mathbf{N} \\
\delta_\tau(zero?) & = & x{:}\,\mathbf{N} \to \mathbf{B}
\end{array}
$$

Figure 7. Constant Typing

$$
\begin{array}{lcll}
\mathsf{update}(\Gamma, \langle\{\omega \mid \psi\}, \mathcal{R}\rangle, \nu, \pi :: \mathbf{car}) & = & \langle\{\omega \mid \psi \wedge \nu_{\pi(\omega)}\}, \mathcal{R}\rangle & \\
\mathsf{update}(\Gamma, \langle\mathcal{R}, \{\omega \mid \psi\}\rangle, \nu, \pi :: \mathbf{cdr}) & = & \langle\mathcal{R}, \{\omega \mid \psi \wedge \nu_{\pi(\omega)}\}\rangle & \\
\mathsf{update}(\Gamma, \tau, \sigma, \epsilon) & = & \mathsf{restrict}(\Gamma, \tau, \sigma) & \\
\mathsf{update}(\Gamma, \tau, \overline{\sigma}, \epsilon) & = & \mathsf{remove}(\Gamma, \tau, \overline{\sigma}) & \\
 & & & \\
\mathsf{restrict}(\Gamma, \tau, \sigma) & = & \bot & \text{if } \nexists v.\, \Gamma \vdash v : \{\omega \mid \sigma_\omega\} \text{ and } \Gamma \vdash v : \{\omega \mid \tau_\omega\} \\
\mathsf{restrict}(\Gamma, (\bigcup \overrightarrow{\tau}), \sigma) & = & (\bigcup \overrightarrow{\mathsf{restrict}(\Gamma, \tau, \sigma)}) & \\
\mathsf{restrict}(\Gamma, \tau, \sigma) & = & \tau & \text{if } \Gamma \vdash \tau <: \sigma \\
\mathsf{restrict}(\Gamma, \tau, \sigma) & = & \sigma & \text{otherwise} \\
 & & & \\
\mathsf{remove}(\Gamma, \tau, \sigma) & = & \bot & \text{if } \Gamma \vdash \tau <: \sigma \\
\mathsf{remove}(\Gamma, (\bigcup \overrightarrow{\tau}), \sigma) & = & (\bigcup \overrightarrow{\mathsf{remove}(\Gamma, \tau, \sigma)}) & \\
\mathsf{remove}(\Gamma, \tau, \sigma) & = & \tau & \text{otherwise}
\end{array}
$$

Figure 8. Type Update