Constrained Types for Object-Oriented Languages

Vijay Saraswat
IBM T. J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598
vsaraswa@us.ibm.com

Nathaniel Nystrom
IBM T. J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598
nystrom@us.ibm.com

Radha Jagadeesan
Depaul University
rjagadeesan@cs.depaul.edu

Jens Palsberg
University of California–Los Angeles
palsberg@cs.ucla.edu

Christian Grothoff
University of Denver
christian@grothoff.org

Syntax. The syntax for the language is specified as follows. We assume a fixed constraint system, $\mathcal{C}$, with inference relation $\vdash_{\mathcal{C}}$. However, we require all constraint systems to support conjunction and existential quantification.

$$
\begin{array}{rrcl}
\text{(Class)} & \mathrm{L} & ::= & \mathtt{class}\ T\ \mathtt{extends}\ T\ \{\bar{T}\,\bar{f};\ K\,\bar{M}\} \\
\text{(Ctor)} & \mathrm{K} & ::= & T(\bar{T}\bar{x})\{\mathtt{super}(\bar{x});\bar{f}=\bar{x}\} \\
\text{(Method)} & \mathrm{M} & ::= & T\ m(\bar{T}\ \bar{x})\{\mathtt{return}\ e;\} \\
\text{(Expr)} & \mathrm{e} & ::= & x \mid e.f \mid e.m(\bar{e}) \mid \mathtt{new}\ C(\bar{e}) \mid (T)e \\
\\
\text{(C Terms)} & \mathrm{t} & ::= & \mathrm{x} \mid \mathtt{self} \mid \mathrm{t.f} \\
\text{(Constraint)} & \mathrm{c,d} & ::= & a \mid t=t \mid c,c \mid T\,x;c \\
\text{(Type)} & \mathrm{S,T,U} & ::= & C(:d)
\end{array}
$$

Subtyping Judgements. We let Γ stand for multisets of type assertions, of the form $T\,x$, and constraints. We define $\sigma(\Gamma)$ to be the set of constraints obtained from Γ by replacing each type assertion $\mathtt{C}(:\mathtt{d})\ \mathtt{x}$ with $\mathtt{d}[\mathtt{x}/\mathtt{self}]$.

$$
\Gamma\vdash\mathtt{T}\sqsubseteq\mathtt{T}
\qquad
\frac{\mathtt{class}\ \mathtt{C}(:\mathtt{c})\,\mathtt{extends}\,\mathtt{D}(:\mathtt{d})\{\ldots\}}{\vdash\mathtt{C}(:\mathtt{c})\sqsubseteq\mathtt{D}(:\mathtt{d})}
$$

$$
\frac{\Gamma\vdash\mathtt{C}\sqsubseteq\mathtt{D}\quad\sigma(\Gamma),\mathtt{c}\vdash_{\mathcal{C}}\mathtt{d}}{\Gamma\vdash\mathtt{C}(:\mathtt{c})\sqsubseteq\mathtt{D}(:\mathtt{d})}
\qquad
\frac{\Gamma\vdash\mathtt{S}\sqsubseteq\mathtt{T}\quad\Gamma\vdash\mathtt{T}\sqsubseteq\mathtt{U}}{\Gamma\vdash\mathtt{S}\sqsubseteq\mathtt{U}}
$$

Type Judgements.

$$
\Gamma,\mathtt{T}\ \mathtt{x}\vdash\mathtt{T}\ \mathtt{x}\ \text{(T-VAR)}
\qquad
\frac{\Gamma\vdash\mathtt{C}(:\mathtt{c})\ \mathtt{x}\quad\sigma(\Gamma)\vdash_{\mathcal{C}}\mathtt{d}[\mathtt{x}/\mathtt{self}]}{\Gamma\vdash\mathtt{C}(:\mathtt{c},\mathtt{d})\ \mathtt{x}}\ \text{(CONSTR)}
$$

$$
\frac{\Gamma\vdash\mathtt{T}_0\ \mathtt{e}\quad \mathit{fields}(\mathtt{T}_0)=\bar{\mathtt{U}}(:\bar{\mathtt{d}})\bar{\mathtt{f}}}{\Gamma\vdash\mathtt{U}_i(:\mathtt{T}_0\ \mathtt{this};\mathtt{this.f}=\mathtt{self},\mathtt{d}_i)\ \mathtt{e.f}_i}\ \text{(T-Field)}
$$

$$
\frac{\Gamma\vdash\mathtt{S}\ \mathtt{e}\quad\Gamma\vdash\mathtt{S}\sqsubseteq\mathtt{T}}{\Gamma\vdash\mathtt{T}\ (\mathtt{T})\mathtt{e}}\ \text{(T-UCast)}
\qquad
\frac{\Gamma\vdash\mathtt{S}\ \mathtt{e}\quad\Gamma\vdash\mathtt{T}\sqsubseteq\mathtt{S}}{\Gamma\vdash\mathtt{T}\ (\mathtt{T})\mathtt{e}}\ \text{(T-DCast)}
$$

$$
\frac{\Gamma\vdash\mathtt{S}\ \mathtt{e}\quad\Gamma\not\vdash\mathtt{T}\sqsubseteq\mathtt{S}\quad\Gamma\not\vdash\mathtt{S}\sqsubseteq\mathtt{T}}{\Gamma\vdash\mathtt{T}\ (\mathtt{T})\mathtt{e}}\ \text{(T-SCast)}
$$

$$
\frac{\begin{array}{l}\Gamma\vdash\mathtt{T}_{0:n}\mathtt{e}_{0:n}\\ \mathtt{T}_0\rhd\mathtt{S}(:\mathtt{d})\mathtt{m}(\mathtt{Z}_{1:n}\,\mathtt{z}_{1:n})\\ \Gamma,\mathtt{T}_0\ \mathtt{this},\mathtt{T}_{1:i-1}\ \mathtt{z}_{1:i-1}\vdash\mathtt{T}_i\sqsubseteq\mathtt{Z}_i\quad(i\in 1:n)\end{array}}{\Gamma\vdash\mathtt{S}(:\mathtt{T}_0\ \mathtt{this};\mathtt{T}_{1:n}\ \mathtt{z}_{1:n};\mathtt{d})\ \mathtt{e}_0.\mathtt{m}(\mathtt{e}_{1:n})}\ \text{(T-INVK)}
\qquad
\frac{\begin{array}{l}\Gamma\vdash\mathtt{T}_{1:n}\ \mathtt{e}_{1:n}\\ \mathtt{C}\rhd\mathtt{C}(:\mathtt{d})(\mathtt{Z}_{1:n}\ \mathtt{f}_{1:n})\\ \Gamma,\mathtt{T}_{1:(i-1)}\ \mathtt{f}_{1:(i-1)}\vdash\mathtt{T}_i\sqsubseteq\mathtt{Z}_i\quad(i\in 1:n)\\ \Gamma,\mathtt{T}_{1:n}\ \mathtt{f}_{1:n}\vdash\mathtt{d}\end{array}}{\Gamma\vdash\mathtt{C}(:\mathtt{T}_{1:n}\ \mathtt{f}_{1:n};\mathtt{self.f}_{1:n}=\mathtt{f}_{1:n},\mathtt{d})\ \mathtt{new}\ \mathtt{C}(\mathtt{e}_{1:n})}\ \text{(T-NEW)}
$$

Method and Class Typing.

$$
\frac{\begin{array}{c}\bar{T}\ \bar{x},C\ \mathtt{this}\vdash S\ e\\ \bar{T}\ \bar{x},C\ \mathtt{this}\vdash S\sqsubseteq T\end{array}}{T\ m(\bar{T}\ \bar{x})\{\mathtt{return}\ e;\}\ \text{OK in}\ C}
\qquad
\frac{\begin{array}{l}K=C(\bar{S}\,\bar{g},\bar{T}\,\bar{f})\{\mathtt{super}(\bar{g});\mathtt{this}.\bar{f}=\bar{f};\}\\ D\rhd\bar{S}\ \bar{g}\\ \bar{M}\ \text{OK in}\ C\end{array}}{\mathtt{class}\ C\ \mathtt{extends}\ D\ \{\bar{T}\,\bar{f};K\bar{M}\}\ \text{OK}}
$$

Table 1. Constrained FJ

THEOREM 0.1 (Subject Reduction). *If $\Gamma\vdash T\ e$ and $e\longrightarrow e'$ then for some type S, $\Gamma\vdash S\ e'$ and $\Gamma\vdash S\sqsubseteq T$.*

Let the normal form of expressions be given by *values*, i.e. expressions

$$\text{(Values)}\quad \mathtt{v}\quad ::=\quad \mathtt{new}\ \mathtt{C}(\bar{\mathtt{v}})$$

THEOREM 0.2 (Type Soundness). *If $\vdash T\ e$ and $e\longrightarrow^{*} e'\not\longrightarrow$ then e' is either (1) a value with $\vdash\mathtt{S}\ \mathtt{v}$ and $\vdash\mathtt{S}\sqsubseteq\mathtt{T}$, for some type $\mathtt{S}$, or, (2) an expression containing a subexpression $(\mathtt{T})\mathtt{new}\ \mathtt{C}(\bar{\mathtt{v}})$ where $\not\vdash\mathtt{C}\sqsubseteq\mathtt{T}[\mathtt{new}\ \mathtt{C}(\bar{\mathtt{v}})/\mathtt{self}]$.*

Computation:

$$\frac{fields(C) = \bar{C}\ \bar{f}}{(\texttt{new C}(\bar{\texttt{e}})).\texttt{f}_i \longrightarrow \texttt{e}_i}\ \text{(R-FIELD)}$$

$$\frac{mbody(\texttt{m},\texttt{C}) = \bar{x}.\bar{e}_0}{(\texttt{new C}(\bar{\texttt{e}})).\texttt{m}(\bar{\texttt{d}}) \longrightarrow [\bar{d}/\bar{x}, \texttt{new}\ C(\bar{e})/\texttt{this}]\texttt{e}_0}\ \text{(R-INVK)}$$

$$\frac{\vdash C \sqsubseteq D[\texttt{new}\ C(\bar{\texttt{d}})/\texttt{self}]}{(\texttt{D})(\texttt{new C}(\bar{\texttt{d}})) \longrightarrow \texttt{new}\ C(\bar{\texttt{d}})}\ \text{(R-CAST)}$$

Congruence:

$$\frac{\texttt{e}_0 \longrightarrow \texttt{e}_0{}'}{\texttt{e}_0.\texttt{f} \longrightarrow \texttt{e}_0{}'.\texttt{f}}\ \text{(RC-FIELD)}$$

$$\frac{\texttt{e}_0 \longrightarrow \texttt{e}_0{}'}{\texttt{e.m}(\bar{\texttt{e}}) \longrightarrow \texttt{e}_0{}'.\texttt{m}(\bar{\texttt{e}})}\ \text{(RC-INVK-RECV)}$$

$$\frac{\texttt{e}_i \longrightarrow \texttt{e}_i{}'}{\texttt{e.m}(\ldots,\texttt{e}_i,\ldots) \longrightarrow \texttt{e}_0.\texttt{m}(\ldots,\texttt{e}_i',\ldots)}\ \text{(RC-INVK-ARG)}$$

$$\frac{\texttt{e}_i \longrightarrow \texttt{e}_i{}'}{\texttt{new C}(\ldots,\texttt{e}_i,\ldots) \longrightarrow \texttt{new C}(\ldots,\texttt{e}_i',\ldots)}\ \text{(RC-NEW-ARG)}$$

$$\frac{\texttt{e}_0 \longrightarrow \texttt{e}_0{}'}{(\texttt{C})\texttt{e}_0 \longrightarrow (\texttt{C})\texttt{e}_0{}'}\ \text{(RC-CAST)}$$

Table 2. Reduction rules for Constrained FJ