A locally nameless solution to the POPLmark challenge

Xavier Leroy

INRIA Rocquencourt

Locally nameless representations (McKinna & Pollack)

Use names for free variables and de Bruijn indices for bound variables.

$$
\begin{array}{rcll}
\tau & ::= & X, Y, Z, \ldots & \text{free variables} \\
& | & 0, 1, 2, \ldots & \text{bound variables} \\
& | & \top & \\
& | & \tau_1 \to \tau_2 & \\
& | & \forall <: \tau_1 .\ \tau_2 & \text{binds variable 0 in } \tau_2
\end{array}
$$

Term equality is α-equivalence.

Substitutions

- $\tau[X \leftarrow \tau']$ substitution of a name.

  Name capture cannot occur.

- $\tau[n \leftarrow \tau']$ substitution of a de Bruijn index.

  No need to shift de Bruijn indices in τ' if we consider only terms that have no free de Bruijn indices.

Working with closed (de Bruijn) terms

Nominal:
recurse from $\forall X <: \tau_1.\ \tau_2$ to τ_2 with a suitably fresh X.

Locally nameless, bad:
recurse from $\forall <: \tau_1.\ \tau_2$ to τ_2.

Locally nameless, good:
recurse from $\forall <: \tau_1.\ \tau_2$ to $\tau_2[0 \leftarrow X]$ for a suitably fresh X.

Well-formedness of types

Bad: τ is well-formed in Γ iff $FdBV(\tau) = \emptyset$ and $FV(\tau) \subseteq \mathrm{Dom}(\Gamma)$.

Good: inductive predicate $\Gamma \vdash \tau \ \mathtt{ok}$.

$$\frac{X \in \mathrm{Dom}(\Gamma)}{\Gamma \vdash X \ \mathtt{ok}} \qquad \Gamma \vdash \top \ \mathtt{ok} \qquad \frac{\Gamma \vdash \tau_1 \ \mathtt{ok} \qquad \Gamma \vdash \tau_2 \ \mathtt{ok}}{\Gamma \vdash \tau_1 \to \tau_2 \ \mathtt{ok}}$$

$$\frac{X \notin \mathrm{Dom}(\Gamma) \qquad X \notin FV(\tau_2) \qquad \begin{array}{c}\Gamma \vdash \tau_1 \ \mathtt{ok} \\ \Gamma, X <: \tau_1 \vdash \tau_2[0 \leftarrow X] \ \mathtt{ok}\end{array}}{\Gamma \vdash \forall <: \tau_1.\ \tau_2 \ \mathtt{ok}}$$

The ∀-∃ game

$$\frac{\Gamma \vdash \tau_1 \ \mathtt{ok} \qquad \forall X,\ \ X \notin \mathsf{Dom}(\Gamma) \wedge X \notin FV(\tau_2) \Rightarrow \Gamma, X <: \tau_1 \vdash \tau_2[0 \leftarrow X] \ \mathtt{ok}}{\Gamma \vdash \forall <: \tau_1.\ \tau_2 \ \mathtt{ok}} \quad (1)$$

$$\frac{\Gamma \vdash \tau_1 \ \mathtt{ok} \qquad \vdash \Gamma \ \mathtt{ok} \qquad \exists X,\ \ X \notin \mathsf{Dom}(\Gamma) \wedge X \notin FV(\tau_2) \Rightarrow \Gamma, X <: \tau_1 \vdash \tau_2[0 \leftarrow X] \ \mathtt{ok}}{\Gamma \vdash \forall <: \tau_1.\ \tau_2 \ \mathtt{ok}} \quad (2)$$

Fact: both rules define equivalent predicates.

Choice: take (1) as the inference rule and show that (2) is admissible.

Justification: the predicate $\Gamma \vdash \tau \ \mathtt{ok}$ is equivariant (stable by swaps).

The challenge, part 1a

Definition of $\Gamma \vdash \tau_1 <: \tau_2$:

$$\frac{\Gamma \vdash \tau_1 <: \sigma_1 \qquad \forall X,\ X \notin \mathrm{Dom}(\Gamma) \Rightarrow \Gamma, X <: \tau_1 \vdash \sigma_2[0 \leftarrow X] <: \tau_2[0 \leftarrow X]}{\Gamma \vdash (\forall <: \sigma_1.\ \sigma_2) <: (\forall <: \tau_1.\ \tau_2)}$$

Same $\forall$-$\exists$ game.

Reflexivity of subtyping: by induction on a derivation of $\Gamma \vdash \tau\ \mathtt{ok}$ (instead of induction on the structure of τ) + use of the $\exists$ rule.

Transitivity of subtyping: as in the paper proof, but replace outer induction on the structure of the middle type by a Peano induction on the size of that type.

The other parts of the challenge

Ran out of time and fortitude.

A feeling of turning the crank.

Overheads

Substitution functions ($\times$ 2).

Definition of free variables.

Swaps.

Equivariance properties.

Admissibility of the $\exists$ rules.

Environment manipulations (e.g. $\Gamma_1, X <: P, \Gamma_2$).