Algorithmic Subtyping for Higher Order Bounded Quantification Revisited

Dulma Rodriguez

Department of Computer Science
Ludwig-Maximilians-University Munich

TYPES Conference - Turin 2008
March 27, 2008

Introduction

- System: $F^{\omega}_{<:} = F^{\omega}$ + subtyping + bounded polymorphism.
- Models subtyping aspects of object oriented type systems.
- Metatheory: Algorithms for deciding typing and **subtyping**.
- Approach: Normalization of constructors and elimination of the transitivity rule.
- New results: Syntactical proofs of completeness, without model construction.

System $F^{\omega}_{<:}$

Type constructors

$$A, B, F, G \quad ::= \quad X \mid \lambda X F \mid F\ G \mid A \to B \mid \forall X \leq G : \kappa.\ A \mid \top$$

U, V, W type constructors in $\beta\eta$-normal form.

Kinds

$$\kappa ::= * \mid \kappa_1 \to \kappa_2$$

Contexts

$$\Gamma ::= \diamond \mid \Gamma, X \leq G : \kappa$$

Kinding

- Kinding

$$\Gamma \vdash F : \kappa$$

- Rules

$$\frac{\Gamma, X \leq G : \kappa \vdash A : *}{\Gamma \vdash \forall X \leq G : \kappa.\, A : *} \quad \text{(K-All)}$$

$$\frac{(X \leq G : \kappa) \in \Gamma \qquad \Gamma \vdash G : \kappa}{\Gamma \vdash X : \kappa} \quad \text{(K-Var-Bound)}$$

Declarative Equality and Subtyping

- Judgments

$$\Gamma \vdash F = F' : \kappa \qquad \beta\eta\text{-equality}$$
$$\Gamma \vdash F \leq F' : \kappa \qquad \text{subtyping}$$

- Rules for subtyping

$$\frac{\Gamma \vdash A : *}{\Gamma \vdash A \leq \top : *}\ (\text{S-Top}) \qquad \frac{\Gamma \vdash \quad X \leq G : \kappa \in \Gamma}{\Gamma \vdash X \leq G : \kappa}\ (\text{S-Var})$$

$$\frac{\Gamma \vdash G = G' : \kappa \qquad \Gamma, X \leq G : \kappa \vdash A \leq A' : *}{\Gamma \vdash \forall X \leq G : \kappa . A \leq \forall X \leq G' : \kappa . A' : *}\ (\text{S-All})$$

$$\frac{\Gamma \vdash F = G : \kappa}{\Gamma \vdash F \leq G : \kappa}\ (\text{S-Eq}) \qquad \frac{\Gamma \vdash F \leq G : \kappa \qquad \Gamma \vdash G \leq H : \kappa}{\Gamma \vdash F \leq H : \kappa}\ (\text{S-Trans})$$

Algorithmic Subtyping: Overview

- Judgment for algorithmic subtyping: $\Gamma \vdash_{\mathsf{a}} V \leq V' : \kappa$
- Approach: Fully $\beta\eta$-normalization of type constructors.

- **Steps**:
- Define normalization function $\mathsf{nf}()$.
- Prove soundness and completeness of $\mathsf{nf}()$.
- Define characterization of normal constructors $\Gamma \vdash V \Uparrow \kappa$.
- Apply the algorithm to normal constructors.
- Prove soundness, completeness and termination of the algorithm.

Normalizing the constructors

- Define $\mathsf{nf}_{\Gamma \vdash \kappa}(F)$ for $\Gamma \vdash F : \kappa$

$$\begin{array}{lcl} \mathsf{nf}_{\Gamma \vdash \vec{\kappa} \to *}(X) & := & \lambda \vec{Y}.X\, \mathsf{nf}_{\Gamma \vdash \vec{\kappa}}(\vec{Y}) \\ \mathsf{nf}_{\Gamma \vdash \kappa'}(F\, G) & := & \mathsf{nf}_{\Gamma \vdash \kappa \to \kappa'}(F)\, @^{\kappa}\, \mathsf{nf}_{\Gamma \vdash \kappa}(G) \end{array}$$

- using $F\, @^{\kappa}\, G$:

$$\begin{array}{lcl} \lambda X F\, @^{\kappa}\, G & := & [G/X]^{\kappa} F \\ N\, @^{\kappa}\, G & := & N\, G \end{array}$$

- and hereditary substitution $[G/X]^{\kappa} F$:

$$\begin{array}{lcl} [G/X]^{\kappa_1 \to \kappa_2}(X\, H) & := & G\, @^{\kappa_2}\, ([G/X]^{\kappa_1 \to \kappa_2} H) \\ [G/X]^{\kappa_1 \to \kappa_2}(Y\, H) & := & Y\, ([G/X]^{\kappa_1 \to \kappa_2} H) \end{array}$$

- $\mathsf{nf}()$ terminates

Characterization of normal forms I

- Define $\Gamma \vdash V \Uparrow \kappa$

$$\frac{(X \leq U : \vec{\kappa} \to *) \in \Gamma \qquad \Gamma \vdash V_i \Uparrow \kappa_i \qquad \Gamma \vdash U \mathbin{@}^{\vec{\kappa}} \vec{V} \Uparrow *}{\Gamma \vdash X\,\vec{V} \Uparrow *}$$

- V is in η-long β-normal form and all *hidden redexes* are normalizable.
- E.g.,

$$\forall X \leq (\lambda Y.V) : * \to *.XW$$

contains the hidden redex

$$(\lambda Y.V)W$$

Characterization of normal forms II

Lemma (Substitution and application for normal forms)

Let $\mathcal{E} :: \Gamma \vdash U \Uparrow \kappa$.

1. *If* $\mathcal{D} :: \Gamma, X:\kappa, \Gamma' \vdash V \Uparrow \kappa'$ *then* $\Gamma, [U/X]^{\kappa}\Gamma' \vdash [U/X]^{\kappa} V \Uparrow \kappa'$.
2. *If* $\mathcal{D} :: \Gamma \vdash V \Uparrow \kappa \to \kappa'$ *then* $\Gamma \vdash V \mathbin{@}^{\kappa} U \Uparrow \kappa'$.

Proof.

Simultaneously by lexicographical induction on $(|\kappa|, \mathcal{D})$. □

- Consequences of the lemma: Completeness
  1. $\Gamma \vdash F : \kappa$ implies $\mathsf{nf}(\Gamma) \vdash \mathsf{nf}(F) \Uparrow \kappa$
  2. $\Gamma \vdash F = F' : \kappa$ implies $\mathsf{nf}(F) \equiv \mathsf{nf}(F')$

Algorithm

- Judgment for algorithmic subtyping: $\Gamma \vdash_{\mathsf{a}} V \leq V' : \kappa$.
- Apply the algorithm to normal forms:

$$U, V, W ::= X\vec{V} \mid \lambda X V \mid V \to V' \mid \forall X \leq U : \kappa.W \mid \top$$

- Elimination of (S-Eq), (S-App) and (S-Trans).
- New rules:

$$\frac{(X \leq U : \kappa) \in \Gamma \qquad \Gamma \vdash_{\mathsf{a}} U @^{\vec{\kappa}} \vec{V} \leq W : *}{\Gamma \vdash_{\mathsf{a}} X\vec{V} \leq W : *} \text{ (SA-Bound)}$$

$$\frac{}{\Gamma \vdash_{\mathsf{a}} X\vec{V} \leq X\vec{V} : *} \text{ (SA-Refl)}$$

Completeness of the algorithm

- Reflexivity and transitivity easy.
- Admissibility of (S-App) needs substitution lemma

$$\frac{\Gamma \vdash F \leq F' : \kappa \to \kappa' \qquad \Gamma \vdash H : \kappa}{\Gamma \vdash FH \leq F'H : \kappa'} \text{ (S-App)}$$

Lemma (Substitution)

Let $\Gamma, X:\kappa, \Gamma' \vdash V, V' \Uparrow \kappa'$ *and* $\Gamma \vdash U \Uparrow \kappa$.
If $\Gamma, X:\kappa, \Gamma' \vdash_{\mathsf{a}} V \leq V' : \kappa'$ *then*
$\Gamma, [U/X]^{\kappa}\Gamma' \vdash_{\mathsf{a}} [U/X]^{\kappa}V \leq [U/X]^{\kappa}V' : \kappa'$.

Proof.

By induction on the algorithmic subtyping derivation. □

Termination of the algorithm

Theorem (Termination of algorithmic subtyping)

If $\mathcal{D}_1 :: \Gamma \vdash V \Uparrow \kappa$ *and* $\mathcal{D}_2 :: \Gamma \vdash V' \Uparrow \kappa$ *then the query* $\Gamma \vdash_{\mathsf{a}} V \leq V' : \kappa$ *terminates.*

Proof.

By simultaneous induction on $\mathcal{D}_1 + \mathcal{D}_2$. The interesting case is:

$$\mathcal{D}_1 :: \frac{(X \leq U : \vec{\kappa} \to *) \in \Gamma \qquad \Gamma \vdash V_i \Uparrow \kappa_i \text{ for all } i \qquad \Gamma \vdash U \mathbin{@}^{\vec{\kappa}} \vec{V} \Uparrow *}{\Gamma \vdash X\vec{V} \Uparrow *}$$

We show: $\Gamma \vdash_{\mathsf{a}} X\vec{V} \leq V' : *$ terminates. By I.H. , $\Gamma \vdash_{\mathsf{a}} U \mathbin{@}^{\vec{\kappa}} \vec{V} \leq V' : *$ terminates. $\square$

Related Work

- Pierce and Steffen 1997: $F^{\omega}_{<:}$ with reductions
- Compagnoni and Goguen 2003: $F^{\omega}_{\leq}$ with typed operational semantics
- Watkins et al. 2003: Hereditary substitutions
- Harper 2007: Canonical Logical Framework

Conclusions

- We provide:
  - Normalization function for $F^{\omega}_{<:}$.
  - Algorithm for deciding subtyping of $F^{\omega}_{<:}$.
- Evaluation of proofs:
  - Short, direct
  - Purely syntactical
  - Avoiding logical relations and models
  - Well suited for formalization (e.g., in Twelf).
- Further work
  - Extending this approach to similar systems
  - polarized system $F^{\omega}_{<:}$, system $F^{\omega}_{\leq}$, ...