Strong Normalization by HOAS

Andrei Popescu

Joint work with Elsa Gunter

Simply-typed λ-calculus - Syntax

First-order syntax (up to α):

- Curry-style: no type annotations
- Data variables x, y, z, data terms X,Y, Z, data abstractions A, B

X ::= x | App X Y | Lam A A ::= x . X

- Type variables tx, ty, tz, type terms tX, tY, tZ, type abstractions tA, tB

tX ::= tx | Arr tX tY

β-reduction (of untyped λ-calculus)

App (Lam (x . Y)) X ~~> Y [X / x] (Beta)

$$\frac{Y \rightsquigarrow Y'}{Lam\ (x\ .\ Y) \rightsquigarrow Lam\ (x\ .\ Y')}\ (Xi)$$

$$\frac{X \rightsquigarrow X'}{App\ X\ Y \rightsquigarrow App\ X'\ Y}\ (App\text{-}Left)$$

Typing

$$\frac{}{\Gamma, x : tX \vdash x : tX}\ [x \text{ fresh } \Gamma]\ (\text{Asm})$$

$$\frac{\Gamma \vdash Y : tY}{\Gamma, x : tX \vdash Y : tY}\ [x \text{ fresh } \Gamma]\ (\text{Weak})$$

$$\frac{\Gamma, x : tX \vdash Y : tY}{\Gamma \vdash \text{Lam } (x \,.\, Y) : \text{Arr } tX\ tY}\ [x \text{ fresh } \Gamma]\ (\text{Arr-I})$$

$$\frac{\Gamma \vdash Z : \text{Arr } tX\ tY \quad \Gamma \vdash X : tX}{\Gamma \vdash \text{App } Z\ X : tY}\ (\text{Arr-E})$$

Abstractions as functions

- FOAS definition/construction: A = (x . X)
- HOAS treatment: A _ Y = A applied to Y, defined to be X [Y / x]
- May regard abstractions as forming a subspace of Term → Term
- This view accommodates a certain way to represent inference relations

HOAS representation of β-reduction

App (Lam (x . Y)) X ~~> Y [X / x] (Beta-FOAS)

App (Lam A) X ~~> A _ X (Beta-HOAS)

$$\frac{Y \rightsquigarrow Y'}{Lam\ (x\ .\ Y) \rightsquigarrow Lam\ (x\ .\ Y')}\ \text{(Xi-FOAS)}$$

$$\frac{\forall\ X.\ A\ \_\ X \rightsquigarrow A'\ \_\ X}{Lam\ A \rightsquigarrow Lam\ A'}\ \text{(Xi-HOAS)}$$

HOAS representation of typing

$\forall \Gamma$ - (typing) context, i.e., list of pairs (data variable, type term):

$$x_1 : tX_1, \ldots, x_n : tX_n$$

$\forall \Delta$ - HOAS context, i.e., list of pairs (data term, type term):

$$X_1 : tX_1, \ldots, X_n : tX_n$$

- Note: we close under substitution

HOAS representation of typing

$$\frac{\Gamma, x : tX \;\vdash\; Y : tZ}{\Gamma \vdash \mathrm{Lam}\ (x\ .\ Y) : \mathrm{Arr}\ tX\ tZ}\ [x \text{ fresh for } \Gamma]\quad \text{(Arr-I-FOAS)}$$

$$\frac{\forall\, X.\ \ \Delta, X : tX \;\Vdash\; A\ \_\ X : tZ}{\Delta \Vdash \mathrm{Lam}\ A : \mathrm{Arr}\ tX\ tZ}\quad \text{(Arr-I-HOAS)}$$

HOAS representation of typing

$$\frac{}{\Delta, X : tX \vdash X : tX}\ (Asm)$$

$$\frac{\Delta \vdash Y : tY}{\Delta, X : tX \vdash Y : tY}\ (Weak)$$

$$\frac{\Delta \vdash Z : Arr\ tX\ tY \qquad \Delta \vdash X : tX}{\Delta \vdash App\ Z\ X : tY}\ (Arr\text{-}E)$$

“Context-free” induction principle for typing

If H : **data-term** → **type-term** → **bool** s.t.:

$$\frac{\forall\, X.\ H\ X\ tX \ \Rightarrow\ H\ (A\ \_\ X)\ tZ}{H\ (Lam\ A)\ (Arr\ tX\ tZ)}\ (ArrI\text{-}H)$$

etc., then $\forall\ X\ \ tX.\ [] \ ||\text{-}\ X : tX \ \Rightarrow\ H\ X\ tX$

(Higher degree of HOAS – not only bindings and substitution, but also inference contexts are pushed to the meta-level)

Strong normalization

- Termination: X is strongly terminating = all reduction sequences X ~~> X' ~~> X'' ~~> … are finite
- If confluence holds, then strongly terminating means the existence of a unique normal form, hence the phrase strongly normalizating
- The strong normalization property:

$$\forall X. \quad X \text{ typable} \quad \Rightarrow$$

$$X \text{ strongly normalizing } (X \in SN)$$

Proof of strong normalization

$$\Gamma \vdash X : tX \quad \Rightarrow \quad X \in SN$$

Proof of strong normalization

Difficulty

$\Gamma \vdash X : tX \Rightarrow X \in SN$

Proof of strong normalization

Difficulty

$$\Gamma \vdash X : tX \Rightarrow X \in SN$$

Solution:

- Strengthen the rhs of the goal
- Integrate contexts into the goal's statement
- Give an SN-semantic interpretation to the relation |-
- Close everything under substitution in arbitrary environments

FOAS proof

- Define $[\ \_\ ] : \mathrm{Tterm} \rightarrow \mathbf{P}(\mathrm{SN})$
  - $[\ tX\ ] = SN$
  - $[\ \mathrm{Arr}\ tX\ tY\ ] = \{Z.\ \forall\ X \in [tX].\ \mathrm{App}\ Z\ X \in [tY]\ \}$
- Define $\Gamma \models X : tX$ to mean:

$$\forall\ \rho : \mathrm{Dvar} \rightarrow \mathbf{P}(\mathrm{SN}).$$

$$(\forall\ (y : tY) \in \Gamma.\ \ \rho\ y \in [tY]) \ \Rightarrow\ \rho\ X \in [\rho\ \ tX]$$

- Prove, by rule induction

$$\Gamma \vdash X : tX \ \Rightarrow\ \Gamma \models X : tX$$

FOAS proof

- Want: $\Gamma, x : tX \;||\!-\; Y : tY$

$$\text{----------[x fresh } \Gamma\text{]}$$

$$\Gamma \;||\!-\; \text{Lam } (x \,.\, Y) : \text{Arr } tX\ tY$$

Assume the upper side. Fix ρ. Assume $\Gamma \;||\!-\; \rho$.

Want $\underline{\rho}$ (Lam (x . Y)) $\in$ [Arr tX tY], i.e.,

Lam (x . $\underline{\rho\ [x \leftarrow x]}$ Y) $\in$ [Arr tX tY].

Fix $X \in [tX]$. Want App (Lam (x . $\underline{\rho\ [x \leftarrow x]}$ Y)) $X \in [tY]$

Since x fresh Γ, have $\Gamma, x : tX \;||\!-\; \rho[x \leftarrow \underline{\rho}\ X]$.

With IH, have $\underline{\rho[x \leftarrow \rho\ X]}\ Y \in [\ tY\ ]$, i.e.,

$(\underline{\rho[x \leftarrow x]}\ Y)\ [X / x]) \in [\ tY\ ]$.

FOAS proof

- Discovered: would suffice that:

  $Y\,[X / x] \in [\,tY\,] \quad \Rightarrow \quad App\,(Lam\,(x\,.\,Y))\,X \in [tY]$

- A stronger version of this follows by induction on the definition of [_]

HOAS proof

= Still define $[\ \_\ ] : \mathrm{Tterm} \rightarrow \mathbf{P}(\mathrm{SN})$

\+ No environments, no typing contexts, no semantic consequence relation

Want: $\forall\ X.\ X \in [tX] \quad \Rightarrow \quad A\ \_\ X \in [tY]$

$$\text{----------}$$

$$\mathrm{Lam}\ A \in [\mathrm{Arr}\ tX\ tY]$$

\+ Discovered immediately: would suffice that:

$$A\ \_\ X \in [\ tY\ ] \quad \Rightarrow \quad \mathrm{App}\ (\mathrm{Lam}\ A)\ X \in [tY]$$

= Again, a stronger version of this follows by induction on the definition of $[\ \_\ ]$

\- Only in empty contexts proved (but extension immediate)