Normalization by Evaluation for System F

Andreas Abel

Department of Computer Science
Ludwig-Maximilians-University Munich

ProgLog Seminar, Chalmers, Göteborg
3 September 2008

Introduction

- NbE is a principled approach to full normalization
- and to deciding $\beta\eta$-equality.
- Previous work with Klaus Aehlig, Thierry Coquand, Peter Dybjer: NbE for predicative dependent type theories.
- Goal: tackle impredicativity.
- Altenkirch, Hofmann, and Streicher described NbE for System F using heavy category-theoretic machinery.
- This work: conventional, set-theoretic development.

Outline

1. System F
2. Weak beta-eta-Normalization
3. Normalization by Evaluation
4. Conclusions

Church-Style System F

- Terms and Typing

$$\frac{}{\Gamma \vdash x : \Gamma(x)}$$

$$\frac{\Gamma, x{:}A \vdash t : B}{\Gamma \vdash \lambda x{:}A.\, t : A \to B} \qquad \frac{\Gamma \vdash r : A \to B \qquad \Gamma \vdash s : A}{\Gamma \vdash r\, s : B}$$

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \Lambda X t : \forall X A}\ X \notin \mathrm{FV}(\Gamma) \qquad \frac{\Gamma \vdash t : \forall X A}{\Gamma \vdash t\, B : A[B/X]}$$

- We write $\Gamma' \leq \Gamma$ if Γ' extends Γ. E.g., $\Gamma, x{:}A \leq \Gamma$.

Equational Theory of System F

- Untyped equality is induced by the rewrite rules:

$$
\begin{array}{rcll}
(\lambda x\!:\!A.\, t)\, s & \longrightarrow_{\beta\eta} & t[s/x] & \\
\lambda x\!:\!A.\, t\, x & \longrightarrow_{\beta\eta} & t & \text{if } x \not\in \mathsf{FV}(t) \\
(\Lambda X t)\, A & \longrightarrow_{\beta\eta} & t[A/X] & \\
\Lambda X.\, t\, X & \longrightarrow_{\beta\eta} & t & \text{if } X \not\in \mathsf{FV}(t)
\end{array}
$$

Long normal forms

- Two mutual judgements:

$\Gamma \vdash t \Uparrow A$	t is a long normal form of type A
$\Gamma \vdash t \Downarrow A$	t is a neutral long normal form of type A

- Rules:

$$\frac{}{\Gamma \vdash x \Downarrow \Gamma(x)} \qquad \frac{\Gamma \vdash r \Downarrow A \to B \qquad \Gamma \vdash s \Uparrow A}{\Gamma \vdash r\, s \Downarrow B} \qquad \frac{\Gamma \vdash r \Downarrow \forall XA}{\Gamma \vdash rB \Downarrow A[B/X]}$$

$$\frac{\Gamma \vdash r \Downarrow X}{\Gamma \vdash r \Uparrow X} \qquad \frac{\Gamma, x{:}A \vdash t \Uparrow B}{\Gamma \vdash \lambda x{:}A.\, t \Uparrow A \to B} \qquad \frac{\Gamma \vdash t \Uparrow A}{\Gamma \vdash \Lambda X t \Uparrow \forall XA}\ X \notin \mathsf{FV}(\Gamma)$$

Kripke relations

- Consider a set D with application $\_ \cdot \_ : \mathsf{D} \times (\mathsf{D} \cup \mathsf{Ty}) \to \mathsf{D}$.
- Consider another such applicative structure D'.
- We interpret types as relations $\mathcal{A} \subseteq \mathsf{Cxt} \times \mathsf{D} \times \mathsf{D}'$.
- We write $\Gamma \vdash d \sim d' \in \mathcal{A}$ for $(\Gamma, d, d') \in \mathcal{A}$.
- $\mathcal{A}$ is *Kripke* if $\Gamma' \leq \Gamma \vdash d \sim d' \in \mathcal{A}$ implies $\Gamma \vdash d \sim d' \in \mathcal{A}$.
- $\mathcal{A}$ is a *Kripke PER* if $\Gamma \vdash \_ \sim \_ \in \mathcal{A}$ is symmetric and transitive.

A specific Kripke PER

- Let $\mathsf{D} = \mathsf{D}' = \mathsf{Tm}/{=_{\beta\eta}}$. Let $\bar{r}$ denote the $\beta\eta$-equivalence class of r.
- For each type A, define two Kripke PERs $\underline{A} \subseteq \overline{A}$.

$$\Gamma \vdash d \sim d' \in \overline{A} \iff \text{exists } r \text{ with } d = d' = \bar{r} \text{ and } \Gamma \vdash r \Uparrow A,$$
$$\Gamma \vdash d \sim d' \in \underline{A} \iff \text{exists } r \text{ with } d = d' = \bar{r} \text{ and } \Gamma \vdash r \Downarrow A.$$

- We have weak $\beta\eta$-normalization if $\Gamma \vdash t : A$ implies $\Gamma \vdash \bar{t} \sim \bar{t} \in \overline{A}$.
- Proof outline: Define type interpretation $\underline{A} \subseteq [\![A]\!] \subseteq \overline{A}$ and prove the fundamental theorem $\Gamma \vdash [\![t]\!] \sim [\![t]\!] \in [\![A]\!]$.

Interpretation space

- Constructions on Kripke relations:

$$
\begin{array}{lcl}
\mathcal{A} \to \mathcal{B} & = & \{(\Gamma, f, f') \mid \text{ for all } d, d', \Gamma' \leq \Gamma, \Gamma' \vdash d \sim d' \in \mathcal{A} \\
 & & \qquad \qquad \text{holds } \Gamma' \vdash f \cdot d \sim f' \cdot d' \in \mathcal{B}\} \\
A.\mathcal{B} & = & \{(\Gamma, d, d') \mid \Gamma \vdash d \cdot A \sim d' \cdot A \in \mathcal{B}\}
\end{array}
$$

- $\underline{A}, \overline{A}$ form an *interpretation space* fulfilling the conditions

$$
\begin{array}{lcll}
\underline{A \to B} & \subseteq & \overline{A} \to \underline{B} & \\
\underline{A} \to \overline{B} & \subseteq & \overline{A \to B} & \\
\underline{\forall Y A} & \subseteq & B.\underline{A[B/Y]} & \text{for any } B \\
X.\overline{A[X/Y]} & \subseteq & \overline{\forall Y A} & \text{for a new } X
\end{array}
$$

- We write $A \Vdash \mathcal{A}$ (pronounced A *realizes* $\mathcal{A}$) if $\underline{A} \subseteq \mathcal{A} \subseteq \overline{A}$.

Type interpretation

- We interpret quantification by an intersection which is indexed only by the *realizable* semantic types.

$$
\begin{array}{rcl}
[\![X]\!]_\rho & = & \rho(X) \\
[\![A \to B]\!]_\rho & = & [\![A]\!]_\rho \to [\![B]\!]_\rho \\
[\![\forall X A]\!]_\rho & = & \bigcap_{B \Vdash \mathcal{B}} B.[\![A]\!]_{\rho[X \mapsto \mathcal{B}]}
\end{array}
$$

- Types realize their interpretation: If $\sigma(X) \Vdash \rho(X)$ for all X, then $A\sigma \Vdash [\![A]\!]_\rho$.
- Proof: Induction on A, using the closure conditions of the interpretation space.

Syntactical combinatory algebras

- We assume an evaluation function $(\!|-|\!)_\eta \in \mathsf{Tm} \to \mathsf{D}$, satisfying

$$
\begin{array}{rcll}
(\!|x|\!)_\eta & = & \eta(x) & \\
(\!|r\,s|\!)_\eta & = & (\!|r|\!)_\eta \cdot (\!|s|\!)_\eta & \\
(\!|r\,A|\!)_\eta & = & (\!|r|\!)_\eta \cdot A\eta & \\
(\!|\lambda x\!:\!A.\,t|\!)_\eta \cdot d & = & (\!|t|\!)_{\eta[x\mapsto d]} & \\
(\!|\Lambda X t|\!)_\eta \cdot A & = & (\!|t|\!)_{\eta[X\mapsto A]} & \\
(\!|t[s/x]|\!)_\eta & = & (\!|t|\!)_{\eta[x\mapsto (\!|s|\!)_\eta]} & \\
(\!|t[A/x]|\!)_\eta & = & (\!|t|\!)_{\eta[x\mapsto A\eta]} & \\
(\!|t|\!)_\eta & = & (\!|t|\!)_{\eta'} & \text{if } \eta(x) = \eta'(x) \text{ for all } x \in \mathsf{FV}(t)
\end{array}
$$

- The last three equations do not hold for all applicative structures, e.g., not for explicit substitution calculi with trivial equality.

Fundamental theorem

Theorem (Validity of typing)

Let $\eta \Vdash \rho$ *and both* $\eta \restriction \mathsf{TyVar} = \eta' \restriction \mathsf{TyVar}$ *and* $\Delta \vdash \eta \sim \eta' \in [\![\Gamma]\!]_\rho$*. If* $\Gamma \vdash t : A$ *then* $\Delta \vdash (\!|t|\!)_\eta \sim (\!|t|\!)_{\eta'} \in [\![A]\!]_\rho$*.*

Corollary (Weak $\beta\eta$-normalization of System F)

If $\Gamma \vdash t : A$ *then* t β*-reduces* η*-expands to a long normal form* t'*.*

Proof.

Clearly, $A \Vdash [\![A]\!]$. By the theorem, $\Gamma \vdash (\!|t|\!) \sim (\!|t|\!) \in [\![A]\!]$, meaning $t =_{\beta\eta} t'$ with $\Gamma \vdash t' \Uparrow A$. We conclude by Church-Rosser for β-reduction η-expansion. □

NbE for System F

- The typed equational theory of System F is induced by

$$\frac{\Gamma, x\!:\!A \vdash t : B \qquad \Gamma \vdash s : A}{\Gamma \vdash (\lambda x\!:\!A.\, t)\, s = t[s/x] : B}$$

$$\frac{\Gamma \vdash t : A \to B}{\Gamma \vdash \lambda x\!:\!A.\, t\, x = t : A \to B}\; x \notin \mathsf{FV}(t)$$

$$\frac{\Gamma \vdash t : A \qquad X \notin \mathsf{FV}(\Gamma)}{\Gamma \vdash (\Lambda X t)\, B = t[B/X] : A[B/X]}$$

$$\frac{\Gamma \vdash t : \forall X A}{\Gamma \vdash \Lambda X.\, t\, X = t : \forall X A}\; X \notin \mathsf{FV}(t)$$

- Task: find function $\mathsf{nf}(\Gamma \vdash t\!:\!A)$ which is
  1. complete, i. e., $\Gamma \vdash t = t' : A$ implies $\mathsf{nf}(\Gamma \vdash t\!:\!A) \equiv \mathsf{nf}(\Gamma \vdash t'\!:\!A)$, and
  2. sound, i. e., if $\Gamma \vdash t : A$ then $\Gamma \vdash t =_{\beta\eta} \mathsf{nf}(\Gamma \vdash t\!:\!A) : A$.

Evaluation

- As combinatory algebra, use Scott domain

$$\mathsf{D} = (\mathsf{Var} \times (\mathsf{D} \cup \mathsf{Ty})^{<\omega}) \oplus [\mathsf{D} \to \mathsf{D}] \oplus (\mathsf{Ty} \to \mathsf{D}).$$

- Three types of values:
  1. neutral objects $e ::= x \mid e\,d \mid e\,A$.
  2. continuous functions $f \in [\mathsf{D} \to \mathsf{D}]$
  3. functions $F \in \mathsf{Ty} \to \mathsf{D}$ from types to values
- Application of values defined obviously.
- Evaluation of abstractions is defined by

$$\begin{array}{rcl} (\!|\lambda x : A.\, t|\!)_\eta(d) & = & (\!|t|\!)_{\eta[x \mapsto d]} \\ (\!|\Lambda X t|\!)_\eta(A) & = & (\!|t|\!)_{\eta[X \mapsto A]}. \end{array}$$

Contextual reification

- We can read back values as terms; this is called reification.

$$\begin{array}{ll} \Gamma \vdash d \searrow t \Uparrow A & \quad d \text{ reifies to } t \text{ at type } A, \\ \Gamma \vdash d \searrow t \Downarrow A & \quad d \text{ reifies to } t \text{, inferring type } A. \end{array}$$

- Rules:

$$\frac{}{\Gamma \vdash x \searrow x \Downarrow \Gamma(x)} \qquad \frac{\Gamma \vdash e \searrow r \Downarrow A \to B \qquad \Gamma \vdash d \searrow s \Uparrow A}{\Gamma \vdash e\,d \searrow r\,s \Downarrow B}$$

$$\frac{\Gamma \vdash e \searrow r \Downarrow \forall X A}{\Gamma \vdash e\,B \searrow r\,B \Downarrow A[B/X]} \qquad \frac{\Gamma \vdash e \searrow r \Downarrow X}{\Gamma \vdash e \searrow r \Uparrow X}$$

$$\frac{\Gamma, x{:}A \vdash f \cdot x \searrow t \Uparrow B}{\Gamma \vdash f \searrow \lambda x{:}A.\, t \Uparrow A \to B} \qquad \frac{\Gamma \vdash F \cdot X \searrow t \Uparrow A}{\Gamma \vdash F \searrow \Lambda X t \Uparrow \forall X A}$$

Completeness of NbE

- $\mathrm{nf}(\Gamma \vdash t : A)$ returns the reification of the evaluation of t, i. e., the t' such that $\Gamma \vdash (\!|t|\!) \searrow t' \Uparrow A$.
- Let an interpretation space be defined by

$$\begin{array}{lcl} \Gamma \vdash d \sim d' \in \overline{A} & \iff & \text{exists } t \text{ with } \Gamma \vdash d, d' \searrow t \Uparrow A, \\ \Gamma \vdash d \sim d' \in \underline{A} & \iff & \text{exists } t \text{ with } \Gamma \vdash d, d' \searrow t \Downarrow A. \end{array}$$

Theorem (Completeness of NbE)

If $\Gamma \vdash t = t' : A$ then $\Gamma \vdash (\!|t|\!) \searrow r \Uparrow A$ and $\Gamma \vdash (\!|t'|\!) \searrow r \Uparrow A$ for some long normal form r.

Soundness of NbE

- Soundness wrt. untyped equality is obtained via setting

$$\begin{array}{lcl} \Gamma \vdash d \sim \bar{t} \in \overline{A} & \iff & \text{exists } t' \text{ with } \Gamma \vdash d \searrow t' \Uparrow A \text{ and } t =_{\beta\eta} t', \\ \Gamma \vdash d \sim \bar{t} \in \underline{A} & \iff & \text{exists } t' \text{ with } \Gamma \vdash d \searrow t' \Downarrow A \text{ and } t =_{\beta\eta} t'. \end{array}$$

- The fundamental theorem implies: If $\Gamma \vdash t : A$ then $\Gamma \vdash (\!|t|\!)_{\eta_{\mathsf{id}}} \searrow t' \Uparrow A$ and $t =_{\beta\eta} t'$.
- What about soundness wrt. judgmental equality?
- Welltyped terms modulo judgmental equality are not a combinatory algebra D.
- Hence, we need a new version of the fundamental theorem.

Kripke logical relations

- Kripke logical relations between syntax and semantics $\mathcal{S} \subseteq \mathsf{Cxt} \times \mathsf{Tm} \times \mathsf{Ty} \times \mathsf{D}$ satisfy for all $(\Gamma, t, A, d) \in \mathcal{S}$:
  1. $\Gamma \vdash t : A$,
  2. $\Gamma' \leq \Gamma$ implies $(\Gamma', t, A, d) \in \mathcal{S}$, and
  3. $\Gamma \vdash t = t' : A$ implies $(\Gamma, t', A, d) \in \mathcal{S}$.
- Redo the whole development: semantic function space, interpretation space, realizability, semantic quantification, fundamental theorem.

Conclusions

- NbE for System F with conventional means.
- Follows the structure of a weak normalization proof.
- Further work:
  - Find an abstraction of semantics that works for both completeness and soundness of NbE.
  - Scale to F^{ω}.
  - Scale to the Calculus of Constructions.
- Acknowledgments: This work was carried out during a visit to Frédéric Blanqui and Cody Roux at LORIA, Nancy, France, financed by the *Bayrisch-Französisches Hochschulzentrum*.

Bibliography

- Andreas Abel, Thierry Coquand, and Peter Dybjer.
  Normalization by evaluation for Martin-Löf Type Theory with typed equality judgements.
  In *Logic in Computer Science (LICS 2007)*.
- Andreas Abel, Thierry Coquand, and Peter Dybjer.
  Verifying a semantic $\beta\eta$-conversion test for Martin-Löf type theory.
  In *Mathematics of Program Construction, MPC'08*.
- Thorsten Altenkirch, Martin Hofmann, and Thomas Streicher.
  Reduction-free normalisation for a polymorphic system.
  In *Logic in Computer Science (LICS'96)*.
- Ulrich Berger and Helmut Schwichtenberg.
  An inverse to the evaluation functional for typed λ-calculus.
  In *Logic in Computer Science (LICS'91)*.