Slide 1

Weak Normalization for the Simply-Typed Lambda-Calculus in Twelf

Andreas Abel

ProgLog, Chalmers
Göteborg, Sweden
June 9, 2004

Work supported by: GKLI (DFG), TYPES & APPSEM-II (EU), CoVer (SFF)

Slide 2

Twelf

- Logical framework based on the Edinburgh LF (dependently-typed λ-calculus)
- Propositions-as-types, derivations-as-objects
- Higher-order abstract syntax
- Terms: abstraction, application, user-def. constants
- Terms considered upto $\beta\eta$-equality
- No user-def. reduction rules: all functions parametric
- Types: dependent function, user-def. type family constants
- Logic programming through proof search

Simply Typed λ-Calculus (STL)

Slide 3

- Syntax.

$$
\begin{array}{lcll}
r, s, t, u & ::= & x \mid \lambda x.t \mid r\, s & \text{untyped terms} \\
A, B, C & ::= & * \mid A \to B & \text{simple types} \\
\Gamma & ::= & \diamond \mid \Gamma,\, x\!:\!A & \text{contexts}
\end{array}
$$

- Type assignment $\Gamma \vdash t : A$.

$$\frac{(x\!:\!A) \in \Gamma}{\Gamma \vdash x : A}\ \texttt{of\_var}$$

$$\frac{\Gamma,\, x\!:\!A \vdash t : B}{\Gamma \vdash \lambda x.t : A \to B}\ \texttt{of\_lam} \qquad \frac{\Gamma \vdash r : A \to B \qquad \Gamma \vdash s : A}{\Gamma \vdash r\, s : B}\ \texttt{of\_app}$$

- Weak head reduction $t \longrightarrow_{\mathsf{w}} t'$.

$$\frac{}{(\lambda x.t)\, s \longrightarrow_{\mathsf{w}} [s/x]t}\ \texttt{beta} \qquad \frac{r \longrightarrow_{\mathsf{w}} r'}{r\, s \longrightarrow_{\mathsf{w}} r'\, s}\ \texttt{appl}$$

Representation of Syntactic Objects in Twelf

Slide 4

- Representation of simple types.

```
ty      : type.
*       : ty.
=>      : ty -> ty -> ty.
```

- Representation of λ-terms.

```
tm      : type.
lam     : (tm -> tm) -> tm.
app     : tm -> tm -> tm.
```

- HOAS = represent object variables by framework variables.

```
twice = lam [f:tm] lam [x:tm] app f (app f x).
```

Slide 5

Representation of Judgements without Hypotheses

Slide 6

- Representation of weak head reduction.

```
-->w  : tm -> tm -> type.

beta  : app (lam T) S -->w T S.
appl  : R -->w R' -> app R S -->w app R' S.
```

- Substitution in object theory is application of the framework.

Representation of Judgements with Hypotheses

Slide 7

- Representation of typing relation: Think in natural deduction trees.

$$\dfrac{\begin{array}{c}\overline{A}^{\,x}\\ \vdots \\ B\end{array}}{A \to B}\ \texttt{of\_lam} \qquad\qquad \dfrac{A \to B \qquad A}{B}\ \texttt{of\_app}$$

- Typing assumption is represented as hypothetical judgement.

```
of     : tm -> ty -> type.
of_lam : ({x:tm} x of A -> (T x) of B)
            -> (lam [x:tm] T x) of (A => B).
of_app : R of (A => B) -> S of A -> (app R S) of B.
```

Weak Head Reduction is Closed under Substitution

Slide 8

- Lemma: If $t \longrightarrow_{\mathsf{w}} t'$ then $[u/y]t \longrightarrow_{\mathsf{w}} [u/y]t'$.
- Proof: By induction on the derivation of $t \longrightarrow_{\mathsf{w}} t'$.
  - Case $(\lambda x.t)\, s \longrightarrow_{\mathsf{w}} [s/x]t$. W.l.o.g. $x \neq y$ and x not free in u. Then,

$$\begin{array}{rcl} [u/y]((\lambda x.t)\, s) & = & (\lambda x.[u/y]t)\ [u/y]s \\ & \longrightarrow_{\mathsf{w}} & [[u/y]s/x][u/y]t \quad = \quad [u/y][s/x]t. \end{array}$$

  - Case $r\, s \longrightarrow_{\mathsf{w}} r'\, s$ with $r \longrightarrow_{\mathsf{w}} r'$. By ind. hyp., $[u/y]r \longrightarrow_{\mathsf{w}} [u/y]r'$. Hence,

$$\begin{array}{rcl} [u/y](r\, s) & = & ([u/y]r)\ ([u/y]s) \\ & \longrightarrow_{\mathsf{w}} & ([u/y]r')\ ([u/y]s) \quad = \quad [u/y](r'\, s) \end{array}$$

$\square$

Representation of Theorems and Proofs

Slide 9

- A theorem is represented as a functional relation.

```
subst_red : {U:tm} ({y:tm} T y -->w T' y)
                        -> T U -->w T' U -> type.
%mode subst_red +U +P -P'.
```

- Its proof is represented as a logic program which implements the relation.

```
subst_red_beta: subst_red U ([y] beta) beta.
subst_red_appl: subst_red U ([y] appl (P y)) (appl P')
                <- subst_red U P P'.
%terminates P (subst_red _ P _).
```

- Function must be total to represent a valid proof.
- This requires *termination* and *coverage* of all possible inputs.

Slide 10

A Formalized Proof of Weak Normalization for the STL

Slide 11

- Structure of a normalization proof:
  1. Define a relation $t \Downarrow A$ which is closed under application.
  2. Show: If $t : A$ then $t \Downarrow A$.
  3. Show: If $t \Downarrow A$ then t is normalizing.
- Tait and crowd: $t \Downarrow A$ is a *logical relation* (semantical).
- Joachimski and Matthes (2004): $t \Downarrow A$ is a *finitary inductive definition*.
- Forerunners: Goguen (1995), van Raamsdonk and Severi (1995).

Inductive Characterization of Weakly Normalizing Terms

Slide 12

- "De-vectorized" version of Joachimski and Matthes (2004)
- $\Gamma \vdash t \Downarrow A$: *t is weakly normalizing of type A*.
- $\Gamma \vdash t \downarrow^x A$: *t is wn and neutral of type A*.
- Rules:

$$\frac{(x : A) \in \Gamma}{\Gamma \vdash x \downarrow^x A} \qquad \frac{\Gamma \vdash r \downarrow^x A \to B \qquad \Gamma \vdash s \Downarrow A}{\Gamma \vdash r\, s \downarrow^x B}\ \texttt{wne\_app}$$

$$\frac{\Gamma \vdash r \downarrow^x A}{\Gamma \vdash r \Downarrow A}\ \texttt{wn\_ne}$$

$$\frac{\Gamma, x : A \vdash t \Downarrow B}{\Gamma \vdash \lambda x.t \Downarrow A \to B}\ \texttt{wn\_lam} \qquad \frac{r \longrightarrow_{\mathsf{w}} r' \qquad \Gamma \vdash r' \Downarrow A}{\Gamma \vdash r \Downarrow A}\ \texttt{wn\_exp}$$

Difficult: Closure under Application

- Lemma: Let $\mathcal{D} :: \Gamma \vdash s \Downarrow A$.

1. If $\mathcal{E} :: \Gamma \vdash r \Downarrow A \to C$ then $\Gamma \vdash r\, s \Downarrow C$.
2. If $\mathcal{E} :: \Gamma, x{:}A \vdash t \Downarrow C$, then $\Gamma \vdash [s/x]t \Downarrow C$.
3. If $\mathcal{E} :: \Gamma, x{:}A \vdash t \downarrow^x C$, then $\Gamma \vdash [s/x]t \Downarrow C$
   and C is a subexpression of A.
4. If $\mathcal{E} :: \Gamma, x{:}A \vdash t \downarrow^y C$ with $x \neq y$, then $\Gamma \vdash [s/x]t \downarrow^y C$.

Slide 13

- Proof: Simultaneously by main induction on type A (for part 3) and side induction on the derivation $\mathcal{E}$.
- Similar to Girard, Lafont and Taylor (1989): Lexicographic induction on highest degree (=type) of a redex and the number of redexes of highest degree.

Closure under Application and Substitution in Twelf

- Representation of lemma as 4 type families.
- "C is a subexpression of A" expressed by `%reduces C <= A`.
- Mutual lexicographic termination order.

Slide 14

Soundness of Inductive Characterization

- Simple induction: $t \Downarrow A$ for every typed term $t : A$.
- Lemma (Soundness): If $t \Downarrow A$ then $t \longrightarrow^* v$ for some v.
- Requires characterization of valued and properties of reduction.
- Technical, but well understood. $\square$

Slide 15

Tait-Style Proofs in Twelf?

- Heart of Tait's proof is the rule:

$$\frac{\forall s.\ \ s \Downarrow A \ \Rightarrow \ r\, s \Downarrow B}{r \Downarrow A \rightarrow B}$$

- Literal encoding in Twelf...

Slide 16

```
({S:tm} wn S A -> wn (app R S) B) -> wn R (A => B).
```

- ... means something else:

  if for a fresh term `S` for which we assume `wn S A` it holds that `wn (app R S) B`, then `wn R (A => B)`.

- Problem: Tait's infinitary premise is not expressible.

Strong Normalization in Twelf?

Slide 17

- Classical definition of *strongly normalizing*: no infinite reduction sequences.
- No good in a constructive setting.
- Inductive definition of *strongly normalizing*: wellfounded part of reduction relation.

$$\frac{\forall t'.\ t \longrightarrow t' \Rightarrow \mathsf{sn}\, t'}{\mathsf{sn}\, t},$$

- Suffers likewise from an infinitary premise.

Conclusion

Slide 18

- Normalization for a proof-theoretically weak object theory directly implementable in Twelf.
- Limits for normalization proofs: expressiveness of Twelf, termination checker.
- Conjecture 1: Infinitary premises not expressible in Twelf.
- Conjecture 2: Strong normalization not expressible in Twelf.
- Conjecture 3: Proof-theoretical strength of Twelf bounded by arithmetic.

Related Work

Slide 19

- Altenkirch (1993): SN for System F in LEGO.
- Filinski in 1990s: Feasibility of logical relations in Twelf. Not published.
- Berghofer and Nipkow: Joachimski and Matthes' proof in Isabelle.
- Watkins and Crary: Normalization for Concurrent LF in Twelf.