Typed Operational Semantics for Intensional Dependent Record Types

Dr. Yangyue FENG

Royal Holloway, University of London
Egham Hill, Egham, Surrey TW20 0EX, UK
yangyue.feng@cs.rhul.ac.uk

Institut für Informatik,
Ludwig-Maximilians-Universität München,
25 November 2011

Outline

Overview

- My PhD is on proving metatheories of dependent record types with a typed operational semantics (TOS);
- Our system – sketch:
  - We have introduced intensional dependent record types (IDRT), and built a typed operational semantics (TOS_{DRT}) for it, following Goguen's method in his PhD thesis (TOS for UTT and LF);
  - Completeness and Soundness of TOS_{DRT} to IDRT are proved;
  - Adequacy of TOS_{DRT} over untyped reductions, as well as Determinacy (unique normal form) are proved.
- Strong Normalization of the DRTs is proved from Soundness Theorem and Adequacy Lemma; as well as Church-Rosser property and Subject Reduction, etc.
- In extra, with Church-Rosser property, we proved a set of coercions added into IDRT to be coherent, which allows coercive subtyping in IDRTs.

IDRT

- Dependent record types are types of records in which the type of a field may depend on the value of an earlier field :

$$\textit{Dependent record types} \quad R := \langle\, l_1 : A_1,\ l_2 : A_2,\ \ldots\ l_n : A_n \,\rangle$$

where A_j may depend on A_i $(0 \leq i < j \leq n)$.

LF

- The Logical Framework [Luo94] (LF) is the typed version of Martin-Löf's logical framework [NPS90].
- it's a type system (types in LF are called kinds) and a meta-language to specify object type theories, such as UTT, LTTs.
- the syntactical entities :

$$\begin{array}{lcll} \textit{Contexts} & C & ::= & () \mid \Gamma, x : A \\ \textit{LF Kinds} & K & ::= & \textit{Type} \mid \textit{El}(A) \mid (x : K)K' \\ \textit{LF Terms} & M & ::= & x \mid [x : K]M \mid M(M') \end{array}$$

- *Type* is the kind representing the collection of all types (A is a type if $A : \textit{Type}$), $\textit{El}(A)$ is the kind of objects of type A, $(x : K)K'$ is the kind of dependent functions.

- We extend the Logical Framework LF [Luo94] with :

$$\begin{array}{rcl} \textit{Record Types } R & ::= & \langle\rangle \mid \langle R,\ l\colon A\rangle\ (\textit{Labels } l \in \mathcal{L}) \\ \textit{Records } r & ::= & \langle\rangle \mid \langle r, l = a\colon A\rangle \mid [r] \mid r.l \end{array}$$

- where [ ] and $.l$ are two operations over records, called restriction and field-selection
- We also have two kinds which collects the record types : *RType* (is actually $\textit{RType}[\mathcal{L}]$) and $\textit{RType}[L]$ (that collects record types with top level labels in L), they are in the kind level of LF
- every record type is a LF type.
- the inference rules of IDRT are given in [Y. FENG 2011]
- Important: weakly extensional equality rules for the dependent records are not included, thus the system is intensional.

TOS – Introduction

- Approach :
  - A type system – A Typed Op. Semantics – prove something on the type system (metatheory, e.g., SN, C-R, subject reduction)
- Healf Goguen's work :
  - (1994) Using TOS to prove metatheory of UTT (a type theory described with Logical Framework LF)
  - (1999) Using TOS with a simpler syntax to prove metatheory of LF
- We have followed Goguen's approach to prove the metatheory for dependent record types.

TOS Syntax

- For a type theory, its typed operational semantics captures its computational behaviour, usually given by its (untyped) reduction relation.
- Judgements in the TOS :

$$\models M \to N \to P : A$$

which informally asserts that, N and P are the weak-head normal form and the normal form of the term M.

Basic forms :

$$\models \Gamma \to \Delta$$

$$\Gamma \models A \to B$$

$$\Gamma \models M \to N \to P : A$$

Abbreviated forms :

$$\Gamma \models ok$$

$$\Gamma \models M \to_w N : A$$

$$\Gamma \models M \to_n P : A$$

$$\Gamma \models M : A$$

informal meaning of judgements in TOS.

Untyped reduction

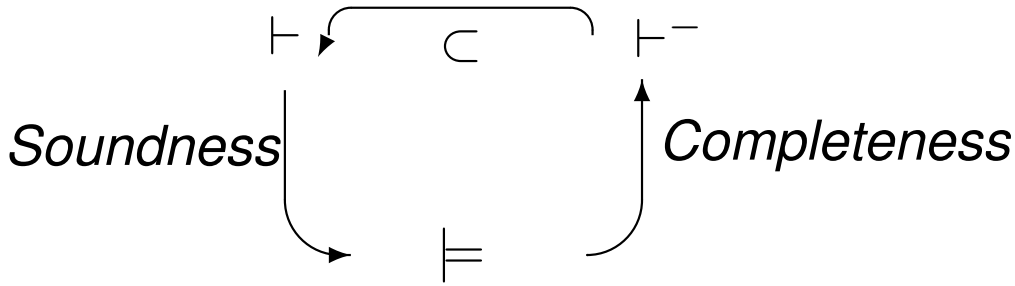
$$
\begin{array}{rll}
(\beta) & ([x : A]M)N \to_{\beta} [N/x]M & \\
(\eta) & [x : A]M(x) \to_{\eta} M & (x \notin FV(M)) \\
(\mathit{restriction}) & [\langle r, l = a\colon A\rangle] \to_{\mathit{RESTR}} r & \\
(\mathit{field} - \mathit{selection}) & \langle r, l = a\colon A\rangle.l \to_{\mathit{FLDSEL}} a & \\
(\mathit{diff}.\ \mathit{field} - \mathit{sele}.) & \langle r, l = a\colon A\rangle.l' \to_{\mathit{FLDSL'}} r.l' & (l \neq l')
\end{array}
$$

TOS_{DRT}

- We have set up a TOS for the IDRT
- Explanantion.
  - Turn proving things concerning "$\vdash$" to those concerning "$\models$"
  - prove "$\vdash \approx \models$" i.e. soundness and completeness
  - prove metatheories in "$\models$" and then we got those for "$\vdash$" from soundness

Key Features of the TOS_{DRT}

- Completeness and Soundness Theorems
  - the proofs of these theorems



- Adequacy Lemma and Determinacy Lemma

Adequacy Lemma

Lemma (Adequacy of TOS for Untyped Reduction)

(1) If $\Gamma \models A \to C$ *then there exists* B *such that* $A \to^*_{\beta R} B \to^*_{\eta} C$;
(2) If $\Gamma \models M \to N \to P : A$, *then there exists* N' *such that* $M \to^*_{\beta R} N \to^*_{\beta R} N' \to^*_{\eta} P$.

Lemma (Adequacy for Normal Forms and WHNFs)

(1) If $\models \Gamma \to \Delta$ *then* Δ *is normal;*
(2) If $\Gamma \models A \to B$ *then* B *is normal;*
(3) If $\Gamma \models M \to N \to P : A$ *then* N *is weak-head normal and* P *and* A *are normal.*

Determinacy

Lemma (Determinacy (Unique Normal Form))

(1) If $\models \Gamma \to \Delta$, $\models \Gamma \to \Phi$, *then* $\Delta \equiv \Phi$;
(2) If $\Gamma \models A \to B$, $\Gamma \models A \to C$, *then* $B \equiv C$;
(3) If $\Gamma \models M \to N \to P : B$, $\Gamma \models M \to Q \to R : C$, *then* $N \equiv Q$, $P \equiv R$, $B \equiv C$.

Lemma (Completeness of TOS w.r.t IDRT)

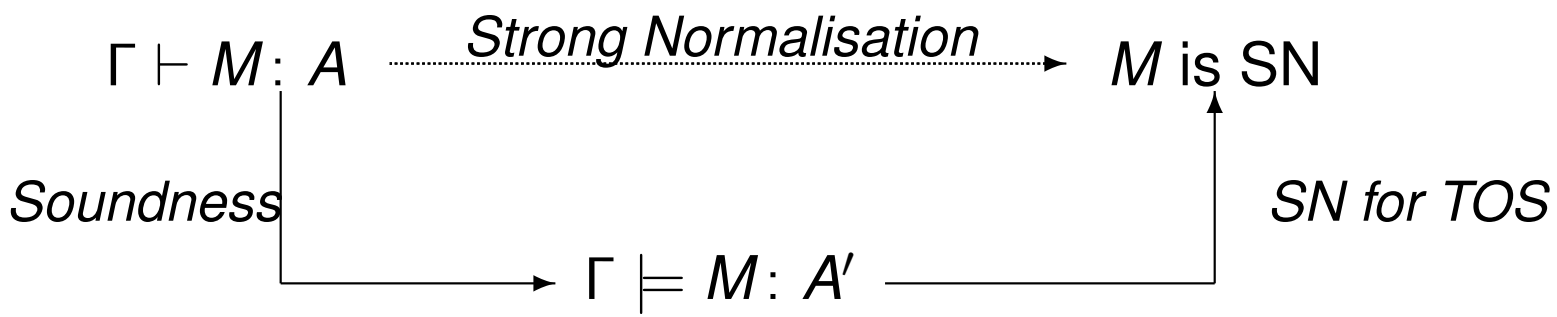
- *If* $\Gamma \models$ *ok then* $\vdash \Gamma$ *valid.*
- *If* $\Gamma \models A \to B$ *then* $\Gamma \vdash A$ *kind and* $\Gamma \vdash A = B$.
- *If* $\Gamma \models M \to N \to P : A$ *then* $\Gamma \vdash M : A$, $\Gamma \vdash M = N : A$, $\Gamma \vdash M = P : A$ *and* $\Gamma \vdash A = A$.

Lemma (Soundness of TOS w.r.t. IDRT)

- *If* $\Gamma \vdash$ *ok, then there exists* Δ *such that* $\models \Gamma \to \Delta$.
- *If* $\Gamma \vdash A$ *kind, then there exists* B *such that* $\Gamma \models A \to B$.
- *If* $\Gamma \vdash A = B$ *then there exists* C *such that* $\Gamma \models A \to C$ *and* $\Gamma \models B \to C$.
- *If* $\Gamma \vdash M : A$ *then there exist* P, B *such that* $\Gamma \models A \to B$ *and* $\Gamma \models M \to_n P : B$.
- *If* $\Gamma \vdash M = N : A$, *then there exist* P, B *such that* $\Gamma \models A \to B$, *and* $\Gamma \models M \to_n P : B$, $\Gamma \models N \to_n P : B$.

Metatheory proven with the TOS_{DRT}

- Strong normalization proven w.r.t. the TOS (the SN Theorem of TOS_{DRT})
- Transfer this property to IDRT due to Soundness



See my paper [Y FENG, Z. LUO in Types 09 postproceeding, 2011].

Lemma (Strong Normalisation of TOS)

1. *If* $\Gamma \models A \to B$ *then* A *is strongly normalisable.*
2. *If* $\Gamma \models M \to N \to P : A$ *then* M *is strongly normalisable.*

proved with Parallel Reduction $\Rightarrow$ and Parallel Subject Reduction Lemma.

Metatheory for IDRT

- Main Goal Achieved: Strong normalization of IDRT;
  - By Soundness and the SN Theorem of TOS_{DRT}
- Church-Rosser Theorem, Subject Reduction, Type Unicity, Kind Correctness are proved.
- all these theorems are presented in the thesis. [Y. FENG 2011]

Lemma (Subject Reduction for IDRT)

If $\Gamma \vdash M : A$ *and* $M \to N$, *then* $\Gamma \vdash N : A$.

Lemma (Strong Normalisation for IDRT)

1. *If* Γ *valid, then* Γ *is strongly normalisable.*
2. *If* $\Gamma \vdash A$ *kind, then* A *is strongly normalisable.*
3. *If* $\Gamma \vdash A = B$, *then both* A *and* B *are strongly normalisable to some* C.
4. *If* $\Gamma \vdash M : A$, *then* M *and* A *are strongly normalisable and* $P : B$, *where* P *and* B *are the normal forms of* M *and* A, *respectively.*
5. *If* $\Gamma \vdash M = N : A$, *then both* M *and* N *are strongly normalisable to some* P, A *is strongly normalisable to some* B *such that* $P : B$.

Lemma (Church-Rosser for IDRT)

If $\Gamma \vdash M = N : A$, *then* $M \to^* P$ *and* $N \to^* P$ *for some* P.

Coherence of A Coercive Set

- Coercive Subtyping
  - Example:

$$\frac{f : List(B) \to D \quad nil(A) : List(A) \quad List(A) \leq_{map(c)} List(B)}{f(nil(A)) = f(map(c)(nil(A))) : D}$$

    where $map(c)$ coerces the canonical object $nil(A)$ to $nil(B)$ which is a canonical object of $List(B)$
- Structural subtyping for DRTs
  - $IDRT[R]$: DRTs extended with the set $\mathcal{R}$ of coercions $\{(\xi), (d^i_R)\}_{i=1,2,3}$
  - Coherence of $\mathcal{R}$ proven
- More applications : Intensional Manifest Fields (IMFs), DRTs modelling module mechanism.

Spotlights, future work, discussion

- The compatible relation of LF and DRTs
- The removal of η rules of DRTs ("IDRT" instead of "DRT")
- Why TOS has worked for proving metatheory
- Future work using the methodology of TOS – or formalizing the proof in some Theorem-prover ?
- Future work using our DRTs

Thank You !