Realisability Semantics for Intersection Types and Expansion Variables

Fairouz Kamareddine, Karim Nour, Vincent Rahli and J. B. Wells

25 March 2008
Expansion Mechanism - Example

- **Expansion**: invented for calculating principal typings for \( \lambda \)-terms in type systems with intersection types.

- **Expansion variables** (E-variables): invented to simplify and help mechanise expansion.

- Let \( M = \lambda x.x(\lambda y. yz) \)

- \( M \) can be assigned the typings:
  - \( \Phi_1 = \langle (z : a) \vdash (((a \rightarrow b) \rightarrow b) \rightarrow c) \rightarrow c \rangle \) **Principal**
  - \( \Phi_2 = \langle (z : a_1 \sqcap a_2) \vdash (((a_1 \rightarrow b_1) \rightarrow b_1) \sqcap ((a_2 \rightarrow b_2) \rightarrow b_2) \rightarrow c) \rightarrow c \rangle \)

- An expansion operation can obtain \( \Phi_2 \) from \( \Phi_1 \).

- In System E, the typing \( \Phi_1 \) from above is replaced by:
  \( \Phi_3 = \langle (z : ea) \vdash (e((a \rightarrow b) \rightarrow b) \rightarrow c) \rightarrow c \rangle \),

- \( \Phi_3 \) differs from \( \Phi_1 \) by the insertion of the E-variable \( e \) at two places.

- \( \Phi_2 \) can be obtained from \( \Phi_3 \) by substituting for \( e \) the expansion term:
  \( E = (a := a_1, b := b_1) \sqcap (a := a_2, b := b_2) \).
Our goal

- Intersection types were introduced to be able to type more terms than in the Simply Typed Lambda Calculus.
- Intersection types are interpreted by set-theoretical intersection of meanings.
- Expansion variables have been introduced to give a simple formalisation of the expansion mechanism, i.e., as a syntactic object.
- We are interested in the meaning of such a syntactic object.
- What does an expansion variable applied to a type stand for?
- In the presence of expansions, how can the relation between terms and types w.r.t. a type system be described?
The challenge: the difficulties of giving a semantics for expansion variables

- Building a semantics for E-variables turns out to be challenging.
- In many kinds of semantics, the meaning of a type $T$ is calculated by an expression $[T]_\nu$ where $\nu$ is a valuation.
- To extend this idea to types with E-variables, we would need to devise some space of possible meanings for E-variables.
- Given that a type $eT$ can be turned by expansion into a new type $S_1(T) \sqcap S_2(T)$, where $S_1$ and $S_2$ are arbitrary substitutions (or expansions), the situation is complicated.
Because it is unclear how to devise a space of meanings for expansions and E-variables:

- We consider only E-variables without the operation of expansion.
- We develop a space of meanings for types that is hierarchical in the sense of having many degrees.
- We develop a realisability semantics where each use of an E-variable in a type corresponds to an independent degree at which evaluation occurs in the $\lambda$-term that is assigned the type.
- In the $\lambda$-term being evaluated, the only interaction possible between portions at different degrees is that higher degree portions can be passed around but never applied to lower degree portions.
- Due to problems supporting the $\omega$- type, we restrict attention to the $\lambda I$-calculus.
Our contributions/Outline of the talk

- Outlining the difficulties in giving a semantics for expansions and expansion variables.
- A hierarchical $\lambda I$-calculus where each variable is marked by a natural number degree.
- A realisability semantics for expansion variables which is applied to two intersection type systems.
- The soundness of the semantics for both systems and numerous examples of how our semantics works.
- Outlining why Completeness fails for the first unrestricted type system.
- Outlining why completeness fails for the second restricted type system if more than one expansion variable is used.
- Establishing the completeness for the second type system in the presence of one single expansion variable. This E-variable may be used in many places and may also occur deeply nested.
- The first denotational semantics (using realisability or any other approach) of intersection type systems with E-variables.
The $\lambda^\mathbb{N}$-Calculus

- Define $\mathcal{M}$ (terms), $\mathbb{M}$ (good terms), free variables, degrees, joinability $M \diamond N$, $\beta$-reduction and $+$ as follows:
  - If $x \in \mathcal{V}$, $n \in \mathbb{N}$, then $x^n \in \mathcal{M} \cap \mathbb{M}$, $FV(x^n) = \{x^n\}$, and $\text{deg}(x^n) = n$.
  - If $M, N \in \mathcal{M}$ such that $M \diamond N$ (see below), then
    - $(M N) \in \mathcal{M}$, $FV((M N)) = FV(M) \cup FV(N)$ and $\text{deg}((M N)) = \min(\text{deg}(M), \text{deg}(N))$ (where $\min$ is the minimum)
    - If $M \in \mathbb{M}$, $N \in \mathcal{M}$ and $\text{deg}(M) \leq \text{deg}(N)$ then $(M N) \in \mathbb{M}$.
  - If $M \in \mathcal{M}$ and $x^n \in FV(M)$, then
    - $(\lambda x^n.M) \in \mathcal{M}$, $FV((\lambda x^n.M)) = FV(M) \setminus \{x^n\}$, and $\text{deg}((\lambda x^n.M)) = \text{deg}(M)$. 
    - If $M \in \mathbb{M}$ then $\lambda x^n.M \in \mathbb{M}$.
  - $M$ and $N$ are joinable ($M \diamond N$) iff $\forall x \in \mathcal{V}$, if $x^m \in FV(M)$ and $x^n \in FV(N)$, then $m = n$.
  - $\triangleright_\beta$ on $\mathcal{M}$ is defined as the least compatible relation closed under:
    - $(\lambda x^n.M)N \triangleright_\beta M[x^n := N]$ if $\text{deg}(N) = n$.
    - $\bullet (x^n)^+ = x^{n+1}$ $\bullet (M_1 M_2)^+ = M_1^+ M_2^+$ $\bullet (\lambda x^n.M)^+ = \lambda x^{n+1}.M^+$
  - Examples (note that $\mathbb{M} \subset \mathcal{M}$ and that in $\mathbb{M}$, the degree of a function is bigger than the degree of an argument):
    - $\lambda x^1.y^0 \notin \mathcal{M}$ $\lambda x^1.x^1x^0 \notin \mathcal{M}$
    - $\lambda x^1.x^1y^3 \in \mathcal{M} \cap \mathbb{M}$ $\lambda x^1.x^1y^0 \in \mathcal{M} \setminus \mathbb{M}$
The Types

- Atomic types $a, b, c \in \mathcal{A}$, expansion variables $e \in \mathcal{E}$.
- In $\mathcal{T} ::= \mathcal{A} | \mathcal{T} \rightarrow \mathcal{T} | \mathcal{T} \sqcap \mathcal{T} | \mathcal{E}\mathcal{T}$, no restrictions on the arrow.
- $\mathcal{U} ::= \mathcal{U} \sqcap \mathcal{U} | \mathcal{E}\mathcal{U} | \mathcal{T}$ where $\mathcal{T} ::= \mathcal{A} | \mathcal{U} \rightarrow \mathcal{T}$. Here $\mathcal{U}$ does not allow arrows to occur to the left of intersections or expansions.
- $\mathcal{T} \subseteq \mathcal{U} \subseteq \mathcal{T}$. Let $\mathcal{T}, \mathcal{U}, \mathcal{V}, \mathcal{W}$ range over $\mathcal{T}$. Let $\mathcal{T}$ range over $\mathcal{T}$. Let $\mathcal{U}, \mathcal{V}, \mathcal{W}$ range over $\mathcal{U}$.
- We quotient types by taking $\sqcap$ to be commutative, associative, idempotent, and to satisfy $e(\mathcal{U}_1 \sqcap \mathcal{U}_2) = e\mathcal{U}_1 \sqcap e\mathcal{U}_2$.
- We define the degrees of types function $\text{deg} : \mathcal{T} \rightarrow \mathbb{N}$ by:
  - $\text{deg}(a) = 0$
  - $\text{deg}(e\mathcal{U}) = \text{deg}(\mathcal{U}) + 1$
  - $\text{deg}(\mathcal{U} \rightarrow \mathcal{T}) = \min(\text{deg}(\mathcal{U}), \text{deg}(\mathcal{T}))$
  - $\text{deg}(\mathcal{U} \sqcap \mathcal{V}) = \min(\text{deg}(\mathcal{U}), \text{deg}(\mathcal{V}))$.
- We define the good types on $\mathcal{T}$ by:
  - $a \in \mathcal{A} \implies a$ good
  - $\mathcal{U}$ good, $e \in \mathcal{E} \implies e\mathcal{U}$ good
  - $\mathcal{U}, \mathcal{T}$ good, $\text{deg}(\mathcal{U}) \geq \text{deg}(\mathcal{T}) \implies \mathcal{U} \rightarrow \mathcal{T}$ good
  - $\mathcal{U}, \mathcal{V}$ good, $\text{deg}(\mathcal{U}) = \text{deg}(\mathcal{V}) \implies \mathcal{U} \sqcap \mathcal{V}$ good
- Let $\mathcal{U} \in \mathcal{U}$. If $\text{deg}(\mathcal{U}) > 0$, we define $\mathcal{U}^-$ as follows:
  - $(\mathcal{U}_1 \sqcap \mathcal{U}_2)^- = \mathcal{U}_1^- \sqcap \mathcal{U}_2^-
  - (e\mathcal{U})^- = \mathcal{U}$
The realisability semantics: saturation and interpretation are key; furthermore, good types contain only good terms

Let $\mathcal{X}, \mathcal{Y} \subseteq \mathcal{M}$. $\mathcal{P}(\mathcal{X})$ denotes the powerset of $\mathcal{X}$.

- $\mathcal{X} \rightsquigarrow \mathcal{Y} = \{ M \in \mathcal{M} \mid \forall N \in \mathcal{X}, \text{ if } M \diamond N \text{ then } M N \in \mathcal{Y} \}$.
- $\mathcal{X}$ is saturated iff whenever $M \rhd^*_\beta N$ and $N \in \mathcal{X}$, then $M \in \mathcal{X}$.
- Let $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2$ where $\mathcal{V}_1 \cap \mathcal{V}_2 = \emptyset$ and $\mathcal{V}_1, \mathcal{V}_2$ are denum. $\infty$.
- Let $x \in \mathcal{V}_1$ and $n \in \mathbb{N}$. We define $\mathcal{N}_x^n = \{ x^n N_1...N_k \in \mathcal{M} \mid k \geq 0 \}$.
- An interpretation $I : A \to \mathcal{P}(\mathcal{M}^0)$ is a function such that $\forall a \in A$:
  - $I(a)$ is saturated and $I(x) \subseteq \mathcal{M}^0$.
- Let an interpretation $I : A \to \mathcal{P}(\mathcal{M}^0)$. We extend $I$ to $\mathcal{T}$ as follows:
  - $I(eU) = I(U)^+ = \{ M^+ \mid M \in I(U) \}$
  - $I(U \cap V) = I(U) \cap I(V)$
  - $I(U \rightarrow T) = I(U) \rightsquigarrow I(T)$
- Let $U \in \mathcal{T}$. We define the meaning $[U]$ of $U$ by:
  $[U] = \{ M \in \mathcal{M} \mid M \text{ is closed and } M \in \bigcap_I \text{ interpretation } I(U) \}$.
- **Lemma**: Type interpretations are saturated and interpretations/meanings of good types contain only good terms.
The typing rules

\[
\begin{align*}
\frac{T \text{ good} \quad \deg(T) = n}{x^n : \langle (x^n : T) \vdash T \rangle} & \text{ (ax)} \\
\frac{T \text{ good}}{x^0 : \langle (x^0 : T) \vdash T \rangle} & \text{ (ax)} \\
M : \langle \Gamma, (x^n : U) \vdash_i T \rangle \quad \lambda x^n : M : \langle \Gamma \vdash_i U \rightarrow T \rangle & \text{ (\(\rightarrow_i\))} \\
M_1 : \langle \Gamma_1 \vdash_i U \rightarrow T \rangle \quad M_2 : \langle \Gamma_2 \vdash_i U \rangle \quad \Gamma_1 \bowtie \Gamma_2 & \text{ (\(\rightarrow_E\))} \\
M_1 M_2 : \langle \Gamma_1 \cap \Gamma_2 \vdash_i T \rangle \\
M : \langle \Gamma_1 \vdash_i U_1 \rangle \quad M : \langle \Gamma_2 \vdash_i U_2 \rangle & \text{ (\(\land\))} \\
M : \langle \Gamma_1 \cap \Gamma_2 \vdash_i U_1 \cap U_2 \rangle \\
M : \langle \Gamma_1 \vdash_i U \rangle & \text{ (exp)} \\
M^+ : \langle e \Gamma \vdash_i eU \rangle \\
M : \langle \Gamma \vdash_2 U \rangle \quad \langle \Gamma \vdash_2 U \rangle \sqsubseteq \langle \Gamma' \vdash_2 U' \rangle & \text{ (\(\sqsubseteq\))} \\
M : \langle \Gamma' \vdash_2 U' \rangle
\end{align*}
\]
The subtyping rules

\[ \phi \sqsubseteq \phi \quad \text{(ref)} \]

\[ \frac{\phi_1 \sqsubseteq \phi_2 \quad \phi_2 \sqsubseteq \phi_3}{\phi_1 \sqsubseteq \phi_3} \quad \text{(tr)} \]

\[ U_2 \text{ good} \quad \deg(U_1) = \deg(U_2) \quad \frac{U_1 \cap U_2 \sqsubseteq U_1}{\text{(\cap_e)}} \]

\[ \frac{U_1 \sqsubseteq V_1 \quad U_2 \sqsubseteq V_2}{U_1 \cap U_2 \sqsubseteq V_1 \cap V_2} \quad \text{(\cap)} \]

\[ \frac{U_2 \sqsubseteq U_1 \quad T_1 \sqsubseteq T_2}{U_1 \rightarrow T_1 \sqsubseteq U_2 \rightarrow T_2} \quad \text{(\rightarrow)} \]

\[ \frac{U_1 \sqsubseteq U_2}{eU_1 \sqsubseteq eU_2} \quad \text{\(\subseteq_{\exp}\)}} \]

\[ \frac{U_1 \sqsubseteq U_2}{\Gamma, (y^n : U_1) \sqsubseteq \Gamma, (y^n : U_2)} \quad \text{\(\subseteq_{c}\)}} \]

\[ \frac{U_1 \sqsubseteq U_2 \quad \Gamma_2 \sqsubseteq \Gamma_1}{\langle \Gamma_1 \vdash U_1 \rangle \sqsubseteq \langle \Gamma_2 \vdash U_2 \rangle} \quad \text{\(\subseteq_{\langle\rangle}\)}} \]
Properties of the type systems and the semantics

- **Lemma** \(\vdash_1 / \vdash_2\) accept only good terms/types; degree of \(M\) is the same as the degree of its type; if \(M\) is typable then its \(\beta\)-redexes can be activated: Let \(i \in \{1, 2\}\). If \(M : \langle (x_{i}^{n_{i}} : U_{i})_{n} \vdash_{i} U \rangle\), then
  1. \(\forall 1 \leq i \leq n, U_{i}\) is good and \(\text{deg}(U_{i}) = n_{i} \geq \text{deg}(M)\).
  2. \(U\) and \(M\) are good and \(\text{deg}(M) = \text{deg}(U)\).
  3. If \(\lambda x^{n} . M_{1}M_{2}\) is a subterm of \(M\), then \(\text{deg}(M_{2}) = n\) and hence \((\lambda x^{n} . M_{1})M_{2} \triangleright_{\beta} M_{1}[x^{n} := M_{2}]\).

- **Lemma** [Soundness of \(\vdash_1 / \vdash_2\): Let \(i \in \{1, 2\}\).
  ▶ If \(M : \langle (x_{i}^{n_{i}} : U_{i})_{n} \vdash_{i} U \rangle\), \(\mathcal{I}\) an interpretation, \(\forall 1 \leq i \leq n N_{i} \in \mathcal{I}(U_{i})\), and \(M[(x_{i}^{n_{i}} := N_{i})_{n}] \in \mathcal{M}\) then \(M[(x_{i}^{n_{i}} := N_{i})_{n}] \in \mathcal{I}(U)\).
  ▶ If \(M : \langle () \vdash_{i} U \rangle\), then \(M \in [U]\).

- **Lemma** [Subject Reduction fails for \(\vdash_1\): Let distinct \(a, b, c \in A\):
  1. \((\lambda x^{0} . x^{0}x^{0})(y^{0}z^{0}) \triangleright_{\beta} (y^{0}z^{0})(y^{0}z^{0})\)
  2. \((\lambda x^{0} . x^{0}x^{0})(y^{0}z^{0}) : \langle y^{0} : b \rightarrow ((a \rightarrow c) \cap a), z^{0} : b \vdash_1 c \rangle\).
  3. It is not possible that \((y^{0}z^{0})(y^{0}z^{0}) : \langle y^{0} : b \rightarrow ((a \rightarrow c) \cap a), z^{0} : b \vdash_1 c \rangle\).

- **Lemma** [Subject Reduction and expansion hold for \(\vdash_2\): If \(M : \langle \Gamma \vdash_2 U \rangle\) and \(M \triangleright_{\beta}^{*} N\), then \(N : \langle \Gamma \vdash_2 U \rangle\).
  If \(N : \langle \Gamma \vdash_2 U \rangle\) and \(M \triangleright_{\beta}^{*} N\) then \(M : \langle \Gamma \vdash_2 U \rangle\)
Examples (let $a \neq b$)

1. Let $Nat_0 = (a \to a) \to (a \to a)$, $Nat_1 = e((a \to a) \to (a \to a))$, $Nat'_1 = e(a \to a) \to (ea \to ea)$ and $Nat'_0 = (ea \to a) \to (ea \to a)$.

2. $[a \to a] = \{ M \in M^0 / M \rhd^*_\beta \lambda y^0.y^0 \}$.

3. $[e(a \to a)] = [ea \to ea] = \{ M \in M^1 / M \rhd^*_\beta \lambda y^1.y^1 \}$.

4. $[(a \sqcap (a \to b)) \to b] = \{ M \in M^0 / M \rhd^*_\beta \lambda y^0.y^0.y^0 \}$.

5. $[Nat_0] = \{ M \in M^0 / M \rhd^*_\beta \lambda f^0.f^0 \text{ or } M \rhd^*_\beta \lambda f^0.\lambda y^0.(f^0)^n y^0 \text{ where } n \geq 1 \}$.

6. $[Nat_1] = [Nat'_1] = \{ M \in M^1 / M \rhd^*_\beta \lambda f^1.f^1 \text{ or } M \rhd^*_\beta \lambda f^1.\lambda x^1.(f^1)^n y^1 \text{ where } n \geq 1 \}$. (Note that $Nat'_1 \not\in \cup$.)

7. $[Nat'_0] = \{ M \in M^0 / M \rhd^*_\beta \lambda f^0.f^0 \text{ or } M \rhd^*_\beta \lambda f^0.\lambda y^1.f^0 y^1 \}$.

8. $[(a \sqcap b) \to a] = \{ M \in M^0 / M \rhd^*_\beta \lambda y^0.y^0 \}$.

9. It is not possible that $\lambda y^0.y^0 : \langle() \vdash_1 (a \sqcap b) \to a\rangle$.

10. $\lambda y^0.y^0 : \langle() \vdash_2 (a \sqcap b) \to a\rangle$.

11. 8 and 9 mean that we cannot have a completeness result for $\vdash_1$. 


The failure of completeness

**The semantics for \(\vdash_1\) is not complete:**
1. \(\lambda y^0.y^0 \in [(a \sqcap b) \to a] = \{ M \in M^0 / M \triangleright^* \lambda y^0.y^0 \}\)
2. it is not possible that \(\lambda y^0.y^0 : \langle () \vdash_1 (a \sqcap b) \to a \rangle\).

**The semantics for \(\vdash_2\) is not complete if we use more than one expansion variable:** Let \(Nat''_0 = (e_1 a \to a) \to (e_2 a \to a)\). We have:
1. \(\lambda f^0.f^0 \in [Nat''_0]\).
2. If \(e_1 \neq e_2\), then it is not possible that \(\lambda f^0.f^0 : \langle () \vdash_2 Nat''_0 \rangle\).

**A crucial property for completeness is:** \(U^- = V^- \implies U = V\).

**This fails if we have more than one expansion variable:**
\((e_1 U)^- = U = (e_2 U)^-\) does not necessarily imply that \(e_1 U = e_2 U\).

**In the rest of this talk, we assume that the set \(E\) contains only one expansion variable \(e_c\).**
The proof of completeness for $\vdash_2$ with a unique expansion variable

- We define $\mathcal{V}_U$'s such that:
  - If $\deg(U) = n$, then $\mathcal{V}_U \subseteq \{y^n | y \in \mathcal{V}_2\}$ and $\mathcal{V}_U$ is infinite.
  - If $U \neq V$ then $\mathcal{V}_U \cap \mathcal{V}_V = \emptyset$.
  - If $y^n \in \mathcal{V}_U$, then $y^{n+1} \in \mathcal{V}_{e_U}$.
  - If $y^{n+1} \in \mathcal{V}_U$, then $y^n \in \mathcal{V}_{U-}$.

- We define infinite sets $\mathcal{G}^n = \{(y^n : U) / U \in \mathcal{U}, \deg(U) = n \text{ and } y^n \in \mathcal{V}_U\}$ and $\mathcal{H}^n = \bigcup_{m \geq n} \mathcal{G}^m$. $\mathcal{H}^n$ will contain $\Gamma$'s that are crucial for the interpretation $\mathcal{I}$ below.

- We write $M : \langle \mathcal{H}^n \vdash_2 U \rangle$ iff there is $\Gamma \subset \mathcal{H}^n$ where $M : \langle \Gamma \vdash_2 U \rangle$.

- We define $\mathcal{V}^n = \{M \in \mathcal{M}^n | x^i \in \text{FV}(M) \text{ where } x \in \mathcal{V}_1 \text{ and } i \geq n\}$.

- We let $\mathcal{I}$ be the interpretation defined by:
  for all type variables $a$, $\mathcal{I}(a) = \mathcal{V}^0 \cup \{M \in \mathcal{M}^0 | M : \langle \mathcal{H}^0 \vdash_2 a \rangle\}$.

- **Lemma [\(\mathcal{I} \text{ is an interpretation}\):** $\forall a \in \mathcal{A}$, $\mathcal{I}(a)$ is saturated and $\forall x \in \mathcal{V}_1$, $\mathcal{N}_x^0 \subseteq \mathcal{I}(a) \subseteq \mathcal{M}^0$.

- **Lemma:** If $U \in \mathcal{U}$ is good and $\deg(U) = n$, then $\mathcal{I}(U) = \mathcal{V}^n \cup \{M \in \mathcal{M}^n | M : \langle \mathcal{H}^n \vdash_2 U \rangle\}$.
Let $U \in \mathcal{U}$ be good such that $\deg(U) = n$.

1. $[U] = \{ M \in \mathbb{M}^n \mid M : \langle() \vdash_2 U \rangle \}$.
2. $[U]$ is stable by reduction:
   if $M \in [U]$ and $M \triangleright^* \beta N$, then $N \in [U]$.
3. $[U]$ is stable by expansion:
   if $N \in [U]$ and $M \triangleright^* \beta N$, then $M \in [U]$. 
Conclusions

▶ Expansion may be viewed to work like a multi-layered simultaneous substitution.
▶ Because the early definitions of expansion were complicated, expansion variables (E-variables) were invented to simplify and mechanize expansion.
▶ Our aim is to give a denotational semantics for intersection type systems with exapansion variables.
▶ Denotational semantics helps in reasoning about the properties of an entire type system and of specific typed terms.
▶ However, E-variables pose serious problems for semantics.
▶ In this paper we gave a realisability semantics based on a hierarchical lambda calculus.
▶ These hierarchical levels can be said to accurately capture the intuition behind E-variables: parts of the $\lambda$-term that are typed inside the uses of the E-variable-introduction typing rule for a particular E-variable $e$ can interact with each other, and parts outside $e$ can only pass the parts inside $e$ around.
Future work

- Due to the difficulties of treating the $\omega$-type which is free to move on any level of the hierarchy, we considered only the $\lambda I$-calculus (hence without an $\omega$-type).

- Due to the loss of completeness in the presence of more than one expansion variable, we restricted the number of expansion variables to one only.

- Future works include giving a semantics for the whole $\lambda$-calculus with an $\omega$-type and an infinite number of expansion variables.

- Furthermore, in addition to the semantics of $E$-variables, it is important to give a semantics for the expansion operation.