Proofs and Programs

Semaine 4, TD 4 - Curry-Howard Expension

Philippe Audebaud, Aurore Alcolei

1 March 2018

HW is due on 6 March, 8am.

Hightlights

- Extending the CH correspondence (syntactic and dynamics aspects), by dealing with other logical connectors than $\Rightarrow$ (ex-1,2).
- Proving meta properties of $\lambda_{\rightarrow}$ using induction (ex-3,4).

Exercice 1 (Product Type)**.** In this exercise we are interested in extending the CH correspondence to NJ($\Rightarrow, \wedge$), the NJ fragment with implication and conjunction. Following the BHK interpretation, a witness for the *conjunction* $A \wedge B$ will correspond to a *pair* of witnesses for A and B.

1. Recall the encoding of **pair**, π_1 and π_2 *combinators* seen in TD1. Can we use them to encode *general* pairs and projection in $\lambda_{\rightarrow}$?
2. Instead, we extend types with *products* ($\times$) and pure λ-terms with three new *constants* **pair**, π_1, π_2 (hence making the calculus unpure. . .):

$$\begin{array}{rcl} S, T, \dots & ::= & X \mid S \rightarrow T \mid S \times T \\ a, b, \dots & ::= & x \mid \lambda x.a \mid ab \mid \mathsf{pair}(a, b) \mid \pi_i(a) \end{array}$$

   Give typing rules for the new constants so that they annotate the intro-elim rules of $\wedge$ in NJ.
3. Similarly to the I/E-detour of $\Rightarrow$ in NJ($\Rightarrow$), explain what detours can be created by $\wedge$ in proof derivations and how to eliminate them.
4. Deduce new reductions (β-rules and η-rules) for the extended λ-calculus. We will denote $\lambda_{\rightarrow,\times}$ this new calculus.
5. Inhabit the following types of $\lambda_{\rightarrow,\times}$:

   a) $(A \rightarrow B \rightarrow C) \rightarrow A \times B \rightarrow C$; b) $(A \times B \rightarrow C) \rightarrow A \rightarrow B \rightarrow C$.
6. What is the grammar for β-normal terms in $\lambda_{\rightarrow,\times}$?
7. Let $\Delta \vdash p : A \times B$, what proof simplification in NJ($\Rightarrow, \wedge$) corresponds to the following reduction?

$$\mathsf{pair}(\pi_1\ p)(\pi_2\ p) \longrightarrow_{\eta} p$$

Exercice 2 (λ_{NJ})**.** Add new extensions to $\lambda_{\rightarrow,\times}$ and build a full correspondence with NJ. Types are extended with sums, $\top$ (similar to the unit type) and $\bot$ (also called the empty type):

$$S, T, \dots \quad ::= \quad X \mid S \rightarrow T \mid S \times T \mid S + T \mid \top \mid \bot$$

The **sum type** $S + T$ has two constructors ι_1, ι_2 and one destructor case . . . in . . . corresponding to the **disjunction** introduction and elimination rules in NJ

$$\frac{\Delta \vdash t : A}{\Delta \vdash \iota_1\ t : A + B}\ (\vee_{I(L)}) \qquad \frac{\Delta \vdash t : B}{\Delta \vdash \iota_2\ t : A + B}\ (\vee_{I(R)}) \qquad \frac{\Delta \vdash s : A + B \quad \Delta, x : A \vdash t_1 : C \quad \Delta, y : B \vdash t_2 : C}{\Delta \vdash \text{case } s \text{ in } |\iota_1 x.t_1\ |\iota_2 y.t_2 : C}\ (\vee_E)$$

case ... in ... allows to use what was encapsulated by the injections ι_i, it is similar to 'match with' in Caml.

The **empty type** $\bot$ corresponds to falsehood $\bot$ in NJ. This only has one elimination rule:

$$\frac{\Delta \vdash t : \bot}{\Delta \vdash \varepsilon^A(t) : A}\ (\bot_E)$$

It is not possible to build a closed term of type $\bot$, however ε can be viewed as a feature for error handling.

The **unit type** $\top$ corresponds to $\top$ in NJ and has only one introduction rule/constructor:

$$\frac{}{\Delta \vdash \star : \top}\ (\top_I)$$

1. Give the β-reduction and η-reduction steps associated to sums.

2. What other proof simplifications can you find in NJ? Give their corresponding term reductions in λ_{NJ}. (Hint: these reductions come from the possibility of commuting some rules in NJ.)

3. **HW** Inhabitate the following types:

   a) $A + B \to B + A$;

   b) $A \times (B + C) \to A \times B + A \times C$.

Exercice 3 (Subject reduction)**.** Assuming the Generation lemma (recall in appendix 1), let us prove that $\lambda_\to$ has the subject reduction property:

$$\text{If } \Gamma \vdash m : T \text{ then for every } m \longrightarrow_\beta^* m',\ \text{the typing judgement } \Gamma \vdash m' : T \text{ holds}$$

1. (term substitution) Prove that if $\Gamma, y : S \vdash t : T$ and $\Gamma \vdash s : S$, then $\Gamma \vdash t\langle s/y\rangle : T$;

2. Now, show the subject reduction property.

3. Show that the contraposite does not hold. (Hint: $\mathbf{\Omega}$ can help you to build a counter example)

Exercice 4 (More properties)**. HW** Choose and prove two of the following property of $\lambda_\to$:

1. (minimal context) If $\Delta \vdash t : T$, then for every $x \in \mathrm{FV}(t)$, $x \in \mathrm{dom}(\Delta)$. Deduce that closed terms are the only typable terms in an empty context.

2. (changing context). If $\Delta \vdash t : T$ and Δ, Δ' are two contexts such that $\Delta_{\restriction \mathrm{FV}(t)} = \Delta'_{\restriction \mathrm{FV}(t)}$, then $\Delta' \vdash t : T$ – where $\Delta_{\restriction \mathrm{FV}(t)}$ denotes the restriction of Δ to free variables in t.

3. (type substitution) If $\Delta \vdash t : T$, then for every type variable X and type S, $\Delta\langle S/X\rangle \vdash t : T\langle S/X\rangle$.

Exercice 5 (Saturated parts)**.** Interpreting simple types as saturated parts of Λ is a way to show strong normalisation for $\lambda_\to$. In this exercise we are intersted in showing preliminary lemmas about saturated parts (definition is recall in Appendix).

1. (warmup) Show that $\mathcal{N}$ is saturated.

2. Show that if $S \subseteq \Lambda$ is saturated, then for every $e \equiv (\lambda x.a)b$ such that $b \in \mathcal{N}$ and $e\langle b/x\rangle \in S$, then $e \in S$. (Hint: you can reason by induction on $l(a)$ and $l(b)$, where $l(t)$ is defined for every normal form t as the maximum lenght of its reduction paths... but you first need to justify this measure!)

3. (+++) Show that if X and Y are saturated, then $X \to Y = \{e \in \Lambda \mid \forall a \in X, e\ a \in Y\}$ is saturated.

A From your lectures

Lemma 1 (Generation lemma)**.** *Let* $\Delta \vdash t : T$*,*

- *if* t *is a variable* x *then* $x : T$ *in* Δ
- *if* $t \equiv a\ b$ *then there exists* S *such that* $\Delta \vdash a : S \rightarrow T$ *and* $\Delta \vdash b : S$
- *if* $t \equiv \lambda x.a$ *with* $x \notin dom(\Delta)$ *then* $T = S \rightarrow U$ *such that* $\Delta, x : S \vdash a : U$

Definition 2. Let $S \subseteq \Lambda$, S is said to be *saturated* if:

1. $\mathcal{N}_0 \subseteq S \subseteq \mathcal{N}$,
2. If $e \in S$ and $e \beta e'$ then $e' \in S$,
3. If $e \in \Lambda$ is not an abstraction and $\mathrm{Succ}(e) \subseteq S$, then $e \in S$.