TD5: Curry-Howard for the (almost full) propositional logic

simon.castellan@ens-lyon.fr

Exercise 1 (Curry-Howard in action)
Inhabit the following types:

1. $A + B \to B + A$
2. $A \times (B + C) \to A \times B + A \times C$
3. $(A + B \to C) \to (A \to C) \times (B \to C)$
4. $(A \to C) \times (B \to C) \to (A + B \to C)$
5. $(A \to B \times C) \to ((A \to B) \times (A \to C))$
6. $((A + (A \to R)) \to R) \to R$
7. $((A \to R) + (B \to R)) \to (A \times B \to R)$
8. $(((A \to R) \to R) \to R) \to (A \to R)$

Exercise 2 (Jusqu'à combien peut-on compter en λ-calcul)
In this exercise we work with the λ-calculus with products. We recall that the church encoding of a natural number is $\overline{n} = \lambda f x.\ f^n\ x$.

1. What is the natural type N for the Church encoding of natural numbers?
2. Show that if $\vdash t : N$, t is β-equal to the church encoding of a natural number.
3. Call a function $f : \mathbb{N}^k \to \mathbb{N}$ representable when there exists a term $\vdash t : N^k \to N$ when $t(\overline{n_1}, \ldots, \overline{n_k})$ normalizes to $\overline{f(n_1, \ldots, n_k)}$.

   Show that the class of representable function is closed under composition, and contains constant functions, projections, addition, multiplication and the conditional defined by:

$$\mathrm{cond}(n_1, n_2, n_3) = \begin{cases} n_2 & \text{if } n_1 = 0 \\ n_3 & \text{otherwise} \end{cases}$$

4. Let M be a λ-term such that $f : S \to S, a_1 : N, \ldots, a_p : N, x_1 : S, \ldots, x_m : S \vdash M : S$. Show that, by induction on the normal form of M that there exists a polynomial $P(n_1, \ldots, n_p)$ and $i \leq m$ such that

$$M[\overline{n_1}/a_1, \ldots, \overline{n_p}/a_p] =_\beta f^{P(n_1, \ldots, n_p)} x_i$$

   for all tuple of **non-zero** integers $(n_1, \ldots, n_p)$.

5. Deduce that the class of representable function is the smallest class of function closed under composition and containing constant functions, projections, addition, multiplication and the conditional.

Exercise 3 (Kripke models)
A Kripke model is a preorder $E, \leq)$ (ie. $\leq$ is a binary relation on E which is transitive and reflexive.) along with a binary relation $\models \subseteq E \times V$ specifying which propositional variables hold at which nodes, satisfying that if $w \models X$ and $w \leq w'$ then $w' \models X$ for $X \in V$.
Given a Kripke model $(E, \leq)$ and a point $w \in E$, we define $(E, w) \models A$ for a proposition A by induction on A:

- $(E, w) \models X$ if $w \models X$.
- $(E, w) \models \bot$ is never true
- $(E, w) \models \top$ is always true
- $(E, w) \models A \Rightarrow B$ if for all $w' \geq w$, if $(E, w') \models A$ then $(E, w') \models B$
- $(E, w) \models A \vee B$ if $(E, w) \models A$ or $(E, w) \models B$
- $(E, w) \models A \wedge B$ if $(E, w) \models A$ and $(E, w) \models B$

1. Show that if $\vdash A$ is derivable in NJ, then for all Kriple model $(E, \leq)$ and $w \in E$, we have $(E, w) \models A$
2. Deduce that the excluded middle is not provable in NJ.
3. Show that if a proposition is true in a Kripke model, then it is true in a Kripke model which is totally ordered.
4. Show that if a proposition is true in a Kripke model, then it is true in a Kripke model which is a tree.
5. Show that if a proposition A is true in a Kripke model, then it is true in a Kriple model which is finite and whose size is bounded by a function of the size of A.
6. Assuming *completeness*: if all propositions true in all Kripke models are provable in NJ, show that provability in NJ is decidable.

Exercise 4 (DM, part II – A computational interpretation of negative translations)
In the previous part, you had to prove that $\Gamma \vdash_{NK} A$ implies that $\neg\neg\Gamma \vdash_{NJ} \neg A$. The proof proceeds by a transformation of proofs. In this part, we try to understand related translations on the program side.
We write $\Lambda_{\rightarrow}$ for the set of pure λ-terms, and $\Lambda_{\rightarrow,\times}$ for the set of λ-terms with constructions for the product (pair and projections). We define negation on types as follows: $\neg_R A$ is $A \rightarrow R$ for a fixed type.

1. In the Glivenko theorem, the case for the introduction of the arrow uses the $\bot$-elim rule. This means we cannot view this proof tranformation as a program transformation because there is no counterpart to this rule in the simply-typed λ-calculus you have seen during the lectures.

   To work around this problem, we define a translation on types:

   $$[\![X]\!]_1 = X \qquad [\![A \Rightarrow B]\!]_1 = [\![A]\!]_1 \Rightarrow \neg\neg[\![B]\!]_1.$$

   Show that if $\Gamma \vdash_{NJ} A$ then $[\![\Gamma]\!]_1 \vdash \neg\neg[\![A]\!]_1$.

2. Deduce a mapping $\cdot^* : \Lambda_\to \to \Lambda_\to$ such that if $\Gamma \vdash t : A$ then $[\![\Gamma]\!]_1 \vdash t^* : \neg_R\neg_R[\![A]\!]_1$ where negation has been replaced by $\neg_R$ in $[\![A]\!]_1$.
3. Explain why we do not have that if $t \to_\beta u$ then $t^* \to_\beta^* u^*$.
4. (*Optional*) Give a restriction on the shape of the redexes for the previous question to hold.
5. To work around this problem (Question 3), we introduce another negative translation, as follows:

$$[\![X]\!]_2 = X \qquad [\![A \to B]\!]_2 = \neg_R\neg_R[\![A]\!]_2 \to \neg_R\neg_R[\![B]\!]_2$$

   Shw that there is a function $\cdot_* : \Lambda_\to \to \Lambda_\to$ such that if $\Gamma \vdash t : A$ then $\neg_R\neg_R[\![\Gamma]\!]_2 \vdash t_* : \neg_R\neg_R[\![A]\!]_2$ with $[\![x : A_1, \ldots, x : A_n]\!]_2 = x : [\![A_1]\!]_2, \ldots x_n : [\![A_n]\!]_2$.
6. Show that if $t \to_\beta u$ then $t_* \to_\beta^* u_*$.
7. (*Optional*) Build a term $\vdash t : \neg_R\neg_R A \to \neg_R\neg_R[\![A]\!]_2$
8. Show that there exists a closed term cc such that $\vdash cc : \neg_R\neg_R[\![((A \to B) \to A) \to A]\!]_2$.
9. (*Optional*) This translation adds a lot of double-negation. One way to optimize it is as follows: define mutually $[\![A]\!]_3$ and $A^\perp$ as follows:

$$[\![A]\!]_3 = \neg_R A^\perp \qquad X^\perp = \neg_R X \qquad (A \Rightarrow B)^\perp = [\![A]\!]_3 \times B^\perp.$$

   Define a new map $[\![\cdot]\!]_3 : \Lambda_\to \to \Lambda_{\to,\times}$ such that:

   - if $\Gamma \vdash t : A$ then $[\![\Gamma]\!]_3 \vdash [\![t]\!]_3 : [\![A]\!]_3$
   - if $t \to_\beta u$ then $[\![t]\!]_3 {\to^*}_\beta [\![u]\!]_3$
10. (*Optional*) Build a closed term of type $[\![((A \to B) \to A) \to A]\!]_3$.