

Curry - Howard correspondence

We will look at how the structure of intuitionistic logic matches that of typed λ -calculus, which we introduced last time. Since we've focused on the simply typed λ -calculus, where the only type constructor is \rightarrow , we should also focus on the \rightarrow -fragment of IPC (the fragment with \rightarrow as unique connective).

Call this fragment $\text{IPC}[\rightarrow]$. However, the results we will look at extend to the full language of IPC and even IQC, provided the λ -calculus side is enriched accordingly.

In order to fully appreciate the correspondence, we must make a minor change to our notion of natural deduction proof.

Labelled proofs

Proofs in natural deduction will be as usual, but:

- every assumption comes with an index
 - every use of $(\rightarrow i)$ also comes with an index $i \in \mathbb{N}$:
if introducing $\varphi \rightarrow \psi$, all and only the assumptions
 φ^i (with index i) occurring above in the proof are
discharged.

It is easy to see that every natural deduction proof can be "labeled" so that the constraint above is respected. For instance:

$$\frac{\frac{[\varphi] [\varphi \rightarrow \psi] \rightarrow e}{\frac{\psi \rightarrow i}{(\varphi \rightarrow \psi) \rightarrow \psi}} \rightarrow i}{\varphi \rightarrow ((\varphi \rightarrow \psi) \rightarrow \psi)} \xrightarrow{i} \text{add labels}$$

$$\frac{\frac{\frac{\psi}{(\psi \rightarrow \psi) \rightarrow \psi} \rightarrow i_2}{(\psi \rightarrow ((\psi \rightarrow \psi) \rightarrow \psi))} \rightarrow i_1}{\psi \rightarrow ((\psi \rightarrow \psi) \rightarrow \psi)}$$

Now let us turn to the correspondence. First, it is clear that if the set of atomic formulas coincides with the set of atomic types, then the set $L_P[\rightarrow]$ of \rightarrow -formulas of IPC and the set T_A of types coincide.

Rem If $P=A$ then $L_P[\rightarrow] = T_A$.

So formulas in $IPC[\rightarrow]$ correspond to types in an obvious way. Perhaps less obvious is the fact that proofs of a formula (with, possibly, some undischarged assumption) correspond to terms of the corresponding type.

Def For each labeled proof ~~of~~ P of ψ in $IPC[\rightarrow]$ we define a corresponding term $T_P : \psi$. The definition is by induction on P , as follows:

Since we are in $IPC[\rightarrow]$ we have only three cases to consider for P : either P consists only of an undischarged assumption; or the last rule in P is $(\rightarrow i)$; or the last rule in P is $(\rightarrow e)$.

$$(i) \quad \varphi^n \models P \longrightarrow M_P := x_\varphi^n : \varphi$$

$$(ii) \quad P \left\{ \begin{array}{c} [\varphi^n] \\ \vdots \\ [\varphi^n] \end{array} \right. \xrightarrow{\psi} \frac{\psi}{\varphi \rightarrow \psi} (\rightarrow i_n) \longrightarrow M_P := \lambda x_\varphi^n. M_{P'} : \varphi \rightarrow \psi$$

$$(iii) \quad P \left\{ \begin{array}{c} P' \\ \vdots \\ P'' \end{array} \right. \xrightarrow{\psi} \frac{\psi \quad \varphi \rightarrow \psi}{\psi} (\rightarrow e) \longrightarrow M_P := M_{P''} M_{P'} : \psi$$

Example

Consider the following proof:

$$\begin{array}{c}
 [\varphi^1] \quad [\varphi \rightarrow \psi^2] \\
 \hline
 \frac{[\psi \rightarrow x^3]}{\psi} \xrightarrow{\rightarrow e} \\
 \frac{x}{\varphi \rightarrow x} \xrightarrow{\rightarrow i_1} \\
 \frac{\varphi \rightarrow x}{(\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow x)} \xrightarrow{\rightarrow i_2} \\
 \hline
 \frac{(\psi \rightarrow x) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow x))}{(\psi \rightarrow x) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow x))} \xrightarrow{\rightarrow i_3}
 \end{array}$$

$$\begin{array}{c}
 \frac{x_\varphi^1 : \varphi \quad x_{\varphi \rightarrow \psi}^2 : \varphi \rightarrow \psi}{x_{\varphi \rightarrow x}^3 : \psi \rightarrow x} \\
 \hline
 \frac{}{x^2 x^1 : \psi} \\
 \frac{}{x^3(x^2 x^1) : x} \\
 \hline
 \frac{}{x x^1. x^3(x^2 x^1) : \varphi \rightarrow x} \\
 \hline
 \frac{}{x x^2. x x^1. x^3(x^2 x^1) : (\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow x)} \\
 \hline
 \frac{}{x x^3. x x^2. x x^1. x^3(x^2 x^1) : (\psi \rightarrow x) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow x))} \\
 \downarrow \text{rename bound variables for convenience}
 \end{array}$$

$$\lambda g_{\psi \rightarrow x}. \lambda f_{\varphi \rightarrow \psi}. \underline{\lambda x_\varphi. g(fx)}, \quad g \circ f$$

This λ -term really shows the computational content of the natural deduction proof: given a proof g of $\psi \rightarrow x$ and a proof f of $\varphi \rightarrow \psi$ (which are functions in the BHK int) the composition $g \circ f$ is a proof of $\varphi \rightarrow x$.

This corresponds to the following term (we display the whole construction tree, which parallels the proof)

So, the λ -term $\lambda g_{\psi \rightarrow x}.\lambda f_{\varphi \rightarrow \psi}.\lambda x_\varphi.g(fx)$ really brings out the method required by the BHK interpretation. Moreover, the term fully encodes the proof. To get the proof back, just deconstruct the term step by step and then replace each term by its type:

$$\begin{array}{c}
 \frac{x^2_{\varphi \rightarrow \psi} x'_\varphi}{x^2 x'} \rightsquigarrow_e \\
 \frac{\frac{x^3_{\psi \rightarrow x}}{x^3(x^2 x')}}{\rightsquigarrow_i} \\
 \frac{\lambda x'. x^3(x^2 x')}{\rightsquigarrow_i} \\
 \frac{\lambda x^2 \lambda x'. x^3(x^2 x')}{\rightsquigarrow_i} \\
 \frac{\lambda x^3. \lambda x^2. \lambda x'. x^3(x^2 x')}{\rightsquigarrow_i}
 \end{array}$$

Replace each term by its type and this is exactly the original proof.
 We obtained it simply by "unfolding" the λ -term.

Prop. For each ψ , $P \mapsto M_P$ is a bijection between proofs of ψ (with und. assumptions) and terms of type ψ . Moreover:

$$FV(M_P) = \{x_\varphi^n \mid \varphi^n \text{ is an undischarged assumption in } P\}$$

In particular, P is a proof without undischarged assumptions iff M_P is a closed term.

So we have the following perfect match:

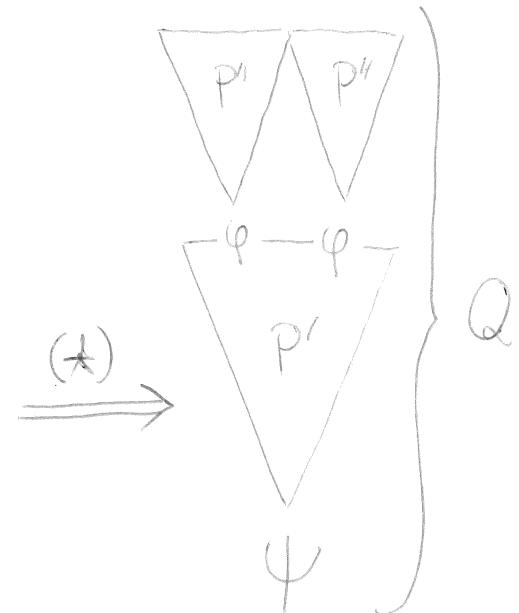
Logic	Computation
formula	type
proof	term
proof w/o assump.	closed term
theorem	inhabited type

One important piece is still missing:
 what is the logic counterpart of Computation?
 More precisely, what are the notions that,
 on the logic side of the correspondence,
 are the counterpart of β -reduction (\rightarrow_β)
 β -reducibility (\rightarrow_β) and normal form?

These are proof-theoretic notions which
 we have not discussed in the course, but
 which play an important role in proof theory:
normalization of a natural deduction proof
 and normal form of a proof. In the con-
 text of $\text{IPC}[\rightarrow]$ these can be explained
 very simply.

Proof normalization

$$\left. \begin{array}{c} \vdash (\varphi \rightarrow \varphi) \\ \varphi \\ \hline \varphi \rightarrow \varphi \end{array} \right\} \xrightarrow{\text{se}} \varphi$$



Def let Π, Π' be proofs in $\text{IPC}[\rightarrow]$

- $\Pi \rightarrow_N \Pi'$ if Π' is obtained from Π by replacing a sub-proof of Π according to (*) above.
- $\Pi \rightarrow_N \Pi'$ if there is a chain $\Pi \xrightarrow{\beta} \dots \xrightarrow{\beta} \Pi'$
- Π is in normal form if $\forall \Pi': \Pi \not\rightarrow_N \Pi'$

Now let P and Q be as above
(i.e., Q results from P by means of (\dagger)).

Then:

$$M_P = (\lambda x_q^n. M_{P'}) M_{P''}$$

$$M_Q = M_{P'} [M_{P''}/x_q^n] \rightarrow \left[\begin{array}{l} \text{prove this by} \\ \text{induction on } P' \end{array} \right]$$

Thus, M_P is a redex and M_Q its reduct!
Using this, it is not hard to show the following.

Prop

- $P \rightarrow_N Q \Leftrightarrow M_P \rightarrow_B M_Q$
- $P \rightarrow_N Q \Leftrightarrow M_P \rightarrow_P M_Q$
- P is in normal form $\Leftrightarrow M_P$ is in normal form

From this connection we can get some of the most important results in proof theory as corollaries of the corresponding results for λ -calculus.

Cor

◦ Church-Rosser:

if $P \rightarrow_N Q$ and $P \rightarrow_N Q'$ then there is Q''
s.t. $Q \rightarrow_N Q''$ and $Q' \rightarrow_N Q''$.

◦ Weak normalization:

$P \rightarrow_N Q$ for some Q in normal form

◦ Strong normalization:

There are no infinite sequences $P \rightarrow P' \rightarrow_N P'' \rightarrow_N \dots$

So, the table can now be completed as follows:

Logic	Computation
Formula	Type
Proof	Term
Proof w/o assump.	Closed term
Theorem	Inhabited type
Normalization	β -reduction
Proof in normal form	Term in normal form

On the logic side and on the λ -calculus side, we have exactly the same formal structure, but we think of it differently: on the logic perspective we think of the objects as formulas, proofs, and simplification of proofs; on the λ -calculus perspective we think of them as types, terms (programs) and computation. So, the same structure emerges naturally from two different perspectives; the connection to computation also witnesses the genuinely constructive character of intuitionistic logic: a proof of $\varphi \rightarrow \psi$ really encodes a method, and this can be written in the form of a λ -term $M: \varphi \rightarrow \psi$ which is a program to turn proofs of φ into proofs of ψ . Whence the slogan: "proofs-as-programs".