The Curry-Howard principle

The Curry-Howard principle says that *proof theory* and the *theory of computation* are two viewpoints on the same underlying mathematical objects – called *proofs* on the one hand and *programs* on the other [SU]. This was made explicit in work of Curry '58 and Howard '69 but an important component of the basic philosophy goes back to Brouwer, Heyting and Kolmogorov (BHK). As was recalled in Shawn's first lecture, BHK take "the view that what we write as a proof is merely a description of something which is already a process in itself" [G, §1.2.2]. More concretely, a proof of $A \longrightarrow B$ should give rise to a *transformation* from proofs of A to proofs of B.

If proofs are transformations, it makes sense to ask if two proofs of $A \longrightarrow B$ give rise to the *same* transformation. In this way the BHK interpretation, while a simple idea, suggests a profound break from traditional logic with its focus on *provability* (does a proof exist) towards a study of *proofs as mathematical objects*, in their own right. Now, it is easy to miss the point here, since one might imagine that one *knows* "what a proof is" by virtue of experience writing proofs in e.g. geometry. But while such experience confers knowledge of *provability* it offers very little insight to the true nature of proofs (whatever that might be). Perhaps linear logic or homotopy type theory illustrate this point most forcefully.

This isn't so surprising: by way of analogy, it is easier to agree on what it means for a function to be a solution of a differential equation (i.e. provability) than to agree on the "true nature" of a differential equation, which requires relatively sophisticated differential geometry using the language of jet bundles [S] or algebraic geometry in the language of D-modules (even the nature of polynomial equations was arguably only settled by Grothendieck in [EGAI]). So far we (arguably) lack similarly satisfying answers to the question "what is a proof?".

However, while we may not know what proofs "are", we do have a first step : a bijection between (closed) proofs in natural deduction and (closed) λ-terms in simply-typed λ-calculus. This is often called the Curry-Howard correspondence (we use "correspondence" to name this particular result and "principle" to denote the broader philosophy which it inspires). This bijection achieves (in some limited, but suggestive way) a realisation of proofs as processes: namely λ-terms under β-reduction to normal form.

The purpose of today's lecture is to prove the Curry-Howard correspondence.

References

[G] J.Y. Girard "Proofs and types" Chapter 3
[NVP] Negri, Von Plato "Structural proof theory" §1.2 and §8.1 particularly.
[Ga] Gallier "On the correspondence between proofs and lambda terms"
[SU] Sorensen, Urzyczyn "Lectures on the Curry-Howard isomorphism"
[S] Saunders, "The geometry of jet bundles"
[M] Martin-Löf "On the meanings of the logical constants and the justifications of the logical laws".
[EGAI] A. Grothendieck, see therisingsea.org for a translation.

Natural Deduction

There are various systems called "natural deduction", see [G, p.5], [NVP] and Shawn's talk for some historical background on why. In any case, while these systems might all agree on which propositions are provable they genuinely differ in their opinions about what a proof is. We must choose the correct system to get a bijection with λ-calculus.

The systems all have the same language: an infinite set of propositional variables $p, q, r, \ldots$ and formulas $\psi \to \varphi$ whenever ψ, φ are formulas (all variables are formulas).

<u>System I</u> As presented in [SU] is about <u>sequents</u> (<u>judgments</u>) $\Gamma \vdash \varphi$ where φ is a formula and Γ is a finite <u>set</u> of formulas. The deduction rules are

$$\Gamma, \varphi \vdash \varphi \quad (Ax) \qquad\qquad (\Gamma \text{ any set not containing } \varphi)$$

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\,(\to I) \qquad\qquad (\Gamma \text{ any set not containing } \varphi) \tag{3.1}$$

$$\frac{\Gamma \vdash \varphi \to \psi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \psi}\,(\to E) \qquad\qquad (\Gamma \text{ any set})$$

The reason we need $\Gamma, \varphi \vdash \varphi$ and not just $\varphi \vdash \varphi$ as axioms for two reasons: it is how we simulate the left introduction of → in sequent calculus, and it enables weakening (the introduction of spurious dependencies). But this is quite a defective system.

<u>Example</u> Is $\varphi, \psi \vdash \varphi \to \psi$ provable? Certainly $\psi \vdash \varphi \to \psi$ is,

$$\frac{\psi, \varphi \vdash \psi}{\psi \vdash \varphi \to \psi}\,\to I \tag{3.2}$$

But if we want to weaken in a copy of φ, we hit the fact that Γ in $\Gamma, \psi \vdash \psi$ has to be a <u>set</u> not a <u>multiset</u>. Similar (but even worse) problems arise when we try to encode standard λ-terms as proofs (e.g. Church numerals). This version of natural deduction "conflates too many proofs".

We could make $\Gamma = \{\varphi_1^{a_1}, \dots, \varphi_n^{a_n}\}$ a multiset, for $a_i \geqslant 1$ and adopt a variation of $\to I$

$$\frac{\varphi_1^{a_1}, \dots, \varphi_n^{a_n} \vdash \psi}{\varphi_1^{a_1}, \dots, \varphi_i^{a_i - 1}, \dots, \varphi_n^{a_n} \vdash \varphi_i \longrightarrow \psi} \to I \qquad (4.1)$$

Or equivalently we can write e.g. φ^3 as $x_1 : \varphi, x_2 : \varphi, x_3 : \varphi$ and work up to α-equivalence. This leads (almost) to "standard" natural deduction as in [G] or [NVP, §1.2, §8.1].

<u>System II</u> We add an infinite collection of variables Y_φ for each formula φ, writing $x : \varphi$ for $x \in Y_\varphi$. Sequents are $\Gamma \vdash \varphi$ where φ is a formula and Γ is a finite set of variables. For convenience we write $\{x_1, \dots, x_n\}$ as

$$\Gamma = \{ x_1 : \varphi_1, \dots, x_n : \varphi_n \} \qquad (4.2)$$

where $x_i \in Y_{\varphi_i}$. The notation $\Gamma, x : A$ is only well-defined if $x \neq x_i$ all i, in which case it denotes $\Gamma \cup \{x\} \supsetneq \Gamma$. The rules are:

$$\Gamma, x : \varphi \vdash \varphi \qquad (Ax)$$

$$\frac{\Gamma, x : \varphi \vdash \psi}{\Gamma \vdash \varphi \longrightarrow \psi} (\to I) \qquad (4.3)$$

$$\frac{\Gamma \vdash \varphi \longrightarrow \psi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \psi} (\to E)$$

A <u>pre-proof</u> of $\Gamma \vdash \psi$ is a tree with rules for vertices, axioms for leaves and $\Gamma \vdash \psi$ as the conclusion of the final rule. A <u>proof</u> is an α-equivalence class of <u>pre-proofs</u> (α-equivalence means simultaneous renaming of all $\sim$-related copies of a variable, in the sense made precise overleaf).

two occurrences of φ in the proof

<u>Example</u>

$$\frac{x:\varphi,\ y:\varphi,\ z:\psi \vdash \psi}{y:\varphi,\ z:\psi \vdash \varphi \to \psi}$$

<u>Def^n</u> An <u>occurrence</u> of a variable x in a pre-proof is a variable in the context Γ of a sequent in some rule of the proof. We define a relation $\sim$ on occurrences of x to be the smallest equivalence relation generated by

- setting the three occurrences of x in $\dfrac{\Gamma \vdash \varphi \to \psi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \psi}$ (5.1) to be related whenever $x \in \Gamma$,
- setting the two occurrences of x in $\dfrac{\Gamma,\ y:\varphi \vdash \psi}{\Gamma : \varphi \to \psi}$ to be related, where $x \in \Gamma$.

<u>Example</u> Consider the proof, for $\Gamma = \{ f:\varphi \to \varphi,\ x:\varphi \}$

$$P := \frac{\dfrac{\dfrac{\Gamma \vdash \varphi \to \varphi \qquad \dfrac{\Gamma \vdash \varphi \to \varphi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \varphi}(\to E)}{f:\varphi \to \varphi, x:\varphi \vdash \varphi}(\to E)}{f:\varphi \to \varphi \vdash \varphi \to \varphi}}{\vdash (\varphi \to \varphi) \to (\varphi \to \varphi)} \qquad (5.1)$$

Here all the occurrences of f are equivalent under $\sim$ (resp. x's).

<u>Example</u> Consider the proof

$$\frac{\dfrac{\boxed{x:\varphi}, \boxed{y:\psi}, f:\varphi \to \psi \vdash \psi}{\boxed{y:\psi} \vdash (\varphi \to \psi) \to (\varphi \to \psi)}(\to I)^2 \qquad \dfrac{\boxed{x:\varphi}, \boxed{y:\psi} \vdash \psi}{\boxed{y:\psi} \vdash \varphi \to \psi}}{\boxed{y:\psi} \vdash \varphi \to \psi}$$

Here all occurrences of y are $\sim$-equivalent but the two x's are not equivalent.

Def^n We write $\langle \Gamma \rangle := \{ \varphi_1^{a_1}, \dots, \varphi_n^{a_n} \}$ if the variables occurring in Γ belong to $Y_{\varphi_1} \cup \dots \cup Y_{\varphi_n}$ (and no smaller union) and exactly a_i elements of Γ lie in Y_{φ_i}.

Lemma There is a bijection between System II proofs of $\Gamma \vdash \varphi$ and proofs of $\langle \Gamma \rangle \vdash \varphi$ using rule (4.1), together with a "good" partition of the occurrences of every formula ψ appearing in the context of a sequent in the proof, i.e.

$$\dfrac{\dfrac{\textcircled{\varphi}, \textcircled{\psi}, \varphi \to \psi \vdash \psi}{\textcircled{\psi} \vdash (\varphi \to \psi) \to (\varphi \to \psi)} \qquad \dfrac{\textcircled{\varphi}, \textcircled{\psi} \vdash \psi}{\textcircled{\psi} \vdash \varphi \to \psi}}{\textcircled{\psi} \vdash \varphi \to \psi} .$$

↓ where we write $\psi^a = \psi^{(1)}, \dots, \psi^{(a)}$ as separate and distinguishable copies of ψ.

Remark Here "good" means that the partition P consists of sets Q satisfying

- Q contains at most one ψ in each sequent
- Q contains a ψ in both Γ's of the numerator of a $\to E$ rule iff. it contains a ψ in the denominator.
- if ψ is not the active formula in a $\to I$ rule then Q contains a ψ in the numerator iff. it contains one in the denominator.
- if ψ is active in $\to I$ then among the sets Q of the partition there is a unique one which contains a ψ in the numerator but not the denominator (so the rest contain a ψ in the denominator).

Moreover, we consider partitions up to permutation of the copies of ψ in each sequent.

Note Thus a System II proof is a proof with multisets of hypotheses and a concept of "identity" for these hypotheses. A good partition is equivalent to package labels + discharge labels in the usual sense for natural deduction proofs which are closed i.e. all hypotheses are discharged (note that in a natural deduction proof we may introduce $A \to B$ discharging no hypothesis: to construct the corresp. System II proof a new copy of A needs to be explicitly propagated from the node of the introduction rule upwards to all the "downstream" leaves).

[From now on, we say "natural deduction" or ND for "System II"]

We may identify the set of formulas of ND with the set $\Phi_{\to}$ of simple types in λ-calculus.

<u>Theorem</u> (Curry-Howard) For any $\varphi \in \Phi_{\to}$ there is a bijection between ND proofs of $\vdash \varphi$ and <u>closed</u> λ-terms of type φ.

<u>Proof</u> Basically a tautology. The typing constraints say: M is of type φ if it can be constructed by the typing rules

$$\overset{ⓐ}{\Gamma, x:\tau \vdash x:\tau} \qquad \overset{ⓑ}{\dfrac{\Gamma, x:\sigma \vdash M:\tau}{\Gamma \vdash (\lambda x : M) : \sigma \to \tau}} \qquad \overset{ⓒ}{\dfrac{\Gamma \vdash M:\sigma\to\tau \quad \Gamma \vdash N:\sigma}{\Gamma \vdash (M\,N):\tau}}$$

Given a proof P of $\vdash \varphi$ in ND apply the construction rules ⓐ,ⓑ,ⓒ in the same order as Ax, $\to I$, $\to E$ to construct a closed λ-term of the same type φ. It is clearly a surjective map onto closed λ-terms. To prove <u>injectivity</u> we have to argue every λ-term (= α-equiv class) has <u>exactly one</u> justification via ⓐ,ⓑ,ⓒ for its type. But as the structure of the λ-term dictates each of the rules and their order, and α-equivalence does not affect the RHS of the proof structure (here we use that the term is closed) this is clear. □

<u>Example</u> The Church numeral $\underline{2} = \lambda f^{\varphi\to\varphi}. \lambda x^{\varphi}. (f(fx))$ comes from P of (5.1).

<u>Remark</u> Let P be a proof of $\vdash \varphi$ with corresponding closed λ-term M. A β-redex in M, say $((\lambda x^{\sigma}. M^{\tau})\, N^{\sigma})$ corresponds to a part of P of the form (note M, N may not be closed, so we define this "part" via the <u>construction</u> $M \mapsto P$)

$$\dfrac{\dfrac{\begin{matrix} P_1 \\ \vdots \\ \Gamma, x:\sigma \vdash \tau \end{matrix}}{\Gamma \vdash \sigma \to \tau}{\scriptstyle \to I} \qquad \begin{matrix} P_2 \\ \vdots \\ \Gamma \vdash \sigma \end{matrix}}{\Gamma : \tau}{\scriptstyle \to E} \qquad (7.1)$$

Such subproofs consisting of an introduction followed immediately by an elimination are called <u>detours</u> in the literature on natural deduction. Intuitively it seems obvious we should be able to construct a proof of $\Gamma \vdash \mathcal{J}$ without using the hypothesis $x : A$. Indeed, if we look at P_1 the leaves must be labelled

$$\Gamma', \Delta, x : B, y : \theta \vdash \theta \quad \text{or} \quad \Gamma, \Delta, x : B \vdash B$$

where $y \neq x$ and either $\Gamma = \Gamma'$ or $\Gamma = \Gamma', y : \theta$. We can form a new deduction for $\Gamma \vdash \mathcal{J}$ as follows: in P_1 whenever a leaf of the form $\Gamma, \Delta, x : B \vdash B$ occurs, replace it by the deduction obtained from P_2 by adding Δ to the premise of each sequent in P_2 (possibly with variable renaming to preserve multiplicities). Finally, delete the assumption $x : B$ from the premise of every sequent in the resulting proof (this includes the $x : B$ in $\Gamma', \Delta, x : B, y : \theta \vdash \theta$ which were anyway never used). The resulting proof, which we may denote $P_1[P_2/x]$ is clearly a kind of <u>substitution</u>.

<u>Lemma</u> $P_1[P_2/x]$ corresponds to the 1-step β-reduction of M at the given redex.

<u>Proof</u> By induction on the structure of M. □

<u>Upshot</u> Under Curry-Howard <u>β-reduction</u> corresponds to <u>detour elimination</u>.

This notion of detour elimination was introduced and studied independently in the natural deduction literature, but we can use CH (= Curry-Howard) to deduce the basic results from theorems we have already proven about λ-calculus.

<u>Defn</u> Let $\cong$ denote the equivalence relation on the set of proofs of $\vdash \mathcal{S}$ generated (in an appropriate sense, i.e. closed under $\rightarrow I$ and $\rightarrow E$) by detour elimination.

Theorem Let P, P' be proofs of $\vdash \varphi$ with corresponding λ-terms M, M'. Then

$$P \cong P' \iff M =_\beta M'. \qquad (9.1)$$

Corollary Every $\cong$-equivalence class of proofs of $\vdash \varphi$ contains a unique detour-free proof.

Proof By Church-Rosser and strong normalisation for λ-calculus. $\square$

This is somewhat remarkable: anything provable in ND can be proven without using Modus Ponens! (i.e. $\rightarrow E$). We also observe that there are genuinely different proofs of the same formula in ND, which differ in their pattern of hypothesis usage.

Example Each Church numeral $\underline{n}$ gives a proof P_n of $\vdash (\varphi \to \varphi) \to (\varphi \to \varphi)$ and $P_n \ncong P_m$ whenever $m \neq n$.

Returning to the general Curry-Howard principle discussed at the beginning of the lecture, we can say that the deeper reason that we wish to distinguish between proofs of the same formula is that we view proofs as transformations, and P_n determines a different transformation of its inputs (a proof of $\vdash \varphi \to \varphi$) to its outputs (another proof of $\vdash \varphi \to \varphi$). This point is made most clearly using the category $\mathcal{L}$ of simply-typed λ-terms discussed in my earlier lecture. Let $\mathcal{L}_c$ (c for closed) denote the subcategory with the same objects as $\mathcal{L}$ but only those morphisms M with $FV_\beta(M) = \emptyset$. Then

$$\mathcal{L}_c(\mathbb{1}, \varphi \to \varphi) = \Lambda_{\varphi \to \varphi} / =_{\beta\eta} \cong \{ \text{proofs of } \vdash \varphi \to \varphi \} / \cong + \eta$$

$$\mathcal{L}_c(\varphi \to \varphi, \varphi \to \varphi) = \Lambda_{(\varphi \to \varphi) \to (\varphi \to \varphi)} / =_{\beta\eta} \cong \{ \text{proofs of } \vdash (\varphi \to \varphi) \to (\varphi \to \varphi) \} / \cong + \eta$$

Using this category we can be more precise about the <u>transformation</u> determined by a proof P of $\vdash (\varphi \to \varphi) \to (\varphi \to \varphi)$. If M is the corresponding λ-term, it is the <u>function</u>

$$\mathcal{L}_c(\mathbb{1}, \varphi \to \varphi) \xrightarrow{M \circ -} \mathcal{L}_c(\mathbb{1}, \varphi \to \varphi)$$

$$\begin{tikzcd} & \mathbb{1} \arrow[dl, dashed] \arrow[dr, dashed] & \\ (\varphi \to \varphi) \arrow[rr, "M"'] & & (\varphi \to \varphi) \end{tikzcd} \qquad (10.1)$$

and, finally, if $m \neq n$ then P_m and P_n determine different functions in (10.1) for a generic φ.

says $x \notin \Gamma$ below

<u>Remark</u> η-equivalence, i.e. $\lambda x^{\xi}.(M\,x) \sim M$ for $x \notin FV(M)$ corresponds to

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma, x:\xi \vdash \xi \to \psi\end{array} \qquad \dfrac{}{\Gamma, x:\xi \vdash \xi}\,Ax}{\Gamma, x:\xi \vdash \psi}\,{\to}E}{\Gamma \vdash \xi \to \psi}\,{\to}I \quad \sim \quad \begin{array}{c}\vdots\\ \Gamma, x:\xi \vdash M\end{array}$$

Regarding the <u>relevance</u> of the Curry-Howard correspondence we leave the last word to Girard from [G, §3.6].

3.6 Relevance of the isomorphism

Strictly speaking, what was defined in 3.5 is a bijection. We cannot say it is an isomorphism: this requires that structures of the same kind already exist on either side.

In fact the tradition of normalisation exists independently for natural deduction: a proof is normal when it does not contain any sequence of an introduction and an elimination rule:

$$\dfrac{\dfrac{\overset{\vdots}{A} \qquad \overset{\vdots}{B}}{A \wedge B}\,\wedge\mathcal{I}}{A}\,\wedge 1\mathcal{E} \qquad\qquad \dfrac{\dfrac{\overset{\vdots}{A} \qquad \overset{\vdots}{B}}{A \wedge B}\,\wedge\mathcal{I}}{B}\,\wedge 2\mathcal{E} \qquad\qquad \dfrac{\overset{\vdots}{A} \qquad \dfrac{\overset{[A]}{\overset{\vdots}{B}}}{A \Rightarrow B}\,{\Rightarrow}\mathcal{I}}{B}\,{\Rightarrow}\mathcal{E}$$

For each of these configurations, it is possible to define a notion of *conversion*. In chapter 2, we *identified* deductions by the word "equals"; we now consider these identifications as *rewriting*, the left member of the equality being rewritten to the right one.

That we have an isomorphism follows from the fact that, modulo the bijection we have already introduced, the notions of *conversion*, *normality* and *reduction* introduced in the two cases (and independently, from the historical viewpoint) correspond perfectly. In particular the *normal form theorem* we announced in 3.4 has an exact counterpart in natural deduction. We shall discuss the analogue of *head normal forms* in section 10.3.1.

Having said this, the interest in an isomorphism lies in a difference between the two participants, otherwise what is the point of it? In the case which interests us, the functional side possesses an operational aspect alien to formal proofs. The proof side is distinguished by its logical aspect, *a priori* alien to algorithmic considerations.

The comparison of the two alien viewpoints has some deep consequences from a methodological point of view (technically none, seen at the weak technical level of the two traditions):

- All good (constructive) logic must have an operational side.
- Conversely, one cannot work with typed calculi without regard to the implicit symmetries, which are those of Logic. In general, the "improvements" of typing based on logical atrocities do not work.

Basically, the two sides of the isomorphism are undoubtedly the the same object, accidentally represented in two different ways. It seems, in the light of recent work, that the “proof” aspect is less tied to contingent intuitions, and is the way in which one should *study* algorithms. The functional aspect is more eloquent, more immediate, and should be kept to a heuristic rôle.