Course Notes
“An Introduction to Proof Equivalence”

ESSLLI 2023

Classes 1 & 2: 07/08.

Matteo Acclavio & Paolo Pistone

1 Class 1. An Overview on the Proof Equivalence Problem

1.1 Proof theory

First of all, this is a course in proof theory. This is a branch of logic that, broadly speaking, has to do with understanding (mathematical) proofs. Hilbert was among the first to speak of “proof theory” as a discipline, in the context of his research programme aiming at establishing the consistency of mathematics. Put in other words, Hilbert’s goal was to establish the following result

In mathematics there exists *no* proof of a contradiction.

Proving a result of this kind required a precise, mathematical, definition of what a proof is, and, notably, of what a proof of a contradiction would be. The situation was not so different from what was happening more or less in the same years around the notion of computation. In order to establish his famous result, stating that there exist mathematical functions which are *not* computable, Turing had to come out with a precise, mathematical, definition of what a computable function is.

As is well-known, Hilbert’s programme was refuted by Gödel’s incompleteness theorems. Yet, proof theory survived the failure of its original motivation. Notably, through the work of logicians like Gentzen and Herbrand (who still reasoned within the perspective of Hilbert’s programme), and, later, of Prawitz, Kreisel, Martin-Löf, Girard, and many others, proof theory has evolved into a rich discipline concerning the formal representation and the structural properties of mathematical proofs.

Prawitz introduced in a series of papers [4, 5, 6] the notion of *general proof theory* to refer to “a study of proofs in their own right where one is interested in general questions about the nature and structure of proofs [...]” [6, p. 11], as opposed to *reductive proof theory*, that is, the study of proof systems aimed at establishing *relative* consistency proofs (i.e. Hilbert’s programme after Gödel). Other texts (e.g. [7]) rather use the term *structural proof theory*.

1.2 “No entity without identity”

Following Prawitz, among the general questions addressed by general proof theory, we have:

> Obvious topics in general proof theory are:
> 2.1. The basic question of defining the notion of proof, including the question of the distinction between different kinds of proofs such as constructive proofs and classical proofs.
> 2.2. Investigation of the structure of (different kinds of) proofs, including e.g. questions concerning the existence of certain normal forms.
> 2.3. The representation of proofs by formal derivations. In the same way as one asks when two formulas define the same set or two sentences express the same proposition, one asks when two derivations represent the same proof; in other words, one asks for identity criteria for proofs or for a “synonymity” (or equivalence) relation between derivations. [4, p. 237]

In this course we will be concerned with question 2.3. As we will see, Prawitz not only raised this questions, but he also proposed a mathematically precise answer to it. For the moment, let us take a closer look at this problem, that we will call the problem of *identity of proofs* [1, 11] or *proof equivalence* (we could also call it “proof synonymity”, following Prawitz again).

The famous philosopher Quine is well-known for maintaining the view that it makes sense to speak of a certain class of entities only if we are capable of specifying when two entities of this class are the same. In mathematics this is just common view: any well-defined class of mathematical entities (e.g. groups or topological spaces, etc.) comes with its own notion of identity (group isomorphisms, homeomorphisms, etc.).

Yet, when it comes to considering proofs, things are quite less clear. Mathematicians usually have some grasp about one proof being "simpler" or "more elegant" than one other. Hilbert himself had considered a 24th problem to be added to his famous 1900 list of 23 problems for the century, asking to "find criteria of simplicity or rather prove the greatest simplicity of given proofs." (see e.g. [10, 8]). However, translating such intuitions into mathematically precise terms is hard, or maybe just meaningless, and this for at least one important reason: in (general?) proof theory one will hardly encounter a truly general definition of proof. Rather, one can find many different definitions of proofs *within a certain formal system.* In this course we will discuss a few formal systems: sequent calculus, natural deduction, proof nets, combinatorial proofs, etc. Notably, we will see that, for a chosen formal system, one can often find different derivations which represent "intuitively", or "morally", the same proof.

When considering a notion of proof equivalence, we have to distinguish between two different situations:

- Proof equivalence *within a fixed formal system.* For example the following simple argument:

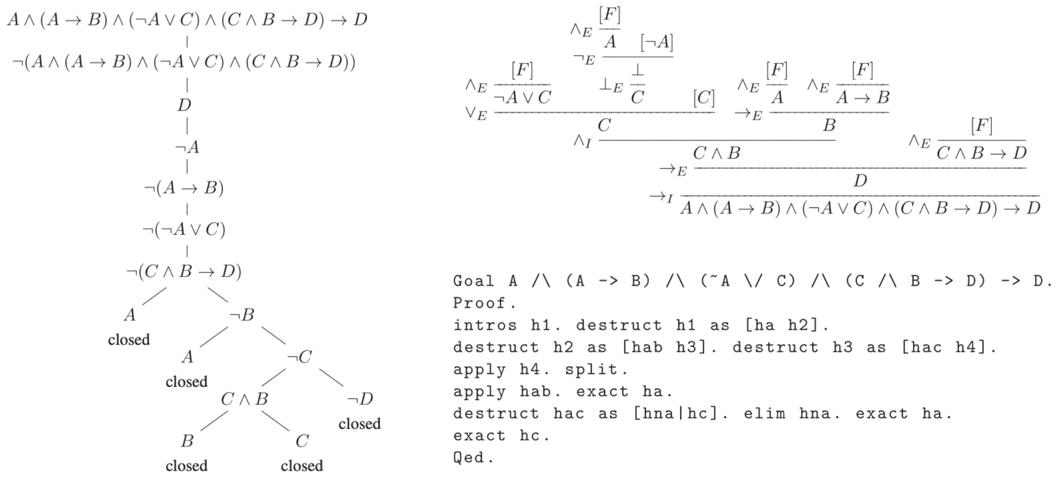
  Claim: if "A" holds, and "C implies B" holds, then "C implies A and B" holds.
  Proof. Suppose C holds. The validity of "A and B" follows then from the validity of "A" and the validity of "B", where the validity of the latter is a consequence of the validity of "C implies B" and the assumption "C"

  can be represented in sequent calculus via two distinct derivations:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,ax \qquad \dfrac{}{B \vdash B}\,ax}{A, B \vdash A \wedge B}\,\wedge\mathrm{R} \qquad \dfrac{}{C \vdash C}\,ax}{A, C \to B, C \vdash A \wedge B}\,\to\mathrm{L}}{A, C \to B \vdash C \to (A \wedge B)}\,\to\mathrm{R} \qquad \dfrac{\dfrac{\dfrac{}{A \vdash A}\,ax \qquad \dfrac{\dfrac{}{B \vdash B}\,ax \qquad \dfrac{}{C \vdash C}\,ax}{C \to B, C \vdash B}\,\to\mathrm{L}}{A, C \to B, C \vdash A \wedge B}\,\wedge\mathrm{R}}{A, C \to B \vdash C \to (A \wedge B)}\,\to\mathrm{R} \tag{1}$$

  These kind of examples can highlight inessential or "bureaucratic" aspects in some formal system, and may suggest alternative, more *canonical*, proof representations.

- Proof equivalence *across different formal systems*: for instance, the following three derivations (from up left to right down, in a tableaux system, natural deduction or Coq), taken from [8]:


$A \wedge (A \to B) \wedge (\neg A \vee C) \wedge (C \wedge B \to D) \to D$
$\neg(A \wedge (A \to B) \wedge (\neg A \vee C) \wedge (C \wedge B \to D))$
D
$\neg A$
$\neg(A \to B)$
$\neg(\neg A \vee C)$
$\neg(C \wedge B \to D)$
A
closed
$\neg B$
A
closed
$\neg C$
$C \wedge B$
$\neg D$
closed
B
closed
C
closed
$[F]$ $\wedge_E$ A $[\neg A]$ $\neg_E$ $\bot$ $\bot_E$ C
$[F]$ $\wedge_E$ $\neg A \vee C$ $[C]$ $\vee_E$ C
$[F]$ $\wedge_E$ A $[F]$ $\wedge_E$ $A \to B$ $\to_E$ B
$\wedge_I$ $C \wedge B$
$[F]$ $\wedge_E$ $C \wedge B \to D$
$\to_E$ D
$\to_I$ $A \wedge (A \to B) \wedge (\neg A \vee C) \wedge (C \wedge B \to D) \to D$

```
Goal A /\ (A -> B) /\ (~A \/ C) /\ (C /\ B -> D) -> D.
Proof.
intros h1. destruct h1 as [ha h2].
destruct h2 as [hab h3]. destruct h3 as [hac h4].
apply h4. split.
apply hab. exact ha.
destruct hac as [hna|hc]. elim hna. exact ha.
exact hc.
Qed.
```

  all represent, intuitively, the same argument showing the validity of the formula

$$(A \wedge (A \to B) \wedge (\neg A \vee C) \wedge (C \wedge B \to D)) \to D.$$

1.3 How Hard is Proof Equivalence?

Understanding if two derivations denote the same proof may be *hard.* As is well known, computability theory and complexity theory provide us with several *degrees* of hardness:

polynomial time a problem may be considered, so to say, "not too hard", when we can devise an algorithm that answers the problem within a reasonable (say, a polynomial) amount of time;

decidable, but not polytime a problem is "too hard" when, at least as far as we know, all algorithms what may answer it require an unreasonable (say, more than polynomial) amount of time to be executed.

undecidable Finally, as mentioned above, Turing proved the existence of problems which are "way too hard" to solve: *no* algorithm is capable of answering to them.

During the course we will meet proof systems for which the proof equivalence problem is "not too hard", "too hard" and "way too hard". How should we react to this? Does it make sense to study a notion of equivalence between proofs, when there is no reasonable or actual way to establish that this equivalence holds? Notice that this is more of a philosophical than a mathematical question: to produce an answer to it, much depends on the kind of philosophical stance we have towards the problem of identity of proof. For instance, under a more *platonist* view, we can postulate that proofs exist in some sense as abstract objects, of which mathematicians have a certain grasp, and that formal derivations are linguistic objects that *refer* to such objects. Hence, understanding the identity of proof relations means understanding when two formal derivations refer to the same proof, just like, say, the numerical expressions $6 + 5$ and $(3 \times 4) - 1$ both refer to the same entity, the number 11. Under this view, the hardness of the problem, although interesting in itself, is not crucial. For example, understanding equality of real numbers (typically, does $x = \pi$?) is a well-known undecidable problem, yet mathematicians did not stop doing real analysis just for that!

By contrast, under a more *deflationist* view, we may remain agnostic as to the existence of proofs as abstract entities; understanding the identity of proof relation would mean then finding reasonable ways to abstract away from inessential or "bureaucratic" differences that appear in formal systems, possibly paving the way for the development of more *canonical* proof systems. In this sense, whether a notion of proof equivalence is hard is important, because it is unreasonable that a workable proof system can be produced out of some hardly computable notion!

2 Class 2. Proof Systems: Natural Deduction and Sequent Calculus

The two most studied proof systems were both introduced by Gentzen in his 1934 PhD thesis. We will briefly recall these formalisms and discuss how they lead to introduce two different criteria for proof equivalence, that we call the *normalization criterion* (NC) and the *permutation criterion* (PC).

It is useful to start our discussion with some fundamental questions that motivate the work of logicians around the notion of proof equivalence can be formulated as follows:

Question 1 Are the normalization and permutation criteria equivalent?

Question 2 Is there a mathematical interpretation of proofs such that, whenever two proofs are equivalent (in one of the two senses above), then their interpretations coincide?

Question 3 Is any of these criteria decidable? Or even decidable in a reasonable time?

Let us fix a standard propositional language $\mathcal{L}$, with formulas defined by the grammar

$$A ::= p \in \mathcal{P} \mid \mathbf{T} \mid \mathbf{F} \mid A \wedge B \mid A \vee B \mid A \to B$$

where $\mathcal{P}$ is a denumerable collection of propositional variables. As usual, we define $\neg A := A \to \mathbf{F}$.

2.1 Natural Deduction and the Normalization Criterion

A derivation in natural deduction is a labeled rooted tree whose leaves are called *hypotheses* and whose root is called the *conclusion* of the tree. We use the notation $\Pi : H_1, \dots, H_n \vdash C$ to indicate a derivation Π of hypotheses $H_1, \dots, H_n$ and conclusion C. More graphically, we may note Π as

$$\begin{matrix} H_1, \dots, H_n \\ \Pi \\ C \end{matrix}$$

As a basic example let us consider the following derivation of $B \to C, A \to B \vdash A \to C$:

$$\dfrac{\dfrac{\overset{0}{B \to C} \qquad \dfrac{\overset{1}{A \to B} \qquad \overset{2}{A}}{B}\,{\to}\mathrm{E}}{C}\,{\to}\mathrm{E}}{A \to C}\,{\to}\mathrm{I}(2)$$

Importantly, while a conclusion of a derivation is just a plain formula of $\mathcal{L}$, an hypothesis is a *labeled* formula $\overset{i}{A}$, where A is a formula of $\mathcal{L}$ and i is an index taken from $\mathbb{N}$. Hence, the hypothesis $\overset{0}{A}$ is distinct from the hypothesis $\overset{3}{A}$. This apparently arbitrary notation will be made clear in a moment.

Let us now introduce the system **NJ** of natural deduction for intuitionistic propositional logic. We define inductively a notion of *pre-derivation* via four different operations:

1. An *assumption* is a derivation of hypothesis $\overset{i}{A}$ and conclusion A. As explained below, an assumption may be *discharged* or *undischarged* in a derivation Π depending on whether the index i is invoked by some other rule of Π.

2. An *introduction rule* is a rule that combines a finite number of derivations to produce a new one whose conclusion is either of the form $\mathbf{T}$ or of the form $A \circ B$, where $\circ$ is one of the logical operators $\wedge, \vee, \to$. The introduction rules of **NJ** are defined as follows:

$$\frac{}{\mathbf{T}}\,\mathbf{TI} \qquad\qquad \frac{A \qquad B}{A \wedge B}\wedge\mathrm{I} \qquad\qquad \frac{A_i}{A \vee B}\vee\mathrm{I}_i \quad (i \in \{0,1\}) \qquad\qquad \frac{\begin{matrix}[\overset{i}{A}]\\ \vdots \\ B\end{matrix}}{A \to B}\to\mathrm{I}(i)$$

The rule $\to$I requires some explanation: in a derivation there might occur several instances of an assumption A, each with its own index (e.g. one with index 0, two with index 3, three with index 5); the introduction rule $\to$I with index (i) *discharges* all assumptions with index i. In this way it becomes possible to discharge, by a single rule, *a finite number* of uses of the assumption A, *yet not necessarily all* of them. Notice that, when an assumption is discharged, its premiss no more plays the role of an hypothesis of the derivation. In other words, given a derivation Π of hypotheses $\Gamma, \overset{i}{A}$ and conclusion B, the rule $\to$I produces a derivation Π' of hypotheses Γ and conclusion $A \to B$.
For example, in the following pre-derivations of $A \to (A \to B) \vdash A \to B$, the rule $\to$I discharges *two* occurrences of an assumption:

$$\dfrac{\dfrac{\dfrac{\overset{0}{A \to (A \to B)} \qquad \overset{1}{A}}{A \to B}\to\mathrm{E} \qquad \overset{1}{A}}{B}\to\mathrm{E}}{A \to B}\to\mathrm{I}(1)$$

The following two pre-derivations of $\vdash A \to (A \to A)$ are *not equivalent*, as their use of indexes is different:

$$\dfrac{\dfrac{\overset{0}{A}}{A \to A}\to\mathrm{I}(1)}{A \to (A \to A)}\to\mathrm{I}(0) \qquad\qquad \dfrac{\dfrac{\overset{1}{A}}{A \to A}\to\mathrm{I}(1)}{A \to (A \to A)}\to\mathrm{I}(0) \tag{2}$$

3. An *elimination rule* is a rule that combines a pre-derivation whose conclusion is either $\mathbf{T}$ or of the form $A \circ B$, with $\circ$ one of the logical operators $\wedge, \vee, \to$, with possibly other derivations, to produce a new pre-derivation. The elimination rules of **NJ** are.

$$\frac{\mathbf{F}}{A}\,\mathbf{FE} \qquad \frac{A_0 \wedge A_1}{A_i}\wedge\mathrm{E}_i \quad (i \in \{0,1\}) \qquad \frac{A \vee B \qquad \begin{matrix}\overset{i}{A}\\ \vdots \\ C\end{matrix} \qquad \begin{matrix}\overset{j}{B}\\ \vdots \\ C\end{matrix}}{C}\vee\mathrm{E}(i,j) \qquad \frac{A \to B \qquad A}{B}\to\mathrm{E}$$

Observe that the rule $\vee$E discharges two assumptions.

The use of indexes is important but introduces some sort of “bureaucracy”: in particular, it leads to distinguish proofs which are “morally” the same. For instance the following two pre-derivations are different, since they use distinct indexes, but should certainly represent the same proof:

$$\frac{\overset{0}{A}}{A \to A}\to\mathrm{I}(0) \qquad\qquad \frac{\overset{1}{A}}{A \to A}\to\mathrm{I}(1)$$

For this reason, we introduce an equivalence relation $\sim$ over pre-derivations, where, given two derivations Π, Π' with same hypotheses and same conclusion, $\Pi \sim \Pi'$ holds when Π' can be obtained from Π' by a suitable *renaming* of its indexes. We define a *derivation* of **NJ** as an equivalence class of pre-derivations modulo the equivalence $\sim$. In this way the two pre-derivations above are instances of the same derivations, while the two derivations in (2) are not.

The system **NK** of natural deduction for *classical* logic can be obtained from **NJ** simply by adding one new rule:

- A *double negation rule* which implements the usual classical tautology $\neg\neg A \to A$:

$$\frac{\neg\neg A}{A}\,\mathrm{DN}.$$

Notice, however, that this rule does not belong to the three classes of rules of **NJ**, and indeed it sensibly alters the structural properties of the calculus. For this reason, we will for the moment restrict ourselves to **NJ**.

Normalization A fundamental discovery of Gentzen was that proofs not only have rules, but they also have a *dynamics*: it is possible to define transformations over proofs that may eliminate certain "redundancies". In the case of natural deduction, a redundancy, or *local peak*, is a configuration of the form

$$\dfrac{\dfrac{\vdots}{A \circ B}\,\circ\,\mathrm{I}}{\vdots}\,\circ\,\mathrm{E}$$

where a logical operator $\circ$ is first introduced and then immediately eliminated. Examples of such peaks are

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ A\end{array}\quad\begin{array}{c}\vdots\\ B\end{array}}{A \wedge B}\,\wedge\mathrm{I}}{A}\,\wedge\mathrm{E}_1 \qquad\qquad \dfrac{\dfrac{\begin{array}{c}\overset{i}{A}\\ \vdots\\ B\end{array}}{A \to B}\,{\to}\mathrm{I}(i)\quad \begin{array}{c}\vdots\\ A\end{array}}{B}\,{\to}\mathrm{E}$$

In each case the conclusion to be proved had already been attained *before* introducing (and eliminating) the redundancy.

The process by which redundancies are eliminated is called *normalization* and is defined via a finite set of transformations $\rightsquigarrow$, e.g.:

$$\dfrac{\dfrac{\begin{array}{c}\Pi_1\\ A\end{array}\quad\begin{array}{c}\Pi_2\\ B\end{array}}{A \wedge B}\,\wedge\mathrm{I}}{A}\,\wedge\mathrm{E}_1 \quad\rightsquigarrow\quad \begin{array}{c}\Pi_1\\ A\end{array}$$

$$\dfrac{\dfrac{\begin{array}{c}\overset{i}{A}\\ \Pi_1\\ B\end{array}}{A \to B}\,{\to}\mathrm{I}(i)\quad \begin{array}{c}\Pi_2\\ A\end{array}}{B}\,{\to}\mathrm{E} \quad\rightsquigarrow\quad \begin{array}{c}\Pi_2\\ [A]\\ \Pi_1\\ B\end{array}$$

where in the second rule the square brackets $[A]$ signal the fact that the hypothesis $\overset{i}{A}$ may occur *several times* in Π_1, and thus we are attaching a copy of Π_2 on top of *each of* these occurrences. In other words, we are possibly *duplicating* Π (if $\overset{i}{A}$ occurs more than one time) or *deleting* if (if $\overset{i}{A}$ does not occur at all).

A derivation is called *normal* if no transformation can be applied to it. The reflexive and transitive closure $\rightsquigarrow^*$ of $\rightsquigarrow$ defines then a *reduction* relation between derivation, and the following fundamental result holds:

Theorem 1 (normalization)**.** *For any derivation* Π *of* **NJ** *there exists a* unique *normal derivation* $\mathrm{nf}(\Pi)$ *such that* $\Pi \rightsquigarrow^* \mathrm{nf}(\Pi)$.

We will go back at this result in the following classes. For the moment, it is important to observe that, when a derivation Π can be transformed in Π' just by eliminating some "redundant" steps, one might reasonably think that Π and Π' should represent the same logical argument, with Π' representing it in a more direct way. In particular, one can think of normal derivations as standing in the most direct relation with the corresponding proofs, and, in view of Theorem 1, of any other derivation as referring to the same proof referred to by its normal form. This is precisely the view introduced by Prawitz in [4], which leads to

Definition 1 (Normalization Criterion for Proof Equivalence (NC))**.** *Let* Π, Π' *be two derivations in* **NJ** *with same hypotheses and same conclusion. Then* Π *and* Π' *are* normalization-equivalent *(noted* $\Pi \equiv_{\mathrm{NC}} \Pi'$*) iff* $\mathrm{nf}(\Pi) = \mathrm{nf}(\Pi')$.

The normalization criterion is probably the most well-studied notion of proof equivalence. It certainly has the merit of providing a mathematically precise definition of proof equivalence, which can be extended to many other proof systems beyond **NJ**.

We will study this criterion for natural deduction derivations in more details in a future lesson. For the moment, let us mention two of its main weak points:

- Its relies on the fact of having a proof system enjoying existence and unicity of normal form (something which is not trivial to have in many situations, as we will see).
- Even if normal forms exist, already in **NJ** the procedure to transform an arbitrary derivation into normal form needs not be feasible in polynomial time. This means that checking if two derivations are normalization-equivalent may be "too hard", in particular, not feasible in polynomial time.

Identity Group

$$\frac{}{A \vdash A}\,\mathrm{ax} \qquad \frac{\Gamma \vdash A, \Delta \qquad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\,\mathrm{cut}$$

Structural Group

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\,\mathrm{LW} \qquad \frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\,\mathrm{LC} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}\,\mathrm{RW} \qquad \frac{\Gamma \vdash, A, A\Delta}{\Gamma \vdash A, \Delta}\,\mathrm{RC}$$

Logical Group

$$\frac{}{\vdash \mathbf{T}}\,\mathrm{R}\mathbf{T} \qquad \frac{}{\mathbf{F} \vdash}\,\mathrm{L}\mathbf{F}$$

$$\frac{\Gamma, A_i \vdash \Delta}{\Gamma, A_0 \wedge A_1 \vdash \Delta}\,\mathrm{L}\wedge_i \qquad \frac{\Gamma, A \vdash \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma, A \vee B \vdash \Delta}\,\mathrm{L}\vee \qquad \frac{\Gamma \vdash A, \Delta \qquad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta}\,\mathrm{R}\wedge \qquad \frac{\Gamma \vdash A_i, \Delta}{\Gamma \vdash A_0 \vee A_1, \Delta}\,\mathrm{R}\vee_i$$

$$\frac{\Gamma \vdash A, \Delta \qquad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \to B \vdash \Delta, \Delta'}\,\mathrm{L}\!\to \qquad \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}\,\mathrm{R}\!\to$$

Figure 1: Rules of **LK**.

The Functional Interpretation Another advantage of restricting ourselves to **NJ** is that derivations in intuitionistic logic admit an interpretation in terms of *functional programs* (also known as the *Curry-Howard correspondence*). First, it is possible to interpret any formula A of $\mathcal{L}$ as a certain *type* of objects $[\![A]\!]$:

- $[\![\mathbf{T}]\!]$ is the type containing precisely one object;
- $[\![\mathbf{F}]\!]$ is the empty type;
- $[\![A \wedge B]\!]$ is the type of pairs (a, b), where $a \in [\![A]\!]$ and $b \in [\![B]\!]$ (also called product type);
- $[\![A \vee B]\!]$ is the type of pairs (i, c) where either $i = 0$ and $c \in [\![A]\!]$, or $i = 1$ and $c \in [\![B]\!]$ (also called disjoint sum type, or coproduct type);
- $[\![A \to B]\!]$ is the type of programs f transforming any object of type $[\![A]\!]$ into an objet of type $[\![B]\!]$.

Now, with any derivation $\Pi : \Gamma \vdash A$ it is possible to associate a certain program

$$[\![\Pi]\!] : [\![\Gamma]\!] \longrightarrow [\![B]\!]$$

yielding, for any object a of type $[\![\Gamma]\!]$, an object $[\![\Pi]\!](a) \in [\![B]\!]$. For instance, the two programs associated with the derivations Π_1, Π_2 in (2) correspond to the projections $\pi_1, \pi_2 : [\![A]\!] \times [\![A]\!] \to [\![A]\!]$:

$$\pi_1 : a, b \mapsto a \qquad\qquad \pi_2 : a, b \mapsto b$$

We will not enter into more details here, but one can define a precise correspondence between derivations in **NJ** and programs in the *simply typed λ-calculus.* More on this will be discussed in Giulio Guerrieri's course.

2.2 Sequent Calculus and the Permutation Criterion

We now recall the second formalism introduced by Gentzen. As we observed, most structural properties of natural deduction (like the normalization theorem) are lost when we consider the system **NK** for classical logic. It is precisely with the purpose of managing the inner symmetries of classical reasoning that Gentzen introduced a different proof system.

A *sequent* is an expression of the form $\Gamma \vdash \Delta$, where Γ, Δ are finite multisets of formulas. A derivation in sequent calculus is simply a finite tree whose nodes are labeled by sequents. Compared to natural deduction, sequent calculus derivations involve no additional "bureaucracy" concerning indexes and assumption discharge.

The sequent calculus **LK** for classical logic is defined by the rules illustrated in Fig. 1.

The first group comprises a basic "axiom" rule as well as the cut rule, probably the most significant rule of the calculus, as we will see. The second group comprises left and right rules for *weakening* and *contraction*, that is, to handle the possible duplication and erasing of formulas. The third group comprises, for each logical operator, a left and a right rule, loosely related to the introduction and elimination rules of **NJ**.

A calculus **LJ** for intuitionistic logic is defined simply by restricting **LK** to sequents of the form $\Gamma \vdash \Delta$, where Δ has *at most* one formula.

Cut-elimination The dynamics of sequent calculus focuses on the cut-rule. Indeed, the "redundancies" in this case can be identified with the occurrences of this rule. *Cut-elimination* is the process by which an arbitrary derivation can be transformed into one in which the cut-rule never occurs. Similarly to natural deduction, this is achieved by defining a class of transformations $\rightsquigarrow$, like for example:

$$\dfrac{\dfrac{\overset{\Pi_1}{\Gamma \vdash A, \Delta} \qquad \overset{\Pi_1}{\Gamma \vdash B, \Delta}}{\Gamma \vdash A \wedge B, \Delta}\,\mathrm{R}\wedge \qquad \dfrac{\overset{\Sigma}{\Gamma', A \vdash \Delta'}}{\Gamma', A \wedge B \vdash \Delta'}\,\mathrm{L}\wedge}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\,\mathrm{cut} \qquad \rightsquigarrow \qquad \dfrac{\overset{\Pi_1}{\Gamma \vdash A, \Delta} \qquad \overset{\Sigma}{\Gamma', A \vdash \Delta'}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\,\mathrm{cut}$$

that transforms a cut on the complex formula $A \wedge B$ into a cut on the simpler formula A.

Letting, as before, $\rightsquigarrow^*$ indicate the reflexive-transitive closure of $\rightsquigarrow$, we have the following fundamental result:

Theorem 2 (Hauptsatz)**.** *For any derivation Π of* **LK** *there exists a normal derivation Π' such that $\Pi \rightsquigarrow^* \Pi'$.*

Observe that, unlike in the case of **NJ**, normal forms in **LK** are *not* in general unique. In particular, the algorithm transforming a derivation into a normal is truly *non-deterministic*. This is one of the reasons that makes sequent calculus a less ideal candidate than natural deduction for the normalization criterion.

Rule Permutations Beyond the failure of unicity of normal forms, that (NC) is not well-adapted to sequent calculus is best seen by observing that different derivations in sequent calculus may well correspond to *the same* natural deduction derivation.

To see this, let us define a translation from **LJ** to **NJ**: to a derivation Π in **LJ** of conclusion $\Gamma \vdash \Delta$, with $\sharp\Delta \leqslant 1$, we associate a derivation $\Pi^* : \Gamma^\sharp \vdash \Delta^\flat$ in **NJ**, where $\Gamma^\sharp$ contains the formulas in Γ, each with a distinct index, and $\Delta^\flat$ is Δ if the latter contains one formula, and is $\mathbf{F}$ otherwise. The translation is defined inductively as follows:

$$\dfrac{}{A \vdash A}\,\mathrm{ax} \qquad \mapsto \qquad \overset{i}{A}$$

$$\dfrac{\overset{\Pi_1}{\Gamma \vdash A} \qquad \overset{\Pi_2}{\Gamma', A \vdash \Delta}}{\Gamma, \Gamma' \vdash \Delta'}\,\mathrm{cut} \qquad \mapsto \qquad \begin{array}{cc} & \Gamma^\sharp \\ & \Pi_1^* \\ (\Gamma')^\sharp & [A] \\ \multicolumn{2}{c}{\Pi_2^*} \\ \multicolumn{2}{c}{\Delta^\flat} \end{array}$$

$$\dfrac{\overset{\Pi}{\Gamma \vdash \Delta}}{\Gamma, A \vdash \Delta}\,\mathrm{LW} \qquad \mapsto \qquad \Pi^*$$

$$\dfrac{\overset{\Pi}{\Gamma, A, A \vdash \Delta}}{\Gamma, A \vdash \Delta}\,\mathrm{LC} \qquad \mapsto \qquad \begin{array}{ccc} \Gamma^\sharp & \overset{i}{A} & \overset{j}{A} \\ & \Pi^* & \\ & \Delta^\flat & \end{array} \left[j \mapsto i \right]$$

$$\dfrac{\overset{\Pi}{\Gamma \vdash}}{\Gamma \vdash A}\,\mathrm{RW} \qquad \mapsto \qquad \begin{array}{c} \Gamma^\sharp \\ \Pi^* \\ \dfrac{\mathbf{F}}{A}\,\mathbf{F}\mathrm{E} \end{array}$$

$$\dfrac{}{\vdash \mathbf{T}}\,\mathrm{R}\mathbf{T} \qquad \mapsto \qquad \dfrac{}{\mathbf{T}}\,\mathbf{T}\mathrm{I}$$

$$\dfrac{}{\mathbf{F} \vdash}\,\mathrm{L}\mathbf{F} \qquad \mapsto \qquad \overset{i}{\mathbf{F}}$$

$$\dfrac{\overset{\Pi}{\Gamma, A_i \vdash \Delta}}{\Gamma, A_0 \wedge A_1 \vdash \Delta}\,\mathrm{L}\wedge_i \qquad \mapsto \qquad \begin{array}{cc} \Gamma^\sharp & \dfrac{\overset{i}{A_0 \wedge A_1}}{A_i}\,\wedge\mathrm{E}_i \\ \multicolumn{2}{c}{\Pi^*} \\ \multicolumn{2}{c}{\Delta^\flat} \end{array}$$

$$\dfrac{\overset{\Pi_1}{\Gamma, A \vdash \Delta} \qquad \overset{\Pi_2}{\Gamma, B \vdash \Delta}}{\Gamma, A \vee B \vdash \Delta}\,\mathrm{L}\vee \qquad \mapsto \qquad \dfrac{\overset{i}{A \vee B} \qquad \begin{array}{cc} \Gamma^\sharp & \overset{j}{A} \\ \multicolumn{2}{c}{\Pi_1^*} \\ \multicolumn{2}{c}{\Delta^\flat} \end{array} \qquad \begin{array}{cc} \Gamma^\sharp & \overset{k}{B} \\ \multicolumn{2}{c}{\Pi_2^*} \\ \multicolumn{2}{c}{\Delta^\flat} \end{array}}{\Delta^\flat}\,\vee\mathrm{E}(j,k)$$

$$\dfrac{\begin{matrix}\Pi_1\\ \Gamma\vdash A\end{matrix}\qquad \begin{matrix}\Pi_2\\ \Gamma\vdash B\end{matrix}}{\Gamma\vdash A\wedge B,\Delta}\,\mathrm{R}\wedge \qquad\mapsto\qquad \dfrac{\begin{matrix}\Gamma^\sharp\\ \Pi_1^*\\ A\end{matrix}\qquad \begin{matrix}\Gamma^\sharp\\ \Pi_2^*\\ B\end{matrix}}{A\wedge B}\,\wedge\mathrm{I}$$

$$\dfrac{\begin{matrix}\Pi\\ \Gamma\vdash A_i,\Delta\end{matrix}}{\Gamma\vdash A_0\vee A_1,\Delta}\,\mathrm{R}\vee_i \qquad\mapsto\qquad \dfrac{\begin{matrix}\Gamma^\sharp\\ \Pi^*\\ A_i\end{matrix}}{A_0\vee A_1}\,\vee\mathrm{I}_i$$

$$\dfrac{\begin{matrix}\Pi_1\\ \Gamma\vdash A\end{matrix}\qquad \begin{matrix}\Pi_2\\ \Gamma',B\vdash\Delta\end{matrix}}{\Gamma,\Gamma',A\to B\vdash\Delta}\,\mathrm{L}\to \qquad\mapsto\qquad (\Gamma')^\sharp \quad \begin{matrix}\dfrac{A\overset{i}{\to} B\qquad \begin{matrix}\Gamma^\sharp\\ \Pi_1^*\\ A\end{matrix}}{[B]}\,\to\mathrm{E}\\ \Pi_2^*\\ \Delta^\flat\end{matrix}$$

$$\dfrac{\begin{matrix}\Pi\\ \Gamma,A\vdash B,\Delta\end{matrix}}{\Gamma\vdash A\to B,\Delta}\,\mathrm{R}\to \qquad\mapsto\qquad \dfrac{\begin{matrix}\Gamma^\sharp\quad \overset{i}{A}\\ \Pi^*\\ B\end{matrix}}{A\to B}\,\to\mathrm{I}(i)$$

It is important to observe that the transformation has an *exponential cost*: the size of the translated derivation Π^* may be at most exponential in the size of Π. This is due to the translation of the rules cut and $\to$E, in which the sub-derivation Π_1^* is possibly duplicated.

Example 1. *The translation of the two distinct* **LJ**-*derivations below*

$$\Pi_1=\dfrac{\dfrac{\dfrac{\dfrac{}{A\vdash A}\,ax}{A,B\vdash A}\,w\qquad \dfrac{\dfrac{}{B\vdash B}\,ax}{A,B\vdash B}\,w}{A,B\vdash A\wedge B}\,\wedge R\qquad \dfrac{}{C\vdash C}\,ax}{A,C\to B,C\vdash A\wedge B}\,\to L \qquad\qquad \Pi_2=\dfrac{\dfrac{\dfrac{}{A\vdash A}\,ax}{A,C\to B,C\vdash A}\,w\qquad \dfrac{\dfrac{}{B\vdash B}\,ax\qquad \dfrac{}{C\vdash C}\,ax}{C\to B,C\vdash B}\,\to L}{A,C\to B,C\vdash A\wedge B}\,\wedge R$$

is the following unique **NJ**-*derivation* $\Pi_1^*=\Pi_2^*$*:*

$$\dfrac{\overset{i}{A}\qquad \dfrac{\overset{j}{C\to B}\qquad \overset{k}{C}}{B}\,\to E}{A\wedge B}\,\wedge I$$

As this example suggests (and as we will see in more detail in a future class) **NJ** provides a more canonical representation of intuitionistic proofs than **LJ**. At the same time, checking proof-equivalence in **LJ** by translation into **NJ** is "too hard", as it comes with an exponential cost.

The problem with **LJ** derivations, as shown by the example above, is that one should consider derivations *up to admissible permutations of rules.* Even if we restrict to the fragment of **LJ** with only the connectives $\wedge$ and $\to$, we already have a long list of permutations. Indeed, these are of three forms:

1. An exchange between two consecutive rules focusing on *distinct* formulas, e.g. :

$$\dfrac{\Gamma\vdash A\qquad \dfrac{B,\Delta,C\vdash D}{B,\Delta\vdash C\to D}\,\mathrm{R}\to}{\Gamma,A\to B,\Delta\vdash C\to D}\,\mathrm{L}\to \qquad\sim_{\mathsf{p}}\qquad \dfrac{\dfrac{\Gamma\vdash A\qquad B,\Delta,C\vdash D}{\Gamma,A\to B,\Delta,C\vdash D}\,\mathrm{L}\to}{\Gamma,A\to B,\Delta\vdash C\to D}\,\mathrm{R}\to$$

2. Conversions between weakening/contraction and the rules for $\wedge$, illustrated in Fig. 2
3. Conversions between weakening/contraction and the rules for $\to$, illustrated in Fig. 3

Remark 1 (Size explosion)**.** *Observe that, while in all permutations of type 1. and 2. the* size *of the two related derivations is comparable, the permutations of type 3. lead to either a duplication or to the erasure of an entire sub-derivation. For this reason, a finite number applications of these rules may lead to an exponential growth of the resulting derivation.*

This suggests a second criterion for proof-equivalence:

Definition 2 (Permutation Criterion for Proof Equivalence (PC))**.** *Let* Π,Π' *be two derivations in* **LJ** *with the same conclusion. Then* Π *and* Π' *are* permutation-equivalent *(noted* $\Pi\equiv_{\mathrm{PC}}\Pi'$ *iff* $\Pi\sim_{\mathrm{p}}\Pi'$*.*

$$\dfrac{\dfrac{\dfrac{\Gamma, A, A, B, B \vdash C}{\Gamma, A, B, B \vdash C}\,\mathrm{LC}}{\Gamma, A, B \vdash C}\,\mathrm{LC}}{\Gamma, A \wedge B \vdash C}\,\mathrm{L}\wedge \qquad \sim_{\mathsf{p}} \qquad \dfrac{\dfrac{\dfrac{\Gamma, A, A, B, B \vdash C}{\Gamma, A \wedge B, A, B \vdash C}\,\mathrm{L}\wedge}{\Gamma, A \wedge B, A \wedge B \vdash C}\,\mathrm{L}\wedge}{\Gamma, A \wedge B \vdash C}\,\mathrm{LC}$$

$$\dfrac{\dfrac{\dfrac{\Gamma \vdash C}{\Gamma, A \vdash C}\,\mathrm{LW}}{\Gamma, A, B \vdash C}\,\mathrm{LW}}{\Gamma, A \wedge B \vdash C}\,\mathrm{L}\wedge \qquad \sim_{\mathsf{p}} \qquad \dfrac{\Gamma \vdash C}{\Gamma, A \wedge B \vdash C}\,\mathrm{LW}$$

$$\dfrac{\dfrac{\Gamma, A \vdash B}{\Gamma, A, A \vdash C}\,\mathrm{LW}}{\Gamma, A \vdash C}\,\mathrm{LC} \qquad \sim_{\mathsf{p}} \qquad \Gamma, A \vdash B$$

Figure 2: $\wedge$/C/W-conversions of **LJ** [9].

$$\dfrac{\Gamma \vdash A \qquad \dfrac{B, B, \Delta \vdash C}{B, \Delta \vdash C}\,\mathrm{LC}}{\Gamma, A \to B, \Delta \vdash C}\,\mathrm{L}{\to} \qquad \sim_{\mathsf{p}} \qquad \dfrac{\dfrac{\Gamma \vdash A \qquad \dfrac{\Gamma \vdash A \qquad B, B, \Delta \vdash C}{B, \Gamma, A \to B, \Delta \vdash C}\,\mathrm{L}{\to}}{\Gamma, A \to B, A \to B, \Delta \vdash C}\,\mathrm{L}{\to}}{\Gamma, A \to B, \Delta \vdash C}\,\mathrm{LC}$$

$$\dfrac{\Gamma \vdash A \qquad \dfrac{\Delta \vdash C}{B, \Delta \vdash C}\,\mathrm{LW}}{\Gamma, A \to B, \Delta \vdash C}\,\mathrm{L}{\to} \qquad \sim_{\mathsf{p}} \qquad \dfrac{\Delta \vdash C}{\Gamma, A \to B, \Delta \vdash C}\,\mathrm{LW}$$

Figure 3: $\to$/C/W-conversions of **LJ** [9].

In other words, Π is permutation-equivalent to Π' if it is possible to transform one into the other by applying a finite number of admissible permutations of rules.

Observe that, in view of Remark 1, checking permutation equivalence needs not be doable in polynomial time. If we think that complexity must be seriously considered in proof equivalence, it makes sense to study weaker notions of permutation-equivalence, e.g. by excluding permutations of type 3. We will go back at this.

Remark 2. *In the literature (e.g. [1]) one finds another proof equivalence criterion, called* generality criterion*. This criterion is tightly related to the permutation criterion. While its proper formulation relies on the language of category theory (in particular, on the notion of* coherence*), the fundamental idea behind the notion of generality (which is due to Lambek's [2, 3]) can be spelled as follows: given a proof of some formula $A[p_1, \dots, p_n]$, depending on propositional variables $p_1, \dots, p_n$, we may try to transform the proof by renaming such variables in a maximal way. For instance, the natural deduction derivation below:*

$$\dfrac{\dfrac{\dfrac{p \overset{0}{\wedge} p}{p}\wedge E_1 \qquad \dfrac{p \overset{i}{\wedge} p}{p}\wedge E_2}{p \wedge p}\wedge I}{(p \wedge p) \to (p \wedge p)}\to I(0)$$

can be "generalized" by distinguishing red and blue occurrences of p as follows:

$$\dfrac{\dfrac{\dfrac{p \overset{0}{\wedge} p}{p}\wedge E_1 \qquad \dfrac{p \overset{i}{\wedge} p}{p}\wedge E_2}{p \wedge p}\wedge I}{(p \wedge p) \to (p \wedge p)}\to I(0)$$

Instead, the derivation below

$$\dfrac{\dfrac{\dfrac{p \overset{0}{\wedge} p}{p}\wedge E_2 \qquad \dfrac{p \overset{i}{\wedge} p}{p}\wedge E_1}{p \wedge p}\wedge I}{(p \wedge p) \to (p \wedge p)}\to I(0)$$

yields the distinct coloring

$$\dfrac{\dfrac{\dfrac{p \overset{0}{\wedge} p}{p}\wedge E_2 \qquad \dfrac{p \overset{i}{\wedge} p}{p}\wedge E_1}{p \wedge p}\wedge I}{(p \wedge p) \to (p \wedge p)}\to I(0)$$

We can then take the produced coloring, or labeling, of the conclusion, as a way to distinguish between the two proofs. Two derivations would coincide then precisely when they produce the same coloring of their conclusion. This is, very roughly, the idea behind the generality criterion, and one can check that generality is invariant under rule permutations, which means that this criterion subsumes the permutation criterion.

References

[1] Kosta Došen. Identity of proofs based on normalization and generality. *The Bulletin of Symbolic Logic*, 9(4):477–503, 2003.

[2] Joachim Lambek. Deductive systems and categories I. Syntactic calculus and residuated categories. *Mathematical systems theory*, 2(4):287–318, 1968. URL: `https://doi.org/10.1007/BF01703261`, `doi:10.1007/BF01703261`.

[3] Joachim Lambek. Deductive systems and categories II. standard constructions and closed categories. In Hilton P.J., editor, *Category Theory, Homology Theory and their Applicataions I*, volume 86 of *Lecture Notes in Mathematics*, pages 76–122, Berlin, Heidelberg, 1969. Springer.

[4] Dag Prawitz. Ideas and results in proof theory. In J.E. Fenstad, editor, *Proceedings of the 2nd Scandinavian Logic Symposium (Oslo)*, volume 63 of *Studies in logic and foundations of mathematics*. North-Holland, 1971.

[5] Dag Prawitz. Towards a foundation of a general proof theory. *Logic, Methodology and Philosophy of Science*, VI, 1971.

[6] Dag Prawitz. On the idea of a general proof theory. *Synthese*, 27:63–77, 1974.

[7] Helmut Schwichtenberg and Anne Sjerp Troelstra. *Basic proof theory.* Cambridge University Press, 2000.

[8] Lutz Straßburger. The problem of proof identity and why computer scientists should care about Hilbert's 24th problem. *Philosophical Transactions of the Royal Society*, A 377, 2019.

[9] Lutz Straßburger, Willem Heijltjes, and Dominic J D Hughes. Intuitionistic proofs without syntax. In *LICS 2019 - 34th Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 1–13, Vancouver, Canada, 2019. IEEE.

[10] R Thiele. Hilbert's twenty-fourth problem. *American Mathematical Monthly*, 110:1–24, 2003.

[11] Luca Tranchini. Proof-theoretic harmony: towards an intensional account. *Synthese*, 198(5):1145–1176, 2021. `doi:10.1007/s11229-016-1200-3`.