What is a logic, and what is a proof?

Lutz Strassburger

October 23, 2006 — Version for the second edition of "Logica Universalis"

What is a logic, and what is a proof ?

Lutz Straßburger

Abstract. I will discuss the two problems of how to define identity between logics and how to define identity between proofs. For the identity of logics, I propose to simply use the notion of preorder equivalence. This might be considered to be folklore, but is exactly what is needed from the viewpoint of the problem of the identity of proofs: If the proofs are considered to be part of the logic, then preorder equivalence becomes equivalence of categories, whose arrows are the proofs. For identifying these, the concept of proof nets is discussed.

1. Introduction

When we study mathematical objects within a certain mathematical theory, we usually know when two of these objects are considered to be the same, i.e., are indistinguishable within the theory. For example in group theory two groups are indistinguishable if they are isomorphic, in topology two spaces are considered the same if they are homeomorphic, and in graph theory we have the notion of graph isomorphism. However, in proof theory the situation is different. Although we are able to manipulate and transform proofs in various ways, we have no satisfactory notion telling us when two proofs are the same, in the sense that they use the same argument. The reason is the lack of understanding of the essence of a proof, which in turn is caused by the bureaucracy involved in the syntactic presentation of proofs. It is therefore an important problem of research to find new ways of presenting proofs, that allow to grasp the essence of a proof by getting rid of bureaucratic syntax, and that identify proofs if and only if they use the same argument. As a matter of fact, the problem was already a concern of Hilbert, when he was preparing his famous lecture in 1900 [Thi03]. The history of mathematical logic and proof theory might have developped in a different way if he had included his "24th problem".

The text for the second edition has been updated by including some points that have been discussed at the UniLog meeting 2005 in Montreux.

Proofs are carried out within logical systems. We can, for example, have proofs in classical logic and proofs in linear logic. It should be obvious, that two proofs that are carried out in different logics must be distinguished (although every intuitionistic proof can also be seen as classical proof). Consequently, before expecting an answer to the question "When are two proofs the same?", we have first to give an answer to the question "When are two logics the same?".[1] The problem of identifying logics is not only of interest for proof theory, but for the whole area of logic, including mathematical logic as well as philosophical logic.

This means that we have to deal with two problems: the identity of proofs, and the identity of logics. Although the two problems are closely related, they are of a completely different nature.

For the identity of proofs, the actual problem is to find the right presentations of proofs that allow us to make the correct identifications. So far, proofs are presented as syntactical objects: we see Hilbert style proofs, natural deduction proofs, resolution proofs, sequent calculus proofs, proofs in the calculus of structures, tableau proofs, and many more—in particular, also proofs written up in natural language. Of course, the same proof can be written up in various different formalisms. And even in a single formalism, the same proof can take different shapes.

For the identity of logics, on the other hand, the actual problem is to find the "least common denominator" for a definition of logic. The reason is that that there is no generally accepted consensus under logicians about the question what a logic actually is. Not only is the model theoreticians understanding of a logic ("a logic is something that has a syntax and a semantics") different from the proof theoreticians understanding ("a logic is a deductive system that has the cut elimination property"), we also see in other areas of research various different notions of "logic", which are all tailored for a particular application.

But a clean definition of logic will immediately lead to a clean notion of equivalence of logics. In the next section, I will give (from the proof theoreticians viewpoint) such a definition together with its notion of equivalence. Although it could certainly be considered to be folklore knowledge—for long it has been used by logicians already—I discuss it here because it provides clear and firm grounds for investigating the problem of identifying proofs. This problem will be discussed in the last section of the paper.

2. What is a logic ?

Definition 2.1. A *logic* $\mathscr{L} = (\mathscr{A}_{\mathscr{L}}, \Rightarrow_{\mathscr{L}})$ is a set $\mathscr{A}_{\mathscr{L}}$ of *formulae*, together with a binary relation $\Rightarrow_{\mathscr{L}} \subseteq \mathscr{A}_{\mathscr{L}} \times \mathscr{A}_{\mathscr{L}}$, called the *consequence relation*, that is reflexive and transitive.

[1] Of course, this problem was of no concern for Hilbert, since at the time when he was thinking about the identity of proofs there was only one logic.

In other words, a logic is simply a preorder. The index $\mathscr{L}$ will be omitted for $\mathscr{A}$ and $\Rightarrow$, if no ambiguity is possible. The elements of $\mathscr{A}$ will be denoted by A, B, C, etc. Instead of $A \Rightarrow B$, we can also write $B \Leftarrow A$. Similarly, we write $A \Leftrightarrow B$ if $A \Rightarrow B$ and $A \Leftarrow B$. Observe that $\Leftrightarrow$ is always an equivalence relation. Let me make some comments about Definition 2.1:

- There are no cardinality restrictions on the set $\mathscr{A}$.
- The definition abstracts away from the structure of the set $\mathscr{A}$. For capturing the "purely logical part" of a logic, it is irrelevant, which and how many connectives, quantifiers, modalities, constants, variables, etc. are there. It is also not necessary (for the time being) what kind of objects the set $\mathscr{A}$ contains. This could be simply well-formed formulae, sets (finite or infinite) of well-formed formulae, mathematical structures like vector spaces, or even sentences of natural language, like "The book is green."[2]
- There are no computability, complexity, or compactness restrictions on the relation $\Rightarrow$, and there is no need to distinguish between syntax and semantics: It is of no relevance whether $\Rightarrow$ is defined in a model theoretic way ($A \Rightarrow B$ iff every model that makes A true does also make B true), by means of a deductive system ($A \Rightarrow B$ iff there is a proof of B from hypothesis A), or in some other way.
- The two properties of being reflexive and transitive are essential for our treatment of $\Rightarrow$. Reflexivity says that $A \Rightarrow A$ for every formula A. Transitivity says that whenever $A \Rightarrow B$ and $B \Rightarrow C$ then also $A \Rightarrow C$.[3]

Often the notion of a logic is presented such that the consequence relation is not defined as a subset of $\mathscr{A} \times \mathscr{A}$ but as a subset of $\mathfrak{P}_f(\mathscr{A}) \times \mathscr{A}$ or even of $\mathfrak{P}(\mathscr{A}) \times \mathscr{A}$, where $\mathfrak{P}(\mathscr{A})$ is the powerset of $\mathscr{A}$, i.e., the set of all subsets, and $\mathfrak{P}_f(\mathscr{A})$ is the set of all finite subsets of $\mathscr{A}$. Let us denote this new consequence relation by $\vdash$. It should be clear that such a definintion is perfectly equivalent to the one in 2.1, provided the structure of $\mathscr{A}$ has access to the concept of "conjunction", for example, via a connective $\wedge$. Then we have

$$\{A_1, \ldots, A_n\} \vdash B \qquad \text{iff} \qquad A_1 \wedge \cdots \wedge A_n \Rightarrow B \quad .$$

In the case of $\mathfrak{P}(\mathscr{A})$ we also need access to the concept of "infinite conjunction". Then we have

$$\Gamma \vdash B \qquad \text{iff} \qquad \bigwedge \Gamma \Rightarrow B \quad ,$$

where $\Gamma \subseteq \mathscr{A}$ is an arbitrary set of well-formed formulae and $\bigwedge \Gamma$ is their conjunction.

Alternatively, the notion of logic can be defined as a pair $(\mathscr{A}, \mathbb{T})$, where $\mathbb{T} \subseteq \mathscr{A}$ is the set of tautologies (or theorems). Again, this definition is perfectly

[2] With a sufficiently sophisticated definition of "well-formed fomula" the set $\mathscr{A}$ can in fact be restricted to that notion. For example we could allow something like "$\{\phi \mid \ldots\}$" to be a "well-formed fomula", and would by this also capture sets of formulae/propositions/sentences/whatever.

[3] Of course, these conditions can also be dropped, but then everything is possible.

equivalent to the one we have seen, provided the connectives that generate $\mathscr{A}$ have access to the concept of "implication" (either via a connective $\supset$, or via a disjunction together with a negation, or in any other way) and the concept of "truth" (for example via a constant $\top$). Then we have

$$A \Rightarrow B \qquad \text{iff} \qquad A \supset B \ \in \ \mathbb{T}$$

and

$$A \in \mathbb{T} \qquad \text{iff} \qquad \top \Rightarrow A \quad .$$

However, in both alternative definitions, we have to ensure the reflexivity and transitivity of the induced consequence relation. Because of the importance of these two conditions I prefer the definition as given in 2.1.

Let us now continue with some standard definitions for preorders.

Definition 2.2. The *skeleton* of a preorder is the partially ordered set $(\mathscr{A}/\!\Leftrightarrow, \leq)$, where $\mathscr{A}/\!\Leftrightarrow$ is the set of equivalence classes of $\mathscr{A}$ under $\Leftrightarrow$, and $\leq$ is defined by

$$[A]_{\Leftrightarrow} \leq [B]_{\Leftrightarrow} \quad \text{if and only if} \quad A \Rightarrow B \quad .$$

Observe that $\leq$ is anti-symmetric, and therefore a partial order.

Definition 2.3. A *homomorphism* F between two logics

$$\mathscr{L} = (\mathscr{A}, \Rightarrow_{\mathscr{L}}) \qquad \text{and} \qquad \mathscr{M} = (\mathscr{B}, \Rightarrow_{\mathscr{M}})$$

is a monotone function $F : \mathscr{A} \to \mathscr{B}$, i.e., if $A \Rightarrow_{\mathscr{L}} B$ then $F(A) \Rightarrow_{\mathscr{M}} F(B)$.

Definition 2.4. An *isomorphism* F between two logics $\mathscr{L} = (\mathscr{A}, \Rightarrow_{\mathscr{L}})$ and $\mathscr{M} = (\mathscr{B}, \Rightarrow_{\mathscr{M}})$ is a bijective function $F : \mathscr{A} \to \mathscr{B}$, where F as well as F^{-1} are both monotone, i.e., $A \Rightarrow_{\mathscr{L}} B$ if and only if $F(A) \Rightarrow_{\mathscr{M}} F(B)$. We say that two logics are *isomorphic* if there is an isomorphism between the two.

Definition 2.5. An *embedding* F of a logic $\mathscr{L} = (\mathscr{A}, \Rightarrow_{\mathscr{L}})$ into another logic $\mathscr{M} = (\mathscr{B}, \Rightarrow_{\mathscr{M}})$ is an injective function $F : \mathscr{A} \to \mathscr{B}$, such that $A \Rightarrow_{\mathscr{L}} B$ if and only if $F(A) \Rightarrow_{\mathscr{M}} F(B)$.

Definition 2.6. Two logics $\mathscr{L} = (\mathscr{A}, \Rightarrow_{\mathscr{L}})$ and $\mathscr{M} = (\mathscr{B}, \Rightarrow_{\mathscr{M}})$ are *equivalent* if there are two monotone functions $F : \mathscr{A} \to \mathscr{B}$ and $G : \mathscr{B} \to \mathscr{A}$ such that for all formulae $A \in \mathscr{A}$ we have $A \Leftrightarrow_{\mathscr{L}} G(F(A))$ and for all formulae $B \in \mathscr{B}$ we have $B \Leftrightarrow_{\mathscr{M}} F(G(B))$.

Although I am using here the standard order theoretic vocabulary, all these concepts have already been studied from the point of view of logic. In particular, note that skeleton of a logic (where $\mathscr{A}$ is the set of formulae) is simply the Lindenbaum-algebra.

To give another example, in [PU03], the terms *sound translation*, *exact translation*, and *translational equivalent* are used for the concepts of *homomorphism*, *embedding*, and *equivalent*, respectively.[4]

One could say that two logics are "the same" if and only if they are isomorphic, but there are also reasons to argue that the notion of isomorphism is too strong for identifying logics. In particular, under the notion of isomorphism we can only compare logics with the same cardinality of statements. Also from the point of view of proof theory, the the notion of equivalence (which is also used in category theory) seems more natural. In other words, I will follow the slogan:

Two logics are "the same"
if and only if
they are equivalent as preorders.

We can make the following immediate observations:

- It is possible that two logics with different cardinality are equivalent.
- Under the notion of equivalence, we can say that the essence of a logic is captured by its skeleton, because we have that two logics are equivalent if and only if their skeletons are isomorphic.
- The proofs of the logic are not taken into account.

It is obvious that our notion of equivalence is able to identify all different formulations of classical propositional logic. For example we can generate the set $\mathscr{A}$ by using only conjunction and negation, and the set $\mathscr{B}$ by using only disjunction and negation. If $\Rightarrow_{\mathscr{A}}$ and $\Rightarrow_{\mathscr{B}}$ are the intended classical consequence relations, then $(\mathscr{A}, \Rightarrow_{\mathscr{A}})$ and $(\mathscr{B}, \Rightarrow_{\mathscr{B}})$ are equivalent, provided we start with the same number of propositional variables. We will not get an equivalence, if say $\mathscr{A}$ is generated from 5 propositional variables, and $\mathscr{B}$ from 2; and this certainly follows the intuition.

Furthermore, the notion of equivalence is able to successfully distinguish between classical logic and intuitionistic logic. Observe that both logics can use the same set $\mathscr{A}$ of statements, but the consequence relation is different for the two: for example, we have that $\neg\neg A \Rightarrow A$ (where $\neg A$ is the negation of A) in classical logic, but not in intuitionistic logic. In fact, in the case of classical logic, the skeleton is a Boolean algebra, and in the case of intuitionistic logic, it is a Heyting algebra.

Similarly, we can single out linear logic [Gir87] and its various fragments. For example the multiplicative fragment of linear logic (MLL) is not equivalent to the multiplicative additive fragment (MALL). In fact, all the known logics, that are considered to be different, can be distinguished by the notion of equivalence. For various modal logics, namely K, T, S4, and S5, this has been shown explicitely in [PU03]. But it can be shown straightforwardly also for other cases.

Notice that the notion of equivalence for logics that I use here is nothing but the category theoretical equivalence, restricted to preorders. The idea of using this well-known concept in the area of logic can be traced back at least to Lambek's

[4] But in [PU03] they are not defined in order theoretic terms.

work [Lam68, Lam69]. However, since in [Uni05] the organizers write: *"Proposals such that one of* [Pol98] *or* [PU03] *apply only to some special situations."*, there might be an interest in some further comments:

In [Pol98], Pollard compares the notion of logic with the notion of function space, as it is studied in clone theory (see e.g. [PK79]). Although in the case of Boolean logic and the Boolean function spaces (as investigated by Post [Pos41]) this question has a certain interest, we should not be surprised by the "negative" result that the two notions do not coincide. The only disturbing fact in [Pol98] is, as pointed out by the author, that sometimes the projection function (in [Pol98] denoted by $=_1$) has a logical significance and sometimes not. The reason is that Pollard uses the notion of preorder isomorphism[5] for identifying logics, and this is too strong. Under the notion of preorder equivalence, the projection function is (as one would expect) irrelevant from the logical point of view, i.e., the logic does not change if $=_1$ is added as binary connective to the set of generators of $\mathscr{A}$.[6]

In [PU03], Pelletier and Urquhart make a convincing case that preorder equivalence[7] is the right notion of identifying logics. As mentioned already, they explicitely show how various modal logics are correctly distinguished under the notion of this equivalence. In the end of of the paper, the authors provide a concrete example illustrating the fact that two logics (i.e., preorders) which can be embedded into each other are not necessarily equivalent. Although this is not surprising from the order theoretic point of view, the example itself is instructive from the point of view of logic.

Also the notion of "equipollence" proposed in [CG05] coincides with preorder equivalence. The only difference is that in [CG05] a logic is defined to be a closure system (via Tarski's consequence operator) and not as a preorder. The disatvantage of that approach is that it does not scale when proofs enter the scene.

3. What is a proof ?

From now on we do no longer content ourselves with utterances like $A \Rightarrow B$, saying that "B is a logical consequence of A", but rather want to see a justification, or *proof*, of such a statement. In order not to end up in a triviality, we have to accept the fact that there can (and must) be different such justifications of the same statement. Instead of writing $A \Rightarrow B$, we will therefore write $f : A \to B$, in order to single out the proof f of the statement that B is a consequence of A.

More formally, this is the step that takes us from preorders to categories. This means that each pair (A, B) of statements is equipped with a (possibly empty) set

[5] [Pol98] does not use the order theoretic vocabulary but introduces the concept from the viewpoint of topology.

[6] This is so because we have $A =_1 B \;\Leftrightarrow\; A$, no matter what A and B are.

[7] As said before, in [PU03] the term "translational equivalence" is used and the relation to order theory is not mentioned. Their definition also relies on the existence of a connective $\leftrightarrow$ internalizing the logical equivalence. However, since classical implication is transitive and reflexive, the preorder structure is there, and the two definitions coincide.

of *proofs* (i.e., *morphisms* or *arrows* in the language of category theory) from A to B. The axioms of category theory demand that

1. for every formula A there is an identity proof $\mathrm{id}_A : A \to A$, and
2. for any two proofs $f : A \to B$ and $g : B \to C$ there is a uniquely defined proof $g \circ f : A \to C$, the *composite* of f and g.

Further, we demand that for every $f : A \to B$ we have that

$$\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A \quad ,$$

and for all $f : A \to B$ and $g : B \to C$ and $h : C \to D$, we have that

$$(h \circ g) \circ f = h \circ (g \circ f) \quad .$$

Under this refinement, a logic is no longer a preorder, but a category. This relation between category theory and proof theory has already been observed by Lambek in the early work [Lam68, Lam69]. What has been a homomorphism (or monotone function) between preorders, is now a functor F between categories $\mathscr{L}$ and $\mathscr{M}$. More precisely, F consists of a map from formulae of $\mathscr{L}$ into formulae of $\mathscr{M}$, and a map from proofs in $\mathscr{L}$ into proofs in $\mathscr{M}$ such that composition and identities are preserved.

Observe that from the point of view of proof theory, demanding the properties of a category is already quite a lot. For example in the sequent calculus the composition of proofs is given by cut elimination, and this is *per se* not necessarily an associative operation. Furthermore, in the sequent calculus for classical logic this operation is not even confluent, which means that the composition of proofs is not uniquely defined.

However, treating a logic as a category has several advantages. Not only do we get the right level of abstraction to investigate the question how to identify proofs, we also can still use our notion of equivalence of logics—two logics are equivalent iff they are equivalent as categories:

Definition 3.1. Two logics $\mathscr{L}$ and $\mathscr{M}$ are *equivalent* if there are functors $F : \mathscr{L} \to \mathscr{M}$ and $G : \mathscr{M} \to \mathscr{L}$, such that for all formulae A in $\mathscr{L}$ and all formulae B in $\mathscr{M}$ we have that $A \cong G(F(A))$ and $B \cong F(G(B))$.[8]

As useful as this might be for identifying logics, it does not tell us anything about the problem of identifying of proofs, which now becomes the problem of identifying arrows in a category. It should be clear, that the problem must be asked for every logic anew, and it has to be expected that it is of various difficulty in different logics.

There are essentially two different approaches towards this problem, which I will call here the *abstract approach* and the *concrete approach*. The abstract one is

[8] Here $A \cong G(F(A))$ means that the two are isomorphic in the category theoretical sense, i.e., there are proofs $f : A \to G(F(A))$ and $g : G(F(A)) \to A$, such that $f \circ g = \mathrm{id}_{G(F(A))}$ and $g \circ f = \mathrm{id}_A$; and similarly for $B \cong F(G(B))$.

purely algebraic. The idea is to find the right axioms covering enough properties of proofs such that the category theory meets exactly the proof theoretical intuition. Then the slogan is:

Two proofs are "the same"
if and only if
they are represented by the same morphism in a certain category.

A successful example of this are the axioms of Cartesian closed categories which precisely capture proofs in propositional intuitionistic logic (see, e.g., [LS86] for an introduction). Furthermore, due to the Curry-Howard-correspondence [How80], we are able to name proofs in intuitionistic logic by λ-terms, which can be identified through the notion of normalization [Pra65, Pra71, ML75].

This leads us to the concrete approach towards the problem of the identity of proofs. Here, the basic idea is to find "concrete" mathematical objects capturing the essence of a proof by avoiding the syntactic bureaucracy that usually comes with a deductive system. In this sense, λ-terms can be seen as objects capturing the essence of intuitionistic proofs. Consider for example the following two proofs in the sequent calculus for intuitionistic logic:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathsf{id}\ \dfrac{}{A \vdash A} \quad \mathsf{id}\ \dfrac{}{A \vdash A}}{\to\mathsf{L}\ \dfrac{}{A \to A, A \vdash A}} \quad \mathsf{id}\ \dfrac{}{A \vdash A}}{\to\mathsf{L}\ \dfrac{}{A \to A, A \to A, A \vdash A}}}{\mathsf{contL}\ \dfrac{}{A \to A, A \vdash A}}}{\to\mathsf{R}\ \dfrac{}{A \to A \vdash A \to A}}}{\to\mathsf{R}\ \dfrac{}{\vdash (A \to A) \to (A \to A)}} \tag{1}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\mathsf{id}\ \dfrac{}{A \vdash A} \quad \dfrac{\dfrac{\mathsf{id}\ \dfrac{}{A \vdash A} \quad \mathsf{id}\ \dfrac{}{A \vdash A}}{\to\mathsf{L}\ \dfrac{}{A, A \to A \vdash A}}}{\to\mathsf{L}\ \dfrac{}{A \to A, A \to A, A \vdash A}}}{\to\mathsf{R}\ \dfrac{}{A \to A, A \to A \vdash A \to A}}}{\mathsf{contL}\ \dfrac{}{A \to A \vdash A \to A}}}{\to\mathsf{R}\ \dfrac{}{\vdash (A \to A) \to (A \to A)}} \tag{2}$$

Although they are different from each other in the sequent calculus, they both translate into the same λ-term

$$\lambda f_{A \to A}.\lambda x_A.ffx \quad .$$

On the other hand, the sequent calculus proof

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A}\,\mathsf{id}}{A \to A, A \vdash A}\,\mathsf{weakL}}{A \to A \vdash A \to A}\,{\to}\mathsf{R}}{\vdash (A \to A) \to (A \to A)}\,{\to}\mathsf{R} \tag{3}$$

of the same formula $(A \to A) \to (A \to A)$ is translated into

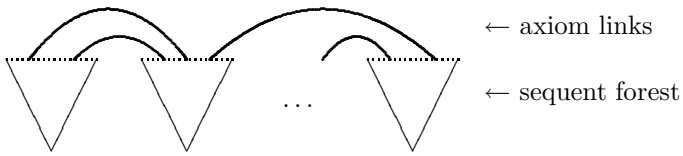
$$\lambda f_{A \to A}.\lambda x_A.x \quad .$$

We can therefore say that the two proofs in (1) and (2) are the same, while the proof in (3) is different.[9]

Let us now turn to linear logic, or more precisely, the multiplicative fragment MLL. For this logic the essence of a proof is captured by *proof nets* [Gir87]. Very roughly speaking, proof nets are for linear logic, what λ-terms are for intuitionistic logic. The slogan here is:

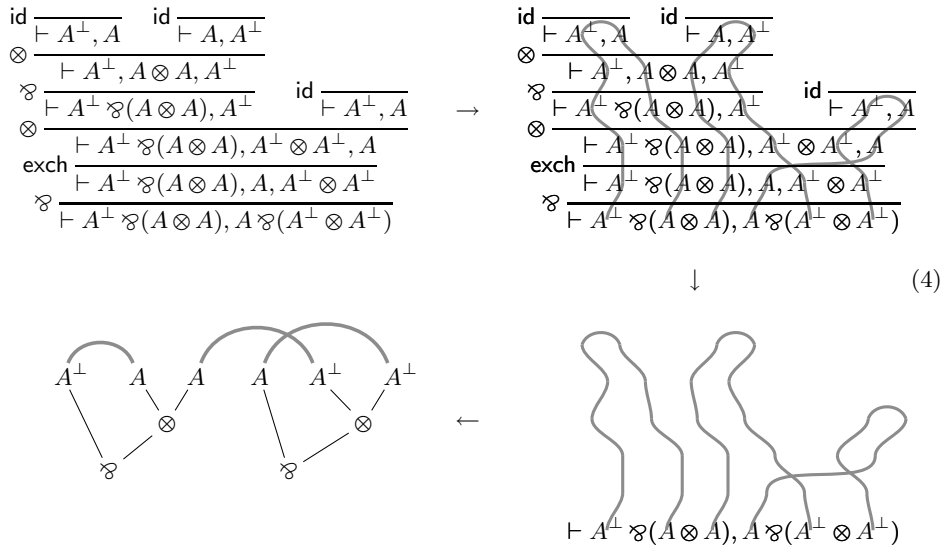
Two proofs are "the same"
if and only if
they are represented by the same proof net.

These proof nets are geometric objects consisting of the formula tree (or sequent forest) extended by some additional graph structure, the so-called *axiom links*. This name is chosen because they represent the identity axioms appearing in the sequent proof:



[9] We have here the two proofs representing the Church numerals 2 and 0.

The following example shows, how a sequent calculus proof in linear logic is translated into a proof net by using the *flow-graph* [Bus91] or *coherence graph* [EK66, KM71].



The reader interested in the details is referred to [Str06]. The proof nets for MLL do not only allow us to make the right identifications on formal proofs presented in the sequent calculus (or any other formalism), but also allow us to construct the free *-autonomous category [Bar79, Blu93, SL04, LS06], and by this substantiate the connection between category theory and proof theory.

It should be a goal of the investigation in the proof theory for any logic to ensure that the abstract and the concrete approach yield the same notion of proof identity. And, in fact, for intuitionistic logic as well for multiplicative linear logic, the two approaches coincide:

morphisms in the free Cartesian closed category	=	***proofs in intuitionistic logic***	=	***typed λ-terms***
morphisms in the free *-autonomous category	=	***proofs in multiplicative linear logic***	=	***proof nets***

These notions of identifying proofs for linear logic and intuitionistic logic are particularly useful for computer science. However, for the logics which are most interesting for mathematics and philosophy, namely, classical logic and modal logics, no such notions exist (yet). This lack of ability of naming proofs in classical logic led Girard in [Gir91] to the statement: *"classical proof theory is inexistent."*

In fact, any approach towards an identification of proofs in classical logic is facing problems from two sides:

1. From the category theoretical side: The obvious categorical axiomatization of classical logic leads to a collapse into a Boolean algebra; all proofs of a given formula B are identified.
2. From the proof theoretical side: as mentioned before, there is no clear notion of composing proofs in classical logic.

In a certain sense, both problems are incarnations of the same phenomenon, which can best be explained with the sequent calculus.[10] Suppose we have two proofs of the formula B in some sequent calculus system:

$$\begin{array}{c}\Pi_1\\ \vdash B\end{array} \qquad \text{and} \qquad \begin{array}{c}\Pi_2\\ \vdash B\end{array}$$

Then we can with the help of the rules weakening, contraction, and cut

$$\mathsf{weak}\,\frac{\vdash \Gamma}{\vdash \Gamma, A} \qquad \mathsf{cont}\,\frac{\vdash \Gamma, A, A}{\vdash \Gamma, A} \qquad \mathsf{cut}\,\frac{\vdash \Gamma, A \quad \vdash \bar{A}, \Delta}{\vdash \Gamma, \Delta}$$

form the following proof of B

$$\mathsf{cont}\,\frac{\mathsf{cut}\,\dfrac{\mathsf{weak}\,\dfrac{\begin{array}{c}\Pi_1\\ \vdash B\end{array}}{\vdash B, A} \qquad \mathsf{weak}\,\dfrac{\begin{array}{c}\Pi_2\\ \vdash B\end{array}}{\vdash \bar{A}, B}}{\vdash B, B}}{\vdash B} \tag{5}$$

If we eliminate the cut from this proof, we get either

$$\mathsf{cont}\,\frac{\mathsf{weak}\,\dfrac{\begin{array}{c}\Pi_1\\ \vdash B\end{array}}{\vdash B, B}}{\vdash B} \qquad \text{or} \qquad \mathsf{cont}\,\frac{\mathsf{weak}\,\dfrac{\begin{array}{c}\Pi_2\\ \vdash B\end{array}}{\vdash B, B}}{\vdash B} \tag{6}$$

depending on a nondeterministic choice. Now note that one can hardly find a reason why for any proof Π, the two proofs

$$\mathsf{cont}\,\frac{\mathsf{weak}\,\dfrac{\begin{array}{c}\Pi\\ \vdash B\end{array}}{\vdash B, B}}{\vdash B} \qquad \text{and} \qquad \begin{array}{c}\Pi\\ \vdash B\end{array} \tag{7}$$

[10] The argument is due to Yves Lafont [GLT89, Appendix B].

should be distinguished. After all, duplicating a formula and immediately afterwards deleting one copy is not doing much. Also the laws of category theory tell us to identify the two.

On the other hand, if we want the nice relationship between deductive system and category theory, we need a confluent cut elimination, which means we have to equate the two proofs in (6). Consequently, by (7), we have to equate Π_1 and Π_2. Since there was no initial condition on Π_1 and Π_2, we conclude that any two proofs of B must be equal.

Note that the problem with weakening can be solved by using the so called mix rule

$$\mathsf{mix}\,\frac{\vdash \Gamma \quad \vdash \Delta}{\vdash \Gamma, \Delta} \quad .$$

Then we can for the two proofs Π_1 and Π_2 give their sum $\Pi_1 + \Pi_2$:

$$\mathsf{mix}\,\frac{\overset{\Pi_1}{\vdash B} \qquad \overset{\Pi_2}{\vdash B}}{\mathsf{cont}\,\dfrac{\vdash B, B}{\vdash B}}$$

Howver, we run into similar problems with the contraction rule. If we try to eliminate the cut from

$$\mathsf{cut}\,\frac{\mathsf{cont}\,\dfrac{\overset{\Pi_1}{\vdash \Gamma, A, A}}{\vdash \Gamma, A} \qquad \mathsf{cont}\,\dfrac{\overset{\Pi_2}{\vdash \bar{A}, \bar{A}, \Delta}}{\vdash \bar{A}, \Delta}}{\vdash \Gamma, \Delta} \quad . \tag{8}$$

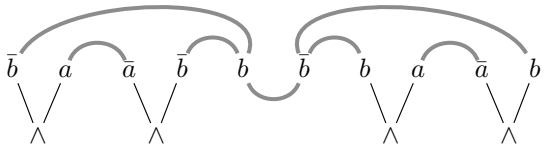
we again have to make a nondeterministic choice. And here, mix is of no help.

Nontheless, recently considerable progress has been made in the quest for a decent proof theory for classical and modal logic. Through the development of the calculus of structures [Gug02, GS01, BT01] it was possible to present new formal systems for classical (propositional and predicate) logic [Brü03] and various modal logics [Sto04]. The proof systems in the calculus of structures have a finer granularity than in the sequent calculus, and by this allow new notions of proof identifications. These led in [LS05b] to a novel kind of proof nets for classical logic. The basic idea is again that the essence of a proof is captured by axiom links that are put on top of the formula tree (or sequent forest). Consider for example the

following proof in the one-sided sequent calculus:

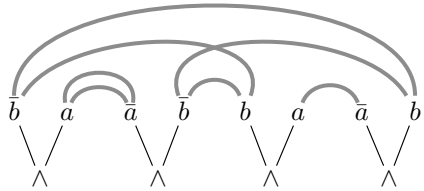
$$\dfrac{\dfrac{\dfrac{\dfrac{\mathsf{id}\ \dfrac{}{\vdash \bar{b}, b} \quad \mathsf{id}\ \dfrac{}{\vdash a, \bar{a}}}{\vdash \bar{b} \wedge a, \bar{a}, b} \wedge \quad \mathsf{id}\ \dfrac{}{\vdash \bar{b}, b}}{\vdash \bar{b} \wedge a, \bar{a} \wedge \bar{b}, b, b} \wedge}{\vdash \bar{b} \wedge a, \bar{a} \wedge \bar{b}, b} \mathsf{cont} \qquad \dfrac{\dfrac{\mathsf{id}\ \dfrac{}{\vdash \bar{b}, b} \quad \dfrac{\mathsf{id}\ \dfrac{}{\vdash a, \bar{a}} \quad \mathsf{id}\ \dfrac{}{\vdash \bar{b}, b}}{\vdash \bar{b}, a, \bar{a} \wedge b} \wedge}{\vdash \bar{b}, \bar{b}, \bar{b} \wedge a, \bar{a} \wedge \bar{b}} \wedge}{\vdash \bar{b}, b \wedge a, \bar{a} \wedge b} \mathsf{cont}}{\vdash \bar{b} \wedge a, \bar{a} \wedge \bar{b}, b \wedge a, \bar{a} \wedge b} \mathsf{cut} \tag{9}$$

Following the idea used in (4), we can obtain a proof net by drawing the flow graph through the sequent proof. The result is

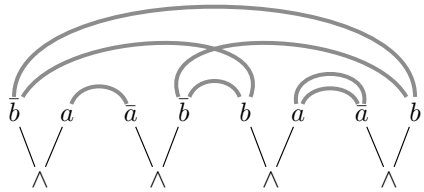


(10)

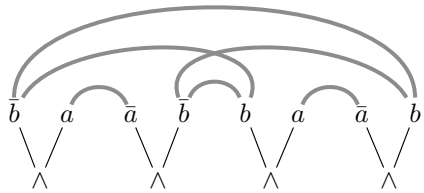
Now the reader is invited to do the following exercise: Take the proof in (9) and eliminate the cut via the usual procedure in the sequent calculus. Then translate the result into a proof net by the same method as above. The result will be either



or

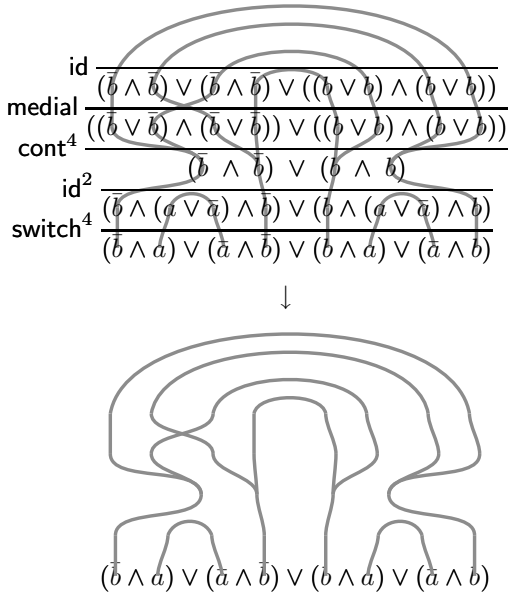


depending on a nondeterministic choice in the sequent calculus cut elimination. On the other hand, if we eliminate the cut directly from the proof net in (10), as described in [LS05b], then we obtain



(11)

Unfortunately, there is no sequent calculus proof whose flow-graph translation into proof nets is (11). However, in the calculus of structures we can give such a proof [LS05b, Str06]:



(12)

Here switch and medial are the inference rules

$$\mathsf{switch}\,\frac{F\{(A \vee B) \wedge C\}}{F\{A \vee (B \wedge C)\}} \qquad \text{and} \qquad \mathsf{medial}\,\frac{F\{(A \wedge B) \vee (C \wedge D)\}}{F\{(A \vee C) \wedge (B \vee D)\}} \quad ,$$

formula context and A, B, C, and D are formula variables (see also [BT01, Brü03]. The important point here is that inference rules are applied deep inside formulae in the same way as we know it from term rewriting. This is reason why we can provide the proof (12) in the calculus of structures but not in the sequent calculus. For further details on the relation between deep inference and proof nets, the reader is referred to [Str05a].

Interestingly, the idea of capturing "the essence" of a proof with pairs of complementary atoms has already been used in Andrews' *matings* [And76] and in Bibel's *connection proofs* [Bib86]. But since they were only interested in proof search, they did not explore the possibility of *composing* proofs. This is done in [LS05b], where composition is defined via a strongly normalizing cut elimination. Therefore we indeed have a category, which could be called a "Boolean" category, since it is to a category what a Boolean algebra is to a poset. In [LS05a], a possible axiomatisation for these kind of categories is given. However, so far there is no axiomatisation that captures precisely the proof identificion induced by the proof nets sketched above (see also [Lam06, Str05b]).

From the point of view of category theory, an alternative approach is given in [FP04a, FP04b], where Führmann and Pym relax the equality on proofs defined by cut elimination to a partial order on proofs, and by this avoid the collapse into a Boolean algebra. Another work in that direction is [Hyl04], where Hyland exhibits concrete mathematical objects, e.g., Frobenius algebras, that can serve as denotations for classical proofs.

In [DP04] the authors use the concept of "coherence" (see, e.g., [Mac71, KM71]) to identify proofs: The category of proofs is defined together with a "graphical" category is defined such that the canonical functor from the category of proofs into the "graphical" category is faithful. Two proofs are the same if they have the same "graphical" representation. In principle, this approach is in the same spirit as the approach based on proof nets: The category of proof nets plays the role of the "graphical" category.[11] However results based on proof nets are usually stronger than results based on "coherence": Not only do they tell when two proof are the same, but also whether a given object actually is a proof. This is usually done via a so-called correctness criterion.

4. Summary

Clearly, the question when two proofs are the same is mathematical more challenging than the question when two logics are the same, which simply reduces to the problem of finding a consensus on the definition. Nonetheless, if one is interested in defining identity between logics, one has to make up his mind whether one wants to ignore the proofs or whether one wants to take the proofs into account. For example, do we want to distinguish a cut-free system for intuitionistic propositional logic from the same system enriched with cut, or do we not? In the one case one can satisfy oneself with preorder equivalence, and in the other one has to take category equivalence.

To give another example, consider the conjuction-only fragment of classical and intuitionistic propositional logic. In both cases, the consequence relation is exactly the same. But the proofs are not: in intuitionistic logic there are two canonical proofs from $A \wedge A$ to A, namely, the two projections, which are also present in classical logic. But in classical logic, we can also form the sum of the two projections, which is not possible in intuitionistic logic.

Let me finish with mentioning some of the questions that are still waiting for an answer:

- Is there a philosophical justification for the identification of proofs made by proof nets?
- Are these identifications useful from the point of view of mathematics (i.e., can we use them for identifying real mathematical proofs)?

[11] In the case of unit-free multiplicative linear logic, proof nets coincide with Kelly-MacLane-graphs.

- Are there ways of extending the notion of proof net to the quantifiers (first order, second order, and higher order), for example by using Miller's *expansion trees* [Mil87]?
- Is it possible to include modalities into proof nets (e.g., by exploring the recent work by Stouppa [Sto04]), in order to get a way of identifying proofs in modal logics?

References

[And76] Peter B. Andrews. Refutations by matings. *IEEE Transactions on Computers*, C-25:801–807, 1976.

[Bar79] Michael Barr. **-Autonomous Categories*, volume 752 of *Lecture Notes in Mathematics*. Springer-Verlag, 1979.

[Bib86] Wolfgang Bibel. A deductive solution for plan generation. *New Generation Computing*, 4:115–132, 1986.

[Blu93] Richard Blute. Linear logic, coherence and dinaturality. *Theoretical Computer Science*, 115:3–41, 1993.

[Brü03] Kai Brünnler. *Deep Inference and Symmetry for Classical Proofs*. PhD thesis, Technische Universität Dresden, 2003.

[BT01] Kai Brünnler and Alwen Fernanto Tiu. A local system for classical logic. In R. Nieuwenhuis and A. Voronkov, editors, *LPAR 2001*, volume 2250 of *Lecture Notes in Artificial Intelligence*, pages 347–361. Springer-Verlag, 2001.

[Bus91] Samuel R. Buss. The undecidability of k-provability. *Annals of Pure and Applied Logic*, 53:72–102, 1991.

[CG05] Carlos Caleiro and Ricardo Gonçalves. Equipollent logical systems. In Jean-Yves Beziau, editor, *Logica Universalis*, pages 99–111. Birkhäuser, 2005.

[DP04] Kosta Došen and Zoran Petrić. *Proof-Theoretical Coherence*. KCL Publications, London, 2004.

[EK66] Samuel Eilenberg and Gregory Maxwell Kelly. A generalization of the functorial calculus. *Journal of Algebra*, 3(3):366–375, 1966.

[FP04a] Carsten Führmann and David Pym. On the geometry of interaction for classical logic. preprint, 2004.

[FP04b] Carsten Führmann and David Pym. On the geometry of interaction for classical logic (extended abstract). In *19th IEEE Symposium on Logic in Computer Science (LICS 2004)*, pages 211–220, 2004.

[Gir87] Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50:1–102, 1987.

[Gir91] Jean-Yves Girard. A new constructive logic: Classical logic. *Mathematical Structures in Computer Science*, 1:255–296, 1991.

[GLT89] Jean-Yves Girard, Yves Lafont, and Paul Taylor. *Proofs and Types*. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 1989.

[GS01] Alessio Guglielmi and Lutz Straßburger. Non-commutativity and MELL in the calculus of structures. In Laurent Fribourg, editor, *Computer Science Logic, CSL 2001*, volume 2142 of *LNCS*, pages 54–68. Springer-Verlag, 2001.

[Gug02] Alessio Guglielmi. A system of interaction and structure. To appear in *ACM Transactions on Computational Logic*, 2002.

[How80] W. A. Howard. The formulae-as-types notion of construction. In J. P. Seldin and J. R. Hindley, editors, *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, pages 479–490. Academic Press, 1980.

[Hyl04] J. Martin E. Hyland. Abstract interpretation of proofs: Classical propositional calculus. In Jerzy Marcinkowski and Andrzej Tarlecki, editors, *Computer Science Logic, CSL 2004*, volume 3210 of *LNCS*, pages 6–21. Springer-Verlag, 2004.

[KM71] Gregory Maxwell Kelly and Saunders Mac Lane. Coherence in closed categories. *Journal of Pure and Applied Algebra*, 1:97–140, 1971.

[Lam68] Joachim Lambek. Deductive systems and categories. I: Syntactic calculus and residuated categories. *Math. Systems Theory*, 2:287–318, 1968.

[Lam69] Joachim Lambek. Deductive systems and categories. II. standard constructions and closed categories. In P. Hilton, editor, *Category Theory, Homology Theory and Applications*, volume 86 of *Lecture Notes in Mathematics*, pages 76–122. Springer, 1969.

[Lam06] François Lamarche. Exploring the gap between linear and classical logic, 2006. Submitted.

[LS86] Joachim Lambek and Phil J. Scott. *Introduction to higher order categorical logic*, volume 7 of *Cambridge studies in advanced mathematics*. Cambridge University Press, 1986.

[LS05a] François Lamarche and Lutz Straßburger. Constructing free Boolean categories. In *Proceedings of the Twentieth Annual IEEE Symposium on Logic in Computer Science (LICS'05)*, pages 209–218, 2005.

[LS05b] François Lamarche and Lutz Straßburger. Naming proofs in classical propositional logic. In Paweł Urzyczyn, editor, *Typed Lambda Calculi and Applications, TLCA 2005*, volume 3461 of *Lecture Notes in Computer Science*, pages 246–261. Springer-Verlag, 2005.

[LS06] François Lamarche and Lutz Straßburger. From proof nets to the free *-autonomous category. *Logical Methods in Computer Science*, 2(4:3):1–44, 2006.

[Mac71] Saunders Mac Lane. *Categories for the Working Mathematician*. Number 5 in Graduate Texts in Mathematics. Springer-Verlag, 1971.

[Mil87] Dale Miller. A compact representation of proofs. *Studia Logica*, 46(4):347–370, 1987.

[ML75] Per Martin-Löf. About models for intuitionistic type theories and the notion of definitional equality. In S. Kangar, editor, *Proceedings of the Third Scandinavian Logic Symposium*, pages 81–109. North-Holland Publishing Co., 1975.

[PK79] R. Pöschel and L. A. Kalužnin. *Funktionen- und Relationenalgebren, Ein Kapitel der Diskreten Mathematik*. Deutscher Verlag der Wissenschaften, Berlin, 1979.

[Pol98] Stephen Pollard. Homeomorphism and the equivalence of logical systems. *Notre Dame Journal of Formal Logic*, 39:422–435, 1998.

[Pos41] E. L. Post. *The Two-Valued Iterative Systems of Mathematical Logic*. Princeton University Press, Princeton, 1941.

[Pra65] Dag Prawitz. *Natural Deduction, A Proof-Theoretical Study*. Almquist and Wiksell, 1965.

[Pra71] Dag Prawitz. Ideas and results in proof theory. In J. E. Fenstad, editor, *Proceedings of the Second Scandinavian Logic Symposium*, pages 235–307. North-Holland Publishing Co., 1971.

[PU03] Francis Jeffry Pelletier and Alasdair Urquhart. Synonymous logics. *Journal of Philosophical Logic*, 32:259–285, 2003.

[SL04] Lutz Straßburger and François Lamarche. On proof nets for multiplicative linear logic with units. In Jerzy Marcinkowski and Andrzej Tarlecki, editors, *Computer Science Logic, CSL 2004*, volume 3210 of *LNCS*, pages 145–159. Springer-Verlag, 2004.

[Sto04] Finiki Stouppa. The design of modal proof theories: the case of S5. Master's thesis, Technische Universität Dresden, 2004.

[Str05a] Lutz Straßburger. From deep inference to proof nets. In *Structures and Deduction — The Quest for the Essence of Proofs (Satellite Workshop of ICALP 2005)*, 2005.

[Str05b] Lutz Straßburger. On the axiomatisation of Boolean categories with and without medial, 2005. Preprint, available at `http://arxiv.org/abs/cs.LO/0512086`.

[Str06] Lutz Straßburger. Proof nets and the identity of proofs, 2006. Lecture notes for ESSLLI'06. Available from `https://hal.inria.fr/inria-00107260/en/` and `http://arxiv.org/abs/cs.LO/0610123`.

[Thi03] Rüdiger Thiele. Hilbert's twenty-fourth problem. *American Mathematical Monthly*, 110:1–24, 2003.

[Uni05] Contest: How to define identity between logics? *1st World Congress and School on Universal Logic*, 2005. On the web at `http://www.uni-log.org/one2.html`.

Lutz Straßburger
INRIA Futurs, Projet Parsifal
École Polytechnique — LIX — Rue de Saclay — 91128 Palaiseau Cedex — France
URL: `http://www.lix.polytechnique.fr/~lutz`