Logic, Methodology and Philosophy of Science IX
D. Prawitz, B. Skyrms and D. Westerståhl (Editors)
© 1994 Elsevier Science B.V. All rights reserved.

SOME ASPECTS OF CATEGORICAL LOGIC

J. LAMBEK

Department of Mathematics and Statistics,
McGill University, Montreal, Quebec, Canada

0. Introduction

Logic, like Caesar's Gaul, used to be divided into three parts: proof theory, recursion theory and model theory. To all these category theory can make some contributions, although more in analyzing basic concepts and determining direction for further development than in addressing specific problems or pursuing technical details. On the other hand, techniques developed by logicians have proved very fruitful when lifted to the categorical level. Here I shall largely confine myself to proof theory, mentioning recursive functions only briefly and barely touching the theory of models.

The present account is largely a survey of results to which the author feels he has made some contributions; it tends to ignore parallel developments by others, in particular the work by Makkai and Reyes [1977] on coherent and infinitary logic and the study of models of elementary theories by Makkai and Paré [1990]. Nor do the many profound contributions to categorical logic by André Joyal fall within the scope of this paper. However, credit must be given to Lawvere [e.g.1969,1970] for the basic insight to encode logical concepts into categorical language. Most of the ideas discussed here have already been treated elsewhere, but a few, such as those concerned with the subcongruence completion of deductive systems, are still under investigation.

1. Categorical proof theory

Proofs can be described in various ways, one of them being in terms of *deductive systems*. A deductive system deals with *deductions*, also called "entailments", $f : A \to B$, where A and B are formulas. In labeling the deduction f, we have already been influenced by category theory. Before the advent of computer science, logicians were usually just interested in

the existence of a deduction $A \to B$ and did not consider the necessity of sometimes distinguishing several such deductions.

The deduction symbol (arrow) is assumed to be reflexive and transitive, so we always have the deduction

$$1_A : A \to A$$

and the rule

$$\frac{f : A \to B \quad g : B \to C}{gf : A \to C} .$$

As categorists we must also study the equality relation on the set of all deductions $A \to B$; in particular, we insist on the following equations:

$$f1_A = f = 1_B f \ , \quad (hg)f = h(gf) \ ,$$

where $h : C \to D$, say. The deductive system then becomes a *category*.

To get away from generalities, let us look at a particular deductive system, the *positive intuitionistic propositional calculus*. Among its formulas there is $\top$ (*true*) and there are given two ways of forming new formulas from old: $A \wedge B$(*A and B*) and $A \Rightarrow B$ (*if A then B*). We postulate the following *axioms* and rules of inference, duly labeled in the spirit of category theory:

$$\circ_A : A \to \top \qquad \pi_{AB} : A \wedge B \to A \qquad \epsilon_{CB} : (C \Rightarrow B) \wedge C \to B$$

$$\pi'_{AB} : A \wedge B \to B$$

$$\frac{f : C \to A \quad g : C \to B}{< f, g > : C \to A \wedge B} \qquad \frac{f : A \wedge C \to B}{f^* : A \to C \Rightarrow B}$$

The logician will recognize all these, for example, ϵ_{CB} as *modus ponens* and the transition from f to f^* as a form of the *deduction rule*.

A categorist will now insist on suitable equations between deductions. In fact, Lawvere [1963] introduced the notion of a *cartesian closed category*, henceforth abbreviated CCC, which can be described by imposing appropriate equations in a positive intuitionistic propositional calculus:

$$k = \circ_A \ ; \qquad \pi_{AB} < f, g >= f \ , \qquad \epsilon_{CB} < f^* \pi_{AC}, \pi'_{AC} >= f \ ,$$

$$\pi'_{AB} < f, g >= g \ , \qquad (\epsilon_{CB} < g\pi_{AC}, \pi'_{AC} >)^* = g \ .$$

$$< \pi_{AB} h, \pi'_{AB} h >= h \ ;$$

It is here assumed that

$$k : A \to \top\ , \qquad h : C \to A \wedge B\ , \qquad g : A \to (C \Rightarrow B)\ .$$

Cartesian closed categories abound in mathematics. To mention just one example, in the familiar category of sets we have:

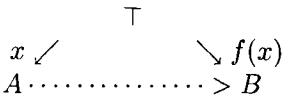
$$\begin{aligned} \top &= \{*\}\ , && \text{a typical one-element set,} \\ A \wedge B &= A \times B\ , && \text{the usual cartesian product,} \\ C \Rightarrow B &= B^C\ , && \text{the set of all functions from } C \text{ to } B\ . \end{aligned}$$

The idea that one should look at an equivalence relation (equality) between proofs was introduced, quite independently of category theory, by Prawitz [1965]. A comparison between his method and ours [L1972] was carried out by Mann [1975]. In his review of Mann's paper, Feferman [1976] suggested that two things should still be incorporated: quantifiers and equalizers. As for quantifiers, over either individual or propositional variables, this is by now well understood, see Lawvere [1970], Seely [1984,1987] and also Section 3 below. The possibility of introducing equalizers, though not perhaps in the most economic way, will be discussed in Section 5. (For a more economic way, see Seely [1984].)

2. Introducing variable arrows

A typical metatheorem in elementary logic is the *deduction theorem*, which may be stated in the present context as asserting the following: if we assume A, or rather $\top \to A$, and if, from this assumption, we can prove B, or rather $\top \to B$, then there must exist a deduction $A \to B$ not depending on this assumption.

We shall label the assumption $x : \top \to A$, then the conclusion $\varphi(x) : \top \to B$ may be viewed as a polynomial in x and the theorem asserts the existence of a deduction $f : A \to B$ not depending on x. The categorist is now inclined to draw a commutative diagram:



In fact, he would insist that there is a unique deduction f such that $fx \underset{x}{=} \varphi(x)$, where $\underset{x}{=}$ is the equality relation in the CCC of all polynomials in x.

This property is known from combinatory logic as *functional completeness* (see Rosenbloom [1950], Curry and Feys [1958], not to be confused with a different notion in universal algebra by the same name). If we write $f = \lambda_{x \in A} \varphi(x)$, it may be summarized by the following two equations:

$$(\beta) \qquad \lambda_{x \in A} \varphi(x) x \underset{x}{=} \varphi(x) \ ,$$

$$(\eta) \qquad \lambda_{x \in A}(fx) = f \ .$$

Using the general algebraic principle of substituting for free variables, we may specialize (β) thus:

$$\lambda_{x \in A} \varphi(x) a = \varphi(a) \ ,$$

where $a : \top \to A$ is any deduction of A from $\top$.

A word of warning: what we have described here is not the usual λ-calculus, where $\lambda_{x \in A} \varphi(x)$ is written not for the deduction $f : A \to B$ but for the deduction $\ulcorner f \urcorner : \top \to B \Rightarrow A$. Still, it serves to illustrate the proof theoretic interpretation of the λ-calculus, known as the Curry-Howard isomorphism, according to which formulas correspond to types and deductions to λ-terms.

For more details on the material of this and the previous section, the reader is referred to the book [LS1986].

3. Introducing variable formulas

What happens if we also allow variable formulas X, Y,etc.? If we also admit universal quantification over variable formulas, we obtain *second order* positive intuitionistic propositional logic or *second order polymorphic λ-calculus*, with the following additional axiom and inference rule:

$$\pi(X) : \forall_X F(X) \to F(X) \ ,$$

$$\frac{\varphi(X) : C \to F(X)}{\Lambda_X \varphi(X) : C \to \forall_X F(X)} \ ,$$

usually called *universal specification* and *generalization* respectively. According to the usual algebraic principle of substituting for free variables, namely

$$\frac{F(X) \to G(X)}{F(A) \to G(A)} \ ,$$

the axiom of universal specification gives rise to

$$\pi(A) : \forall_X F(X) \to F(A) \ .$$

We shall also insist on the following additional equations:

$$\pi(X)\Lambda_X\varphi(X) = \varphi(X) \ ,$$

where we have suppressed the subscript X on the equality sign, and

$$\Lambda_X(\pi(X)f) = f \ .$$

Moreover, the usual principle

$$\frac{\varphi(X) = \psi(X)}{\varphi(A) = \psi(A)}$$

allows us to specialize the first of these equations to

$$\pi(A)\Lambda_X\varphi(X) = \varphi(A) \ .$$

With this additional structure, we obtain a *cartesian closed category* with formal *products*, to be abbreviated as CCCP. However, a proper treatment of these involves simultaneous consideration of the categories $\mathcal{C}, \mathcal{C}[X], \mathcal{C}[X,Y], \ldots$ together with functors $\forall_X : \mathcal{C}[X] \to \mathcal{C}, \forall_Y \mathcal{C}[X,Y] \to \mathcal{C}[X]$, and so on (see Seely [1987]).

By confining attention to positive intuitionistic logic, we have completely ignored $\bot$ (*false*), $A \vee B$(*A or B*) and $\exists_X F(X)$. Here, for example, are the axioms, rule of inference and equations to be satisfied by disjunction if it is to agree with the categorical *coproduct*:

$$\kappa_{AB} : A \to A \vee B \ , \qquad \kappa'_{AB} : B \to A \vee B \ , \qquad \frac{f : A \to C \quad g : B \to C}{[f,g] : A \vee B \to C} \ ,$$

$$[f,g]\kappa_{AB} = f \ , \qquad [f,g]\kappa'_{AB} = g \ , \qquad [h\kappa_{AB}, h\kappa'_{AB}] = g \ ,$$

where it is assumed that $h : A \vee B \to C$.

In the presence of universal quantifiers, it is easily shown that

$$A \vee B \leftrightarrow \forall_X F_{AB}(X) \ ,$$

where

$$F_{AB}(X) = ((A \Rightarrow X) \wedge (B \Rightarrow X)) \Rightarrow X \ .$$

Indeed, Prawitz [1965] has suggested this as a definition of $A \vee B$. Unfortunately, $\leftrightarrow$ does not always translate into categorical isomorphism. The best known counter-example is

$$((A \Rightarrow C) \Rightarrow C) \Rightarrow C \leftrightarrow A \Rightarrow C \ ,$$

whereas, in the category of sets,

$$C^{C^{C^A}} \not\cong C^A \ .$$

At best we can say that the right hand side is a *retract* of the left hand side. Similarly, $A \vee B$, when interpreted as a categorical coproduct, turns out to be only a retract of $\forall_X F_{AB}(X)$ in a CCCP.

4. Introducing equalizers

Not all is lost however. One easily obtains an arrow $\varphi_{AB}(X) : A \to F_{AB}(X)$ in $\mathcal{C}[X]$, where $\mathcal{C}$ is any CCC, hence an arrow

$$k_{AB} = \Lambda_X \varphi_{AB}(X) : A \to \forall_X F_{AB}(X)$$

in any CCCP, and similarly an arrow k'_{AB} starting from B. As in [L1991b], it is now easily shown that

$$A \overset{k_{AB}}{\to} \forall_X F_{AB}(X) \overset{k'_{AB}}{\leftarrow} B$$

is a *weakly* initial object in the category of all $A \overset{f}{\to} C \overset{g}{\leftarrow} B$ (meaning that there is an arrow from the former to the latter which is not necessarily unique). If follows that we have a *weak coproduct* of A and B (meaning that all but the last equation in the definition of a coproduct in the previous section are satisfied.)

If our CCCP also has joint equalizers of families of parallel arrows [*loc.cit.*], we can define the coproduct $A \vee B$ as the subobject of $\forall_X F_{AB}(X)$ which equalizes all pairs of arrows (h, h') from the latter into any object C such that

$$hk_{AB} = h'k_{AB} \quad , \quad hk'_{AB} = h'k'_{AB} \ .$$

We recall from general category theory that the *equalizer* of two arrows $f, g : A \rightrightarrows B$ is an arrow $m : E(f,g) \to A$ such that $fm = gm$ and m is universal with respect to this property: if also $m' : C \to A$ is such that $fm' = gm'$ then there is a unique arrow $k : C \to E(f,g)$ such that

$m' = mk$. In the category of sets, equalizers are easily constructed: let $E(f,g) = \{a \in A | fa = ga\}$ and take m to be the inclusion.

What could we possibly mean by $E(f,g)$ in a deductive system? Martin-Löf [1984] might speak of a "judgement" that the deductions f and g are equal, but such a judgement does not come equipped with an arrow into A. To imitate the above set-theoretic construction we should rather carry out the *Brouwer-Heyting-Kolmogorov* interpretation of intuitionistic logic, in which formulas are replaced by sets (see Troelstra and van Dalen [1988]), say the formula A by the set $\{A\}$ of all *reasons* for A. I say "reason" rather than "proof", since otherwise $\{A\}$ would be empty whenever A is not a theorem.

Without enlarging our ontology, we may take as a reason for A any deduction $C \to A$ from an arbitrary formula C. (Categorists have called this a "generalized element" of A.) Thus $\{A\}$ is the union of all sets $Hom(C,A)$, where C ranges over all objects of the category $\mathcal{C}$.

We can then introduce $E(f,g)$ as the set of all reasons $a : C \to A$ such that $fa = ga$. Then $E(f,g)$ is not a formula, or object of $\mathcal{C}$, but a *right ideal* or *sieve* $\mathfrak{a}$ of A, which assigns to each formula C a subset $\mathfrak{a}_C \subseteq Hom(C,A)$ such that, whenever $a \in \mathfrak{a}_C$ and $c : D \to C$, then also $ac \in \mathfrak{a}_D$. (If $\mathcal{C}$ is a monoid, that is, a one-object category, then this agrees with the usual definition of right ideal in a monoid.) In categorical language, $\mathfrak{a}$ is nothing else than a subfunctor of the representable functor $Hom(-,A)$.

We can now form a new category whose objects are right ideals of $\mathcal{C}$ and whose arrows are induced from those in $\mathcal{C}$. This new category will have equalizers, but unfortunately it won't inherit the CCC structure of $\mathcal{C}$. It turns out that we can remedy the situation by considering right ideals modulo congruence relations instead. In other words, we pass from subfunctors of representables to quotients of such. By an application of Occam'a razor, we shall replace the right ideals modulo congruence relations by the congruence relations on the right ideals.

5. A subcongruence completion

A (*right*) *subcongruence* α of A assigns to each formula C a partial equivalence relation α_C on $Hom(C,A)$ such that, whenever $a, a' : C \to A$ and $c : D \to C$, then

$$a \alpha_C a' \text{ implies } (ac) \alpha_D (a'c) .$$

It is easily seen that the domain $Dom\ \alpha$ of any (right) subcongruence of A is a right ideal of A.

We now form the category $\mathcal{C}^R$: its objects are subcongruences of objects of $\mathcal{C}$ and its arrows $(\beta, f, \alpha) : \alpha \to \beta$ are induced by arrows $f : A \to B$ in $\mathcal{C}$ (assuming α to be a subcongruence of A and β one of B) such that, for each object C and all $a, a' : C \to A$,

$$(*) \qquad a\alpha_C a' \text{ implies } (fa)\beta_C(fa') .$$

We shall often just write $f : \alpha \to \beta$. If also $g : \alpha \to \beta$, we shall say that $(\beta, f, \alpha) = (\beta, g, \alpha)$ provided, under the same conditions,

$$(**) \qquad a\alpha_C a' \text{ implies } (fa)\beta_C(ga') .$$

Here $(*)$ was chosen to ensure that f induces a mapping $Dom\ \alpha_C/\alpha_C \to Dom\ \beta_C/\beta_C$. Then $(**)$ just means that f and g induce the same mapping. However, there is another way of interpreting $(**)$. Observe that α gives rise to a functor $F_\alpha : \mathcal{C}^{op} \to$ Set such that

$$F_\alpha(C) = Dom\ \alpha_C/\alpha_C .$$

If β similarly gives rise to $F_\beta(C)$, then (β, f, α) gives rise to a natural transformation $t_f : F_\alpha \to F_\beta$. Then $(**)$ means precisely that $t_f = t_g$.

However, not all natural transformations $F_\alpha \to F_\beta$ are obtained in this fashion. To describe all of them we would have to consider (*right homomorphic*) *relations* ρ between A and B, which to each object C assign a binary relation ρ_C between $Hom(C, A)$ and $Hom(C, B)$ such that, whenever $a : C \to A, b : C \to B$ and $c : D \to C$, then

$$b\rho_C a \text{ implies } (bc)\rho_D(ac) .$$

Then ρ induces a mapping $Dom\ \alpha/\alpha \to Dom\ \beta/\beta$, or a natural transformation $F_\alpha \to F_\beta$, if and only if, for all objects C,

$$(\dagger) \qquad \alpha_C \subseteq \rho_C^{\cup}\beta\rho_C \text{ and } \rho_C\alpha_C\rho_C^{\cup} \subseteq \beta_C ,$$

where juxtaposition denotes the *relative product* and $\rho_C^{\cup}$ is the *converse* of ρ_C. Moreover two relations ρ and σ between A and B induce the same mapping, or natural transformation, if and only if, for all objects C,

$$(\dagger\dagger) \qquad \alpha_C \subseteq \rho_C^{\cup}\beta\sigma_C \text{ or } \rho_C\alpha_C\sigma_C^{\cup} \subseteq \beta_C .$$

(In view of $(\dagger)$, the two clauses of $(\dagger\dagger)$ are equivalent.)

In this way one obtains all natural transformations $F_\alpha \to F_\beta$, hence a full subcategory $\mathcal{C}^{(R)}$ of the functor category $\text{Set}^{\mathcal{C}^{op}}$. (I believe that the

transition from $\mathcal{C}^R$ to $\mathcal{C}^{(R)}$ resembles a construction recently described by McLarty.) We shall not consider the category $\mathcal{C}^{(R)}$ any further in this article, except for drawing the following picture, in which all arrows represent faithful functors, but not all of them are full:

$$\begin{array}{ccc} \mathcal{C} & \overset{\text{Yoneda}}{\underset{\text{full}}{\longrightarrow}} & \mathrm{Set}^{\mathcal{C}^{\mathrm{op}}} \\ \text{full}\downarrow & & \uparrow\text{full} \\ \mathcal{C}^R & \underset{\text{not full}}{\longrightarrow} & \mathcal{C}^{(R)} \end{array}$$

Of course, the functor $\mathcal{C}^R \to \mathcal{C}^{(R)}$ sends the arrow $f : \alpha \to \beta$ onto $\rho_f : \alpha \to \beta$, where $b(\rho_f)_C a$ means $b = fa$, for all $a : C \to A$ and $b : C \to B$. I hope to return to a consideration of $\mathcal{C}^{(R)}$ on another occasion.

6. Some properties of $\mathcal{C}^R$

Readers not too familiar with category theory may wish to skip this section, some of which describes work in progress.

If α and α' are subcongruences of A such that $\alpha \subseteq \alpha'$, then $(\alpha', 1_A, \alpha)$ will be an arrow $\alpha \to \alpha'$ in $\mathcal{C}^R$. Two extreme cases are of special interest.

(a) If α is the restriction of α' to $Dom\ \alpha$, that is, if $\alpha\alpha'\alpha = \alpha, 1_A : \alpha \to \alpha'$ is a (canonical) *subobject* of α'. The subobjects of α' form a complete lattice.

(b) If $Dom\ \alpha = Dom\ \alpha'$, that is, if $\alpha\alpha'\alpha = \alpha'$, α' induces a congruence relation on $Dom\ \alpha$ and $1_A : \alpha \to \alpha'$ is a (canonical) *quotient* of α. The quotient objects of α form a complete lattice.

The original motivation for introducing $\mathcal{C}^R$ was to construct equalizers. Indeed, the equalizer of $f, g : \alpha \rightrightarrows \beta$ is $1_A : \kappa \to \alpha$, where

$$\kappa_C = \alpha_C \cap f^{\cup}\beta_C g\ .$$

(We identify f with the relation ρ_f mentioned at the end of Section 5.) Since the lattice of subobjects is complete, we also have equalizers of families of parallel arrows. (Perhaps, we have achieved too much; we would have been happy with joint equalizers of, in some sense, "definable" families.) We also have coequalizers: the coequalizer of $f, g : \alpha \rightrightarrows \beta$ is $\beta \to \lambda$, where λ is the smallest congruence on $Dom\ \beta$ extending $\beta \cup f\alpha g^{\cup}$. By completeness, we also have joint coequalizers of families of parallel arrows.

We shall discuss some further properties of $\mathcal{C}^R$ under various assumptions about $\mathcal{C}$. In doing so, we shall switch from logical to categorical notation and terminology, replacing $\top, A \wedge B, A \Rightarrow B, \bot, A \vee B$ by

$1, A \times B, B^A, 0, A + B$ respectively, speaking of terminal object, product, exponentiaion, initial object and coproduct.

(1) If $\mathcal{C}$ has finite products, then so does $\mathcal{C}^R$. In fact $\mathcal{C}^R$ is then a *regular* category. (I am endebted to Duško Pavlović for pointing this out.) This is so since regular epimorphisms are isomorphic to quotient objects and are preserved under pullbacks.

(2) If $\mathcal{C}$ is a CCC, then so is $\mathcal{C}^R$ and the functor $\mathcal{C} \to \mathcal{C}^R$ preserves the CCC structure. (See [L1991b, Proposition 10.1].)

(3) If $\mathcal{C}$ is a CCCP, then $\mathcal{C}^R$ is also cocartesian and any finite coproduct of definable endofunctors of $\mathcal{C}$ has a least fixpoint in $\mathcal{C}^R$. (See loc.cit., Proposition 10.2, where a precise definition of "definable" is given. Suffice it here to point out that e.g. $1, X, X^2$ and C^{C^X} are definable.)

(4) If $\mathcal{C}$ is a poset, then $\mathcal{C}^R$ is the complete lattice of downward closed subsets of $\mathcal{C}$. (Unfortunately, this is not the same as the Dedekind-MacNeille completion, see Birkhoff [1967].)

(5) If $\mathcal{C}$ is the monoid of partial recursive funtions $\mathbb{N} \to \mathbb{N}$, that is, partial functions whose graphs are recursively enumerable, $\mathcal{C}^R$ contains the category PER, whose objects are partial equivalence relations on $\mathbb{N}$. To see this, one associates with every partial equivalence relation A on $\mathbb{N}$ the subcongruence $\alpha(A)$ such that, for all partial recursive funtions $f, g : \mathbb{N} \to \mathbb{N}$,

$$f\alpha(A)g \text{ if and only if, for all } n \in \mathbb{N}, \ (fn)A(gn) ,$$

and with every subcongruence α the partial equivalence relation $A(\alpha)$ such that

$$mA(\alpha)n \text{ if and only if } k_m \alpha k_n ,$$

where k_m is the constant function with value m. Every finite coproduct of definable endofunctors of PER has a least fixpoint (see loc.cit. Proposition 8.1.). Hyland[1988] and Moggi have shown PER to be a model of polymorphic λ-calculus, though not in the usual universe of sets.

(6) *Weak binary products* are defined like binary products, except that the equation $< \pi_{AB} h, \pi'_{AB} h >= h$ is missing. If $\mathcal{C}$ has weak binary products, then $\mathcal{C}^R$ has binary products; if α and β are subcongruences of A and B respectively, we define

$$\alpha \times \beta = \pi_{AB}^{\cup} \alpha \pi_{AB} \cap \pi'^{\cup}_{AB} \beta \pi'_{AB}$$

and check that $\pi_{AB} : \alpha \times \beta \to \alpha$ and $\pi'_{AB} : \alpha \times \beta \to \beta$. Moreover, if $a : \gamma \to \alpha$ and $b : \gamma \to \beta$, then $< a, b >: \gamma \to \alpha \times \beta$ and, if $h : \gamma \to \alpha \times \beta$, then $< \pi_{AB}h, \pi'_{AB}h >$ induces the same arrow as h. A similar result holds for nullary products, that is, terminal objects, and for exponentiation.

(7) If $\mathcal{C}$ has weak coproducts, then $\mathcal{C}^R$ has coproducts; if $\mathcal{C}$ has a weak natural numbers object, then $\mathcal{C}^R$ has a natural numbers object. These and similar results are buried in the proof of (3), bearing in mind that a natural numbers object is a least fixpoint of the endofunctor $1 + X$.

(8) We say that $\mathcal{C}$ has a *weak subobject classifier* $t : I \to \Omega$ provided I is a weak terminal object (that is, for each C there is an arrow $i_C : C \to I$) and, for each right ideal $\mathfrak{a}$ of any object A, there is an arrow $h : A \to \Omega$ such that $\mathfrak{a} = Ker\ h$, where

$$(Ker\ h)_C = \{a : C \to A | \exists_{i:C \to I} ti = ha\} .$$

Let $i \iota_C i'$ for all $i, i' : C \to I$ and let

$$h \omega_A h' \text{ if and only if } Ker\ h = Ker\ h' ,$$

then ι is a congruence on I and ω is a congruence on Ω. One easily checks that ι is a terminal object (just take $\circ_A = i_A$) and we shall see that ω is a subobject classifier in the usual sense.

In fact, it is easily verified that (ω, t, ι) is an arrow. Now let $1_A : \alpha' \to \alpha$ be any subobject of α, we pick $h : A \to \Omega$ such that $Dom\ \alpha' = Ker\ h$ and verify that $h : \alpha \to \omega$ and $\alpha' = \alpha \cap h^{\cup} \omega t \circ_A$. Moreover, it follows that (ω, h, α) is unique with this property.

7. Gentzen style proof theory (intuitionistic)

A different way of presenting proofs was discovered by Gentzen. For dealing with intuitionistic logic he introduced generalized deductions, usually called *sequents*, of the form

$$f : A_1 \cdots A_m \to B ,$$

where the A_i and B are formulas. When the set of sequents $\Gamma \to B$ (we use capital Greek letters to denote strings of formulas) is subjected to appropriate equations, we obtain a *Gentzen multicategory*. It is not so obvious how to describe these equations directly [Szabo 1978], we shall

here follow [L1989a] and pass to the internal language of a multicategory, in which the sequents act as operations, while equations between sequents are best described through equations between terms.

Here then is the language: for each object A of the multicategory we introduce countably many variables. Rather than burdening our terminology by labeling these variables once and for all, we shall just say that x is a variable of type A and write $x \in A$. Terms of given types are defined inductively: every variable is a term of its type and, if $f : A_1 \cdots A_m \to B$ is a sequent and a_i is a term of type A_i, for $i = 1, \cdots, m$, then $fa_1 \cdots a_m$ is a term of type B. In particular, if $x_i \in A_i$, then $fx_1 \cdots x_m \in B$. There can also be constants of type B, namely any sequent $b : \ \to B$, with $m = 0$.

Algebraically speaking, $fx_1 \cdots x_m$ is a *polynomial*; we think of x_i as an indeterminate of type A_i and of f as an m-ary operation. In fact, a Gentzen multicategory is nothing else than a *many-sorted algebraic theory* (see Higgins [1963], Birkhoff and Lipson [1970]).

Logically speaking, $fx_1 \cdots x_m$ is a *proof* from certain hypotheses; we think of x_i as an occurrence of the hypothesis A_i and of f as a deduction of B from these hypotheses. Thus a Gentzen multicategory may also be viewed as a *natural deduction system* as promulgated by Prawitz [1965].

Gentzen postulated for each formula A the sequent

$$1_A : A \to A$$

and he admitted four rules for deriving new sequents from old, the *cut rule*

$$\frac{f : \Lambda \to A \quad g : \Gamma A \Delta \to B}{g < f > : \Gamma \Lambda \Delta \to B}$$

and three *structural rules*:

$$\frac{f : \Gamma AB\Delta \to C}{f^i : \Gamma BA\Delta \to C} \qquad \text{(interchange)} ,$$

$$\frac{f : \Gamma AA\Delta \to B}{f^c : \Gamma A\Delta \to B} \qquad \text{(contraction)} ,$$

$$\frac{f : \Gamma\Delta \to B}{f^w : \Gamma A\Delta \to B} \qquad \text{(weakening)} .$$

The intended algebraic interpretation requires that the internal language of a multicategory be subject to the following equations and, of

course, others derivable from them by the usual rules of equality:

$$1_A x = x \ ,$$

$$g < f > \overline{uwv} = g\overline{u}f\overline{wv} \ ,$$

$$f^i\overline{u}yx\overline{v} = f\overline{u}xy\overline{v} \ ,$$

$$f^c\overline{u}x\overline{v} = f\overline{u}xx\overline{v} \ ,$$

$$f^w\overline{u}x\overline{v} = f\overline{uv} \ .$$

Here $\overline{u} = x_1 \cdots x_m$, where $x_i \in A_i$ and $\Gamma = A_1 \cdots A_m$. Similarly $\overline{v}$ is related to Δ and $\overline{w}$ to Λ, while $x \in A$ and $y \in B$. (Our account is somewhat incomplete, as we have not bothered to *declare* variables; e.g. the first equation should really be written $1_A x \underset{x}{=} x$.)

To return to the question: what are the equations of a multicategory, we are now in a position to define equality between operations $f, g : A_1 \cdots A_m \to B$ to mean that $fx_1 \cdots x_m = gx_1 \cdots x_n$ is provable in the internal language.

There is quite an industry involved in studying *substructural* logics, in which some or all of the structural rules are absent. For example, the weakening rule is omitted in relevance logic, the weakening and contraction rules are both omitted in Girard's [1987] linear logic and all three rules are omitted in the syntactic calculus [L1958], a form of bidirectional categorial grammar.

Gentzen's original motivation was to show that, for example, in the positive intuitionistic propositional calculus freely generated from a given multicategory, the cut rule (and incidentally also, for compound A, the axiom $1_A : A \to A$) is redundant, provided the connectives $\top$, $\wedge$ and $\Rightarrow$ are subjected to appropriate introduction rules. Thus, for given Γ and B, he was able to find all provable sequents $\Gamma \to B$. His method can also be used for deciding when two sequents from Γ to B are equal. (See e.g. Szabo [1978], [L1958] and [L1991a] for the case without structural rules.) At least one of Gentzen's introduction rules was discovered independently by Bourbaki [1948] in his study of multilinear operations.

8. The algebraic theory of primitive recursive functions

I learned about Gentzen's sequence calculus from Kleene [1952]. While Kleene does not discuss many-sorted algebraic theories, equations very much like the above occur in his treatment of primitive recursive functions. The question thus arises: can these be viewed as realizations of operations of an algebraic theory? Indeed, there is such an algebraic theory, even a single-sorted one.

Consider a sort N, operations

$$0 : \rightarrow N(\text{zero}) \quad , \quad S : N \rightarrow N(\text{successor})$$

and the following rule for forming new operations from old:

$$\frac{a : N^n \rightarrow N \quad h : N^{n+2} \rightarrow N}{R_{ah} : N^{n+1} \rightarrow N} \quad (\text{recursion}) \ .$$

These operations are subject to the following equations, which already appear in Kleene's book:

$$(E_{ah}) \qquad \begin{aligned} R_{ah}\overline{x}0 &= a\overline{x} \\ R_{ah}\overline{x}Sy &= h\overline{x}yR_{ah}\overline{x}y \ , \end{aligned}$$

where $\overline{x} = x_1 \cdots x_n$.

Since the operation defined by recursion is supposed to be uniquely determined, one would also like to satisfy the conditions:

$$(U_{fh}) \qquad \text{if} \quad f\overline{x}Sy = h\overline{x}yf\overline{x}y \quad \text{then} \quad f = R_{f<0>h} \ ,$$

where $f : N^{n+1} \rightarrow N$ and $f < 0 > \overline{x} = f\overline{x}0$, an example of the cut rule. It had been an embarrassment for some time that the conditions (U_{fh}) were not presented in equational form (see Gödel [1958], Sanchis [1967], [LS1986]). Yet they can be so presented [L1988], although the argument is a little tricky.

A ternary operation $m : N^3 \rightarrow N$ is called a *Mal'cev operation* if it satisfies:

$$mxyy = x \quad , \quad myyz = z \ .$$

(Mal'cev [1954] had shown that the existence of such an operation is necessary and sufficient for congruence relations in every model of the algebraic theory to permute.) There are many Mal'cev operations in primitive recursive arithmetic, e.g.

$$mxyz = (x + z) \dot{-} y \ ,$$

where $x+y$ and $x \dot{-} y$, the naive difference, are easily defined by recursion.

With the help of a Mal'cev operation m, we can construct a new $n+2$-ary operation H_{mfh} from h and f:

$$H_{mfh}\overline{x}yz = m(h\overline{x}yz)(h\overline{x}yf\overline{x}y)(f\overline{x}Sy) \ .$$

We can now replace (U_{fh}) by

$$(M_{mfh}) \qquad\qquad R_{f<0>H_{mfh}} = f \ .$$

More precisely, one notices that

$$(M_{mfh}) \Rightarrow (U_{fh}) \ ,$$
$$(U_{fH_{mfh}}) \Rightarrow (M_{mfh}) \ .$$

Once stated, these implications are easily verified.

If we choose $mxyz = (x + z) \dot{-} y$, we finally arrive at the following equational presentation of primitive recursive arithmetic:

$$(E_{ah}) \ , \ (M_{mfh}) \ , \ (x + y) \dot{-} y = x \ .$$

The last equation must be postulated, because its usual proof depends on (U_{fh}), whereas here it is used to derive (U_{fh}) from (M_{mfh}).

It is quite easy to find a primitive recursive function $fxyzt$ such that Fermat's conjecture asserts that f is the function with constant value 0. It is not impossible that $fxyz4 = 0$ already in the algebraic theory discussed here, in view of Fermat's method of descent. (A similar question was raised conversationally by Joyal.) We can, of course, replace f by a function of one argument here. Work on reducing such polynomials to normal form is being done by Okada and Scott. Unfortunately, as they point out, one cannot expect to have both strong normalization and the Church-Rosser property, in view of Gödel's result that provability in Peano arithmetic is not decidable.

Note added in proof: Gregory Mints informs me that Mal'cev and his students have also studied algebras of primitive recursive functions.

9. Gentzen style proof theory (classical)

Gentzen devised a different sequent calculus for classical logic, with sequents of the form

$$f : A_1 \cdots A_m \to B_1 \cdots B_n \ .$$

These were supposed to be interpreted as

$$f : A_1 \wedge \cdots \wedge A_m \to B_1 \vee \cdots \vee B_n \ ,$$

in categorical language

$$f : A_1 \times \cdots \times A_m \to B_1 + \cdots + B_n \ .$$

Having convinced oneself that Gentzen's intuitionistic sequents are nothing else than operations in a many-sorted algebraic theory, one wonders why his classical sequents have not surfaced in algebra.

Take, for example, a single-sorted "bi-operation"

$$f : A \times A \to A + A \ .$$

Up to isomorphism, this may be written

$$f : A^2 \to A \times 2 \ ,$$

where $2 = \{\top, \bot\}$ is a representative two-element set. We can write $f =< f_0, f_1 >$, where

$$f_0 : A^2 \to A \quad , \quad f_1 : A^2 \to 2 \ ,$$

the former being a binary operation, the latter a binary relation. It would therefore appear that, in the single-sorted case, bi-operations may be analyzed into operations and relations. Indeed, algebraists study ordered groups and similar structures.

The classical Gentzen calculus can also be extended to the substructural situation, where one should interpret $f : A_1 \cdots A_m \to B_1 \cdots B_n$ as

$$f : A_1 \otimes \cdots \otimes A_m \to B_1 \oplus \cdots \oplus B_n \ .$$

The tensor product $\otimes$ comes up in multilinear algebra. Its dual $\oplus$ appears in Girard's linear logic, although in a different notation. It so happens that in Hopf algebras $\oplus$ coincides with $\otimes$, and the same is true in production grammars. However, it is easy to give examples in which $\oplus$ and $\otimes$ are different.

In the algebra of all binary relations on a set X, we may write:

$$a(R \otimes S)b \quad \text{for} \quad \exists_{x \in X}(aRx \wedge xSb) \ ,$$
$$a(R \oplus S)b \quad \text{for} \quad \forall_{x \in X}(aRx \vee xSb) \ .$$

The former is the usual relative product. The latter may be described classically as its De Morgan dual by

$$R \oplus S = \neg(\neg R \otimes \neg S) ,$$

but it also exists intuitionistically. Unfortunately, intuitionistic logic does not suffice to prove that $\oplus$ is associative. (See [L 1991 c].)

The categorical treatment of classical Gentzen style proof theory requires something new in place of multicategories, namely "polycategories". These have been discussed by Szabo [1975] and others, but not yet in sufficient generality to handle the last example above.

10. Completeness of higher order logic

Categories may also be used to clarify and sharpen some basic ideas in model theory, though these may be far removed from the combinatorial preoccupations of specialists in that area. We shall only briefly sketch the situation as it concerns higher order logic.

On the one hand, there are certain intuitionistic higher order languages or type theories; they form a category, whose arrows may be called "translations". On the other hand, there are elementary toposes, namely cartesian closed categories with subobject classifier and, for the present purpose, also a natural numbers object; they form a category too, whose arrows are called "logical functors".

For each higher order language $\mathcal{L}$ we may construct a topos $T(\mathcal{L})$, the *topos generated* by $\mathcal{L}$, essentially what logicians call the "term model", which might also have been called the "Tarski-Lindenbaum topos". With each topos we may associate a higher order language $L(\mathcal{T})$, its *internal language*. It turns out that L and T are functors between the two categories under consideration and that T is left adjoint to L. (Actually, this assumes that toposes have "canonical" subobjects, a technical detail which we shall ignore here, see [LS1986] for a fuller account.) In particular, this means that we have a one-to-one correspondence between logical functors

$$T(\mathcal{L}) \to \mathcal{T}$$

and translations

$$\mathcal{L} \to L(\mathcal{T}) ,$$

either of which may be called an *interpretation* of $\mathcal{L}$ in $\mathcal{T}$.

If we allow every such interpretation as a model, the completeness theorem would be quite trivial, as a single model would suffice, namely

$\mathcal{L} \rightarrow LT(\mathcal{L})$. We shall, however, define a *model topos* as one whose internal language has very special properties:

(1) $\bot$ is not true in $\mathcal{T}$, that is, not provable in $L(\mathcal{T})$;

(2) if $p \vee q$ is true in $\mathcal{T}$, then p is true or q is true;

(3) if $\exists_{x \in A} \varphi(x)$ is true in $\mathcal{T}$, then $\varphi(a)$ is true for some closed term of type A in $L(\mathcal{T})$.

Peter Freyd observed that these properties can be translated into algebraic properties of the terminal object 1 of $\mathcal{T}$:

(1) $1 \neq 0$;

(2) 1 is indecomposable;

(3) 1 is projective.

Here "projective" means exactly the same as in module theory, where the term originated. It turns out that, when $L(\mathcal{T})$ is classical, a model topos is precisely a non-standard model in the sense of Henkin [1950].

The completeness theorem for intuitionistic higher order logic, in the tradition of Gödel [1931], Henkin [1950], Aczel [1969] and others, may now be stated as follows:

every higher order language $\mathcal{L}$ has enough models, meaning that a formula p is provable in $\mathcal{L}$ if and only if it is true under every interpretation of $\mathcal{L}$ in a model topos $\mathcal{T}$.

Algebraically, this result asserts:

every topos is equivalent to a subtopos of a product of model toposes.

This last statement bears a formal resemblance to the following result about commutative rings:

every commutative ring is isomorphic to a subring of a product of local rings.

But actually we know more. According to Grothendieck and Dieudonné [1960]:

every commutative ring is isomorphic to the ring of continuous sections of a sheaf of local rings.

A similar result holds for toposes in which *all subobjects of 1 are projective.* This is so for toposes of the form $\mathsf{T}(\mathcal{L})$ when $\mathcal{L}$ satisfies Hilbert's rule (see Hilbert and Bernays [1970]):

for any inhabited type A (i.e. $\exists_{x \in A} \top$ is provable in $\mathcal{L}$), *if $\alpha = \{x \in A | \varphi(x)\}$ is a closed term of type PA, then there is a closed term $e_\alpha = \varepsilon_{x \in A} \varphi(x)$ of type A such that $\exists_{x \in A} \varphi(x) \vdash \varphi(e_\alpha)$ in $\mathcal{L}$.*

In [L1989] I wrongly asserted also the converse of this; I am endebted to John Bell for pointing out the error.

One can get rid of the restriction to Hilbert's rule, provided one looks at toposes generated by languages with sufficiently many constants. The idea goes back to Henkin [1949]. One may think of the constants as variables held constant: if V is a set of variables, $\mathcal{L}(V)$ is the same language as $\mathcal{L}$, except that now a formula is called "closed" if it contains no free variables other than those from V. Here is the final result:

if $\mathcal{L}$ is any higher order language and V is a sufficiently large set of variables, then $T(\mathcal{L}(V))$ is the topos of continuous sections of a sheaf of model toposes.

I have been told that Grothendieck actually used the expression "local topos" for what has here been called "model topos", although in a different context, making the analogy with commutative rings even more striking.

For successive versions of this sheaf representation the reader is referred to [LM1982], [LS1986] and [L1989].

REFERENCES

P. H. ACZEL, *Saturated intuitionistic theories*, in: H.A. Schmidt et al. (eds), Contributions to mathematical logic, North Holland Publ. Co., Amsterdam 1969, 1–11.

G. BIRKHOFF, *Lattice theory*, AMS Coll. Publ. 25, 1967.

G. BIRKHOFF and J. D. LIPSON, *Heterogeneous algebras*, J. Combinatorial Theory 8 (1970), 115–133.

N. BOURBAKI, *Algèbre multilinéaire*, , Hermann, Paris 1948.

H. B. CURRY, *Some logical aspects of grammatical structures*, AMS Proceedings Symposium Applied Math. 12 (1961), 56–68.

H. B. CURRY and R. FEYS, *Combinatory Logic I*, North Holland Publ. Co., Amsterdam 1958.

S. FEFERMAN, *Review of Mann* [1975], Math. Reviews 52 (1976), 7869.

J.-Y. GIRARD, *Linear logic*, J. Theoretical Computer Science 50 (1987), 1–102.

K. GÖDEL, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Monatshefte für Mathematik und Physik 38 (1931), 173-198.

K. GÖDEL, *Über eine bisher noch nicht benutzte Erweiterung des finiten Standpunktes*, Dialectica 12 (1958), 280-287.

A. GROTHENDIECK and J. DIEUDONNÉ, *Eléments de géométrie algébrique I*, IHES Publ. Math. 4, Paris 1960.

L. A. HENKIN, *The completeness of first-order functional calculus*, J. Symbolic Logic 14 (1949), 159–166.

L. A. HENKIN, *Completeness in the theory of types*, J. Symbolic Logic 15 (1950), 81–91.

P. J. HIGGINS, *Algebras with a scheme of operators*, Math. Nachrichten 27 (1963), 115–132.

D. HILBERT and P. BERNAYS, *Grundlagen der Mathematik II*, Springer Verlag, Berlin 1939, 1970.

M. HYLAND, *A small complete category*, Ann. Pure and Applied Logic 40 (1988), 135–165.

S. C. KLEENE, *Introduction to metamathematics*, Van Nostrand, New York 1952.

J. LAMBEK, *The mathematics of sentence structure*, Amer. Math. Monthly 65 (1958), 154–169.

J. LAMBEK, *Deductive systems and categories III*, Springer LNM 274 (1972), 57–82.

J. LAMBEK, *On the unity of algebra and logic*, in: F.Borceux (ed.), Categorical algebra and its applications, Springer LNM 1348 (1988), 221–229.

J. LAMBEK, *Multicategories revisited*, Contemporary Math. 92 (1988), 217–339.

J. LAMBEK, *On the sheaf of possible worlds*, in: J. Adámek and S. MacLane (eds.), Categorical topology, World Scientific, Singapore 1989, 36–53.

J. LAMBEK, *Logic without structural rules*, Reports from the Dept. of Math. 91-02, McGill University, Montreal 1991; to appear in; K. Došen and P. Schroeder-Heister, Substructural logics, Oxford University Press.

J. LAMBEK, *Least fixpoints of endofunctors of cartesian closed categories*, Report from the Dept. of Math. 91-11, McGill University, Montreal 1991; to appear in *Mathematical Structures in Computer Science*.

J. LAMBEK, *From categorial grammar to bilinear logic*, Report from the Dept. of Math. 91-14, McGill University, Montreal 1991; to appear in: K. Došen and P. Schroeder-Heister, Substructural logics, Oxford University Press.

J. LAMBEK and I. MOERDIJK, *Two sheaf representations of elementary toposes*, in: A.S. Troelstra and D. van Dalen (eds.), The L.E.J. Brouwer Centenary Symposium, Studies in Logic and Foundations of Math. 110, North Holland Publ. Co., Amsterdam 1982, 275–295.

J. LAMBEK and P. J. SCOTT, *Introduction to higher order categorical logic*, Cambridge University Press, Cambridge 1986.

F. W. LAWVERE, *Functorial semantics of algebraic theories*, Dissertation, Columbia University, New York 1963.

F. W. LAWVERE, *Adjointness in foundations*, Dialectica 23 (1969), 281–296.

F. W. LAWVERE, *Equality in hyperdoctrines and comprehension schema as an adjoint functor*, in: A. Heller (ed.), Proc. New York Symp. on Applications of Categorical Algebra, Amer. Math. Soc., Providence, R.I. (1970), 1–14.

M. MAKKAI and R. PARÉ, *Accessible categories; the foundations of categorical model theory*, Contemporary Math. 104 (1990).

M. MAKKAI and G. E. REYES, *First order categorical logic*, Springer LNMG11 (1977).

A. I. MAL'CEV, *On a general theory of algebraic systems*, Math. Sbornik NS35 (1954), 3–20.

C. R. MANN, *The connection between equivalence of proofs and cartesian closed categories*, Proc. London Math. Soc. 31 (1975), 289–310.

P. MARTIN-LÖF, *Intuitionistic type theory*, Studies in Proof Theory I, Bibliopolis, Naples 1984.

D. PRAWITZ, *Natural deduction*, Almquist and Wiksell, Stockholm 1965.

G. E. REYES and H. ZOLFAGHARI, *Bi-Heyting algebras, toposes and modalities*, Rapports de récherches 91-9, Université de Montréal, 1991.

P. C. ROSENBLOOM, *The elements of mathematical logic*, Dover Publ., New York, 1950.

L. E. SANCHIS, *Functionals defined by recursion*, Notre Dame J. of Formal Logic 8 (1967), 161–174.

R. A. G. SEELY, *Locally cartesian closed categories and type theory*, Math. Proc. Cambridge Philosophical Soc. 95 (1984), 33–48.

R. A. G. SEELY, *Categorical semantics for higher order polymorphic lambda calculus*, J. Symbolic Logic 52 (1987), 969–989.

M. E. SZABO (ed.) The collected papers of Gerhard Gentzen, Studies in Logic and the Foundations of Math., North-Holland Publ. Co., Amsterdam 1969.

M. E. SZABO, *Polycategories*, Communications in Algebra 3 (1975), 663–689.

M. E. SZABO, *Algebra of proofs*, Studies in Logic and the Foundations of Math. 88, North-Holland Publ. Co., Amsterdam 1978.

A. S. TROELSTRA and D. VAN DALEN, *Constructivism in Mathematics I*, Studies in Logic and the Foundations of Math. 121, Elsevier Science Publishers, Amsterdam 1988.