INTRODUCTION TO CATEGORICAL LOGIC

JOSEPH HELFER

1. Motivation

We want to discuss Logic "from scratch" – that is, without any assumptions about any notions the reader may have of what logic is about or what "mathematical logic" is as a field.

We start simply by saying that logic is some part of our experience of reality that we want to understand – something to do with our capacity for thought, and the fact that our thought seems to have some kind of structure, or follow some kind of rules. We first want to identify (at least as a first approximation) *what logic is about*. As an analogy, *physics* is also about a part of our experience of reality. Our basic intuition about physics is that it is about *physical objects* – books, chairs, balls, and the like – and their properties. Indeed, the first (mathematical) physical theories – those of Galileo, Descartes, and Newton – describe the motion of such objects, the forces which act upon them, and so forth. Later, the kinds of things studied by physics – for example fields and thermodynamics systems – become more refined and complicated.

Similarly, we start with a simple view of what logic is about, allowing for refinements later on: logic is primarily about *propositions* and their *truth*. That is: it is a basic phenomenon that people make statements, and sometimes we observe them to be true (or false), and sometimes it is not immediately clear whether they are true, but we can decide it after some consideration. In logic, then, we are trying to investigate the relation of propositions to their truth, and to our capacity for deciding it.

Before continuing, let us say now what we only mentioned at the end of the talk: in the following, we will make free use of the concepts and constructions from usual modern mathematical practice. We will defining things called "logical operations" and something else called "sets", but we are not by any means trying to define the very notions we are making use of in discussing these things. That activity – namely, the absolutely primitive and self-contained explication of mathematical reasoning – is the development of the *foundations* of mathematics; it is also a very interesting and (for its purposes) important task. It is simply not what we are doing in this talk.

2. Setup

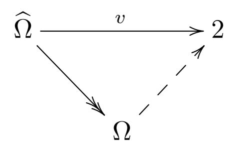
We begin then by positing as the basic ingredients of our theory:

(1) A set $\widehat{\Omega}$ of *propositions*
(2) A set $2 = \{T, F\}$ of *truth values* (which we call "True" and "False"), and
(3) A valuation function $v : \widehat{\Omega} \to 2$, which we think of as assigning to each proposition its truth value

Of course, we don't mean to imply that for any given proposition, we know what its truth value is, but we take it for granted that it has some truth value regardless.

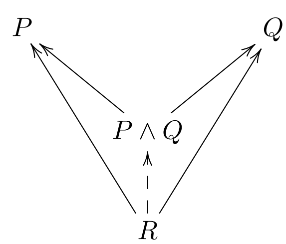
Next, we note the important phenomenon of *hypothetical reasoning*; that is, we can often conclude that one proposition must be true under the assumption that another is true, without knowing whether either of the propositions at hand actually is true. This we describe by a binary relation $P \leq Q$ on $\widehat{\Omega}$, with the property that if $P \leq Q$, then $v(P) = T$ implies $v(Q) = T$ (and hence also $v(Q) = F$ implies $v(P) = F$). We immediately see that we should take $\leq$ to be *transitive* and *reflexive*, thus making it into a *preorder*. We might also want to impose that its a *partial order* – i.e., anti-symmetric – but this isn't quite natural; there can easily be two propositions which imply each other (and are hence logically equivalent) but not identical. However, as always, we can form a quotient preorder Ω of $\widehat{\Omega}$ by identifying equivalent elements, which is a partial order. It is often more convenient to work with Ω.

It is also convenient to put an ordering on 2, by declaring that $F < T$, so that the function v is order-preserving. Since 2 is in fact a partial order, v factors through Ω:



We next turn to the well known *logical connectives*, with which we can combine propositions to form a new one whose truth value is in a certain definite relation to the truth values of the original propositions. The easiest (though by no means necessary) way to describe this is to note that $\widehat{\Omega}$, being a preorder, is also a *category*; namely, the one whose objects are the elements of the preorder and such that there is a unique arrow $P \to Q$ whenever $P \leq Q$. The existence of composites and identities corresponds to the reflexivity and transitivity of the preorder.

First, we consider logical conjunction ("and"). The fact that we can form the conjunction of any two propositions corresponds to the assumption that our category $\widehat{\Omega}$ has *products*. That is, for any propositions P, Q, there is a proposition $P \wedge Q$ with "projections" $P \leftarrow P \wedge Q \to Q$ (i.e., such that $(P \wedge Q) \leq P, Q$) and such that we can always complete the following diagram uniquely with a dotted arrow



Some reflection will reveal that this does indeed capture our intuition concerning the meaning of conjunction.

Of course, the uniqueness of the dotted arrow above is unimportant since we are dealing with a preorder. It is more convenient to write the defining property of $P \wedge Q$ in terms of its "adjunction relation":

$$\frac{R \leq P, Q}{R \leq (P \wedge Q)}$$

where the horizontal line indicates "if and only if".

Note that the defining property of $P \wedge Q$ (and of the other connectives below) does not determine it uniquely, but only up to equivalence. This is quite natural, as there is in general not a unique proposition expressing the logical conjunction of two others.

Next, we have disjunction ("or"). This corresponds to requiring $\widehat{\Omega}$ to have coproducts, and is given by the adjunction relation:

$$\frac{P, Q \leq R}{(P \vee Q) \leq R}$$

We also demand that $\widehat{\Omega}$ has a *terminal object*; i.e. an object 1 such that $P \leq 1$ for all P. This corresponds to the fact that there are *tautologies* – that is, propositions which are vacuously true – which can be deduced under the assumption of any proposition whatsoever.

Similarly, there are *absurdities* – propositions which are vacuously false. It is less clear *a priori*, but is nonetheless confirmed by experience, that we can deduce anything whatsoever once we assume an absurdity. Hence, we assume that $\widehat{\Omega}$ also has an *initial object*.

Next, we can form the *implication* between two propositions – that is, the proposition that one proposition follows from another. This is seen to be described by the adjunction relation

$$\frac{P \wedge Q \leq R}{P \leq (Q \Rightarrow R)}$$

Note that we can deduce "*modus ponens*"; i.e., the fact that $(P \wedge (P \Rightarrow Q)) \leq Q$ for any P and Q.

Next, we have *negation*. This can be defined using implication and absurdity by saying that to negate a proposition is to say that it implies an absurdity: $\neg P := (P \Rightarrow \bot)$. It follows immediately from this (by *modus ponens*) that $P \wedge \neg P \leq \bot$; anything together with its negation implies an absurdity. Although this definition of negation determines $\neg P$ up to isomorphism, it does not follow from this that $\neg(\neg P)$ is equivalent to P, as we might expect. Therefore, we impose this as an extra condition. We will have more to say about this later on. Once we assume $\neg(\neg P)$ it can be shown that $P \Rightarrow Q$ is equivalent to $\neg P \vee Q$ for every P, Q.

The structure defined above on $\widehat{\Omega}$ induces the same structure on Ω, turning the latter into a so-called *Boolean algebra*, which is exactly a partial order with all the above-mentioned properties (that is, finite products and coproducts, implications and negations)[1]. This structure can also be defined algebraically, as a set with three binary operations $\wedge, \vee, \Rightarrow$ and two constants $0, 1$ satisfying certain laws. It follows from the laws that the conditions $P \wedge Q = P$, $P \vee Q = Q$, and $P \Rightarrow Q = 1$ are all equivalent, and if we define $P \leq Q$ to be given by this condition, we find that it is a partial order having the properties of a Boolean algebra for which the operations $\vee, \wedge, \Rightarrow$ and the elements $0, 1$ are the ones we started with. We will not give the laws here, since we will not need them – however, as a very inefficient set of laws, we could simply take every equation which holds in all Boolean algebras.

Let us call the corresponding structure on $\widehat{\Omega}$ a *Boolean prealgebra*; that is, a Boolean prealgebra is a preorder whose quotient partial order is a Boolean algebra.

It is easy to see that 2, with its ordering, is also a Boolean algebra, for which the operations are the usual Boolean operations familiar from computer science. In fact, there is an obvious category of Boolean algebras (the morphisms are the functions which preserve the operations $\wedge, \vee, \Rightarrow$), in which 2 is an *initial object*. The reason is that any morphism out of 2 must send F to 0 and T to 1, and this of course determines the morphism completely.

2.1. **Truth tables.** Let us now consider a very general example of the kind of structure we might find inside $\widehat{\Omega}$. Let us assume that there are n propositions $P_1, \ldots, P_n \in \widehat{\Omega}$ that are "logically independent", in the sense that the truth of any of them has no bearing on the truth of any of the others (for example, P_1 might be "It rained in Tokyo on September 23,

[1]There is actually one more law, namely the *distributive* law, which says that $\wedge$ and $\vee$ distribute over each other.

1972" and P_2 might be "Every even number is the sum of two primes", etc.); in particular, we should not have $P_i \leq P_j$ for any $i \neq j$. We let them generate a subset $B \subset \widehat{\Omega}$, in the sense that B is a minimal subset of $\widehat{\Omega}$ containing $P_1, \ldots, P_n$ and closed under conjunction, disjunction, and negation. We find that the ordering restricted to B is in fact a *partial order*; that is, B is a Boolean algebra and, corresponding to the assumption that the P_i are "logically independent", we suppose that B is *free* on the generators $P_1, \ldots, P_n$. This means that any n elements $a_1, \ldots, a_n$ of a Boolean algebra B' determine a unique Boolean algebra homomorphism $B \to B'$ sending P_i to a_i for each i. In particular, letting $B' = 2$, we find that the value of v on the elements of B is determined by its value on the P_i. The algorithm by which $v(P)$ can be calculated given the $v(P_i)$ is the well known method of "truth tables".

3. Things

3.1. **An insight.** We now make the crucial observation – which was surely recognized intuitively for a long time, but first made explicit by Gottlob Frege and his contemporaries – that propositions are *about things*. This corresponds to the fact that grammatically correct sentences have a *subject* and a *predicate*.

Following Frege, we assume there is a set U which contains all the things; that is, U contains everything you might ever want to make a statement about. We then define a *predicate* P to be a function $U \to \widehat{\Omega}$ which assigns to each thing x a proposition $P(x)$. Hence, if P is the predicate "is at the center of the universe" and x is the thing "The earth", then $P(x)$ is the proposition "The earth is at the center of the universe". Similarly, an *n-ary relation* is a function $U^n \to \widehat{\Omega}$; for example, "is at the center of" is a binary relation. We denote the set of n-ary relations by $\widehat{\Omega}_n$.

The preorder on $\widehat{\Omega}$ induces one on $\widehat{\Omega}_n$ by comparing two relations "pointwise"; that is, we say that $P \leq Q$ if $P(a) \leq Q(a)$ for each $a \in U$. We can again identify equivalent elements under this preorder to obtain a set Ω_n, which can also be defined as the set of functions from U^n to Ω. The set Ω_n with the induced ordering is immediately seen to be a Boolean algebra, where the operations $\wedge, \vee, \neg$ are given "pointwise". Similarly, $\widehat{\Omega}_n$ is a Boolean prealgebra. Note that $\widehat{\Omega}_0$ is isomorphic to $\widehat{\Omega}$.

Given n things $a_1, \ldots, a_k \in U$, we get an "evaluation" homomorphism $\widehat{\Omega}_k \to \widehat{\Omega}$ (or $\Omega_k \to \Omega$), which we can compose with $v : \widehat{\Omega} \to 2$ to obtain a homomorphism $\widehat{\Omega}_n \to 2$ indicating for each relation whether it holds of $a_1, \ldots, a_n$. We also more generally obtain homomorphisms $\widehat{\Omega}_n \to \widehat{\Omega}_{n-k}$ by "partially evaluating".

The first and most important example of a relation is equality. That is, we assume the existence of a particular predicate $eq : U^2 \to \widehat{\Omega}$ such that $eq(a, a)$ is tautologous (reflexivity), $eq(a, b) \leq eq(b, a)$ (symmetry) and $eq(a, b) \wedge eq(b, c) \leq eq(a, c)$ (transitivity) for $a, b, c \in U$.[2]

3.2. **Some model theory.** We now consider an example of the kind of thing we might expect to find in $\widehat{\Omega}_n$. Let us suppose that natural numbers are things, i.e. that $\mathbb{N} \subseteq U$, and let us restrict our attention to predicates and relations about the natural numbers. More precisely, we consider those relations $R \in \widehat{\Omega}_n$ which are "supported on $\mathbb{N}$", i.e. such that $R(a_1, \ldots, a_n)$ is absurd whenever some $a_i \notin \mathbb{N}$. We denote the set of n-ary relations supported on $\mathbb{N}$ by $\widehat{\Omega}_n^{\mathbb{N}}$. It is easy to see that $\widehat{\Omega}_n^{\mathbb{N}}$, with the restricted preorder, is a Boolean

[2]It might seem that in addition to the assumption that $eq(a, a)$ is always tautologous, we should also have that $eq(a, b)$ is always absurd (or at least false) whenever a and b are distinct elements of U. However, there are clearly statements of the form "a is equal to b" which are true even though a and b are not identical. What this indicates is that we should not really think of U as the set of *things*, but rather as the set of "descriptions of things".

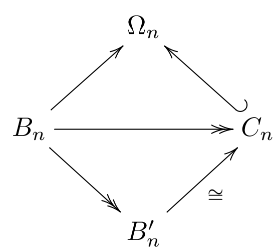
prealgebra in its own right. A maximal element $R(x_1, \ldots, x_n)$ of $\widehat{\Omega}_n^{\mathbb{N}}$ is one which says exactly "$x_1, \ldots, x_n$ are natural numbers" – i.e., which is tautologous whenever each $x_i \in \mathbb{N}$ and absurd otherwise.[3]

A typical example of something we might find in $\widehat{\Omega}_3$, say, is "x plus y equals z". We can more generally consider the subalgebra $\widehat{C}_n$ of $\widehat{\Omega}_n^{\mathbb{N}}$ consisting of all of the "arithmetic relations". That is, it is the smallest subset closed under conjunction, disjunction, and negation and which contains, for each pair $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ of polynomials with coefficients in $\mathbb{N}$, the proposition $eq(p(x_1, \ldots, x_n), q(x_1, \ldots, x_n))$[4]. We denote by C_n the image of $\widehat{C}_n$ in Ω_n.

We now give an alternative construction of C_n. Let $F_n = \mathbb{N}[x_1, \ldots, x_n]$ be the semi-ring[5] of polynomials in n variables with coefficients in $\mathbb{N}$, and let B_n be the Boolean algebra freely generated by the set $F_n \times F_n$ of pairs of polynomials (where we think of the pair (p, q) as the equation "$p = q$"). Notice that, unlike in the free Boolean algebra considered in Section 2.1, the generators here are (intuitively speaking) *not* "logically independent". For example, we should have that $(p, q) \leq (q, p)$ for any polynomials p and q. That is, we have the "wrong" Boolean algebra.

However, we can associate to a pair $(p, q) \in F_n \times F_n$ the predicate defined above sending $a_1, \ldots, a_n$ to $eq(p(a_1, \ldots, a_n), q(a_1, \ldots, a_n))$. Since B_n is free, this assignment of generators determines a unique morphism $B_n \to \Omega_n$. The image of this is of course precisely C_n.

Now, Boolean algebras satisfy the usual "first isomorphism theorem" from algebra. That is, associated to the morphism $B_n \to \Omega_n$ there is a "kernel", namely the set of all elements of B_n whose image is 1. A set of this form – that is one arising as the kernel of a homomorphism – is called an *ultrafilter*. We can then form a quotient Boolean-algebra B'_n by identifying elements p and q whenever $p \Rightarrow q$ and $q \Rightarrow p$ are both in the ultrafilter. As usual, we get that the quotient of B_n by this ultrafilter is isomorphic to the image of the original morphism:



Now, for each tuple $(a_1, \ldots, a_n) \in \mathbb{N}^n$, we obtain a morphism $B_n \to 2$ by the composite

$$B_n \to C_n \hookrightarrow \Omega_n \to \Omega \xrightarrow{v} 2$$

---

[3]Every 0-ary relation – i.e., proposition – is supported on $\mathbb{N}$ and hence "about the natural numbers" according to this definition. It therefore seems better to treat the 0-ary case of "the set of propositions about natural numbers" separately and define it as the set of all propositions $R(n_1, \ldots, n_k)$ where R is a relation about natural numbers (with $k \geq 1$) and $n_1, \ldots, n_k \in \mathbb{N}$. Note that these form a Boolean prealgebra.

[4]There is a subtle distinction here related to footnote 2 above. Namely, there are two ways of understanding what is meant, say, by "the predicate taking x, y to, $eq(x^{10000}, y^{5000})$". On the one hand, we may mean the predicate which evaluates eq on the numbers x^{10000} and y^{5000}. But it seems better to consider "x raised to the 10000th power" and "y raised to the 5000th power" themselves as things, distinct from the numbers x^{10000} and y^{5000}, and that it is these things on which eq is being evaluated. Of course, for a given x, we should expect the proposition $eq(x^{10000},$ "x raised to the 10000th power") to be true (though probably not tautologous).

[5]By a semi-ring (which we should perhaps call a "commutative, unital semi-ring") we mean a set with two binary operations ("addition" and "multiplication") such that each one is associative, addition is commutative, and multiplication distributes over addition.

where the third morphism is "evaluation at $(a_1, \dots, a_n)$". This composite says whether the given arithmetic relation is true for the given tuple.

We now note that there is nothing special about $\mathbb{N}$ for the above construction. Any n elements $a_1, \dots, a_n$ of *any* semi-ring R whatsoever determine a unique morphism $f : F_n \to R$ sending x_i to a_i for each i. We can then define a morphism $B_n \to 2$ by sending the generator (p, q) to T if $f(p) = f(q)$ and F otherwise. The corresponding morphism $B_n \to 2$ then says for each element of B_n whether the given arithmetic relation holds for $a_1, \dots, a_n \in R$.

Now, for each such choice of R and $a_1, \dots, a_n$, we get an ultrafilter by taking the kernel of the associated morphism $B_n \to 2$. It is easily seen that the intersection of an arbitrary family of ultrafilters is again an ultrafilter. Let us take the intersection of all these ultrafilters and denote by $\bar{B}_n$ the quotient by it. We then clearly have that each morphism $B_n \to 2$ described above factors through $\bar{B}_n$.

Conversely, it can be shown that any morphism $\bar{B}_n \to 2$ whatsoever arises in this way (we leave this as an exercise). Thus, $\bar{B}_n$ in some sense captures the "theory of n-ary arithmetic relations on semi-rings".

Now, for a fixed semi-ring R we can factor the associated morphisms $\bar{B}_n \to 2$ as follows. We first note that the set $\mathcal{P}(X)$ of subsets of any set X naturally carries the structure of a Boolean algebra, where the ordering is the subset relation, and conjunction, disjunction, and negation are given by intersection, union, and complement, respectively. Given any element $a \in X$, we obtain a morphism $X \to 2$ which indicates for a given subset whether it contains a.

We now define a morphism $\bar{B}_n \to \mathcal{P}(R^n)$ by sending each relation in $\bar{B}_n$ to the set of tuples of R^n for which it holds. The morphisms $\bar{B}_n \to 2$ associated to R and a tuple $(a_1, \dots, a_n)$ is then the composite

$$\bar{B}_n \to \mathcal{P}(R^n) \to 2$$

where the second morphism is the one associated to the element $(a_1, \dots, a_n) \in R^n$.

This provides a certain intuition about the meaning of $\bar{B}_n$. Namely, we can think of its elements as being certain subsets of (the n-th cartesian product of) a "generic semi-ring" – namely the "arithmetically definable" ones. Given any semi-ring R, the morphism $\bar{B}_n \to \mathcal{P}(R^n)$ then realizes each such "generic" arithmetically definable subset as an actual arithmetically definable subset of R^n. We will make this intuition somewhat more precise later.

We note however that there is something unsatisfying about the present setup. Namely, whereas the morphisms $\bar{B}_n \to 2$ were exactly the ones arising from an n-tuple of elements of a ring, it is by no means the case that every morphism from $\bar{B}_n$ to a Boolean algebra arises as one of these morphisms $\bar{B}_n \to \mathcal{P}(R^n)$ for some semi-ring R. There is an additional mystery which is that, given a semi-ring R, we get a morphism $\bar{B}_n \to \mathcal{P}(R^n)$ *for each* n, but these don't seem to fit together in any interesting or coherent way. Both of these mysteries will be resolved later, once we switch to a more categorical perspective.

3.3. **Quantification.** Returning to the general story, we now introduce the last important propositional constructions, namely the quantifiers "for all" and "there exists". Before diving into this, we want to describe a certain *thesis* – which we call "Frege's thesis"[6] associated to the system obtained by adjoining the quantifiers to the Boolean operations that we have already introduced. The thesis is that the system thus obtained – which Frege called a "formal language of thought", and which we now call "first-order logic" – along with

[6] I have since discovered that some people call this "Hilbert's thesis", which is presumably more appropriate/historically accurate.

its associated rules, in some sense *completely captures* the phenomenon of logical reasoning. We will return to this below.

The significant feature of quantification which was absent in the logical constructions introduced thus far is that it involves an interplay between the Ω_n for different values of n. For example, if $R(x, y, z)$ is a ternary relation – i.e., an element of $\widehat{\Omega}_3$, then $\forall z : R(x, y, z)$ should be an element of $\widehat{\Omega}_2$.

We should first note the connections between the various $\widehat{\Omega}_n$ which are already present in what we have introduced so far. These are best seen by first observing that the definition of $\widehat{\Omega}_n$ given above (and in the talk) – namely, as the set of all functions $U^n \to \widehat{\Omega}$ whatsoever, is both unnecessary and also unnatural, since it allows predicates which assign completely unrelated propositions to different things.

Rather, we should only demand that $\widehat{\Omega}_n$ be a certain *subset* of the set of functions $U^n \to \widehat{\Omega}$, whereupon certain "closure conditions" naturally suggest themselves. First, we still have, as before, an induced preorder on $\widehat{\Omega}_n$, but we must now *demand* that this preorder turn $\widehat{\Omega}_n$ into a Boolean prealgebra (moreover – we're not sure if this follows automatically – the operations $\wedge, \vee, \neg$ should be given by applying them pointwise in $\widehat{\Omega}$). The second condition is that given an n-ary relation $R \in \widehat{\Omega}_n$ and a function $\sigma : \{1, \ldots, n\} \to \{1, \ldots, k\}$, the function $U^k \to \widehat{\Omega}$ which sends $a_1, \ldots, a_k$ to $R(a_{\sigma(1)}, \ldots, a_{\sigma(n)})$ should be a k-ary relation. The third condition is similar: it is that we should be able to view an n-ary relation as an $(n+1)$-ary relation by ignoring one of the arguments.

More precisely, we have a function $\pi_{\hat{\imath}} : U^{n+1} \to U^n$ obtained by projecting onto all but the i-th factor (where $1 \leq i \leq n+1$). The condition, then, is that for each n-ary relation $R : U^n \to \widehat{\Omega}$, the composite $(R \circ \pi_{\hat{\imath}}) : U^{n+1} \to \widehat{\Omega}$ is an $(n+1)$-ary relation.

This last condition brings us directly to the definition of quantifiers. Namely, the above-described operation $s_i : \widehat{\Omega}_n \to \widehat{\Omega}_{n+1}$ obtained by composing with $\pi_{\hat{\imath}}$ preserves the preorder, and hence defines a *functor*. Demanding that the relations be closed under quantification is then seem simply to amount to asking that this functor has a left and right adjoint.

More explicitly, this means that (say) the existential quantifier $\exists$ should be characterized by the following condition. If $\phi \in \widehat{\Omega}_{n+1}$ and $\psi \in \widehat{\Omega}_n$, then we should have

$$\frac{\phi \leq (s_i \psi)}{\exists x_i : \phi \leq \psi}$$

where the horizontal line as usual means "if and only if". This is best understood by staring at and pondering over it for a while, but we will try our best to explain it.

We recall that the preorder on k-ary relations is defined so that $R \leq S$ if and only if $R(b_1, \ldots, b_k) \leq S(b_1, \ldots, b_k)$ for *every* possible choice of $b_1, \ldots, b_k \in U$. Hence, the condition above the line is that

$$\phi(x_1, \ldots, x_{n+1}) \leq \psi(x_1, \ldots, \hat{x}_i, \ldots, x_{n+1})$$

(where $\hat{x}_i$ indicates that the argument x_i is omitted) for every choice of $x_1, \ldots, x_{n+1}$. But since the right side does not depend on x_i, it is clear that it will follows as soon as there is *some* x_i for which $\phi(x_1, \ldots, x_{n+1})$. But this amounts (according to our intuitive understanding of the symbol $\exists$) to the condition that

$$\exists x_i : \phi(x_1, \ldots, x_{n+1}) \leq \psi(x_1, \ldots, \hat{x}_i, \ldots, x_{n+1})$$

for every $x_1, \ldots, \hat{x}_i, \ldots, x_{n+1}$, which is precisely the condition below the line.

Similarly, universal quantification is defined by the condition

$$\frac{(s_i \psi) \leq \phi}{\psi \leq \forall x_i : \phi}$$

Again, this is seen to correspond to our intuition: if

$$\psi(x_1, \ldots, \hat{x_i}, \ldots, x_{n+1}) \leq \phi(x_1, \ldots, x_{n+1})$$

for *every* possible possible value of $x_1, \ldots, x_{n+1}$ then, since the left side does not depend on x_i, we have that for a fixed $x_1, \ldots, \hat{x_i}, \ldots, x_{n+1} \in U$, $\phi(x_1, \ldots, x_{n+1})$ will hold *for every* x_i as soon as $\psi(x_1, \ldots, \hat{x_i}, \ldots, x_{n+1})$ holds.

Hence, we add to our list of assumptions that these adjoints exist for every $s_i : \widehat{\Omega}_n \to \widehat{\Omega}_{n+1}$.

Returning now to Frege's thesis, we note that it has two parts

(1) Every mathematical statement that can be expressed can be expressed in the language of first-order logic
(2) Every *true* mathematical statement can be proven using the rules of first-order logic

The first statement is something like the famous Church-Turing thesis (which says that everything which can be effectively computed can be computed by a Turing machine), in that it involves an undefined term – here "mathematical statement that can be expressed" – and hence cannot be proven. Rather, we can only ask the empirical question of whether any mathematical statement that anyone has expressed *so far* can be expressed in first-order logic. Here, the answer is *yes*, though with the important qualification that the language be extended with a *vocabulary* for describing the mathematical objects under consideration; in particular, it is very important that we be able to talk about *sets* (as we will describe in the next section). In fact, the amazing discovery of Frege, Georg Cantor, and their contemporaries is that the *only* thing you need to be able to talk about is sets.

The second statement, on the other hand, can be given a rigorous formulation, by formulating a suitable definition of *truth* (as we have been trying to do), and also of *provability* (that is, provability according to the rules of first-order logic). When this is done, the second statement is confirmed, and goes under the name of *Gödel's completeness theorem.*

4. Sets

Let us now return to the set U of things, and introduce a more general assumption about it than the one above (that it includes the natural numbers).

First, we suppose that certain things are *sets.* That is, we suppose that there is a binary relation $\varepsilon \in \widehat{\Omega}_2$ which we call "membership", so that we read $a \varepsilon b$ as "b is a set and a is a member of b".

Following Cantor and Frege, we then make the following assumption on U: that for each predicate $p \in \widehat{\Omega}_1$, there is a (unique) thing $[p] \in U$ such that for every thing $a \in U$, we have $a\varepsilon[p] \cong p(a)$. That is, $[p]$ is the "set of all things satisfying p".

Now, this axiom, which is called "unrestricted comprehension" is extremely powerful, as Frege demonstrated. Its repeated application allows for the generation of all known mathematical objects.

As an example, we can define the natural numbers as sets using the "Von Neumann encoding". We define 0 to be the empty set, which can be defined using comprehension as $[p]$ where p is an absurdity. We then define the successor of the Von Neumann number n to be $[p]$, where $p(x) = (x \varepsilon n) \vee eq(x, n)$. We then have that the set encoding n is equal to $\{0, \ldots, n-1\}$.

In like manner, one can go on to define addition and multiplication of natural numbers, the rational and real numbers, as well as everything else. We will not say any more about this, but it is explained in any text on set-theoretical foundations.

As a matter of fact, the principle of unrestricted comprehension is far *too* powerful, in that you can use it to prove literally *everything* – that is to say, it is inconsistent! We are referring, of course, to the famous "Russell's paradox", which we now describe.

Let us define the predicate q by $q(x) = \neg(x \varepsilon x)$. We then have

$$[q]\varepsilon[q] \cong q([q]) \cong \neg([q]\varepsilon[q])$$

That is, we have that the element $[q]\varepsilon[q]$ of $\widehat{\Omega}$ is equivalent to its negation. It is easily seen that this can never happen in a Boolean (pre)algebra. Hence, we conclude that there simply *cannot* be for each predicate $p \in \widehat{\Omega}_1$ a thing $[p] \in U$ with the desired property.

However, we do not actually need, in practice, the comprehension principle for *any predicate p whatsoever*, but only for certain ones, for example the ones arising in the above construction of the natural numbers. Hence, instead of taking the full unrestricted comprehension principle, we can try to identify a certain set of special cases which suffice for all practical purposes, but which (at least appear to) exclude the construction needed for Russell's paradox. Doing so, one arrives at the modern system of axiomatic set theory, which allows one in a very satisfactory manner to formulate and prove all known mathematical statements, as promised by Frege.

It should be mentioned that when these set-theoretical axioms are used as a foundation for mathematics, they are of course not described, as they were here, *in terms of sets*. Rather, it is done completely "linguistically"; one constructs a certain formal system consisting of strings of symbols and rules for manipulating them which, intuitively, represent the objects we have been discussing here. However, as mentioned in the introduction, it is not our goal to discuss these foundational aspects here.

It seems, then, that we've wrapped up everything very nicely. We have our set of things, which contains sets and with it all the mathematical objects. However, let us not forget the lingering mystery from before, about connecting the various $\bar{\bar{B}}_n$ in order to produce an object which more fully embodies the "theory of rings"...

5. Topoi

5.1. **A fresh start.** We will now make a somewhat confusing change of perspective, so please bear with me.

In our previous discussion, there were two notions of *set*. First, there was the "ambient" notion. This is the one we used from the very beginning of our discussion, in saying things like "Ω is a set with such and such additional structure" and "we introduce a set U which we call the set of things". We did not make the notion explicit, but relied on our mutual understanding of which operations on sets are admissible, and what their properties are. This is of course the tacit assumption that goes into usual every-day discussion about mathematical topics and – as usual – although we *could* make our talk of sets more precise, we do not bother to do so because it is irrelevant for our present purposes.

On the other hand, *within* our discussion, we had a second notion of set. According to this second notion, a *set* is a certain element of U.[7]

To add to the confusion, these two notions of sets are not completely incommensurable; sometimes we can compare a set in the ambient sense, to the "sets" in U. Namely, given any subset $S \subset U$, we can ask if there is an element $s \in U$ for which $x \varepsilon s$ is tautologous whenever $x \in S$ and is absurd otherwise. In fact, the "axioms of set theory" alluded to above, which are special cases of the comprehension principle, ensure the existence of

[7]Though note that our discussion doesn't single out precisely *which* elements of U are sets. Rather, it at best allows us to define a predicate (i.e., Ω-valued function on U) $P(x)$ which (intuitively) expresses "x is a set". We could then go on to single out those elements which are "definitely sets" – i.e., those x for which $P(x)$ is tautologous.

such s for many subsets $S \subset U$. However, under the very reasonable assumption that the correspondence taking S to s be injective, we see by Cantor's theorem (which says that the power set operation strictly increases cardinality) that there must be subsets $S \subset U$ for which there is no corresponding s. In particular, assuming the well-known "axiom of subsets", we have by the same argument given above ("Russell's paradox") that U itself cannot be thus represented.

Of course, all these problems were unknown to Frege when he first conceived of this picture of reality; as far as he knew, the universe U simply *could* be regarded as one of the sets in U, and there was generally no serious distinction between sets in the "ambient" and "internal" senses. However, we must acknowledge that there *is* such a distinction, and – while the theory remains quite satisfactory for the purposes of doing mathematics – there is something decidedly unsettling about being forced to carry around this distinction between "large" and "small" sets.

So we would now like to change our perspective. Rather than assuming to begin with a universe U of all things, and then singling out sets as specific things, we will introduce sets right from the beginning. That is, according to our new conception, there will be no conception of *thing* besides "element of a set". In particular, our set Ω of propositions will now be a set in the "internal" sense, and not in the "ambient" sense. As we will see presently, our new approach will be based on categories, and the only extent to which we will need to refer to the "ambient" sets is insofar as we need them to define categories.

5.2. **Axioms.** Our new definition of "set" will proceed as follows: we will impose certain axioms on a category $\mathbf{C}$ which insure that all the usual operations on sets can be performed on the objects of $\mathbf{C}$, and then we will simply define a *set* to be an object of $\mathbf{C}$. Let us now state the relevant axioms.

Axiom 1. $\mathbf{C}$ *has a terminal object* $\mathbf{1_C}$.

The terminal object is understood to be the "one element set". The importance of this axiom lies chiefly in that it allows us to define the notion of *element*; namely, an element of an object X is simply a morphism $\mathbf{1_C} \to X$. But let now us call attention to a possible confusion which may arise: for any object X, we will now have the (ambient) set $\mathbf{C}(\mathbf{1_C}, X)$ of morphisms from $\mathbf{1_C}$ to X – that is, of "elements of X". We emphasize that the object X is *not in any way* identified with the (ambient) set $\mathbf{C}(\mathbf{1_C}, X)$. They are simply different kinds of things; one is an object of a category, the other is a set.

Axiom 2. $\mathbf{C}$ *has binary products*

This corresponds to the assumption that we should be able to form the product of any two sets.

Axiom 3. $\mathbf{C}$ *has exponential objects*

Here, we mean "exponential objects" in the usual categorical sense – the "implication objects" in our Boolean (pre)algebras above were special cases of this. Namely, for any objects X, Y, there should be an object Y^X and a morphism $ev_{X,Y} : Y^X \times X \to Y$ such that for any object Z and morphism $t : Z \times X \to Y$, there should be a unique morphism $\lambda_X t : Z \to Y^X$ such that

$$\begin{array}{ccc} Y^X \times X & \xrightarrow{e} & Y \\ {\scriptstyle (\lambda_X t)\times \mathrm{id}_X}\uparrow & \nearrow_{t} & \\ Z \times X & & \end{array}$$

commutes.

This corresponds to the assumption that we should be able to form the set of functions from any set to any other set.

It is important to note that the categorical notions "terminal object", "product", "exponential object" do indeed characterize – in the category **Set** of (ambient) sets – up to isomorphism (that is, bijection) the one-element set, the product set, and the function set. However, to convince ourselves that this a "reasonable" generalization of the corresponding "ambient" notions requires some reflection: we should convince ourselves that the categorical characterizations are "sufficient" in practice – i.e., that anything we might want to say about, say, the product, follows from this characterization.

5.3. **Logic.** Next, we want to introduce the very important axiom of *subsets*, which says that given any set X and property p, we should be able to form the set $\{x \in X \mid p(x)\}$. Of course, to make sense of this, we have to say what we mean by "property". We clarify this by reintroducing Ω (the set of propositions), as promised, as an object in our category $\mathbf{C}$; a property of elements of X will then be a "predicate on X", i.e. a morphism $X \to \Omega$.

As before, we want to impose certain natural structures (a partial order and the various logical operations) on Ω. But how are we to do this, now that Ω is no longer a(n ambient) set, but simply an object in our category $\mathbf{C}$?

The simplest thing one could ask for is a Boolean algebra structure on the "ambient" set $\mathbf{C}(\mathbf{1_C}, \Omega)$. However, this is a very unnatural requirement from the viewpoint of category theory. A more general and natural requirement is that of a Boolean algebra structure on the ambient sets $\mathbf{C}(X, \Omega)$ (equivalently, on the sets $\mathbf{C}(\mathbf{1_C}, \Omega^X)$) for *all* objects X of $\mathbf{C}$. Moreover, there is a *naturality* condition which presents itself: given two objects X and Y and a morphism $f : X \to Y$, composing with f produces a function $f^* : \mathbf{C}(Y, \Omega) \to \mathbf{C}(X, \Omega)$. The condition is that this always be a Boolean algebra homomorphism. (This is indeed very plausible, as f^* is, intuitively, just the function taking each predicate "$p(y)$" to the predicate "$p(f(x))$").

By usual category-theoretic nonsense, this naturality condition allows us to reformulate the whole requirement in a way which does not make any reference at all to ambient sets, but rather only to the internal structure of the category.

For example, the requirement that there be an operation $\wedge_X : \mathbf{C}(X, \Omega) \times \mathbf{C}(X, \Omega) \to \mathbf{C}(X, \Omega)$ for each object X implies in particular that there is one with $X = \Omega \times \Omega$:

$$\wedge_{\Omega\times\Omega} : \mathbf{C}(\Omega \times \Omega, \Omega) \times \mathbf{C}(\Omega \times \Omega, \Omega) \to \mathbf{C}(\Omega \times \Omega, \Omega) \tag{1}$$

The set on the left side of (1) is naturally in bijection with $\mathbf{C}(\Omega \times \Omega, \Omega \times \Omega)$ and therefore contains a special element (namely the pair (π_1, π_2) of projections) corresponding to $\mathrm{id}_{\Omega\times\Omega}$. Let us denote the image in $\mathbf{C}(\Omega \times \Omega, \Omega)$ of this element under the function (1) simply by $\wedge$.

The naturality condition implies that, for any object X and morphisms $p, q : X \to \Omega$, the square

$$\begin{array}{ccc} \mathbf{C}(\Omega \times \Omega, \Omega) \times \mathbf{C}(\Omega \times \Omega, \Omega) & \xrightarrow{\wedge_{\Omega\times\Omega}} & \mathbf{C}(\Omega \times \Omega, \Omega) \\ \downarrow {\scriptstyle \langle p,q\rangle^* \times \langle p,q\rangle^*} & & \downarrow {\scriptstyle \langle p,q\rangle^*} \\ \mathbf{C}(X \times X, \Omega) \times \mathbf{C}(X \times X, \Omega) & \xrightarrow{\wedge_X} & \mathbf{C}(X \times X, \Omega) \end{array}$$

is commutative. Starting with the element (π_1, π_2) in the top left and chasing it around, we find that

$$p \wedge_X q = \wedge \circ \langle p, q \rangle \tag{2}$$

In particular, each $\wedge_X$ is determined by $\wedge$. We can then start with $\Omega \times \Omega \xrightarrow{\wedge} \Omega$ and *define* $\wedge_X$ using (2). The "naturality condition" that f^* takes $\wedge_Y$ to $\wedge_X$ for any $f : X \to Y$ then follows automatically.

If we now have morphisms $\top, \bot : 1 \to \Omega$ and $\wedge, \vee, \Rightarrow : \Omega \times \Omega \to \Omega$, they will induce corresponding operations on each $\mathbf{C}(X, \Omega)$ and these will be preserved by each f^*. If we moreover demand that the above morphisms satisfy the equations defining a Boolean algebra – we say in this case that they make Ω into a *Boolean algebra object* or *internal Boolean algebra* – then it follows that the operations on each $\mathbf{C}(X, \Omega)$ make these sets into Boolean algebras as well.

Let us now returning to the question of subsets. First, before discussing the formation of subsets $\{x \in X \mid p(x)\}$, let us discuss the categorical substitute for the general notion of subset.

Given an object X, a subset A of X should first of all be another object A together with an inclusion morphism $A \xrightarrow{i_A} X$. That i_A exhibits A as a subset of X is captured by the property that any morphism $Y \xrightarrow{\bar{f}} A$ should be determined by the composite $Y \xrightarrow{\bar{f}} A \xrightarrow{i_A} X$. That is, for a given morphism $Y \xrightarrow{f} X$, there should be *at most one* factorization

$$\begin{array}{ccc} & & A \\ & \overset{\bar{f}}{\nearrow} & \downarrow{\scriptstyle i_A} \\ Y & \xrightarrow[f]{} & X \end{array} \tag{3}$$

This is of course the familiar categorical notion of i_A being a *monomorphism*.

Now, given a predicate $p : X \to \Omega$, what should it mean that the subset $i_A : A \to X$ is the one $\{x \in X \mid p(x)\}$ determined by p? We again characterize this by a lifting property as in (3).

Given a morphism $f : Y \to X$, we can compose it with $p : X \to \Omega$ to obtain the predicate $p \circ f : Y \to \Omega$. Clearly, the image of f should land in the subset $\{x \in X | p(x)\}$ if and only if this predicate $p \circ f$ is *true* for every element of Y – that is, if and only if $p \circ f$ is equal to the composite $\top_Y$ of $Y \to \mathbf{1_C} \xrightarrow{\top} \Omega$.

Thus, we say that $i_A : A \to X$ is the subset determined by p if for each $f : Y \to X$ the unique lift $\bar{f}$ of (3) exists if and only if $p \circ f = \top_Y$. This is equivalent to the following being a pullback diagram

$$\begin{array}{ccc} A & \longrightarrow & \mathbf{1_C} \\ {\scriptstyle i_A}\downarrow & & \downarrow{\scriptstyle \top} \\ X & \xrightarrow{p} & \Omega \end{array} \tag{4}$$

We would now like to demand that this subset exists for every predicate p:

Axiom 4. $\mathbf{C}$ *has pullbacks.*

This seems stronger than just demanding the existence of the pullbacks (4), but assuming Axiom 5 below characterizing Ω (which we have not yet introduced into our axioms), the existence of general pullbacks follows from those of the form (4). Note that Axioms 1 and 4 together make Axiom 2 redundant.

Next, we observe that for any subset A of X, we should be able to form the predicate $p(x) =$"x is in A" on X, and that the subset determined by p is precisely A. This corresponds to a "converse" of the construction (4). Namely, we see that for *every* monomorphism $i_A : A \to X$, there should be a unique $p : X \to \Omega$ making (4) a pullback square. An object Ω having an element $\mathbf{1_C} \xrightarrow{\top} \Omega$ satisfying this condition is called a *subobject classifier*.

Axiom 5. **C** *has a subobject classifier* $\mathbf{1_C} \xrightarrow{\top} \Omega$.

We now return to the question of Ω being a Boolean algebra object. Rather remarkably, this "almost" already follows from the axioms already introduced, though this is by no means trivial, and we will not prove it here. The main observation is that there is a natural ordering on the subobjects of a given object X which therefore induces a partial order on the predicates $X \to \Omega$ classifying these subobjects, and these orders are automatically preserved by the functions f^*. It is then a matter of showing that these partial orders on each $\mathbf{C}(X, \Omega)$ are in fact "almost" Boolean algebras.

The reason for "almost" is that it does not follow that these partial orders are Boolean algebra, but rather only *Heyting algebras*; these is a partial orders with all the structure of a Boolean algebra, as described in Section 2, but without the condition that $\neg(\neg P) = P$. Similarly, Ω is not a Boolean algebra object, but only a Heyting algebra object.

Hence, we must explicitly demand that these Heyting algebras are in fact Boolean algebras. In order to be able to state this, we must define the negation morphism $\neg : \Omega \to \Omega$. We will do this in a rough-and-ready (and incomprehensible) fashion.[8]

First, we have the monomorphism $\Omega \xrightarrow{\langle \mathrm{id}_\Omega, \mathrm{id}_\Omega \rangle} \Omega \times \Omega$, which is classified by a predicate $\Omega \times \Omega \to \Omega$, which we denote by eq_Ω. We then have the corresponding morphism $\lambda_\Omega eq_\Omega : \Omega \to \Omega^\Omega$. We also have the morphism $\top_{\Omega\times\Omega} : \Omega \times \Omega \to \Omega$ as well as $\lambda_\Omega \top_{\Omega\times\Omega} : \Omega \to \Omega^\Omega$. Finally, we have the monomorphism $\Omega^\Omega \xrightarrow{\left\langle \mathrm{id}_{\Omega^\Omega}, \mathrm{id}_{\Omega^\Omega} \right\rangle} \Omega^\Omega \times \Omega^\Omega$ which is classified by a predicate $eq_{\Omega^\Omega} : \Omega^\Omega \times \Omega^\Omega \to \Omega$. We now define $\neg : \Omega \to \Omega$ as the composite

$$\Omega \xrightarrow{\langle \lambda_\Omega eq_\Omega, \lambda_\Omega \top_{\Omega\times\Omega} \rangle} \Omega^\Omega \times \Omega^\Omega \xrightarrow{eq_{\Omega^\Omega}} \Omega$$

Axiom 6. $\neg : \Omega \to \Omega$ *is an involution:* $\neg \circ \neg = \mathrm{id}_\Omega$.

A category satisfying the Axioms 1-6 is called a *Boolean topos.* If Axiom 6 is omitted, then it is just called a *topos* (or sometimes "elementary topos" to distinguish it from the related (and earlier) notion of "Grothendieck topos"). There are also interesting example of topoi which are not Boolean; we will say a little more about this below.

5.4. **Freebies.** There are several more axioms we might naturally want to impose, but surprisingly, they all follow from the axioms we have so far (even omitting the Boolean Axiom 6).

First, while we have the structure of a Boolean (or Heyting) algebra on the (ambient) set of predicates $X \to \Omega$, we also need a "starting point" – a basic predicate from which to build more complicated ones – namely equality. It is is clear that the subset defined by the predicate $eq_X : X \times X \to \Omega$ should be $X \xrightarrow{\langle \mathrm{id}_X, \mathrm{id}_X \rangle} X \times X$ (i.e., the set of all pairs (x, x)), and so we can take this as the definition of eq_X. It can then be seen that it has all the desired properties: for example, two morphisms $f, g : Y \to X$ are equal if and only if the composite

$$Y \xrightarrow{\langle f,g \rangle} X \times X \xrightarrow{eq_X} \Omega$$

is equal to $\top_Y$.

We would also like to be able to define the *power set* of any set X, but this can simply be defined as Ω^X.

Next, we have not yet said anything about the all-important *quantifiers.* Demanding the existence of universal and existential quantification amounts to requiring that the order-preserving functions $p^* : \mathbf{C}(X, \Omega) \to \mathbf{C}(X \times Y, \Omega)$ induced from product projections p :

[8]The definition corresponds to the "second-order" definition of negation: $\neg P := \forall Q \in \Omega, (P \Leftrightarrow Q)$.

$X \times Y \to X$ always have right and left adjoints. It can be shown that this follows from our axioms.

Finally, we have already demanded that $\mathbf{C}$ have finite *limits* (that is, a terminal object and pullbacks). It is also natural to ask that it have finite *colimits*. This means (i) $\mathbf{C}$ has an initial object; this is the "empty set", (ii) $\mathbf{C}$ has coproducts; this is the "disjoint union", and (iii), $\mathbf{C}$ has coequalizers; for morphisms $f, g : X \to Y$, the co-equalizer represents the quotient of Y by the equivalence relation generated by the image of $\langle f, g\rangle : X \to Y \times Y$. Again, it can be shown that the existence of all of these follow from our axioms.

5.5. **Math.** In order to get started with defining interesting mathematical objects in a topos, we need a starting point: the natural numbers. There is a simple categorical notion of a natural numbers object, which we will not give here, since we will not need it. Once we have the natural numbers – since we also have products, power sets, and quotients by equivalence relations – we can go on to define the integers, the rationals and the reals in the usual fashion, and then begin to make the basic definitions and formulate and prove the basic theorems from analysis, and so on.

It should be noted that there is a significant difference as to how much of the classical mathematical facts we can prove depending on whether we assume Axiom 6.

6. Logical categories

We would now like to return to the considerations of Section 3.2, in which we defined the Boolean algebras $\bar{B}_n$, and we promised that we would be able to use categories to somehow fit these into a nice structure.

For any object X of our category $\mathbf{C}$, consider the sequence of objects $X^0 \cong \mathbf{1_C}$, $X^1 \cong X$, X^2, X^3, etc., and the associated sequence of Boolean algebras $\mathbf{C}(\mathbf{1_C}, \Omega)$, $\mathbf{C}(X, \Omega)$, $C(X^2, \Omega)$, etc. These Boolean algebras are connected to each other by the substitution homomorphisms f^* coming from the morphisms $f : X^m \to X^n$, as well as the universal and existential quantification maps $\mathbf{C}(X^n, \Omega) \to \mathbf{C}(X^{n-1}, \Omega)$.

Because Ω is a subobject classifier, we can take each Boolean algebra $\mathbf{C}(X^n, \Omega)$ (or rather, an equivalent Boolean prealgebra) to be a certain subcategory of $\mathbf{C}$ – namely, the subcategory whose objects are the domains of monomorphisms $i_A : A \to X^n$, and whose morphisms are all monomorphisms between these.

Let us collect all of these together by taking the full subcategory of $\mathbf{C}$ on all the X^n and all the domains of monomorphisms $i_A : A \to X^n$. This category has many (but not all) of the nice properties of a Boolean topos. In particular:

(1) It has finite limits
(2) The set $\mathrm{Sub}(X)$ of subobjects of each object X form a Boolean algebra
(3) For each $f : X \to Y$, the induced morphism $f^* : \mathrm{Sub}(Y) \to \mathrm{Sub}(X)$ (which takes each subobject of Y to its pullback along f) is a Boolean algebra homomorphism
(4) Each such f^* has left and right adjoints $\exists_f$ and $\forall_f$
(5) It fulfills a certain technical compatibility condition between the quantifiers $\exists_f, \forall_f$ and the pullback homomorphisms g^* called the "Beck-Chevalley condition", which we will not spell out

A category satisfying these conditions is called a *Boolean category.*

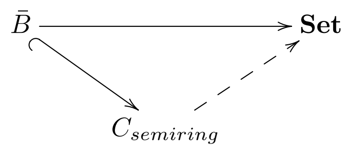
Now, suppose our category $\mathbf{C}$ is **Set**, the category of (ambient) Sets. This is indeed a Boolean topos, in which the subobject classifier is just the two-element set[9], and let the set

[9]Under our designation of Ω as the set of (logical equivalence classes of) propositions, this corresponds to the strange-seeming assumption that there are only two propositions up to equivalence. This corresponds to the simplifying and very traditional assumption that the equivalence of two propositions simply amounts to their both being either true or false.

X be the underlying set of a semi-ring R. Then the Boolean algebras $\mathbf{C}(X^n, \Omega)$ is just the power set $\mathcal{P}(R^n)$ of R^n, familiar from Section 3.2.

Hence, if we collect all the Boolean algebras $\bar{B}_n$ from Section 3.2 into a category $\bar{B}$ (by simply taking their disjoint union), we find that the various morphisms $\bar{B}_n \to \mathcal{P}(R^n)$ defined there get collected into a functor $\bar{B} \to \mathbf{Set}$. We now wish to "thicken" $\bar{B}$ into a logical category. One can prove

Theorem. *There exists a Boolean category $C_{semiring}$ and an embedding $\bar{B} \hookrightarrow C_{semiring}$ such that each functor $\bar{B} \to \mathbf{Set}$ arising from the choice of a semi-ring R as above factors through a logical functor (i.e., one preserving all the structure of a logical category) $C_{semiring} \to \mathbf{Set}$:*



Moreover, every logical functor $C_{semiring} \to \mathbf{Set}$ arises in this way.

As we did with the $\bar{B}_n$, we can think of the objects of $C_{semiring}$ to be the "first-order definable" subsets of (cartesian powers of) a generic semi-ring R, and each logical functor $C_{semiring} \to \mathbf{Set}$ as realizing these as subsets of (cartesian powers of) an actual semi-ring.

It is easy to see that if two semi-rings are isomorphic, then the corresponding functors $C_{semiring} \to \mathbf{Set}$ will be natural isomorphic, and *vice versa*. Hence the above theorem sets up an equivalence between the category of logical functors $C_{semiring} \to \mathbf{Set}$ and the category of semi-rings.

Of course, there is nothing special about semi-rings. The same discussion could be repeated with a wide variety of other algebraic structures.

7. Final remarks

As we said, there are interesting examples of non-Boolean topoi. In particular, the very first examples of topoi (besides Set) – namely, categories of sheaves on topological spaces – which arose in algebraic geometry from considerations far removed from those discussed here, are very rarely Boolean.

But the non-Boolean topoi are of logical interest too. In fact, the "Heyting" from "Heyting algebra" was a student of L.E.J. Brouwer, the father of *intuitionism*, a radical mathematician who rejected traditional mathematical reasoning and tried to reestablish mathematics on the basis of his new, constructive approach. The concept of Heyting algebra was Heyting's attempt to extract the logical essence of (a part of) Brouwer's ideas and formalize them in an algebraic structure.

The concept of intuitionism has received varied interest from mathematicians since then; it is central in the sub-field of mathematical logic known as *proof theory*, and in the related area of theoretical computer science called *type theory*. In particular, it plays a central role in *homotopy type theory*, a quite recent development revealing connections between homotopy theory and logic.

Certainly, one event which stimulated or revived interest in intuitionistic logic was the discovery of topoi as a natural setting for it; in particular, topoi give us a clear picture of what *intuitionistic set theory* is, which is otherwise somewhat hard to grasp.

As far as their capacity to formalize mathematics is concerned, topoi have certain limitations compared to the traditional formalization of set theory; there are things which can be expressed in the traditional set theory which have no analogues in a topos. This deficiency indicates that we should try to go *beyond* topoi and find some new, even better, structures.

Topoi represent the *beginning* of a project of “categorical foundations”, but hopefully not the end!