Dear Bill and Peter,

I asked the question about free toposes in connection with an old dream of mine which now seems to be getting more solid. The ultimate goal is to find a way to formulate mathematics which would be suitable for creating a formal "database" of math knowledge (on a computer). This should eventually require all the proofs there to be computer verified but as a first step it looks more important to find a good way to catalogue the definitions and the statements which we (mathematicians) claim to be proved.

Anyway, the approaches currently in use (type theory etc.) always looked to me very unfortunate from the intuitive point of view. In my mind, at least, the math world looks like a category. Its objects (called further m-objects) correspond to the classes of math objects i.e. there is an m-object called $[sets]$ and an m-object called $[rings]$ and an m-object called $[sheavesofringsonatopologicalspace]$. Its morphisms (called further m-morphisms) correspond to constructions. For example there is an m-morphism $[groups] \to [groups]$ which takes a group to its group of automorphisms. Subobjects correspond to properties of math objects (e.g $[abeliangroups]$ is a subobject of $[groups]$). Mathematical theorems are statements asserting that two morphisms coincide or that one subobject lies in another.

"Concrete" mathematical objects are m-constants i.e. morphisms from the final m-object pt. E.g there is a morphism $pt \to [abelian\ groups]$ called "natural numbers" and a morphism $pt \to [categories]$ called "the category of (small) sets". In particular, morphisms $pt \to [sets]$ should correspond to the constructively definable sets. The whole category should be countable. A particular "model" of mathematics is a good functor from this category to the category of sets (sufficiently large sets will be required) but these models are not of much importance. There not enough models to use them directly to establish theorems but they may be used to establish that some theorems do not hold (i.e. are not provable).

For all this to be useful from the practical point of view there should be an effective way to describe our state of knowledge about this category. Eventually one expects to have a searchable and somehow structured database containing known m-objects, m-morphisms , identities between morphisms etc.

There are probably many categories which can be used for this purpose just as there are many programming languages. Here is a possible candidate. Let me denote it by $\mathcal{M}$. It is an elementary booleans topos freely generated by a "seed". To describe the seed and for the further use let me denote the power object of an object X in a topos by $\bar{S}X$. One of the reasons I am not using the standard notation PX is that I want to treat $X \mapsto \bar{X}$ as a covariant functor.

The seed looks as follows. It is given by two objects E and S and two monomorphisms $\nu : S \to E$ and $\iota : S \to \bar{S}E$. The second one will be considered as the defining i.e. we'll think of S as a subobject in $\bar{S}E$. The triple (S, ν, ι) should satisfy some conditions which I will discuss in a moment.

The meaning of the components of the seed are as follows. The unusual one is E. It is to be understood as the class of everything in the world which can be an element. Intuitively it includes apples, trees, real numbers etc. By definition $\bar{S}E$ corresponds to subobjects of E. They correspond to (possibly large) sets. The subobject S in $\bar{S}E$ corresponds to small sets. The map ν is the "naming map" it takes a small set to its name which is considered as an element.

The elementary conditions on the seed are as follows:

1. all singletons are small sets
2. union of two small sets is a small set
3. any subset of a small set is small
4. for any small set the set of names of its subsets is small

When only these conditions are required there is a "finite" model for our category which sends E to any infinite set and S to the set of finite subsets of E. We will now introduce "axiom of infinity". Consider the m-morphism $\phi : S \to S$ which takes a small set A to the small set $A \cup \nu(A)$. Define ZF-natural numbers $Z\mathbf{N} \subset S$ as the intersection of all subobjects of S which contain $\emptyset$ and are closed under operation ϕ. Then $\nu(Z\mathbf{N})$ is a subobject in E. We require that $\nu(Z\mathbf{N}) \in S$ i.e. $\nu(Z\mathbf{N})$ is a small set. This is the axiom of infinity. The small set $\mathbf{N} = \nu(Z\mathbf{N})$ is called the set of natural numbers. I have not quite checked it yet but it seems likely that one can prove that $\mathbf{N}$ is a natural numbers object in our topos.

As far as I understand the infinity axiom implies that any model of our category (or equivalently of the seed) will have to send E to a large cardinal.

There is another way to introduce the natural numbers which does not require the naming map. Denote $\bar{S}E$ by $[sets]$. It is not hard then to define the m-object $[maps]$ and morphisms $s, t : [maps] \to [sets]$, $Id : [sets] \to [maps]$, $\circ : [maps] \times_{[sets]} [maps] \to [maps]$ which form an internal category in $\mathcal{M}$ and such that $[maps]$ corresponds in models to maps between sets. After that one can define the isomorphism equivalence relation $Iso \subset [sets] \times [sets]$ on $[sets]$. Then one can define finite sets as the ones not isomorphic to a proper subset. Then one can define a subobject $C\mathbf{N}$ of $\bar{S}\bar{S}[sets] = \bar{S}\bar{S}\bar{S}E$ whose elements are isomorphism classes of finite sets. Provided the naming map satisfying the appropriate properties is given one should be able to show that $C\mathbf{N} \cong Z\mathbf{N}$ and in particular can be embedded into $\bar{S}E$. The infinity axiom would them imply that it can be further embedded into E.

While the seed (E, S, ν, ι) is probably sufficient in order to formulate most of mathematics it seems that in reality we use a more complex seed in our thinking. One of the attractive points of the point of view outlined above is that it is easy to modify the seed without introducing dramatic changes to the general approach. One particular modification which appears both quite harmless and very useful is as follows. Let us add to our see a morphism $c : E \times E \to E$ about which we will assume two things

1. c is associative
2. c is a monomorphism.

Intuitively, the idea is that if we have two elements a, b then we can form their "ordered pair" ab in a strictly associative way. I do not know if one may construct c with these properties from ν and ι. In any event such a morphism corresponds quite well to our intuitive way of thinking about finite sequences of elements. Once we added c to the seed we can, for example, define strictly associative finite products of sets (which should also imply strictly associative finite coproducts) which makes life dramatically easier.

There may be other useful enlargements of the seed. As long as we keep the seed consisting of structures which are intuitively accepted and follow strict rules of generating further structures from the seed we should be OK.