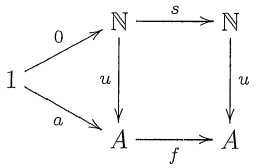
Arithmetic Universes and the Gödel Incompleteness Theorem

André Joyal

July 22, 2004

1 Natural Numbers Objects

Definition 1.1. Let $\mathcal{C}$ be a category with a terminal object. A natural numbers object (NNO) in $\mathcal{C}$ is an object $\mathbb{N}$ of $\mathcal{C}$, equipped with maps $1 \xrightarrow{0} \mathbb{N} \xrightarrow{s} \mathbb{N}$ called *zero* and *successor*, such that given any maps $1 \xrightarrow{a} A \xrightarrow{f} A$ in $\mathcal{C}$, there is a unique "sequence" $u : \mathbb{N} \to A$ such that

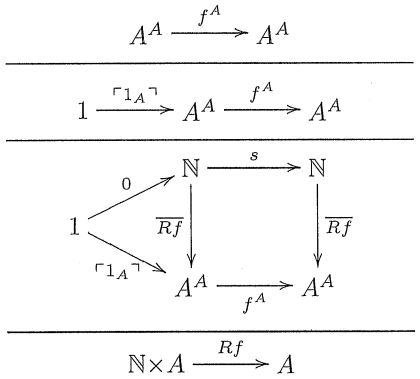


commutes. That is, $u(0) = a$ and $u(s(n)) = f(u(n))$.

If exponentiation is available in $\mathcal{C}$, then we can phrase this a little better: given a map $f : A \to A$ in $\mathcal{C}$, there exists a unique map $Rf : \mathbb{N} \times A \to A$ called the *recursion* of f, such that

$$Rf(n, a) = \underbrace{(f \circ \ldots \circ f)}_{n}(a).$$

We can rederive Rf from f as follows:



However, we can actually achieve this nicer formulation without exponentiation in $\mathcal{C}$. Instead start with a monoidal category $(\mathcal{C}, \otimes, I, \alpha, \lambda, \rho)$ where α, λ and ρ are the associativity, left unit and right unit coherence isomorphisms. We define what is meant by the free monoid $M(S)$ on an object $S \in \mathcal{C}$: the data required are an action of S on $M(S)$:

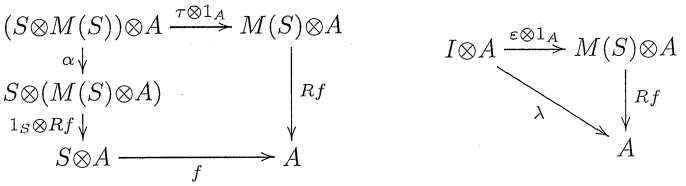
$$\tau : S \otimes M(S) \to M(S)$$

(thought of as specifying "how to add on a new symbol to a word") and a map:

$$\varepsilon : I \to M(S)$$

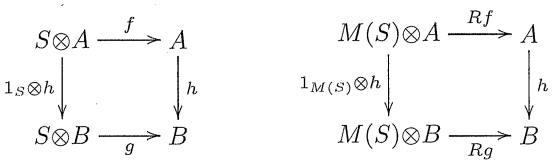
(which specifies the "empty word"); these data satisfy two axioms:

1. given $f : S \otimes A \to A$, then there is a unique "extension" $Rf : M(S) \otimes A \to A$ of f, called the recursion of f, such that the diagrams



   commute.

2. if given f, g and h such that the square on the left



   commutes, then the square on the right commutes also.

The monoid structure for $M(S)$ is:

$$I \xrightarrow{\varepsilon} M(S) \xleftarrow{R\tau} M(S)\otimes M(S)$$

and the embedding $\iota : S \to M(S)$ is achieved as the composite:

$$S \xrightarrow{\rho^{-1}} S\otimes I \xrightarrow{1_S\otimes\varepsilon} S\otimes M(S) \xrightarrow{\tau} M(S)\ ;$$

one can then prove the standard universality for ι (inside $\mathcal{C}$). One can give a second description of the free monoid $M(S)$, just in terms of the monoid structure as follows: $M(S)$ will have a multiplication $\mu : M(S)\otimes M(S) \to M(S)$ and a unit $\varepsilon : I \to M(S)$, together with an "embedding" $\iota : S \to M(S)$, such that the "restriction functor"

$$\iota^* : \mathcal{C}^{M(S)} \to \mathcal{C}^S$$

(from the category of actions of $M(S)$ on objects of $\mathcal{C}$ to the category of (discrete) actions of S on objects of $\mathcal{C}$) is an equivalence.

With these concepts of free monoid, one then sees that a NNO is nothing more than a free monoid on a terminal object – $M(1)$ – that is the data:

$$\begin{array}{rl} +\ :\ \mathbb{N}^2 \to \mathbb{N} & \text{(sum)} \\ 0\ :\ 1 \to \mathbb{N} & \text{(unit)} \\ 1\ :\ 1 \to \mathbb{N} & \text{(embedding)} \end{array}$$

such that given any $f : A \to A$ in $\mathcal{C}$, there is a unique extension $Rf : \mathbb{N}\times A \to A$, with the properties described above.

Note that $\mathbb{N}$ is essentially just strong enough to define functions by primitive recursion: one says that f is given by primitive recursion relative to g, when one has a definition of the form

$$\begin{array}{rcl} f(0) & = & a \\ f(s(n)) & = & g(n, f(n)); \end{array}$$

given $a : 1 \to A$ and $g : \mathbb{N}\times A \to A$, how do we construct $f : \mathbb{N} \to A$? First, form

$$(s\circ \mathrm{pr}_1, g) : \mathbb{N}\times A \to \mathbb{N}\times A;$$

next, take its recursion

$$R(s\circ \mathrm{pr}_1, g) : \mathbb{N}\times\mathbb{N}\times A \to \mathbb{N}\times A;$$

then

$$\begin{array}{ccc} \mathbb{N}\times\mathbb{N}\times A & \xrightarrow{R(s\circ \mathrm{pr}_1, g)} & \mathbb{N}\times A \\ {\scriptstyle (1_{\mathbb{N}},0,a)}\uparrow & & \downarrow{\scriptstyle \mathrm{pr}_2} \\ \mathbb{N} & \xrightarrow[f]{} & A \end{array}$$

Armed with definition by primitive recursion we now define some useful functions:

1. $\dot{-} : \mathbb{N}^2 \to \mathbb{N}$ is given by

$$n \dot{-} m = \begin{cases} n - m & \text{if } n \geq m \\ 0 & \text{if } n < m \end{cases}$$

Notice that we have the adjunction: $n \dot{-} m \leq p$ iff $n \leq m + p$. The definition of $\dot{-}$ by primitive recursion:

$$\begin{array}{rcl} n \dot{-} 1 & : & \left\{ \begin{array}{rcl} 0 \dot{-} 1 & = & 0 \\ s(n) \dot{-} 1 & = & n \end{array} \right\} \\ n \dot{-} m & : & \left\{ \begin{array}{rcl} n \dot{-} 0 & = & n \\ n \dot{-} s(m) & = & (n \dot{-} m) \dot{-} 1 \end{array} \right\} \end{array}$$

2. conjunction and disjunction:

$$\begin{array}{rcl} \vee : \mathbb{N}^2 \to \mathbb{N} & : & n \vee m \stackrel{\text{def}}{=} (n \dot{-} m) + m \\ \wedge : \mathbb{N}^2 \to \mathbb{N} & : & n \wedge m \stackrel{\text{def}}{=} (n + m) \dot{-} (n \vee m) \end{array}$$

3. $E : \mathbb{N}^2 \to \mathbb{N}$ is given by

$$E(n, m) \quad = \quad [\![n = m]\!] \quad = \quad \begin{cases} 1 & \text{if} \quad n = m \\ 0 & \text{if} \quad n \neq m \end{cases}$$

The definition of E by primitive recursion:

$$\begin{array}{rcl} E(n, 0) & : & \left\{ \begin{array}{rcl} E(0, 0) & = & 1 \\ E(s(n), 0) & = & 0 \end{array} \right\} \\ E(n, m) & = & E(n \dot{-} m, 0) \wedge E(m \dot{-} n, 0) \end{array}$$

2 Skolem Theories and Arithmetic Universes

Definition 2.1. A Skolem Theory $\mathcal{S}$ is an algebraic theory in the sense of Lawvere, in which the generating "basic symbol" is a NNO: so the objects of $\mathcal{S}$ consist of powers $1, \mathbb{N}, \mathbb{N}^2, \ldots$ of $\mathbb{N}$, which is the free monoid on 1 in $\mathcal{S}$, with its

$$\begin{array}{rl} + : \mathbb{N}^2 \to \mathbb{N} & \text{(sum)} \\ 0 : 1 \to \mathbb{N} & \text{(unit)} \\ 1 : 1 \to \mathbb{N} & \text{(embedding)} \end{array}$$

and such that given $f : \mathbb{N}^k \to \mathbb{N}^r$, there exists a unique $Rf : \mathbb{N} \times \mathbb{N}^k \to \mathbb{N}^r$, with the required property. One can define in an obvious manner, morphisms of Skolem Theories and a category of Skolem Theories. This category has an inital object $\mathcal{S}_o$ which might be called the minimal Skolem Theory, or the "free theory" (generated on the basic data).

Caveat 2.2. One cannot identify the arrows of $\mathcal{S}_o$ with actual functions; for, let $\mathcal{S}_{\text{standard}}$ be the full subcategory of **Set** with objects $1, \mathbb{N}, \mathbb{N}^2, ...$: then since $\mathcal{S}_o$ is initial we have a map of Skolem Theories:

$$\mathcal{S}_o \longrightarrow \mathcal{S}_{\text{standard}}$$

$$f : \mathbb{N}^k \to \mathbb{N}^r \longmapsto |f| : \mathbb{N}^k \to \mathbb{N}^r \ ;$$

the idea is that f exists as an algorithm for the actual function $|f|$, (actually a primitive recursive algorithm) and it can happen that $|f| = |g|$ but $f \neq g$ (ie no proof of $f = g$ exists which just appeals to primitive recursions).

Aside 2.3. It turns out that the Skolem Theory of all recursive functions is just the category of primitive recursive functions formed from the Skolem Theory of primitive recursive functions by inverting those arrows which are bijections.

A procedure will now be described which completes any Skolem Theory to a category with finite limits. So let $\mathcal{S}$ be a Skolem Theory. The idea is to adjoin "decidable subsets": define a subset of $\mathbb{N}^k$ to be a map $x : \mathbb{N}^k \to \mathbb{N}$ such that $x \wedge 1 = x$. Thus a subset is given by an "algorithm for deciding membership in it". Write $\mathcal{P}_{\text{dec}}(\mathbb{N}^k)$ for this class of subsets. Then $\mathcal{P}_{\text{dec}}$ is actually a contravariant functor in the usual way:

$$\mathbb{N}^k \xrightarrow{f} \mathbb{N}^r \qquad \text{induces} \qquad \mathcal{P}_{\text{dec}}(\mathbb{N}^r) \xrightarrow{f^{-1}} \mathcal{P}_{\text{dec}}(\mathbb{N}^k)$$

the diagonal $\Delta \in \mathcal{P}_{\text{dec}}(\mathbb{N})$ is given by $E : \mathbb{N}^2 \to \mathbb{N}$ defined above; similarly one defines a diagonal $\Delta_k \in \mathcal{P}_{\text{dec}}((\mathbb{N}^k)^2)$, for all k. $\mathcal{P}_{\text{dec}}(\mathbb{N}^k)$ actually carries a Boolean algebra structure: unions, intersections and complements of subsets correspond to the sup, inf, and 1 minus the corresponding characteristic functions.

Define a new category $\hat{\mathcal{S}}$ whose objects are just the subsets of powers of $\mathbb{N} \in \mathcal{S}$. The maps $f : S \to T$, where $S \in \mathcal{P}_{\text{dec}}(\mathbb{N}^k)$ and $T \in \mathcal{P}_{\text{dec}}(\mathbb{N}^r)$, may be identified with their "extensions by zero" (ie extend f to $\mathbb{N}^k$ by letting f be 0 outside S) back in $\mathcal{S}$.

Here are some properties of $\mathcal{S} \to \hat{\mathcal{S}}$:

1. $\hat{\mathcal{S}}$ has finite limits: for example the equaliser of $f, g : \mathbb{N}^k \rightrightarrows \mathbb{N}^r$ is just the subset $S \in \mathcal{P}_{\text{dec}}(\mathbb{N}^k)$ given by

$$\mathbb{N}^k \xrightarrow{(f,g)} \mathbb{N}^r \times \mathbb{N}^r \xrightarrow{E} \mathbb{N} \ .$$

2. $\hat{\mathcal{S}}$ is regular and satisfies the axiom of choice: actually every arrow factors as split epi followed by mono (warning: do not confuse monos with subsets

as defined above). For, suppose given $f : \mathbb{N} \to \mathbb{N}$: think of f as specifying the sequence of fibres:

$$f^{-1}(0), f^{-1}(1), f^{-1}(2), \ldots$$

The idea is to factor f as $\mathbb{N} \twoheadrightarrow I \rightarrowtail \mathbb{N}$ where, if

$$\tau(n) \stackrel{\text{def}}{=} \mu m\{\ m \leq n \quad \text{and} \quad f(m) = n\ \}$$

then $I = \{n : \tau(n) = n\}$ has an obvious decision algorithm, and the maps are:

$$\mathbb{N} \stackrel{\tau}{\twoheadrightarrow} I \stackrel{f}{\rightarrowtail} \mathbb{N}$$

3. coproducts exist in $\hat{\mathcal{S}}$: given decidable subsets S, T of $\mathbb{N}$, for example, take the union of the decidable subsets $S \times \{0\}$ and $T \times \{1\}$ of $\mathbb{N}^2$.

4. for any graph object

$$G \underset{\partial_1}{\overset{\partial_0}{\rightrightarrows}} A_0$$

in $\mathcal{S}$, there exists a free category object $A_1 \underset{\partial_1}{\overset{\partial_0}{\rightrightarrows}} A_0$ over G in $\hat{\mathcal{S}}$; this is the same thing as a free monoid object for the monoidal category of A_0-graph objects in $\mathcal{S}$.

It is necessary to make a second completion $\mathcal{S} \to \hat{\mathcal{S}} \to \tilde{\hat{\mathcal{S}}}$ which adds quotients. This is accomplished by forming a new category whose objects are pairs (R, A) with $R \rightrightarrows A$ an equivalence relation on A, and whose maps $(R, A) \to (R, B)$ are classes of maps $f : A \to B$ such that $R \leq (f \times f)^{-1}(Q)$, under the relation: $f \sim g$ iff there exists a lifting of (f, g):

$$\begin{array}{ccc} & & Q \\ & \nearrow & \downarrow \\ A & \xrightarrow[(f,g)]{} & B \times B \end{array}$$

The properties of $\tilde{\hat{\mathcal{S}}}$ are as follows:

1. finite limits exist.
2. regular category (but notice that the step $\hat{\mathcal{S}} \to \tilde{\hat{\mathcal{S}}}$ spoils the axiom of choice).
3. coproducts exist.
4. free category objects exist for any graph object.
5. quotients exist (but are not split in general).

These axioms (1)$\to$(5) are the defining properties for the notion of Arithmetic universe (AU). Applying the completion procedure to $\mathcal{S}_0$ yields the AU $\mathcal{U}_0$ which is the initial AU, and consists of the primitive recursive functions.

3 The Gödel Incompleteness Theorem

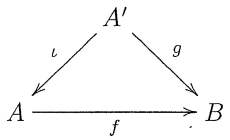
Definition 3.1. A theory $\mathcal{C}$ is consistent iff $0 \in \mathcal{P}1$ and $I \in \mathcal{P}1$ are distinct. A theory $\mathcal{C}$ is complete iff given $u \in \mathcal{P}1$, then $u = 0$ or $u = 1$.

Consider **Set** as an AU; since $\mathcal{U}_0$ is initial we have a functor

$$\mathcal{U}_o \longrightarrow \mathbf{Set}$$

$$g : A \to B \longmapsto |g| : |A| \to |B| \ ;$$

which assigns to an "algorithm" g the primitive recursive function $|g|$ that it specifies. Let Σ be the class of arrows of $\mathcal{U}_0$ such that $|f|$ is a bijection: then Σ carries a calculus of left fractions and $\Sigma^{-1}\mathcal{U}_0 = \mathcal{U}_{\text{rec}}$ is the arithmetic universe of recursive functions. The main point is that any recursive function $f : A \to B$ can be "spanned" as a bijective primitive recursive $\iota : A' \to A$ and a primitive recursive $g : A' \to B$:



Gödel's Incompleteness Theorem can now be stated:

Theorem 3.2. *Any arithmetic universe object (AUO) in $\mathcal{U}_{\text{rec}}$ is necessarily incomplete.*

Discussion 3.3. Let $\mathcal{U}_0'$ be the initial AUO in $\mathcal{U}_0$. Here are some notations that will be used:

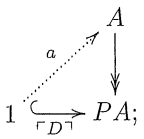
1. $1 \xrightarrow{A'} \mathcal{U}_0'$ is an object of $\mathcal{U}_0'$.
2. given $1 \underset{B'}{\overset{A'}{\rightrightarrows}} \mathcal{U}_0'$ there is an object of morphisms $\mathcal{U}_0'(A', B')$ written simply as $[A', B']$: this is an object of $\mathcal{U}_0$.
3. $\mathcal{P}'A'$ can be formed as another object of $\mathcal{U}_0$.
4. there is an internal pullback map $[B', A'] \times \mathcal{P}'A' \longrightarrow \mathcal{P}'A'$.

At this point a translation of Cantor's Diagonal argument into categorical terms is given for motivation and later comparison.

Suppose $\mathcal{E}$ is a topos in which 1 is projective; then if there exists an enumeration $f : A \twoheadrightarrow PA$, $\mathcal{E}$ is degenerate; for, suppose f exists: form the pullback

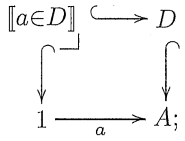
$$\begin{array}{ccccccc} D & \longrightarrow & & & & & 1 \\ \downarrow & \lrcorner & & & & & \downarrow \text{false} \\ A & \xrightarrow[\Delta_A]{} & A \times A & \xrightarrow[1_A \times f]{} & A \times PA & \xrightarrow[\text{eval}]{} & P1, \end{array}$$

and consider $\ulcorner D \urcorner : 1 \mapsto PA$; there is a lifting a of $\ulcorner D \urcorner$:

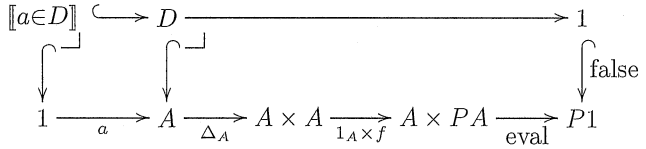


because 1 is projective

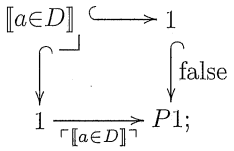
then $[\![a \in D]\!]$ is defined by the pullback



the composite pullback



is then just



$[\![a \in D]\!] = \{ * \mid "* \in [\![a \in D]\!]" = \text{false} \}$

it follows that

$$[\![a \in D]\!] \hookrightarrow 1 \underset{\ulcorner 1 \urcorner}{\overset{\ulcorner 0 \urcorner}{\rightrightarrows}} P1$$

is an equalizer; it then follows that $([\![a \in D]\!] \hookrightarrow 1) \approx (0 \hookrightarrow 1)$: but then $[\![a \in D]\!]$ is also the pullback of false along false, so $([\![a \in D]\!] \hookrightarrow 1) \approx (1 \hookrightarrow 1)$ also: but then $0 = 1$.

Discussion 3.4. Here are two facts about $\tilde{\hat{\mathcal{S}}}$ which will be needed:

1. any object of $\tilde{\hat{\mathcal{S}}}$ with global support can be enumerated by $\mathbb{N}$.

2. if $1 \xrightarrow{\mathbb{N}'} \mathcal{U}'_0$ is the formal natural numbers object, then there is an enumeration
$$e : \mathbb{N} \twoheadrightarrow \mathcal{P}'\mathbb{N}'$$
of "all formulae with one variable free."

An appeal to the glueing construction of Freyd is also needed; take a topos $\mathcal{E}$ and the global sections functor $\Gamma : \mathcal{E} \to \mathbf{Set}$: form a new category $C(\mathcal{E})$ whose objects are maps $\alpha : S \to \Gamma(A)$ and whose morphisms are the obvious commutative diagrams. The construction yields a new topos. Actually one can start with an AU $\mathcal{U}$, and one gets another AU: apply this construction internally to glue $\mathcal{U}_0'$ to $\mathcal{U}_0$, and call the result $\mathcal{U}_1$. Since $\mathcal{U}_0$ is initial there is a functor

$$\mathcal{U}_0 \longrightarrow \mathcal{U}_1 \ ;$$

and it turns out that this functor sends

$$A \longmapsto (\alpha : A \to [1', A']) \ ;$$

in particular,

$$\mathbb{N} \longmapsto (\iota : \mathbb{N} \to [1', \mathbb{N}']) \ ;$$

where ι is the map which assigns each natural number its "formal expression".

Cantor's Diagonal argument will now be imitated to prove Incompleteness in a special case. Form the pullback:

$$\begin{array}{ccccccc} D & \longrightarrow & & & & & 1 \\ \downarrow & \lrcorner & & & & & \downarrow \text{false} \\ \mathbb{N} & \xrightarrow[\Delta_{\mathbb{N}}]{} & \mathbb{N} \times \mathbb{N} & \xrightarrow[\iota \times e]{} & [1', \mathbb{N}'] \times \mathcal{P}'\mathbb{N}' & \xrightarrow[\text{eval}]{} & \mathcal{P}'1' \end{array}$$

then since 1 is projective in any AU: form the lift n of D':

$$\begin{array}{ccc} & & \mathbb{N} \\ & \overset{n}{\nearrow} & \downarrow e \\ 1 & \xrightarrow[D']{} & \mathcal{P}'\mathbb{N}' \end{array} \ ;$$

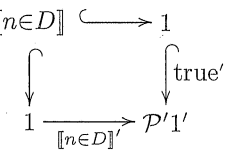
then

$$\begin{array}{ccccccccc} [\![n \in D]\!] & \hookrightarrow & D & & & & & & 1 \\ \downarrow & \lrcorner & \downarrow & \lrcorner & & & & & \downarrow \text{false} \\ 1 & \xrightarrow[n]{} & \mathbb{N} & \xrightarrow[\Delta_{\mathbb{N}}]{} & \mathbb{N} \times \mathbb{N} & \xrightarrow[\iota \times e]{} & [1', \mathbb{N}'] \times \mathcal{P}'\mathbb{N}' & \xrightarrow[\text{eval}]{} & \mathcal{P}'1' \end{array}$$

is given by pullback; consider $[\![n \in D]\!]' : 1 \hookrightarrow \mathcal{P}'1'$: it follows that this is a pullback square by composition:

$$\begin{array}{ccc} [\![n \in D]\!] & \hookrightarrow & 1 \\ \downarrow & \lrcorner & \downarrow \text{false}' \\ 1 & \xrightarrow[[\![n \in D]\!]']{} & \mathcal{P}'1' ; \end{array}$$

on the other hand



is commutative.

Conclusion 3.5. $[\![n{\in}D]\!] \hookrightarrow 1 \underset{\text{true}'}{\overset{\text{false}'}{\rightrightarrows}} \mathcal{P}'1'$ is an equalizer. Now if $[\![n{\in}D]\!]$ were 0, then $[\![n{\in}D]\!]$ is the pullback of false′ along false′, hence $[\![n{\in}D]\!]$ is 1, contradicting the consistency of $\mathcal{U}_0$. It follows that $[\![n{\in}D]\!]$ is not 0, and the consistency of $\mathcal{U}_0'$ is not provable.

g.curi@cs.bham.ac.uk

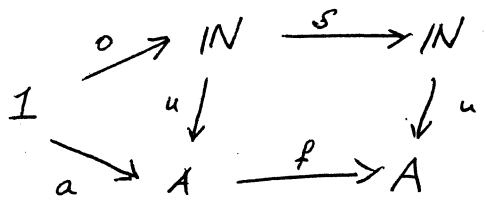
CATEGORIES & LOGIC

André Joyal

26 November 1979

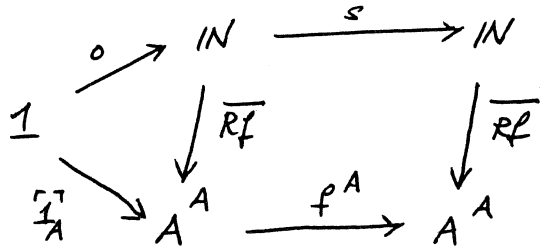
§4 The Gödel Incompleteness Theorem

Definition A natural number object (NNO) $\mathbb{N}$ in a category $\mathcal{C}$ is an object equipped with maps $1 \xrightarrow{0} \mathbb{N} \xrightarrow{s} \mathbb{N}$ called "zero" and "successor" ($\mathcal{C}$ must have a terminal object 1) such that given maps $1 \xrightarrow{a} A \xrightarrow{f} A$ in $\mathcal{C}$, there is an unique "sequence" $\mathbb{N} \xrightarrow{u} A$ such that



commutes, i.e $u(0) = a$, $u(s(n)) = f(u(n))$.

NB If exponentiation is available in $\mathcal{C}$, then we can phrase this a little better: given a map $A \xrightarrow{f} A$ in $\mathcal{C}$ there exists a unique map $Rf : \mathbb{N} \times A \longrightarrow A$, called the recursion of f such that $Rf(n,a) = f^n(a)$, where $f^0 = 1_A$, $f^{s(n)} = f \cdot f^n$. We can derive Rf as follows:



However, we can actually achieve this nicer formulation without exponentiation in $\mathcal{C}$. Instead, start with a monoidal category $(\mathcal{C}, \otimes, I, \alpha, \lambda, \rho)$ — α is the associativity, λ and ρ the left and right unit identifications.

We define what is meant by the free monoid $M(S)$ on an object $S \in C$: the data required are an action

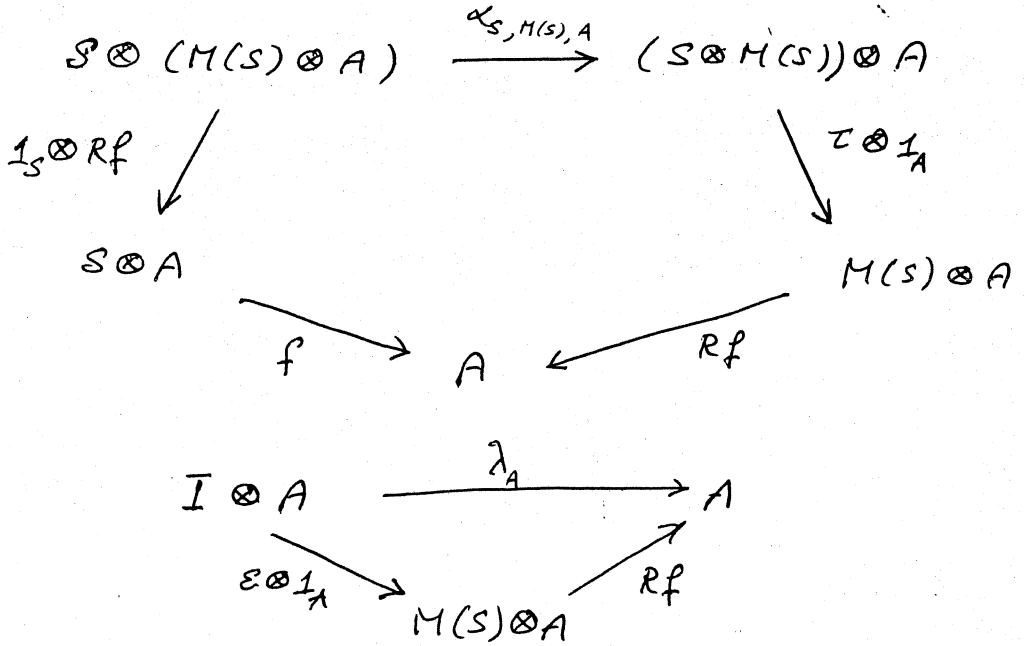
$$\tau : S \otimes M(S) \longrightarrow M(S)$$

(think of this as specifying "how to add on a new symbol to a word") and a map

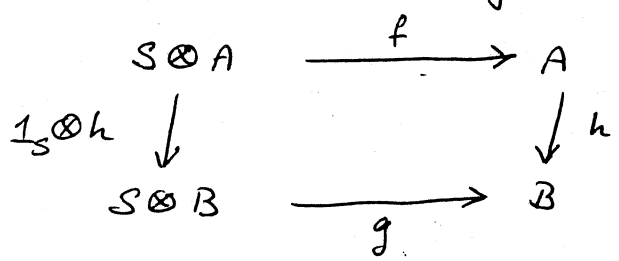
$$\varepsilon : I \longrightarrow M(S)$$

(which specifies the "empty word") satisfying the two axioms :

1) given $S \otimes A \xrightarrow{f} A$ there is an unique "extension" $Rf : M(S) \otimes A \longrightarrow A$ of f, called the recursion of f, such that the following two diagrams commute :



2) given a commutative diagram



the following diagram commutes:

$$\begin{array}{ccc} M(S)\otimes A & \xrightarrow{Rf} & A \\ {\scriptstyle 1_{M(S)}\otimes h}\downarrow & & \downarrow{\scriptstyle h} \\ M(S)\otimes B & \xrightarrow{Rg} & B \end{array}$$

The monoid in question is of course the following multiplication and unity on $M(S)$:

$$M(S)\otimes M(S) \xrightarrow{R\Gamma} M(S)$$

$$I \xrightarrow{\varepsilon} M(S)$$

The "embedding" $S \xrightarrow{\lambda} M(S)$ is achieved as

$$S \xrightarrow{\rho_S^{-1}} S\otimes I \xrightarrow{1_S\otimes\varepsilon} S\otimes M(S) \xrightarrow{\Gamma} M(S)$$

One may then prove the standard universality property for λ inside $\mathcal{C}$.

One can give a second description of the free monoid $M(S)$, just in terms of its monoid structure, as follows:

$M(S)$ will have a multiplication $\mu: M(S)\otimes M(S) \longrightarrow M(S)$ and unity $\varepsilon: I \longrightarrow M(S)$, together with an "embedding" $\lambda: S \longrightarrow M(S)$ such that the restriction functor λ^*, from the category of actions of $M(S)$ on objects of $\mathcal{C}$ to the category of (discrete) actions of S on objects of $\mathcal{C}$, is an equivalence.

With these concepts of free monoid, one then sees that a NNO is nothing more than a free monoid on a Terminal object, i.e $\mathbb{N} = M(1)$:

i.e the data: $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ (sum)

$0 : 1 \longrightarrow \mathbb{N}$ (unit)

$1 : 1 \longrightarrow \mathbb{N}$ (embedding)

such that, given any $f : A \to A$ in $\mathcal{C}$, there is an unique extension $Rf : \mathbb{N} \times A \longrightarrow A$ with the correct properties as above ($\otimes$ is cartesian product in this case).

[André later preferred to discuss the slightly more general notion, not of free monoid on an object, but of free category generated by a graph, and in particular the "action variant", whereby each action of a graph on an object indexed by the object of vertices lifts to a presheaf on the category of paths on the graph]

NB $\mathbb{N}$ is essentially just strong enough to define maps by primitive recursion: one says f is given by primitive recursion relative to g and a, when one has a definition of the form

$$f(0) = a \quad , \quad f(s(n)) = g(n, f(n))$$

given $1 \xrightarrow{a} A$, $\mathbb{N} \times A \xrightarrow{g} A$. To construct f, form

$$\mathbb{N} \times A \xrightarrow{(s \circ pr_1 , g)} \mathbb{N} \times A$$

take its recursion $R(s \circ pr_1, g) : \mathbb{N} \times \mathbb{N} \times A \longrightarrow \mathbb{N} \times A$ and define $\mathbb{N} \xrightarrow{f} A$ to be

$$\mathbb{N} \xrightarrow{(1_{\mathbb{N}}, 0, a)} \mathbb{N} \times \mathbb{N} \times A \xrightarrow{R(s \circ pr_1, g)} \mathbb{N} \times A \xrightarrow{pr_2} A$$

Armed with definition by primitive recursion we now define some useful functions:

a) $\dot{-} : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ "Truncated subtraction"

$n \dot{-} m$ = if $n \geq m$ then $n - m$ else 0

adjunction: $n \dot{-} m \leq p$ iff $n \leq p + m$

Defined by $n \dot{-} \underline{1}$: $0 \dot{-} 1 = 0$

$s(n) \dot{-} 1 = n$

and $n \dot{-} m$: $n \dot{-} 0 = n$

$n \dot{-} s(m) = (n \dot{-} m) \dot{-} 1$

b) $\vee, \wedge : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$

$n \vee m = (n \dot{-} m) + m$

$n \wedge m = (n + m) \dot{-} (n \vee m)$

c) $E : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$

$E(n,m) = E(n \dot{-} m, 0) \wedge E(m \dot{-} n, 0)$

where $E(n,0)$ is defined by

$E(0,0) = 1$

$E(s(n),0) = 0$

So $E(n,m) = \begin{cases} 1 & \text{if } n = m \\ 0 & \text{if } n \neq m \end{cases}$

We also write $[\![n = m]\!]$ for $E(n,m)$.

Definition A Skolem theory is an algebraic theory in the sense of Lawvere, in which the generating "basic symbol" is a NNO; so the objects of a Skolem theory $\mathbb{S}$ consist of the finite powers $1, \mathbb{N}, \mathbb{N}^2, \ldots$ of $\mathbb{N}$, which is the free monoid on 1 in $\mathbb{S}$, with its

$+ : \mathbb{N}^2 \longrightarrow \mathbb{N}$ (sum)

$0 : 1 \longrightarrow \mathbb{N}$ (unity)

$\underline{1} : 1 \longrightarrow \mathbb{N}$ (embedding)

and such that given $\mathbb{N}^k \xrightarrow{f} \mathbb{N}^\ell$ there exists an unique

$\mathbb{N} \times \mathbb{N}^k \xrightarrow{Rf} \mathbb{N}^\wedge$ with the required property.

One can define in an obvious manner, morphisms of Skolem theories and a category of Skolem theories. This category has an initial object $\mathcal{S}_0$ which might be called the minimal Skolem theory, generated by nothing but the basic data.

[One might equally well define the notion of a Skolem category - a category with finite products and a NNO. An initial Skolem category will automatically be an initial Skolem theory]

[The existence of primitive recursive pairing and de-pairing functions shows that in any Skolem category $\mathbb{N}^k$ is isomorphic to $\mathbb{N}$ for $k>0$.]

Caveat One cannot identify the arrows of $\mathcal{S}_0$ with actual primitive recursive functions. Let $\mathcal{S}_{standard}$ be the full subcategory of Sets with objects $1, \mathbb{N}, \mathbb{N}^2, \ldots$ and maps the primitive recursive functions. Since $\mathcal{S}_0$ is initial, we have a map of Skolem theories

$$\mathcal{S}_0 \longrightarrow \mathcal{S}_{standard}$$

$$(\mathbb{N}^k \xrightarrow{f} \mathbb{N}^\wedge) \longmapsto (\mathbb{N}^k \xrightarrow{|f|} \mathbb{N}^\wedge)$$

We use $\mathbb{N}$ to denote the NNO in Sets. The idea is that f exists as a primitive recursive algorithm for the function $|f|$, but it can happen that $|f| = |g|$ without having $f = g$; there may be no proof that the two algorithms "are the same" which just appeals to primitive recursions.

[We could introduce the following rudimentary programming language (call it PRIM ?):
the language has "variables" or "registers" $x, y, \ldots$
and statements

CLR x (i.e set x to zero)

INC x (i.e increment x)

REPEAT x { ..... }

where the block contains no references to x.
With some extra effort, it should be clear that maps in $\mathcal{S}_0$ can be described as equivalence classes of appropriately labelled PRIM programs. Describing the equivalence relation is more subtle.]

Aside Let Σ be the class of maps in $\mathcal{S}_0$ which are inverted by the unique map of Skolem theories $\mathcal{S}_0 \longrightarrow \mathcal{S}_{standard}$. Then the category of fractions $\mathcal{S}_0[\Sigma^{-1}]$ is the Skolem Theory of all recursive functions.

A procedure will now be described which completes any Skolem Theory to a category with finite limits. So let $\mathcal{S}$ be a Skolem Theory. The idea is to adjoin "decidable subsets": define a subset of $\mathbb{N}^k$ to be a map $u : \mathbb{N}^k \longrightarrow \mathbb{N}$ such that $u(\underline{n}) \wedge 1 = u(\underline{n})$ (or equivalently, such that $u(\underline{n})^2 = u(\underline{n})$), so that u only takes the values 0 or 1. Thus a subset is given by an algorithm for deciding membership in it. Write $P_{dec}(\mathbb{N}^k)$ for the set of maps $\mathbb{N}^k \longrightarrow \mathbb{N}$ in $\mathcal{S}$ with the above property. This defines a contravariant functor Pdec in the usual way, by composition. We write f^{-1} for $P_{dec}(f)$. For example, the map $E : \mathbb{N}^2 \longrightarrow \mathbb{N}$ defines the "subset" $\Delta \in P_{dec}(\mathbb{N}^2)$, the "diagonal". Similarly, we can define $\Delta_k \in P_{dec}(\mathbb{N}^k \times \mathbb{N}^k)$ for all k, by $\Delta_k(\underline{n}, \underline{m}) = \bigwedge_{r=1}^{k} \Delta(n_r, m_r)$.

$P_{dec}(\mathbb{N}^k)$ carries a natural Boolean algebra structure, whose details we omit.

Now define a new category $\hat{\mathcal{S}}$ as follows:

Objects are pairs $(A, \mathbb{N}^k)$ where $A \in P_{dec}(\mathbb{N}^k)$.
A map $f : (A, \mathbb{N}^k) \longrightarrow (B, \mathbb{N}^\ell)$ is an equivalence class of maps $g : \mathbb{N}^k \longrightarrow \mathbb{N}^\ell$ satisfying $A \leq f^{-1}(B)$ where g_1, g_2 are equivalent if $A \leq (g_1, g_2)^{-1}(\Delta_\ell)$.

Composition is defined in the obvious way. We may embed $\mathcal{S}$ in $\hat{\mathcal{S}}$ by taking $\mathbb{N}^k$ to $(\mathbb{N}^k, \mathbb{N}^k)$ where the first symbol denotes the constant map $\mathbb{N}^k \longrightarrow \mathbb{N}$ taking the value 1, i.e. $\mathbb{N}^k \longrightarrow 1 \xrightarrow{\ulcorner 1 \urcorner} \mathbb{N}$.

Here are some properties of $\mathcal{S} \longrightarrow \hat{\mathcal{S}}$:

1) $\hat{\mathcal{S}}$ has finite limits, and $\mathcal{S} \longrightarrow \hat{\mathcal{S}}$ preserves products.
2) $\hat{\mathcal{S}}$ is a regular category, and every map factorises as a split epi followed by a mono.
(Warning: do not confuse monos with subsets as defined above).
[That regular epis split is a consequence of bounded minimization. If $f : \mathbb{N} \longrightarrow \mathbb{N}$ is primitive recursive, we can define $\bar{f}(n) = \mu m . \{ m \leq n , f(m) = f(n) \}$.]
3) $\hat{\mathcal{S}}$ has coproducts, which are disjoint and preserved by pullback.
4) The free category on a graph object exists.

Any regular category can be completed to a regular category in which equivalence relations have quotients. The completion is quite standard. The new objects are pairs (X, R) where R is an equivalence relation on X.

Maps $(X,R) \longrightarrow (Y,S)$ are equivalence classes of maps $X \xrightarrow{f} Y$ for which $R \subseteq (f,f)^{-1}(S)$, where f_1 and f_2 are equivalent if $R \subseteq (f_1,f_2)^{-1}(S)$.

We have, starting with a Skolem Theory $\mathcal{S}$, a two stage completion process:

$$\mathcal{S} \longrightarrow \hat{\mathcal{S}} \longrightarrow \bar{\hat{\mathcal{S}}}$$

add in subobjects — add in quotients

Definition An arithmetic universe (AU) is a pretopos in which free category objects on graph objects exist.

The point of our completion process is that $\bar{\hat{\mathcal{S}}}$ is an AU.

Definition An object X is decidable if the subobject $X \xrightarrow{(1_X,1_X)} X \times X$ of $X \times X$ has a complement.

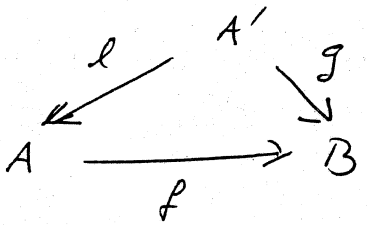
Here are some interesting facts about $\bar{\hat{\mathcal{S}}}$:

1. If $T \longrightarrow 1$ is epi, there is an epi $\mathbb{N} \longrightarrow T$ ("nonempty objects are enumerable").
2. If X is decidable, and there is a mono $\mathbb{N} \rightarrow X$, then X is isomorphic to $\mathbb{N}$.
3. If X is decidable, then $\mathrm{Hom}(X,-)$ preserves epis ("decidable objects are projective")
4. If X is decidable then $\mathbb{N}$ is isomorphic to $X+Y$ for some Y.
5. Every object is a quotient of a decidable object.
6. The decidable objects are the ones isomorphic to objects in the image of $\hat{\mathcal{S}} \longrightarrow \bar{\hat{\mathcal{S}}}$.

Definition An arithmetic universe is consistent if $0 \in P(1)$ and $1 \in P(1)$ are distinct. An arithmetic universe is complete if given $u \in P(1)$ either $u = 0$ or $u = 1$.

We denote by $\mathcal{A}_0$ the initial arithmetic universe $\widehat{\mathcal{S}_0}$. Of course, $\underline{Set}$ is an AU, so there is a unique map of AU $\mathcal{A}_0 \longrightarrow \underline{Set}$, taking an "algorithm" g to the function $|g|$ that it specifies. We have already mentioned that $\mathcal{A}_0[\Sigma^{-1}]$, where Σ is the class of maps inverted by $\mathcal{A}_0 \longrightarrow \underline{Set}$, is the arithmetic universe of recursive functions.

[Kleene's normal form essentially states that any recursive function $A \xrightarrow{f} B$ is a "span"



where g is primitive recursive and l is a bijective primitive recursive function.]

Gödel's Incompleteness Theorem can now be stated:

Any arithmetic universe object in $\mathcal{A}_0[\Sigma^{-1}]$ is necessarily incomplete.

[Internal categories.

If $\mathcal{C}$ is a category with pullbacks, we can define the notion of a "category object" or "internal category" in $\mathcal{C}$. Similarly, we can define the notion of a graph object in $\mathcal{C}$. The category of internal graphs in $\mathcal{C}$ is the category of functors from $\bullet \rightrightarrows \bullet$ to $\mathcal{C}$ and natural maps.

More generally, we suppose that $\mathcal{C}$ has finite limits. Then for any "essentially algebraic" theory $\mathcal{T}$, we have the category $\mathcal{T}(\mathcal{C})$ of $\mathcal{T}$-models in $\mathcal{C}$. This is just $Lex(\mathcal{T}, \mathcal{C})$, where $\mathcal{T}$ is a category with finite limits, and $Lex(\mathcal{T}, \mathcal{C})$ denotes the category of finite limit preserving functors from $\mathcal{T}$ to $\mathcal{C}$. We may identify $\mathcal{T}$ with the category of finitely-presented $\mathcal{T}$-models in Sets.

Thus, the notions of graph, category etc. are essentially algebraic. So are the notions of category-with-finite-limits, and AU. Recall that an AU is a pretopos $\mathcal{A}$ (regular category with stable coproducts, and quotients by equivalence relations) for which the forgetful functor

$$Cat(\mathcal{A}) \longrightarrow Graph(\mathcal{A})$$

has a left adjoint. It may be deduced from this, that if $\mathcal{A}$ is an AU, then the forgetful functor

$$AU(\mathcal{A}) \longrightarrow Graph(\mathcal{A})$$

has a left adjoint! In particular, in any AU $\mathcal{A}$ we may form the initial AU-object $\mathcal{A}_{\mathcal{A}}$. If $\mathcal{A}$ is $\mathcal{A}_0$, the initial AU, it follows that (as 1 is projective) since $T = Hom_{\mathcal{A}_0}(1, -)$ is a map of arithmetic universes,

$$T(\mathcal{A}_{\mathcal{A}_0}) \simeq \mathcal{A}_0$$

]

In other words, for the initial arithmetic universe $\mathcal{A}_0$, we have an "encoding" functor

$$E: \mathcal{A}_0 \xrightarrow{\sim} T(\mathcal{A}_{\mathcal{A}_0}) \qquad X \longmapsto X'$$

which is an equivalence. So for each $X \in \mathcal{A}_0$ we have a map $1 \xrightarrow{x'} Ob(\mathcal{A}_{\mathcal{A}_0})$, and for each $X \xrightarrow{f} Y \in \mathcal{A}_0$ we have a map $1 \xrightarrow{f'} Map(\mathcal{A}_{\mathcal{A}_0})$ for which $dom(f') = X'$, $cod(f') = Y'$, etc.

We use the notation $\mathcal{A}_{\mathcal{A}_0}(X', Y')$ for the pullback

$$\begin{array}{ccc} \mathcal{A}_{\mathcal{A}_0}(X',Y') & \longrightarrow & 1 \\ \downarrow & & \downarrow (X',Y') \\ Map(\mathcal{A}_{\mathcal{A}_0}) & \xrightarrow{(dom,\,cod)} & Ob(\mathcal{A}_{\mathcal{A}_0}) \times Ob(\mathcal{A}_{\mathcal{A}_0}) \end{array}$$

Proposition

There is a unique natural map $X \xrightarrow{\gamma_X} \mathcal{A}_{\mathcal{A}_0}(1', X')$.

Proof

Construct the category $\mathcal{B}$ whose objects are pairs (X, x) with $X \in \mathcal{A}_0$ and $X \xrightarrow{x} \mathcal{A}_{\mathcal{A}_0}(1', X')$, and whose maps $(X, x) \to (Y, y)$ are given by those $X \xrightarrow{f} Y$ in $\mathcal{A}_0$ for which

$$\begin{array}{ccc} X & \xrightarrow{x} & \mathcal{A}_{\mathcal{A}_0}(1', X') \\ f \downarrow & & \downarrow \mathcal{A}_{\mathcal{A}_0}(1', f') \\ Y & \xrightarrow{y} & \mathcal{A}_{\mathcal{A}_0}(1', Y') \end{array} \qquad \text{commutes.}$$

One proves that $\mathcal{B}$ is an AU, so there is a unique map of AU $\mathcal{A}_0 \to \mathcal{B}$, which clearly has the form $X \longmapsto (X, \gamma_X)$.

For any "object" X' of $\mathcal{H}_{\mathcal{H}_0}$ we can form the object $P'(X')$ of its "subobjects" in $\mathcal{H}_0$.

Choose an enumeration $\mathbb{N} \xrightarrow{q} P'(\mathbb{N}')$ and form the pullback

$$\begin{array}{ccccc} D & \longrightarrow & & & 1 \\ \downarrow & & & & \downarrow 0 \\ \mathbb{N} & \xrightarrow{(1_{\mathbb{N}}, 1_{\mathbb{N}})} & \mathbb{N}\times\mathbb{N} & \xrightarrow{\eta_{\mathbb{N}}\times q} & \mathcal{H}_{\mathcal{H}_0}(1',\mathbb{N}')\times P'(\mathbb{N}') \xrightarrow{\text{eval}} P'(1') \end{array}$$

Since 1 is projective in any $\mathcal{HU}$, choose a map $1 \xrightarrow{n} \mathbb{N}$ such that $D' = q(n)$. Now define the pullback

$$\begin{array}{ccc} [\![n \in D]\!] & \longrightarrow & D \\ \downarrow & & \downarrow \\ 1 & \xrightarrow{n} & \mathbb{N} \end{array}$$

and consider $[\![n \in D]\!]' : 1 \longrightarrow P'(1')$. Then we get the pullback diagram

$$\begin{array}{ccc} [\![n \in D]\!] & \longrightarrow & 1 \\ \downarrow & & \downarrow 0' \\ 1 & \xrightarrow{[\![n \in D]\!]'} & P'(1') \end{array}$$

but also the commutative diagram

$$\begin{array}{ccc} [\![n \in D]\!] & \longrightarrow & 1 \\ \downarrow & & \downarrow 1' \\ 1 & \xrightarrow{[\![n \in D]\!]'} & P'(1') \end{array}$$

If $[\![n \in D]\!]$ were $\emptyset$, then $[\![n \in D]\!]$ is the pullback of $0'$ along $0'$, hence is 1, contradicting consistency. So the consistency of $\mathcal{H}_{\mathcal{H}_0}$ is not provable if $\mathcal{H}_0$ is consistent.