Categorical Models of Constructive Logic

Thomas STREICHER
Fachbereich 4 Mathematik, TU Darmstadt
Schloßgartenstr. 7, D-64289 Darmstadt
streicher@mathematik.tu-darmstadt.de

January 2003

1 Introduction

If asked why one should be interested in constructive (intuitionistic) logic besides saying that it is a nice subject that makes a lot of fun I could give the following two more serious reasons

(1) from proofs in constructive logic one may extract algorithms, bounds etc.[1]

(2) weakening the logic allows one to postulate axioms that are classically false, e.g. *all functions are computable* or *all functions are continuous*.

The issues raised in (1) are typically dealt with by proof theory whereas those raised in (2) are best treated via the methods of *Categorical Logic* and that's what these lectures are about: in other words the *model theory of constructive logic*.

However, its flavour will be very different from classical model theory. The essential difference is that for the purposes of constructive logic we can *not* restrict ourselves to 2-valued models (as 2-valued models automatically validate the principle of excluded middle). Notice that even for classical logic and set theory non-2-valued boolean models are important as e.g. in *forcing* models needed for obtaining independence results in set theory. In any case 2-valuedness is an illusion of naive Platonism as any reasonable theory T (containing a modicum of arithmetic) will leave some propositions undecided (e.g. the Lindenbaum-Tarski algebra of Peano arithmetic or ZF(C) is a highly non-trivial infinite boolean algebra).

Non-2-valued models of *propositional* logic have already a long tradition. We recall the basic notions here as they form the basic building blocks for an extension to first and higher order predicate logic. The basic idea of *algebraic semantics* is to view the collection of *propositions* (i.e. what sentences denote) as a quasiorder or partial order $(A, \leq)$ where the elements of A are thought of as propositions and $a \leq b$ as "a entails b". Of course, it is not an arbitrary

[1] though to some extent this is also possible for classical logic!

poset as it has to satisfy certain structural requirements needed for interpreting the propositional connectives. The true proposition $\top$ will be identified with the greatest element of A and the false proposition $\bot$ will be identified with the least element of A. Conjunction and disjunction correspond to binary infima and suprema in A which due to this analogy are denoted as $\wedge$ and $\vee$ respectively. Constructive implication is given by *Heyting implication* requiring that for all $a, b \in A$ there is an element $a \to b$ in A such that

$$c \leq a \to b \qquad \text{iff} \qquad c \wedge a \leq b$$

for all $c \in A$. Notice that $a \to b$ is determined uniquely by this property as the *greatest* element of $\{c \in A \mid c \wedge a \leq b\}$. We call $(A, \leq)$ a *Heyting algebra* or *Heyting lattice* iff $(A, \leq)$ is a lattice and $a \to b$ exists for all $a, b \in A$. In a Heyting lattice negation is defined as $\neg a = a \to \bot$. A *boolean lattice* is a Heyting lattice A where negation is involutive, i.e. $\neg\neg a \leq a$ for all $a \in A$.[2] Typical examples of (complete) Heyting lattices are those of the form $(\mathcal{O}(X), \subseteq)$ where X is a topological space and $\mathcal{O}(X)$ stands for the collection of its open sets. Notice that $U \to V$ is given as the union of all W with $W \cap U \subseteq V$. The traditional notion of *Kripke* models now appears as a particular instance: let P be a poset and consider $A = \mathsf{dcl}(P)$, the set of downward closed subsets of P ordered by set inclusion. In this case Heyting implication is given by

$$x \in A \to B \qquad \text{iff} \qquad \forall y \leq x.\, y \in A \Rightarrow y \in B$$

which to check we leave as an exercise to the inclined reader.

One advantage of Heyting/boolean lattices is that they subsume "term models" obtained by factorizing syntax modulo provable entailment (traditionally called Lindenbaum-Tarski algebras). Thus, w.r.t. general Heyting or boolean algebras completeness is a triviality. Notice that we don't consider this generality as a great achievement. It rather happens accidently as there is no natural way to tell "interesting" models form purely syntactic ones. Of course, mathematically the non-term models are more interesting as the pay you more than you have invested (syntactically).

2 Hyperdoctrines

The aim of this section is to solve the proportional equation

$$\text{prop. logic} : \text{Heyt./bool. lattices} = \text{first/higher order predicate logic} : ?$$

The problem we have to face is that in predicate logic we can't simply deal with one Heyting (or boolean algebra) but for *every context* $\Gamma \equiv x_1 : A_1, \ldots, x_n : A_n$ we have to consider the propositions in context Γ. Usually, the context of object variables is not made explicit but we do for the moment for the sake of clarity. We write $\Gamma \mid \varphi$ if φ is a proposition whose free variables are all declared in

[2] this suffices as $a \leq \neg\neg a$ holds in every Heyting lattice.

Γ and we write $\Gamma \mid \psi \vdash \varphi$ to state that (in context Γ) proposition ψ entails proposition φ. Evidently, for fixed Γ the collection of $\Gamma \mid \varphi$ *modulo* $\vdash_\Gamma$ (where $\psi \vdash_\Gamma \varphi$ stands for $\Gamma \mid \psi \vdash \varphi$) forms a (quasi-)order $\mathcal{P}(\Gamma)$. Of course, the various $\mathcal{P}(\Gamma)$ are not at all unrelated: for every *substitution* $\sigma : \Delta \to \Gamma$ (as given by a tuple $\langle t_1, \ldots, t_n \rangle$ with $\Delta \mid t_i : A_i$) we have $\Delta \mid \psi[\sigma] \vdash \varphi[\sigma]$ whenever $\Gamma \mid \psi \vdash \varphi$. Moreover, substitution preserves the propositional connectives and, therefore, a substitution $\sigma : \Delta \to \Gamma$ induces a map $\mathcal{P}(\sigma) = \sigma^* : \mathcal{P}(\Gamma) \to \mathcal{P}(\Delta)$ by sending (the equivalence class of) φ to (the equivalence class of) $\varphi[\sigma]$. Thus, writing $\mathcal{C}$ for the category of contexts and substitutions we have

$$\mathcal{P} : \mathcal{C}^{\mathsf{op}} \to \mathbf{pHa}$$

where **pHa** is the category of pre-Heyting lattices and their morphisms.

Now let us turn to quantification. The crucial rule for universal quantification is

$$\psi \vdash \varphi \qquad \text{iff} \qquad \psi \vdash \forall x{:}A.\varphi$$

where, most importantly, the variable x must not appear freely in ψ. In our notation making contexts explicit this reads as follows

$$\Gamma, x : A \mid \psi \vdash \varphi \qquad \text{iff} \qquad \Gamma \mid \psi \vdash \forall x{:}A.\varphi$$

where $\Gamma, x : A \mid \varphi$ and $\Gamma \mid \psi$ (the latter bringing the variable condition to the point!). Even more pedantically we could write

$$\Gamma, x : A \mid \psi[\pi] \vdash \varphi \qquad \text{iff} \qquad \Gamma \mid \psi \vdash \forall x{:}A.\varphi$$

from which we see that $\forall x{:}A.$ is *right adjoint* to $[\pi]$. Similarly, one can convince oneself that $\exists x{:}A.$ is *left adjoint* to $[\pi]$. These observations made by F. W. Lawvere at the end of the 1960ies were his motivation to define *hyperdoctrines* as a categorical notion of model for predicate logic.

Definition 2.1 (posetal hyperdoctrine)
A (posetal) hyperdoctrine *is a functor* $\mathcal{P} : \mathcal{C}^{\mathsf{op}} \to \mathbf{pHa}$ *such that* $\mathcal{C}$ *has finite limits and for every* $f : J \to I$ *in* $\mathcal{C}$ *the functor* $f^* = \mathcal{P}(f) : \mathcal{P}(I) \to \mathcal{P}(J)$ *has both adjoints, i.e.*

$$\exists_f \dashv f^* \dashv \forall_f \,,$$

satisfying the so-called Beck-Chevalley condition (BC) *requiring that for every pullback diagram in* $\mathcal{C}$

$$\begin{array}{ccc} \cdot & \xrightarrow{q} & K \\ {\scriptstyle p}\downarrow & \lrcorner & \downarrow{\scriptstyle g} \\ J & \xrightarrow[f]{} & I \end{array}$$

and every $\varphi \in \mathcal{P}(J)$ it holds that the canonical morphism $g^*\forall_f\varphi \to \forall_q p^*\varphi$ (obtained by transposing $q^*g^*\forall_f\varphi \cong p^*f^*\forall_f\varphi \overset{p^*\varepsilon}{\to} p^*\varphi$ where $\varepsilon : f^*\forall_f\varphi \to \varphi$ is the counit of $f^* \dashv \forall_f$ at φ) is an isomorphism and similarly for $\exists_f$.[3]

*A posetal hyperdoctrine $\mathcal{P} : \mathcal{C}^{\mathsf{op}} \to$ **pHa** is called a* tripos *iff for every object I in $\mathcal{C}$ there are $P(I)$ in $\mathcal{C}$ and $\in_I$ in $\mathcal{P}(I{\times}P(I))$ such that for every $\rho \in \mathcal{P}(I{\times}J)$ there is a morphism $\chi = \chi_\rho : J \to P(I)$ with ρ equivalent to $\mathcal{P}(I{\times}\chi)(\in_I)$ in $\mathcal{P}(I{\times}J)$.* ◊

The purpose of BC is to guarantee that substitution commutes with quantification in the appropriate way. Consider for example the pullback

$$\begin{array}{ccc} \Delta \times A & \xrightarrow{\sigma \times id_A} & \Gamma \times A \\ {\scriptstyle\pi}\downarrow & \text{(I)} & \downarrow{\scriptstyle\pi} \\ \Delta & \xrightarrow[\sigma]{} & \Gamma \end{array}$$

in which case BC states the equivalence of $(\forall x{:}A.\varphi)[\sigma]$ and $\forall x{:}A.\varphi[\sigma{\times}id_A]$.

Remarkably an equality predicate on $I \in \mathcal{C}$ can be obtained as

$$Eq_I = \exists_\delta \top$$

where $\delta = \delta_I = \langle id_I, id_I\rangle$. Thus Eq_I is characterised by $Eq_I \leq_{I\times I} \rho$ iff $\top \leq_I \delta^*\rho$. On the syntactical level this amounts to the proof rule

$$Eq(x,y) \vdash R(x,y) \qquad \text{iff} \qquad \vdash R(x,x)$$

from which it is an easy exercise to derive reflexivity and substitutivity of Eq. Of course, this should also hold in presence of some parameters as given by a context Γ amounting on the semantic side to the requirement that left adjoints exists to substitution along $\Gamma{\times}\delta_A$ and that these satisfy BC for pullbacks of the form

$$\begin{array}{ccc} \Delta \times A & \xrightarrow{\sigma \times A} & \Gamma \times A \\ {\scriptstyle\Delta\times\delta_A}\downarrow & \text{(II)} & \downarrow{\scriptstyle\Gamma\times\delta_A} \\ \Delta \times A \times A & \xrightarrow[\sigma\times A\times A]{} & \Gamma \times A \times A \end{array}$$

Thus, for the sake of interpreting first order logic (FOL) in a posetal hyperdoctrines it would suffice to require adjoints only along projections and morphisms of the form $\Gamma \times \delta$ and BC only for pullbacks of the form (I) and (II) as considered above. Thus, in our definition of hyperdoctrine we have required a

[3] more explicitly, we require that the canonical map $\exists_q p^*\varphi \to g^*\exists_f\varphi$ (obtained as transpose of $p^*\varphi \overset{p^*\eta}{\to} p^*f^*\exists_f\varphi \cong q^*g^*\exists_f\varphi$ where $\eta : \varphi \to f^*\exists_f\varphi$ is the unit of $\exists_f \dashv f^*$ at φ) is an isomorphism

bit more than needed for interpreting predicate logic. However, in most interesting examples (not including term models) we do have quantification along arbitrary morphisms in the base and BC for all pullbacks in the base.

Just as posetal hyperdoctrines provide a notion of model for FOL triposes provide a notion of model for higher order logic (HOL) as they allow one to quantify over $P(I)$, the type of predicates on I. We leave it as an exercise to show that in triposes the equality predicate $Eq_I(i,j)$ is equivalent to Leibniz equality $\forall P : P(I).\, (i \in_I P) \to (j \in_I P)$. Although triposes allow one to interpret the comprehension schema of HOL they do not in general validate extensionality for predicates. The reason is that *different* morphism $\chi_1, \chi_2 : J \to P(I)$ may induce *equivalent* predicates $(I \times \chi_1)^* \in_I$ and $(I \times \chi_2) * \in_I$ in $\mathcal{P}(I \times J)$ (as we shall see later). Notice that if the base category $\mathcal{C}$ of a hyperdoctrine $\mathcal{P}$ is cartesian closed then for being a tripos it suffices[4] to postulate the existence of a so-called *generic predicate* $Tr \in \mathcal{P}(\Omega)$ satisfying the requirement that for all $\varphi \in \mathcal{P}(I)$ there exists a morphism $\chi = \chi_\varphi : I \to \Omega$ such that φ is equivalent to $\chi^* Tr$ in $\mathcal{P}(I)$. As most triposes considered subsequently will be based on **Set** (which is cartesian closed) the existence of a generic (truth) predicate will suffice.

Triposes were introduced under the name *formal topos* by J. Bénabou already beginning of the 1970ies and later reinvented by Hyland, Johnstone and Pitts around 1980.

Finally notice that one may also consider non-posetal hyperdoctrines where not all proofs of entailments between predicates are identified. Then one has to consider so-called *pseudo-functors* from $\mathcal{C}^{\mathsf{op}}$ to the category of, say, (bi)cartesian closed categories. To make things precise would require some knowledge about fibred categories. However, as for the purpose of the current course we are not interested in modeling proofs and their equality it will be sufficient to consider only posetal hyperdoctrines which just capture the notion of constructive validity.

Now it's time to come to examples.

As (it should have become) evident from our motivation of hyperdoctrines factorizing syntax modulo provable equivalence gives rise to (almost) hyperdoctrines where existence of quantifiers is guaranteed only along projections and morphisms of the form $\Gamma \times \delta$ and BC is only required for pullbacks of the form (I) and (II).

The tripos corresponding to the usual set-theoretic semantics of HOL (with predicate types interpreted as full power sets) is provided by $\mathcal{P} : \mathbf{Set}^{\mathsf{op}} \to \mathbf{pHa}$ sending I to the powerset $\mathcal{P}(I)$ and $f : J \to I$ to the map $\mathcal{P}(f) = f^{-1} : \mathcal{P}(I) \to \mathcal{P}(J) : A \mapsto f^{-1}[A] = \{j \in J \mid f(j) \in A\}$.

More interesting, however, are triposes of Heyting-valued sets and realizability triposes which will be discussed next.

[4] from a generic predicate $Tr \in \mathcal{P}(\Omega)$ one can define $P(I)$ as Ω^I and $\in_I$ as $\varepsilon^* Tr$ where $\varepsilon : \Omega^I \times I \to \Omega$ is the evaluation map in $\mathcal{C}$

Heyting-valued Sets

Let A be a *complete* Heyting algebra, i.e. a Heyting algebra having arbitrary suprema (and infima). Then we may define a **Set**-based tripos $\mathcal{P} = \mathcal{P}_A$ by assigning to every set I the (complete) Heyting algebra $\mathcal{P}_A(I) = A^I$ (ordered pointwise) and to every $f : J \to I$ in **Set** the function $\mathcal{P}_A(f) : \mathcal{P}(I) \to \mathcal{P}(J) : \varphi \mapsto \varphi \circ f$ which, obviously, preserves the Heyting algebra structure (and all suprema and infima as well).

Quantification along $f : J \to I$ is given by

$$\exists_f(\varphi)(i) = \bigvee_{j \in J} Eq(i, f(j)) \wedge \varphi(j)$$

and

$$\forall_f(\varphi)(i) = \bigwedge_{j \in J} Eq(i, f(j)) \to \varphi(j)$$

where $Eq(x, y) = \bigvee\{\top \mid x = y\}$.[5] We verify that $\psi \vdash_I \forall_f(\varphi)$ if and only if $f^*\psi \vdash_J \varphi$. We have

$$\psi \vdash_I \forall_f(\varphi)$$

iff

$$\text{for all } i \in I, j \in J \text{ it holds that } \psi(i) \vdash Eq(i, f(j)) \to \varphi(j)$$

which due to the definition of Eq is equivalent to

$$\text{for all } j \in J \text{ it holds that } \psi(f(j)) \leq \varphi(j)$$

i.e. iff

$$f^*\psi \leq \varphi$$

as required. We leave it as an exercise to the reader to verify that these quantifiers do satisfy BC.

Finally, a generic predicate for $\mathcal{P}_A$ is given by $\Omega = A$ and $Tr(a) = a$ thus establishing the claim that $\mathcal{P}_A$ actually is a tripos.

Realizability Triposes

In this section we will construct triposes from an arbitrary partial combinatory algebra (pca) $\mathcal{A}$.[6] Such a pca is thought of as a model of untyped computation, i.e. the elements of $\mathcal{A}$ are considered as (sort of possibly *abstract*) algorithms.

[5] Notice that, actually, it holds that $\exists_\delta(\top)(i_1, i_2) = Eq(i_1, i_2)$ as suggested by notation.

[6] Recall that a pca is given by a set (also called $\mathcal{A}$) together with a binary partial operation $\cdot$ on it such that there exists $k, s \in \mathcal{A}$ satisfying

$$k{\cdot}x{\cdot}y = x \qquad s{\cdot}x{\cdot}y\downarrow \qquad s{\cdot}x{\cdot}y{\cdot}z \simeq x{\cdot}y{\cdot}(y{\cdot}z)$$

for all $x, y, z \in \mathcal{A}$. Typical examples of pcas are natural numbers with Kleene application ($n{\cdot}m = \{n\}(m)$) or models of untyped λ-calculus. As in untyped λ-calulus in pca's one can encode pairing, projections, natural numbers and all partial recursive functions on them of which fact we will make essential use in the sequel.

The ensuing *realizability tripos* $\mathcal{P}_{\mathcal{A}} : \mathbf{Set}^{\mathsf{op}} \to \mathbf{pHa}$ will be constructed as follows: for every set I we define $\mathcal{P}_{\mathcal{A}}(I)$ as the set $\mathcal{P}(\mathcal{A})^I$ of all functions from I to the powerset of $\mathcal{A}$ (pre-)ordered as follows

$$\varphi \leq_I \psi \qquad \text{iff} \qquad \exists e \in \mathcal{A}. \forall i \in I. \forall a \in \varphi(i).\ e{\cdot}a \downarrow \wedge\ e{\cdot}a \in \psi(i)$$

i.e. φ entails ψ (over I) iff there is an algorithm e that uniformly in i sends realizers (i.e. elements) of $\varphi(i)$ to realizers of $\psi(i)$.

Due to the coding capacities of pca's we can define propositional connectives on the set $\Omega = \mathcal{P}(\mathcal{A})$ of propositions as follows

$$\begin{aligned}
&\bot = \emptyset \qquad \top = \mathcal{A} \\
&A \to B = \{e \in \mathcal{A} \mid \forall a \in \mathcal{A}.\ a \in A \Rightarrow e{\cdot}a \downarrow \wedge\ e{\cdot}a \in B\} \\
&A \wedge B = \{\langle a, b\rangle \mid a \in A, b \in B\} \\
&A \vee B = A + B = \big(\{0\}{\times}A\big) \cup \big(\{1\}{\times}B\big)
\end{aligned}$$

which in a sense can be understood as an "implementation" of the Brouwer-Heyting-Kolmogoroff interpretation of constructive logic where a proposition is identified with the collection of its "proofs", here more neutrally referred to as *realizers*.

Now we come to quantification. For $\pi : I{\times}J \to I$ and $\varphi \in \mathcal{P}_{\mathcal{A}}(I{\times}J)$ existential and universal quantification along π are given by

$$\exists_\pi(\varphi)(i) = \bigcup_{j \in J} \varphi(i,j) \qquad \text{and} \qquad \forall_\pi(\varphi)(i) = \bigcap_{j \in J} \varphi(i,j)$$

respectively. For constructing quantifiers along along arbitrary maps we first have to introduce an equality predicate

$$Eq_I(i_1, i_2) = \{a \in \mathcal{A} \mid i_1 = i_2\}$$

for every set I. Now for $f : J \to I$ in **Set** quantification along f is given by

$$\exists_f(\varphi)(i) = \bigcup_{j \in J} Eq_I(i, f(j)) {\wedge} \varphi(j) \qquad \text{and} \qquad \forall_f(\varphi)(i) = \bigcap_{j \in J} Eq(i, f(j)) \to \varphi(j)$$

respectively. Showing hat these are actually left and right adjoints to f^*, respectively, and satisfy BC for arbitrary pullbacks in the base we leave as a lengthy, but straightforward exercise to the inclined reader.

For seeing that $\mathcal{P}_{\mathcal{A}}$ is a tripos put $\Omega = \mathcal{P}(\mathcal{A})$ and $Tr = id_\Omega$. The latter is a generic predicate as for every $\varphi \in \mathcal{P}_{\mathcal{A}}(I) = \mathcal{P}(\mathcal{A})^I$ we have $\varphi^* Tr = id_\Omega \circ \varphi = \varphi$.

The following exercise might be instructive: show that for every $\varphi \in \mathcal{P}_{\mathcal{A}}(I{\times}J)$ and $\psi \in \mathcal{P}_{\mathcal{A}}(I)$ the predicates $\big(\forall j{:}J.\varphi(i,j)\big) \vee \psi(i)$ and $\forall j{:}J.\big(\varphi(i,j) \vee \psi(i)\big)$ are equivalent predicates over I provided J is not empty.[7]

[7]The reason is that in **Set** for non-empty I we have $\bigcap_{i \in I}(B + A_i) = B + \bigcap_{i \in I} A_i$ where $+$ stands for disjoint union.

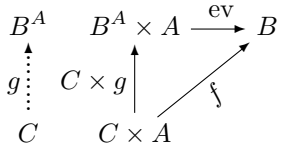
3 Elementary Toposes

One might have got the impression that triposes are fairly complicated structures. Actually, there is something much simpler, namely *elementary toposes*.[8] We shall see soon that every topos can be considered as a hyperdoctrine in a canonical way and that with any tripos $\mathcal{P} : \mathcal{C}^{\mathsf{op}} \to \mathbf{pHa}$ one may associate an elementary topos $\mathcal{C}[\mathcal{P}]$. Thus, elementary toposes can be considered as abstractions of triposes.

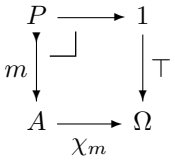
Probably the simplest definition of an elementary topos is the following one.

Definition 3.1 (Elementary Topos)
An (elementary) topos *is a category $\mathcal{E}$ with finite limits, exponentials and a subobject classifier $\top : 1 \to \Omega$.* ◊

Recall that an exponential of B by A is given by an object B^A together with an evaluation map $\mathrm{ev} : B^A \times A \to B$ such that for every $f : C \times A \to B$ there exists a unique map $g : C \to B^A$, denoted as $\lambda(f)$, such that $\mathrm{ev} \circ (C \times g) = f$, i.e.



and that a subobject classifier is a map $\top : 1 \to \Omega$ such that for every mono(morphism) $m : P \rightarrowtail A$ there exists a unique map $\chi = \chi_m : A \to \Omega$ (called *classifying* map for m) such that



is a pullback.

Notice that exponentials are uniquely determined up to isomorphism by the requirement that

$$\mathcal{E}(C \times A, B) \cong \mathcal{E}(C, B^A)$$

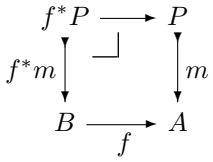
naturally in C. Similarly, one can see that subobject classifiers are determined uniquely up to isomorphism by the requirement that

$$\mathrm{Sub}_{\mathcal{E}}(A) \cong \mathcal{E}(A, \Omega)$$

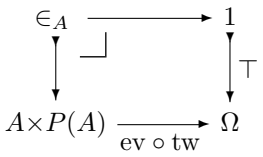
naturally in A where $\mathrm{Sub}_{\mathcal{E}} : \mathcal{E}^{\mathsf{op}} \to \mathbf{PoSet}$ is the functor sending $A \in \mathcal{E}$ to the poset $\mathrm{Sub}_{\mathcal{E}}(A)$ of subobjects of A (as given by equivalence classes of monos into A) and for $f : B \to A$ the mapping $\mathrm{Sub}_{\mathcal{E}}(f)$ sends (the equivalence class of)

[8] introduced by F. W. Lawvere and M. Tierney in 1969-70

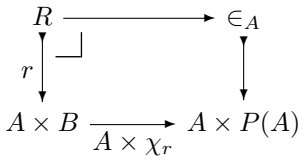
m to (the equivalence class of) f^*m, i.e. the pullback of m along f as in the diagram



Using exponentials together with the subobject classifier we can define now predicate types $P(A) = \Omega^A$ and an "element relation" between A and $P(A)$ by taking the following pullback



where the bottom map is twisting, i.e. $\mathrm{tw} = \langle \pi_2, \pi_1 \rangle$, followed by the evaluation map $\mathrm{ev} : P(A) \times A \to \Omega$. One readily checks that for every $r : R \rightarrowtail A \times B$ there exists a unique $\chi_r : B \to P(A)$ such that



Actually, one may axiomatize toposes in terms of power objects $P(A)$ and the element relations $\in_A$ by requiring for it the universal property just described.

Thus, more abstractly, one may define toposes as categories $\mathcal{E}$ with finite limits such that for all objects A of $\mathcal{E}$ we have

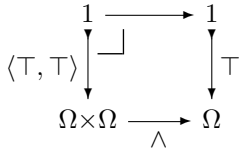
$$\mathrm{Sub}_{\mathcal{E}}(A \times B) \cong \mathcal{E}(B, P(A))$$

naturally in B, i.e. that the presheaf $\mathrm{Sub}_{\mathcal{E}}(A \times -)$ is representable for all A.

In any case the definition of elementary topos is surprisingly simple and, more importantly, absolutely syntax-free. It might come as a surprise that nevertheless these axioms imply sufficient structure for interpreting constructive higher order logic.

We now sketch a proof why this actually is the case.

Conjunction on Ω is given as the classifying map for the subobject $\langle \top, \top \rangle : 1 \rightarrowtail \Omega \times \Omega$ as exhibited in the diagram



Logical equivalence is given as the classifying map for the subobject $\delta_\Omega = \langle id_\Omega, id_\Omega \rangle : \Omega \to \Omega \times \Omega$ as in the diagram

$$\begin{array}{ccc} \Omega & \longrightarrow & 1 \\ {\scriptstyle \delta_\Omega}\downarrow & \lrcorner & \downarrow{\scriptstyle \top} \\ \Omega\times\Omega & \underset{\leftrightarrow}{\longrightarrow} & \Omega \end{array}$$

Notice that $\leftrightarrow$ is the equality predicate on Ω which for arbitrary objects A is constructed similarly, namely as the classifying map for δ_A. Now from $\leftrightarrow$ we can define implication $\to : \Omega \times \Omega \to \Omega$ as[9] the composite $\leftrightarrow \circ \langle \wedge, \pi_1 \rangle$. Finally, universal quantification over A is provided by the classifying map $\forall_A : \Omega^A \to \Omega$ for the subobject $1 \to \Omega^A$ obtained as the exponential transpose of $\top \circ \pi_1 : 1 \times A \to \Omega$.

We suggest it as a lengthy, but straightforward exercise to show that the gadgets just defined are actually behaving as expected. If you need any hints I recommend to look at the respective chapter in [MLM]. Typically, what one has to show is that

- for $f, g : X \to A$ it holds that $= \circ \langle f, g \rangle$ factors through $\top : 1 \rightarrowtail \Omega$ iff $f = g$
- if $p, q : A \to \Omega$ and $a : X \to A$ then $\to \circ \langle p, q \rangle \circ a$ factors through $\top : 1 \rightarrowtail \Omega$ iff for all $f : Y \to X$ if $p \circ a \circ f$ factors through $\top$ then so does $g \circ a \circ f$
- for arbitrary $r : B \times A \to \Omega$ and $b : X \to B$ it holds that $\forall_A \circ \lambda(r) \circ b$ factors through $\top$ iff $r \circ (b \times A)$ factors through $\top$

and a few more other things like that. Having done this one may define $\bot$, disjunction and existential quantification à la Prawitz, i.e. $\bot = \forall p{:}\Omega.p$, $p \vee q = \forall r{:}\Omega.(p \to r) \wedge (q \to r) \to r$ and $\exists x{:}A.p(x) = \forall r{:}\Omega.(\forall x{:}A.p(x) \to r) \to r$.

After having performed this lengthy exercise it is evident that for every topos $\mathcal{E}$ the subobject functor $\mathrm{Sub}_\mathcal{E} : \mathcal{E}^{\mathsf{op}} \to \mathbf{PoSet}$ is a tripos (over $\mathcal{E}$).

Now some examples are more than due.

Of course, the category **Set** of sets and functions is trivially a topos. But also for small categories $\mathbb{C}$ the category $\widehat{\mathbb{C}} = \mathbf{Set}^{\mathbb{C}^{\mathsf{op}}}$ of **Set**-valued functors on $\mathbb{C}$, the so-called *presheaves* over $\mathbb{C}$, are typical examples of toposes. In presheaf toposes limits (and also colimits) exist and are constructed pointwise, i.e. they are inherited from **Set**. Exponentials and subobject classifiers are constructed following the advice of the Yoneda lemma as follows. If B^A exists then by Yoneda we know that

$$B^A(I) \cong \widehat{\mathbb{C}}(\mathsf{Y}_\mathbb{C}(I), B^A) \cong \widehat{\mathbb{C}}(\mathsf{Y}_\mathbb{C}(I) \times A, B))$$

naturally in $I \in \mathbb{C}$ thus suggesting us how B^A has to look like provided it exists. Then proving the existence of B^A simply amounts to checking that putting

$$B^A(I) = \widehat{\mathbb{C}}(\mathsf{Y}_\mathbb{C}(I) \times A, B) \qquad \text{and} \qquad B^A(\alpha) = \widehat{\mathbb{C}}(\mathsf{Y}_\mathbb{C}(\alpha) \times A, B)$$

[9] the idea is that $x \leq y$ iff $x \wedge y = x$

actually does the job.[10] Similarly, the subobject classifier Ω has to satisfy according to Yoneda that

$$\Omega(I) \cong \widehat{\mathbb{C}}(\mathsf{Y}_{\mathbb{C}}(I), \Omega) \cong \mathrm{Sub}_{\widehat{\mathbb{C}}}(\mathsf{Y}_{\mathbb{C}}(I))$$

naturally in $I \in \mathbb{C}$. Thus $\Omega(I)$ consists of all subobjects of $\mathsf{Y}_{\mathbb{C}}(I)$, i.e. so-called *sieves* which are defined as collections of morphisms in $\mathbb{C}$ with codomain I and closed under composition (with arbitary morphisms) from the right. As $\mathrm{Sub}_{\widehat{\mathbb{C}}}$ sends $f : B \to A$ to the pullback functor $f^* : \mathrm{Sub}_{\widehat{\mathbb{C}}}(B) \to \mathrm{Sub}_{\widehat{\mathbb{C}}}(A)$ it is clear that for $\alpha : J \to I$ we have $\Omega(\alpha) = \mathsf{Y}_{\mathbb{C}}(\alpha)^*$ which in terms of sieves amounts to

$$\Omega(\alpha)(S) = \{\beta \mid \alpha \circ \beta \in S\}$$

The map $\top : 1 \to \Omega$ simply selects for all $I \in \mathbb{C}$ the maximal sieve on I consisting of *all* morphisms to I. One readily checks that for $m : P \rightarrowtail A$ in $\widehat{\mathbb{C}}$ its classifying morphism $\chi : A \to \Omega$ is given by

$$\chi_I(a) = \{\alpha : J \to I \mid A(\alpha)(a) \in P(J)\}$$

and we leave it as an exercise to show that χ is unique with the property $m \cong \chi^* \top$.

One could say a lot more about presheaf toposes as they encompass a lot of mathematical structures occuring "in nature" such as monoid and group actions (including dynamical systems), graphs, trees etc. (see [LS]).

We just mention that there is an important wider class of toposes than merely presheaf toposes, namely the so-called *Grothendieck toposes*, which appear as *localizations* of presheaf toposes, i.e. full subcategories $\mathcal{E}$ of some presheaf topos $\widehat{\mathbb{C}}$ such that the inclusion functor $i : \mathcal{E} \hookrightarrow \widehat{\mathbb{C}}$ has a left adjoint a which preserves finite limits. Such an $\mathcal{E}$ can be described as the category of *sheaves* over the site $(\mathbb{C}, \mathcal{J})$ where a sieve of $I \in C$ is a $\mathcal{J}$–cover if the so-called *sheafification* functor a sends the inclusion $S \hookrightarrow \mathsf{Y}_{\mathbb{C}}(I)$ to an isomorpism. More abstractly, Grothendieck toposes can be characterised as those elementary toposes $\mathcal{E}$ which have small sums and a small set of generators[11]. Toposes of Heyting-valued sets are precisely those Grothendieck toposes $\mathcal{E}$ which are *localic* in the sense that the subobjects of $1_{\mathcal{E}}$ form a small generating family.

But coming back to our main thread I will next show how every tripos $\mathcal{P} : \mathcal{C}^{\mathsf{op}} \to \mathbf{pHa}$ induces an associated topos $\mathcal{C}[\mathcal{P}]$. Applying this construction to the triposes $\mathcal{P}_A$ and $\mathcal{P}_{\mathcal{A}}$ will give rise to the topos of A-valued sets and the realizability topos over $\mathcal{A}$, respectively.

From Triposes to Toposes

Let $\mathcal{P} : \mathcal{C}^{\mathsf{op}} \to \mathbf{pHa}$ be a tripos. Then the topos $\mathcal{C}[\mathcal{P}]$ associated with $\mathcal{P}$ is constructed as follows.[12]

[10] The evaluation map $\mathrm{ev} : B^A \times A \to B$ is given as $\mathrm{ev}_I(\varphi, a) = \varphi_I(id_I, a)$ and we leave it as an exercise to construct λ-abstraction.

[11] i.e. there exists a family of objects $(G_i)_{i \in I}$ such that for all distinct $f, g : X \to Y$ in $\mathcal{E}$ there is a map $h : G_i \to X$ with $f \circ h \neq g \circ h$

[12] This construction is due to A. M.Pitts from his PhD Thesis in 1981.

The objects of $\mathcal{C}[\mathcal{P}]$ are pairs $X = (|X|, \sim_X)$ where $|X|$ is an object of $\mathcal{C}$ and $\sim_X \in \mathcal{P}(|X|\times|X|)$, i.e. a binary predicate on X in the sense of $\mathcal{P}$, satisfying the following conditions

$$\begin{array}{ll} \text{(symm)} & x_1 \sim_X x_2 \vdash x_2 \sim_X x_1 \\ \text{(trans)} & x_1 \sim_X x_2 \wedge x_2 \sim_X x_3 \vdash x_1 \sim_X x_3 \end{array}$$

when interpreted in $\mathcal{P}$ (where the x_i range over $|X|$). In the following let us write $E_X(x)$ as an abbreviation for $x \sim_X x$ (read "x exists"). Morphism from X to Y in $\mathcal{C}[\mathcal{P}]$ are defined as predicates $F \in \mathcal{P}(|X|\times|Y|)$ modulo (logical) equivalence satisfying the following conditions

$$\begin{array}{ll} \text{(strict)} & F(x,y) \vdash E_X(x) \wedge E_Y(y) \\ \text{(congr)} & x \sim_X x' \wedge y \sim_Y y' \wedge F(x,y) \vdash F(x',y') \\ \text{(sv)} & F(x,y) \wedge F(x,y') \vdash y \sim_Y y' \\ \text{(tot)} & E_X(x) \vdash \exists y{:}|Y|.F(x,y) \end{array}$$

where x, x' range over $|X|$ and y, y' range over $|Y|$.[13] The identity morphism on X is given by $\sim_X$ and if F and G represent morphism from X to Y and from Y to Z, respectively, then their composite is represented by the predicate $\exists y{:}|Y|.F(x,y) \wedge G(y,z)$ in $\mathcal{P}(|X|\times|Z|)$. One easily checks that this defines a category (using condition (congr) all the time).

The category $\mathcal{C}[\mathcal{P}]$ has finite products which are constructed as follows: for objects X, Y in $\mathcal{C}[\mathcal{P}]$ their product $X\times Y$ is given by $|X\times Y| = |X|\times|Y|$ and $\langle x,y\rangle \sim_{X\times Y} \langle x',y'\rangle \equiv x \sim_X x' \wedge y \sim_Y y'$ and first and second projection are given by $P_1(z,x) \equiv \pi_1(z) \sim_X x$ and $P_2(z,y) \equiv \pi_2(z) \sim_Y y$ where π_1 and π_2 are the projections in $\mathcal{C}$.

Subobjects of X in $\mathcal{C}[\mathcal{P}]$ are given by predicates $A \in \mathcal{P}(|X|)$ satisfying the conditions

$$A(x) \vdash E_X(x) \qquad \text{and} \qquad A(x) \wedge x \sim_X x' \vdash A(x')$$

with which one may associate the predicate $X|A \in \mathcal{P}(|X|\times|X|)$ which is defined as $X|A(x_1,x_2) \equiv A(x_1) \wedge x_1 \sim_X x_2$, the corresponding subobject is $(|X|, X|A)$ and its embedding into X is represented by $X|A$ as well. If $F, G \in \mathcal{P}(|X|\times|Y|)$ represent morphism from X to Y then their equaliser is represented by the predicate $A(x) \equiv \exists y{:}|Y|.F(x,y) \wedge G(x,y)$.

Now we come to the construction of power objects. Let X be an object in $\mathcal{C}[\mathcal{P}]$. Then the underlying object of $P(X)$ is given by $P(|X|)$. For defining $\sim_{P(X)}$ we first have to define the following existence predicate

$$E_{P(X)}(A) \equiv \big(\forall x{:}|X|.A(x) \to E_X(x)\big) \wedge \big(\forall x,x'{:}|X|.A(x) \wedge x \sim_X x' \to A(x')\big)$$

[13] Notice the analogy with the usual set-theoretic explanation of a function as a total and single valued relation! We just have added (strict) for guaranteeing that the relation holds only for "existing" elements, we have added (congr) for guaranteeing compatibility with equality in the sense of $\sim_X$ and $\sim_Y$ and required in (tot) definedness only for "existing" arguments.

saying that "A represents a subobject of X". Now the equality predicate of $P(|X|)$ is defined as

$$A \sim_{P(X)} B \;\equiv\; E_{P(X)}(A) \wedge E_{P(X)}(B) \wedge \forall x{:}|X|.(A(x) \leftrightarrow B(x))$$

where $A(x)$ is a shorthand for $\in_{|X|}(x, A)$ and similarly for $B(x)$. The subobject $\in_X \rightarrowtail X \times \mathcal{P}(X)$ is represented by $\in_{|X|} \in \mathcal{P}(|X| \times P(|X|))$ as expected. It is now a lengthy, but straightforward exercise left to the reader to show that every subobject $R \rightarrowtail Y \times X$ is isomorphic to $(Y \times \chi)^*$ for a unique $\chi : Y \to P(X)$.[14]

Now the exponential Y^X may be constructed as the subobject of single-valued and total relations in $P(X \times Y)$ either within the topos $\mathcal{C}[\mathcal{P}]$ or directly within the tripos $\mathcal{P}$. If one does it directly in $\mathcal{P}$ then the underlying object of Y^X is $P(|X| \times |Y|)$ and $R_1 \sim_{Y^X} R_2$ takes the form

$$E_{Y^X}(R_1) \wedge E_{Y^X}(R_2) \wedge \forall x{:}|X|, y{:}|Y|.R_1(x, y) \leftrightarrow R_2(x, y)$$

where $E_{Y^X}(R)$ is the conjunction of (the universal closures of) the conditions (strict), (congr), (sv), (tot) in the definition of morphisms in $\mathcal{C}[\mathcal{P}]$.

A partial combinatory algebra $\mathcal{A}$ provides some notion of untyped computation. The *realizability topos* $\mathsf{RT}(\mathcal{A}) = \mathbf{Set}[\mathcal{P}_\mathcal{A}]$ can be considered as a very organized synthesis of the world of sets and the world of algorithms as given by $\mathcal{A}$. The realizability topos $\mathsf{RT}(\mathcal{A})$ contains $\mathbf{Set}$ via the right adjoint $\nabla : \mathbf{Set} \hookrightarrow \mathsf{RT}(\mathcal{A})$ to the *global sections* functor $\Gamma = \mathsf{RT}(\mathcal{A})(1, -) : \mathsf{RT}(\mathcal{A}) \to \mathbf{Set}$. More concretely, the right adjoint ∇ sends a set I to $\nabla(I) = (I, Eq_I)$ and a function $f : I \to J$ to the morphism $\nabla(f) : \nabla(I) \to \nabla(J)$ represented by the relation $Eq_J(f(i), j)$.

Notice further as a peculiarity that in realizability toposes the subobject classifier Ω has just two global sections $\top, \bot : 1 \to \Omega$ and thus in a sense its logic is "2-valued". This, however, does *not* mean that its logic is boolean (i.e. that $\Omega \cong 2 = 1{+}1$) in general. For example in the *effective topos*, i.e. the realizability topos over $\mathbb{N}$ with Kleene application (*aka* the 1st Kleene algebra), for non-recursive predicates P on $\mathbb{N}$ it does *not* hold that $\forall n{:}\mathbb{N}.P(n) \vee \neg P(n)$ as a realizer for this proposition would give rise to a decision prodedure for P. Actually, one can show by a similar simple (cardinality) argument that for all non-trivial pca's $\mathcal{A}$ (i.e. pca's with more than one element) the realizability topos $\mathsf{RT}(\mathcal{A})$ is not boolean. Thus, for nontrivial pca's $\mathcal{A}$ the realizability topos $\mathsf{RT}(\mathcal{A})$ can not be well-pointed as well-pointed toposes are boolean (and 2-valued) as can be shown easily (see Ch. 6 of [MLM]).

[14] If $\rho \in \mathcal{P}(|Y| \times |X|)$ represents a subobject of $Y \times X$ then its classifying map from Y to $P(X)$ is represented by the predicate $\chi \in \mathcal{P}(|Y| \times P(|X|))$ defined as

$$\chi(y, A) \;\equiv\; \forall x{:}|X|.\, \rho(y, x) \leftrightarrow A(x) \;\;.$$

4 Assemblies over Partial Combinatory Algebras

For nontrivial pca's $\mathcal{A}$ the realizability toposes $\mathsf{RT}(\mathcal{A})$ may look quite wild in the sense that it is difficult to compute semantics in it. The reason essentially is that $\mathsf{RT}(\mathcal{A})$ is not well-pointed. However, it does contain a most well-behaved full subcategory, the category of so-called $\neg\neg$-separated objects, i.e. those objects A for which $\forall x, y{:}A.\neg\neg x{=}y \Rightarrow x{=}y$ holds in $\mathsf{RT}(\mathcal{A})$. Equivalently, one may characterise $\neg\neg$-separated objects as subobjects of the $\nabla(I)$'s (as A has $\neg\neg$-closed equality iff the unit $\eta_A : A \to \nabla(\Gamma(A))$ (for $\Gamma \dashv \nabla$) is monic). More concretely, an object is $\neg\neg$-separated iff it is isomorphic to an object $X = (|X|, \sim_X)$ of $\mathsf{RT}(\mathcal{A})$ where $x_1 \sim_X x_2$ is inhabited iff $x_1 = x_2$. Thus, the full subcategory $\mathsf{Sep}_{\neg\neg}(\mathsf{RT}(\mathcal{A}))$ of $\neg\neg$-separated objects of $\mathsf{RT}(\mathcal{A})$ is equivalent to the category $\mathsf{Asm}(\mathcal{A})$ of *assemblies over* $\mathcal{A}$ which we are going to define next.

An *assembly (over $\mathcal{A}$)* is a pair $X = (|X|, ||\cdot||_X)$ where $|X|$ is a set and $||\cdot||_X : |X| \to \mathcal{P}(\mathcal{A})$ such that $||x||_X \neq \emptyset$ for all $x \in |X|$. We write $e \Vdash_X x$ for $e \in ||x||_X$ and say that e *is a realizer for* x. A morphism in $\mathsf{Asm}(\mathcal{A})$ from X to Y is a function $f : |X| \to |Y|$ *realizable* by some $e \in \mathcal{A}$ meaning that $\forall x \in |X|.\forall a \in ||x||_X.\, e{\cdot}a \downarrow \wedge\, e{\cdot}a \in ||f(x)||_Y$. Obviously, the category $\mathsf{Asm}(A)$ is well-pointed. One can show without pain that $\mathsf{Asm}(\mathcal{A})$ is also regular, locally cartesian closed and has finite colimits. Moreover, it has got a *generic* mono $m_{Tr} : Tr \rightarrowtail Prop$ where $Prop = \nabla(\mathcal{P}(\mathcal{A}))$, $|Tr| = \mathcal{P}(\mathcal{A})\backslash\{\emptyset\}$, $||A||_{Tr} = A$ and m_{Tr} is the inclusion from $\mathcal{P}(\mathcal{A})\backslash\{\emptyset\}$ into $\mathcal{P}(\mathcal{A})$. This mono m_{Tr} is generic in the sense that for every subobject $m : P \rightarrowtail A$ there is a morphism $\chi : A \to Prop$ with $m \cong \chi^* m_{Tr}$, i.e.

$$\begin{array}{ccc} P & \longrightarrow & Tr \\ {\scriptstyle m}\downarrow & \lrcorner & \downarrow{\scriptstyle m_{Tr}} \\ A & \xrightarrow[\chi]{} & Prop \end{array}$$

Notice, however, that unlike in a topos χ is in most cases not uniquely determined by m.[15] It can be shown that $\mathsf{RT}(\mathcal{A})$ can be obtained from $\mathsf{Asm}(\mathcal{A})$ as its *exact completion*, i.e. by freely adding so-called exact[16] quotients (e.g. Ω is obtained as the quotient of *Prop* by logical equivalence $\leftrightarrow$).

A further attractive feature of $\mathsf{Asm}(\mathcal{A})$ is that it contains a non-trivial small full internal subcategory $\mathsf{Mod}(\mathcal{A})$ of so-called "modest sets" which is complete internal to $\mathsf{Asm}(\mathcal{A})$. An assembly X is called *modest* iff

$$\forall x_1, x_2{:}|X|.\forall e{:}\mathcal{A}.\; e \in ||x_1||_X \cap ||x_2||_X \Rightarrow x_1 = x_2$$

i.e. iff every $e \in \mathcal{A}$ realizes at most one element of $|X|$. More generally, a morphism $a : A \to X$ in $\mathsf{Asm}(\mathcal{A})$ is called a *family of modest sets* iff for all

[15] For example for $id_1 : 1 \to 1$ we have $id_1 \cong \chi^* m_{Tr}$ if and only if $\chi(*) \neq \emptyset$.

[16] An *exact quotient* of an equivalence relation $r = \langle r_1, r_2\rangle : R \rightarrowtail A{\times}A$ is a coequalizer $q : A \twoheadrightarrow Q$ of r_1 and r_2 for which (r_1, r_2) is a kernel pair (i.e. aRb iff $q(a) = q(b) \in Q$).

$x : 1 \to X$ the object x^*A is a modest set, i.e. iff

$$\forall a_1, a_2{:}|A|.\, a(a_1) = a(a_2) \Rightarrow \forall e{:}\mathcal{A}.\, e \in ||a_1||_A \cap ||a_2||_A \Rightarrow a_1 = a_2$$

We write $\mathcal{P}$ for the collection of families of modest sets in $\mathsf{Asm}(\mathcal{A})$. One can show that $\Pi_u a \in \mathcal{P}$ whenever $a \in \mathcal{P}$ and there is a generic family $Prf \to Prop$ for $\mathcal{P}$. This allows one to interpret the Calculus of Constructions in $\mathsf{Asm}(\mathcal{A})$ with $\mathcal{P}$ providing a *proof-relevant* interpretation of the type of *impredicative* propositions.

5 Toposes vs. Set Theory

In many books and papers on categorical logic or topos theory one often reads that toposes provide models of "intuitionistic set theory". In a sense that's right and in another sense that's wrong. Certainly every topos with a natural numbers object provides a model of constructive higher order arithmetic and that's a framework where most of mathematics can be performed. On the other hand intuitionistic Zermelo-Fraenkel set theory (IZF) is definitely stronger than higher order arithmetic as the former proves the consistency of the latter. Moreover, there are mathematical theorems (like *Borel determinacy* etc.) which can be proved in set theory but *not* in higher order arithmetic.

Thus, there arises the question whether one can strengthen the notion of topos so that one arrives at a type theory as strong as IZF. The answer to this question is to postulate in a topos $\mathcal{E}$ with natural numbers object N a so-called *universe*, i.e. a collection $\mathcal{S}$ of maps in $\mathcal{E}$ such that

(1) $\mathcal{S}$ is stable under pullbacks along arbitrary morphisms in $\mathcal{E}$, i.e. for every pullback

$$\begin{array}{ccc} B & \longrightarrow & A \\ {\scriptstyle b}\downarrow & \lrcorner & \downarrow{\scriptstyle a} \\ J & \xrightarrow[f]{} & I \end{array}$$

in $\mathcal{E}$ the map b is in $\mathcal{S}$ whenever a is in $\mathcal{S}$

(2) $\mathcal{S}$ contains all monos in $\mathcal{E}$

(3) $\mathcal{S}$ is closed under composition

(4) $\Pi_a b$ is in $\mathcal{S}$ whenever a and b are in $\mathcal{S}$

(5) there is a *generic family* for $\mathcal{S}$, i.e. a map $El : E \to U$ in $\mathcal{S}$ such that for every $a : A \to I$ in $\mathcal{S}$ there is a $\chi : I \to U$ with

$$\begin{array}{ccc} A & \longrightarrow & E \\ {\scriptstyle a}\downarrow & \lrcorner & \downarrow{\scriptstyle El} \\ I & \xrightarrow[\chi]{} & U \end{array}$$

(6) the terminal projection $N \to 1$ is in $\mathcal{S}$

(7) the terminal projection $\Omega \to 1$ is in $\mathcal{S}$.

One should think of $\mathcal{S}$ as the collection of families of "small" types and El as a universal family of small types where U is the "big" type of (codes of) small types and $El(a)$ is the small type associated with every $a \in U$. Necessarily families of small types are closed under reindexing (condition (1)). Condition (2) says that all subterminals are small types. Conditions (3) and (4) express that small types are closed under *disjoint sums* and *dependent products* of families of small types indexed over a small type. Conditions (6) and (7) say that N and Ω are small types. It has been shown recently by the author that *all Grothendieck toposes and all realizability toposes do contain a universe* in the above sense.

Notice that a universe in **Set** necessarily has strongly inaccessible cardinality as it is (a) closed under powersets and (b) regular (as it is closed under disjoint unions of families whose index set is in the universe). In a sense a universe as above is something like a "non-set-theoretic" version of a Grothendieck universe.[17]

Employing methods of [JM] from a universe $\mathcal{S}$ in a topos $\mathcal{E}$ with natural numbers object one can construct[18] a so-called *initial* ZF*-algebra* playing the role of the *cumulative hierarchy* in ordinary set theory.

References

[Jac] B. Jacobs *Categorical Logic and Type Theory* North Holland (1999).

[Joh] Peter T. Johnstone *Sketches of an Elephant. A Compendium of Topos Theory* 2 vols., Oxford Univ. Press (2002).

[JM] A. Joyal, I. Moerdijk *Algebraic Set Theory* Cambridge University Press (1995).

[LS] F. W. Lawvere, S. H. Schanuel *Conceptual Mathematics. A First Introduction to Categories.* Cambridge Univ. Press (1997).

[MLM] S. MacLane, I. Moerdijk *Sheaves in Geometry and Logic. A First Introduction to Topos Theory* Springer (1992).

[Str] T. Streicher *Semantics of Type Theory* Birkhäuser (1991).

[17] As pointed out to me independently by Bill Lawvere and Alex Simpson the above mentioned closure under small disjoint sums is actually a stronger requirement than Fraenkel's *replacement axiom* claiming this closure property only for families *definable* in the language of first order set theory. (Set theoretically speaking, a small inner model need not be a Grothendieck universe!)

[18] factorizing trees modulo *bisimulation*