Journal of Pure and Applied Algebra 19 (1980) 103–125
© North-Holland Publishing Company

THE AXIOM OF CHOICE

Peter FREYD

Department of Mathematics, University of Pennsylvania, Philadelphia, PA19104, USA

For every complete topos Fourman has described an interpretation of set-theory [1], to wit, a set of "true" first-order sentences in the predicates of set theory (equality and membership) which contains all Zermelo–Fraenkel axioms and which is closed under intuitionistic deduction. If the topos is TWO-VALUED, that is, if the terminator has just two subobjects, then the Fourman interpretation is complete – every sentence or its negation is "true." If the topos is BOOLEAN, that is, if the lattice of subobjects of each object is a boolean algebra, then (and only then) the Fourman interpretation is closed under classical, not just intuitionistic, deduction.

We say that a topos is AC, short for axiom of choice, if every epimorphism is left-invertable. It's easy to find complete two-valued boolean topoi which fail to be AC but such does not suffice: for two different reasons the Fourman interpretation may still include the axiom of choice.

For example, let G be any non-trivial group and consider the topos $\mathscr{S}^G$ of G-sets. The map from the regular representation to the terminator, $G \to 1$, is not invertable, hence the topos is not AC. But the Fourman interpretation will say that every epimorphism does split. Given $f: A \to B$ in any topos, consider the pullback diagram

$$\begin{array}{ccc} Q & \longrightarrow & 1 \\ \downarrow & & \downarrow \\ A^B & \xrightarrow[f^B]{} & B^B \end{array}$$

where $1 \to B^B$ is the name of the identity map. The object Q may be viewed as the "object of left-inverses" of f. The sentence $\exists_g(gf = 1)$ will be interpreted as "true" iff $Q \to 1$ is epi. The forgetful functor from $\mathscr{S}^G$ to $\mathscr{S}$ preserves all structure in sight, hence if f is epic then so is f^B and consequently, so is $Q \to 1$.

A topos is said to satisfy the INTERNAL AXIOM OF CHOICE, IAC for short, if the endofunctor $(-)^B$ preserves epis for each B. We need a topos which fails IAC.

But the failure of IAC is not enough. Consider the full subcategory, $\mathscr{C}$, of $\mathscr{S}^Z$ (where Z is the infinite cyclic group) of those Z-sets in which all orbits are finite. $\mathscr{C}$ is a coreflective subcategory, closed under the formation of arbitrary subobjects and

finite products, which easily implies that $\mathscr{C}$ is a topos. Given a sequence of objects $B_0, B_1, B_2, \ldots$ in $\mathscr{C}$ we may construct the product $\prod_{B_n}$ by first taking the standard product in $\mathscr{S}^Z$ and then cutting down to the coreflection, which in this case is the union of all finite orbits. If B_n in the n-cycle, each n, then the product in $\mathscr{C}$ is empty. And from this we may conclude that $(-)^N$ fails to preserve epics, where N is the natural numbers object (in this case the ordinary natural numbers with the trivial Z-action): let $A = \sum B_n$ and $f : A \to N$ be the map which sends B_n to $n \in N$. Then in the above displayed pullback, $Q = \prod B_n$.

Nonetheless, the Fourman interpretation arising from $\mathscr{C}$ is no different from that arising from $\mathscr{S}$. The problem is a little more subtle and its illumination requires a few definitions.

In any complete topos we may recursively define a transfinite sequence of objects, indexed by the ordinals, by $P_\alpha = P(\sum_{\beta<\alpha} P_\beta)$, where $P(-)$ is the power-object functor ($P(A) = \Omega^A$). We say that B is a WELL-FOUNDED OBJECT if it appears as a subobject of some P_α. The WELL-FOUNDED PART of a topos is the full subcategory of well-founded objects and a WELL-FOUNDED TOPOS is one which is its own well-founded part.

The Fourman interpretation can not distinguish a topos from its well-founded part and an easy induction reveals that the well-founded objects of $\mathscr{C}$ are precisely those with trivial Z-action, hence the well-founded part of $\mathscr{C}$ is isomorphic to $\mathscr{S}$.

We wish, therefore, to describe a complete two-valued boolean *well-founded* topos which contains a sequence of non-zero objects $B_1, B_2, \ldots$ such that $\prod B_n = 0$. If any such topos exists then it is easy to see that we can ask that it be a Grothendieck topos and any boolean Grothendieck topos may be assumed to arise in the particular way as described in the next section.

1. Boolean sheaves

In an arbitrary topos we say that a subobject $B' \subset B$ is DENSE if it meets every non-empty subobject. An object, A, is a BOOLEAN SHEAF (sometimes *double-negation sheaf*) if for every dense $B' \subset B$ and map $B' \to A$ there exists a unique extension $B \to A$. A consequence of the axiomatic theory of sheaves is that the full subcategory of boolean sheaves is a topos and is easily verified to be a boolean topos [2]. It is a reflective subcategory and the reflection functor is exact. (It may, therefore, be viewed not as a subcategory but as a quotient structure. If a topos is viewed as an interpretation of intuitionistic higher-order logic, then the topos of boolean sheaves may be viewed as what the logicians call its *negative interpretation*.)

For a small category $\mathbb{A}$ we will denote the category of boolean sheaves in $\mathscr{S}^{\mathbb{A}^\circ}$ by $\mathscr{B}(\mathbb{A})$. Every boolean Grothendieck topos so arises, a fact we will not use directly but do use in order to narrow the search.

We thus seek a small category $\mathbb{A}$ such that $\mathscr{B}(\mathbb{A})$ is two-valued, well-founded and possesses a sequence of non-zero objects $B_1, B_2, \ldots$ such that $\prod B_n = 0$. We will, it

may be noticed, work in $\mathscr{B}(\mathbb{A})$ by "remote control." We spend a large part of the time in the ambient category, $\mathscr{S}^{\mathbb{A}^\circ}$, and most of that time among the representable functors. As always when working with functor categories, the Yoneda lemma plays a central role. For $A \in \mathbb{A}$ let H_A denote the contravariant functor represented by A. The Yoneda lemma says that the set of maps from H_A to an arbitrary contravariant functor T is naturally equivalent to $T(A)$. In particular, $\mathbb{A}$ reappears in $\mathscr{S}^{\mathbb{A}^\circ}$ as the full subcategory of representable functors.

2. The first example

Let $\mathbb{S}$ be the category whose objects are finite ordinals and whose maps are arbitrary functions between them. We will use the Von Neumann convention that an ordinal is the set of previous ordinals: $n = \{0, 1, 2, \ldots\ n-1\}$.

For the first example we define $\mathbb{A}$ as a subcategory of $\mathbb{S}$. The objects of $\mathbb{A}$ are the non-zero finite ordinals. A function $f: m \to n$ is in A iff $m \geq n$ and $n \xrightarrow{i} m \xrightarrow{f} n = 1_n$ where $i: n \to m$ is the inclusion map. We record:

Property 1. *The objects of $\mathbb{A}$ are finite non-zero ordinals and there exists a map $m \to n$ iff $m \geq n$.*

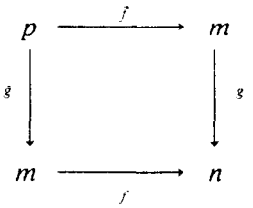
This property, by itself, allows us to compute the subobjects of 1 in $\mathscr{S}^{\mathbb{A}^\circ}$. The terminator, is, of course, the functor all of whose values are one-element sets. A subfunctor T' is determined by its *support*, that is by $\mathrm{Spt}(T') = \{n \mid T'(n) \neq \emptyset\}$. If $n \in \mathrm{Spt}(T')$ and if $m \geq n$ then, since there exists a function $T'(n) \to T'(m)$ we may conclude that $m \in \mathrm{Spt}(T')$. Hence T' is determined by the minimal element in its support. The lattice of subobjects of 1 consists of a descending sequence which converges down to the empty functor.

Corollary. *$\mathscr{B}(\mathbb{A})$ is two-valued.*

Proof. The inclusion of $\mathscr{B}(\mathbb{A})$ into $\mathscr{S}^{\mathbb{A}^\circ}$ preserves limits. In particular it preserves the terminator and it preserves monomorphisms, hence a subobject of 1 in $\mathscr{B}(\mathbb{A})$ is still such in $\mathscr{S}^{\mathbb{A}^\circ}$. But the definition of boolean sheaf clearly forbids any object that can appear as a dense proper subobject. All non-zero subobjects of 1 are dense, hence only one of them (the entire one) can be a boolean sheaf. □

We pause here to note that the lattice of subterminators in $\mathscr{S}^{\mathbb{A}^\circ}$ must be at least this complicated. In any functor category cartesian products preserve support. The sequence of boolean sheaves to be constructed must have the property that $B_n \to 1$ is dense in 1, hence $\bigcap B_n = 0$ implies that there exists a descending sequence of dense subobjects converging to 0.

Property 2. *If*

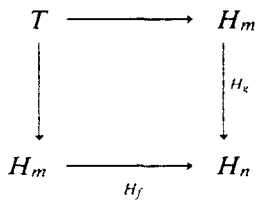


commutes in $\mathbb{A}$, *then* $f=g$.

Proof. In $\mathbb{S}$, $\bar{f}$ and $\bar{g}$ have a common left-inverse. □

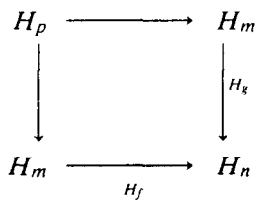
Corollary. *Distinct elements in* $H_n(m)$ *generate disjoint subfunctors.*

Proof. The subfunctor generated by $f: m \to n$ is the image of $H_f: H_m \to H_n$. Given another $g: m \to n$ consider the pullback



As in any regular category, $\mathrm{Im}(T \to H_n) = \mathrm{Im}(H_f) \cap \mathrm{Im}(H_g)$.

If $T \neq \emptyset$ choose p such that $T(p) \neq \emptyset$ and by the Yoneda lemma, a map $H_p \to T$. We then obtain a commutative square:



The full subcategory of representables is, as noted, isomorphic to $\mathbb{A}$ and Property 2 forces $f=g$. □

Let $\hat{2}$ be the reflection of $1+1$ in $\mathscr{B}(\mathbb{A})$. $\hat{2}$ is easily verified to be the power-object of 1 as defined in the category of boolean sheaves. It is an injective object in $\mathscr{S}^{\mathbb{A}^{\circ}}$: given $T' \subset T$ and a map $T' \to \hat{2}$ let $T'' \subset T$ be the union of all the subfunctors disjoint from T'. We may extend $T' \to \hat{2}$ to $(T' \cup T'') \to \hat{2}$ because there exists a map $T'' \to \hat{2}$ (e.g., $T'' \to 1 \to (1+1) \to \hat{2}$). $T' \cup T''$ is dense in T hence by the definition of boolean sheaf there exists an extension $T \to \hat{2}$.

Corollary. *The maps from H_n to $\hat{2}$ are collectively faithful.*

Proof. Given distinct elements $f, g \in H_n(m)$ we have just seen that they generate a subfunctor which decomposes into two halves, one containing f, the other g. This subfunctor may thus be mapped into $1+1$ in a way to separate f and g and by following with the inclusion functor we obtain a map into $\hat{2}$ which separates f and g. Finally, the injectivity of $\hat{2}$ allows us to extend to a map $H_n \to \hat{2}$ still, of course, separating f and g. □

Because $\mathbb{A}$ is countable we have

Corollary. *H_n may be embedded in a countable cartesian power, $\prod \hat{2}$.* □

Choose an embedding $H_n \to \prod \hat{2}$ and define $\hat{H}_n$ as the CLOSURE of its image that is, the union of all subfunctors in which H_n lies densely. $\prod \hat{2}$ is a boolean sheaf and any CLOSED subobject of such is again such (a subobject is closed if it lies densely in no larger subobject). Hence $\hat{H}_n$ is a boolean sheaf and it becomes a tautology (since H_n lies densely in $\hat{H}_n$) that it is a reflection of H_n in $\mathscr{B}(\mathbb{A})$.

Corollary. *$\mathscr{B}(\mathbb{A})$ is well-founded.*

Proof. The well-founded part of any topos is closed under every conceivable operation: arbitrary subobjects, quotient objects, products, coproducts and power-objects. (It is trivial that a subobject of a well-founded object is again such. In any topos, $B \subset A$ implies $P(B) \subset P(A)$ hence if $B \subset P_\alpha$ then $P(B) \subset P(P_\alpha) \subset P_{\alpha+1}$. In any topos, if $B \to C$ is epic, then C appears as a subobject of $P(B)$. The formula $P_\alpha(\sum_{\beta<\alpha} P_\beta) = \prod_{\beta<\alpha} P(P_\beta)$ easily yields the closure under arbitrary products and coproducts.)

Clearly, $\hat{2}$ is a well-founded object (in fact, $\hat{2} = P_1$) and clearly, so is its countable power (in fact $\prod \hat{2} = P_\omega$), hence each $\hat{H}_n$ is well-founded. For any functor T the Yoneda lemma implies that the maps of the form $H_n \to T$ cover T. If T is a boolean sheaf then, a fortiore, the maps of the form $\hat{H}_n \to T$ cover T. Thus each object of $\mathscr{B}(\mathbb{A})$ is a quotient of a coproduct of well-founded objects and therefore, is itself well-founded. □

Property 3. *Given $f : m \to n$ and $g : m \to (n+1)$ in $\mathbb{A}$ there exist $h, h' : (m+1) \to m$ such that $hf = h'f$ and $hg \neq h'g$.*

Proof. We may define h, h' by $h(m) = n$, $h'(m) = f(n)$. Of course, $h(i) = h'(i) = i$ for $i < m$. □

Corollary. *Any partial map from H_n to H_{n+1} is empty.*

Proof. Suppose there were to exist $T \to H_{n+1}$ for some $0 \neq T \subset H_n$. Choose m such that $T(m) \neq \emptyset$ and by Yoneda, choose $H_m \to T$. Define $H_f = H_m \to T \to H_n$, $H_g = H_m \to T \to H_{n+1}$. Let $h, h' : (m+1) \to m$ be as described in Property 3. Then since $T \to H_n$ is monic, we have $H_{m+1} \xrightarrow{H_h} H_m \to T = H_{m+1} \xrightarrow{H_{h'}} H_m \to T$ which yields a contradiction since H_g factors through $H_m \to T$. □

Corollary. *There are no maps from H_n to $\hat{H}_{n+1}$.*

Proof. Suppose $H_n \to \hat{H}_{n+1}$ existed. Consider the pullback

$$\begin{array}{ccc} T & \longrightarrow & H_{n+1} \\ \downarrow & & \downarrow \\ H_n & \longrightarrow & \hat{H}_{n+1} \end{array}$$

We have just shown that $T = \emptyset$, hence the image of $H_n \to \hat{H}_{n+1}$ is disjoint from H_{n+1}. But H_{n+1} is dense in $\hat{H}_{n+1}$. □

The Yoneda lemma allows an immediate restatement:

Corollary. $\hat{H}_{n+1}(n) = \emptyset$. □

From which it is clear that

Corollary. $\prod_n \hat{H}_n = \emptyset$. □

As noted before, we thus have an epic $\sum \hat{H}_n \to \hat{N}$ which violates the internal axiom of choice. It is easy to see that $\sum \hat{H}_n$ may be embedded in the countable power $\prod \hat{2}$, and that the latter is the power-object of $\hat{N}$, that is, it is the real-numbers-object, $\mathbb{R}$. We may thus obtain an epic $\mathbb{R} \to \hat{N}$ which violates IAC. Hence in the Fourman interpretation $\mathbb{R}$ does not have a choice function and can not be well-ordered.

3. The second example

In the first example there are n^k maps from $n+k$ to n:

$$|\mathbb{A}(n+k,\ n)| = n^k$$

The fact that $\mathbb{A}$ is as desired follows from the three stated properties. One may show that those properties force $\mathbb{A}(n+k,\ n)$ to have at least n^k elements, that is, $\mathbb{A}$ is something of a minimal example.

For the second example we simply erase the absolute-value signs. Let $\mathbb{B}$ be the

category whose objects are the non-zero finite ordinals and define the morphisms from $n+k$ to n to be k-tuples of elements of n. Define composition via concatenation. To be precise, given $\langle a_0, a_1, \ldots, a_{b-1}\rangle \in (n+k+b,\ k+b)$ and $\langle b_0, b_1, \ldots, b_{k-1}\rangle \in (n+k,\ n)$ their composition is $\langle \bar{a}_0, \bar{a}_1, \ldots, \bar{a}_{b-1},\ b_0, b_1, \ldots, b_{k-1}\rangle \in (n+k+b,\ n)$ where $\bar{a}_i = \min(a_i,\ n+k-1)$.

The three properties in the last section are easily verified for $\mathbb{B}$. (For Property 3, let $h = \langle n\rangle$ and $h' = \langle n-1\rangle$, no dependence on f or g.)

(*A personal note.* I knew $\mathbb{B}$ before $\mathbb{A}$. $\mathbb{B}$ was found by peeling away the unneeded part of a much more complicated example that arose from considerations as described in section 10. The three Properties were found by peeling away unneccessary parts of a much more complicated proof. $\mathbb{A}$ was found by looking for an easily described concrete category with the right number of maps between objects. I have found no other.)

4. The two examples compared

Proposition. *Every object in* $\mathscr{B}(\mathbb{A})$ *has a linear ordering.*

Proof. For $p \in \mathbb{S}$ consider the functor $T_p : \mathbb{A} \to \mathbb{S} \xrightarrow{(\cdot, p)} \mathscr{S}$. If $f, g \in T_p(m)$ then f and g generate disjoint subfunctors. The proof is the same as for $H_p(m)$. T_p, therefore, may be embedded in $\mathbb{R}$ and, thereby, acquires a linear ordering. T_p in fact, has a canonical linear ordering: define $f < g$ if there exists i such that $f(i) < g(i)$ and $f(j) = g(j)$ all $j < i$.

Say that a functor is *special* if it is isomorphic to a principal subfunctor of some T_p. Note that the subfunctor generated by $h : n \to p$ is determined up to isomorphism by the equivalence relation on n induced by h and that, conversely, any equivalence relation on n so arises (for some p).

We show first that any non-zero functor, F, contains a special subfunctor. First a bit of notation: given k and $i < k$ let $s_i : (k+1) \to k$ be the function that sends the top element of $k+1$ to i. Fix $x \in F(n)$. For $f : m \to n$ and $i, j < n$ define $i \equiv j \pmod f$ if for all $g : k \to m$ it is the case that $F(s_i gf)x = F(s_j gf)x$. Note that $i \equiv j \pmod f$ implies $i \equiv j \pmod{gf}$. Choose $f : m \to n$ so as to maximize the equivalence relation induced on n. Then $F(s_i gf)x = F(s_j gf)x$ implies $i \equiv j \pmod f$. $y = (Ff)x$ generates a special subfunctor: if $h : n \to p$ realizes the equivalence relation on n induced by f then an easy induction shows that

$$k \xrightarrow{g} m \xrightarrow{f} n \xrightarrow{h} p = k \xrightarrow{g'} m \xrightarrow{f} n \xrightarrow{h} p$$

implies $(Fg)y = (Fg')y$; conversely, suppose $(Fg)y = (Fg')y$. For any $i < k$ we have $(Fs_i gf)x = F(s_i g'f)x$. But $s_i gf = s_{g(i)} gf$ and $s_i g'f = s_{g'(i)} g'f$ hence

$$\begin{aligned}(Fs_{g(i)}gf)x = (Fs_i gf)x = (Fs_i g'f)x = (Fs_{g'(i)}g'f)x = (Fs_{g'(i)})(Fg')y \\ = (Fs_{g'(i)})(Fg)y = (Fs_{g(i)}gf)x\end{aligned}$$

and $g(i) \equiv g'(i) \pmod f$.

By choosing a maximal family of pairwise disjoint special subfunctors of F we see that every functor contains a dense subfunctor isomorphic to a coproduct of special subfunctors. If we reflect into $\mathscr{B}(\mathbb{A})$ we see that every boolean sheaf is a coproduct of reflections of special subfunctors (coproducts as defined in $\mathscr{B}(\mathbb{A})$), and, hence that every object in $\mathscr{B}(\mathbb{A})$ can be embedded in a cartesian power of $\hat{2}$ and thus each object has a linear ordering. □

We now easily obtain:

Theorem. *The Fourman interpretation arising from $\mathscr{B}(\mathbb{A})$ contains the sentence that every object may be linearly ordered, but does not contain the axiom of choice.*

The Fourman interpretation arising from $\mathscr{B}(\mathbb{B})$ is quite different in this respect. If every set may be linearly ordered then it is clear that any family of non-empty finite sets has a non-empty product (just order the union and choose the minimum element from each). But:

Theorem. *There exists a sequence of objects $B_1, B_2, \ldots$ in $\mathscr{B}(\mathbb{B})$, each of which has two elements but $\prod B_n = 0$.*

Proof. We define B_n to be the functor such that $B_n(m) = \emptyset$ if $n > m$ and $B_n(m) = \{a, b\}$ if $m \geq n$. Given $\langle a_0, a_1, \ldots, a_{m-1}\rangle \in (m, p)$, then $B_n(p) \to B_n(m)$ is either the identity function or the twist function depending on whether $\{a_i \mid a_i < n-1\}$ is even or not. From the general theory it is easy to see that B_n is *double-negation separated,* that is, it is embedded in its reflection B_n. B_n easily satisfies

$$\forall_{x,y,z}((x=y)\vee(x=z)\vee(y=z))$$

and since reflections are exact, so does $\hat{B}_n$. A modification of Property 3 is needed: given $f : m \to n$ and $\alpha : H_m \to B_{n+1}$ there exist $h, h' : (m+1) \to m$ such that $hf = h'f$ but $H_h \circ \alpha \neq H_{h'} \circ \alpha$ (again let $h = \langle n\rangle$, $h' = \langle n-1\rangle$). Just as before, this implies that all partial maps from H_n to B_{n+1} are empty and consequently, that there are no maps from H_n to $\hat{B}_{n+1}$. Hence $\hat{B}_{n+1}(n) = \phi$ and $\prod \hat{B}_n = 0$. □

5. Choice objects

In any regular category an object A is projective iff every entire relation with A as source, contains a map. We say that an object B is CHOICE if every entire relation with B as *target* contains a map. Clearly AC is equivalent to the condition that each object is choice.

It is transparent that subobjects of choice objects are choice. If B is choice and $f : B \to B'$ epic, then $f^\circ : B' \to B$ is entire. If $g \subset f^\circ$, then one may readily infer that g is a left-inverse of f. In particular every quotient object of B appears as a subobject

and thus is choice. (A fact we will not need, but record, is that finite products of choice objects are choice. We *will* use the obvious case that the empty product is choice: every entire relation targeted at the terminator is already a map. We further record the following variation on a theme by Diaconescu: The following are equivalent for pre-topoi: coproducts of choice objects are choice; $1 + 1$ is choice; the pre-topos is boolean.)

In a topos each object has a universal entire relation, namely the universal relation $\ni : P(B) \to B$ restricted to its domain $P^+(B)$. It is easily checked that all entire relations targeted at B contain maps iff this one does (the name for the last is, of course, a "choice function").

Note that logical morphisms therefore preserve choice objects (unlike projectives but like injectives).

Lemma. *In a complete boolean topos an object is choice iff it is a coproduct of subterminators.*

Proof. Given entire $R : A \to \sum_I U_i$ let F be a maximal partial map contained in R. Let A' be the complement of the domain of F. If $A' \neq 0$ then for some $i \in I$ the relation

$$G = (A' \to A \xrightarrow{R} \sum U_i \xrightarrow{U_i^0} U_i) \cup F$$

is a non-empty partial-map but bigger than F.

Conversly, given a choice object, let B' be maximal among subobjects which are isomorphic to disjoint unions of subterminators. If the complement, B'', of B' were non-empty then since $B'' \to \mathrm{Im}(B'' \to 1)$ has a left-inverse (B'' is still choice) we obtain a contradiction. □

Some years ago I gave a long proof of:

Corollary. *A Grothendieck topos is* IAC *iff it is a boolean etendu.*

Proof. That IAC implies boolean is a well known variation on Diaconescu. Clearly, any boolean etendu is IAC.

For the converse, let G be a PROGENITOR, that is, an object whose subobjects form a generating set. Let $T \to P^+G$, $T \to G$ be a pair of maps that span the universal entire relation and let

$$\begin{array}{ccc} Q & \longrightarrow & 1 \\ \downarrow & & \downarrow \\ (P^+G)^T & \longrightarrow & (P^+G)^{P^+G} \end{array}$$

be a pullback. If we move to the slice-category obtained by slicing by Q, then $T \to P^+ G$ acquires a left-inverse and G becomes a choice object. As for all slices, G remains a progenitor and by the last lemma the terminator becomes a progenitor. □

6. The third example

By the AXIOM OF WELL-ORDERED CHOICE we mean the following sentence in set theory:

The product of any well-ordered family of non-empty sets is non-empty.

We may restate this axiom as:

If every entire relation with a given set as target contains a function then so does every entire relation with that set as source.

And in the language of the last section:

Every choice set is projective.

Our third example shows that the axiom of well-ordered choice does not imply the full axiom of choice, indeed it does not imply even THE AXIOM OF REAL-ORDERED CHOICE:

The product of any family of non-empty sets indexed by the reals is non-empty.

Consider the algebraic (but not equational) theory with two constants, 1 and s; three unary operations with values denoted as $\hat{x}$, $\bar{x}$ and $\underline{x}$, and two binary operations xy, $[x,y]$. The axioms:

Q1: $x1 = x = 1x$.
Q2: $x(yz) = (xy)z$.
Q3: $u[x, y]x = v[x, y]y \Rightarrow x = y$.
Q4: $sx = \hat{x}s$.
Q5: $\bar{x}x = \underline{x}\,x \Leftrightarrow x = 1$.
Q6: $\bar{x}xs = xs = \underline{x}\,xs$.
Q7: $y\bar{x} = z\bar{x} \Leftrightarrow yx = zx \Leftrightarrow y\,\underline{x} = z\,\underline{x}$.

The first two axioms are, of course, the standard axioms of monoids. The rest of the axioms are best left uninterpreted until each, in turn, is used.

Lemma. *The above axioms do not imply that* $s = 1$.

We defer the proof until the end of this section.

Let F be the free algebra generated by the constants. Besides the fact that F carries

the structure as proscribed we will use the fact that it has more than one element but not uncountably many.

Being a monoid, F may be viewed as a category (with a single object). As for any monoid, $\mathscr{S}^{F^\circ}$, and a fortiore $\mathscr{B}(F)$, is two-valued. We will show that the axiom of well-ordered choice holds in the Fourman interpretation arising from $\mathscr{B}(F)$ but not the axiom of real-ordered choice.

Given elements x, y in any monoid we will write $x \perp y$ if they generate disjoint left-ideals, that is, if $(Fx) \cap (Fy) = \emptyset$. Axiom Q3 says that if $x \neq y$, then $[x,y]x \perp [x,y]y$. As in Section 1 we may map $(F[x,y]x) \cap (F[x,y]y)$ to $\hat{2}$ in a way as to separate $[x,y]x$ and $[x,y]y$, and that map may be extended to a map $F \to \hat{2}$ which, afortiori, separates x and y. Since F is countable there exists an embedding $F \to \mathbb{R}$ and, as before, we may construct $\hat{F}$ as the closure of its image.

Q4 says that $sF \subset Fs$, hence that Fs is a two sided ideal. Any non-empty two-sided ideal is dense. The map $s : F \to F$ (which sends x to xs) thus has a dense image and its reflection $\hat{s} : \hat{F} \to \hat{F}$ is epic in $\mathscr{B}(F)$. But:

Lemma. *$\hat{s} : \hat{F} \to \hat{F}$ is not epic in $\mathscr{S}^{F^\circ}$.*

Proof. $\hat{s}$ is nowhere monomorphic, that is, there is no non-empty subobject $A \subset F$ such that $\hat{s}|A$ is monic: suppose not; let

$$\begin{array}{ccc} \mathfrak{A} & \longrightarrow & A \\ \downarrow & & \downarrow \\ F & \longrightarrow & \hat{F} \end{array}$$

be a pullback; then $s|\mathfrak{A}$ is monic and the non-triviality of F implies that there exists $1 \neq x \in \mathfrak{A}$; $\bar{x}x$ and $\underline{x}x$ are different by Q5, both are in $\mathfrak{A}$ but $\bar{x}xs = \underline{x}xs$ by Q6.

If $\hat{s} : \hat{F} \to \hat{F}$ were epic in $\mathscr{S}^{F^\circ}$ then, since F is projective there would exist a map $F \to \hat{F}$ such that $F \to \hat{F} \xrightarrow{\hat{s}} \hat{F}$ is the canonical inclusion of F into its reflection. Thus $\hat{s}$ would not be nowhere monomorphic. □

Corollary. *$\mathscr{B}(F)$ fails* IAC.

Proof. The inclusion of $\mathscr{B}(F)$ into $\mathscr{S}^{F^\circ}$ preserves limits and exponentiation, hence the pullback diagram

$$\begin{array}{ccc} Q & \longrightarrow & 1 \\ \downarrow & & \downarrow \\ \hat{F}^{\hat{F}} & \xrightarrow[\hat{s}^{\hat{F}}]{} & \hat{F}^{\hat{F}} \end{array}$$

may be viewed as such in both categories. IAC says that $Q \neq 0$, hence that $\hat{s}$ is epic in $\mathscr{S}^{F^\circ}$. □

$\hat{F}$ was constructed as a subobject of the reals. Let G be its complement. The map $\hat{s}+1 : (\hat{F}+G) \to (\hat{F}+G)$ is an epimorphism on the reals which in the Fourman interpretation can not have a left-inverse, and hence the axiom of real-ordered choice will fail.

In order to prove that the Fourman interpretation arising from $\mathscr{B}(F)$ satisfies the axiom of well-ordered choice it suffices to show that for every slice category $\mathscr{B}(F)/B$ it is the case that choice objects are internally projective. Since choice objects in complete boolean topoi were shown in the last section to be coproducts of subterminators, we must show — in each slice category — that any epic $A \to \sum V_i$, $V_i \subset 1$ yields a pullback diagram

$$\begin{array}{ccc} Q & \longrightarrow & 1 \\ \downarrow & & \downarrow \\ A^{\sum V_i} & \longrightarrow & \sum V_i^{\sum V_i} \end{array}$$

in which Q is well-supported, that is, $Q \to 1$ is epic. Define $A_i \subset A$ by the pullback diagram

$$\begin{array}{ccc} A_i & \longrightarrow & A \\ \downarrow & & \downarrow \\ V_i & \longrightarrow & \sum V_i \end{array}$$

Then $A = \sum A_i$ and $Q = \prod A_i^{V_i}$. V_i is the support of A_i hence $A_i^{V_i} = A_i + (V_i)$ is well-supported. It suffices to show – for each slice – that products of well-supported objects are well-supported. Suppose there were a counterexample in $\mathscr{B}(F)/B$. B can not be empty, hence there is a map $f : \hat{F} \to B$. The induced logical morphism $\mathscr{B}(F)/B \to \mathscr{B}(F)/\hat{F}$ would produce a counterexample in $\mathscr{B}(F)/\hat{F}$. We need consider just one slice.

It suffices to show that there is a single well-supported object in $\mathscr{B}(F)/\hat{F}$ which has a map into every well-supported object, that is, that there exists a map $g : B \to \hat{F}$ with a dense image such that for any map $f : A \to \hat{F}$ with dense image there exists $h : B \to A$ such that $g = hf$. We take g to be $\hat{s} : \hat{F} \to \hat{F}$.

Given $f : A \to \hat{F}$ let

$$\begin{array}{ccc} A' & \longrightarrow & A \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle f} \\ F & \longrightarrow & \hat{F} \end{array}$$

be a pullback. It suffices to find a dense ideal $\mathfrak{B} \subset F$ and a map $\mathfrak{B} \to A'$ such that $\mathfrak{B} \to A' \xrightarrow{f'} F = \mathfrak{B} \to F \xrightarrow{s} F$ because then the reflection of $\mathfrak{B} \to A' \xrightarrow{f'} F$ is $\hat{F} \to A \xrightarrow{f} F = \hat{s}$.

Let $\mathfrak{A}$ be the image of f'. Consider the pullback

$$\begin{array}{ccc} \mathfrak{A}^s & \longrightarrow & F \\ \downarrow & & \downarrow s \\ \mathfrak{A} & \longrightarrow & F' \end{array}$$

Pullbacks preserve denseness, hence $\mathfrak{A}^s = \{b \mid bs \in \mathfrak{A}\}$ is dense. Let $B \subset \mathfrak{A}^s$ be a maximal family among the sets with the property $(b,\ b' \in B) \wedge (b \neq b') \Rightarrow b \perp b'$. $\mathfrak{B} = FB$ is dense in $\mathfrak{A}^s$, hence in F. For each $b \in B$ chooce $a \in A'$ such that $f(a) = bs$. Map Fb to A' by sending xb to $x\bar{b}a$. (Q7 says that this is a map.) Then $Fb \to A \to F$ sends xb to $x\bar{b}bs = (xb)s$. $\mathfrak{B}$ is the disjoint union of all such (Fb)'s hence we obtain $\mathfrak{B} \to A$ such that $\mathfrak{B} \to A' \to F$ sends each x to xs. □

Finally, we turn to the consistency of the axioms Q1 through Q7. It suffices to construct a model with more than one element (if $s = 1$, then Q6 implies $\bar{x}x = \underline{x}x$ and Q5 would imply $x = 1$). The only easily describable model we have found not only has more than one element, it has $2^{\aleph_1}$ elements.

Let X be an uncountable set. (To avoid all further use of the axiom of choice, take X to be the set of countable ordinals). We define M to be the monoid of endofunctions on X which satisfy the conditions:

(M1) $f^{-1}(x)$ *is finite for all* x.

(M2) $f^{-1}(x)$ *has at most one element for all but countably many* x.

(M3) *Either* $f = 1_X$ *or* $X - f(X)$ *has the same cardinality as* X.

Our model is obtained as a quotient monoid of M. Define $f \equiv f'$ if $f(x) = f'(x)$ for all but finitely many x. (M1 is needed to make this a congruence.) If $f \not\equiv f'$ we need to construct (for Q3) $g \in M$ such that $gf \perp gf'$ in $M/\equiv$. Let $x_0, x_1, x_2, \ldots$ be a sequence in X such that there are no repeated elements in the sequence $f(x_0), f'(x_0), f(x_1), f'(x_1), \ldots$. Let $g \in M$ be such that $gf(x_{2n}) = gf(x_{2n+1})$ and $gf'(x_{2n+1}) = gf'(x_{2n-2})$ for all n. Suppose there were h, h' such that $hgf \equiv h'gf$. Then for all sufficiently large n

$$hgf(x_{2n}) = hgf(x_{2n+1}) = h'gf'(x_{2n+2}) = hgf(x_{2n+2})$$

and the function hgf fails M1.

We let s be any monic element of M other than 1. Ms is easily seen to be the set of all elements in M other than 1, which yields a unary operation to satisfy Q4. Given any $f \neq 1$, we seek $\bar{f}$, $\underline{f}$ so that $\bar{f}f \not\equiv \underline{f}f$ (Q5), $\bar{f} \mid (fs(X)) = 1_{fs(X)} = \underline{f} \mid (fs(X))$ (Q6) and $\bar{f}(X) = f(X) = \underline{f}(X)$ (Q7). M2 says that $f(X) - fs(X)$ has the same cardinality as X. $\bar{f}$ and $\underline{f}$ may therefore be constructed by extending the identity function on $fs(X)$ to monic functions that map $X - fs(X)$ onto $f(X) - fs(X)$, taking care that $\bar{f} \mid (f(X) - fs(X))$ and $\underline{f} \mid f(X) - fs(X))$ disagree infinitely often. □

(*For the record:* the Fourman interpretation arising from any monoid M satisfies the axiom of well-ordered choice iff M can carry the further algebraic structure of one constant s and two binary operations $\langle x, y\rangle$, $\langle x, y\rangle'$ such that

$$(xs = zy) \quad \Rightarrow \quad (\langle x, y\rangle xs = \langle x, y\rangle' ys),$$

$$(z\langle x, y\rangle x = z'\langle x, y\rangle x) \quad \Rightarrow \quad (z\langle x, y\rangle' = z'\langle x, y\rangle').$$

The existence of such a structure, note, is an elementary condition on M.)

7. The first two examples extended

Let κ be any ordinal and define $\mathbb{A}_\kappa$ as the category whose objects are non-zero ordinals less than κ and whose maps are functions of the form $f : \alpha \to \beta$ where $\beta \subset \alpha$ and $f|\beta$ is the identity function. Our previous example is the case $\kappa = \omega$. Property two of section two is clearly true for $\mathbb{A}_\kappa$ any κ, hence $\mathscr{B}(\mathbb{A}_\kappa)$ is well-founded. Property three is true whenever κ is a limit ordinal and thus, in that case, $\prod \hat{H}_\alpha = 0$. Property one, of course, must be restated but when done so it easily implies that the lattice of subterminators in $\mathbb{A}_\kappa$ is $(\kappa+1)^\circ$. If κ, therefore, is the first ordinal of a given cardinality, then any family, $\{B_i\}_I$, $|I| < |\kappa|$, of non-zero subobjects in $\mathscr{B}(\mathbb{A}_\kappa)$ has a non-zero product.

To define $\mathbb{B}_\kappa$ we must adjust our previous conventions. The objects of $\mathbb{B}_\kappa$ are all ordinals (including zero) less than κ. Given $\alpha \geq \beta$ there is a unique ordinal $(\alpha - \beta)$ such that α is the *ordered sum* $\beta + (\alpha - \beta)$ (first β then $(\alpha - \beta)$). We define $\mathbb{B}_\kappa(\alpha, \beta)$ to be the set of functions from $\alpha - \beta$ to $\bar{\beta} = \{\gamma \mid \gamma \leq \beta\}$. Given $g \in \mathbb{B}_\kappa(\gamma, \alpha)$, $f \in \mathbb{B}_\kappa(\alpha, \beta)$ note that $\gamma - \beta = (\alpha - \beta) + (\gamma - \alpha)$. Define $(g \circ f) \in \mathbb{B}_\kappa(\gamma, \beta)$ so that $(g \circ f)|(\alpha - \beta) = f$ and $(g \circ f)|(\gamma - \alpha) = \min(g, \beta)$. The remarks on the three properties above are valid for $\mathbb{B}_\kappa$.

For κ the first ordinal of given cardinality we can verify (using the axiom of choice) for both $\mathbb{A}_\kappa$, $\mathbb{B}_\kappa$ that any family $\{\mathfrak{A}_i\}_I$, $|I| < |\kappa|$ of dense subobjects of H_α has a dense intersection. That is precisely what is needed to show that the reflection functor from the category of functors to the boolean part preserves not just finite products, but all products of cardinality less than $|\kappa|$.

The *diagonal functor* $\mathscr{S} \to \mathscr{S}^{\mathbb{C}^\circ}$, for any small category $\mathbb{C}$, is bicontinuous. (It sends a set I to the constant functor, also denoted I, all of whose values are the identity function on I). We therefore obtain functors $\mathscr{S} \to \mathscr{B}(\mathbb{A}_\kappa)$, $\mathscr{S} \to \mathscr{B}(\mathbb{B}_\kappa)$ each of which is cocontinuous, each is exact and each preserves products of cardinality less than $|\kappa|$. The fact that the target categories are two-valued is all that is needed to see that the functors are full. For any set I it is the case that $P(I)$, as defined in $\mathscr{B}$, may be constructed as $\prod_I \hat{2}$, hence if $|I| < |\kappa|$ then $P(\hat{I}) = 2^I$. Recalling our definition, $P_\alpha = P(\sum_{\beta<\alpha} P_\beta)$, we can state that $\mathscr{S} \to \mathscr{B}$ preserves P_α for $|P_\alpha| < |\kappa|$. If the language of set-theory is extended to include each of the standard ordinals as a constant then the Fourman interpretations arising from $\mathbb{A}_\kappa$ and $\mathbb{B}_\kappa$ are the same as that arising

from $\mathscr{S}$ if all quantification is restricted to sets of rank less than α if we choose κ to be the first ordinal such that $|\kappa| = |P_\alpha|$.

We have not succeeded in finding linear orderings for the objects of $\mathscr{R}(\mathbb{A}_\kappa)$, but we can extend the pathology of $\mathscr{R}(\mathbb{B})$. Let Z_2 be the two-element group, $\sum_\kappa Z_2$ the κ-fold abelian coproduct, $\sum_\kappa Z_2 \xrightarrow{d} Z_2$ the co-diagonal (each coordinate map is the identity.) Extend d to the κ-fold product $\sum_\kappa Z_2 = (Z_2)^\kappa$. Define $B_\beta : \mathbb{B}_\kappa^\circ \to \mathscr{S}$ to be the functor such that $B_\beta(\alpha) = \emptyset$ if $\alpha < \beta$ and $B_\beta(\alpha) = \{a, b\}$ if $\alpha \geq \beta$. Given $f : \alpha \to \gamma$ define $B_\beta(f)$ to be either the identity function or the twist function depending on whether $d(\hat{f})$ is 0 or 1, where $\hat{f} \in (Z_2)^\kappa$ is the function which sends ε to 0 iff $\alpha - \beta \leq \varepsilon$ or if $\varepsilon < \alpha - \gamma$ and $f(\varepsilon) = \beta$. Then each $\hat{B}_\beta$ will appear as a two-element object in $\mathscr{R}(\mathbb{B}_\kappa)$ but $\prod_{\beta<\kappa} \hat{B}_\beta = 0$. (It is curious that the axiom of choice seems to be needed for this construction: we have used its consistency to prove the consistency of a weak form of its negation.)

8. Exponential varieties

A full subcategory of a complete topos is an EXPONENTIAL VARIETY if it is closed under the formation of subobjects, cartesian products and the construction of power-objects. Any exponential variety is a BIVARIETY, that is, it is also closed under the formation of quotient objects and coproducts: if B' is a quotient of B, then B' appears as a subobject of $P(B)$; $\sum B_i$ appears as a subobject of $P(\sum B_i) = \prod P(B_i)$.

The well-founded part of any complete topos is, of course, its minimal exponential variety.

Let $\mathbb{C}$ be a small category and j a Grothendieck topology thereon. We wish to describe all exponential varieties in $\mathrm{Sh}_j(\mathbb{C})$. In the next two sections we consider the two special cases, to wit, the discrete and the boolean.

By a congruence on $\mathbb{C}$ we mean an equivalence relation such that $(x \equiv x') \wedge (y \equiv y') \Rightarrow xy \equiv x'y'$ and we exclude – by fiat – the possibility of identifying different identity maps. The quotient cateogy, $\mathbb{C}/\equiv$, in other words, may be viewed as having the same objects as $\mathbb{C}$. (For monoids, of course, this is no exclusion.)

Given a congruence E we define its j-CLOSURE by

$$a \bar{E} a' \quad \textit{iff} \quad \{b \mid baEba'\} \textit{ is } j\textit{-dense.}$$

We define its j-SEMI-DERIVATIVE by

$$a \leq_E a' \quad \textit{iff} \quad \textit{for all } b,\ \{c \mid \exists_{c'} c'ba = cba' \wedge cEc'\} \textit{ is } j\textit{-dense.}$$

This definition makes perfect sense for the case of a monoid. The universal quantifier in the case of an arbitrary category must be interpreted with tolerance: we really mean "for all b such that ba, ba' are defined." Semi-derivatives are not symmetric but otherwise satisfy the conditions for a congruence: $(x \leq y) \wedge (x' \leq y') \Rightarrow (xx' \leq yy')$ and $x \leq x$ and $(x \leq y) \wedge (y \leq z) \Rightarrow x \leq z$. The transitivity is

best left unproved for the moment. It follows easily from the characterization of the semi-derivative implicit in the proofs of the first two lemmas below. We define the j-DERIVATIVE of E as the symmetric part of its semi-derivative:

$$aE'a' \quad \textit{iff} \quad a \leq_E a' \textit{ and } a' \leq_E a.$$

Things that are equal to their derivatives are, of course, exponential things. We, therefore, say that E is a j-EXPONENTIAL CONGRUENCE if $E = E'$.

We say that $T: \mathbb{C}^\circ \to \mathscr{S}$ *respects* E if $aEa' \Rightarrow Ta = Ta'$.

Theorem. *The exponential varieties in* $\mathrm{Sh}_j(\mathbb{C})$ *are in natural correspondence with the j-exponential congruences. If E is j-exponential then the full subcategory of* $\mathrm{Sh}_j(\mathbb{C})$ *of those functors that respect E is an exponential variety and every exponential variety uniquely so arises.*

The proof rests on the following two lemmas:

Lemma. *If T respects E, then* $P_j(T)$ *respects E'.*

Proof. We may construct P_jT by defining $(P_jT)(A)$ to be the set of j-closed subobjects of $H_A \times T$. For $R \subset H_A \times T$, we write aRx instead of $\langle a, x\rangle \in R$. Given $a : B \to A$, $(P_jT)(a)$ sends $R \subset H_A \times T$ to $(aR) \subset H_B \times T$ where $b(aR)x \Leftrightarrow (ba)Rx$. We wish to show that $(a \leq_E a') \Rightarrow (aR \subset a'R)$.

It suffices to show that aR is contained in the j-closure of $a'R$, and for that it suffices to show that $aR \cap a'R$ is j-dense in aR, equivalently, that if $b(aR)x$ then $\{c \mid cba'Rxx\}$ is j-dense. By assumption, $\{c \mid \exists_{c'} c'ba = cba' \wedge cEc'\}$ is j-dense. But if cEc' then $c'x = cx$ and if, further, $c'ba = cba'$ then $cba'Rcx$. □

Lemma. *If E is the congruence induced by T, then E' is the congruence induced by* $P_j(\prod_I T)$ *for sufficiently large I.*

Proof. If the cardinality of I is at least as large as that of $\mathbb{C} \times \mathbb{C}$ then for any A there exists $x \in \prod_I T(A)$ such that $ax = a'x \Leftrightarrow aEa'$. We may, therefore, assume that T already had this property. Given $a, a' : B \to A$ such that $aR \subset a'R$ for all j-closed $R \subset H_A \times T$ we wish to show that $a \leq_E a'$. Let $x \in T(B)$ be such that $cx = c'x \Leftrightarrow cEc'$. Let $S \subset H_A \times T$ be the subobject generated by the pair $\langle a, x\rangle$, that is, dRy iff $\exists_{c'} d = c'a \wedge y = c'x$. By assumption aS is contained in the j-closure of $a'S$, hence $aS \cap a'S$ is j-dense in aS and since $1(aR)x$ we know that $\{c \mid ca'Rcx\}$ is j-dense. That is $\{c \mid \exists_{c'} ca' = c'a \wedge cx = c'x\}$ is j-dense. For all b it is still the case that $(baR) \subset (ba'R)$, all closed R, hence $a \leq_E a$. □

Given an exponential congruence E let $\mathscr{V} \subset \mathrm{Sh}_j(\mathbb{C})$ be the full subcategory of functors which respect E. As for any congruence, $\mathscr{V}$ is closed under the formation of subobjects and products. The first lemma says that $\mathscr{V}$ is closed under power-object construction.

Conversely, given an exponential variety $\mathscr{V} \subset \mathrm{Sh}_j(\mathbb{C})$ let E be the congruence induced by $\mathscr{V}$. We may choose a single $T \in \mathscr{V}$ such that E is induced by T. The last lemma says that $E = E'$. As before, we may assume that for all A there exists $x \in T(A)$ such that $ax = a'x \Leftrightarrow aEa'$. Let (H_A/E) denote the image of the map $H_A \to T$ which sends 1_A to x and note that $((H_A/E)a = (H_A/E)a') \Leftrightarrow aEa'$. Let F be any functor that respects E. For any $y \in FA$ the associated map $H_A \to F$ factors through H_A/E hence F may be covered by maps of the form $\widehat{H_A/E} \to F$ where $\widehat{H_A/E}$ is the reflection of $\widehat{H_A/E}$ in $\mathrm{Sh}_j(\mathbb{C})$. By construction H_A/E appears as a subobject of T, hence F is a quotient of a coproduct of objects in $\mathscr{L}$. Since $\mathscr{V}$ is a bivariety, $F \in \mathscr{V}$. □

Lemma. *If T respects E, then the image of $T \to \hat{T}$ respects $\bar{E}$.*

Proof. $T \to \hat{T}$ identities $x, x' \in TA$ iff $\{a \mid ax = ax'\}$ is j-dense. □

Lemma. *If E is induced by T, then $\bar{E}$ is induced by the image of $\prod_I T \to \prod_I T$ for sufficiently large I.* □

The four lemmas provide proofs for the following identities. Each of course, may be proved directly from the definition.

$$E \subset \bar{E}, \qquad \bar{E} = \bar{\bar{E}}, \qquad \bar{E}_1 \cap \bar{E}_2 = \overline{E_1 \cap E_2},$$

$$E_1 \subset E_2 \Rightarrow E'_1 \subset E'_2 \quad (\text{or } (E_1 \cap E_2)' \subset E'_1),$$

$$E' = (\bar{E}), \qquad E = \overline{E'}, \qquad E' \subset \bar{E}.$$

The last two say that on the lattice of closed congruences differentiation is a deflationary operation. (Note however, that for the identity congruence we have $I \subset I'$ hence $\bar{I} \subset \bar{I}' = I' \subset \bar{I}$. The derivative of I is its closure.) Define $E^{(0)} = \bar{E}$ and recursively define $E^{(\alpha)}$ for non-zero ordinals by $E^{(\alpha)} = \bigcap_{\beta < \alpha} (E^{(\beta)})'$. We understand ∞ to be larger than any ordinal. The smallness of $\mathbb{C}$ implies that there exists α such that $E^{(\alpha)} = E^{(\alpha+1)}$ hence $E^{(\alpha)} = E^{(\infty)}$. $E^{(\infty)}$ is the largest exponential congruence contained in $\bar{E}$.

Let O denote the maximal congruence: $\mathbb{C}/O$ is the preordered set naturally associated with $\mathbb{C}$. $O^{(\infty)}$ is the largest exponential congruence and $\mathrm{Sh}_j(\mathbb{C}/O^{(\infty)})$ is the smallest exponential variety, that is, the well-founded part of $\mathrm{Sh}_j(\mathbb{C})$. A site, therefore, yields a well-founded topos iff $O^{(\infty)} = \bar{I}$.

9. Discrete derivatives and normality

We specialize to the discrete topology: $\mathrm{Sh}_j(\mathbb{C}) = S^{\mathbb{C}^\circ}$. A sieve is dense iff it contains the identity map. Clearly $E = \bar{E}$ and $aE'a'$ iff

$$\forall_b \exists_{c,c'} (c'ba = ba') \wedge (ba = cba') \wedge cE1 \wedge c'E1.$$

E' depends only on Ker(E), the subcategory of endomorphisms congruent to identity maps. If $u \in \mathrm{Ker}(E')$ then, as just one piece of the definition of E', u has a left inverse. As for any congruence, $(vu = 1) \wedge (uE'1) \Rightarrow vE'1$. Thus each element in Ker(E') has a left-inverse in Ker(E'), which in turn has a left-inverse, forcing Ker(E') to be a subgroupoid of automorphisms.

By a LEFT-NORMAL SUBGROUPOID of $\mathbb{C}$ we mean a subcategory of automorphisms, $\mathbb{K}$, with the property that each identity map is in $\mathbb{K}$ and such that for all u; $A \to A \in \mathbb{K}$ and $b : B \to A$ there exists $v : B \to B$ in $\mathbb{K}$ such that $bu = vb$. If E is exponential then Ker(E) is clearly left-normal. Conversely, for any left-normal $\mathbb{K}$, define $a \equiv a'$ (mod $\mathbb{K}$) if there exists $u \in K$ such that $ua = a'$. Left-normality implies that this is a congruence and after that, it implies that it is an exponential congruence. Clearly $(1 \equiv u) \Leftrightarrow (u \in \mathbb{K})$. Thus the exponential varieties in $S^{\mathbb{C}^{\circ}}$ are in natural correspondence with the left-normal subgroupoids of $\mathbb{C}$.

We will indicate a proof at the end of this paper that the well-foundedness of $S^{\mathbb{C}^{\circ}}$ is not an elementary property on $\mathbb{C}$. There are a host of elementary conditions, however, that imply well-foundedness. The simplest is that all automorphisms be one. Hence the category of FD complexes is well-founded.

10. Boolean derivatives and the primordial example

A sieve on B is dense in the boolean (or double-negation) topology iff for all $b : C \to B$ there exists $c : D \to C$ such that cb is in the sieve. (It is the largest topology in which no empty sieves are dense). Hence

$$a\bar{E}a' \quad \text{iff} \quad \forall_b \exists_c (cba) E (cba'),$$

$$aE'a' \quad \text{iff} \quad \forall_b \exists_{c,c'} (c'ba = cba') \wedge c'Ec.$$

(There is a curious pair of binary operations on the lattice of congruences of any category. Define $[E_1, E_2]$ by

$$a[E_1, E_2]a' \quad \Leftrightarrow \quad \forall_b \exists_{c,c'} (c'ba) E_1 (cba') \wedge c' E_2 c.$$

Then $[E, I] = \bar{E}$, $[I, E] = E'$. The other binary operation is obtained by reversing the order of composition. Aside from the monotonicity in both variables, and the identities already observed for $[E, I]$ and $[I, E]$, I can find no other identities. Has this particular algebraic structure on the lattice of congruences, even of a monoid, been the object of anyone's attention?)

In all of our examples it has been the case that $O' = I$ (insured by property two for the first two examples and their extensions, and by Q3 for the third example.) Such is not typical. We will indicate at the end of the next section that the well-foundedness of $\mathscr{B}(\mathbb{C})$ is not an elementary property on $\mathbb{C}$. It is somewhat surprising therefore that the internal axiom of choice holding in the well-founded part of $\mathscr{B}(\mathbb{C})$ *is* an elementary property on $\mathbb{C}$. We consider here just the case for monoids. The general case is a straightforward elaboration.

Theorem. *The well-founded part of* $\mathscr{B}(M)$ *is* IAC *iff*

$$(*) \qquad \forall_a \exists_b [\forall_{cc'} (cba = c'ba \Rightarrow \exists_{d,d'} d'cb = dc'b)].$$

The proof is a consequence of a series of lemmas.

Lemma. $\mathscr{B}(\mathbb{C})$ *is* AC *iff* $\mathbb{C}$ *satisfies*

$$\forall_A \exists_{b : B \to A} \forall_{c,c'} \exists_{d,d'} d'cb = dc'b.$$

Proof. The condition is equivalent to

$$\forall_A \exists_{b : B \to A} \forall_{c,c'} (c'b) \bar{I} (c, b).$$

Since $\mathscr{B}(\mathbb{C}) = \mathscr{B}(\mathbb{C}/\bar{I})$ we may assume, without loss of generality that $I = \bar{I}$, equivalently, that H_A is embedded in its reflection $\hat{H}_A$ for each A.

A complete boolean topos is AC iff every object is choice and as seen in section five that, in turn, is equivalent to each object being a coproduct of subterminators. In a complete boolean topos, the last condition is equivalent, of course, to the statement that each non-zero object contain a non-zero subobject isomorphic to a subobject of 1. We shall call such subobjects, *partial-points*.

If $0 \neq T \in \mathscr{B}(\mathbb{C})$, then there exists a map of the form $\hat{H}_A \to T$. It is necessary and sufficient that $\hat{H}_A$ have a partial-point. Since H_A lies densely in $\hat{H}_A$ it is necessary and sufficient that H_A have a partial-point. We may assume that a partial-point in H_A (if it exists) is the image of a map of the form $H_B \to H_A$. The image of any map, in any regular category, is a partial-point iff the map is constant. $H_c : H_B \to H_a$ is constant iff for all $f, f' : F \to H_B$ it is the case that $f \circ H_b = f' \circ H_b$. Since the representables generate, it suffices to consider maps of the form $H_c H_{c'} : H_C \to H_B$. □

Lemma. *Suppose* M *is a monoid such that* $I = \bar{I}$. *Then* $\mathscr{B}(M)$ *is* IAC *iff it satisfies the condition*

$$\forall_a \exists_b \forall_{c,c'} (cba = c'ba) \Rightarrow (cb = c'b)$$

Proof. As seen in Section 5, $\mathscr{B}(M)$ is IAC iff there exists $0 \neq B \in \mathscr{B}(M)$ such that $\mathscr{B}(M)/B$ is AC. For any such B there exists $\hat{M} \to B$ and since any slice of an AC category is again such, we know that $\mathscr{B}(M)/\hat{M}$ would be AC. But for any $\mathbb{C}$ and $A \in \mathbb{C}$ it is the case that $\mathscr{B}(\mathbb{C})/H_A \simeq \mathscr{B}(\mathbb{C}/A)$. Let $\mathbf{tr}(M)$ be the Quillan translation category arising from M, that is, M sliced by its unique object. $\mathscr{B}(M)$ is IAC iff $\mathscr{B}(\mathbf{tr}(M))$ is AC. The condition of the lemma is precisely the last lemma's condition for $\mathbf{tr}(M)$ assuming $I = \bar{I}$. □

Clearly, then, the well-founded part of $\mathscr{B}(M)$ is IAC iff

$$\forall_a \exists_b \forall_{c,c'} (cba) O^{(\infty)} (c'ba) \quad \Rightarrow \quad (cb) O^{(\infty)} (c'b).$$

Since $I \subset O^{(\infty)} \subset O'$ we see that the well-founded part of $\mathscr{B}(M)$ being IAC implies

$$\forall_a \exists_b \forall_{c,c'} (cba = c'ba) \quad \Rightarrow \quad (cb) O' (c'b),$$

equivalently

$$\forall_a \exists_b \forall_{c,c'} (cba = c'ba) \quad \Rightarrow \quad \forall_e \exists_{d,d'} \, d'ecb = dec'b.$$

The universaly quantified variable e may be absorbed into c, c' yielding condition $(*)$ of the theorem.

It is remarkable that this apparently small consequence of IAC actually implies it. The trick is that this condition implies that O' is exponential. We need to show that $O' \subset O''$, that is, that $aO'a'$ implies that for all b there exist x, x' such that $(x'ba = xba') \wedge x' O' x$. Since $aO'a'$ implies $(ba)O'(ba')$ it suffices to show that $aO'a'$ implies a solution of $(x'a = xa') \wedge x' O' x$. Restated, it suffices to show in the presence of $(*)$ that $aO'a'$ implies the existence of x', x such that $x'a = xa'$ and for all y there exists z, z' such that $zyx' = z'yx$.

Let b be such that $(uba = u'ba) \Rightarrow \exists_{e,e'} e'ub = eu'b$ as guaranteed by $(*)$. Since $(ba)O'(ba')$ we may choose c, c' such that $c'ba = cba'$. We shall take $x' = c'b$, $x = cb$. For any y, $(ycba)O'(ycba')$ and we may choose d', d such that $d'ycba = dycba'$. Since $dycba' = dyc'ba$ we may apply the special property of b (with $u = d'yc$, $u' = dyc'$) to obtain e, e' such that $ed'ycb = e'dyc'b$. Let $z = e'd$, $z' = ed'$. Then $x'a = xa'$ and $zyx' = z'yx$.

Thus $(*)$ implies $O' = O^{(\infty)}$. We therefore finish by showing that $(*)$ implies

$$\forall_a \exists_b \forall_{c,c'} (cba = c'ba) \quad \Rightarrow \quad (cb) O' (c'b).$$

Given a choose b such that

$$\forall_a \exists_b \forall_{c,c'} (cba = c'ba) \quad \Rightarrow \quad \exists_{d,d'} \, d'cb = dc'b.$$

Suppose $(cba)O'(c'ba)$. We wish to show $(cb)O'(c'b)$, that is, for any e, we wish to show that there exist x', x such that $x'ecb = xec'b$. But $(ecba)O'(ec'ba)$, hence there exist f, f' such that $f'ecba = fec'ba$. $(*)$ now says there exist g, g' such that $gf'ecb = g'fec'b$ and clearly we may take $x' = gf'$, $x = g'f$. □

The negation of $(*)$ is $\exists_a \forall_b \exists_{c,c'} (cba = c'ba) \wedge (c \perp c')$ (recall that $c \perp c'$ iff $\forall_{d',d} d'c \neq dc'$.)

M satisfies this condition iff it carries the further algebraic structure of a constant s and two unary operators $[x]$, $[x]'$ satisfying the equation $[x]xs = [x]'xs$, and the non-equational condition $[x]x \perp [x]'x$.

We are driven to consider the free-algebra F generated by the constants and the equation: if F had an example for $y'[x]x = y[x]'x$ then every monoid would satisfy condition $(*)$ and every well-founded topos of the form $\mathscr{B}(M)$ would be IAC.

Let $\{s, [,],]'\}^*$ be the set of finite words of the four indicated symbols viewed as a monoid under concatenation. Let M be the submonoid of words in which the brackets (ignoring prime-marks) are correctly mated. M is the free algebra for the

operators and the monoid-equations but not $[x]xs = [x]'xs$. Let $\equiv$ be the congruence on M induced by the last equation. Then $F = M/\equiv$ is the free algebra we seek.

The congruence only removes or adds prime marks – it does not change the mating of the brackets nor the number of symbols between mated brackets. It can replace] with]' only when the number of symbols to the right of] is greater than the number of symbols between] and its left-mate. Hence $y'[x]x \equiv y[x]'x$ is impossible. Hence the independence of the axiom of choice.

Note that the last sentence does not need the fact that (*) is equivalent with IAC on the well-founded part of $\mathscr{B}(F)$ only the more straightforward half: IAC implies (*). If the Lawvere thesis that topoi may be viewed as interpretations of higher-order logic – particularly that part of the thesis as formalised by the Fourman interpretation – if that thesis had been understood in late 50's, then more than enough was then known about topoi to have made this example inevitable.

$\mathscr{B}(F)$ is well-founded, indeed $O' = I$ and as in the first three examples we may demonstrate the failure of IAC on the reals.

11. Degrees of well-foundedness

Some well-founded Grothendieck topoi are more well-founded than others. One measure arises as follows: since each object appears, by definition, as a subobject of P_α (recall: $P = P(\sum_{\beta<\alpha} P_\beta)$) there is a first α such that the subobjects of P_α generate, that is, such that P_α is a progenitor. For boolean topoi, $P_0 = 1$ is a progenitor iff the axiom of choice holds. Since, in boolean topoi, P_n, for each finite n, is just a finite copower of 1 it is the case that P_n is a progenitor iff P_0 is. In the primoridal and first three examples P_ω was the first to be a progenitor. The extensions of the first two examples allow us to raise the index of the first progenitor P_α arbitrarily large.

The sequence of P_α's is somewhat arbitrary. Consider instead the transfinite sequence of full subcategories defined by:

> *$A \in \mathscr{T}_\alpha$ iff A appears as a subobject of a cartesian product of power-objects from previous $\mathscr{T}_\beta$'s. That is, $\mathscr{T}$ is the result of closing $\bigcup_{\beta<\alpha} \mathscr{T}_\beta$ under the power-object construction, then cartesian products, then subobject formation.*

$\mathscr{T}_0$ consists, therefore, just of subterminators, and $\mathscr{T}_1$ of subobjects of cartesian powers of $P(1) = \Omega$. If $\mathscr{T}_\alpha$ contains a progenitor then (since the power-object of any progenitor is a cogenerator) $\mathscr{T}_{\alpha+1}$ is the entire category. In all the examples so far, $\mathscr{T}_1$ contains a progenitor. In the first example, but not the second, $\mathscr{T}_1$ is already the entire category.

The union of all the $\mathscr{T}_\alpha$'s is the well-founded part. The well-founded part is always a reflective subcategory and the reflection of a generating set is again such, hence in any Grothendieck topos there must exist α such that $\mathscr{T}_\alpha = \mathscr{T}_{\alpha+1}$.

As before, we let O be the maximal congruence on a small category $\mathbb{C}$. For any

topology, the congruence induced by $\forall_\alpha$ is $O^{(\alpha)}$, the αth derivative.

For any prime number p and p-primary torsion abelian group G, let $pG' = \{px \mid x \in G'\}$ for $G' \subset G$. Recursively define $p^\alpha G = \bigcap_{\beta<\alpha} p(p^\beta G)$. $p^\infty G$ is the *divisable part* of G. If $p^\infty G$ is trivial, G is said to be *reduced*. For any ordinal α there exist reduced G such that $p^\alpha G \neq 0$. We will assume, below, that G is reduced and not of finite exponent, in particular, $p^n G \neq p^{n+1} G$ all finite n.

Given G let M be the monoid of endofunctions on G of the form $p^n x + a$. M is the monoid of endofunctions on G generated by the translations and by multiplication by p and it may be viewed as a semi-direct product of N and G. We will denote its elements as pairs in $N \times G$ with product given by the formula

$$\langle n, a\rangle \langle m, b\rangle = \langle n+m, p^m a + b\rangle.$$

Lemma. *For all topologies on M other than the indiscrete, and for all $\alpha > 0$*

$$\langle n, a\rangle O^{(\alpha)} \langle n', a'\rangle \quad \textit{iff} \quad n = n' \textit{ and } a - a' \in p^{\omega\alpha} G.$$

($\omega\alpha$ is the αth limit ordinal.)

Proof. Let E be any congruence and $\bar{E}$ its boolean closure. Then $\langle n, a\rangle \bar{E} \langle n, a'\rangle$ implies $\langle 0, a - a'\rangle \in \mathrm{Ker}(\bar{E})$ because for any m and b, it implies that

$$\langle m, 0\rangle \langle n, a\rangle \langle 0, b - a'\rangle \bar{E} \langle m, 0\rangle \langle n, a'\rangle \langle 0, b - a'\rangle,$$

that is, $\langle m+n, b+a-a'\rangle \bar{E} \langle m+n, b\rangle$. For any $\langle m, b\rangle$ there exists x such that $x\langle m, b\rangle \langle 0, a - a'\rangle E\, x\langle m, b\rangle \langle 0, 0\rangle$, to wit, $x = \langle n, 0\rangle$.

For any congruence, the greater the family of dense ideals the larger its derivative. The discrete derivative is the smallest and among topologies that exclude the empty ideal as dense, the boolean derivative is the largest. We first show that the boolean and discrete derivative of $\bar{E}$ coincide and for that it suffices to show that the boolean derivative is contained in the discrete.

By direct translation, for the boolean topology

$$\begin{aligned} \langle n, a\rangle \bar{E} \langle n', a'\rangle \quad \text{iff} \quad & \forall \langle m, b\rangle \exists_{r,r',c,c'} (n+m+r' = n'+m+r) \\ & \wedge (p^{n+m} c' + p^n b + a = p^{n'+m} c + p^{n'} b + a') \\ & \wedge \langle r, c\rangle E \langle r', c'\rangle. \end{aligned}$$

Suppose $n \neq n'$. We any assume that $n' = n + k$, $k > 0$. We may choose $m = 1$ to see that $\langle n, a\rangle E' \langle n', a'\rangle$ implies

$$\forall_b \exists_{c,c'} (p^k - 1) p^n b = (a - a') + p^{n+1}(c' - p^k c).$$

Multiplication by $p^k - 1$, $k > 0$, on any p-primary torsion abelian group, is an automorphism. Hence $\langle m, a\rangle E' \langle n+k, a'\rangle$ implies $(p^n G) \subset (a - a') + p^{n+1} G$. Necessarily $0 \in (a - a') + p^{n+1} G$ hence $(a - a') + p^{n+1} G = p^{n+1} G$ and $p^n G \subset p^{n+1} G$. Thus $\langle n, a\rangle E' \langle n', a'\rangle$ implies $n = n$. For $E = \bar{E}$ we may choose $r = r' = 0$ and we may replace c with $c - c'$ to obtain

$$\langle n, a\rangle\ E'\ \langle n', a'\rangle \quad \text{iff} \quad (n = n')\wedge\forall\langle m, b\rangle\,\exists_c(\langle 0, c\rangle\ \langle m, b\rangle\ \langle n, a\rangle = \langle m, b\rangle\ \langle n', a'\rangle)\wedge(\langle 0, c\rangle \in \mathrm{Ker}(\tilde{E})).$$

Anything of the form $\langle 0, c\rangle$ is a unit. Thus the boolean derivative of a boolean-closed congruence is contained in the discrete derivative and they are equal.

For an arbitrary subgroup $H \subset G$ define $\langle n, a\rangle\ E_H\ \langle n', a'\rangle$ if $n = n'$ and $a - a' \in H$. (One reason this is a congruence is that all subgroups of G are *right-normal* in M.) We will know, by construction, that E_H is boolean-closed for all H in which we will be interested. (In fact, $H \subset p^\omega G$ suffices.) Then $\mathrm{Ker}(E'_H) = \{\langle 0, a\rangle \mid \forall_m \exists_{a' \in H} p^m a' = a\}$ and $E'_H = E_{p^\omega H}$. Starting with O, therefore, we have $O' = E_{p^\omega G}$ and by induction, $O^{(\alpha)} = E_{p^{\omega\alpha} G}$. □

For either the discrete or boolean topology (or any other topology with an elementary definition, e.g. the canonical topology) the statement that $\mathrm{Sh}_J(\mathbb{C})$ is *not* well-founded is an existential second-order condition on $\mathbb{C}$, to wit, the existence of an exponential congruence not equal to $\bar{I}$. Such a condition, of course, is preserved by ultraproducts.

If M, however, is a monoid in which $O^{(\omega)} = I$ but $O^{(n)} \neq I$ for any finite n, then $\mathscr{B}(M)$ is well-founded but for $\tilde{M}$, any non-principal countable ultrapower of M, $\mathscr{B}(\tilde{M})$ is easily seen not to be well-founded. ($xO^{(\omega)}y$ in $\tilde{M}$ if for all n, $x_i O^{(n)} y_i$ in M for almost all i.)

References

[1] M.P. Fourman, Sheaf models for set theory, J. Pure Appl. Algebra 19 (1980), in this volume.
[2] J.P. Freyd, Aspects of topoi, Bull. Austral. Math. Soc. 7 (1972).